

Forum:[Hack Forums](#)

Thread: [2025 Daily hacking training check-in thread](#)

Bastille - January 3, 2025, 5:11 am

2025 Day counter

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158

[/align]

1. PRESENTATION

For many, starting a new year means setting resolutions to achieve their goals. Beyond fitness and health, I want to invite those who are interested—and who sometimes lack a bit of motivation—to join this thread with the following objectives:

- ? Share your daily progress in the field (GitHub contributions, rooms on TryHackMe, etc.).
- ? Exchange ideas and get inspired by others to explore new things and see how others study/practice.
- ? Discuss common or interesting topics.
- ? Share your knowledge with others.
- ? Celebrate your achievements (it's important to feel proud and boost your ego).

2. THE LEARNING PYRAMID

For those who don't know, we retain information differently depending on how we learn. Here's the pyramid:

- ? Passive Reading : 10%
- ? Audio / Visual : 20%
- ? Demonstration : 30%
- ? Group Discussion : 50%
- ? Practice by doing : 75%
- ? Teach Others : 90%?

It's important to practice, but you can even go further by teaching to others in this thread what you did, improve your learning retention rate !

3. SOURCES TO PRACTICE

In my thread : <https://hackforums.net/showthread.php?tid=6263412> I shared many platforms where you can learn for free, I'm joining the list below to give you some ideas :

[If you begin, and you don't want to spend money, I highly recommend you to start with TryHackMe, then you can decide to spend more.]

- o [OverTheWire](#) (interesting if you begin, especially to get comfortable with Linux)
- o [TryHackMe](#) (the one I recommend if you begin)
- o [HackTheBox](#) (more advanced than TryHackMe, you can go on it after being familiar with cybersecurity)
- o [Root-Me](#) (general)
- o [Cryptohack \[url\]](#) (for learning modern cryptography)
- o [VulnHub \[url\]](#) (downloadable vulnerable virtual machines)
- o [TCM Security](#) (from CyberMentorChief mentioned earlier from YouTube's learning section)
- o [Let's Defend](#) (more oriented blue team)
- o [Cyber Defenders](#) (more oriented blue team)

4. HALL OF FAME / LEADERBOARD

I want to implement a leaderboard on this post based on the activity of the participants, let me know what do you think about it. Feel free to share any of useful metrics such as :

Profile

Yearly activity

In your daily post you're free to share :

- Links to rooms you've completed
- Badges you earned
- Streaks
- Contributions
- and any other thing that could be relevant !

I wish you all a good luck, a productive year, do the necessary to achieve your goals and become who you want to be.

Hackers - January 3, 2025, 5:12 am

100% agreed with this:
practice by doing & teach others

This is the best way for me to learn

Bastille - January 3, 2025, 5:15 am

(Jan 3, 2025 06:12 AM)nodes Wrote: [\[CITE\]](#) 100% agreed with this:
practice by doing & teach others

This is the best way for me to learn

Hope to see you participating to this thread in 2025 ! Let's bring back hackforums to what is used to be, a hacking forum ?

ttbr0 - January 3, 2025, 5:26 am

are you going to finally commit to learning programming?

Hackers - January 3, 2025, 5:32 am

(Jan 3, 2025 06:15 AM)Bastille Wrote: [\[CITE\]](#) Hope to see you participating to this thread in 2025 ! Let's bring back hackforums to what is used to be, a hacking forum ?

News & Happenings & Hacks

;)

Yes, this will be good!

I will see what I can do here

Bastille - January 3, 2025, 5:59 am

(Jan 3, 2025 06:26 AM)ttbr0 Wrote: [\[CITE\]](#) are you going to finally commit to learning programming? Yes sir ?

Step 1 : I need to consolidate my knowledge and experience regarding SOC analyst daily tasks because I want to work as a SOC analyst tier 2, as tier 1 doesn't sound really interesting ... and I think preparing myself to work as a SOC analyst is my priority (that's why I'm also studying on Letsdefend which has a lot of SOC learning content).

After that, I'll go back to the basics with Python. I'm already familiar with the language, including lists, dictionaries, and so on. My goal is to work on Python-based malware—both creating my own and analyzing existing ones—since my main interest in programming is for malware analysis and reverse engineering purposes.

If I feel comfortable enough, I'll then dive into C/C++. However, since it operates at a lower level and interacts more directly with the system, I think I'll need to spend some time learning the internals of Windows first (right ?)

There's just so much to learn haha

theapostlex - January 3, 2025, 9:36 am

Hello everyone, Glad to be here.

Bastille - January 3, 2025, 11:09 am

Just completed :

- 1 SOC case on letsdefend.io : really easy, didn't encounter difficulties. I really love to solve those SOC cases, some of them are from real case scenarios. With the free version of Letsdefend I can only do 15 cases per month. I'm thinking about upgrading to the premium version but Letsdefend is a little bit more expensive compared to tryhackme (annually : 17€ per month for letsdefend, and around 11€ per month for tryhackme) and for the time being I cannot subscribe to paid version for both of them lol

- 1 room on tryhackme.com : EEEEEZ, OSINT / email analysis

<https://tryhackme.com/r/room/threatinteltools>

Mooooookie - January 3, 2025, 12:00 pm

I'm not much a hacker myself, but I like the idea. Can always use something new for the community, that will help build engagement and spark conversation. Great idea.

RangoWorld - January 3, 2025, 1:20 pm

Nice one.

I shall look to learn more.

ttbr0 - January 3, 2025, 6:26 pm

(Jan 3, 2025 06:59 AM)Bastille Wrote: [\[CITE\]](#) Yes sir ?

Step 1 : I need to consolidate my knowledge and experience regarding SOC analyst daily tasks because I want to work as a SOC analyst tier 2, as tier 1 doesn't sound really interesting ... and I think preparing myself to work as a SOC analyst is my priority (that's why I'm also studying on Letsdefend which has a lot of SOC learning content).

After that, I'll go back to the basics with Python. I'm already familiar with the language, including lists, dictionaries, and so on. My goal is to work on Python-based malware—both creating my own and analyzing existing ones—since my main interest in programming is for malware analysis and reverse engineering purposes.

If I feel comfortable enough, I'll then dive into C/C++. However, since it operates at a lower level and interacts more directly with the system, I think I'll need to spend some time learning the internals of Windows first (right ?)

There's just so much to learn haha
interested in starting a github and maybe some community projects?

TENET - January 4, 2025, 8:38 am

"Recently, I've been studying the Kali Backdoor Factory..."(^)

Bastille - January 4, 2025, 10:11 am

(Jan 3, 2025 01:00 PM)Mooooookie Wrote: [\[CITE\]](#) I'm not much a hacker myself, but I like the idea. Can always use something new for the community, that will help build engagement and spark conversation. Great idea.

I would be glad to see you active here and share your progress :)

(Jan 3, 2025 02:20 PM)RangoWorld Wrote: [\[CITE\]](#) Nice one.

I shall look to learn more.

Yeahhh, that's the vibe man, feel free to share any thing you accomplished !

(Jan 3, 2025 07:26 PM)ttbr0 Wrote: [\[CITE\]](#) interested in starting a github and maybe some community projects?

I'm not against it but I'm not sure if my programs would be worth it. I still consider myself as a beginner regarding programming for the moment

(Jan 4, 2025 09:38 AM)TENET Wrote: [\[CITE\]](#) "Recently, I've been studying the Kali Backdoor Factory..."(^)

I didn't know this tool and it sounds interesting, did it work for you ? I see that you can inject different types of payloads, which one did you use ?

I see that the payload is injected into a legit program, did you try to run it on VirusTotal or hybrid analysis to see if they detect the payload ?

I'll definitely take a look at this tool, I'm not sure if it's really effective as I guess it can be easily detected, but that's still something interesting to be aware of.

Just completed my daily hacking training, I had an exhaustive day (just went back from hours at a tattoo shop)

As usual I went with Letsdefend.io and tryhackme.com. For the first one I solved a SOC case using utilman.exe as a LOLbas. However, surprisingly, I didn't find "utilman.exe" on the following site : <https://lolbas-project.github.io/#>

utilman.exe is a legit Windows system executable file, known as the "Utility Manager" or "Ease of Access Manager." It is used to provide accessibility tools on the login screen, such as Narrator, Magnifier, On-Screen Keyboard, or contrast settings. However it's possible to circumvent the primary objective of the tool to get a cmd.exe running as administrator.

Then with Tryhackme I went with an easy room : <https://tryhackme.com/r/room/pentestingfundamentals> as I'm tired and don't want to spend too much time on it today.

I already knew most of the things however there are few things I've learned. By the way I answered few questions online based on the CompTIA Security+ cert and one of them was about a document during a pentesting, called "Rules of Engagement" (ROE). I answered the question on the test, and completely forgot as I had the same question on tryhackme and wasn't able to answer without reading the text. This room was a good reminder.

I've also learned something new that would have been useful when I was conducting security tests on infrastructures, it's called OSSTMM (Open Source Security Testing Methodology Manual). I didn't spend time on the manual yet (<https://github.com/mtesauro/owasp-wte/blob/master/temp-projects/wte-docs/contents/usr/share/doc/WTE-Documentation/OSSTMM/OSSTMM.3.pdf>) but I think I should check it soon

ttbr0 - January 4, 2025, 3:34 pm

(Jan 4, 2025 11:11 AM)Bastille Wrote: [\[CITE\]](#) I'm not against it but I'm not sure if my programs would be worth it. I still consider myself as a beginner regarding programming for the moment you should make something useful or start a project that will teach you things. you already have all this theory and knowledge behind detection and analysis so write a program that helps you automate some of it or use it to push yourself to learn more. you can even try replicate functionality from other existing programs without looking at its source (think about how it would work in your head and code it). everyone starts as a beginner and theres no better way to learn something than to just dive in. i can shadow and help you out if you want.

Bastille - January 5, 2025, 1:41 am

(Jan 4, 2025 04:34 PM)ttbr0 Wrote: [\[CITE\]](#) you should make something useful or start a project that will teach you things. you already have all this theory and knowledge behind detection and analysis so write a program that helps you automate some of it or use it to push yourself to learn more. you

can even try replicate functionality from other existing programs without looking at its source (think about how it would work in your head and code it). everyone starts as a beginner and theres no better way to learn something than to just dive in. i can shadow and help you out if you want.

That's really kind thanks for the proposal [ttbr0](#) ! I've seen your post before going to bed and during the night I thought about a program. When I'm performing malware analysis, sometimes the malware also has other files such as .dll with it in the same folder so I need to upload them manually on VT too, one by one, and sometimes it takes time when there are like 20 files.

So I thought about the following tool :

- You put your VT API key in the program
- you select the files you want to analyze, it will firstly perform a md5 hash and upload the hash
- for each hash already known you'll see the result (how many AV detected it as malicious), green if 0/70, red if some AV flagged it
- for unknown hashes, the tool will propose you to upload the files

Maybe it already exists but that could be something interesting to make to learn new things.

EDIT : not even surprised that it already exists <https://github.com/VirusTotal/vt-cli> ?

ttbr0 - January 5, 2025, 1:52 am

(Jan 5, 2025 02:41 AM)Bastille Wrote: [\[CITE\]](#) That's really kind thanks for the proposal [ttbr0](#) ! I've seen your post before going to bed and during the night I thought about a program. When I'm performing malware analysis, sometimes the malware also has other files such as .dll with it in the same folder so I need to upload them manually on VT too, one by one, and sometimes it takes time when there are like 20 files.

So I thought about the following tool :

- You put your VT API key in the program
- you select the files you want to analyze, it will firstly perform a md5 hash and upload the hash
- for each hash already known you'll see the result (how many AV detected it as malicious), green if 0/70, red if some AV flagged it
- for unknown hashes, the tool will propose you to upload the files

Maybe it already exists but that could be something interesting to make to learn new things.

EDIT : not even surprised that it already exists <https://github.com/VirusTotal/vt-cli> ?

yeah it would definitely be a thing thats either standalone (like the tool you linked) or integrated into other programs like pestudio for triaging. it would be a good way to learn how to use a web api. you can also expand your tool to do more analysis on executable files so you can learn about them too like pe file formats and knowing what indicators to look for (again see pestudio).

Bastille - January 5, 2025, 3:42 am

(Jan 5, 2025 02:52 AM)ttbr0 Wrote: [\[CITE\]](#) yeah it would definitely be a thing thats either standalone (like the tool you linked) or integrated into other programs like pestudio for triaging. it would be a good way to learn how to use a web api. you can also expand your tool to do more analysis on executable files so you can learn about them too like pe file formats and knowing what indicators to look for (again see pestudio).

I'll definitely explore these things, thanks for the advice !

Tyr - January 5, 2025, 7:21 am

Would be cool to get a team going on HTB or something of that nature with the HF prefix. Nice work on the thread design as usual and thanks for the hard work you put into this.

Bastille - January 5, 2025, 8:03 am

(Jan 5, 2025 08:21 AM)Tyr Wrote: [\[CITE\]](#) Would be cool to get a team going on HTB or something of

that nature with the HF prefix. Nice work on the thread design as usual and thanks for the hard work you put into this.

Thanks buddy ! I think you're right, I'm mainly on THM but I definitely wouldn't be against exploring HTB

Feel free to share your progress / achievements here when you want

Today I've completed :

- 2 SOC analyst cases on letsdefend, but I do not agree with one of them, especially an answer
- I started 1 tryhackme room about DLL hijacking: <https://tryhackme.com/r/room/dllhijacking> but I wasn't able to finish, I was doing something else in parallel and the virtual machine was available only for 1 hour as I have a free account

- I've made a hacking tutorial thread : <https://hackforums.net/showthread.php?tid=6288583> not as HQ as other I've made but I'm in a rush to get the award I only have few days left before the 90th day, and to be honest I've been kinda disappointed regarding how few replies I've got for HQ hacking tutorials thread threads I've made previously, doesn't seem worth it to spend too much time on HQ threads unfortunately

EDIT : after that I studied on Linux too, I wanted to understand the differences between standard (.deb / .rpm / .aur) and non-standard (snpa, appimage, flatpak) packages. This year I plan to follow the LFS (Linux From Scratch) documentation, I think that will be an important achievement to improve my Linux knowledge

plops - January 6, 2025, 9:42 am

Thanks for making this.

I have done a lot of reading on small applications here and there. Still on my python adventure.

I started thm yesterday and completed Ohsint and agent sudo. Agent sudo was pretty frustrating but the first time i ever actually did a full 'hacking' thing. It was exciting and cant wait to do another one.

I will lose an hour of sleep tonight but i will at least start a module this evening.

I want to be able to contribute a couple of my own tutorials when i get there.

RootRXXT - January 6, 2025, 10:43 am

im only on HTB, but would like to be apart of a team, if you have a slot open, please dm me and I will join up!

Bastille - January 6, 2025, 11:50 am

(Jan 6, 2025 11:43 AM)RootRXXT Wrote: [\[CITE\]](#) im only on HTB, but would like to be apart of a team, if you have a slot open, please dm me and I will join up!

Hello, there is no team or things like that for the moment, the objective of the thread is to share your daily progress, you can share what room you've completed on HTB so people could discuss about it with you.

(Jan 6, 2025 10:42 AM)Robert Walker Wrote: [\[CITE\]](#) Thanks for making this.

I have done a lot of reading on small applications here and there. Still on my python adventure.

I started thm yesterday and completed Ohsint and agent sudo. Agent sudo was pretty frustrating but the first time i ever actually did a full 'hacking' thing. It was exciting and cant wait to do another one.

I will lose an hour of sleep tonight but i will at least start a module this evening.

I want to be able to contribute a couple of my own tutorials when i get there.

Python is definitely the programming language to go with, I discussed with another member about it and I need to devote more time to it. Even if I'm into cybersecurity, programming is my weak point.

Haha, but don't worry, you're right. Even doing 1 hour per day is good, the most important thing is constancy. Many people will rush for few days, then left for few weeks, you'll forgot most of the things.

I would be glad to see your tutorials, any kind of tutorial is useful, from beginners to advanced :)
Daily hacking :

Letsdefend : Streak 8 days ???

Completed SOC227 - Microsoft SharePoint Server Elevation of Privilege (Possible CVE-2023-29357)

Tryhackme : Streak 6 days ???

Almost finished the room I've started yesterday about DLL Hijacking (medium room), but I think I missed something because I wasn't able to complete the room. Will take a look at it tomorrow, I was limited to 1 hour because of the free account, there is a currently a 25% discount for subscription, that would be something like less than 8€ per month, seriously thinking about it ...

Bastille - January 7, 2025, 9:12 am

Just completed :

- 1 SOC case on letsdefend.io : SOC326 - Impersonating Domain MX Record Change Detected
It was quite interesting but didn't encounter difficulties

- 1 room on tryhackme.com : <https://tryhackme.com/r/room/investigatingwindows>

I had to help myself 2 times with a writeup, I'm definitely not comfortable on investigating Windows computers through the built-in tools (powershell, event viewer, ...). But I really enjoyed this room and I've learned many things

We can see that Windows Exploitation is my weak point compared to others on the graph :

I'll definitely spend more time on this, I also need to get familiar with EventID, Powershell, and so on, as I want to work as a SOC analyst.

Current streaks

Tryhackme : 7???

Letsdefend : 9???

captn_nemo - January 7, 2025, 9:32 am

I started my journey on THM today. I did a lot on HackTheBox, let's see what I can do here.

Bastille - January 7, 2025, 9:38 am

(Jan 7, 2025 10:32 AM)captn_nemo Wrote: [CITE](#) I started my journey on THM today. I did a lot on

HackTheBox, let's see what I can do here.

Nice to see that you join us ! I'm not familiar with HTB, but I've heard that it's usually harder than THM, is it true ? If so, THM will not be a big deal for you I guess :p

Feel free to share any room you complete, it's always a good opportunity for other members to learn more things and complete the same rooms

brandowservices - January 7, 2025, 11:41 am

This is good , i am very interested in joining and following the procedure, exactly as outlined.

capt_nemo - January 7, 2025, 12:08 pm

(Jan 7, 2025 10:38 AM)Bastille Wrote: [\[CITE\]](#) Nice to see that you join us ! I'm not familiar with HTB, but I've heard that it's usually harder than THM, is it true ? If so, THM will not be a big deal for you I guess :p

Feel free to share any room you complete, it's always a good opportunity for other members to learn more things and complete the same rooms

First User Flag done.

I can't make a comparison at the moment, I haven't seen enough. The Expose Box was easier on the one hand, but also a bit more confusing for me because it was very far away from the real world. I think HackTheBox is simply more real so far. But let's wait and see what happens over the next few days.

Bastille - January 7, 2025, 11:55 pm

(Jan 7, 2025 12:41 PM)brandowservices Wrote: [\[CITE\]](#) This is good , i am very interested in joining and following the procedure, exactly as outlined.

Feel free to share your progresses, what are you into ? Hacking ? Programming ? Something else ?

(Jan 7, 2025 01:08 PM)capt_nemo Wrote: [\[CITE\]](#) First User Flag done.

I can't make a comparison at the moment, I haven't seen enough. The Expose Box was easier on the one hand, but also a bit more confusing for me because it was very far away from the real world. I think HackTheBox is simply more real so far. But let's wait and see what happens over the next few days.

Oh I know what you mean. I'll do as much as I can this year on tryhackme and give a try in 2026 to HackTheBox

First User Flag ? Is this a room ? Feel free to share the link of the rooms so other members can take a look at it too :)

capt_nemo - January 8, 2025, 12:03 am

(Jan 8, 2025 12:55 AM)Bastille Wrote: [\[CITE\]](#) Feel free to share your progresses, what are you into ? Hacking ? Programming ? Something else ?

Oh I know what you mean. I'll do as much as I can this year on tryhackme and give a try in 2026 to HackTheBox

First User Flag ? Is this a room ? Feel free to share the link of the rooms so other members can take a look at it too :)

I got the User Flag and Root Flag in the [Expose](#) Box. They may be called rooms at THM.

Spoiler ([Click to View](#)) As I said, the user flag was simple, a bit of SQLi here and a bit of LFI there. The root flag was also relatively simple.

I think THM's tutorials are definitely better and more detailed, I haven't seen anything like that at HTB. I will definitely continue later (another day has already begun here).

Bastille - January 8, 2025, 8:38 am

Just completed :

- 1 SOC case on letsdefend.io : SOC101 - Phishing Mail Detected

Nothing really difficult, just a malicious email with a malicious URL a user clicked on. Nothing interesting to say. However I'm thinking to upgrading to the premium version as I'm limited to 15 SOC cases per month with the free version, but it's expensive (at least 16€ per month), there was a discount during the new year (50% off) but didn't take it ... Hope they will do one more discount

- 1 room on tryhackme.com : <https://tryhackme.com/r/room/blueprint>

Yesterday I said that my weak point was windows hacking / investigation, so I decided to complete a room based on Windows Exploitation. It was not easy for me, I had to help myself with a writeup but I discovered many tools such as :

- enum4linux (SMB)
- a nmap script for SMB (smb-enum-users, with others such as smb-enum-shares and smb-protocols)

In order to keep myself organized and easily find tools I've already used I use bookmarks on Firefox :

After that, I had to exploit few files in C:\Windows\System32\config\ called : SAM > store information about users, such as username and password

SECURITY > store information related to the system security and registry, it's used with SAM to decrypt the hashed passwords (you don't get the clear password, you just get the hash)

SYSTEM > store information about users privileges, authorizations and other things

I then used samdump2 to retrieve the hash, and then crackstation to crack the hash.

I think I'll continue with the rooms based on Windows, I should also continue with SAM exploits such as Pass-the-hash methods and so on. This will be done tomorrow

Letsdefend : Streak 10 days ???

Tryhackme : Streak 8 days ???

captn_nemo - January 8, 2025, 9:17 am

Check-in for Today.

Started the "Jr Penetration Tester" path today and completed the first 3 modules.

They were all really easy but I want to finish the whole path, I think it will help me at work too.

Bastille - January 8, 2025, 10:46 am

(Jan 8, 2025 10:17 AM)captn_nemo Wrote: [\[CITE\]](#) Check-in for Today.

Started the "Jr Penetration Tester" path today and completed the first 3 modules.

They were all really easy but I want to finish the whole path, I think it will help me at work too.

Nice mate ! Congrats on completing the first modules. Even if it felt like a walk in the park, haha, it's still good to warm up a bit before diving into the serious stuff ?

Can I ask you what do you do for living ? As you mentioned it could help you for your work I guess you're into cybersecurity, or at least IT ?

capt_nemo - January 8, 2025, 10:59 am

(Jan 8, 2025 11:46 AM)Bastille Wrote: [CITE](#) Nice mate ! Congrats on completing the first modules. Even if it felt like a walk in the park, haha, it's still good to warm up a bit before diving into the serious stuff ?

Can I ask you what do you do for living ? As you mentioned it could help you for your work I guess you're into cybersecurity, or at least IT ?

No, I don't work directly in security. I work as a DevOps architect and advise customers on scaling, monitoring and new developments.

Bastille - January 9, 2025, 1:13 am

Just completed :

1 SOC case on <https://letsdefend.io> : SOC250 - APT35 HyperScrape Data Exfiltration Tool Detected

STREAK : 11 ???

This one was interesting as it was based on a real incident, when you see a star ? on the SOC case that means it's a real incident that happened. It was related to APT35 group and data exfiltration.

1 room on <https://tryhackme.com> : [Anthem](#)

STREAK : 9 ???

Quite easy, didn't encounter difficulties, however during the room I had to browse a website unfortunately it was really slow (dont know if it was intentional or not) so instead of using Firefox I used CLI tools such as Curl. It was a good opportunity to get more familiar with CLI tools.

capt_nemo - January 9, 2025, 4:47 am

Check-in for today.

Unfortunately I didn't have much time today, so I just made a small module with XSS. But the streak is still alive.

Mexicano - January 9, 2025, 8:43 am

Daily check in.

I have found <https://overthewire.org/> project which is kinda interesting and well structured, so the user can have gamelike experience while doing it.

It is mainly Linux skills there and even thoe I have some Linux Admin courses behind my back, it's giving me hard time specially Level 6 -> 7 and Level 12 -> 13 if not mistaken where you have to deal with some hexdump file which was compressed few times. That was hell for me had to go to youtube to deal with it.

Currently for the past few days I've managed to get to " Bandit level 22 ", where some script needs to be created, but I got to part where I have insufficient permissions and the solutions I found on the internet are outdated.

Will update once more if manage to get through level 22, but if can't maybe will seek some help in their discord community where people are extremely helpful.

captn_nemo - January 10, 2025, 8:00 am

Check-In for today.

Did something with Command Injection. Streak day 4.

Bastille - January 10, 2025, 8:11 am

(Jan 10, 2025 09:00 AM)captn_nemo Wrote: [\[CITE\]](#) Check-In for today.

Did something with Command Injection. Streak day 4.

Nice to see you active in this thread ! I guess that you're talking about command injection on a web server, right ? Command injection is an attack but can get different forms depending on the target, such as Databases, Network, Systems, Web, ...

(Jan 9, 2025 09:43 AM)Mexicano Wrote: [\[CITE\]](#) Daily check in.

I have found <https://overthewire.org/> project which is kinda interesting and well structured, so the user can have gamelike experience while doing it.

It is mainly Linux skills there and even thoe I have some Linux Admin courses behind my back, it's giving me hard time specially Level 6 -> 7 and Level 12 -> 13 if not mistaken where you have to deal with some hexdump file which was compressed few times. That was hell for me had to go to youtube to deal with it.

Currently for the past few days I've managed to get to " Bandit level 22 ", where some script needs to be created, but I got to part where I have insufficient permissions and the solutions I found on the internet are outdated.

Will update once more if manage to get through level 22, but if can't maybe will seek some help in their discord community where people are extremely helpful.

Overthewire is really cool to start, especially to get familiar with Linux CLI and basic hacking stuff, but as you mentioned that you already have Linux Admin courses I understand that's not a big deal for you haha

Yeah of course ! Would love to hear from you sharing your progress, feel free to post when you want :) In case you're struggling because the solutions are outdated, feel free to ask on HF (in this thread, or maybe creating a new thread to get more visibility)

Miracula - January 10, 2025, 8:24 am

I am more into malware development than CTFs (mostly playing koth/ad with friends), can I check-in here as well to remind myself to work more on my projects? A little demotivated this week.

Bastille - January 10, 2025, 9:07 am

(Jan 10, 2025 09:24 AM)Miracula Wrote: [\[CITE\]](#) I am more into malware development than CTFs (mostly playing koth/ad with friends), can I check-in here as well to remind myself to work more on my projects? A little demotivated this week.

The goal of this thread is precisely to motivate members and share their progress, whether it's in hacking, cybersecurity, programming, or malware development.

By the way, I've set myself the goal of getting back into Python specifically to create malware and better understand how it works during my malware analysis. So I would definitely be glad if you share some stuff even in other languages ?

Just completed 1 SOC case on letsdefend : SOC235 - Atlassian Confluence Broken Access Control 0-Day CVE-2023-22515 and 1 tryhackme room : <https://tryhackme.com/r/room/registrypersistencedetection>

Miracula - January 11, 2025, 12:38 am

(Jan 10, 2025 10:07 AM)Bastille Wrote: [\[CITE\]](#) The goal of this thread is precisely to motivate members and share their progress, whether it's in hacking, cybersecurity, programming, or malware development.

By the way, I've set myself the goal of getting back into Python specifically to create malware and better understand how it works during my malware analysis. So I would definitely be glad if you share some stuff even in other languages ?

Thank you! Will do for sure in the future!

Bastille - January 11, 2025, 4:17 am

Just completed :

- 1 SOC case on letsdefend.io based on a CVE : ? SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation (CVE-2024-3400), that was really interesting

- 1 room on tryhackme.com : <https://tryhackme.com/r/room/chillhack> , this is labelled as an "easy room" but to be honest I've struggled and I had to help myself with a writeup, I've forgot a lot of things as I didn't use THM for a while, I definitely need to go back to some basics ...

Streaks :

Tryhackme : 11 ?

Letsdefend : 13 ?

Bastille - January 13, 2025, 2:52 am

I had to take a day off yesterday, completed 1 SOC case and replied to few questions on Tryhackme just to don't loose my streak

capt_nemo - January 13, 2025, 2:53 am

The same with me. I edited a few questions in the tutorial so as not to lose the Streak. Today I want to tackle the new HTB box and see if I can do it.

Bastille - January 13, 2025, 8:39 am

Just completed 1 SOC case on letsdefend.io, really easy, no difficulties encountered :
? SOC287 - Arbitrary File Read on Checkpoint Security Gateway [CVE-2024-24919]

Completed 1 basic room on tryhackme : <https://tryhackme.com/r/room/networkingconcepts>

I didn't feel ready good recently (sleeping disorders), hope I'll be in a better shape tomorrow to spend more time on these platforms.

I also want to work on some threads for HF

Streaks :

Tryhackme : 13?

Letsdefend : 15?

Metacenter - January 13, 2025, 11:45 am

I've completed the networking VM and am now diving into learning Kali Linux ?.
I'm on my way to becoming a cyber soldier!

Good luck to everyone, and have a happy hacking year!

7 - January 13, 2025, 12:05 pm

Love this!.

Eventually when I get AGI ill have more time to join in

Bastille - January 13, 2025, 1:13 pm

(Jan 13, 2025 12:45 PM)Metacenter Wrote: [\[CITE\]](#) I've completed the networking VM and am now diving into learning Kali Linux ?.

I'm on my way to becoming a cyber soldier!

Good luck to everyone, and have a happy hacking year!

I'm glad that you're already on track since your threads about learning hacking and networking.
You're on the right path, buddy!

Good luck to you as well. I hope you'll still be here at the end of the year so we can look back at this thread and say, "Damn, man, look how far you've come. You can be proud of yourself."

By the way, I noticed the part about ADD and meds. HF isn't just a hacking forum. If you ever need to talk or get help, there are other sections for that and people who are willing to listen (just avoid sharing personal information ?).

(Jan 13, 2025 01:05 PM)7 Wrote: [\[CITE\]](#) Love this!.

Eventually when I get AGI ill have more time to join in

Hope to see you active here, curious to know what you'll work / practice on ?

captn_nemo - January 13, 2025, 2:39 pm

Check-In.

I continued working on the Jr. Pentester Path today and have now reached the Networking Path.
Let's see if we can learn something there.

ubermensch38 - January 13, 2025, 3:33 pm

Hi ! Hope it's ok to hop in this late.

Doing a career change right now -- and hoping to get a helpdesk job in the upcoming months.

I've been doing a bit of HackTheBox and TryHackMe these past days (and even spent the entire yesterday trying to do a 4-way handshake attack on my WiFi lol)

Although I've decided to go full-blow on Google's Cybersecurity Certificate.

Will keep you guys updated.

Thanks

Bastille - January 13, 2025, 3:37 pm

(Jan 13, 2025 04:33 PM)ubermensch38 Wrote: [\[CITE\]](#) Hi ! Hope it's ok to hop in this late.

Doing a career change right now -- and hoping to get a helpdesk job in the upcoming months.

I've been doing a bit of HackTheBox and TryHackMe these past days (and even spent the entire yesterday trying to do a 4-way handshake attack on my WiFi lol)

Although I've decided to go full-blow on Google's Cybersecurity Certificate.

Will keep you guys updated.

Thanks

Hey buddy, welcome to HF, never too late to join, this is just the beginning of the year by the way ! Are you already familiar with IT ? Cybersecurity certs aren't overkilled for a helpdesk job ? I've worked in a helpdesk for years by the way

And if you're interested in cybersecurity I recommend you to check my thread : <https://hackforums.net/showthread.php?tid=6263412> I've made it as I wish I had it when I started to study cybersecurity 6 years ago (when I was a helpdesk tech).

Hope you hear your updates soon :) feel free to share you daily progresses here !

ubermensch38 - January 13, 2025, 5:51 pm

(Jan 13, 2025 04:37 PM)Bastille Wrote: [\[CITE\]](#) Hey buddy, welcome to HF, never too late to join, this is just the beginning of the year by the way ! Are you already familiar with IT ? Cybersecurity certs aren't overkilled for a helpdesk job ? I've worked in a helpdesk for years by the way

And if you're interested in cybersecurity I recommend you to check my thread : I've made it as I wish I had it when I started to study cybersecurity 6 years ago (when I was a helpdesk tech).

Hope you hear your updates soon :) feel free to share you daily progresses here !
Oh thanks a lot for the guide.

Getting into cybersecurity is my main goal (not sure what path yet) -- although I've seen that many people recommend getting a helpdesk gig first, so I'm aiming for that first.

Saw the Google's cybersecurity cert being recommended in a vid... and I went head first without thinking much lol.

CompTIA A+ feels a bit intimidating right now.

I'm doing the Technical Support Fundamentals Course (from Google) as well. Gonna pair it with some Professor Messer vids...

And then get the CompTIA A+ when I proved myself that I'm actually serious about this lol.

So first goal is to get 2h minimum each day total on these courses.

And I don't have IT experience besides high-school and some classes during college.

Going to dig further into your guide in any case. Much appreciated.

P.S: I've been a heavy lurker on HF in 2014-2016 haha. This forum was a great pass time.

Bastille - January 14, 2025, 12:12 am

(Jan 13, 2025 06:51 PM)ubermensch38 Wrote: [\[CITE\]](#) Oh thanks a lot for the guide.

Getting into cybersecurity is my main goal (not sure what path yet) -- although I've seen that many people recommend getting a helpdesk gig first, so I'm aiming for that first.

Saw the Google's cybersecurity cert being recommended in a vid... and I went head first without thinking much lol.

CompTIA A+ feels a bit intimidating right now.

I'm doing the Technical Support Fundamentals Course (from Google) as well. Gonna pair it with some Professor Messer vids...

And then get the CompTIA A+ when I proved myself that I'm actually serious about this lol.

So first goal is to get 2h minimum each day total on these courses.

And I don't have IT experience besides high-school and some classes during college.

Going to dig further into your guide in any case. Much appreciated.

P.S: I've been a heavy lurker on HF in 2014-2016 haha. This forum was a great pass time. Helpdesk is definitely the best entry point because you'll be able to see and touch a lot of things, besides you'll work with other people in the same desk so you can rely on them when you need, you can easily learn new things with them, and you can also move to higher positions such as Helpdesk level 2, level 3, then sys admin, etc ... I'm not familiar with Google certs but I can definitely tell you that CompTIA certs are very appreciated by recruiters. A+ is basically the basics of IT, if you plan to work in a helpdesk you should have the knowledge to get A+ cert at least, to give you an idea of the difficulty, someone who is techy / geek at home could get it, so don't worry :)

2h a day is definitely a good time ! I'm sure you'll have no difficulties with A+ cert. Feel free to read my thread, there is a section about certs and I also provide links of websites where you can answer questions from A+ exams for free, so you'll be able to get an idea if you're ready or not ;)

Never too late :D nice to see that you're on the rails now :)

Bastille - January 14, 2025, 8:47 am

[Bumped the thread to not merge my posts]

Completed 1 challenge on letsdefend.io : Excel 4.0 macros, but this challenge was a pain in the ass, not because it was difficult, but because the tools provided didn't work. I discovered one tool that was interesting (called XLMDeobfuscator) but I wasn't able to make it work, even when I started to follow writeups, I had many errors, I finally find a way to solve the challenge without using those tools but I've waste 1 hour on a simple challenge, this really pissed me off.

And it was not over, I then moved on Tryhackme and almost the same, don't know why but I ALWAYS encounter issues when trying to browse web pages related to the target machine from the attack box. After 30 minutes the target machine crashed, so the IP changed and I had to start over. I ended up configuring the VPN access with OpenVPN, I tried to generate .ovpn files. From 4 servers, 3 of them generated a 0bytes .ovpn file, after trying each of them many times EU server 2 gave me

a config file, ok, let's go ? I didn't work. I struggled almost 45 minutes on this, so I've decided to try with US servers, finally one of them gave me a valid config file for .ovpn and I was able to connect.

Finally, I completed <https://tryhackme.com/r/room/lookup> , not that easy, I learned few things and it was quite interesting, but I wasn't very productive today, hope tomorrow will be better.

Now that I have the VPN working I'll go with my virtual machine instead of the attack box. By the end of the month I'm planing either to make 2 SOC case per day, or 2 rooms per day.

ubermensch38 - January 14, 2025, 1:55 pm

So today I went through Professor Messer's CompTIA A+ core 1 training today until Module 3. (Might do the module 3 as well after this check-in)

Guess I'm doing the CompTIA A+ now lol

I'm currently going through the material fast: going at 1.75x speed and not taking many notes. Just to grasp the big idea and see the notions before I get into it deeper.

The priority now is to finish the modules -- and then think how I can structure some projects around this + ask Claude to give me some more analytical questions + make some Anki flashcards.

I've looked at the HomeLab subreddit -- and it somewhat intimidates me lol. Going to look deeper on how I can setup a lab for somewhat cheap. I suppose I don't need super crazy stuff.

As for the questions... I guess Dean exam prep is OK for lower-level learning (even though Dean's exam prep is similar to CompTIA's exam)...

But I'd like to get a more deeper understanding by solving questions that require me to combine a broader range of concepts -- which I hope Claude will be able to do that for me.

I think I can realistically get the Core 1 cert in like 1 month or so if I keep going at this pace. So that's my soft goal for me rn to work around with.

Hope everyone is still going strong

Sociopath - January 14, 2025, 11:47 pm

Love this! Thanks for the post ?

Bastille - January 15, 2025, 12:41 am

(Jan 14, 2025 02:55 PM)ubermensch38 Wrote: [\[CITE\]](#) So today I went through Professor Messer's CompTIA A+ core 1 training today until Module 3. (Might do the module 3 as well after this check-in)

Guess I'm doing the CompTIA A+ now lol

I'm currently going through the material fast: going at 1.75x speed and not taking many notes. Just to grasp the big idea and see the notions before I get into it deeper.

The priority now is to finish the modules -- and then think how I can structure some projects around this + ask Claude to give me some more analytical questions + make some Anki flashcards.

I've looked at the HomeLab subreddit -- and it somewhat intimidates me lol. Going to look deeper on how I can setup a lab for somewhat cheap. I suppose I don't need super crazy stuff.

As for the questions... I guess Dean exam prep is OK for lower-level learning (even though Dean's exam prep is similar to CompTIA's exam)...

But I'd like to get a more deeper understanding by solving questions that require me to combine a

broader range of concepts -- which I hope Claude will be able to do that for me.

I think I can realistically get the Core 1 cert in like 1 month or so if I keep going at this pace. So that's my soft goal for me rn to work around with.

Hope everyone is still going strong

I'm sure you can get the A+ ! Working with AI for questions is also a good way to practice, don't forget those links where you can find real questions :

- <https://www.examttopics.com/>
- <https://www.itexams.com/>
- <https://www.examcompass.com/>

If you need help for your homelab feel free to open a thread on HF, it can be intimidating at first glance but don't worry, it's not that complicated. And yeah, just use an old laptop / desktop with enough RAM for your virtual machines

Still doing strong, it's nice to read your feedbacks ! That makes me want to do some SOC analysis cases and Tryhackme rooms haha

(Jan 15, 2025 12:47 AM)Sociopath Wrote: [\[CITE\]](#) Love this! Thanks for the post ?
Hope to see you participating ;)

Bastille - January 15, 2025, 5:49 am

[Bumped the thread to not merge my posts]

After 2 weeks I wanted to increase the work load so I've went through :

- 1 SOC case analysis on letsdefend.io : SOC132 - Same Malicious File Found on Multiple Sources (fingers in the nose), it was a .bat file performing malicious things over Python with plain-text information such as C2 server IP and so on..

- 2 rooms on tryhackme.com <https://tryhackme.com/r/room/ignite> > did it almost without help
<https://tryhackme.com/r/room/bsidesgtthompson> > struggled a little bit more

- 1 practice test on <https://www.examcompass.com> : I plan to pass the exam of CompTIA Security+, I was going to pass the exam few years ago but never did. As you probably know those exams are updated every year or two years so it changed since version SY0-501, it shouldn't be that difficult but I need to update my knowledge. There are a lot of practice tests, I'll try to go through all of them at least twice to be sure I'll not waste my money

I'll probably increase the number of SOC analysis cases but for that I need to go with the premium version of letsdefend and I'm waiting for a discount, sometimes I regret that I didn't go with the 50% discount on the new year but nevermind, I didn't know that I would have been able to study that much due to my burnout.

Hope you're doing good, hope you're doing your homeworks fellow

Current streaks :

Letsdefend.io : 17?

Tryachkme : 15?

ubermensch38 - January 15, 2025, 1:20 pm

(Jan 15, 2025 01:41 AM)Bastille Wrote: [\[CITE\]](#) If you need help for your homelab feel free to open a

thread on HF, it can be intimidating at first glance but don't worry, it's not that complicated. And yeah, just use an old laptop / desktop with enough RAM for your virtual machines
I asked Claude what affordable options I can do...

And it told me that the game "PC Building Simulator" is a suitable replacement lol.

I'll probably settle with virtual stuff for now.

Also I'm seeing you want to pursue a cert as well, huh?

Haha, go for it.

As for my daily check-in:

I finished the Module 3 from Professor Messer's course. It was the longest Module and it was literally 1/2 of the entire course -- so that's still something.

I was momentarily discouraged by the fact that no one gives a fugg about CompTIA certs in Europe.

But eventually found out that helpdesk jobs here don't ask for any training -- and so I tailored my CV and cover letter for helpdesk jobs and applied to about 20 of them.

I'm still going to continue learning for CompTIA for sure. As it's not boring at all. But I'm wondering what my next step will be.

I'm thinking of slashing my learning time in 70/30.

70% on CompTIA, and 30% on doing stuff on HTB.

See y'all tomorrow :D

Edit: I see the most appreciated certification in Europe is the CCNA/CCNP.

CCNA looks like a nice goal to explore after CompTIA

RootRXXT - January 15, 2025, 1:39 pm

checking in for today -

Start with bit more intermediate python stuff - lets see how long it lasts

xrphbar - January 15, 2025, 9:49 pm

checking in for today. You guys have a great day.

Bastille - January 16, 2025, 1:56 am

(Jan 15, 2025 02:20 PM)ubermensch38 Wrote: [\[CITE\]](#) I asked Claude what affordable options I can do...

...

Edit: I see the most appreciated certification in Europe is the CCNA/CCNP.

CCNA looks like a nice goal to explore after CompTIA

I've never tried Claude but it sounds like it's the time to move to ChatGPT x)

Yep, looking for the Security+

Where did you see that no one give a fuck about CompTIA certs in Europe ? (just saw the edit, CCNA and CCNP are Cisco related certs about networking, CompTIA has a wider field of domain [from Basics, to cloud, servers, networking, security, ...], CCNA is good for sys/network admin, and CCNP is higher, probably for network architect)

Good luck for the applications, feel free to keep us informed on how it goes !

(Jan 15, 2025 02:39 PM)RootRXXT Wrote: [\[CITE\]](#) checking in for today -

Start with bit more intermediate python stuff - lets see how long it lasts

Glade to see you posting ! How do you plan to use those Python skills/knowledge ?

(Jan 15, 2025 10:49 PM)xrphbar Wrote: [\[CITE\]](#) checking in for today. You guys have a great day. Hello, feel free to share what you worked on, the objective of the thread is also to share what you did so we can discuss about

ubermensch38 - January 16, 2025, 6:15 am

(Jan 16, 2025 02:56 AM)Bastille Wrote: [\[CITE\]](#) Where did you see that no one give a fuck about CompTIA certs in Europe ? (just saw the edit, CCNA and CCNP are Cisco related certs about networking, CompTIA has a wider field of domain [from Basics, to cloud, servers, networking, security, ...], CCNA is good for sys/network admin, and CCNP is higher, probably for network architect)

Good luck for the applications, feel free to keep us informed on how it goes !

I can't find any job posting that mentions any CompTIA certification here. Looked on LinkedIn and Indeed.

I've also discussed with 2 InfoSec veterans on Professor Messer's discord server who are both from Europe -- and it seems like no employer knew about CompTIA either when they applied in the past.

The only certs I see are all Cisco's. Or Microsoft Azure Network stuff. But those 2 certs are more advanced.

For entry-level stuff, only a 2-year degree is asked so I don't know.

Seeing that I can get a helpdesk job without CompTIA A+ really makes me doubt if it's worth pursuing further...

But I'll keep going anyway. It's good practice and it's exciting lol.

See ya tonight for the check-in.

capt_nemo - January 16, 2025, 6:35 am

Checking in for today.

I have been working with Burp Suite today.

10th day in a row, really cool to stay on the ball like this. The thread helps a lot.

Have a great day!

Bastille - January 16, 2025, 6:52 am

(Jan 16, 2025 07:15 AM)ubermensch38 Wrote: [\[CITE\]](#) I can't find any job posting that mentions any CompTIA certification here. Looked on LinkedIn and Indeed.

...

The only certs I see are all Cisco's. Or Microsoft Azure Network stuff. But those 2 certs are more

advanced.

But I'll keep going anyway. It's good practice and it's exciting lol.

See ya tonight for the check-in.

The certification (A+) is useful if you have no degree or prior knowledge, but if you have a degree related on IT don't bother with it yes :)

Haha see you tonight !

(Jan 16, 2025 07:35 AM)captn_nemo Wrote: [\[CITE\]](#) Checking in for today.

I have been working with Burp Suite today.

10th day in a row, really cool to stay on the ball like this. The thread helps a lot.

Have a great day!

I studied this tool over THM when I started in "hacking" and at this time I wasn't really comfortable with, now when I see rooms relying on Burp I usually avoid them lol ... but I should definitely go back to it now as I'm more comfortable in this realm.

I'm really glad that it helps you, sometimes it's really "annoying" to study alone, and not easy to find the motivation; I'm always happy to see you guys posting your daily progress, and I'm happy to see more activity on the forum about hacking, I was afraid to see less and less "hackers" on the forum, now I'm sure we're not dead and 2025 will be our year with so many things coming ?

I haven't heard from you lately on this thread, guys. Where are you ?? [RangoWorld](#) [TENET](#) [plops](#) [Mexicano](#) [Miracula](#)

TENET - January 16, 2025, 7:24 am

I went to study shellcode, but failed.....

Bastille - January 16, 2025, 7:34 am

(Jan 16, 2025 08:24 AM)TENET Wrote: [\[CITE\]](#) I went to study shellcode, but failed.....

Mmmmh, not an easy topic ... Do you have prior knowledge with assembly ? programming ? How did you learn ? What material did you use, what was your approach and how do you know you've failed, what problem did you encounter ?

TENET - January 16, 2025, 8:15 am

(Jan 16, 2025 08:34 AM)Bastille Wrote: [\[CITE\]](#) Mmmmh, not an easy topic ... Do you have prior knowledge with assembly ? programming ? How did you learn ? What material did you use, what was your approach and how do you know you've failed, what problem did you encounter ?

Just started learning about shellcode, and it's really challenging. I tried to start by creating a simple shellcode loader. First, I converted "hello" into shellcode and ran it using the loader, and it worked fine. However, after converting an executable file into shellcode, it failed to run.

Miracula - January 16, 2025, 8:27 am

(Jan 16, 2025 09:15 AM)TENET Wrote: [\[CITE\]](#) Just started learning about shellcode, and it's really challenging. I tried to start by creating a simple shellcode loader. First, I converted "hello" into shellcode and ran it using the loader, and it worked fine. However, after converting an executable file into shellcode, it failed to run.

Hey! How are you converting your executable into shellcode and what type of payload are you

using?

For native (written in C/C++/etc.) you may try pe2shc ([github](#) / [release](#))

For managed (.NET) you can try donut ([github](#) / [releases](#))

Checking in for today as well, worked on some personal tools.

RootRXXT - January 16, 2025, 9:36 am

(Jan 16, 2025 07:15 AM)ubermensch38 Wrote: [\[CITE\]](#) I can't find any job posting that mentions any CompTIA certification here. Looked on LinkedIn and Indeed.

I've also discussed with 2 InfoSec veterans on Professor Messer's discord server who are both from Europe -- and it seems like no employer knew about CompTIA either when they applied in the past.

The only certs I see are all Cisco's. Or Microsoft Azure Network stuff. But those 2 certs are more advanced.

For entry-level stuff, only a 2-year degree is asked so I don't know.

Seeing that I can get a helpdesk job without CompTIA A+ really makes me doubt if it's worth pursuing further...

But I'll keep going anyway. It's good practice and it's exciting lol.

See ya tonight for the check-in.

Just trying to up my skills for security and then a bit of logic app automations

plops - January 16, 2025, 9:54 am

(Jan 16, 2025 07:52 AM)Bastille Wrote: [\[CITE\]](#) I haven't heard from you lately on this thread, guys. Where are you ?? [RangoWorld](#) [TENET](#) [plops](#) [Mexicano](#) [Miracula](#)

Ha Thanks [Bastille](#), i made a habit of regular daily check in but I need to be here too!

I am still on a streak since my post 10 days ago and I intend on holding it.

I will compile a list of tryhackmes i completed later.

If its not thm or practicing python or building my web server, I am working on a project for someone and trying to beat their detection system. It has introduced me to basic encoding/decoding and obfuscation. As much as it makes me want to pull my hair out it is a fun journey and am learning a lot quickly.

I will continue to check in!

Bastille - January 16, 2025, 11:45 am

(Jan 16, 2025 10:54 AM)Robert Walker Wrote: [\[CITE\]](#) Ha Thanks [Bastille](#), i made a habit of regular daily check in but I need to be here too!

I am still on a streak since my post 10 days ago and I intend on holding it.

I will compile a list of tryhackmes i completed later.

If its not thm or practicing python or building my web server, I am working on a project for someone and trying to beat their detection system. It has introduced me to basic encoding/decoding and

obfuscation. As much as it makes me want to pull my hair out it is a fun journey and am learning a lot quickly.

I will continue to check in!

I'm glad to know we didn't lose you on the way :p

That's really nice man, you have a lot of things to do and many fields to improve / explore, if you're allowed to talk about it I would love to hear more about how you're trying to deceive their detection system.

For my part, today I've completed :

- 1 SOC analysis case on letsdefend.io : SOC135 - Multiple FTP Connection Attempt (that's my 45th case)

- 1 room on tryhackme : <https://tryhackme.com/r/room/bsidesgtlibrary> really easy, I really feel more comfortable regarding the first days, it's good to go back to the basics after a while

Yesterday I drunk too much, didn't feel very good today, I didn't want to do too much, tomorrow I'll have more energy ?

kreito - January 16, 2025, 11:53 am

Overthewire isn't that bad either

Tyr - January 16, 2025, 11:59 am

(Jan 16, 2025 07:15 AM)ubermensch38 Wrote: [\[CITE\]](#) I can't find any job posting that mentions any CompTIA certification here. Looked on LinkedIn and Indeed.

I've also discussed with 2 InfoSec veterans on Professor Messer's discord server who are both from Europe -- and it seems like no employer knew about CompTIA either when they applied in the past.

The only certs I see are all Cisco's. Or Microsoft Azure Network stuff. But those 2 certs are more advanced.

For entry-level stuff, only a 2-year degree is asked so I don't know.

Seeing that I can get a helpdesk job without CompTIA A+ really makes me doubt if it's worth pursuing further...

But I'll keep going anyway. It's good practice and it's exciting lol.

See ya tonight for the check-in.

As someone who has the triad with a degree in cybersecurity as well as comp info sys, I can assure you that there are some still left out there if you want to make around minimum wage. IT is a battleground. You starve for a year or so by proving yourself and then eventually the numbers start to rack up as you make more connections and become promoted. With this said, openings are becoming less and less common as many companies are rethinking the way they go on about hiring new candidates and requiring a college diploma alongside certs whereas during the pandemic you could get the A+ (or other certs from Cisco or CompTIA) and find remote work fairly easily compared to now, for example.

AWS certs are very highly sought after, correct. CCNA is more viable than the Network+ from my perspective when it comes to job hunting because I see a ton of employers wanting this and it is less broad of a certification than the N+ for example, so you can narrow down search results or market yourself to companies that are in need of network engineer's that can manage Cisco devices

which is something that was overlooked by HR during the pandemic. Subsequently, this led to many layoffs as well. I personally believe will be here to stay for a very long time and might give you the ability to get your foot in the door more than the N+ or A+ which only cover fundamental networking procedures. Certificates are becoming replaced with "xyz experience and proven track record in Palo Alto doing abc" etc.

Just my 2 cents.

Btw, anyone ever use TryHackMe in the past and had a good experience with their labs? HTB is great and all but I really do not even have the time for a lot of what they got on their dashboard, especially right now...

ubermensch38 - January 16, 2025, 2:59 pm

(Jan 16, 2025 12:45 PM) Bastille Wrote: [\[CITE\]](#) For my part, today I've completed :

- 1 SOC analysis case on letsdefend.io : SOC135 - Multiple FTP Connection Attempt (that's my 45th case)
- 1 room on tryhackme : <https://tryhackme.com/r/room/bsidesgtlibrary> really easy, I really feel more comfortable regarding the first days, it's good to go back to the basics after a while

Yesterday I drunk too much, didn't feel very good today, I didn't want to do too much, tomorrow I'll have more energy ?

GJ on keeping yourself on track despite not feeling well.

Boss moves ?

(Jan 16, 2025 12:59 PM) Tyr Wrote: [\[CITE\]](#) Certificates are becoming replaced with "xyz experience and proven track record in Palo Alto doing abc" etc.

Hi -- tyvm for sharing your perspective. Truly appreciate it :D

Yea, I've picked up on the trend that "certificates = higher pay/guarantee to get hired" idea is a myth. Seeing lots of people online complaining about it lol.

"I've gotten the trifecta and couldn't get hired"; "I got the CCNA and it did nothing to my career"; "I got the CCNP and can't get hired for a Network Engineer position" etc...

Lots of these on Reddit from people with no experience and went just for the certificates.

Eh -- my aim is to get work experience asap anyway.

Getting a helpdesk position... then finish the A+ anyway since I've already started it...

Then go for CCNA and see from there.

For my daily check-in:

I finished the Professor Messer's videos.

Modules 4 and 5 (about Printers and Troubleshooting) were somewhat simple.

Had more issues to remember all the acronyms in Module 3 about Hardware lol.

Tomorrow the goal is to start attacking 30-40 questions...

Searching what acronyms are required to know in the CompTIA exam requirements and do Anki flashcards on them...

And then decide on some project.

Haven't done any HTB today sadly.

Tyr - January 16, 2025, 5:01 pm

(Jan 16, 2025 03:59 PM)ubermensch38 Wrote: [\[CITE\]](#) GJ on keeping yourself on track despite not feeling well.

Boss moves ?

Hi -- tyvm for sharing your perspective. Truly appreciate it :D

Yea, I've picked up on the trend that "certificates = higher pay/guarantee to get hired" idea is a myth. Seeing lots of people online complaining about it lol.

"I've gotten the trifecta and couldn't get hired"; "I got the CCNA and it did nothing to my career"; "I got the CCNP and can't get hired for a Network Engineer position" etc...

Lots of these on Reddit from people with no experience and went just for the certificates.

Eh -- my aim is to get work experience asap anyway.

Getting a helpdesk position... then finish the A+ anyway since I've already started it...

Then go for CCNA and see from there.

For my daily check-in:

I finished the Professor Messer's videos.

Modules 4 and 5 (about Printers and Troubleshooting) were somewhat simple.

Had more issues to remember all the acronyms in Module 3 about Hardware lol.

Tomorrow the goal is to start attacking 30-40 questions...

Searching what acronyms are required to know in the CompTIA exam requirements and do Anki flashcards on them...

And then decide on some project.

Haven't done any HTB today sadly.

Good good. I highly recommend his course material mixed with Jason Dion but most importantly studying in voice chat with others in PFM's discord (many of them have been doing this for 20+ years like Messer himself) and simply spend hours evaluating each question very carefully and each answer then we'd all make our guesses and the hoster (many kind people in there who have purchased very accurate practice tests) will share their screen and elaborately explain everything.

By taking initiative and not being scared I have learned so much through being corrected and spaced repetition as I studied for all three at once.

Regarding flash cards, I created my own deck with pen and pencil and carried it around with me for a month or so. I have about 100-200+

Also not trying to upsell professor messer as there are also other fantastic resources but he has an extensive vocab list and so does CompTIA on their website actually. But mine are mixed with S+, CCNA, A+, N+, and CEH all together and then I have them color coded. I know this isn't conventional but this is just how I learned. For the CCNA I watched these videos on YouTube but also took a course in college that prepared me for it for my first degree.

Quote: Had more issues to remember all the acronyms in Module 3 about Hardware lol. It's ok. That's probably the hardest part of the A+ because they're throwing 2 exams at you at once with different weights on each of them.

I just info dumped so much stuff about these exams and accidentally tabbed away so if you want more info just shoot me a PM and I will be glad to help you out sometime. It looks very good on a resume so long as you have a degree and other important soft skills for example.

TENET - January 16, 2025, 7:01 pm

(Jan 16, 2025 09:27 AM)Miracula Wrote: [\[CITE\]](#) Hey! How are you converting your executable into shellcode and what type of payload are you using?

For native (written in C/C++/etc.) you may try pe2shc ([github](#) / [release](#))

For managed (.NET) you can try donut ([github](#) / [releases](#))

Checking in for today as well, worked on some personal tools.

[release](#))

This is pretty good~~ But I want to ask, the project doesn't explain the process of creating the loader, and does the loader have to match the shellcode, or is it universal????

Bastille - January 17, 2025, 12:14 am

(Jan 16, 2025 12:53 PM)kreito Wrote: [\[CITE\]](#) Overthewire isn't that bad either

Yep, just added it to the list, thanks :)

(Jan 16, 2025 12:59 PM)Tyr Wrote: [\[CITE\]](#)

Btw, anyone ever use TryHackMe in the past and had a good experience with their labs? HTB is great and all but I really do not even have the time for a lot of what they got on their dashboard, especially right now...

I'm only using Tryhackme (and letsdefend.io for Blue Team stuff) and I've been really happy with it, the rooms sound more easy than HTB, give it a try to compare, I would like to get your feedback too

(Jan 16, 2025 03:59 PM)ubermensch38 Wrote: [\[CITE\]](#) GJ on keeping yourself on track despite not feeling well.

Boss moves ?

For my daily check-in:

I finished the Professor Messer's videos.

Modules 4 and 5 (about Printers and Troubleshooting) were somewhat simple.

Had more issues to remember all the acronyms in Module 3 about Hardware lol.

Tomorrow the goal is to start attacking 30-40 questions...

Searching what acronyms are required to know in the CompTIA exam requirements and do Anki flashcards on them...

And then decide on some project.

Haven't done any HTB today sadly.

Haha thanks, I don't want to fail at the beginning of this challenge ?

Damn you did a lot, and yeah there are a lot of acronyms in IT but you'll get familiar with because they're often used.

Feel free to share a screenshot of your results if you don't mind; it could also help you see the percentage of good questions increasing over time through this thread

plops - January 17, 2025, 5:44 am

Day 10 completed last night.

Was tired and did not want to commit any time But, like usual, after 30 minutes I am fully invested and a couple hours later i had to force myself off the computer and get to bed.

Anyways, no thm's. Continued building my current revision of a webpage to sneak past a detection system. Did not submit anything but i should complete this version tonight.

An old thread was dug up and a lovely member quoted a now scrubbed member which gave me another idea to try out. (hiding small text to break up keywords). I doubt this will work but I am going to try it out along with encoding even smaller bits and building back up.

I think im up against ai, so im not sure how I will trick this bot. Im on version 7 now lol.

Plan for tonight:

1. Spend some time and submit version 7.

2. Continue <https://tryhackme.com/r/room/ignite>.

This one has been a bit of a challenge. This one doesn't have the usual questions that kind of lead you the other easy ones do. It has me reasearching good questions and exposing me to more.

Have a good day!

Miracula - January 17, 2025, 8:04 am

(Jan 16, 2025 08:01 PM)TENET Wrote: [\[CITE\] release](#))

This is pretty good~~ But I want to ask, the project doesn't explain the process of creating the loader, and does the loader have to match the shellcode, or is it universal????

I am not sure I understand what you mean by "match" (by architecture?), but here are some good posts on how to write shellcode loaders in c++/asm: [cocomelonc](#), [ired team](#) and [Oxpat](#)

Also checking in for today, worked on some designs for my droppers, maybe I will sell some on hf too.

Bastille - January 17, 2025, 1:04 pm

(Jan 17, 2025 06:44 AM)Robert Walker Wrote: [\[CITE\]](#) Day 10 completed last night.

Was tired and did not want to commit any time But, like usual, after 30 minutes I am fully invested and a couple hours later i had to force myself off the computer and get to bed.

Anyways, no thm's. Continued building my current revision of a webpage to sneak past a detection system. Did not submit anything but i should complete this version tonight.

An old thread was dug up and a lovely member quoted a now scrubbed member which gave me another idea to try out. (hiding small text to break up keywords). I doubt this will work but I am going to try it out along with encoding even smaller bits and building back up.

I think im up against ai, so im not sure how I will trick this bot. Im on version 7 now lol.

Plan for tonight:

1. Spend some time and submit version 7.

2. Continue <https://tryhackme.com/r/room/ignite>.

This one has been a bit of a challenge. This one doesn't have the usual questions that kind of lead you the other easy ones do. It has me reasearching good questions and exposing me to more.

Have a good day!

Wish you good luck for tonight buddy ! Feel free to share what you've done from the list

I've been through ignite few days ago and I understand what you mean, some rooms are "guided" on THM, but other just give you the VM and ask for user flag and root flag haha. To be honest those rooms require some knowledge and to be comfortable with hacking. Feel free to check writeups / walktrhough to help you a little bit, don't go straight to the answers, try the tools shown and so on.

Writing from my bed, completed 1 SOC case today on letsdefend.io and started a room on tryhackme.com which cover many steps in hacking (gaining access, priv esc, ...)

ubermensch38 - January 17, 2025, 3:21 pm

Daily check-in:

Haven't done much today -- work took all my attention (freelance stuff)

Only 30 questions. I got correct 20 of them. Eh.

Took me like 10-15 minutes to get through the questions. So I can do lots more per day.

Tomorrow I'll have more time to pay attention to learning.

Glad everyone is still going strong haha

Tyr - January 17, 2025, 4:49 pm

Daily check in:

Have been practicing SE again in person (no not here) and realized today just how far being a persuasive individual with good charisma goes regardless of your intentions in all avenues of life whether hacking or not because either way networking is how you inevitably get better at what you do via learning from those who are more skilled at things; in this case human behavioral analysis.

Bastille - January 18, 2025, 12:24 am

(Jan 17, 2025 04:21 PM)ubermensch38 Wrote: [\[CITE\]](#) Daily check-in:

Haven't done much today -- work took all my attention (freelance stuff)

Only 30 questions. I got correct 20 of them. Eh.

Took me like 10-15 minutes to get through the questions. So I can do lots more per day.

Tomorrow I'll have more time to pay attention to learning.

Glad everyone is still going strong haha

66% of good answers, that's a nice score for the beginning, if I remember well the pass score is 80%, you're not far to be able to say that you have A+ level

Still going strong buddy, 2024 was the worst year of my life, I have to take a revenge and go back to my feet, 2025 will be my year, but I need to put effort into it, nothing is free ?

(Jan 17, 2025 05:49 PM)Tyr Wrote: [\[CITE\]](#) Daily check in:

Have been practicing SE again in person (no not here) and realized today just how far being a persuasive individual with good charisma goes regardless of your intentions in all avenues of life whether hacking or not because either way networking is how you inevitably get better at what you do via learning from those who are more skilled at things; in this case human behavioral analysis. Do you use materials to learn SE or you just practice and learn by yourself ? I've read few books from Christopher Hadnagy's, he seems to be the reference in this field

Tyr - January 18, 2025, 12:35 am

(Jan 18, 2025 01:24 AM)Bastille Wrote: [\[CITE\]](#) 66% of good answers, that's a nice score for the beginning, if I remember well the pass score is 80%, you're not far to be able to say that you have A+ level

Still going strong buddy, 2024 was the worst year of my life, I have to take a revenge and go back to my feet, 2025 will be my year, but I need to put effort into it, nothing is free ?

Do you use materials to learn SE or you just practice and learn by yourself ? I've read few books from Christopher Hadnagy's, he seems to be the reference in this field

Hmm, tough question. I think it just comes naturally and I come from a family of salespeople. At the same time though, when I first joined these forums many years ago I gravitated to the SE part of the forum where I learned different TTP which were implanted into my brain at a very young age. But honestly, I think being a people person, listening to others and learning the art of persuasion through subtle influences via installing a belief in the target to create different emotions which will make them in turn react a certain way giving you more information allowing you to further pivot into their mind by exfiltrating useful information or convincing them of something. It's about manipulating the belief system one has accumulated as a controller and challenging these so that your expectations in their mind view their environment as something you want them to. It is something that I cannot really explain in words so yes, 75% of it comes naturally but 12 years later when studying for my first degree and for CompTIA I revisited a lot of the more complex avenues of SE such as using principles of urgency, social proof, flattery, and their corresponding sub-categories as they relate to human psychology and behavior while I took Psychology as an elective so a large amount of it came from that too.

My favorite material is a tad non-conventional and involves everything from hypnosis to dark NLP. Ironically, it's really quite common sense when you reflect on the book. It is quite long but you would likely enjoy it if you put it on 1.25x ?

I actually have never heard of Christopher Hadnagy. I will need to check him out tonight on my

phone before bed perhaps.

If you mean specifically for CompTIA, I used the PFM material to study if that's what you were referring to.

Bastille - January 18, 2025, 1:29 am

(Jan 18, 2025 01:35 AM)Tyr Wrote: [\[CITE\]](#) Hmm, tough question. I think it just comes naturally and I come from a family of salespeople. At the same time though, when I first joined these forums many years ago I gravitated to the SE part of the forum where I learned different TTP which were implanted into my brain at a very young age. But honestly, I think being a people person, listening to others and learning the art of persuasion through subtle influences via installing a belief in the target to create different emotions which will make them in turn react a certain way giving you more information allowing you to further pivot into their mind by exfiltrating useful information or convincing them of something. It's about manipulating the belief system one has accumulated as a controller and challenging these so that your expectations in their mind view their environment as something you want them to. It is something that I cannot really explain in words so yes, 75% of it comes naturally but 12 years later when studying for my first degree and for CompTIA I revisited a lot of the more complex avenues of SE such as using principles of urgency, social proof, flattery, and their corresponding sub-categories as they relate to human psychology and behavior while I took Psychology as an elective so a large amount of it came from that too.

My favorite material is a tad non-conventional and involves everything from hypnosis to dark NLP. Ironically, it's really quite common sense when you reflect on the book. It is quite long but you would likely enjoy it if you put it on 1.25x ?

I actually have never heard of Christopher Hadnagy. I will need to check him out tonight on my phone before bed perhaps.

If you mean specifically for CompTIA, I used the PFM material to study if that's what you were referring to.

That is definitely something I should spend time on it, it's not only helpful for hacking, but also for day to day things, and it's an important part if you want to success in life I think. I've worked as a seller for few years but to be honest I didn't feel good in this role, it's also linked to people's personality I guess.

Damn 10 hours haha, x1.25 will help but I'm not going to lie don't know if I'll be find the courage to listen the entire video haha

There are many books from him on Amazon, and they're well rated so I went with them and wasn't disappointed. However I don't know if it's advanced or if he's just explaining the basics.

ttbr0 - January 18, 2025, 2:32 am

learned some virustotal api usage on python for some automation to upload and check files. check out the script here: <https://hackforums.net/showthread.php?pid=62645533>

ubermensch38 - January 18, 2025, 2:46 am

(Jan 18, 2025 01:35 AM)Tyr Wrote: [\[CITE\]](#) It is something that I cannot really explain in words so yes, 75% of it comes naturally but 12 years later when studying for my first degree and for CompTIA I revisited a lot of the more complex avenues of SE such as using principles of urgency, social proof, flattery, and their corresponding sub-categories as they relate to human psychology and behavior while I took Psychology as an elective so a large amount of it came from that too.

I actually have never heard of Christopher Hadnagy. I will need to check him out tonight on my phone before bed perhaps.

If you mean specifically for CompTIA, I used the PFM material to study if that's what you were referring to.

Hmm interesting book -- I'm going to have a listen to it.

Back in 2014 - 2016 when I was roaming around HF as a bored script kiddie, I'd read stuff on SE...

And it actually made me go into sales/marketing lol

You can try looking into Ian Rowland's Full Facts Book of Cold Reading.

Pretty neat tool to actually seem like you deeply understand a person without actually knowing much about them.

The Forbidden Keys to Persuasion by Blair Warren is nice too.

I suppose you already read Robert Cialdini stuff.

Bastille - January 18, 2025, 6:08 am

Today I've completed :

- 1 SOC analysis case on letsdefend.io : SOC131 - Reverse TCP Backdoor Detected > EZ, a simple bat file with a reverse shell. I would like to do more of these cases but I'm limited with the free version. I'm thinking about upgrading but wondering if I should upgrade THM or Letdefend.io

- 1 room on tryhackme.com, that I've started yesterday : <https://tryhackme.com/r/room/thecodcaper>
I'm divided regarding this room, it was a good exercise to go back to the basics, however I struggled on the SQLmap part and on the gdb part. I definitely need to take a look in depth at these tools.

I've also took a look at [ttbr0](#) 's thread : <https://hackforums.net/showthread.php?pid=62645533>
Recently, I shared with him that I wanted to go back to Python and thought about making a program to send files to VirusTotal in CLI, he made it and I was able to see how it works. I've understood and now I feel more comfortable with the idea of making my programs. By the way, while doing my Tryhackme room, I stubon upon the following course : <https://tryhackme.com/r/room/pythonbasics> I'll probably go with this room tomorrow to remember me the basics of Python.

Within the next days or weeks I would like to make some malware for educational purposes, such as keyloggers or stealers. I think that it could be a good way to improve my skills and knowledge with Python.

Current streak :

Letsdefend.io : 20 ?

Tryhackme.com : 18 ?

ttbr0 - January 18, 2025, 2:38 pm

(Jan 18, 2025 07:08 AM)Bastille Wrote: [\[CITE\]](#) I've also took a look at [ttbr0](#) 's thread : <https://hackforums.net/showthread.php?pid=62645533>

Recently, I shared with him that I wanted to go back to Python and thought about making a program to send files to VirusTotal in CLI, he made it and I was able to see how it works. I've understood and

now I feel more comfortable with the idea of making my programs. By the way, while doing my Tryhackme room, I stubon upon the following course : <https://tryhackme.com/r/room/pythonbasics> I'll probably go with this room tomorrow to remember me the basics of Python.

Within the next days or weeks I would like to make some malware for educational purposes, such as keyloggers or stealers. I think that it could be a good way to improve my skills and knowledge with Python.

you should write some malware and then write detections for it. i think that would be a great feedback loop to improve both your detection game and malware evasion game

ubermensch38 - January 18, 2025, 2:53 pm

(Jan 18, 2025 01:24 AM)Bastille Wrote: [\[CITE\]](#) Still going strong buddy, 2024 was the worst year of my life, I have to take a revenge and go back to my feet, 2025 will be my year, but I need to put effort into it, nothing is free ?

I'm truly sorry to hear that. But I can argue that happiness is free ?

What are some things you wish to happen differently in 2025?

For my Daily check-in:

I did 2 tests that had 25 questions each. One I got like 65% and the other 75%. Still need to remember the 1000 acronyms and what they mean lol

I think I can do more than 50 questions per day -- and should go to about 200 minimum.

Also did 20 anki cards today.

Andy Matuschak has some banger takes on making effective anki cards -- so it took me like 2h to write these cards lol

AI is truly a God like teacher. I'm curious about how I can minmax it to save hours on my daily studying.

In any case -- I think I'll only create decks only once every other day. I struggle to focus on doing multiple tasks per day -- so I work best when I allocate each task for its dedicated day.

So tomorrow I will most likely just do exam preps and reviewing my 20 cards.

See y'all tomorrow ???

Bastille - January 19, 2025, 12:44 am

(Jan 18, 2025 03:38 PM)ttbr0 Wrote: [\[CITE\]](#) you should write some malware and then write detections for it. i think that would be a great feedback loop to improve both your detection game and malware evasion game

That's definitely a good idea, I've seen few books that could help, such as (amazon links) :

- [Malware Development for Ethical Hackers: Learn how to develop various types of malware to strengthen cybersecurity](#)
- [Evading EDR: The Definitive Guide to Defeating Endpoint Detection Systems](#)
- [Evasive Malware: A Field Guide to Detecting, Analyzing, and Defeating Advanced Threats](#)

(Jan 18, 2025 03:53 PM)ubermensch38 Wrote: [\[CITE\]](#) I'm truly sorry to hear that. But I can argue that happiness is free ?

What are some things you wish to happen differently in 2025?

- Getting in a better shape
- Being able to work again (I'm planning to work as a SOC analyst before September, I think I could work as tier 1 SOC analyst but it sounds a little bit boring ... I would prefer to start as tier 2)

Those two will help a lot as I've lost a job due to a burnout and many other things.

(Jan 18, 2025 03:53 PM)ubermensch38 Wrote: [\[CITE\]](#) For my Daily check-in:

I did 2 tests that had 25 questions each. One I got like 65% and the other 75%. Still need to remember the 1000 acronyms and what they mean lol

I think I can do more than 50 questions per day -- and should go to about 200 minimum.

Also did 20 anki cards today.

Andy Matuschak has some banger takes on making effective anki cards -- so it took me like 2h to write these cards lol

AI is truly a God like teacher. I'm curious about how I can minmax it to save hours on my daily studying.

In any case -- I think I'll only create decks only once every other day. I struggle to focus on doing multiple tasks per day -- so I work best when I allocate each task for its dedicated day.

So tomorrow I will most likely just do exam preps and reviewing my 20 cards.

See y'all tomorrow ???

Congrats man ! 75% is something, and 2 series of question per day is also very good, you'll remember the acronyms with time don't worry, most of the time we speak with acronyms in IT haha

ttbr0 - January 19, 2025, 2:25 am

(Jan 19, 2025 01:44 AM)Bastille Wrote: [\[CITE\]](#) That's definitely a good idea, I've seen few books that could help, such as (amazon links) :

- [Malware Development for Ethical Hackers: Learn how to develop various types of malware to strengthen cybersecurity](#)

- [Evading EDR: The Definitive Guide to Defeating Endpoint Detection Systems](#)

- [Evasive Malware: A Field Guide to Detecting, Analyzing, and Defeating Advanced Threats](#)

never heard of the first book before but it looks alright. i generally wouldnt recommend books from packt since theyre usually not that great. this one seems fine for beginners. i should note that good detection is a much more complex game compared to malware development

Bastille - January 19, 2025, 4:07 am

Completed 1 SOC analysis case on letsdefend.io : SOC134 - Suspicious WMI Activity but I failed on one question, for my defense logs were missing, instructions were not clear. I can admit when I'm wrong however this case is definitely not well made.

Completed 3 rooms on tryhackme.com : <https://tryhackme.com/r/room/lofi> > LFI

<https://tryhackme.com/r/room/thestickershop> > XSS

<https://tryhackme.com/r/room/webapplicationbasics> > web app basics

It's nice to go back to the basics, I'll continue to do more basics rooms until I feel comfortable

enough again

I'm going to workout some (boxing), then probably continue with either SOC things, or maybe Python, or maybe making threads for HF.

Current streak :
Letsdefend.io : 21?
Tryhackme.com : 19 ?

plops - January 19, 2025, 5:26 am

I think I forgot to post yesterday but the streak is still rolling.

I was able to complete Ignite on thm. Opening up a http server to deliver an exploit to the victim machine was an exciting thing to learn.

The next day I completed 'Library' and 'Simple CTF'.

Its exciting to know that things are sticking, the last two I did I was able to complete, mostly, without some sort of write up for tips. The constant learning and being able to think through these new problems are a big motivation to keep going and not loose it.

Good luck all, keep up the streaks!

Bastille - January 20, 2025, 11:48 am

(Jan 19, 2025 06:26 AM)Robert Walker Wrote: [\[CITE\]](#) I think I forgot to post yesterday but the streak is still rolling.

I was able to complete Ignite on thm. Opening up a http server to deliver an exploit to the victim machine was an exciting thing to learn.

The next day I completed 'Library' and 'Simple CTF'.

Its exciting to know that things are sticking, the last two I did I was able to complete, mostly, without some sort of write up for tips. The constant learning and being able to think through these new problems are a big motivation to keep going and not loose it.

Good luck all, keep up the streaks!

I completed Ignite few days ago too, yeah the "python3 -m http.service 8080" haha ? I think I've also been though library, but "Simple CTF" doesn't ring a bell to me, I'll take a look at it

I'm really happy that constant learning helps you buddy, constancy is key ! And for motivation we're here ?

I'm going to make a short post (had a lot of things to do today and I'm not in a good mood..). Completed a SOC analysis case, and started a tryhackme room to don't loose my streak (easy questions about security : <https://tryhackme.com/r/room/securityprinciples>)

I'll devote more time to hacking tomorrow, the only moments I'm feeling good is when hacking is embracing me. I've been through a lot of hard things lately, and only hacking helped me, it helped me to realize that I'm worth something, that I'm good at something.

Keep going guys, constancy is key. Do the necessary now to become who you want to be in the

future.

Current streak :
Letsdefend.io : 22 ?
Tryhackme.com : 20 ?

captn_nemo - January 20, 2025, 12:22 pm

Like last weekend, I didn't have time to post here, but I did my daily dose of tryhackme. I finished the Burp chapter today.

Finally ?

tryhackme streak: 14

plops - January 20, 2025, 7:45 pm

(Jan 20, 2025 12:48 PM) Bastille Wrote: [\[CITE\]](#) I completed Ignite few days ago too, yeah the "python3 -m http.service 8080" haha ? I think I've also been though library, but "Simple CTF" doesn't ring a bell to me, I'll take a look at it

I'm really happy that constant learning helps you buddy, constancy is key ! And for motivation we're here ?

I'm going to make a short post (had a lot of things to do today and I'm not in a good mood..). Completed a SOC analysis case, and started a tryhackme room to don't loose my streak (easy questions about security : <https://tryhackme.com/r/room/securityprinciples>)

I'll devote more time to hacking tomorrow, the only moments I'm feeling good is when hacking is embracing me. I've been through a lot of hard things lately, and only hacking helped me, it helped me to realize that I'm worth something, that I'm good at something.

Keep going guys, constancy is key. Do the necessary now to become who you want to be in the future.

Current streak :
Letsdefend.io : 22 ?
Tryhackme.com : 20 ?
"python3 -m http.service 8080" - Yeah lol, thats right

Sorry shits been hard man, you'll pick it back up. Can never have our high times without the lows. That's the way she goes, boys - Ray LaFleur

Bastille - January 21, 2025, 10:45 am

Just completed a SOC analysis case on letsdefend.io : SOC139 - Meterpreter or Empire Activity, really easy, no difficulty. I feel more and more comfortable on SOC cases.

Finished the <https://tryhackme.com/r/room/securityprinciples> room I've started yesterday. Didn't sleep well, had a lot of things to do today too. I hope I will be bale to devote more time to hacking tomorrow.

Keep going guys !

ZubZeroXd - January 21, 2025, 2:44 pm

(Jan 3, 2025 01:00 PM)Mooooookie Wrote: [\[CITE\]](#) I'm not much a hacker myself, but I like the idea. Can always use something new for the community, that will help build engagement and spark conversation. Great idea.

plops - January 22, 2025, 4:49 am

Have not done full check in, in a couple of days. But I'm still at it.

Only finished one thm room - Thompson. This was fun deploying a .war on the server to gain access. Was pretty scary considering how many open servers there are out there. A lot for me to keep in mind when I finish and host my own site.

Working on sneaking past detection on a buddies app took my time for a couple days. And was ultimately successful. I don't want to put a lot out there because even the feedback I would receive was pretty vague. But I am coming out of it with a strong interest in encoding and obfuscation, in many different forms. I will still be trying to beat it again but with different formats. But this was a big accomplishment for me.

But it's time to invest a part of those hours back to python.

Also spent some time learning aircrack. Which after day one, is fun. But pretty frustrating trying to adjust the wifi cards settings to try to get the 4 way handshake with my home ap. But I'll get there, I always do.

Side note, made it to three weeks sober. Definitely a huge contributor to my increased productivity and all around better mood. I thought though I would finally be going to bed on time because I'm not drunk in the middle of the night doing pointless stuff.

Nope, now I am still up late, sober, but doing something productive. So I don't feel all too bad. It's the only time I get after work and putting the kids to bed.

Anyways, good luck all. See you next time

Bastille - January 22, 2025, 9:46 am

(Jan 22, 2025 05:49 AM)Robert Walker Wrote: [\[CITE\]](#) Have not done full check in, in a couple of days. But I'm still at it.

Only finished one thm room - Thompson. This was fun deploying a .war on the server to gain access. Was pretty scary considering how many open servers there are out there. A lot for me to keep in mind when I finish and host my own site.

Working on sneaking past detection on a buddies app took my time for a couple days. And was ultimately successful. I don't want to put a lot out there because even the feedback I would receive was pretty vague. But I am coming out of it with a strong interest in encoding and obfuscation, in many different forms. I will still be trying to beat it again but with different formats. But this was a big accomplishment for me.

But it's time to invest a part of those hours back to python.

Also spent some time learning aircrack. Which after day one, is fun. But pretty frustrating trying to adjust the wifi cards settings to try to get the 4 way handshake with my home ap. But I'll get there, I always do.

Anyways, good luck all. See you next time

Completed the Thompson few days ago too, I'm maybe wrong but it sounds like you're starting with the oldest rooms and going toward the newest ? Personally I'm doing that haha

I'm glad to know that you succeed on the project with your friend ! I think that you spoke about it few days / weeks ago in this thread, right ?

Wifi hacking is a really satisfying hacking when it works in my opinion, keep going man :)

(Jan 22, 2025 05:49 AM)Robert Walker Wrote: [\[CITE\]](#) Side note, made it to three weeks sober. Definetly a huge contributor to my increased productivity and all around better mood. I thought though I would finally be going to bed on time because Im not drunk in the middle of the night doing pointless stuff.

Nope, now i am still up late, sober, but doing something productive. So i dont feel all too bad. Its the only time i get after work and putting the kids to bed.

Congrats buddy, from my experience of 6 years on HF I realized that alcohol and drugs issues are often a "common problem" of "hackers", many of us went through that, I've personally quite drugs (cocaine, mdma, and so on) 2 years ago, and I feel soooo much better, so I know what you mean. You're now the real you, and you're proving you that you're capable of many things. ? If you used to drink a lot, you probably had memory troubles, you'll improve your memory with time being sober and recover your capacities, it will be beneficial with your new objectives ;)

plops - January 22, 2025, 10:07 am

(Jan 22, 2025 10:46 AM)Bastille Wrote: [\[CITE\]](#) Completed the Thompson few days ago too, I'm maybe wrong but it sounds like you're starting with the oldest rooms and going toward the newest ? Personally I'm doing that haha

I'm glad to know that you succeed on the project with your friend ! I think that you spoke about it few days / weeks ago in this thread, right ?

Wifi hacking is a really satisfying hacking when it works in my opinion, keep going man :)

Congrats buddy, from my experience of 6 years on HF I realized that alcohol and drugs issues are often a "common problem" of "hackers", many of us went through that, I've personally quite drugs (cocaine, mdma, and so on) 2 years ago, and I feel soooo much better, so I know what you mean. You're now the real you, and you're proving you that you're capable of many things. ? If you used to drink a lot, you probably had memory troubles, you'll improve your memory with time being sober and recover your capacities, it will be beneficial with your new objectives ;)

Thanks man, im excited for how i mold my future. By luck and on purpose.

I might be starting with the oldest first by accident. Honestly, i go to the practice tab and just choose the first box on the first row. Maybe that is sorted by date. Makes sense, when i see dates on the servers and stuff its always 2019 lol

I was wondering if there even was any new modules, i should probably explore the site more when i get a chance haha

Bastille - January 22, 2025, 12:02 pm

Quick post today, I'm running out of SOC analysis cases with the free version of Letsdefend.io, so I'm doing courses, I started a course on Splunk as I'm planing to setup a Splunk server and make a homelab based on SOC tools.

I've completed a "big room" on THM : <https://tryhackme.com/r/room/ctfcollectionvol1> , quite easy, it's about encryption, decryption, stegano, and so on. No difficulties, it helped me to remember old

things I've already studied.

I've also worked on a thread for a new activity on HF with the Brotherhood group. Should be release soon

Keep going guys !

ttbr0 - January 22, 2025, 12:39 pm

learned how to use the yara-python library to automate compilation and matching of industry standard yara rules for malicious indicator detection. borrowed the pyinstaller sample again posted in <https://hackforums.net/showthread.php?tid=6280678> to do the testing. i used it to write a script posted here <https://hackforums.net/showthread.php?tid=6290187> to represent what a real world scanner would do with yara and it can scan a file on disk or process memory using the yara-python library. it is the "next step up" from the previous simple detection post i made here <https://hackforums.net/showthread.php?tid=6290089> which implemented custom and naive signature detections. it can also automate pyinstaller extraction and decompilation too if you are interested to see what that looks like.

Bastille - January 23, 2025, 9:32 am

I did a lot of things today, I'm increasing the number of hours I devote to learning

Not really important but I got rid off useless rooms such as :

<https://tryhackme.com/r/room/tutorial> > just to reduce number of rooms

<https://tryhackme.com/r/room/howtousetryhackme> > just to reduce number of rooms

I want to reduce the number of room remaining, I currently have 16 pages of easy room to complete (on 24).

Then I completed the following :

<https://tryhackme.com/r/room/lessonlearned> > allowed me to refresh my memory about SQLi, and practice hydra

<https://tryhackme.com/r/room/attackerkb> > web exploitation

<https://tryhackme.com/r/room/source> > web exploitation (actually the same as above)

<https://tryhackme.com/r/room/gamingserver> > crack ssh key with john, I also had to deal with an LXC exploit

About Letsdefend.io I'm running out of SOC analysis cases, as I'm limited to 15 per month with the free version... I thought about upgrading but I have a lot of free path to explore, so I'll wait for the time being. However I realized that the SOC cases with the free version are related to Tier 1 SOC analysts, and I'm targetting a Tier 2 SOC analyst position. I think I'll upgrade for few months once I've completed the free paths, and then focus on their Incident Responder paths and SOC cases (at it seems to be related to Tier 2).

On Letsdefens I started a new course : <https://app.letsdefend.io/training/lessons/security-solutions> , hope I'll finish it quickly, it's not that complicated, I already know many things.

Tomorrow I'll try to devote more time to Security+ questions, as I'm planing to pass the exam soon

Current streak :

Letsdefend.io : 25?

Tryhackme.com : 23?

padrino - January 23, 2025, 4:58 pm

Ok so this is my first check-in for the year, hopefully many more to come. I've decided to start the SOC level 1 learning path on TryHackMe. Most of my experience thus far has been in red team / pentesting training (CEH and the like) but I think career wise blue team / SOC is going to be my way into making this a career and not just a hobby.

Today I've gone over and started the Pyramid of Pain module of the learning path. Nothing new so far, all basic entry level stuff, but I want to start from the ground up to make sure I don't miss anything (even if my CS degree and 7 years as a software engineer is making the first few modules quite trivial - there's going to be blind spots I need to address, especially on the foundational knowledge).

So far my Current streak is... 1?

Really looking forward to this and making an effort to actually use my TryHackMe subscription lol

Overdose - January 23, 2025, 5:06 pm

My first check in of the year hope everyone is doing well,

It's been a while but I've started a new job, learning new skills about physical access control which is connecting dots in my head about software access control

I would like to get back on the security side of things, penetration testing etc....

Been trying to focus on making music and gaining my creativity back. We still breathing and learning!!

Bastille - January 24, 2025, 2:38 am

(Jan 23, 2025 05:58 PM)padrino Wrote: [\[CITE\]](#) Ok so this is my first check-in for the year, hopefully many more to come. I've decided to start the SOC level 1 learning path on TryHackMe. Most of my experience thus far has been in red team / pentesting training (CEH and the like) but I think career wise blue team / SOC is going to be my way into making this a career and not just a hobby.

Today I've gone over and started the Pyramid of Pain module of the learning path. Nothing new so far, all basic entry level stuff, but I want to start from the ground up to make sure I don't miss anything (even if my CS degree and 7 years as a software engineer is making the first few modules quite trivial - there's going to be blind spots I need to address, especially on the foundational knowledge).

So far my Current streak is... 1?

Really looking forward to this and making an effort to actually use my TryHackMe subscription lol
Nice to see you joined us ? can't wait to see us looking back at this thread at the end of the year saying : Damn, we did a lot this year ! Haha

Having prior experience in red team will definitely help for blue team jobs, that's what I also like in IT, you can "easily" pivot from a position to another if you want to change your career. Do you have like "dead lines" or an "objective" on when you want to start as SOC analyst ?

I agree to start from the ground it's important to start from a solid basis, and sometimes it helps to refresh memory haha

(Jan 23, 2025 06:06 PM)Overdose Wrote: [\[CITE\]](#) My first check in of the year hope everyone is doing well,

It's been a while but I've started a new job, learning new skills about physical access control which is connecting dots in my head about software access control

I would like to get back on the security side of things, penetration testing etc....

Been trying to focus on making music and gaining my creativity back. We still breathing and learning!!

Glad to see you joining us ! ? Can I ask you what's the new job ? How do you plan to get back on the security side of things, with tryhackme, hackthebox, certifications ?

padrino - January 24, 2025, 12:11 pm

(Jan 24, 2025 03:38 AM)Bastille Wrote: [\[CITE\]](#) Nice to see you joined us ? can't wait to see us looking back at this thread at the end of the year saying : Damn, we did a lot this year ! Haha

Having prior experience in red team will definitely help for blue team jobs, that's what I also like in IT, you can "easily" pivot from a position to another if you want to change your career. Do you have like "dead lines" or an "objective" on when you want to start as SOC analyst ?

I agree to start from the ground it's important to start from a solid basis, and sometimes it helps to refresh memory haha

Glad to be hear, and yeah hopefully we'll impress ourselves by how much we've learnt! I don't have a deadline as such, as a minimum I just want to be taking on more and more SOC-esque responsibilities over the course of the year, and move more into a blue team / SOC role. The problem I have is that if I take leap into another company for an entry level SOC role I will lose a good chunk of my salary, as mid level software engineers tend to bring in more than entry level SOC analysts where i'm based- so I'm trying to work my finances to make it possible.

What about yourself, what are your goals and targets for the coming year?

Bastille - January 25, 2025, 12:58 am

(Jan 24, 2025 01:11 PM)padrino Wrote: [\[CITE\]](#) Glad to be hear, and yeah hopefully we'll impress ourselves by how much we've learnt! I don't have a deadline as such, as a minimum I just want to be taking on more and more SOC-esque responsibilities over the course of the year, and move more into a blue team / SOC role. The problem I have is that if I take leap into another company for an entry level SOC role I will lose a good chunk of my salary, as mid level software engineers tend to bring in more than entry level SOC analysts where i'm based- so I'm trying to work my finances to make it possible.

What about yourself, what are your goals and targets for the coming year?

In november 2023 I went through a burnout, still recovering but I'm feeling better. My deadline would be September 2025 because in France we have some social security, if you loose your job you're still paid at 70%, and that allows me to pay the credit of my apartment. After September 2025 it will be over so I hope to fully recover and be able to work before this date.

As I already have experience as sys/network admin and in cybersecurity (GRC, audit, handling security incident, and so on ..) I'm targetting a SOC 2 position, because of the same concerns as you (money... especially about the credit of my apartment). Salary between SOC 1 and 2 can be quite different, besides SOC 1 is basically alert triage, and I think that it can become kinda annoying after few months if you're already familiar with this field, while SOC 2 is mainly based on investigations, and that's what I'm doing on HF with malware analysis :

<https://hackforums.net/showthread.php?tid=6276795>

The timeline would be the following :

- February : passing the Security+ exam (I should be fine with this)
- March : finishing almost all easy rooms on THM
- April : building my SOC home lab
- May : following tier 2 SOC analysis path on Letsdefend.io
- June : ???
- July : passing the CySa+ exam
- August : holidays
- September : back to work

During those months I still need to improve my knowledge regarding :

- Bash, PowerShell, Python, Linux

Bastille - January 25, 2025, 1:05 am

Thread bumped to not merge my posts

Yesterday I was too tired to post, but I've completed :

- <https://app.letsdefend.io/training/lessons/security-solutions> (really easy, but I wasn't aware that there were so many Proxy types, that was interesting).

- <https://tryhackme.com/r/room/whiterose> > I definitely struggled on this one, I had to use a writeup ... but I've learned a lot, especially one kind of attack I didn't know called SSTI attack (besides, I had to use again Burp and in a previous post I shared that I forgot everything about this tool, that was a good opportunity to refresh my memory).

Finally, I've completed 4 series of questions regarding Security+, here are the results based on categories : Penetration testing : 12/12 = 100%

Password concepts : 17/20 = 85.71%

Threat Actor : 2/6 = 69.23%

Malware : 9/11 = 81.82%

I messed up at the threat actor because I answered too fast and didn't read well .. Now I know that I need to devote more time even if I know I feel comfortable on the topic of the question, over confidence can be unfavorable.

I'm planing to pass the exam during February, wish me luck guys ?

Not a long post, completed the following room on THM to not loose my streak :

<https://tryhackme.com/r/room/securityawarenessintro>

Just connected on Letsdefend.io and I got by 27th streak

I've been to the tattoo this afternoon I'm exhausted, I'll devote more time tomorrow, hope you're doing your homeworks guys :) keep going !

padrino - January 25, 2025, 4:40 pm

(Jan 25, 2025 01:58 AM)Bastille Wrote: [\[CITE\]](#) In november 2023 I went through a burnout, still recovering but I'm feeling better. My deadline would be September 2025 because in France we have some social security, if you loose your job you're still paid at 70%, and that allows me to pay the credit of my apartmenet. After September 2025 it will be over so I hope to fully recover and be able to work before this date.

As I already have experience as sys/network admin and in cybersecurity (GRC, audit, handling security incident, and so on ..) I'm targetting a SOC 2 position, because of the same concerns as

you (money... especially about the credit of my apartment). Salary between SOC 1 and 2 can be quite different, besides SOC 1 is basically alert triage, and I think that it can become kinda annoying after few months if you're already familiar with this field, while SOC 2 is mainly based on investigations, and that's what I'm doing on HF with malware analysis :

<https://hackforums.net/showthread.php?tid=6276795>

The timeline would be the following :

- February : passing the Security+ exam (I should be fine with this)
- March : finishing almost all easy rooms on THM
- April : building my SOC home lab
- May : following tier 2 SOC analysis path on Letsdefend.io
- June : ???
- July : passing the CySa+ exam
- August : holidays
- September : back to work

During those months I still need to improve my knowledge regarding :

- Bash, PowerShell, Python, Linux

Glad to hear you're doing better man, and sorry to hear you had to deal with it in the first place - can happen to anyone though, especially if you're a driven person aiming for success, which it sounds like you are.

Have you had a look at codecademy at all? I had to do some Python when I was in University and it was a pretty useful resource, although I've not used it for a long time. I'm pretty sure it has bash on there too.

Oh also, forgot to add what I did today:

I've been pretty wiped out today so only managed to get through the next room on the Cyber Defense Frameworks module of the TryhackMe SOC learning path. Pretty dry and I've already covered it on my CEH certification training but I got through it and captured the flag (somewhat, unenthusiastically) so counting that as a small win for today considering how unmotivated I was. Just looking forward to getting past the framework stuff and into the actual hands on stuff.

Think I left it more than 24 hours since my last attempt on THM so my streak is back down to 1 ?

Oh and also, to anyone planning on doing the CEH at any point [this](#) book is a pretty great study companion. It's a bit old now but the core concepts are still valid.

Bastille - January 26, 2025, 4:18 pm

[Bumping the thread to not merge my posts]

Completed a Nessus based room on THM

Complete some courses about Logs on Letsdefend.io

Went through some quizz on examcompass for the Security + cert :

Hashing : 7/7 = 100

Social engineering 14/14 = 100

Encryption : 22/36 = 61.1

Encryption is definitely one of my weakest point, I need to work on that, there are so many things between symmetric and assymetric, also about CBC, GCM, and other things like that ...

I think I'll use notion for my revision on this topic, but to be honest I think I'm not far of being able to get the cert. I've already studied to get Security+ like 3 years ago but I've fogot many things and the topics slightly changed too, I just need to referesh my memory and some update.

I think we've lost few members on the road ...

Current streak :
Letsdend.io : 28?
Tryhacme.com : 26?

padrino - January 26, 2025, 4:39 pm

Ok so check-in for Sunday, had a lot on today but I managed to get a few things squeezed in before the day was over.

I'm so done with Cyber Defense Frameworks I can't look at them any longer... I'm going to dip in and out of one each week because doing them day after day is driving me insane. Today instead I moved onto Learning some threat intelligence tools, far more interesting and it worked well to keep me motivated. I looked into using urlscan.io and abuse.ch - pretty interesting stuff. I've also been going over my old CEH notes to keep that tiking over in my head, little bit of late night reading to keep it fresh.

I hope you guys have had a great day and are staying productive! Even if you can only manage to spare a few minutes, it's better than nothing.

I'm taking the approach my guitar teacher always says, 10 minutes a day 7 days a week is better than an hour once a week. It worked with the guitar so i have to figure it would work here too lol

Get after it guys, My streak is now sitting at a pretty hefty 2...?

(Jan 26, 2025 05:18 PM)Bastille Wrote: [\[CITE\]](#) Encryption is definitely one of my weakest point, I need to work on that, there are so many things between symmetric and assymetric, also about CBC, GCM, and other things like that ...

Man encryption has always been a blind spot for me, asside form the basics of symmertric, assymetric, private and public keys, and certificates and certificate authorities my knowledge is pretty sparse. As a developer my philosophy has always been I'll use what everyone else thinks is the best and not worry about how it works too much... the guys who develop the encryption algorithms are much smarter than me lol

Oh I forgot to mention I've also signed up to LetsDefend. Never heard of it before seeing it on this thread, but I've enrolled on the Incident responder path and looking forward to diving into that a little too.

Bastille - January 27, 2025, 10:38 am

(Jan 26, 2025 05:39 PM)padrino Wrote: [\[CITE\]](#) Oh I forgot to mention I've also signed up to LetsDefend. Never heard of it before seeing it on this thread, but I've enrolled on the Incident responder path and looking forward to diving into that a little too.

Congrats for the Incident Responder path ! If I'm not wrong it should be the equivalent of Tier 2 SOC Analyst, let me know your feeling on it after few days / weeks, I thought about purchasing a VIP account for few months for those additional paths that sound more interesting and related to what I want to do.

Quickly :

- Completed few courses on Letedefend
- Completed 2 rooms on Tryhackme :

<https://tryhackme.com/r/room/bsidesgtdav> :

- I'm now more familiar with : reverse shells, sudo -l priv esc
- I've discovered a new tool named "cadaver", that seems to be used for "WebDav"

- I've discovered that you can upload with curl and the argument -X and the method "PUT", I used to use curl to retrieve content from webpages, I now know that you can also upload

<https://tryhackme.com/r/room/mkingdom>

I've spent a lot of time on HF for many things, speaking with people, replying to threads, working on cybersecurity related tutorials, didn't had enough time for some Security+ exams, will work on it tomorrow.

Good night fellows see you tomorrow :)

padrino - January 28, 2025, 8:56 am

Small update from me today, chaps - mad busy in work and out with the family immediately after so study time today will be pretty sparse. I did however manage to get some time on TryHackMe and did a few bits of theory on the unified kill chain model. Not much but it's enough to keep my streak alive and it's better than nothing!

Hope you all had a productive day!

Bastille - January 29, 2025, 4:40 am

Posting for yesterday, I wasn't in a good mood at the end of the day.

Completed 2 rooms on tryhackme.com :

<https://tryhackme.com/r/room/compiled>

<https://tryhackme.com/r/room/gallery666>

Completed one course on letsdefend.io :

<https://app.letsdefend.io/training/lessons/incident-management-101>

I also worked on Security+ with 2 quizz :

Application attacks : 6/9 =66.67

Data protection concepts : 15/18 / 83.33

I was kinda disappointed regarding application attacks, I need to work more on the security+ cert. Planing to pass the exam by the end of February

[Overdose](#) [ubermensch38](#) [capt_nemo](#) [Tyr](#) [TENET](#) [Miracula](#) [Mexicano](#) hope you're doing well and you keep going guys. It's been already 1 month since I made this thread, 1 month over 12, don't procrastinate guys, time flies ...

padrino - January 29, 2025, 3:48 pm

Another dire check-in from me today - been out visiting family again in the evening but back to the grind tomorrow. I have however managed to get a small amount of time time free and I've managed to do more reading on defense frameworks on THM, and I've also been learning about of dark web monitoring service we use in work - hands on experience with real tools in my industry is a pretty great step in the drierction I want to go so I'm counting it!

Stay productive guys!

Bastille - January 29, 2025, 9:51 pm

Posting for yesterday, started a course on Letsdefend.io but I need to upgrade to answer questions because I need to connect to a RDP which is a limited feature with a free account.

Answered few questions on tryhackme, just to keep the streak.

I was less assiduous during the two previous days, I'll spend more time learning for the next days.

Also planing to buy some components to make a server for my SOC-based homelab. I think I'll go with a Ryzen 9 5950X, I thought about the Ryzen 7 5700G as it as an integrated GPU, but I'm afraid that 8/16 couldn't be enough to handle the workload with many servers, especially the SIEM and the SOAR.

Buffet_Serrano - January 29, 2025, 10:26 pm

new to the chat and looking to communicate with some like minded people... i have been takking cyber security pretty serious for about 2 months now but have always been interested , but these past few months ive locked in and decided to take it serious.... im currently learning about enumeration with nmap from host, to network, to web service/app enumeration... ive also learned about scoping, virtual machines , enviroments. the resourcefulness of the many methodolgies with att&ck being my favorite so far ...and now that im at the vulnerability scanning phase of my journey it would help alot to have some people to ask questions and yes im doing the cisco ethical hacking course some stuff seems outdated but amongst a lot of other leanring avenues that is my foundation any thoughts or advice ?

Bastille - January 29, 2025, 11:05 pm

(Jan 29, 2025 11:26 PM)Buffet_Serrano Wrote: [\[CITE\]](#) new to the chat and looking to communicate with some like minded people... i have been takking cyber security pretty serious for about 2 months now but have always been interested , but these past few months ive locked in and decided to take it serious.... im currently learning about enumeration with nmap from host, to network, to web service/app enumeration... ive also learned about scoping, virtual machines , enviroments. the resourcefulness of the many methodolgies with att&ck being my favorite so far ...and now that im at the vulnerability scanning phase of my journey it would help alot to have some people to ask questions and yes im doing the cisco ethical hacking course some stuff seems outdated but amongst a lot of other leanring avenues that is my foundation any thoughts or advice ?

Welcome to HF buddy, there are many (me included) cybersecurity experts and enthusiasts here. I highly recmmend you to check my thread :

<https://hackforums.net/showthread.php?tid=6263412> (feel free to leave a post, that helps ..)

I've made it as I wish I had it when I started 6 years ago. You can also share your daily progresses on this thread, we try to motivate each of us to study (even a little bit) every day. We'll start a new month soon, it would be nice to count you among us !

Buffet_Serrano - January 30, 2025, 8:59 am

(Jan 30, 2025 12:05 AM)Bastille Wrote: [\[CITE\]](#) Welcome to HF buddy, there are many (me included) cybersecurity experts and enthusiasts here. I highly recmmend you to check my thread :

<https://hackforums.net/showthread.php?tid=6263412> (feel free to leave a post, that helps ..)

I've made it as I wish I had it when I started 6 years ago. You can also share your daily progresses on this thread, we try to motivate each of us to study (even a little bit) every day. We'll start a new month soon, it would be nice to count you among us !

exactly what i was looking for !! someting where i can feel a sense of community and accountability...easy to lose track doin this alone

Bastille - January 30, 2025, 9:34 am

(Jan 30, 2025 09:59 AM)Buffet_Serrano Wrote: [\[CITE\]](#) exactly what i was looking for !! something where i can feel a sense of community and accountability...easy to lose track doing this alone
You're welcome buddy, you'll see by yourself that HF is a strong community, the forum exists since 2007 and we have a lot of professionals. Don't forget to leave a post in the thread and feel free to come back to post here your progresses whenever you want !

For my part, I've completed a course on letdefend.io just to keep the streak :
https://app.letsdefend.io/training/lesson_detail/introduction-to-it-security-basis-for-corporates

I've completed a room that I really liked on tryhackme.com :
<https://tryhackme.com/r/room/reverselfiles> , it allowed me to :
- discover ltrace debugging tool
- get more familiar with Ghidra and RE

I really enjoy RE but I definitely need to get more into programming (that's on to do list)

I tried to start <https://tryhackme.com/r/room/wreath> but I encountered an issue generating the .ovpn file on their website, it seems to be a common issue, I'll try tomorrow after I did few things recommended by the support.

Keep going guys, January is almost done, let's start a new month soon :)

Current streak :
Letsdefend.io : 32 ?
Tryhackme.com : 30 ?

SIM-5614280 - January 30, 2025, 10:56 am
Hello everyone, Glad to be here.

lams - January 31, 2025, 1:27 am
Such a great thread! Thanks a mil for suggesting this great challenge and for sharing learning resources!

Bastille - January 31, 2025, 3:07 pm
(Jan 30, 2025 11:56 AM)FabFox007 Wrote: [\[CITE\]](#) Hello everyone, Glad to be here.
(Jan 31, 2025 02:27 AM)lams Wrote: [\[CITE\]](#) Such a great thread! Thanks a mil for suggesting this great challenge and for sharing learning resources!
Hope to see you both active guys ! Feel free to share your daily progresses whenever you want

Completed 2 courses on Letsdefend.io, I want to smash the first SOC Analyst path to then move to Incident Responder path (which seems to be more related to tier 2 SOC analyst).

Completed an easy room about few cybersecurity topics on THM just to keep my streak.

I had a lot of things to do today, will spend more time learning tomorrow

Current streak :
- Letsdefend.io : 33 ?
- Tryhackme.com : 31 ?

SIM-5614029 - January 31, 2025, 11:43 pm

Nice concept! goodluck all

Bastille - January 31, 2025, 11:49 pm

(Feb 1, 2025 12:43 AM)laslaslaslas Wrote: [\[CITE\]](#) Nice concept! goodluck all
Thanks buddy, hope to see you participating ;) it's a good way to exchange with people about hacking / programming / cybersecurity and other, and learn from them !

TENET - February 1, 2025, 2:02 am

I've recently been working on antivirus circumvention, and it works very well, perfectly bypassing windows defender to execute other commands without being detected!~~~^_^

Bastille - February 1, 2025, 2:13 am

(Feb 1, 2025 03:02 AM)TENET Wrote: [\[CITE\]](#) I've recently been working on antivirus circumvention, and it works very well, perfectly bypassing windows defender to execute other commands without being detected!~~~^_^

I would love to hear more about this topic, I posted about this topic on this thread and I thought about reading the following books :

(Jan 16, 2025 02:56 AM)Bastille Wrote: [\[CITE\]](#) That's definitely a good idea, I've seen few books that could help, such as (amazon links) :

- [Malware Development for Ethical Hackers: Learn how to develop various types of malware to strengthen cybersecurity](#)
 - [Evading EDR: The Definitive Guide to Defeating Endpoint Detection Systems](#)
 - [Evasive Malware: A Field Guide to Detecting, Analyzing, and Defeating Advanced Threats](#)
- I'm wondering if they are worth it

If you want to make a thread to explain this it would definitely be cool ! ?

Bastille - February 1, 2025, 9:30 am

[Bumped my thread so my posts will not be merged]

Completed 2 courses on letsdefend and 1 challenge :

<https://app.letsdefend.io/training/lessons/building-a-soc-lab-at-home>

<https://app.letsdefend.io/training/lessons/building-malware-analysis-lab>

<https://app.letsdefend.io/challenge/brute-force-attacks>

Completed 1 easy room on tryhackme just to keep the streak :

<https://tryhackme.com/room/tickets1>

I spent a lot of time on other things for HF this morning, wasn't able to devote more time to learn ...

[ttbr0](#) I bought "Joy of programming" on Steam :

https://store.steampowered.com/app/2216770/JOY_OF_PROGRAMMING_Software_Engineering_Simulator/

Could be a fun way to practice more on Python, I guess. I'll see how it goes, the game has good reviews so far, but it's really new.

I would love to devote everyday :

- 1 hour on letsdefend
- 1 hour on tryhackme
- 1 hour on my security+ cert
- 1 hour on Python
- 1 hour on Linux

I would be nice to also add 1 hour of sport every day too, I need to go back to the gym, but mixing everything is kinda exhausting after a burnout, I need to chill sometimes

plops - February 2, 2025, 7:47 am

(Feb 1, 2025 10:30 AM) Bastille Wrote: [\[CITE\]](#) I bought "Joy of programming" on Steam : https://store.steampowered.com/app/2216770/JOY_OF_PROGRAMMING_Software_Engineering_Simulator/

Could be a fun way to practice more on Python, I guess.

....

I would be nice to also add 1 hour of sport every day too, I need to go back to the gym, but mixing everything is kinda exhausting after a burnout, I need to chill sometimes

Hey that's cool, I never though of looking into a simulator like that. Honestly i need to dust off my Arduino and use python on it. Hmm.

Always beed to make time to work out man, the body needs it. It craves it!

Checking in after a bit. Still going strong and doing something each day.

As far as hacking goes, I participate in thm everyday, at least one hour. I've really started to focus on independence when it comes to the rooms. Which, naturally, makes them take longer but it is rewarding. Burpsuite, hydra, the different '..

busters', xss, sqli, idor etc... aren't such foreign concepts anymore. I have a list to go through and clues to look for now. When it is finally exhausted, I know there is something new to learn.

I have kind of fell off on python for a bit. But that time has been spent stepping back into full stack web development. LAMP, but really focused on php atm.

I have a project I want to accomplish that will be beneficial to a niche community but also hopefully make me a couple dollars a month on a subscription or pay as you use type thing. So not necessarily hacking, but the red team stuff I am learning has made me very aware of keeping the app as tight as i can.

Still sober, 32 days. I have not been this sober since i was 19, in boot camp. Crazy, still feeling the productivity boost unless i am on a win streak at LoL and my video games addiction kicks in.

mdmaty - February 2, 2025, 9:10 am

Woow thank u for this experirnce

padrino - February 2, 2025, 4:00 pm

Pretty bad weekend for me - managed to get a little bit done though. I've been building on my phishing and phishtool learning on the SOC course on tryhack me. Learning about Email Indicators of Compromise among other things. This week has been pretty dire for me I'm not going to lie and I've broken my streak on THM but I've tried to squeeze in a bit of learning here and there when I can. Hoping this week will be a bit chillier so i can really get my nose to the grindstone.

ttbr0 - February 2, 2025, 10:14 pm

if anyone cares about advice on learning, my recommendation is to not stay too comfortable for too long. always aim to push your boundaries and be just out of your comfort zone and abilities. it is also a mistake to jump too far out of your depth because progress will be less efficient. imagine you are climbing a ladder, try to go 2 steps at a time and not 3 if you cannot realistically achieve it.

TheGoldenRelik - February 2, 2025, 10:17 pm

Is there any good source for learning social engineering?

Bastille - February 3, 2025, 3:35 am

(Feb 2, 2025 05:00 PM)padrino Wrote: [\[CITE\]](#) Pretty bad weekend for me - managed to get a little bit done though. I've been building on my phishing and phishtool learning on the SOC course on tryhack me. Learning about Email Indicators of Compromise among other things. This week has been pretty dire for me I'm not going to lie and I've broken my streak on THM but I've tried to squeeze in a bit of learning here and there when I can. Hoping this week will be a bit chillier so i can really get my nose to the grindstone.

Sorry to hear that, hope you're doing better.

Feel free to check this thread if you're interested in email analysis :

<https://hackforums.net/showthread.php?tid=6255999> (i've made it based on this book :

<https://a.co/d/8PG4fZt> , I'll try to summerize other parts of the book and share here on HF)

Don't worry about the streak, as long as you're constant in your learning it's the most important, feel free to take a break when you need !

(Feb 2, 2025 11:14 PM)ttbr0 Wrote: [\[CITE\]](#) if anyone cares about advice on learning, my recommendation is to not stay too comfortable for too long. always aim to push your boundaries and be just out of your comfort zone and abilities. it is also a mistake to jump too far out of your depth because progress will be less efficient. imagine you are climbing a ladder, try to go 2 steps at a time and not 3 if you cannot realistically achieve it.

Definitely a relevant advice !

(Feb 2, 2025 11:17 PM)TheGoldenRelik Wrote: [\[CITE\]](#) Is there any good source for learning social engineering?

Take a look at tryhackme.com and at Christopher Hadnagy's books, they are available on Amazon

padrino - February 3, 2025, 4:59 pm

OK Check-in time! Today I've been diving into the inrto to endpoint security module on TryHackMe. I've been going over and getting to grips with the core windows processes that usually run on a machine and have also been looking into the Sysinternals tool set that allows for more in-depth monitoring of processes and network activity. There's like 70+ tools in that package but the main ones we focus on in that intro room are TCP View and Process Explorer. Interesting stuff!

Hope you've all had a productive day!

Bastille - February 3, 2025, 11:55 pm

Checking in for yesterday :

- Completed 1 Letsdefend course (CTI), and completed 3 SOC analysis cases (they were a part of the course)
- Started an Advent of Cyber room on tryhackme.com, I plan to go through all of them, I'll try to do at least 3 "days" per day
- Went through a series of questions on examcompass.com for the Security+ cert, I struggled on questions about encryption, certificates and signatures, I need to devote like a hour or two, and write every of them in a notebook and compare them and learn.

I feel that as we don't write we memorize less, we don't always think about hand writing because we're studying on computers, but we definitely need to go back to the old methods to improve the retention rate.

I'm almost stuck on Letsdefend.io because of the limitations free version, thinking about getting either the VIP or VIP+, I'll maybe start with monthly VIP, and then upgrade to monthly VIP+ whenever I complete all VIP courses and feel limited again.

Regarding tryhackme.com I have so many rooms for free to complete, no need to go with the Premium version for the time being.

Current streak

Letsdefend.io : 36 ?

Tryhackme : 34 ?

OtherBarry - February 4, 2025, 12:17 pm

Just pawned meow on Hack The Box! Sidenote: the website offered using "OpenVPN" and I thought it was the website OpenVPN(.)net. Was a head scratcher trying to figure out why I had to use a VPN service to connect to HackTheBox vpn lol.

Bastille - February 5, 2025, 12:29 am

(Feb 4, 2025 01:17 PM)OtherBarry Wrote: [\[CITE\]](#) Just pawned meow on Hack The Box! Sidenote: the website offered using "OpenVPN" and I thought it was the website OpenVPN(.)net. Was a head scratcher trying to figure out why I had to use a VPN service to connect to HackTheBox vpn lol.

Haha that's also how we learn, when facing issues ! How did you connect the VPN, through Windows or Linux ? Did you go with Kali ? Are you familiar already with hacking ?

Posting for yesterday :

- Completed 1 SOC case analysis
- Completed 1 day (about Burp) on the Advent of Cyber
- Performed 2 malware analysis on HF, one was malicious : Malicious :

<https://hackforums.net/showthread.php?pid=62666100>

Not malicious : <https://hackforums.net/showthread.php?pid=62667135#pid62667135>

Hope you guys keep going !

Current Streak :

Letsdefend.io : 38 ?

Tryhackme.com : 36 ?

OtherBarry - February 5, 2025, 4:45 am

(Feb 5, 2025 01:29 AM)Bastille Wrote: [\[CITE\]](#) Haha that's also how we learn, when facing issues ! How did you connect the VPN, through Windows or Linux ? Did you go with Kali ? Are you familiar already with hacking ?

Posting for yesterday :

- Completed 1 SOC case analysis
- Completed 1 day (about Burp) on the Advent of Cyber
- Performed 2 malware analysis on HF, one was malicious : Malicious :

<https://hackforums.net/showthread.php?pid=62666100>

Not malicious : <https://hackforums.net/showthread.php?pid=62667135#pid62667135>

Hope you guys keep going !

Current Streak :

Letsdefend.io : 38 ?

Tryhackme.com : 36 ?

Very True! Yes I connected through Kali. A few years ago I got recommended OverTheWire as an introduction to Linux so I do have some familiarity.

Current Streak:

Hackthebox.com: 2 ?

Completed Tier 1 yesterday!

SIM-5614029 - February 5, 2025, 11:34 am

Hi,

So to finally be consistent in my journey i will also keep a daily log in this forum.

So far ive been busy with my own infotree on how to execute a pentest operation. On which i also have a question (see below) (1)

Currently busy with reading nmap's e-book. answered a few questions i had so far.

Also active on HTB although i have been lacking so far this year, maybe logged in at most 6 times since 01-01.

I will also keep my streak updated.

My questions,

Currently i am stuck on thinking of ways that malware or any initial acces payloads are generated, what i have so far are:

(please keep in mind i am a total novice to this. some of these might not even work anymore.)

1. Malware

Hiding the malware in a file.

Hiding the malware inside a locked .zip folder.

Malicious links.

2. Reverse shell/executing files

3. LNK shortcuts

4. Fysicial delivery (badusb)

5. Acces brokers.

I would appreciate it if this list could be stretched a bit more with your input

Same thing for maintaining access after getting initial access, i have read one of the ways would be NETCAT or something like DNS tunneling. however for netcat an external program needs to be installed and i do not know if i am a big fan of that since i would like to do as little as possible to avoid any detection. (this does not mean i am lazy and don't want to put anything in, i am willing to go as far as needed)

Also for this i would greatly appreciate if any of you guys can add more to the list!

Last but not least:

Thank you for taking your precious time to read my message and hopefully answer any of my questions.

My pm is always open for any debates, tips or any talk! i will also always answer when tagged in this thread!

Again thank you for your time and i look forward to speaking to you!

bye,

Bastille - February 6, 2025, 2:35 am

(Feb 5, 2025 12:34 PM)laslaslaslas Wrote: [\[CITE\]](#) Hi,

So to finally be consistent in my journey i will also keep a daily log in this forum.

Glad to see you back !

(Feb 5, 2025 12:34 PM)laslaslaslas Wrote: [\[CITE\]](#) My questions,

Currently i am stuck on thinking of ways that malware or any initial acces payloads are generated, what i have so far are:

(please keep in mind i am a total novice to this. some of these might not even work anymore.)

1. Malware

Hiding the malware in a file.

Hiding the malware inside a locked .zip folder.

Malicious links.

2. Reverse shell/executing files

3. LNK shortcuts

4. Fysicial delivery (badusb)

5. Acces brokers.

I would appreciate it if this list could be stretched a bit more with your input

I think there are many things to clarify, "How malware are generated ?" :

> you can program them, mostly using C/C++, also via higher level languages such as Python, or even lower like ASM. This requires programming skills, and also a lot of knowledge on how systems work (like : system files, .dll, services, processes, threads, registry, ...)

> you can generate payloads with tools such as metasploit (basically, you enter some information required for each payload, like : local IP (your IP), remote IP (the target), same for the ports, and so on... take a look at metasploit.

> you can also find payloads online, such as through : db-exploit, github, ...

"How do you get an initial access ?" :

> You need to scan the target with nmap, find a vulnerability, and exploit it. Usually, you run the "-sV" options to get the version of the service running. If a service is outdated, there chances that an exploit is available. For this, you can use : searchsploit on Kali, exploit-db, ...

> You can also get initial access with other methods such as bruteforcing with Hydra.

Regarding your list, maybe you were asking "How to deliver a malware ?" ? There are many ways :

> Trojan : embedded the payload in the "legit" tool, that often happens on cracked software, you think you get a free tool that is supposed to be paid, but you've been actually infected.

> Dropper : you make a powershell script that will download the real payload

> Loader : lighter than droppers, try to be more silent, less detectable, they also don't write files if I'm not wrong and store every thing in the RAM

Locked .zip files are used to avoid AV engines scanning.

(Feb 5, 2025 12:34 PM)laslaslaslas Wrote: [\[CITE\]](#) Same thing for maintaining access after getting initial access, i have read one of the ways would be NETCAT or something like DNS tunneling. however for netcat an external program needs to be installed and i do not know if i am a big fan of that since i would like to do as little as possible to avoid any detection. (this does not mean i am lazy and don't want to put anything in, i am willing to go as far as needed)

> You can add persistancy (through scheduled tasks or registry)

> You can open the firewall to allow remote access (requires to get an access to another computer

from the same network, or to open the required port on the router and allow traffic)

> You can install a RAT

This topic is almost limitless, there are a lot of things about it, but I think that's a good start point with the content above

SIM-5614029 - February 6, 2025, 6:17 am

Quote:I think there are many things to clarify, "How malware are generated ?" :

> you can program them, mostly using C/C++, also via higher level languages such as Python, or even lower like ASM. This requires programming skills, and also a lot of knowledge on how systems work (like : system files, .dll, services, processes, threads, registry, ...)

> you can generate payloads with tools such as metasploit (basically, you enter some information required for each payload, like : local IP (your IP), remote IP (the target), same for the ports, and so on... take a look at metasploit.

> you can also find payloads online, such as through : db-exploit, github, ...

Hey, Thanks for replying!

What i meant with the generating of malware/initial access would be what ways there are to gain control over a system, i summed to many different things up unto 1 question, this may give any confusion. I was indeed more looking into how malware are delivered and how initial access is gained instead of how malware are actually created.

To clarify my question a bit with my lists:

Delivery of malware, in ways like,

1. SMTP,
2. SMS.
3. Physical delivery like badusb.
4. QR codes
5. URLs

Gaining initial access in ways like,

1. Acces brokers.
2. Exploiting vulnerabilities as you mentioned
3. Trojans as you mentioned

Quote:"How do you get an initial access ?" :

> You need to scan the target with nmap, find a vulnerability, and exploit it. Usually, you run the "-sV" options to get the version of the service running. If a service is outdated, there chances that an exploit is available. For this, you can use : searchsploit on Kali, exploit-db, ...

> You can also get initial access with other methods such as bruteforcing with Hydra.

Locked .zip files are used to avoid AV engines scanning.

I was aware of this but still thank you for reminding me.

Quote:

Regarding your list, maybe you were asking "How to deliver a malware ?" ? There are many ways :
> Trojan : embedded the payload in the "legit" tool, that often happens on cracked software, you think you get a free tool that is supposed to be paid, but you've been actually infected.

> Dropper : you make a powershell script that will download the real payload

> Loader : lighter than droppers, try to be more silent, less detectable, they also don't write files if I'm not wrong and store every thing in the RAM

These answers gave me a better picture, Thank you!

Quote:> You can add persistancy (through scheduled tasks or registry)

> You can open the firewall to allow remote access (requires to get an access to another computer from the same network, or to open the required port on the router and allow traffic)

> You can install a RAT

These also gave me a better picture on how to act during such a situation.

Do you know this out of your head or do you use a specific source?

If interested i could send you my infotree in pm to give you a better picture of my knowledge, do not feel obliged to do so tho, i understand you are a busy person!

My update on my progress will be posted later on!

bye,

Bastille - February 6, 2025, 8:31 am

(Feb 6, 2025 07:17 AM)laslaslaslas Wrote: [\[CITE\]](#) Do you know this out of your head or do you use a specific source?

Out of my head, but there are many more answers, I would need to write many pages to mention every possibility.

(Feb 6, 2025 07:17 AM)laslaslaslas Wrote: [\[CITE\]](#) If interested i could send you my infotree in pm to give you a better picture of my knowledge, do not feel obliged to do so tho, i understand you are a busy person!

Feel free to send

Posting for yerstday :

- Completed 1 SOC case on letsdefend.io
- Completed 2 "days" on tryhackme.com (one about SQLmap, which was really interesting, and another one on XSS and ZAP)

Bastille - February 6, 2025, 8:54 am

Bumped the thread to not merge my posts

Completed 1 SOC analysis case on Letsdefend, I feel really more comfortable since I have been practicing every day for more than a month.

Answered few questions on Tryhackme to not loose my streak.

I've mostly been working on Security+ today; made some revision sheets on Notion about :

- Windows IOC
- MITRE matrice
- Encryption

As I've worked on encryption (because it's my main weak point regarding the Security+ cert) I gave a second try to questions about this topic on <https://www.examcompass.com/>

First series > 22/36 good questions = 61.1% of good answers

Second series > 27/36 good questions = 75% of good answers

I've worked mainly on symetric and asymetric algorithms, those used for digital signatures, and so on ... Now I need to study about those things called CBC, ECB, GCM and stuff, about block and stream cipher. I'll do it tomorrow

Hope you keep going guys !

Current Streak :

Letsdefend.io : 39 ?

Tryhackme.cm : 37 ?

SIM-5614029 - February 7, 2025, 2:19 pm

Today is weekend!

Didn't do much today since i was busy with rl occupations.

Will do at least 2 hours of research tomorrow, 2-3 hours of training and 2 hours of reading tomorrow.

How did your day go?

Have a nice weekend

OtherBarry - February 7, 2025, 4:28 pm

Turns out no matter how well you keep your laptop, fans will always fail at some point. Have to re-start my streaks :(

HackTheBox.com: 1?Finished tier 2 of starting point.

Also, gobuster + common.txt = ;)

Song of the day: Todo o Mundo e Ninguém - Quarteto 1111

Bastille - February 7, 2025, 10:52 pm

(Feb 7, 2025 03:19 PM)laslaslaslas Wrote: [\[CITE\]](#) Today is weekend!

Didn't do much today since i was busy with rl occupations.

Will do at least 2 hours of research tomorrow, 2-3 hours of training and 2 hours of reading tomorrow.

How did your day go?

Have a nice weekend

If you can study so many hours it would be awesome !

(Feb 7, 2025 05:28 PM)OtherBarry Wrote: [\[CITE\]](#) Turns out no matter how well you keep your laptop, fans will always fail at some point. Have to re-start my streaks :(

HackTheBox.com: 1?Finished tier 2 of starting point.

Also, gobuster + common.txt = ;)

No worries buddy, as long as you're regular it's worth it ! Gobuster is definitely a must have tool, if you're into fuzzing you should also take a look at FUFF and WFUZZ.

Posting for yesterday, completed 1 SOC analysis case on letsdefend.io

Completed 3 days of an Advent of Cyber (about : Wireshark, nmap, and FTP)

Didn't have a lot of time yesterday, I wanted to continue to study for the Security+ cert but I went out with friends, it's also important to rest sometimes.

I didn't sleep very well, but today I hope I'll be able to complete :

- 1 SOC analysis case

- 3 days of the Advent of Cyber
- Continue to study for the Security+ cert (I'll work on these MFs CBC, ECB, GCM, and so on things I don't know what they do).

Keep going guys, feel free to share your progresses :)

SIM-5614029 - February 8, 2025, 5:34 am

(Feb 7, 2025 05:28 PM)OtherBarry Wrote: [\[CITE\]](#) Turns out no matter how well you keep your laptop, fans will always fail at some point. Have to re-start my streaks :(

HackTheBox.com: 1?Finished tier 2 of starting point.

Also, gobuster + common.txt = ;)

Song of the day: Todo o Mundo e Ninguém - Quarteto 1111

Where did you train gobuster? just form its basic manual or from a medium?

Thanks in advance!

raceconditioned - February 8, 2025, 6:09 am

You will need to become familiar with grabbing all those tools and checking their help page and experimenting. Medium or not, it's a matter of always running it against a test website (for example you could put some hidden file z4434xcef234.txt and have it in the wordlist you feed to gobuster and see if it will find it).

This approach you will learn and know what's going on exactly.

Most of these fuzzers such as GoBuster/ffuf have an option to proxy their HTTP traffic, so learn to configure to run through Burp Suite so you can watch what requests they send and learn or modify any configuration.

PS: One extra encoding level or `\'`, will yield different results sometimes.

Bastille - February 8, 2025, 10:25 am

(Feb 8, 2025 06:34 AM)laslaslaslas Wrote: [\[CITE\]](#) Where did you train gobuster? just form its basic manual or from a medium?

Thanks in advance!

(Feb 8, 2025 07:09 AM)raceconditioned Wrote: [\[CITE\]](#) You will need to become familiar with grabbing all those tools and checking their help page and experimenting. Medium or not, it's a matter of always running it against a test website (for example you could put some hidden file z4434xcef234.txt and have it in the wordlist you feed to gobuster and see if it will find it).

This approach you will learn and know what's going on exactly.

Most of these fuzzers such as GoBuster/ffuf have an option to proxy their HTTP traffic, so learn to configure to run through Burp Suite so you can watch what requests they send and learn or modify any configuration.

PS: One extra encoding level or `\'`, will yield different results sometimes.

Don't forget to quote or mention other members when you reply, otherwise they'll not receive notifications ?

I worked a looooooot on my Security+ cert today, so less time for Tryhackme and Letsdefend. I managed to keep my streaks tho, so it's good. I'm feeling more comfortable with the Encryption domain. I was at 90% of good answers on the quizz, the next "domain" will be about US laws, administrative stuff, and so on, that I'm not familiar with as I'm not leaving in the US. I'm not really concerned by these things but I have to so ... Besides with such certs I could be able to work in the US, who knows, maybe one day I'll give a try for a couple of years.

For those interested, I'm making my "revision sheets" (not sure about the expression) on Notion, it helps me a lot to study, here is a preview :

Current Streak :
Letsdefend.io : 40 ?
Tryhackme.com : 38 ?

Hope you keep going guys !

raceconditioned - February 8, 2025, 10:26 am

(Feb 8, 2025 11:25 AM)Bastille Wrote: [\[CITE\]](#) Don't forget to quote or mention other members when you reply, otherwise they'll not receive notifications ?

I worked a looooooot on my Security+ cert today, so less time for Tryhackme and Letsdefend. I managed to keep my streaks tho, so it's good. I'm feeling more comfortable with the Encryption domain. I was at 90% of good answers on the quizz, the next "domain" will be about US laws, administrative stuff, and so on, that I'm not familiar with as I'm not leaving in the US. I'm not really concerned by these things but I have to so ... Besides with such certs I could be able to work in the US, who knows, maybe one day I'll give a try for a couple of years.

For those interested, I'm making my "revision sheets" (not sure about the expression) on Notion, it helps me a lot to study, here is a preview :

Current Streak :
Letsdefend.io : 40 ?
Tryhackme.com : 38 ?

Hope you keep going guys !

Good luck studying and doing labs, precious time and try to enjoy it and ask a lot and learn, time you cannot regain back or won't have energy to spend in the future possibly.

SIM-5614029 - February 8, 2025, 10:44 am

(Feb 8, 2025 07:09 AM)raceconditioned Wrote: [\[CITE\]](#) You will need to become familiar with grabbing all those tools and checking their help page and experimenting. Medium or not, it's a matter of always running it against a test website (for example you could put some hidden file z4434xcef234.txt and have it in the wordlist you feed to gobuster and see if it will find it).

This approach you will learn and know what's going on exactly.

Most of these fuzzers such as GoBuster/ffuf have an option to proxy their HTTP traffic, so learn to configure to run through Burp Suite so you can watch what requests they send and learn or modify any configuration.

PS: One extra encoding level or `\'`, will yield different results sometimes.

(Feb 8, 2025 11:25 AM)Bastille Wrote: [\[CITE\]](#) Don't forget to quote or mention other members when you reply, otherwise they'll not receive notifications ?

I worked a looooooot on my Security+ cert today, so less time for Tryhackme and Letsdefend. I managed to keep my streaks tho, so it's good. I'm feeling more comfortable with the Encryption domain. I was at 90% of good answers on the quizz, the next "domain" will be about US laws, administrative stuff, and so on, that I'm not familiar with as I'm not leaving in the US. I'm not really concerned by these things but I have to so ... Besides with such certs I could be able to work in the US, who knows, maybe one day I'll give a try for a couple of years.

For those interested, I'm making my "revision sheets" (not sure about the expression) on Notion, it helps me a lot to study, here is a preview :

Current Streak :

Letsdefend.io : 40 ?

Tryhackme.com : 38 ?

Hope you keep going guys !

(Feb 8, 2025 11:26 AM)raceconditioned Wrote: [\[CITE\]](#) Good luck studying and doing labs, precious time and try to enjoy it and ask a lot and learn, time you cannot regain back or won't have energy to spend in the future possibly.

Thanks to both of you!

(Feb 8, 2025 11:25 AM)Bastille Wrote: [\[CITE\]](#) Don't forget to quote or mention other members when you reply, otherwise they'll not receive notifications ?

I worked a looooooot on my Security+ cert today, so less time for Tryhackme and Letsdefend. I managed to keep my streaks tho, so it's good. I'm feeling more comfortable with the Encryption domain. I was at 90% of good answers on the quizz, the next "domain" will be about US laws, administrative stuff, and so on, that I'm not familiar with as I'm not leaving in the US. I'm not really concerned by these things but I have to so ... Besides with such certs I could be able to work in the US, who knows, maybe one day I'll give a try for a couple of years.

For those interested, I'm making my "revision sheets" (not sure about the expression) on Notion, it helps me a lot to study, here is a preview :

Current Streak :

Letsdefend.io : 40 ?

Tryhackme.com : 38 ?

Hope you keep going guys !

Bytheway please check your pm, ive send you a message.

Thank you,

M?tt - February 8, 2025, 10:49 am

Despite it not being in my current line of work. I'm taking GCIA and it's an absolute beast of a certification. I'm pretty burned out right now but I'm just about halfway done. Exam will be next

month and I'm hoping I can keep my GPA up.

Bastille - February 8, 2025, 10:54 am

(Feb 8, 2025 11:49 AM)M?tt Wrote: [\[CITE\]](#) Despite it not being in my current line of work. I'm taking GCIA and it's an absolute beast of a certification. I'm pretty burned out right now but I'm just about halfway done. Exam will be next month and I'm hoping I can keep my GPA up.

I'm glad to see you posting in this thread, if you need to talk about it, if you're looking for motivation, feel free to participate here, we try to post our daily progresses and motivate each of us ? but don't forget to rest some too to avoid the burnout !

The GIAC looks like it could be useful for me as a SOC analyst, I'm planing to pass the Security+ (this month) and the CySa+ within the next months), but this one could be on my list too. How do you prepare yourself to pass it ? How is it useful for your job / career ?

M?tt - February 8, 2025, 8:29 pm

(Feb 8, 2025 11:54 AM)Bastille Wrote: [\[CITE\]](#) I'm glad to see you posting in this thread, if you need to talk about it, if you're looking for motivation, feel free to participate here, we try to post our daily progresses and motivate each of us ? but don't forget to rest some too to avoid the burnout !

The GIAC looks like it could be useful for me as a SOC analyst, I'm planing to pass the Security+ (this month) and the CySa+ within the next months), but this one could be on my list too. How do you prepare yourself to pass it ? How is it useful for your job / career ?

GCIA is part of my Masters program. It definitely gives you a firmer understanding of network traffic, packets, and how to use tools to detect activity. It's very in depth and despite enjoying all the information, it's just a lot all at once. I'll manage, but it's hard.

Bastille - February 9, 2025, 11:35 am

Compeleted 3 days on the Advent of cyber, compeleted 1 SOC analysis case

Current streak :
Letsdefend.io : 42 ?
Tryhackme.com : 40 ?

Bastille - February 10, 2025, 6:38 am

Bumping to not merge my posts

Completed 3 days on the Advent of Cyber on tryhackme.com, I've completed the room at 67%, there are more Advent of Cyber I'm going to complete after I finish this one. The 2024 Advent of Cyber is mainly focused on blue team roles, I think I'm gonna enjoy this one

Completed 1 SOC analysis case on letsdefend.io, I'm a little bit tired, don't want to push myself, I'll rest for the end of the day.

Hope you guys keep going !

Current Streak :
Letsdefend.io : 43 ?
Tryhackme.cm : 41 ?

M?tt - February 11, 2025, 3:48 am

Another day reading for GCIA. Just finished Book 3. Hoping to finish Book 4 before the end of the week.

Bastille - February 11, 2025, 3:52 am

(Feb 11, 2025 04:48 AM)M?tt Wrote: [\[CITE\]](#) Another day reading for GCIA. Just finished Book 3. Hoping to finish Book 4 before the end of the week.

What books are you talking about, did you buy them on Amazon or are they free materials you can download ?

Do you take notes or are you just reading ? I've learned that just reading will allow you to retain only 10% of what you read, taking notes or practicing at the same time can increase the retention rate

M?tt - February 11, 2025, 10:27 am

(Feb 11, 2025 04:52 AM)Bastille Wrote: [\[CITE\]](#) What books are you talking about, did you buy them on Amazon or are they free materials you can download ?

Do you take notes or are you just reading ? I've learned that just reading will allow you to retain only 10% of what you read, taking notes or practicing at the same time can increase the retention rate

SANS courses come with reading material; which are the books. Some of the labs are also within a workbook and required you to read the questions and perform the exercises in a VM you're given. This course has 6 books of reading and 1 workbook.

padrino - February 11, 2025, 4:17 pm

Been a while since my last check-in - but recently I've been looking at Hack the Box as well as TryHackMe. I've started with the Brutus Sherlock to ease my self in - pretty interesting.

M?tt - February 12, 2025, 6:40 am

This course has taught me that I know absolutely fuck-all for packet information. Bytes, bits, headers, offsets, etc. I literally feel dumb lmao.

Bastille - February 12, 2025, 6:55 am

(Feb 11, 2025 05:17 PM)padrino Wrote: [\[CITE\]](#) Been a while since my last check-in - but recently I've been looking at Hack the Box as well as TryHackMe. I've started with the Brutus Sherlock to ease my self in - pretty interesting.

Seems a very interesting room based on grep and log researches ! I've heard many times about HTB, I plan to complete most of the free content on THM before moving to HTB, feel free to share your thoughts between those 2 platforms after a week or two of experience :)

(Feb 12, 2025 07:40 AM)M?tt Wrote: [\[CITE\]](#) This course has taught me that I know absolutely fuck-all for packet information. Bytes, bits, headers, offsets, etc. I literally feel dumb lmao.

Haha I know what you mean, for few weeks I've been into wireshark and it was like a new universe, you can dive so deep into this field it's crazy how many things you need to know and how these things work together, I wish you good luck for it, did you schedule a date for the exam or not yet ?

M?tt - February 12, 2025, 7:33 am

(Feb 12, 2025 07:55 AM)Bastille Wrote: [\[CITE\]](#) Haha I know what you mean, for few weeks I've been into wireshark and it was like a new universe, you can dive so deep into this field it's crazy how many things you need to know and how these things work together, I wish you good luck for it, did you schedule a date for the exam or not yet ?

Looking to take it in March. Not sure the date yet, but it'll probably be towards the end.

Bastille - February 12, 2025, 11:23 am

(Feb 12, 2025 08:33 AM)M?tt Wrote: [\[CITE\]](#) Looking to take it in March. Not sure the date yet, but it'll probably be towards the end.

Wish you good luck buddy :)

Completed 3 days of the advent of cyber on tryhackme.com, almost done. I went with one day about RE it was interesting but I was kinda lost, it was about a tool named "radare2", very very interesting but I need to devote more time to it.

Completed 1 SOC analysis case on letsdefend.io

Current streak :
Letsdefend.io : 44 ?
Tryhackme.com : 42 ?

SIM-5594896 - February 13, 2025, 3:10 am

Hi everyone!

I just found this topic and it gives me strength to study more :)

I'll try and post some of my achievements.

Currently I am working on TryHackMe basic rooms, trying to achieve getting into top 5% worldwide !

Let's dig more and sharpen our skillzz !

Cheers!

Bastille - February 13, 2025, 3:16 am

(Feb 13, 2025 04:10 AM)SIM-5594896 Wrote: [\[CITE\]](#) Hi everyone!

I just found this topic and it gives me strength to study more :)

I'll try and post some of my achievements.

Currently I am working on TryHackMe basic rooms, trying to achieve getting into top 5% worldwide !

Let's dig more and sharpen our skillzz !

Cheers!

Welcome to the thread buddy ! Top 5% would be a great achievement wish you good luck ! And Tryhackme is definitely my favorite platform to learn, are you using the free or paid version ?

I hope to see you participating until the end of the year :)

SIM-5594896 - February 13, 2025, 3:32 am

Hi man!

Thanks for the popularity points, those were my first ones hehe.

I really like THM as well and feel like there is a looong way to go with it. Would love to get an account on Let's defend as well but it's kinda pricy so i'll hone my skill on THM first and get to it later on. So yes I am using the paid version and just send you a request :)

?Hi all? !

So to give a bit of context I am ranked 104700th on THM, which is top 8% and my goal middle-term (2-3 months) is to get into top 5%.

As of now, I'm enrolled into the path called cybersecurity 101 which has a lot of rooms and is not that basic actually lol.

Did not go far yesterday but still completed a room on THM (Moniker Link and Outlook CVE ?). Pretty scary btw!

I'm getting at it for today at the moment, working on the Metasploit rooms.

Let everybody know what you are working on and what goals you did set for yourself, it helps me stay focus :)

Also i'll do as Bastille and hold a streak count so then it is a bit more visual.

Cheers for those who'll get some work done today !

THM streak: 2? (gotta start somewhere lol)

SIM-5594896 - February 14, 2025, 8:58 am

Ok i'm done for the day !

So I did not manage to achieve much???

I'm still fighting with Metasploit rooms and that's a hell of a ride... Anyone that completed them experienced the same troubles?

(Metasploit:Exploitation room)

Anyway I managed to get 1000 ranks up so that's not too bad?

Have a good evening peeps!

THM streak: 2 ?

Bastille - February 14, 2025, 9:17 am

(Feb 14, 2025 09:58 AM)SIM-5594896 Wrote: [\[CITE\]](#) Ok i'm done for the day !

So I did not manage to achieve much???

I'm still fighting with Metasploit rooms and that's a hell of a ride... Anyone that completed them experienced the same troubles?

(Metasploit:Exploitation room)

Anyway I managed to get 1000 ranks up so that's not too bad?

Have a good evening peeps!

THM streak: 2 ?

I completed it at 29 back in the days when I was premium ... but don't have access to it anymore

What issue do you encounter ?

Didn't do a lot today, I was out yesterday at night, I drunk a little bit too much .. did enough to keep my streak on THM and Letsdenfend, will do more tomorrow :)

Enjoy the week-end guys !

Overdose - February 14, 2025, 1:18 pm

(Jan 24, 2025 03:38 AM)Bastille Wrote: [\[CITE\]](#) Nice to see you joined us ? can't wait to see us looking back at this thread at the end of the year saying : Damn, we did a lot this year ! Haha

Having prior experience in red team will definitely help for blue team jobs, that's what I also like in IT, you can "easily" pivot from a position to another if you want to change your career. Do you have like "dead lines" or an "objective" on when you want to start as SOC analyst ?

I agree to start from the ground it's important to start from a solid basis, and sometimes it helps to refresh memory haha

Glad to see you joining us ! ? Can I ask you what's the new job ? How do you plan to get back on

the security side of things, with tryhackme, hackthebox, certifications ?

I have my cyber security certification currently, security+ to be specific, I would like to start utilizing training such as tryhackme and hack the box, my new job is physical access control, bad readers motion sensors mag locks etc

Bastille - February 15, 2025, 11:00 am

Big day ! Finished the Advent of Cyber : <https://tryhackme.com/room/learnCyberin25days>

Went through a series of questions for the Security+ exam, went well. Still planing to pass the exam by the end of february.

Completed 1 SOC analysis case on Letsdefend, I feel kinda limited now because I must upgrade to access more content and do more SOC analysis cases, not sure if it's worth it, I'm also planing to build a dedicated computer for my SOC-based homelab, I'll have a lot of things to do on it. I will maybe break my streak on Letsdefend until I really need to upgrade to access more content.

Bragging : I'm now among the first 10 000 THM members ? : Rank 9857

Tyr - February 15, 2025, 11:12 am

(Feb 15, 2025 12:00 PM)Bastille Wrote: [\[CITE\]](#) Big day ! Finished the Advent of Cyber : <https://tryhackme.com/room/learnCyberin25days>

Went through a series of questions for the Security+ exam, went well. Still planing to pass the exam by the end of february.

Completed 1 SOC analysis case on Letsdefend, I feel kinda limited now because I must upgrade to access more content and do more SOC analysis cases, not sure if it's worth it, I'm also planing to build a dedicated computer for my SOC-based homelab, I'll have a lot of things to do on it. I will maybe break my streak on Letsdefend until I really need to upgrade to access more content.

Bragging : I'm now among the first 10 000 THM members ? : Rank 9857

Nice job. Gave me some inspiration to try and actually climb up. Do you know how valued their certifications are by any chance?

Bastille - February 15, 2025, 11:14 am

(Feb 15, 2025 12:12 PM)Tyr Wrote: [\[CITE\]](#) Nice job. Gave me some inspiration to try and actually climb up. Do you know how valued their certifications are by any chance?

That's the objective of this thread ! To motivate each of us to do more every day

Yoy mean Tryhackme certs ? I don't know to be honest, not sure if it worth something as you can easily cheat.

Regarding security+; I know it's well appreciated. The objective for me is to pass the Security+ (which shouldn't be a big deal), the pass the CySA+

Tyr - February 15, 2025, 11:17 am

(Feb 15, 2025 12:14 PM)Bastille Wrote: [\[CITE\]](#) That's the objective of this thread ! To motivate each of us to do more every day

Yoy mean Tryhackme certs ? I don't know to be honest, not sure if it worth something as you can easily cheat.

Regarding security+; I know it's well appreciated. The objective for me is to pass the Security+ (which shouldn't be a big deal), then pass the CySA+

You'll knock the Security+ out of the park if you passed the CySA+. Easiest IT exam I have taken although I over-studied for it. Unfortunately it doesn't go far unless you have the triad. I see a lot of employers wanting the CCNA right now and other more specific certs but I suppose it depends what spectrum of cyber you're in.

75% of it is honestly understanding SE. lol

Bastille - February 15, 2025, 11:23 am

(Feb 15, 2025 12:17 PM)Tyr Wrote: [\[CITE\]](#) You'll knock the Security+ out of the park if you passed the CySA+. Easiest IT exam I have taken although I over-studied for it. Unfortunately it doesn't go far unless you have the triad. I see a lot of employers wanting the CCNA right now and other more specific certs but I suppose it depends what spectrum of cyber you're in.

I didn't pass the CySA+ yet but it's the next step (I meant : the objective is to pass the Security+ by the end of february, THEN - after that - the CySA+). But I'm confident, I'm really comfortable with cybersecurity in general. I've worked as a helpdesk tech, then sys/network admin for years, and also handled cybersecurity tasks for a year and a half. Now I'm targetting a Tier 2 SOC analyst role, I've heard that Tier 1 can be quite boring, and that's what I'm currently doing on Letsdefend.io and that annoys me ... I'm just waiting to move from my current apartment to a new one to buy a machine to make my SOC-based homelab.

I'm conducting malware analysis on HF <https://hackforums.net/showthread.php?tid=6276795> and helping for malware removal. Investigating for Tier 2 SOC analysis shouldn't be a big deal ?

By the way, I see you have many certs (regarding your sig), would you mind sharing your current role and your wishes for the future ?

Bastille - February 18, 2025, 12:26 am

Posting for yesterday, I changed a little bit my daily studies.

I kept tryhackme, I started a very interesting room about Linux Analysis :

<https://tryhackme.com/room/linuxfilesystemanalysis>

It's gold for me as I'm planing to work as a SOC Analyst.

I try to keep my streak on Letsdefend however I'm kinda stuck with the free version .. Not sure it's worth it paying now.

I started to work on my homelab, started with the SIEM (Splunk), the objective for today is to configure my first forwarders to send logs from a Windows Server to my Splunk server. This will be the composition of the SOC homelab :

I'm also writing notes during the configuration so I can easily do it again later. The objective is to try now, and then make a final homelab on a dedicated machine. I think notion is really good for this :

At the end, during job interviews, I'll be able to access the homelab remotely through a VPN I will configure and show them what I did on my free time. They always appreciate people working on personal projects, this emphasize many qualities like : self-taught, autonomous, passionate, and so on ...

Current Streak :
Letsdefend.io : 50 ?
Tryhackme.com : 48 ?

SIM-5594896 - February 19, 2025, 12:48 am

Hi all !

I got a bit lazy those last 2 days but i'm back at it right now :)
So still finding my way out of Metasploit rooms on THM ?.

(Feb 14, 2025 10:17 AM)Bastille Wrote: [\[CITE\]](#) What issue do you encounter ?
I don't remember anymore but might just be that I needed some air before getting back to it.
Thanks for the help though, I'll let you now if i'm stuck :)

Have a great day everyone !

THM streak : 1 ?

Bastille - February 19, 2025, 1:11 am

(Feb 19, 2025 01:48 AM)SIM-5594896 Wrote: [\[CITE\]](#) Hi all !

I got a bit lazy those last 2 days but i'm back at it right now :)
So still finding my way out of Metasploit rooms on THM ?.

I don't remember anymore but might just be that I needed some air before getting back to it.
Thanks for the help though, I'll let you now if i'm stuck :)

Have a great day everyone !

THM streak : 1 ?

Glad to see you back, don't put too many pressure on you, sometimes it's ok (and even beneficial)
to chill, studying a couple of times a week is already very good !

In case you encounter other troubles feel free to take some screenshots and ask here ?

Thul3a - February 20, 2025, 12:26 am

After a long time of procrastination and after reading this thread I've gained enough motivation to
start learning once again. Gonna do a THM room once I get home. Thanks ya'll for the motivation.
Looking forward to give you updates.

Bastille - February 20, 2025, 12:49 am

(Feb 20, 2025 01:26 AM)Thul3a Wrote: [\[CITE\]](#) After a long time of procrastination and after reading
this thread I've gained enough motivation to start learning once again. Gonna do a THM room once I
get home. Thanks ya'll for the motivation. Looking forward to give you updates.

Hey buddy, welcome to the team ! Feel free to post whenever you want to share your achievements,
if you need help you can also ask, and check sometimes what other people post to discover new
tools / fields of activities, and learn from others ?

I can't wait to look back at this thread at the end of the year so we can say together : damn, it was
worth it ?

Hope to see you around ! ?

SIM-5594896 - February 20, 2025, 2:13 am

??? Hello guys!

Yesterday I've done quite a lot on THM and I got below 100.000 as well as got into the top 7% ?
Getting closer to my short term goal of top 5% ^^

I completed several rooms yesterday and I thought I would recommend one that was very nice:
"Blue".

It is a beginner friendly red team room where you get to escalate privileges starting with a simple scan on a windows system.
Well explained and very fun !

I'm back at it today, thanks for the emulation !

Cheers !

THM streak: 2 ?

OK I'm done for today!

Got to complete couple of rooms on THM about SOC fundamentals. They were pretty nice and easy compared to other I went through before.
I'm now around 95.000 ?

There is another goal I have for the end of this week:

- Make a new CV
- Clean my GitHub
- Make a linkedIn profile

If you guys have any tips on these tasks, don't be shy ?

It goes without saying I hate this kind of stuff ??? but I need it to get an internship/Job as a SOC or Sys-admin.

Getting top 5% is also an element to reach that goal. (top 3% would for sure be better)

Anyway, let's just do it !

Good luck to y'all for reaching your goals ?

THM streak: 2 ?

Hello fellows !

Here is my morning check in :)

Kinda funny how it is now a part of my routine and helps me clarify my daily goals ?.

Today i'll try to: Watch and practice my Linux SysAdmin skills (usually 2 to 3 episodes) with [this](#)

Complete at least one room on THM

Wander around on the forum discovering new stuff ?

Good luck for today !

THM streak : 3 ?

Bastille - February 22, 2025, 1:22 am

(Feb 20, 2025 03:13 AM)SIM-5594896 Wrote: [\[CITE\]](#) ??? Hello guys!

I completed several rooms yesterday and I thought I would recommend one that was very nice: "Blue".

It is a beginner friendly red team room where you get to escalate privileges starting with a simple scan on a windows system.

Well explained and very fun !

Nice to see you still active ! I really need to go back to Windows hacking, I've already complete Blue but if you find other interesting room based on Windows I would be glad to know them :)

(Feb 20, 2025 03:13 AM)SIM-5594896 Wrote: [\[CITE\]](#) Got to complete couple of rooms on THM about SOC fundamentals. They were pretty nice and easy compared to other I went through before. I'm now around 95.000 ?

There is another goal I have for the end of this week:

- Make a new CV
- Clean my GitHub
- Make a linkedIn profile

If you guys have any tips on these tasks, don't be shy ?

It goes without saying I hate this kind of stuff ??? but I need it to get an internship/Job as a SOC or Sys-admin.

Getting top 5% is also an element to reach that goal. (top 3% would for sure be better)

I worked as a sys-admin for few years and now I'm planing to work as a tier 2 SOC analyst, if you have any questions feel free to ask !

Do you already have experience in IT ? Are you a student ? Are you graduated ?

If I can give you right now few tips :

- do not overwhelm your CV, it can seems good to put a lot of things but it's often a pain in the ass for recruiters to read them
- share things that are relevant for the job you apply for (puting on the CV that you've worked as a cashier 8 years ago during the summer is not relevant, for example)
- instead of puting things like : Python ??? > inseat put what you've accomplished, concrete examples, "3 stars" (or whatever metric) can say everything and nothing :/
- share personal projects you've worked on ! They like it, that shows you're self-taught, you can keep yourself uptodate with new technolgies, you can go beyond what we ask you
- you can even add you THM / HTB profile

(Feb 20, 2025 03:13 AM)SIM-5594896 Wrote: [\[CITE\]](#) Here is my morning check in :)

Kinda funny how it is now a part of my routine and helps me clarify my daily goals ?.

Today i'll try to: Watch and pratice my Linux SysAdmin skills (usually 2 to 3 episodes) with [this](#)

Complete at least one room on THM

Wander around on the forum discovering new stuff ?

Good luck for today !

THM streak : 3 ?

I'm really glad that this thread is helping ! :)

If you want to learn more about Linux there is something really really good for that (can seem impressive too at the same time) it's called LFS (Linux From Scratch), it's a tutorial to build your own Linux system, there is a guide available in many languages : <https://www.linuxfromscratch.org/>

Bastille - February 22, 2025, 1:25 am

[Bumping to not merge my posts]

Havn't post for a while, but I'm still active. I almost left Letsdefend because of the limitation of the free version, I'm only answering one question a day to keep my streak.

On the other hand, I've spent a lot of time on tryhackme especially about Log Analysis topic (really useful for me as I'm planing to work as a SOC analys). At the same time I'm also working on my SOC-based homelab, I've configured Splunk and I'm exploring it.

Going thorough Linux too with Linux From Scratch

Hope everyone is good and keep going :)

Current streak :

Letsdefend.io : 54 ?

Tryhackme.com : 52 ?

SIM-5594896 - February 22, 2025, 2:27 am

?? Hi guys ??

Thanks a lot for all the tips @Bastille! I'll for sure take a look at that Linux crazy project, that seems just perfect ! Also your advises on CV making sound accurate indeed.

To give more details about my current situation:

It's been a year now that I am enrolled in full time IT trainings, working also on my free time, but had no experience before.

I was always really fascinated by hacking culture but never really got the opportunity to delve into it until then. There fore I have no work experience in this field.

My first training was a Dev one (7 months). It went crazy fast, bootcamp like, and I did not manage to learn much but just got used to some basics and gained a basic understanding of how websites and servers work as well as some knowledge in JS and especially Python.

After working my ass off during last summer I managed to get into a cybersecurity training (lasting 7 months as well) that I am still pursuing (3 month remaining).

During this training I really learnt a looooot of things and got quite relaxed with many basics and got to the point where I am 100% autonomous to learn new things. It really felt like the first training gave me a sort of base onto which I can now built some more elaborate knowledge structure.

I managed to get a one month internship last summer were I was tasked to built a Debian server from an OVH VPS.

This Cyber training is supposed to train me to get the level to pretend to a soc 1 position but since I don't have any degree and those two trainings are not really well known (it's not university or a proper school), I'm considering a help-desk position for one year or two (also given the shitty economic context coming).

I feel that being that new in this field make me a bit nervous about my skills, so getting an entry level job could ease that.

My personal goal would be to work get a SOC or a SysAdmin position (which are appear kind of related in my eyes since becoming a SOC without having good understanding of OS's and computer internals means nothing).

Beside that I am working to get the MS SC-900 cert (short term) and later on Comptia-sec+ or CCNA.

Other than that, I completed two THM rooms yesterday (Firewalls, IDS and log analysis) and got to rank 90.500 ?, and worked on my linux sysadmin program (It covered linux file system).

I'll get back to it today somewhere in the afternoon but (and for once it is not Bastille ?), I had a fun night yesterday and changed my body composition in favor of beer. ??
So let's see huhu

Have a great day peeps and keep it up !

THM streak: 4 ?

Chorozon - February 22, 2025, 1:35 pm

i just stumbled upon this and what a good idea ! i will make sure to check in with some things i am learning about web based exploits

Bastille - February 23, 2025, 12:45 am

(Feb 22, 2025 02:35 PM)Chorozon Wrote: [\[CITE\]](#) i just stumbled upon this and what a good idea ! i will make sure to check in with some things i am learning about web based exploits

Glad that you're joining us ;) what platforms are you using, THM ? HTB ? It seems that you're already familiar with hacking, right ?

(Feb 22, 2025 03:27 AM)SIM-5594896 Wrote: [\[CITE\]](#) ?? Hi guys ??

Thanks a lot for all the tips @Bastille! I'll for sure take a look at that Linux crazy project, that seems just perfect ! Also your advises on CV making sound accurate indeed.

To give more details about my current situation:

It's been a year now that I am enrolled in full time IT trainings, working also on my free time, but had no experience before.

I was always really fascinated by hacking culture but never really got the opportunity to delve into it until then. There fore I have no work experience in this field.

My first training was a Dev one (7 months). It went crazy fast, bootcamp like, and I did not manage to learn much but just got used to some basics and gained a basic understanding of how websites and servers work as well as some knowledge in JS and especially Python.

After working my ass off during last summer I managed to get into a cybersecurity training (lasting 7 months as well) that I am still pursuing (3 month remaining).

During this training I really learnt a looooot of things and got quite relaxed with many basics and got to the point where I am 100% autonomous to learn new things. It really felt like the first training gave me a sort of base onto which I can now built some more elaborate knowledge structure.

I managed to get a one month internship last summer were I was tasked to built a Debian server from an OVH VPS.

This Cyber training is supposed to train me to get the level to pretend to a soc 1 position but since I don't have any degree and those two trainings are not really well known (it's not university or a

proper school), I'm considering a help-desk position for one year or two (also given the shitty economic context coming).

I feel that being that new in this field make me a bit nervous about my skills, so getting an entry level job could ease that.

My personal goal would be to work get a SOC or a SysAdmin position (which are appear kind of related in my eyes since becoming a SOC without having good understanding of OS's and computer internals means nothing).

Beside that I am working to get the MS SC-900 cert (short term) and later on Comptia-sec+ or CCNA.

Other than that, I completed two THM rooms yesterday (Firewalls, IDS and log analysis) and got to rank 90.500 ?, and worked on my linux sysadmin program (It covered linux file system).

I'll get back to it today somewhere in the afternoon but (and for once it is not Bastille ?), I had a fun night yesterday and changed my body composition in favor of beer. ??
So let's see huhu

Have a great day peeps and keep it up !

THM streak: 4 ?

Your Dev bootcamp will definitely help with security, especially for web servers; Python is also highly valued, by the way!

Being autonomous is one of the most important skills recruiters are looking for.

Unfortunately, these training courses aren't highly regarded by recruiters. I don't know the specifics of the training or its content, but most of the time they only cover the basics. The typical path to work in cybersecurity usually involves:

- at least 1 or 2 years of IT studies (computers, servers, networking, protocols, etc.)
- at least 1 year of cybersecurity (although 1 year is the minimum)

You'll have to compete with people who have degrees, but in this field you can stand out with your personal projects (like TryHackMe training, building a SOC-based lab, and so on). I remember when I used to receive applicants for job interviews—many had just graduated and showed just a little interest in IT. They weren't able to go beyond what they were taught in school, and to be honest, I preferred hiring someone with little or no degree but with more passion for IT/cybersecurity; someone who worked on personal projects and improved their skills on their own.

I'm not saying this to discourage you—just to let you know how recruiters typically view these trainings. Now that you know what they think, you'll be able to do what's necessary to show them what they want to see ;)

SOC and Sysadmin are two different jobs, getting an IT job before a cybersecurity job could be helpful, though. Starting right with SOC could be rough but it's doable.

MS SC-900 is useful for Sysadmins (especially if your company uses Microsoft products, such as Entra ID).

CCNA is beneficial for Network/Sysadmin roles.

Security+ is the best starting point for people who want to dive into blue team jobs!

Haha, I vouch for the beers ! ?

Have a great day too, buddy ! ?

JoseMar - February 23, 2025, 1:41 am

(Feb 23, 2025 01:45 AM) Bastille Wrote: [\[CITE\]](#) You'll have to compete with people who have degrees, but in this field you can stand out with your personal projects (like TryHackMe training, building a SOC-based lab, and so on). I remember when I used to receive applicants for job interviews—many had just graduated and showed just a little interest in IT. They weren't able to go beyond what they were taught in school, and to be honest, I preferred hiring someone with little or no degree but with more passion for IT/cybersecurity; someone who worked on personal projects and improved their skills on their own.

Great insights! Passion and hands-on experience truly make a difference in cybersecurity.

A few hours ago, I wrote a blog about careers in cybersecurity (waiting for approval), and I completely agree, practice is key, not just certifications.

Don't get me wrong, certifications are valuable, but if someone without certifications outperforms you in real-world skills, your certificates won't matter. You might get the job, but only for a short trial period, skills always win in the long run!

BTW, I love this thread mate and your work you do!???

Chorozon - February 23, 2025, 2:18 am

(Feb 23, 2025 01:45 AM) Bastille Wrote: [\[CITE\]](#) Glad that you're joining us ;) what platforms are you using, THM ? HTB ? It seems that you're already familiar with hacking, right ?

Your Dev bootcamp will definitely help with security, especially for web servers; Python is also highly valued, by the way!

Being autonomous is one of the most important skills recruiters are looking for.

Unfortunately, these training courses aren't highly regarded by recruiters. I don't know the specifics of the training or its content, but most of the time they only cover the basics. The typical path to work in cybersecurity usually involves:

- at least 1 or 2 years of IT studies (computers, servers, networking, protocols, etc.)
- at least 1 year of cybersecurity (although 1 year is the minimum)

You'll have to compete with people who have degrees, but in this field you can stand out with your personal projects (like TryHackMe training, building a SOC-based lab, and so on). I remember when I used to receive applicants for job interviews—many had just graduated and showed just a little interest in IT. They weren't able to go beyond what they were taught in school, and to be honest, I preferred hiring someone with little or no degree but with more passion for IT/cybersecurity; someone who worked on personal projects and improved their skills on their own.

I'm not saying this to discourage you—just to let you know how recruiters typically view these trainings. Now that you know what they think, you'll be able to do what's necessary to show them what they want to see ;)

SOC and Sysadmin are two different jobs, getting an IT job before a cybersecurity job could be helpful, though. Starting right with SOC could be rough but it's doable.

MS SC-900 is useful for Sysadmins (especially if your company uses Microsoft products, such as Entra ID).

CCNA is beneficial for Network/Sysadmin roles.

Security+ is the best starting point for people who want to dive into blue team jobs!

Haha, I vouch for the beers ! ?

Have a great day too, buddy ! ?

Quote:Glad that you're joining us ;) what plaforms are you using, THM ? HTB ? It seems that you're already familiar with hacking, right ?

I have used THM a long time ago and HTB considerably , i preferred HTB

preparing for a Security+ going to try and get a bunch of certs done this year , not sure i want to work on that side of the fence but it will be rewarding getting the certs

SIM-5594896 - February 23, 2025, 5:14 am

??? Hi all ! ???

Well it is sunday and pretty sunny outside so won't be exercising much today but few push-ups will do ?

I've just started the Capa room on THM and will finish it before getting vitamin D outside ? (important as well!).

Enjoy the day guys !

THM streak: 5 ?

THM rank: 89120

dannyswindle - February 23, 2025, 10:46 am

Monday 3am. Time to get it going!!

SIM-5594896 - February 23, 2025, 12:40 pm

???Yo !???

Today I finished the CAPA room on THM as intended. It was a bit too detailed in my opinion but still quite interesting to get an idea of how automated malware analysis works. Afterwards I went for the REMnux intro room (malicious document analysis, inetsim and volatility) and cleared another episode (on file types) of my linux SysAdmin serie on YT.

I gave a very quick look at the "Linux from scratch" project that @Bastille advocated for, but it seems gigantic and way above my current skills?.

But of course the gains are proportional to the challenge so let's see.

Maybe I'll just get carried away some day and start this foolish quest haha ???

Does a fly get wisdom from banging on the lightbulb ?

Seems very interesting thought.

That's all for today for me, but good luck to the night birds ?

THM streak: 5?

THM rank: 85600

(Feb 23, 2025 11:46 AM)dannyswindle Wrote: [\[CITE\]](#) Monday 3am. Time to get it going!!

Hahaha ? have a good ride man !

Bastille - February 24, 2025, 2:02 am

(Feb 23, 2025 02:41 AM)JoseMar Wrote: [\[CITE\]](#) Great insights! Passion and hands-on experience truly make a difference in cybersecurity.

A few hours ago, I wrote a blog about careers in cybersecurity (waiting for approval), and I completely agree, practice is key, not just certifications.

Don't get me wrong, certifications are valuable, but if someone without certifications outperforms you in real-world skills, your certificates won't matter. You might get the job, but only for a short trial period, skills always win in the long run!

BTW, I love this thread mate and your work you do!???

Thanks for the feedback and the blog buddy ! Feel free to join us and share your daily progresses in this field if you want ?

(Feb 23, 2025 03:18 AM)Chorozon Wrote: [\[CITE\]](#) preparing for a Security+ going to try and get a bunch of certs done this year , not sure i want to work on that side of the fence but it will be rewarding getting the certs

Good luck for the cert, do you know <https://www.examcompass.com/> and <https://www.examttopics.com/> ? There are free questions if you want to get an idea of your level and if you're prepared

(Feb 23, 2025 11:46 AM)dannyswindle Wrote: [\[CITE\]](#) Monday 3am. Time to get it going!!
Welcome on board mate ! Feel free to share your daily progresses ;)

(Feb 23, 2025 01:40 PM)SIM-5594896 Wrote: [\[CITE\]](#) ???Yo !???

Today I finished the CAPA room on THM as intended. It was a bit too detailed in my opinion but still quite interesting to get an idea of how automated malware analysis works. Afterwards I went for the REMnux intro room (malicious document analysis, inetsim and volatility) and cleared another episode (on file types) of my linux SysAdmin serie on YT.

I gave a very quick look at the "Linux from scratch" project that @Bastille advocated for, but it seems gigantic and way above my current skills?.

But of course the gains are proportional to the challenge so let's see.

Maybe I'll just get carried away some day and start this foolish quest haha ???

Does a fly get wisdom from banging on the lightbulb ?

Seems very interesting thought.

That's all for today for me, but good luck to the night birds ?

THM streak: 5?

THM rank: 85600

Hahaha ? have a good ride man !

Arf, CAPA is a Premium room haha, I'll save it for later, still focused on free rooms before upgrading, but when we speak about Malware Analysis I have goosebumps ?

Regarding Linux if you want to feel more comfortable without dedicating too much time to learn, I highly recommend you to use Linux as your daily OS. Personally, I'm in a dual boot configuration, so when I want to play video games I switch to Windows, otherwise I'm using Linux all day long and it helped me a lot to get more comfortable with, you could start with this :)

Bastille - February 24, 2025, 2:16 am

Yesterday I worked on a malware analysis for few hours, it dove into fields and tools I didn't know such as DIE (Detect It Easy!), dnSpy, analyzing .NET malware, it took me a lot of time, I hope I'll be able to finish it today (it's about a new member sharing a "hacking tool" for free).

I answered few questions on tryhackme and letsdefend to keep my streak.

Going to spend more time on these platforms today, especially tryhackme

Keep going guys :)

Dystortion - February 24, 2025, 4:30 am

(Feb 24, 2025 03:16 AM)Bastille Wrote: [\[CITE\]](#) Yesterday I worked on a malware analysis for few hours, it dove into fields and tools I didn't know such as DIE (Detect It Easy!), dnSpy, analyzing .NET malware, it took me a lot of time, I hope I'll be able to finish it today (it's about a new member sharing a "hacking tool" for free).

I answered few questions on tryhackme and letsdefend to keep my streak.

Going to spend more time on these platforms today, especially tryhackme

Keep going guys :)

Thanks for making this thread, just spent a ton of time reading through everthing - Will definitely contribute when I get a minute. You killing it brother for real

Bastille - February 24, 2025, 11:44 am

(Feb 24, 2025 05:30 AM)Dystortion Wrote: [\[CITE\]](#) Thanks for making this thread, just spent a ton of time reading through everthing - Will definitely contribute when I get a minute. You killing it brother for real

Hey man, thanks for the kind words ! With this thread, I really wanted to put things back into perspective and drive the activity that is at the heart of HF—and what we're here for : hacking ?

SIM-5594896 - February 25, 2025, 12:18 pm

??? Hi all ! ???

I did not post since 2 days but I've been very busy ?

I completed 4 easy CTFs on THM:

---> OHSINT, Pickle Rick, Simple CTF and Basic Pentesting (which was quite hard for me haha)

Those were the firt CTF's I completed on THM and it was quite a lot to go through !

I recommend them, it was a lot of fun and hair scratching.

Lastly I also studied a bit more ways to safely delete data (wipe a whole volume, only a file/dir or clean only free space). It is a topic I am very interested in and I found this article that gave me some new insights about it. Especially that it is no longer the case that you should go for multiple passes of zeroes or random bits.

[Here :\)](#)

I have started today another THM CTF about hash cracking, using hashcat is kinda new for me but let's see how it goes ?

Good luck to you guys and keep it up ! ??

PS: my short term goal of reaching top 5% on THM is reached ?
So I'm going for 1% now ? let's goooooo !

THM streak: 7 ?
THM rank: 73.800

Thul3a - February 26, 2025, 2:36 am

After a few days I'm here once again. Did procrastinate a lot unfortunately but managed to do some rooms on THM about a tool called Wazuh (which I wish to implement on my home network) and a room on LetsDefend about creating your own VM for malware analysis, which was kinda meh. It didn't need a whole room in my opinion. Als

Also I'm setting myself a goal of getting to 5% in THM (I hope it's realistic lmao).

Anyway wish everyone a good and productive day. See you tomorrow!

SIM-5594896 - February 26, 2025, 5:19 am

(Feb 26, 2025 03:36 AM)Thul3a Wrote: [\[CITE\]](#) After a few days I'm here once again. Did procrastinate a lot unfortunately but managed to do some rooms on THM about a tool called Wazuh (which I wish to implement on my home network) and a room on LetsDefend about creating your own VM for malware analysis, which was kinda meh. It didn't need a whole room in my opinion. Als

Also I'm setting myself a goal of getting to 5% in THM (I hope it's realistic lmao).

Anyway wish everyone a good and productive day. See you tomorrow!
? Hi Thul3a !

Glad to see we are working on similar goals :)
Just a quick reply to tell you 5% is very realistic.
Of course I don't know you but I now I reached it almost only going through easy-walkthrough type rooms which anyone can do with a bit of dedication and consistency. So if you want it, just go for it ?

Have a good day too !

Galaxe - February 26, 2025, 9:29 am

(Feb 26, 2025 06:19 AM)SIM-5594896 Wrote: [\[CITE\]](#) ? Hi Thul3a !

Glad to see we are working on similar goals :)
Just a quick reply to tell you 5% is very realistic.
Of course I don't know you but I now I reached it almost only going through easy-walkthrough type rooms which anyone can do with a bit of dedication and consistency. So if you want it, just go for it ?

Have a good day too !
ooo, i love people motivating each other in learning...really gives me motivation, even just hearing about somebody who was struggling with procrastination and then did some great progress...we all struggle with something in our learning paths, so seeing other peoples experiences really makes me feel better

have a good one too man...

Bastille - February 26, 2025, 9:43 am

(Feb 26, 2025 03:36 AM)Thul3a Wrote: [\[CITE\]](#) After a few days I'm here once again. Did procrastinate a lot unfortunately but managed to do some rooms on THM about a tool called Wazuh (which I wish to implement on my home network) and a room on LetsDefend about creating your own VM for malware analysis, which was kinda meh. It didn't need a whole room in my opinion. Als

Also I'm setting myself a goal of getting to 5% in THM (I hope it's realistic lmao).

Anyway wish everyone a good and productive day. See you tomorrow!

Glad to see you back man ! Wazuh is an amazing tool, I'm planing to play with it soon and implements it in my SOC-based homelab.

Yeah 5% is definitely realistic ! It will be so cool to see you and [SIM-5594896](#) reaching the top 5% as it's his goal too. It's 100% doable ?

(Feb 26, 2025 10:29 AM)Galaxe Wrote: [\[CITE\]](#) ooo, i love people motivating each other in learning...really gives me motivation, even just hearing about somebody who was struggling with procrastination and then did some great progress...we all struggle with something in our learning paths, so seeing other peoples experiences really makes me feel better

have a good one too man...

Glad to see you in this thread, feel free to share your progresses whenever you want, even small achievements are important, constancy is key, don't forget ! ?

By the way, feel free to make an Introduction thread to tell us more about you, why do you want to study hacking, if you're targeting a specific job in cybersecurity maybe ? If you're already familiar with hacking, linux, programming; and so on. You can post it here : [The Lounge](#)

SIM-5594896 - February 26, 2025, 11:59 am

??? Hi guys ???

I hope your day has been either chill or productive ! Mine was cool, I finished a THM CTF on hash cracking and started a new one called "Root Me" But I had to stop after uploading a php reverse shell because escalating privileges was too much for me at the moment. I need to study more.

I watched another Linux SysAdmin videos of my playlist about crontab, and that's about it.

(Feb 26, 2025 10:29 AM)Galaxe Wrote: [\[CITE\]](#) ooo, i love people motivating each other in learning...really gives me motivation, even just hearing about somebody who was struggling with procrastination and then did some great progress...we all struggle with something in our learning paths, so seeing other peoples experiences really makes me feel better

Glad to see we are like minded about that ?

At the moment I am enjoying a good and consistent energy to study but it is obviously not always that way haha. As I said before this thead helps a lot and I am very glad I discovered it ! Thanks again @Bastille :)

Cheers @Galaxe

THM streak: 8 ?

THM rank: 70.100

??? Hi everyone ???

Today was a bit slow but I managed to complete 2 rooms on THM: Linux forensics and Redteam recon.

Then I played a bit with another CTF: Lazyadmin but in the middle of it, I got stuck once again because I suck at privilege escalation ?

Sooo I used my last drop of motivation to start a new room called..... Common linux privesc lol. I've learnt the lesson ?

Also, If anyone has an idea of a way to get better at mastering linux I'm very interested.

My idea would be either a project idea or a specific ressource I could use. Bastille mentioned Linux from scratch but it is too much to carry for me at the moment.

To give you a bit of a context, I am already riding debian based distros since 2 years (currently Parrot) and more than half of my activity is going through terminal. I feel like I am getting better with time and I kinda know my way around it but it seems a little bit superficial sometimes.

Does it ring any bells ?

Have a good evening !

THM streak: 9 ?

THM rank: 67.900

Bastille - February 28, 2025, 12:05 am

(Feb 26, 2025 12:59 PM)SIM-5594896 Wrote: [CITE](#) ??? Hi everyone ???

Also, If anyone has an idea of a way to get better at mastering linux I'm very interested.

My idea would be either a project idea or a specific ressource I could use. Bastille mentioned Linux from scratch but it is too much to carry for me at the moment.

To give you a bit of a context, I am already riding debian based distros since 2 years (currently Parrot) and more than half of my activity is going through terminal. I feel like I am getting better with time and I kinda know my way around it but it seems a little bit superficial sometimes.

Does it ring any bells ?

Have a good evening !

THM streak: 9 ?

THM rank: 67.900

Is Parrot your daily distro ? If not, you should switch to a Linux based daily distro. For example, I'm using Fedora as my daily OS, and I have also Windows installed on a second disk when I want to play video games, but 90% of my time I'm using Fedora.

Secondly, if you didn't yet, I recommend you to make a homelab and setup some Linux servers. Installing the required packages, tweaking the settings, fixing issues, will help you to improve your understanding of Linux.

Few interesting YouTube channels (french) :

- <https://www.youtube.com/@AdrienLinuxtricks> > one of my favorite, sometimes you just watch the video with a beverage and you learn things, you get more familiar with Linux, he knows a lot and he's well appreciated in French Linux users community

- <https://www.youtube.com/@topklean/streams> > topklean is a good reference too, he goes deeper in Linux, more technical topics

- <https://www.youtube.com/@yrougy> > this guy is very good too, he posts videos and make streams

on twitch (every sunday nights I think?). By the way he made a tutorial in French for Linux From Scratch, if one day you decide to go back into it

If Linux From Scratch sounds too much for you, you should take a look at Linux Essentials or LPIC documentations, there are some available in French, for example :

- <https://learning.lpi.org/pdfstore/LPI-Learning-Material-010-160-fr.pdf>

- or in English : <https://learning.lpi.org/pdfstore/LPI-Learning-Material-010-160-en.pdf>

These PDF are free, if it's too easy for you then you should take a look at LPIC-1 and then LPIC-2. But not sure that the books are available in french tho

Finally, the best way to learn how to use Linux is to put your hands inside, sometimes I just browse some folders, then switch to ChatGPT and ask to it what's the purpose of a folder / binary. Sometimes I also browse the bin/sbin folders and use the man page to understand what a tool does. Then I use Notion.so to put everything I learn so I can go back to it, for example :

- What is a bootloader, what are the different bootloaders, what's a shell, what are the different shells, what is the kernel, a desktop environment, a window manager, what are the differences between sysvinit and systemd, why there are so many Linux distros, etc ...

Linux is a wide topic, but before diving into it I think it's important to understand what it is and where it comes from, for this I recommend you to check the following video (still in french) :

<https://www.youtube.com/watch?v=baxmRgeX7-E>

Let me know what you think about the tips above and if it helped ?

SIM-5594896 - February 28, 2025, 3:37 am

??? Hi ! ???

Thanks a lot for the tips I'll look them up.

(Feb 28, 2025 01:05 AM) Bastille Wrote: [\[CITE\]](#) Is Parrot your daily distro ?

Yes Parrot is my daily distro, I don't even have a windows anymore since one year so i'm full on ? I did setup a debian server some time ago but I could not explain it anymore so maybe that's a good project to start with in the near future !

I also thought about an Arch project but i'm not sure if it's worth it. May be better to go straight at the meat and embrace LFS.

Thanks again and have a good and productive day ?

Bastille - March 2, 2025, 3:59 am

It's been few days since I posted last time, I missed one day, not lost my streaks because I had a freeze streaks on both THM and Letsdefend, but I'm kinda disappointed.

Anyway, I rested for 2 days almost, full of energy, ready to go back into those things !

Hope you're doing well guys, don't forget to enjoy the week-end too before going back into studies !

Just completed a room on THM : <https://tryhackme.com/room/linuxprocessanalysis>

I really liked diving into Linux system analysis, it's definitely vital for working as a tier 2 SOC analyst.

SIM-5594896 - March 3, 2025, 2:34 am

??? Hello hello ! ???

Well I did not do much those last 2 day either, but the weather was nice so I enjoyed it :)

I completed some rooms on THM but they were basic ones, not worthy of being mentioned here. Sometimes it's good to get back to the very basics, especially on lazy dayzzz ?

Apart from that, a friend of mine wanted to switch to Linux so I installed the latest LTS Ubuntu and got him a little setup.

Besides apps he requested, I focused on security. For that I followed some of the points mentioned in ?Lowkey's thread "Staying Safe & Anonymous on Ubuntu".

Great ressource !

As it is for a complete newb that is not interested in digging into computer stuffs, I kept it basic:

- > Encrypted partition
- > UFW enabled with standard rules
- > Automatic security related updates
- > Apparmor enabled (might be troublesome at some point ?)
- > Cloudflare and Quad9 custom DNS
- > Disable webRTC
- > TOR, BleachBit and ClamAV install (I'm still unsure if I should use cronjob for clamscans or if it's overkill ?)

That was fun and I learnt new stuffs along the way ?

Let's jump into monday the 3rd !

Have a good day all :)

THM streak: 13 ?

THM rank: 66900

Thul3a - March 3, 2025, 6:57 am

Hello once again after a few days.

Didn't really do much unfortunately, at least some basic rooms in THM and LetsDefend to keep my streaks. I finished the Wazuh room I talked about in my earlier post. In LetsDefend I began doing the Splunk room, both of these are really interesting to me and I hope I'll work with them in the future.

Stay strong!

Galaxe - March 3, 2025, 3:21 pm

(Feb 26, 2025 10:43 AM)Bastille Wrote: [\[CITE\]](#) Glad to see you back man ! Wazuh is an amazing tool, I'm planing to play with it soon and implements it in my SOC-based homelab.

Yeah 5% is definitely realistic ! It will be so cool to see you and [SIM-5594896](#) reaching the top 5% as it's his goal too. It's 100% doable ?

Glad to see you in this thread, feel free to share your progresses whenever you want, even small achievments are important, constancy is key, don't forget ! ?

By the way, feel free to make an Introduction thread to tell us more about you, why do you want to study hacking, if you're targeting a specific job in cybersecurity maybe ? If you're already familiar

with hacking, linux, programming; and so on. You can post it here : [The Lounge](#)

Wow..i did not expect HF to be this type of community..thanks a lot for encouraging me to do so. this was supposed to be a throwaway account, so i might text you on my new main one. However what i wanted to say is this really put a smile on my face..i just wasn't expecting such a welcoming attitude...not only from you Bastille. And constancy is key, ur right :)

Thul3a - March 4, 2025, 12:08 am

(Mar 3, 2025 04:21 PM)Galaxe Wrote: [\[CITE\]](#) Wow..i did not expect HF to be this type of community..thanks a lot for encouraging me to do so. this was supposed to be a throwaway account, so i might text you on my new main one. However what i wanted to say is this really put a smile on my face..i just wasn't expecting such a welcoming attitude...not only from you Bastille. And constancy is key, ur right :)

Lmao same, I had the kind of impression that it's just some toxic skid forum, but it actually turned out really nice and welcoming.

Hope to see you again.

Bastille - March 4, 2025, 12:19 am

(Mar 3, 2025 03:34 AM)SIM-5594896 Wrote: [\[CITE\]](#) ??? Hello hello ! ???

Well I did not do much those last 2 days either, but the weather was nice so I enjoyed it :)

I completed some rooms on THM but they were basic ones, not worthy of being mentioned here. Sometimes it's good to get back to the very basics, especially on lazy days ?

Apart from that, a friend of mine wanted to switch to Linux so I installed the latest LTS Ubuntu and got him a little setup.

Besides apps he requested, I focused on security. For that I followed some of the points mentioned in ?Lowkey's thread "Staying Safe & Anonymous on Ubuntu".

Great resource !

As it is for a complete newbie that is not interested in digging into computer stuffs, I kept it basic:

- > Encrypted partition
- > UFW enabled with standard rules
- > Automatic security related updates
- > Apparmor enabled (might be troublesome at some point ?)
- > Cloudflare and Quad9 custom DNS
- > Disable webRTC
- > TOR, BleachBit and ClamAV install (I'm still unsure if I should use cronjob for clamscans or if it's overkill ?)

That was fun and I learnt new stuffs along the way ?

Let's jump into Monday the 3rd !

Have a good day all :)

THM streak: 13 ?

THM rank: 66900

A good way to learn more about Linux, glad that you enjoyed helping your friend installing Ubuntu :)

(Mar 3, 2025 04:21 PM)Galaxe Wrote: [\[CITE\]](#) Wow..i did not expect HF to be this type of community..thanks a lot for encouraging me to do so. this was supposed to be a throwaway account, so i might text you on my new main one. However what i wanted to say is this really put a

smile on my face..i just wasn't expecting such a welcoming attitude...not only from you Bastille. And constancy is key, ur right :)

Glad that HF community gave you a smile and some motivation. I thought the same when I registered 6 years ago, I was just starting in IT and now I'm working in cybersecurity thanks to HF. Can't wait to see how far you'll go ?

(Mar 4, 2025 01:08 AM)Thul3a Wrote: [\[CITE\]](#) Lmao same, I had the kind of impression that it's just some toxic skid forum, but it actually turned out really nice and welcoming.

Hope to see you again.

HF has a "skid" reputation mostly because it's the first forum you stumble upon when you're looking for a "hacking forum" on Google, so a lot of beginners come. Besides, some black hat topics are not allowed to be discussed compared to other forums, but that's also why HF is still online after almost 18 years, and that's why competitive forums have been seized over time, recent example :

<https://hackforums.net/showthread.php?tid=6290868>

You'll find some toxic people but as on every website on the Internet, trolls are everywhere, but it's not a majority :)

SIM-5594896 - March 5, 2025, 7:13 am

??? Hello guys ! ???

As the sun gets back the energy level does as well, but not so much towards studying ?

But as long as I manage to complete a couple of THM questions here and there, it's at least moving towards my goals :)

Today I finished the Linux Incident Surface room which was kinda nice. Focusing very much on log analysis with little grep commands here and there. Nothing crazy but good practices to maintain a linux system healthy.

I have just started the Zeek room to deepen my knowledge in linux defence. There is also an exercise room that can be done afterwards.

I think you would very much like it @Bastille, unless it is too basic for you of course ?

Finally finished to make my CV and LinkedIn ? so I'll soon try and get an internship as a linux sysAdmin. Hopefully it won't be too much of a hassle since I have almost no XP.

Keep up the good work guys !

Even a little byte a day makes a huge difference at the end of the month ?

---> Here I am editing this post because I've been reading Bastille's initial post once more (about sharing and learning strategies) and from now on I'll try to do that as often as possible: Kind of summarize what I learnt in the rooms I did and not only post my achievements.

Disclaimer: I'll write what I have understood with my own words so it will most likely be incomplete and shaky often, even just not true sometimes. But please don't hesitate to bounce on it, would it be to trigger a discussion, correct me or add additional informations ??

So let's go !

Linux Incident Surface room

The room introduced the difference between attack and incident surface.

? Attack surface being the "area" that is potentially vulnerable, such as user inputs or open ports with running services where an attacker can inject or retrieve data.

? Incident surface being the "areas" onto which an attack or an intrusion leaves traces such as different kinds of log files and network traffic.

Then the second part of the room was dedicated to incident surfaces that I'll make a small list of for linux OSs:

- > " ps aux " to list processes of all kinds (all users+not attached to terminal+process' owner or user)
- > " lsof -p " this command (list open files) fed with a PID will list the files implicated by a given process
- > " lsof -i -P -n " same command but this time it focuses on network connections opened by processes. The -n formats them as IP addresses.
- > " osqueryi " that invokes the osquery tool. This tool is very versatile since it allows you to use SQL-like queries to get different informations on your system, such as processes, network connections, open files, file system details etc. This tool looks great but was a bit confusing to me and it took me a long time to write those last 2 line lol.
- > " /var/log/auth.log " While /var/log contains all common logs, the auth.log file combines logs related to authentication in general.
- > " /etc/passwd " can also be interesting as it contains information about users created.
- > " crontab -e " to check how the future looks like ?
- > " /var/spool/cron/crontabs/[username] " to check for a specific user.
- > " /etc/systemd/system " to check for fishy services running or enabled on your machine.
- > " /var/log/syslog | grep weirdService " to get more info about a potential bastard.
- > " /var/log/dpkg.log " to look for parasite packages.
- > " /var/log/syslog " to check for general events and alerts.

And voilà !

It was quite beneficial for me to make this edit as it will for sure strengthen my new knowledge but might not be that great for you guys haha. Anyways it's here now so be it ?

Maybe next one will be better ?

THM streak: 15 ?

THM rank: 65100

Thul3a - March 6, 2025, 3:18 am

Hello once again,

finally I managed to have a 7 day streak in THM. Today I did finished a room about Metasploit fundamentals teaching me how much powerful this tool is. Also did some questions on LetsDefend about Splunk and its alerts and reports.

I'll make sure to contact my ISP so I could finally begin to work on my homelab. My first intention is to create a basic pi-hole container and try it out. Next I'd like to add Wazuh (which I've talked about in earlier posts). We'll see where this gets me.

Don't procrastinate too much, it's not worth it. See you tomorrow!

SIM-5594896 - March 6, 2025, 4:58 am

(Mar 6, 2025 04:18 AM)Thul3a Wrote: [\[CITE\]](#) Hello once again,

finally I managed to have a 7 day streak in THM. Today I did finished a room about Metasploit fundamentals teaching me how much powerful this tool is. Also did some questions on LetsDefend about Splunk and its alerts and reports.

I'll make sure to contact my ISP so I could finally begin to work on my homelab. My first intention is to create a basic pi-hole container and try it out. Next I'd like to add Wazuh (which I've talked about in earlier posts). We'll see where this gets me.

Don't procrastinate too much, it's not worth it. See you tomorrow!
??? Hello hello ! ???

Nice to see you back ! And you've been working hard ??!
I was just wondering, why do you need to contact your ISP for your homelab/pihole project?

"Don't procrastinate too much, it's not worth it."
Yes sir !! ??

Today I worked on a THM CTF, Agent sudo. Quite a nice one but still somehow tricky for my skills. I'll finish it tomorrow afternoon.

Also went over 80 questions of the MS SC-900 that I'll try to pass in some weeks. A real pain in the ass haha.

Don't have much time to develop on my CTF experience, but I'll try to give a bit more next time.

Have a great evening guys ! And see you tomorrow ?

THM streak: 16 ?
THM rank: 62700

SickM - March 6, 2025, 2:45 pm

If anyone would like to learn by teaching, I'd definitely be grateful for the lessons

SIM-5594896 - March 6, 2025, 3:40 pm

(Mar 6, 2025 03:45 PM)SickM Wrote: [\[CITE\]](#) If anyone would like to learn by teaching, I'd definitely be grateful for the lessons

Hi SickM ! Welcome on the thread !

I'm pretty new on HF myself but I'll do my best to give you tips on learning.

First of, you got to the right spot as this very thread is indeed about learning, keeping the motivation up and sharing.

Other than that, I advise you warmly to go [there](#) and enjoy an amazing tutorial assembled by Bastille for beginners. And I don't mean beginners in a bad way since the topics discussed are sort of mapping all the subjects or knowledge areas one should explore to get better at hacking and computer sciences in general.

Then when it comes to your wish of being taught or having people explaining you stuffs, I guess it is also appropriate here.

Just ask about a specific topic/question or a project you'd like to make and you'll for sure get guidance and advises.

It would also be nice to introduce yourself a bit so then people here have an idea of your current knowledge status/personal interests so they can help you better:

- > What machine do you have ?
- > Have any experience about coding ?
- > Do you know some stuffs about networking ?
- > What do you want to learn ?
- > What would you like to achieve ?

-> ...

And if you are a pure rookie it's ok, we all started there at some point.

Have a nice day tomorrow and hopefully see you soon ?

Bastille - March 7, 2025, 1:58 am

I'm back everyoooooone ! Was off for two days, I had to fix a friend's computer, however I had to disassemble mine to test every components so didn't have my computer for two days.

I managed to keep my streaks on THM and Letsdefend tho. Even if I didn't practice a lot on these platforms I improved my computer repair skills haha. First time I had to remove thermal paste from the pins of a CPU, and to rebend CPU pins

Everything is now working on his computer, I finally rebuilt mine (was a good opportunity to replace the thermal paste and clean the dust).

I'm now also thinking about buying an ultrasonic bath to clean components (it would have been really useful to clean the thermal paste on the pins of the CPU).

Enough hardware things, now it's the time to go back to cybersecurity ?

Current streak :
Letsdefend.io : 65 ?
Tryhackme : 65 ?

Started <https://app.letsdefend.io/challenge/risen-ransomware> on Letsdefend.io, really interesting but I ran out of time as I'm using the free version.

Completed : <https://tryhackme.com/room/identificationandscoping> on tryhackme.com, I was going to complete the full <https://tryhackme.com/module/incident-response> path, but the next modules are for the premium users.

I guess it's maybe time to consider upgrading. Both are really interesting but I'm not sure if it's worth. I don't spend too much time on it, like maybe 2 hours per day, it could be interesting if I spend more time but I'm still recovering from a burnout and don't want to overwhelm myself.

Hope you keep going guys, I haven't seen few names on this thread for a long time tho ?

SIM-5614029 - March 8, 2025, 11:57 am

Hi,

So besides promising i would be more persistent in daily checking, i did the opposite, i worked a lot on my infortree and tend to finish the 8th of march, been working on it for 3-4 months now and really can say i learned a lot on the process of executing an operation.

However i am still having doubts about persistence methods. so i would like to give you all the following question.

What is a preferred persistence model used for windows:

Personally i think it would be either placing a backdoor in startup or logon, however it is quite easy to detect.

2nd choice would be to get credentials of an existing account or using a "hidden" account,

Thank you all for reading and i hope to get a response

Pr0m3th3us - March 8, 2025, 6:06 pm

I guess i will start checking in on this thread.

I just completed Networking

Something that i learned that i didn't already know. MAC addresses are separated into 2 sections and gives the ID of the company and the device both (sorta like a VIN# for a vehicle is what my mind compared it to except not as much detail)

I have to pay to continue so when demon buys my bytes i will hopefully do that with crypto!

Bastille - March 8, 2025, 11:40 pm

(Mar 8, 2025 12:57 PM)SIM-5614029 Wrote: [CITE](#) Hi,

So besides promising i would be more persistent in daily checking, i did the opposite, i worked a lot on my infortree and tend to finish the 8th of march, been working on it for 3-4 months now and really can say i learned a lot on the process of executing an operation.

However i am still having doubts about persistence methods. so i would like to give you all the following question.

What is a preferred persistence model used for windows:

Personally i think it would be either placing a backdoor in startup or logon, however it is quite easy to detect.

2nd choice would be to get credentials of an existing account or using a "hidden" account,

Thank you all for reading and i hope to get a response

Those you mentioned are the most commons, but also the easiest to detect, here is an exhaustive list, sorted from easier to harder to setup (and also detect) : Registry Run Keys: Inserting entries in keys like HKLM\Software\Microsoft\Windows\CurrentVersion\Run or HKCU\Software\Microsoft\Windows\CurrentVersion\Run.

Startup Folder: Dropping shortcuts or executables into the Windows startup folder.

Scheduled Tasks / Cron Jobs: Creating tasks that run the malware at set intervals or triggers.

Services: Installing the malware as a Windows service to launch at boot.

WMI Event Subscriptions: Using WMI event filters and consumers to re-launch the payload after system events.

DLL Hijacking / AppInit_DLLs: Placing malicious DLLs where trusted applications load them.

COM Hijacking: Modifying COM object registration to load malicious components.

Kernel Modules/Drivers: Installing drivers or kernel modules that remain active with system privileges.

Bootkits: Infecting the boot process (e.g., MBR or UEFI) to control the system from the very start.

Firmware Infections: Embedding code in BIOS or device firmware for deep persistence.

Additionally you should check the following link : <https://attack.mitre.org/tactics/TA0003/> . The MITRE matrice gather all known technics / methods used by malicious hackers, the TA0003 is about Persistance, but feel free to check the entire matrice if you want : <https://attack.mitre.org/>

(Mar 8, 2025 07:06 PM)SIM-2567248 Wrote: [\[CITE\]](#) I guess i will start checking in on this thread.

I just completed Networking

Something that i learned that i didn't already know. MAC addresses are separated into 2 sections and gives the ID of the company and the device both (sorta like a VIN# for a vehicle is what my mind compared it to except not as much detail)

I have to pay to continue so when demon buys my bytes i will hopefully do that with crypto!
Glad that you started on tryhackme ! Yeah it's the OUI (Organizational Unique Identifier), you can use links such as this one to know to what manufacturer the OUI is related :
<https://www.wireshark.org/tools/oui-lookup.html>

This is pretty useful when doing reconnaissance (like nmap) to know what kind of device you're facing to. For example, I mentioned how important it is here :
<https://hackforums.net/showthread.php?tid=6282516> , getting the MAC address and then the manufacturer is useful to then know what vulnerability you can exploit on security cameras

Bastille - March 8, 2025, 11:44 pm

[Bumping to not merge my posts]

Finally got the premium version of tryhackme, I'll mainly focus on it as I'm limited on Letsdefend.io (reached 66 streak but nevermind). As I'm paying for the premium version I'm more motivated to do more every day, besides the learning paths are really convenient. Before that I used to browse for minutes to know what I'll study every day, sometimes I stubbed on paid rooms and I had to search again ..

I completed a lot of rooms yesterday (117 questions, 182 events), mainly trying to finish the 101 Cybersecurity path, I'll then enroll to SOC level 1 and then SOC level 2.

Tryhackme streak : 67 ?
Rank : 8435 ?

Now, one of my goal, is to be on the leadder of French users, let's see how it goes !

Keep going guys :)

SIM-5614029 - March 9, 2025, 10:32 am

(Mar 9, 2025 12:40 AM)Bastille Wrote: [\[CITE\]](#) Those you mentioned are the most commons, but also the easiest to detect, here is an exhaustive list, sorted from easier to harder to setup (and also detect) : Registry Run Keys: Inserting entries in keys like HKLM\Software\Microsoft\Windows\CurrentVersion\Run or HKCU\Software\Microsoft\Windows\CurrentVersion\Run.

Startup Folder: Dropping shortcuts or executables into the Windows startup folder.
Scheduled Tasks / Cron Jobs: Creating tasks that run the malware at set intervals or triggers.
Services: Installing the malware as a Windows service to launch at boot.
WMI Event Subscriptions: Using WMI event filters and consumers to re-launch the payload after system events.
DLL Hijacking / AppInit_DLLs: Placing malicious DLLs where trusted applications load them.
COM Hijacking: Modifying COM object registration to load malicious components.
Kernel Modules/Drivers: Installing drivers or kernel modules that remain active with system privileges.
Bootkits: Infecting the boot process (e.g., MBR or UEFI) to control the system from the very start.

Firmware Infections: Embedding code in BIOS or device firmware for deep persistence.

Additionally you should check the following link : <https://attack.mitre.org/tactics/TA0003/> . The MITRE matrix gather all known technics / methods used by malicious hackers, the TA0003 is about Persistence, but feel free to check the entire matrix if you want : <https://attack.mitre.org/>

Glad that you started on tryhackme ! Yeah it's the OUI (Organizational Unique Identifier), you can use links such as this one to know to what manufacturer the OUI is related :

<https://www.wireshark.org/tools/oui-lookup.html>

This is pretty useful when doing reconnaissance (like nmap) to know what kind of device you're facing to. For example, I mentioned how important it is here :

<https://hackforums.net/showthread.php?tid=6282516> , getting the MAC address and then the manufacturer is useful to then know what vulnerability you can exploit on security cameras

Hi,

Thanks for the recommended list. i have used mitre a few times now but still struggle with the actual discovery of the used methods.

Will check on mitra again for more!

Thanks

everynight - March 10, 2025, 3:59 am

Quite troubled, I've been stuck on HTTP basic authentication lately, and I can't find any relevant information online. I'm feeling helpless.

Quite troubled, I've been stuck on HTTP basic authentication lately, and I can't find any relevant information online. I'm feeling helpless.

Bastille - March 10, 2025, 4:49 am

(Mar 10, 2025 03:59 AM)everynight Wrote: [\[CITE\]](#) Quite troubled, I've been stuck on HTTP basic authentication lately, and I can't find any relevant information online. I'm feeling helpless.

Quite troubled, I've been stuck on HTTP basic authentication lately, and I can't find any relevant information online. I'm feeling helpless.

What are you trying to do / understand exactly ? If it's not related to this thread I encourage you to make your own thread in the right section, we'll take a look at your thread.

Posting for yesterday, completed 3 rooms on THM :

<https://tryhackme.com/room/logsfundamentals>

<https://tryhackme.com/room/incidentresponsefundamentals>

<https://tryhackme.com/room/gobusterthebasics>

I finally left Letsdefend.io, will go back to it later, after I complete Learning Path SOC Level 1 and SOC Level 2 on THM

Bastille - March 11, 2025, 6:54 am

Posting for today, completed <https://tryhackme.com/room/windowspowershell>

Not sure if I'll have more time to do more today but this one already took me some time, will do more tomorrow I think !

Hope you keep going guys,

Current streak : 70 ?

Rank : 8160 ?

Thul3a - March 12, 2025, 4:53 am

Hey,

nothing much to talk about as I'm preparing for my finals. But I did bought tryhackme premium and started the beginner blue team path (whatever it's called).

So yeah, it's not much, but at least it's something.

See you next time.

SIM-5614029 - March 12, 2025, 12:25 pm

Day 69,

Thanks to bastille for always giving answers and taking the time to respond to each message,

Just made the switch to THM from HTB, Big difference, the room connecting is much smoother and more beginner friendly. also the fact that THM is not as chaotically organized as HTB is very pleasant. Going on day 3 now of the THM streak

a question:

What tools for Privilege escalation are recommended/ do you the reader use?

I am learning about winpeass and bloodhound now. but besides those 2 what are more tools?

Thats it for today, see ya later

Bastille - March 12, 2025, 1:56 pm

(Mar 12, 2025 04:53 AM)Thul3a Wrote: [\[CITE\]](#) Hey,

nothing much to talk about as I'm preparing for my finals. But I did bought tryhackme premium and started the beginner blue team path (whatever it's called).

So yeah, it's not much, but at least it's something.

See you next time.

Congrats for the premium, bought it too, more convenient to learn I think

Wish you good luck for your finals, let us know how it went !

(Mar 12, 2025 12:25 PM)SIM-5614029 Wrote: [\[CITE\]](#) Day 69,

Thanks to bastille for always giving answers and taking the time to respond to each message,

Just made the switch to THM from HTB, Big difference, the room connecting is much smoother and more beginner friendly. also the fact that THM is not as chaotically organized as HTB is very pleasant. Going on day 3 now of the THM streak

a question:

What tools for Privilege escalation are recommended/ do you the reader use?

I am learning about winpeass and bloodhound now. but besides those 2 what are more tools?

Thats it for today, see ya later

Glad that you appreciate THM, I also think it's better when you start

Regarding PrivEsc :

- LinPEAS (for Linux)
- WinPEA (for Windows)
- linux-exploit-suggester
- LinEnum : <https://github.com/rebootuser/LinEnum>

Then, I also recommend you to take a look at the LOLBas and GTF0Bins :

- <https://gtf0bins.github.io/> > Linux
- <https://lolbas-project.github.io/> > Windows

These websites are useful to know which native / built-in binaries can be exploited for many things like PrivEsc but not only limited to this.

Completed the following room : <https://tryhackme.com/room/linuxshells>

Streak : 71 ?

Rank : 8085 ?

Bastille - March 14, 2025, 5:59 am

I've completed 2 rooms on THM :

- <https://tryhackme.com/room/wiresharkthebasics>
- <https://tryhackme.com/room/cyberchefbasics>

Hope to finish the Cyber Security 101 Path soon (currently at 71%), I'm already familiar with most of the content, but it's always good to refresh our memory.

Planing to do more today but taking a break for the time being

Streak : 73 ?

Rank : 7672 ?

I've also worked on the MRT-X Academy on HF to get graduated, planing to continue to work on a VirusTotal full guide for HF, I've already started it

Hope you keep going guys !

UPDATING MY POST : completed 3 more rooms today :

- <https://tryhackme.com/room/johntheripperbasics>
- <https://tryhackme.com/room/wiresharkthebasics>
- <https://tryhackme.com/room/monikerlink>

Bastille - March 16, 2025, 2:09 am

Posting for yesterday, completed two rooms :

- <https://tryhackme.com/room/monikerlink>
- <https://tryhackme.com/room/metasploitexploitation>

Completed the Cyber Security 101 path at 77%, then I'll move to SOC Level 1, and then SOC Level 2. I've already completed many rooms related to these paths, currently at 26% for Level 1 and 11% for Level 2. The objective is to finish all of them by the end of April, then start working on my homelab in May.

Streak : 74 ?

Rank : 7662 ?

I also need to pass the Security+ exam ...

Hope you're doing good guys, I've noticed less activity on this thread, maybe you're focused on some personal projects. Keep going !

padrino - March 16, 2025, 4:54 pm

Been a long while since I've done a check-in. Work has been crazy and my personal life has been all over the place, however, I'm back in the game! myself and some buddies have joined on the HTB event "Cyber Apocalypse". Could be quite fun for a few of the members here? get some teams on the go! <https://www.hackthebox.com/events/cyber-apocalypse-2025>

Anyway, hoping to get back into training seriously again after a little break so wish me luck!

Hope everyone has had a productive and hack-y day!

Bastille - March 16, 2025, 5:04 pm

(Mar 16, 2025 04:54 PM)padrino Wrote: [\[CITE\]](#) Been a long while since I've done a check-in. Work has been crazy and my personal life has been all over the place, however, I'm back in the game! myself and some buddies have joined on the HTB event "Cyber Apocalypse". Could be quite fun for a few of the members here? get some teams on the go!
<https://www.hackthebox.com/events/cyber-apocalypse-2025>

Anyway, hoping to get back into training seriously again after a little break so wish me luck!

Hope everyone has had a productive and hack-y day!

Glad to see you back man :)

I would have join HTB but just bought THM premium, and I'm also working on many things for the new group such as threads / tutorials <https://hackforums.net/showthread.php?tid=6294379> , besides Staff things also require a lot of time so I don't have enough to join you on HTB... However I will be glad to see you sharing content / boxes / rooms about it on HF !

We've also mentioned to the Admin about integrating HTB / THM profiles on HF, that could be really cool like this :

padrino - March 16, 2025, 5:42 pm

(Mar 16, 2025 05:04 PM)Bastille Wrote: [\[CITE\]](#) Glad to see you back man :)

I would have join HTB but just bought THM premium, and I'm also working on many things for the new group such as threads / tutorials <https://hackforums.net/showthread.php?tid=6294379> , besides Staff things also require a lot of time so I don't have enough to join you on HTB... However I will be glad to see you sharing content / boxes / rooms about it on HF !

We've also mentioned to the Admin about integrating HTB / THM profiles on HF, that could be really cool like this :

Ah that's awesome man! I have THM Premium and I REALLY need to make use of it lol

And yeah man, integrating HTB and THM profiles would be sick.

Bastille - March 17, 2025, 3:14 am

Posting for today, completed 1 room on THM : <https://tryhackme.com/room/meterpreter> I'll do more later, but posting to save this spot.

Streak : 75 ?

Rank : 7543 ?

I'm also planing to continue my HUGE VirusTotal thread for people interested in malware analysis with a ton of tips and sharing personal experience.

I should also go through some Security+ questions to finally pass the exam, I feel that I'm delaying it as 270\$ is not a low amount and it would piss me off to fail the exam. I hope to get it before the end of the month, it should be good to then move to CySA+

EDIT :

Completed the following room too : <https://tryhackme.com/room/javascriptessentials> (I'm now at 81% of the Cyber Security 101 path), I wanted to start other rooms but I'll now work on my VirusTotal guide

Bastille - March 18, 2025, 4:31 am

Posting for today, just completed the following room on THM : <https://tryhackme.com/room/capabasics> , I didn't know this tool but it's really interesting and I'll definitely take a look in-depth at it, especially when I'm into malware analysis.

I have many things to do today, need to continue my VirusTotal guide, I also need to work on some animated GIF for MRT-X like signature, profile banner, etc.

I need to continue the Malware Removal Academy program

I need to work on my Security+ cert

Streak : 77 ?

Rank : 7425 ?

Hope you're good and you keep going guys, it's been a while since you posted last time : [SIM-5594896](#) [Thul3a](#) [Galaxe](#) [Pr0m3th3us](#) [dannyswindle](#) [mention=8080] [Dystortion](#) [Chorozon](#) [JoseMar](#) [M?tt](#) [Overdose](#) [OtherBarry](#) [raceconditioned](#) [TENET](#) [plops](#) [ubermensch38](#) [capt_nemo](#) [Miracula](#)

plops - March 18, 2025, 7:17 am

Thanks Bastille.

Checking in now.

I fell off the past couple of weeks. I let myself give too much time to healthier habits. But I am slowly getting back at it.

Yesterday I started <https://tryhackme.com/room/billing>. I hope to finish this one tonight. This one is interesting considering most of the easy rooms I have finished usually had some for of bruteforce required. But not this room.

I also will start finding ways to incorporate more of the defensive side into my training next when I

re-establish this groove. I'm excited for this one. There's seems to be a lot of training and real world things I can do here.

I've said it once and I'll say it again (this time I mean it), ill check in daily here along with the classic checkin. Helps with personal accountability.

Good luck folks

M?tt - March 18, 2025, 6:16 pm

Taking GCIA next week. Going through labs again to make sure I'm good to test next week. It has definitely been an exhausting last few months balancing work, school, and life. As with anything, grinding through the hard times proves to be worth it. Now let's hope I can continue my hot streak with exams and get over a 90 on this one as well.

ybu1234 - March 18, 2025, 6:51 pm

New to this. Could anyone help me?

ybu1234 - March 18, 2025, 7:02 pm

(Mar 18, 2025 06:51 PM)ybu1234 Wrote: [\[CITE\]](#) New to this. Could anyone help me?
I guess how to hack haha. Don't really know how to code and do other stuff.

SIM-5594896 - March 19, 2025, 3:43 am

??? Hello hello peeps ! ???

I have not been posting for a long time, sorry for that ! Been trapped in a weird mix of busy/lazy ?
Also I was away from THM and lost my streak, but I've been doing some practical work.
I acquired some second hand Rpis for cheap and am practicing on them.

Last project I completed is a NAS server to store backups of my system using rsync. The server is operating a headless raspbian and the harddrive is encrypted.
I am almost done with it but I still need to make some sort of a menu with couple of options when initiating the ssh connexion with the server. So then I don't need to type all the commands to mount the external storage (encrypted) and maybe the same on my local host to perform the backup.
/The menu is important because since I am focusing on security and the hdd is encrypted, I can't really automate the whole process without losing on the sec side/
Appart from that it works well.

On the list of the rpi projects, I'd also like to setup a piHole, maybe a home VPN and a nextcloud server also.

The idea is to populate a list of practical projects related to both cyberSec and sysAdmin (linux). So then I can speak about it in a job interview and balance my lack of pro xp.

I hope you guys have been working well.

Thanks for hose who kept on posting, It gave me strength! ??

THM streak: 1 ?

THM rank: 62100

plops - March 19, 2025, 7:59 am

I completed <https://tryhackme.com/room/billing> last night. It was a fun one and I definitely overlooked some stuff.

No real work today so,
Today's agenda:
Complete a THM room
Start studying blue team resources

Bastille - March 19, 2025, 11:35 am

(Mar 18, 2025 07:02 PM)ybu1234 Wrote: [\[CITE\]](#) I guess how to hack haha. Don't really know how to code and do other stuff.
Hello, welcome to HF

If you want to learn more about hacking I encourage you to :

Read the following thread : <https://hackforums.net/showthread.php?tid=6263412>
Register and start practicing here : <https://tryhackme.com> > there are hundred of rooms about web exploitation

You can then share your daily progresses here :
<https://hackforums.net/showthread.php?tid=6288695>
we speak about hacking and motivate each of use to study even a little bit every day

If you have questions you can ask on HF

Don't forget to read the [Help Docs](#)

Enjoy your stay !

Bastille - March 20, 2025, 5:02 am

[Bumping to not merge my posts]

Just completed the following room on TryHackMe : <https://tryhackme.com/room/sqlfundamentals>
I was really skeptical about SQL as I'm not wired for programming but this is by far the easiest language I went with.

Not sure if I'll have enough time to do more rooms today, because I need to work on :
- MRT-X Academy
- VirusTotal Guide
- a "sub" thread of the VirusTotal Guide about file padding
- Security+ cert

Besides there is a sunny weather right now, I'll probably go out with my skateboard and ride some

Tryhackme streak : 79 ?
Rank : 7340 ?

Hope you're doing good and you keep going guys !

SIM-5594896 - March 20, 2025, 5:29 am

??? hey guys ! ???

This morning I completed a very nice (and quite easy) room on thm:
<https://tryhackme.com/room/disgruntled>

The room is a challenge about incident surface in Linux systems.
You'll be tasked to investigate the system after a shady script has been planted.
Other than that I finished my Nas server by editing the .bashrc file and creating aliases to ease the administration.

Keep the fire burning ???

+++

THM streak: 2 ?
THM rank: 59600

Bastille - March 21, 2025, 12:38 pm

Posting for today, completed the following room on THM :
<https://tryhackme.com/room/burpsuitebasics>

Cyber Security 101 path completed at 89% !

[SIM-5594896](#) thanks for the disgruntled room, I'll definitely take a look at it, perfect for my SOC analyst path !

Tryhackme streak : 80?
Rank : 7309?

Hope you doing good guys !

SIM-5594896 - March 22, 2025, 2:43 am

??? hallo hallo ! ???

Yesterday I worked on a new THM [room](#) called "Linux file system analysis".

The room is very similar to the previous one I worked on: a sort of guided tour of the areas to investigate after an incident as well as some very usefull comands such as the stat one that I did not know before and gives you alot of info on a file.

@Bastille, you might like this one as well if it's not already crushed on your side haha.

I'm halfway through it and will try and finish it today but a great carnival starts at 14.00 today and I spent 3 hours making a mask yesterday so let's see :)

Keep the steal hot ???

+++

THM streak: 3 ?
THM rank: 59000

Bastille - March 22, 2025, 2:58 am

(Mar 22, 2025 02:43 AM)SIM-5594896 Wrote: [\[CITE\]](#) ??? hallo hallo ! ???

Yesterday I worked on a new THM [room](#) called "Linux file system analysis".

The room is very similar to the previous one I worked on: a sort of guided tour of the areas to investigate after an incident as well as some very usefull comands such as the stat one that I did not

know before and gives you a lot of info on a file.

@Bastille, you might like this one as well if it's not already crushed on your side haha.

I'm halfway through it and will try and finish it today but a great carnival starts at 14.00 today and I spent 3 hours making a mask yesterday so let's see :)

Keep the steal hot ???

+++

THM streak: 3 ?

THM rank: 59000

Already crushed Linux file system analysis room haha, I save all my notes on Notion.so :

By the way if you want to tag someone put his username between two @ signs like : @Bastille @ (without the last space)

plops - March 22, 2025, 2:55 pm

Ayo,

Checking in for day 4.

I managed to get through a couple of rooms the past few days:

<https://tryhackme.com/room/w1seguy> -

I have never worked on XOR encryption, and to be honest, I'm still mildly confused coming out of that room. Oh well, it's something to add to list read ups.

<https://tryhackme.com/room/cyberlensp6> -

This was a lot of fun since it introduced me to hacking a windows machine. Which was crazy to me, I have spent so much time working with linux cli that it has become easy and I know what to do for the most part if needed. But even though windows is my daily driver, I had no idea what I was doing at first lol. All my google searches were '[linux cmd] equivalent to windows'. I need to set myself up with a couple more windows boxes.

The groove and motivation is coming back, feels good. After Day 7 I am going to start digging back into wireshark, packets and networking.

Good lucks folks, see you soon

Bastille - March 23, 2025, 9:25 am

Hey learning-mates,

Completed 3 rooms today :

- <https://tryhackme.com/room/sqlmapthebasics>
- <https://tryhackme.com/room/digitalforensicsfundamentals>
- <https://tryhackme.com/room/remnuxgettingstarted>

The only one remaining to complete the 101 Cybersecurity path (currently at 98%) is <https://tryhackme.com/room/flarevmarsenaloftools>

I'll take a look at it tomorrow, it's Sunday, don't want to overwhelm myself.

I'll start the Level 1 SOC path Tuesday I think (April), then Level 2 SOC path (May), then I'll start working on my homelab (June + July)

Hope you keep going and enjoy the week-end guys !

Streak : 82 ?

Rank : 7090 ?

M?tt - March 23, 2025, 7:00 pm

Didn't do so well on my GCIA Practice Exam. Going to spend the next 3 days re-reading some parts I didn't do well on and churcing up my index. At the least, I crushed the labs which I was actually worried about.

ybu1234 - March 23, 2025, 7:11 pm

Can't even get an interview. Thinking college was a big scam after all huh.

Zitoenontop - March 23, 2025, 10:59 pm

Thank you very much this is what I was looking for

Bastille - March 24, 2025, 12:41 am

(Mar 23, 2025 07:00 PM)M?tt Wrote: [\[CITE\]](#) Didn't do so well on my GCIA Practice Exam. Going to spend the next 3 days re-reading some parts I didn't do well on and churcing up my index. At the least, I crushed the labs which I was actually worried about.

You're on the right track and you've done the hardest part. I'm keeping my fingers crossed for you ??

(Mar 23, 2025 07:11 PM)ybu1234 Wrote: [\[CITE\]](#) Can't even get an interview. Thinking college was a big scam after all huh.

What did you study ? What job are you looking for ? How many times have you applied ? In which country ? Are you sure about your CV ? Did you work on personal projects ? did you get any certification ? is it the same for your classmates ?

(Mar 23, 2025 10:59 PM)Zitoenontop Wrote: [\[CITE\]](#) Thank you very much this is what I was looking for

You're welcome buddy, hope to see you active here, don't forget to read the following thread for a good start : <https://hackforums.net/showthread.php?tid=6263412> (and feel free to leave a post too !)

SIM-5594896 - March 24, 2025, 6:40 am

??? hej ! ???

I did nothing yesterday, the carnival got me on saturday so I spend the whole sunday picking up pieces of myself...

Back at it today though, I finished the "Linux file system analysis" room and the "Summit" one <https://tryhackme.com/room/summit>. The second was a challenge room type and was about managing to block malwares from behavioral analysis reports. Really liked it.

Now I just embarked on the Investigating Windows room that is kind of the same sort of room <https://tryhackme.com/room/investigatingwindows>, Blue teaming on windows OS.

[Bastille](#) now I can also properly tag someone ?

Anyways, nice to see so much activity on the thread! Gives me strength for sure ??
Hope you guys are good.

Keep it up ???

+++

THM streak: 1 ?
THM rank: 57400

Bastille - March 24, 2025, 1:34 pm

Just completed the following room on tryhackme.com :
<https://tryhackme.com/room/flarevmarsenaloftools> , I was already familiar with most of the tools but I also discovered few others, such as FLOSS and CFF Explorer. Malware analysis is probably my favorite field right now, don't have enough skills / knowledge to work as a malware analyst tho, but maybe in the future after getting bored working few years as a SOC analyst.

Completing this room also allowed me to complete the Cyber Security 101 path. Tomorrow I'll dive into the next one : <https://tryhackme.com/path/outline/soclevel1>

Hope you keep going guys, almost 3 months since we've started this thread, 25% of the year already behind us, let's make the remaining very productive !

Streak : 83 ?
Rank : 7024 ?

M?tt - March 24, 2025, 5:48 pm

(Mar 23, 2025 11:29 PM)vrs Wrote: [\[CITE\]](#) Sorry to hear that buddy, but glad you have that great attitude to keep pushing forward ?

I've been spinning the wheels myself this past few days,

Hope to get it going this week. Will try to hack at least 1 satellite tomorrow.
I mean, I'm learning a lot so that's the intent. I'm just trying to at least uphold my GPA at this point.
Thursday we will see how it goes.

(Mar 24, 2025 12:41 AM)Bastille Wrote: [\[CITE\]](#) You're on the right track and you've done the hardest part. I'm keeping my fingers crossed for you ??
I'll definitely post how it goes.

Bastille - March 25, 2025, 7:28 am

Just started the Level 1 SOC path on tryhackme, I've already completed few rooms in the past, so I started with the following : <https://tryhackme.com/room/yara>

I've heard about Yara few times, but wasn't familiar with. It helped me to understand better the role of this tool and how it's helping during malware analysis / threat hunting.

I hope to do more rooms today, it could be nice to complete the Level 1 SOC path before May, so I could complete Level 2 in May, and start working on my homelab in June.

Hope you keep going guys !

Streak : 84 ?

Rank : 6917 ?

EDIT : Just completed one more room : <https://tryhackme.com/room/fridayovertime>

I hope to do one more today, to be honest I was kinda reluctant on the previous path as it was not 100% related to cybersecurity, but I'm definitely more motivated by this one.

ybu1234 - March 25, 2025, 7:12 pm

(Mar 23, 2025 11:29 PM)vrs Wrote: [\[CITE\]](#) Sorry to hear that buddy, but glad you have that great attitude to keep pushing forward ?

I've been spinning the wheels myself this past few days,

Hope to get it going this week. Will try to hack at least 1 satellite tomorrow.

I studied Business and I do have security plus

Bastille - March 26, 2025, 1:30 am

Just completed a room on tryhackme.com based on CTI and OpenCTI :

<https://tryhackme.com/room/trooper>

No major difficulties, however I had to use OpenCTI and I'm definitely fond of this tool, added to my servers to setup in my homelab's list. That also motivated me to dive into the MITRE ATT&CK matrice which I need to know because it's often mentioned in job offers.

Streak : 85 ?

Rank : 6617 ?

Hope to complete more rooms today, but I also need to go back into MRT-X academy on HF

Hope you keep going guys !

EDIT :

- Completed the third exercise of the MRT-X Academy of HackForums.net

- Completed the following room (which was boring AF to be honest) :

<https://tryhackme.com/room/trafficanalysissentials>

- Completed the following room : <https://tryhackme.com/room/introtoendpointsecurity>

- This one was a pain in the ass and to be honest I had to use write-ups, not because I struggled but because it took too much times and I didn't want to waste more time on it :

<https://tryhackme.com/room/windowseventlogs>

SIM-5594896 - March 26, 2025, 2:41 am

??? Hi all ! ???

Yesterday I went through couple of rooms including some Challenge type rooms: Investigating windows, The greenholt phish and principals of security.

Today I am starting the day with this: <https://tryhackme.com/room/btwindowsinternals>

The thing is that I've had a Linux as my main OS for some time now and I have kinda forgotten how windows works so I need to get back to it ???

I am also very glad because I'm getting close to my goal which was to be within top 3% on THM ?

Hope you guys are good.

Let's rock this wednesday ! ???

+++

THM streak: 2 ?
THM rank: 50500

Thul3a - March 27, 2025, 2:36 am

Hey, after some time I'm back.

Unfortunately lost my THM streak but I'm already at 3 so that's something. Completed a room about MITRE tools which was interesting and but what interests me more are forensics, so I started doing the Windows forensics 2 (I already finished Win forensics 1). I don't have much to say unfortunately but I hope that changes.

Also wonder if any of you have some funky tor websites (could be anything but not markets etc.). Kinda interested how people find them.

See you next time!

Bastille - March 27, 2025, 3:32 am

(Mar 26, 2025 02:41 AM)SIM-5594896 Wrote: [\[CITE\]](#) ??? Hi all ! ??[color=#17B529]?[/color]

I am also very glad because I'm getting close to my goal which was to be within top 3% on THM ?

Hope you guys are good.

Let's rock this wednesday ! ???

Congrats for getting closer to your goal of top 3%, step by step, day by day, constancy is key ?

(Mar 27, 2025 02:36 AM)Thul3a Wrote: [\[CITE\]](#) Hey, after some time I'm back.

Unfortunately lost my THM streak but I'm already at 3 so that's something. Completed a room about MITRE tools which was interesting and but what interests me more are forensics, so I started doing the Windows forensics 2 (I already finished Win forensics 1). I don't have much to say unfortunately but I hope that changes.

Also wonder if any of you have some funky tor websites (could be anything but not markets etc.). Kinda interested how people find them.

See you next time!

Hey ! Nice to see you back on track ? I didn't know your were interested in forensic, TryHackMe has a lot of content related to this field, I'm sure you'll learn a lot

Regarding the dark web, there are two main "repositories" :

- <https://thehiddenwiki.org/>

- <https://tor.taxi/>

I know few things about the dark net and dark web, mainly technical stuff, but I do not browse these websites, so don't have particular to recommend you, I stay away from these websites and their illegal activities.

Aside of these repos, you can find them on Discord and TG channels, but most of these channels are actually made by scammers to scam beginners because they are easy preys as they don't know what they do. That's also why I stay away from Discord and TG channels

M?tt - March 27, 2025, 5:49 pm

Got a 95 on my GCIA today. I'll definitely say that I didn't expect this score, but going with that gut feeling when in doubt probably helped me most. Ultimately, I was glad I aced all the labs at least.

SIM-5594896 - March 28, 2025, 3:33 am

??? Hello knights of the cyber realms ! ???

Yesterday I did not work on THM since I had completed the rooms I had started the day before and I dedicated the whole day to my current lab project:

-> Setting up my own VPN server at home using a headless Rpi4 (8GB RAM) and wireguard w/ dynamic DNS service (freedns.afraid.org).

It did not work after a whole day and then I had a breakthrough around 19.30 and it is almost complete now.

As often I was a typo in my credentials that was the main problem ???

Anyways I was telling about it and it finally happened, I am now among top 3% on THM ??

It ain't much, but it's honest work !

? To celebrate the fact I reached my previous goal I propose a little improvised party challenge ?

---> The first who finds out the answer gets not 10, not 30 buuuuuut =====> ?50% of ALL my bytes? !

Crazy right ? ?

61 65 74 69 73 6f 6f 2f 6f 6c 6e 6f 77 63 74 74 70 61 2f 32 31 6e 62 2d 72 2d 33 78 31 70 63 74 69
65 65 6c 6e 61 6d 69 2e 6d 70 6f 65 2f 6c 64 32 31 32 75 65 74 65 33 30 31 2e 67 68 69 70 73 63
6c 2f 6e 61 65 63 2f 2d 6e 6e 75 6f 73 30 2f 2f 6d 72 68 65 2d 30 38 6a

=> Who did Pythagoras learn from ??

Clue: Who were the members of the first triumvirate ?

???

Wish you a great day !

bang bang ???

+++

(Mar 27, 2025 03:32 AM)Bastille Wrote: [\[CITE\]](#) Congrats for getting closer to your goal of top 3%, step by step, day by day, constancy is key ? Thanks for cheering man ! ?

(Mar 27, 2025 05:49 PM)M?tt Wrote: [\[CITE\]](#) Got a 95 on my GCIA today. [...] Ultimately, I was glad I aced all the labs at least. Well done sir!! ??

THM streak: 0 ?

THM rank: 49800

Bastille - March 28, 2025, 12:15 pm

(Mar 28, 2025 03:33 AM)SIM-5594896 Wrote: [\[CITE\]](#) ??? Hello knights of the cyber realms ! ???

Yesterday I did not work on THM since I had completed the rooms I had started the day before and I dedicated the whole day to my current lab project:

-> Setting up my own VPN server at home using a headless Rpi4 (8GB RAM) and wireguard w/ dynamic DNS service (freedns.afraid.org).

It did not work after a whole day and then I had a breakthrough around 19.30 and it is almost complete now.

As often I was a typo in my credentials that was the main problem ???

Anyways I was telling about it and it finally happened, I am now among top 3% on THM ??
It ain't much, but it's honest work !

? To celebrate the fact I reached my previous goal I propose a little improvised party challenge ?
---> The first who finds out the answer gets not 10, not 30 buuuuuut =====> ?50% of ALL my bytes? !
Crazy right ? ?

61 65 74 69 73 6f 6f 2f 6f 6c 6e 6f 77 63 74 74 70 61 2f 32 31 6e 62 2d 72 2d 33 78 31 70 63 74 69
65 65 6c 6e 61 6d 69 2e 6d 70 6f 65 2f 6c 64 32 31 32 75 65 74 65 33 30 31 2e 67 68 69 70 73 63
6c 2f 6e 61 65 63 2f 2d 6e 6e 75 6f 73 30 2f 2f 6d 72 68 65 2d 30 38 6a

=> Who did Pythagoras learn from ??

Clue: Who were the members of the first triumvirate ?
???

Wish you a great day !

bang bang ???

+++

Thanks for cheering man ! ?
Well done sir!! ??

THM streak: 0 ?

THM rank: 49800

The VPN server is definitely an interesting project to work on, congrats for this and your rank on THM :)

I tried to decrypt the hex part but got the following :

aetisoo/olnowcttpa/21nb-r-3x1pctieelnami.mpoe/ld212uete301.ghipscl/naec/-nnuos0//mrhe-08j

Don't know how to continue, not sure if I'm doing things right or no

Bastille - March 29, 2025, 12:34 am

[Bumping to not merge my posts]

Didn't post for the 2 previous days, did a lot on Thursday, definitely less on Friday (hungover), but I did the necessary to keep my streak.

Just completed the following room : <https://tryhackme.com/room/sysmon> , very interesting and it was something I planed to setup in my homelab. I saved the procedure to configure the tool for later.

I hope to complete more rooms today, I really want to finish the TryHackMe training part to dive into the homelab and more practical stuff.

Streak : 88 ?

Rank : 6264 ?

EDIT : Just saw that by the way ??

Completed the following room : <https://tryhackme.com/room/osqueryf8> very powerfull tool, I've also planed to integrate it in my SOC-based homelab

Completed one more room : <https://tryhackme.com/room/wazuhct> , also planed to get this in my homelab, the room definitely helped me to better understand how it works, what's the purpose of the tool and the difference with others like Sysmon, Osquery, and so on

Completed one more room : <https://tryhackme.com/room/mondaymonitor> I definitely like rooms based on SOC roles, it's been a while since I've spend so much time on THM in a single day

captn_nemo - March 29, 2025, 2:55 am

I've started again.

How do you manage to keep at it every day?

Everyday life keeps getting in the way, work and family are more important to me.

Let's see how far I get this time.

Bastille - March 29, 2025, 3:09 am

(Mar 29, 2025 02:55 AM)captn_nemo Wrote: [\[CITE\]](#) I've started again.

How do you manage to keep at it every day?

Everyday life keeps getting in the way, work and family are more important to me.

Let's see how far I get this time.

Hey, glad to see you back on track !

I guess it's easier for me because I'm unemployed right now and I'm single. I usually start my day with TryHackMe right after going out of the bed, when I'm at 100% of my energy and attention level.

I do not study more than a hour, I take breaks and do something else lik chores, or groceries, or sport. Then I go back to THM if I can.

If I was employed I would study maybe on the lunch break, or at night after going back to home (that's what I used to do, when I worked). But the second option works only if you don't have kids / wife I guess

captn_nemo - March 29, 2025, 12:41 pm

I was really successful today.

I finished the learning Path Jr Penetration Tester and have now made the 'Next.js: CVE-2025-29927' box.

It's really scary how Next.js solved this with the middleware. The blog [post](#) on this is also very good. I learnt a lot.

Bastille - March 30, 2025, 3:46 am

Just completed a room on THM : <https://tryhackme.com/room/retracted> , allowed me to practice what I've learned about Sysmon to get more familiar with the event IDs. Completing this room allowed me to finish the "Endpoint Security Monitoring" section of the Level 1 SOC learning path. The path is now completed at 42%

Planning to do a lot more today if I can

Streak : 89 ?

Rank : 6200 ?

Regarding the rank, I've took a look at the leaderboard and I would need to reach at least rank 1100 to be in the first 50 french members. The members at the bottom of the leaderboard have at least 400 rooms completed and I'm only at 204, that's crazy ! Not sure I could reach it before the end of the year but let's try !

Hope you're doing good guys, keep going ;)

captn_nemo - March 31, 2025, 12:43 pm

I did 3 boxes today and learnt a lot.
tryhackme.com/room/injectics
tryhackme.com/room/creative
tryhackme.com/room/hammer

At the box [Creative](#) I learnt about [GTF0Bins](#).
This is really helpful for CTFs.

Bastille - March 31, 2025, 1:51 pm

Just completed the following room (late) : <https://tryhackme.com/room/intromalwareanalysis>

Quite trivial, I'm already into malware analysis and it wasn't that advanced. I completed the room at almost 11PM to not lose my streak and to keep going.

I didn't do much on THM because I actually spent most of my day on topics related to RFID cards. I wanted to learn how to read data from them, how rewriting works, the security mechanisms, vulnerabilities, etc. I started making a tutorial thread about it, it's such a fascinating subject. I used an ACR122U device for this, and I found out there's also the Proxmark3, which is well-known in the field and more advanced, allowing for more capabilities.

I've also received a IDE to USB device to read old HDD that I've found while setting up a 1998 IBM computer for projects I have in my mind (I'll share them on HF).

Streak : 89 ?

Rank : 6151 ?

Hope you keep going guys, it's been 3months since 2025 started, time flies, hope you're proud of what you've achieved so far, if not, you know what you need to do.

Robert Rouge - March 31, 2025, 3:58 pm

Hello again Bastille, am joining your challenge.

is going to not be able to do every day concurrently, is going to make days miss up

Day 1:

Join CodeWars - Did couple challenges

Join Code Academy - 15% Through Learn C# course

Watched Video about shellcode injection

Finished batch virus generator in C#

Bastille - April 1, 2025, 1:33 am

(Mar 31, 2025 03:58 PM)Robert Rouge Wrote: [\[CITE\]](#) Hello again Bastille, am joining your challenge.

is going to not be able to do every day concurrently, is going to make days miss up

Day 1:

Join CodeWars - Did couple challenges

Join Code Academy - 15% Through Learn C# course

Watched Video about shellcode injection

Finished batch virus generator in C#

Glad to see you joining us ! Constancy is key, as long as you study regularly it's ok if you're not active every day

Hope to see you around !

Bastille - April 1, 2025, 4:45 am

[Bumping my thread to not merge my posts]

Just completed the <https://tryhackme.com/room/windowsforensics1> room, not an easy room, especially with all the different important registry locations and new tools to learn, there are 2 or 3 rooms like this one in the Level 1 SOC learning path.

Not in a good mood today, I don't think I'll do more TryHackMe today, however yesterday I went to bed with a huge motivation to learn C/C++ and make my own malware. I'll maybe dive into this or go back to RFID hacking I was into yesterday.

Today I've completed a 90 days streak !

Hope you keep going guys, even a little bit every day.

Streak : 90 ??

Rank : 6059 ?

EDIT : Just watched 2 hours of C programming courses, there is approximately 12 hours remaining, if I keep the same rhythm I should be able to finish in 1 week. I think alternating between THM and programming is good. Hope after the courses I'll be able to play with Windows API and kill some systems (I'm really nostalgic of the 90's viruses, I'm more interested in displaying skulls with glitches and weird sound to crash the computer than black hat stuff, but I'll dive into loader, evasion techniques, and so on, for malware analysis purposes).

SIM-5594896 - April 1, 2025, 5:50 am

??? Hello guys ???

Not much to tell but thought about saying "hi" anyways.

I've lost my THM streak again ? since I've been working on Rpi based projects for the last days. I've almost finished the VPN server project and also made a little PiHole for my home network. Works like a charm :)

[Bastille](#) You were on the right track for my little game. But, it may be not that well made and the cash prize is not that hot either ?.

I thought someone else would try it but it seems I'll keep my Bytes for myself ?

Also, congrats for the 90 days streak, solid habit!

Wish you all a nice day !

THM streak: 0 ?

THM rank: 49800

captn_nemo - April 2, 2025, 9:33 am

Fourth day in a row. ?

I'm very motivated at the moment because I'm currently in 2nd place in Germany.

This month I would like to try to maintain a good ranking.

Right now I am working on the 'CompTIA Pentest+' path and have finished 40%.

Robert Rouge - April 2, 2025, 12:45 pm

Hello, checking in for last two days.

-Updated and shared DivineLogger keylogger with different features.

-Made it to 30% Learn C#. no copy-pasta

Bastille - April 2, 2025, 2:48 pm

Quick checking-in, I had a lot of things to do today, so I studied a little bit on THM, then switched to C programming courses for 1 hour

Hope to do more tomorrow

ttbr0 - April 2, 2025, 11:14 pm

(Apr 2, 2025 02:48 PM)Bastille Wrote: [\[CITE\]](#) Quick checking-in, I had a lot of things to do today, so I studied a little bit on THM, then switched to C programming courses for 1 hour

Hope to do more tomorrow

show us some malware written in c

Bastille - April 3, 2025, 2:03 am

(Apr 2, 2025 11:14 PM)ttbr0 Wrote: [\[CITE\]](#) show us some malware written in c

I'm still at the beginning, started back with the basics like loops, conditions and so on ? I think I'll be able to make interesting things when I start learning how to use Windows APIs. I also need to find Mald3v or Sekt0r7 courses, somewhere ...

Bastille - April 3, 2025, 4:08 am

[Bumping my thread to not merge my posts]

Just completed the following room : <https://tryhackme.com/room/windowsforensics2> , I'm now at 48% of the SOC Level 1 path.

Very interesting, especially about recovering deleted files from disk images with Autopsy. I've learned many things

Not sure if I'll be able to complete more THM rooms today, however I'll definitely go back to C programming courses.

Streak : 92 ?

Rank : 5984 ? (let's goooo, below 6000 ?)

I'm going to the gym, I'll continue later, keep going guys !

Bastille - April 4, 2025, 4:23 am

Just completed 4 rooms on THM, I wanted to get rid of the phishing module :

- <https://tryhackme.com/room/phishingemails3tryoe>
- <https://tryhackme.com/room/phishingemails4gkxh>
- <https://tryhackme.com/room/phishingemails5fgjlzxc>
- <https://tryhackme.com/room/snappedphishingline>

It was trivial, the most interesting part was about analyzing PCAP files with SMTP traffic.

I'm now at 52% of the Level 1 SOC path, I hope to be able to finish it soon to then move onto Level 2 which sounds definitely more interesting.

Streak : 93 ?

Rank : 5483 ?

I'll maybe continue THM later, I really want to finish this Level 1 path to move onto Level 2 .. But I also want to go back into C programming.

Hope you keep going guys !

EDIT : Just completed an additional room : <https://tryhackme.com/room/btautopsye0> which was very interesting ! Crazy how simple it is to retrieve information from a disk image. I thought about working as a forensic analyst after few years as a SOC analyst, it's definitely something I'll do !

EDIT 2 : Just watched 1h30 of C programming courses about functions, modular and pointers, will continue tomorrow. Can't wait to make my first malware, those things are really boring .. but probably necessary too.

Rsynced - April 4, 2025, 8:16 pm

Thanks for doing this, I never really thought about Teaching Others is the best way to retain information.

captn_nemo - April 6, 2025, 6:36 am

I was able to defend my position to some extent. I'm now in 5th place in Germany this month. This ranking system really motivates me to keep at it and keep going.

Streak: 8 ?

Robert Rouge - April 6, 2025, 5:23 pm

hello again, i am now 45% through the 30 hour C# course
i have realized how spoiled on ide and ai i am to fix codes because i am using their built in emulator.

have also started taking lessons on another phone application before i go to bed.

gnojedkire - April 6, 2025, 5:31 pm

Thats a interessant way to share you and get knowledge

HashAccounts - April 6, 2025, 5:38 pm

Hey, checking in for today

Money- - April 6, 2025, 6:22 pm

(Apr 6, 2025 05:38 PM)HashAccounts Wrote: [\[CITE\]](#) Hey, checking in for today

Lol this is not the bytes check in thread. Funny. I too sometimes thought it was that honestly.

Bastille - April 7, 2025, 7:40 am

It's been a while since I posted last time, I managed to keep my streak but didn't do a lot, needed few days to rest.

Just completed the following room : <https://tryhackme.com/room/btredlinejoxr3d> interesting but forensic is not my favorite part for now. I already have so many things to learn about SOC tasks / tools, it could come later but as it's part of the Level 1 SOC path, I'm doing my best to complete it.

Streak : 96 ?

Rank : 5384 ?

Hope you keep going guys !

Just completed one more room on THM : <https://tryhackme.com/room/linuxforensics> , the path is now completed at 58%, can't wait to start Level 2 SOC which is way more interesting

Robert Rouge - April 7, 2025, 7:44 am

don't have much time today but spent the last few hours getting to 55% completion on c# lesson. (Codecademy) am going to try to start learning a little more about hacking now that feel like I have a stronger base to work from.

Bastille - April 7, 2025, 5:20 pm

Just completed a new room on TryHackMe : <https://tryhackme.com/room/kape>

The forensics part is not my favorite, still don't know why it's in the Level 1 SOC as it's not a part from the position of Level 1 SOC analyst ...

Streak : 97 ?

Rank : 4966 ? Below 5000 !

2AM now, can't sleep, let's rush some rooms while listening to Liquid DnB with a 00's vibe

Hope you keep going guys, almost 100 days since we've started this thread.

EDIT : just completed a room based on Volatility to analyze memory dumps : <https://tryhackme.com/room/volatility> , I really enjoyed this one, definitely super useful for malware / artificats loaded in memory only during malware analysis.

EDIT : just completed the following room : <https://tryhackme.com/room/thehiveproject> very interesting ! I'll definitely setup TheHive and Cortex in my SOC-based homelab, I must get familiar with it

EDIT : completed one more room : <https://tryhackme.com/room/unattended> , it was interesting to solve a "real case" to practice

EDIT : just completed the following room <https://tryhackme.com/room/disgruntled> very very interesting, I prefer investigations on Linux than Windows. Path completed at 67%

Robert Rouge - April 8, 2025, 7:23 pm

am now up to 75% of the way through with the codecademy. am going to have to remember to come back to this one because looked at the answer and messed everything up. starting a free networking course on Udemy (warez disallowed) too

Bastille - April 9, 2025, 1:07 am

Just completed the following room on tryhackme : <https://tryhackme.com/room/critical> I definitely LOVE volatility, that will be an amazing tool during malware analysis on infected machines.

I hope to do more today, can't wait to finish the Level 1 SOC path, I'll then slow down for Level 2 SOC path as I need to pass my Security+ exam before the end of the month

Streak : 98 ?
Rank : 4885 ?

Hope you keep going guys !

EDIT : Just completed an additional room : <https://tryhackme.com/room/registry4n6> , Registry Explorer is an amazing tool, however I definitely need to get more familiar with the most common / useful registry entries. There are so many things it's kinda hard to remember all of them, wondering how SOC analysts / Forensic analyst do, if there are tips / cheat sheets / or if they remember everything.

EDIT : Just completed one more room : <https://tryhackme.com/room/investigatingwithelk101> , I was afraid of diving into ELK because I was familiar with Splunk and I didn't want to overwhelm my brain with "useless" info, but it turns out that they are very similar and I think Splunk is based on ELK. I completed the room quickly, no difficulties.

Just4kickz - April 9, 2025, 11:53 am

I started 3 days ago, I signed up for THM as recommended and it's helped me through the bare essentials of Linux and doesn't seem all that scary now.

By the end of day 3 I learnt how to flash / boot Kali with a stick, still having trouble with persistence though.

Will keep updates from here on in.
To everybody here, ask questions, keep going, it's all daunting at first sight but the puzzle slowly pieces together.

Bastille - April 9, 2025, 12:03 pm

(Apr 9, 2025 11:53 AM)Just4kickz Wrote: [CITE](#) I started 3 days ago, I signed up for THM as recommended and it's helped me through the bare essentials of Linux and doesn't seem all that scary now.

By the end of day 3 I learnt how to flash / boot Kali with a stick, still having trouble with persistence though.

Will keep updates from here on in.

To everybody here, ask questions, keep going, it's all daunting at first sight but the puzzle slowly pieces together.

Glad to hear that you're enjoying learning and that you keep going ! Linux can be pretty impressive at first sight especially the command line interface if you have no Desktop Environment, but as you probably learned how to use Windows by using it, you'll learn how to use Linux by using it :)

Feel free to setup virtual machines to use Linux, with virtual machines you can easily revert your modifications with snapshots. When you'll feel comfortable enough feel free to install Linux in a dualboot configuration with Windows, so you'll be able to use Linux as your daily distro, and switch to Windows when you need (I personally use Linux as my daily distro, but for gaming I switch to Windows)

Hope to see you posting regularly here, if you have questions feel free to ask !

okceshi - April 9, 2025, 6:33 pm

100% ??????:

????,???,

???????????

Bastille - April 9, 2025, 7:42 pm

(Apr 9, 2025 06:33 PM)okceshi Wrote: [\[CITE\]](#) 100% ??????:

????,???,

???????????

Hello, welcome to HF, please read our [Help Docs](#) / rules :

6. All text must be in English or readable as English in the case of fancy unicode.

Thanks

Bastille - April 9, 2025, 7:46 pm

[Bumping my thread to not merge my posts]

4AM here, can't sleep, so why not completing more TryHackMe rooms ? Just completed the following : <https://tryhackme.com/room/itsybitsy>

Quite easy, no difficulties, can't wait to setup my SOC-based homelab to practice more on a SIEM (Splunk).

Streak : 99 ? (100 soon)

Rank : 4754 ? (I should be able to be in the Top 50 France if I can reach at least rank 3000, only 1754 ranks remaining !)

Hope you kepe going guys, learning hacking is a matter of time and constency.

EDIT : Almost 1PM here, just completed the following room :

<https://tryhackme.com/room/wiresharkpacketoperations> , I'm not fond of Wireshark, really powerful tool but too many options, filters, and so on. I was already familiar with it so it was complicated.

Bastille - April 11, 2025, 3:44 am

Just completed one more room : <https://tryhackme.com/room/tempestincident>

It was a simulation, involving Windows Logs, packet captures, sysmon, and a computer compromise. Very interesting, I had to rely on a write-up some times especially on the Wireshark part, but I'm getting more familiar with other tools such as EvtxEmul, sysmon, Brim and TimeLineExplorer (this one is very useful).

Streak : ??

Rank : 4551 ?

I need want to complete the Level 1 SOC path to have more free time to work on my Security+ cert, I must pass the exam before the end of the month, hope I'll get it.

plops - April 11, 2025, 6:26 am

Here for my once in a while check in.

My learning and training has been consistent but I have started turn quantity into quality. I was stuck trying to make sure i did not break my streak in completing boxes in a day. But I only have a couple hours each day to train/learn. This made me start to rely on writeups and ai to solve problems instead of thinking through them and building scripts myself.

So I have readjusted the way I approach my learning. I downloaded KeepNote and create my own write up as I work through the rooms. Documenting my phases, attempts and journal. Its insane what 'thinking(typing my thought process) out loud' has done for my ability to zooming in on a problem and find a solution. I still use ai but i set it to not give me answers and instead act as a coach when I am stuck.

This causes my rooms to take much longer, but the value of learning and thinking I have gotten had been invaluable and boosts my confidence.

I completed THM's Capture! Last night after working on my first successful, self built, script:

<https://hackforums.net/showthread.php?tid=6296026>

For a couple of days lol.

Good luck folks, see you next time on the check in.

Robert Rouge - April 11, 2025, 2:52 pm

good luck with exam [Bastille](#)

today i was supposed to finish c# but need to take break on the last lesson.

I will finish tomorrow, last section is with LINQ and have not practiced very much with this at all yet.

Bastille - April 11, 2025, 11:07 pm

(Apr 11, 2025 06:26 AM)plops Wrote: [\[CITE\]](#) Here for my once in a while check in.

My learning and training has been consistent but I have started turn quantity into quality. I was stuck trying to make sure i did not break my streak in completing boxes in a day. But I only have a couple hours each day to train/learn. This made me start to rely on writeups and ai to solve problems instead of thinking through them and building scripts myself.

So I have readjusted the way I approach my learning. I downloaded KeepNote and create my own write up as I work through the rooms. Documenting my phases, attempts and journal. Its insane what 'thinking(typing my thought process) out loud' has done for my ability to zooming in on a problem and find a solution. I still use ai but i set it to not give me answers and instead act as a coach when I am stuck.

This causes my rooms to take much longer, but the value of learning and thinking I have gotten had been invaluable and boosts my confidence.

I completed THM's Capture! Last night after working on my first successful, self built, script:

<https://hackforums.net/showthread.php?tid=6296026>

For a couple of days lol.

Good luck folks, see you next time on the check in.

Glad to see you back ! Yeah relying on write-ups can be counter productive, I try to not but sometimes when I spend too much time on a room I giveup and look at write-ups.

(Apr 11, 2025 02:52 PM)Robert Rouge Wrote: [\[CITE\]](#) good luck with exam [Bastille](#) today i was supposed to finish c# but need to take break on the last lesson.
I will finish tomorrow, last section is with LINQ and have not practiced very much with this at all yet.
Thanks man ! I started to make flash cards yesterday from notes I've taken, based on practice exams I've went through. I plan to pass it 2 times if I fail at the first try, I'll then work on CySA+ I think, sounds valuable for a SOC analyst position.

Just completed the following room : <https://tryhackme.com/room/boogeyman1> , the Wireshark part still gets me ... but as I'm practicing I'm getting more comfortable with.

Streak : 101 ?

Rank : 4363 ?

EDIT : just completed an additional room <https://tryhackme.com/room/boogeyman2> , I definitely LOVE volatility, I think I'm going some time to explore all the options and practice with it, this will definitely be in my tool list for malware analysis

Robert Rouge - April 13, 2025, 5:07 am

have finished C# course and introduction to Cybersecurity course on codecademy
want to put it all together so am trying to think of final project.

13parliament37 - April 13, 2025, 6:29 am

(Jan 3, 2025 12:09 PM)Bastille Wrote: [\[CITE\]](#) Just completed :

- 1 SOC case on letsdefend.io : really easy, didn't encounter difficulties. I really love to solve those SOC cases, some of them are from real case scenarios. With the free version of Letsdefend I can only do 15 cases per months. I'm thinking about upgrading to the premium version but Letsdefend is a little bit more expensive compared to tryhack me (anually : 17€ per month for letsdefend, and around 11€ per month for tryhackme) and for the time being I cannot subscribe to paid version for both of them lol

- 1 room on tryhackme.com : EEEEEZ, OSINT / email analysis

<https://tryhackme.com/r/room/threatinteltools>

Hello, i just started today on THM. I got some basic skills but cant define at what level, so i just did the intros and will go on with the one you mentioned on the 1st page in this thread. love osint

Bastille - April 13, 2025, 7:07 am

(Apr 13, 2025 05:07 AM)Robert Rouge Wrote: [\[CITE\]](#) have finished C# course and introduction to Cybersecurity course on codecademy
want to put it all together so am trying to think of final project.

Nice to see that you keep going buddy ! Is Codeacademy good ? I've started to learn C language and wondering if it would be a good addition ?

(Apr 13, 2025 06:29 AM)13parliament37 Wrote: [\[CITE\]](#) Hello, i just started today on THM. I got some basic skills but can't define at what level, so i just did the intros and will go on with the one you mentioned on the 1st page in this thread. love osint

Welcome on board man ! Glad to see that you've started, learning hacking is a matter of time and consistency, feel free to share your daily progresses / accomplishments on platforms like THM or even personal projects. Sometimes I also share here threads I've made such as tutorials / guides and so on.

Hope that at the end of the year you'll look back at your first post here and say "Damn, how far I've come from" ?

13parliament37 - April 13, 2025, 8:10 am

(Apr 13, 2025 07:07 AM)Bastille Wrote: [\[CITE\]](#) Nice to see that you keep going buddy ! Is Codeacademy good ? I've started to learn C language and wondering if it would be a good addition ?

Welcome on board man ! Glad to see that you've started, learning hacking is a matter of time and consistency, feel free to share your daily progresses / accomplishments on platforms like THM or even personal projects. Sometimes I also share here threads I've made such as tutorials / guides and so on.

Hope that at the end of the year you'll look back at your first post here and say "Damn, how far I've come from" ?

Thank you! I am still on it. Having trouble with the VM on the site.

..

30 minutes later i got it. was fun and challenging, definitely had a learning. I try to share when i start a project one day!

Robert Rouge - April 13, 2025, 1:26 pm

(Apr 13, 2025 07:07 AM)Bastille Wrote: [\[CITE\]](#) Nice to see that you keep going buddy ! Is Codeacademy good ? I've started to learn C language and wondering if it would be a good addition ? It is very good if you do not let yourself cheat.
No AI or no "view solution". at most you must "view hint".

will keep going there, but I am now wanting to try the hackthebox thing you play. I make account but I do not know how to play.
can you point me?

Bastille - April 14, 2025, 1:43 am

(Apr 13, 2025 01:26 PM)Robert Rouge Wrote: [\[CITE\]](#) I am now wanting to try the hackthebox thing you play. I make account but I do not know how to play.
can you point me?

Unfortunately I'm not on HTB, don't know how it works. I know there are different hack the box, like hack the box academy which is easier for beginners, but that's all I can do

Just completed the following room : <https://tryhackme.com/room/boogeyman3>

Didn't do a lot yesterday, I was sick, still recovering today, I'm not going to do more. I'll probably work on threads or on my Security+ cert

Streak : 103 ?
Rank : 4217 ?

Robert Rouge - April 14, 2025, 9:14 am

(Apr 14, 2025 01:43 AM) Bastille Wrote: [CITE](#) Unfortunately I'm not on HTB, don't know how it works. I know there are different hack the box, like hack the box academy which is easier for beginners, but that's all I can do

Just completed the following room : <https://tryhackme.com/room/boogeyman3>

Didn't do a lot yesterday, I was sick, still recovering today, I'm not going to do more. I'll probably work on threads or on my Security+ cert

Streak : 103 ?
Rank : 4217 ?

read this every day and do not know why got confused.

signed up for tryhack me and finished all the starter rooms: <https://tryhackme.com/p/RobRouge>

TryHackMe Streak: 1

have finished Codecademy C#, Intro to Cybersecurity, Intro to generative AI, Introduction to ai Operating system basics.

the ones that were not coding seemed very basic. starting asp.net lesson under C# though since it helped. i saw google is paying software people to not work in europe so am doubling down again on getting good before ai and picked up daily practice on tenfastfingers because faster words is faster code. will do every day i tryhackme.

Bastille - April 16, 2025, 2:49 am

Ok guys, back on track ! I've been sick for few days, wasn't able to do a lot, but ready to continue !

Just completed two rooms this morning :

- <https://tryhackme.com/room/soc1alerttriage>

- <https://tryhackme.com/room/intelcreationandcontainment>

I've left the Level 1 SOC path for the time being, I didn't complete the network related part but it's going to take me so long and don't have the motivation for this right now. So instead of lurking I've decided to do something that motivates me more (definitely one of the benefits of working in IT, there are so many different fields that you can just switch from one to another if you're bored).

Streak : 105 ?
Rank : 4190 ?

I'll continue to study for the Security+ exam, I must pass it by the end of the month.

Hope you're doing good guys

Robert Rouge - April 16, 2025, 1:27 pm

have done introduction to networking but am having issues with the course structure for tryhackme. anytime i do a room, it recommends me another similar room, and when i click it it wants me to pay.

i will get it though, did network room today. streak 3

codecademy I started c++ instead of asp.net because i was feeling motivated. it is very similar to c#

so i feel myself picking it up much faster. I am 40% through the "Learn C++" course and plan on doing it and intermediate before reevaluating

ybu1234 - April 16, 2025, 5:45 pm

So if you suck at coding you can't hack right? I've failed so many coding courses in high school and college?

Bastille - April 16, 2025, 10:15 pm

(Apr 16, 2025 01:27 PM)Robert Rouge Wrote: [\[CITE\]](#) have done introduction to networking but am having issues with the course structure for tryhackme.

anytime i do a room, it recommends me another similar room, and when i click it it want's me to pay.

i will get it though, did network room today. streak 3

codecademy I started c++ instead of asp.net because i was feeling motivated. it is very similar to c# so i feel myself picking it up much faster. I am 40% through the "Learn C++" course and plan on doing it and intermediate before reevaluating

There is a lot of free content, but yeah some rooms are available for premium users only. There are enough free room to learn for months for free, but if you can afford the paid version you'll improve your productivity with the paths.

(Apr 16, 2025 05:45 PM)ybu1234 Wrote: [\[CITE\]](#) So if you suck at coding you can't hack right? I've failed so many coding courses in high school and college?

Where did you see that ? If you didn't already, feel free to read the following thread, everything is expained there, there is section for coding : <https://hackforums.net/showthread.php?tid=6263412>

Bastille - April 18, 2025, 2:06 am

I have been less active on tryhackme recently, more focused on my security+ exam.

I've just completed the following room <https://tryhackme.com/room/lessonslearned> , started Level 2 SOC anayst path

Streak : 107 ?

Rank : 4095 ?

I hope to complete more rooms, there is a new feature called "Weekly Leagues", you start from bronze and can climb the ranks, currently at silver, I should be able to go to gold in two days, I need to continue at this rate and everything should be ok.

EDIT : just completed the following room : <https://tryhackme.com/room/tardigrade> no real difficulties

EDIT : one more room <https://tryhackme.com/room/soc1alertreporting> , made me think about the helpdesk I worked at, the fact that I've worked as a helpdesk tech will sure help to work as a SOC analyst

Bastille - April 18, 2025, 8:04 pm

[Bumping my thread to not merge my posts]

4 AM, can't sleep, so why not completing some rooms. However I don't think I choosed the right topic. I wanted to improve my malware analysis skills so I completed the following room : <https://tryhackme.com/room/x8664arch> , I've read few things about CPU and Memory architecture few years ago. I'm not a complete noob but some concepts were not easy to understand, especially at 4 AM, but I think I'm fine.

Streak : 108 ?

Rank : 4019 ? it's getting harder to climb the ladder, people are more active so they constantly get back their position. Besides the gap in points between ranks is now bigger.

Hope you're doing good, keep going guys ..

I've competed three more rooms :

- <https://tryhackme.com/room/introtodetectionengineering>
- <https://tryhackme.com/room/tacticaldetection>
- <https://tryhackme.com/room/socl1alertreporting>

Im High - April 18, 2025, 8:15 pm

There's some good stuff you're working through. I did a lot of tryhackme and hackthebox to fill in some of the hands on/knowledge gaps that I had before switching over to a SOC role myself. I think what helped me the most was just the repetition and overall familiarity you get from working through CLI.

I'll take a look and see what boxes I still need to work on and see if I can't participate myself.
Great journey.

Just4kickz - April 18, 2025, 11:33 pm

Kali Update - Understood the basics, playing around with hashcat, airgeddon. Really getting the feel for the Linux OS, definitely driven my enthusiasm to keep learning.

Anybody out there who's reading all these guides and trying to mass everything into their brain in one night. You're new, you're not bad or hopeless. If you're reading this KEEP GOING.

s0lo - April 18, 2025, 11:56 pm

(Apr 18, 2025 11:33 PM)Just4kickz Wrote: [\[CITE\]](#) Kali Update - Understood the basics, playing around with hashcat, airgeddon. Really getting the feel for the Linux OS, definitely driven my enthusiasm to keep learning.

Anybody out there who's reading all these guides and trying to mass everything into their brain in one night. You're new, you're not bad or hopeless. If you're reading this KEEP GOING.

im also playing around with airgeddon, fun stuff, im thinking about buying a second wifi adapter to try to push the max out of airgeddon

Just4kickz - April 19, 2025, 1:12 am

(Apr 18, 2025 11:56 PM)s0lo Wrote: [\[CITE\]](#) im also playing around with airgeddon, fun stuff, im thinking about buying a second wifi adapter to try to push the max out of airgeddon

I was actually having a look at them today when I was out and about, it's a good way to start.

Bastille - April 19, 2025, 2:10 pm

(Apr 18, 2025 08:15 PM)Im High Wrote: [\[CITE\]](#) There's some good stuff you're working through. I did a lot of tryhackme and hackthebox to fill in some of the hands on/knowledge gaps that I had before switching over to a SOC role myself. I think what helped me the most was just the repetition and overall familiarity you get from working through CLI.

I'll take a look and see what boxes I still need to work on and see if I can't participate myself.
Great journey.

Thanks for sharing your experience, I've definitely planed to get more familiar with CLI in both Windows and Linux. I'll play with a SOC-based homelab for 2 or 3 months with attack simulation with Caldera or Atomic Red, before starting job interviews. I'll also present my lab during the job

interviews, I think it will help.

Hope to see you around this thread :)

(Apr 18, 2025 11:33 PM)Just4kickz Wrote: [\[CITE\]](#) Kali Update - Understood the basics, playing around with hashcat, airgeddon. Really getting the feel for the Linux OS, definitely driven my enthusiasm to keep learning.

Anybody out there who's reading all these guides and trying to mass everything into their brain in one night. You're new, you're not bad or hopeless. If you're reading this KEEP GOING. KEEP GOOOIIINNNNNNG ? It's not easy to remember everything, the most effective way is to teach. Otherwise, practicing regularly will help remember and memorize. That's also why practicing every day (even a little bit) helps !

(Apr 18, 2025 11:56 PM)s0lo Wrote: [\[CITE\]](#) im also playing around with airgeddon, fun stuff, im thinking about buying a second wifi adapter to try to push the max out of airgeddon
Feel free to make a tutorial if you can, I'm sure many members will appreciate, and teaching is the best way to retain what you learn ?

Bastille - April 20, 2025, 12:26 am

[Bumping my thread to not merge my posts]

Just completed a room on tryhackme : <https://tryhackme.com/room/threatintelligenceforsoc> , helped me to get more familiar with rules on ELK with <https://uncoder.io/>

Streak : 109 ?

Rank : 3991 ? (below 4000 ?)

I can't wait to build my SOC-based homelab, studying (even if I can practice on THM) starts being kinda boring, I really want to practice more, attacking my servers and detect it on the tools. I will have at least 2 or 3 months to practice before starting job interviews. I think it will be enough

Robert Rouge - April 20, 2025, 8:00 am

Hello again, did not post for a couple days but was working hard

have figured out tryhackme, at the top of the learn section, they categorize between free and paid, and been clicking paid ones. had been doing one a day but yesterday i messed up. (still have streak tho)

made the vpn setup that 7 talked about, but it took me much longer than 2 minutes because he is very smart. wonder if it is safety concern to use vps for multitask if it is vpn; also wonder if should stop using opera built in vpn now that am protected or if double is good.

50% through "Learn C++" before starting today.

Working on "Fundamental skills" section in try hackme.

10fastfingers tests (58 wmp)

Edit: found out tryhack.me takes you to hackthebox, so that is where messed up at first

Bastille - April 21, 2025, 11:33 am

Didn't do a lot today on TryHackMe, just enough to keep my streak, instead I've released a thread : <https://hackforums.net/showthread.php?tid=6296678>

The topic is really interesting and I could make a thread with a video making a demo on how LE crack phones

I've also conducted a malware analysis on this tool :
<https://hackforums.net/showthread.php?tid=6296631>

Streak : 110 ?

Bastille - April 21, 2025, 11:57 pm

[Bumping my thread to not merge my posts]

Just completed the following room on tryhackme :
<https://tryhackme.com/room/introductiontothreathunting> , quite easy, I was able to practice on the MITRE Navigator to get more familiar with it, for the rest of the day I'll work on my Security+ cert.

Streak : 111 ?
Rank : 3973 ?

Hope you keep going guys, it's been a while since I saw some members last time

Bastille - April 23, 2025, 12:42 am

Just completed a room on tryhackme : <https://tryhackme.com/room/sigma>

I've started with another room but the Kibana daemon wasn't able to start, I've lost like 30 minutes, re-starting the VM 4 times, waiting at least 5 minutes each time as recommended on the room to give enough time to the server to start correctly. Wasted time investigating, scanning with nmap and so on. I've reported the issue to THM, and I moved to the Sigma room.

Streak : 112 ?
Rank : 3946 ?

Bastille - April 24, 2025, 12:55 am

Just completed the following room on tryhackme : <https://tryhackme.com/room/sighunt> definitely one of my favorite, repeating 9 times similar things definitely helps to memorize. The room was oriented around Sigma rules to create based on a given scenario.

Streak : 113 ?
Rank : 3872 ?

Hope you keep going guys

Dystortion - April 24, 2025, 11:25 am

(Apr 24, 2025 12:55 AM)Bastille Wrote: [\[CITE\]](#) Streak : 113 ?

Rank : 3872 ?

Killing it brother!!

franc-jeu

Bastille - April 24, 2025, 11:27 am

(Apr 24, 2025 11:25 AM)Dystortion Wrote: [\[CITE\]](#) Killing it brother!!

franc-jeu

Thanks mate ! Step by step, with steady effort, even a little every day, it helps.

Feel free to join this thread and share your achievements whenever you want !

Dystortion - April 24, 2025, 12:13 pm

(Apr 24, 2025 11:27 AM)Bastille Wrote: [\[CITE\]](#) Thanks mate ! Step by step, with steady effort, even a little every day, it helps.

Feel free to join this thread and share your achievements whenever you want !
For sure when I get my hands back on a computer - hopefully soon. My son poured water on my last one lol

Bastille - April 24, 2025, 11:59 pm

Morning everyone ! Just completed a bugged room on tryhackme (again) :
<https://tryhackme.com/room/auroraedr>

Second time in two days I come across a bugged room, I've waste a lot of time, especially on this one because I had to look for answers online (no choice, full bugged VM), and THM changed one of the answer (those idiots), so I had to put on ChatGPT the batch script executed, then how many words and characters per words expected for the answer, be aware that ChatGPT is definitely not good at counting chars, I asked for the second word being 14 chars, took me almost 5 real minutes, asking multiple times because he always generated words with not the good number of characters, like :

ChatGPT : "Modification" > 14 characters, we have our second word !

Me : No, it's only 12 characters

ChatGPT : Oh yes you're right, let me correct that ! I think the word is "Hollowing" > 14 characters"

Me : NOOO THAT'S 9 CHARACTERS

and so on, for like 5 real minutes

Don't know if I'll complete more rooms, I still need to work on my security+ cert, I must pass the exam during the next week.

Streak : 114 ?

Rank : 3848 ?

Hope you keep going guys !

padrino - April 25, 2025, 3:46 am

Checking in for the first time in ages. I really need to commit more time to it, but in all honesty, I've fallen down a rabbit hole of just spending my free time playing video games rather than working on my cyber security knowledge - something i don't see getting better now that the oblivion remaster has been released haha.

Anyway I think my major update would be that I'm attending the InfoSec Europe conference with work - super excited about this as it will be my first cyber security conference so I'm uper excited to speak to all the vendors and learn a lot from the talks. I'm thinking of taking loads of notes and maybe giving a detailed run down of what was there, what talks I went to, what I learnt etc. Maybe it could help some people on here / make some interesting reading? Let me know what you think!

Anyway - Hope you're all thriving and doing well personally and proessionally! Hopefully I'll start to be a little more active haha

Depicide - April 26, 2025, 5:18 pm

This is awesome! I have to jump on this train to keep up with training

Bastille - April 26, 2025, 8:42 pm

(Apr 25, 2025 03:46 AM)padrino Wrote: [\[CITE\]](#) Checking in for the first time in ages. I really need to

commit more time to it, but in all honesty, I've fallen down a rabbit hole of just spending my free time playing video games rather than working on my cyber security knowledge - something I don't see getting better now that the Oblivion remaster has been released haha.

Anyway I think my major update would be that I'm attending the InfoSec Europe conference with work - super excited about this as it will be my first cyber security conference so I'm super excited to speak to all the vendors and learn a lot from the talks. I'm thinking of taking loads of notes and maybe giving a detailed run down of what was there, what talks I went to, what I learnt etc. Maybe it could help some people on here / make some interesting reading? Let me know what you think!

Anyway - Hope you're all thriving and doing well personally and professionally! Hopefully I'll start to be a little more active haha

Glad to see you back ! I was waiting for another Elder Scrolls, I've enjoyed Oblivion but I expected a new game after Skyrim. Bethesda seems to just recycle old games ... We had like 6 versions of Skyrim since 2011 that's crazy, and now they're going back with Oblivion lol.

If you struggle to study, just put small objectives, even half an hour a day is still better than nothing ;)

Enjoy the conference ! And yeah feel free to share what you've learned, hope to see you around !

(Apr 26, 2025 05:18 PM)Depicide Wrote: [\[CITE\]](#) This is awesome! I have to jump on this train to keep up with training

Let's goooo, one more fellow joining us ! Remember, even a little every day is good, constancy is key ;)

Depicide - April 26, 2025, 9:28 pm

(Apr 26, 2025 08:42 PM)Bastille Wrote: [\[CITE\]](#) Glad to see you back ! I was waiting for another Elder Scrolls, I've enjoyed Oblivion but I expected a new game after Skyrim. Bethesda seems to just recycle old games ... We had like 6 versions of Skyrim since 2011 that's crazy, and now they're going back with Oblivion lol.

If you struggle to study, just put small objectives, even half an hour a day is still better than nothing ;)

Enjoy the conference ! And yeah feel free to share what you've learned, hope to see you around !

Let's goooo, one more fellow joining us ! Remember, even a little every day is good, constancy is key ;)

Isn't that the truth. Practicing and sharing the resources to help others is what makes us all better

s0lo - April 28, 2025, 1:13 am

(Apr 19, 2025 02:10 PM)Bastille Wrote: [\[CITE\]](#) Feel free to make a tutorial if you can, I'm sure many members will appreciate, and teaching is the best way to retain what you learn ?

tl;dr - I'm combating myself

I could make a tutorial and I would like to make tutorials or know-hows in general, I like to teach and explain to someone who is interested in things, but I think it's good to know that I'm around all this only for a year, so I'm kind of new myself.

Either way, a few weeks back I wanted to build and deploy a web login page that I can learn to brute-force on, I got so interested in all that, I have ended up with 5 different webpages, deployed on 3 different VPS. I've made a temp text & file share with PGP support, a web chat, a honeypot and a URL & file test against VirusTotal and other APIs. I got lost in all that for a few weeks, but I have learned things.

Yes, I did use a lot of ChatGPT, because I have not made a website in general before, not even using pre-made platforms, so yeah, now I have all these things running and I need to upgrade my management a bit, cuz all it works 90%, some small adjustments so I can say it's 100% working, but sometimes I do forget where I have a given backend or bot running. :D

Bastille - April 28, 2025, 11:20 am

Quick post, did a lot yesterday because I'm on THM League (currently Sapphire), but this morning I've scheduled my Security+ exam date so now I'm 90% focused on the exam, for the next days I'll just complete few tasks on THM to not lose my streak but will not do that much. Security+ is my priority right now (can't afford losing 400€ on this exam .. this is not not the right moment), if everything goes well I'll then focus on CySA+.

Wish me luck guys

Streak : 117 ?
Rank : 3683 ?

13parliament37 - April 28, 2025, 2:59 pm

Hello.

Just want to give an update. I definitely don't get to post here every day, but I kept going! Finally found a project I can learn much about python and is not too hard for the start. It's basically just to calculate and show the paths of 2 balls in an old goofy 8 Ball game that is based on JS. The GUI looks like a piece of shit but I love it.

[8 Ball angles](#)

Much work left.

padrino - April 28, 2025, 4:40 pm

Back hitting the THM stuff. Trying to keep the habit alive. I've boxed off the linux fundamentals part 1 today - all easy stuff I already know but I need a refresher in some on linux /unix terminal commands (as a windows dev I rarely have to use it) and wanted to start from the very beginning so I don't miss anything. Basic commands like cd, cat, ls, whoami, pwd, grep, echo, find etc. and some basic unix operators like &, &&, >, >>.

Good refresh all in all. Will be moving onto module 2 tomorrow.

Keep at it, fellas!

Lefty - April 28, 2025, 5:17 pm

Never hurts to learn a bit more. Thank you

SilentTrace - April 29, 2025, 2:05 am

(Apr 28, 2025 11:20 AM)Bastille Wrote: [\[CITE\]](#) Quick post, did a lot yesterday because I'm on THM

League (currently Sapphire), but this morning I've scheduled my Security+ exam date so now I'm 90% focused on the exam, for the next days I'll just complete few tasks on THM to not lose my streak but will not do that much. Security+ is my priority right now (can't afford losing 400€ on this exam .. this is not the right moment), if everything goes well I'll then focus on CySA+.

Wish me luck guys

Streak : 117 ?

Rank : 3683 ?

Oh man! Ur are in the good stuff. Have u already seen the eJPT certification from INE Security? Its my next step in the roadmap. Now i'm doing the pentesting path of HTB to reach the cert. Then i will go behind eJPT.

padrino - April 29, 2025, 4:50 pm

Another checkin from me - continuing with the linux fundamentals and learning about how to manipulate files using mv, cp, mkdir, touch, rm, and file. All basic stuff but a super useful refresher. Also covered permissions and changing users along with common directories such as /var /tmp /etc and /root.

Just need to box off Linux fundamentals part 3 of THM to complete my refresher before starting a new learning path. Stuck on what to choose though. Career wise I want to look more into blue team stuff, but the redteaming and pentesting stuff is always so much more fun to learn.

Bastille - April 30, 2025, 2:02 am

(Apr 28, 2025 02:59 PM)13parliament37 Wrote: [\[CITE\]](#) Hello.

Just want to give an update. I definitely don't get to post here every day, but I kept going! Finally found a project I can learn much about python and is not too hard for the start. Its basically just to calculate and show the paths of 2 balls in an old goofy 8 Ball game that is based on JS. The GUI looks like a piece of shit but i love it.

[8 Ball angles](#)

Much work left.

Glad to see you posting, as long as you keep going it's the most important ;) that would be fun to go to a bar with your computer and run the program to test if it works in real with a pool haha (would love to see pics of that moment !)

(Apr 28, 2025 05:17 PM)Lefty Wrote: [\[CITE\]](#) Never hurts to learn a bit more. Thank you
Feel free to join us and share what you've learned / accomplished recently ;)

(Apr 29, 2025 02:05 AM)SilentTrace Wrote: [\[CITE\]](#) Oh man! Ur are in the good stuff. Have u already seen the eJPT certification from INE Security? Its my next step in the roadmap. Now i'm doing the pentesting path of HTB to reach the cert. Then i will go behind eJPT.

Wish you good luck for your certs :) Didn't go through these as they are pentesting oriented and I'm following a blue team path for my career, starting with a SOC Analyst position

(Apr 29, 2025 04:50 PM)padrino Wrote: [\[CITE\]](#) Another checkin from me - continuing with the linux fundamentals and learning about how to manipulate files using mv, cp, mkdir, touch, rm, and file. All basic stuff but a super useful refresher. Also covered permissions and changing users along with common directories such as /var /tmp /etc and /root.

Just need to box off Linux fundamentals part 3 of THM to complete my refresher before starting a new learning path. Stuck on what to choose though. Career wise I want to look more into blue team

stuff, but the redteaming and pentesting stuff is always so much more fun to learn.

Nice ! Linux is definitely a must have knowlegde when it comes to cybersecurity, in case you didn't yet, I recommend you to move on Linux as your daily distro, it will help practicing every day even when you're not studying, I did that and it helped me a lot, I kept a second disk for Windows tho (dual boot) when I need to play video games that can't run on Linux for example.

What's good with blue team is that it also requires red team knowledge, for example if you're into SOC analysis you'll need to be aware of how hackers conduct their activities, with what tools, what traces they left in the logs, and so on. And what's good with cybersecurity is that you can work a year or two in a job, and then move to something else, it's easy to pivot from one position to another, and your experience will be beneficial in all cybersecurity jobs you go through

cyclone254 - April 30, 2025, 5:01 am

Thanks alot for the definitive guide, this will really be of help

Bastille - April 30, 2025, 5:11 am

(Apr 30, 2025 05:01 AM)cyclone254 Wrote: [\[CITE\]](#) Thanks alot for the definitive guide, this will really be of help

You're welcome, if you have a question feel free to ask, don't forget to share your achievments here, we motivate each of us to study / practice even a little every day, hope to see you around !

Bastille - April 30, 2025, 5:31 am

(Apr 30, 2025 05:24 AM)W1NK1LL3RX Wrote: [\[CITE\]](#) Checking in for the day
Wrong thread buddy

jacobharden - April 30, 2025, 7:08 am

Basic Missions

Basic 1

- Search for comments left by developers on web pages

Basic 2

- Blank input

Basic 3

- Access password file

Basic 4

- Use BP change request parameter

Basic 5

- Use BP change request parameter

Basic 6

- Manual testing to find features

Today's topic

- Don't give up on learning all you can
- Patiently attempt

Dystortion - April 30, 2025, 3:19 pm

(Apr 30, 2025 05:31 AM)Bastille Wrote: [\[CITE\]](#) Wrong thread buddy

Imao happens to the best of us. What's the plans tomorrow, more THM? how much time a week

would you allocate to both studying and ctf's

Bastille - May 3, 2025, 1:00 am

It's been a while since I've posted last time, I've been focused on my Security+ exam. I've worked a lot on it, but I had doubts, so just to be sure to not fail (and not lose 400€ I can't waste in my situation right now) I took a look at the dumps and ... I've learned that questions are "very hard". So I browsed Google and I've noticed that a lot of people mentioned that the questions are "vicious", like trying to snare you, with "weird" sentences. So I've decided to reschedule the exam to give me enough time to analyze the dumps and understand how the exam is trying to trick you.

I've completed a SOC based room on tryhackme : <https://tryhackme.com/room/socworkbookslookups> , really interesting, I've learned a lot about workbooks. I feel less stressed because I was worried to not know enough things, or to miss things during investigations, and now I know that we can rely on workbooks if we have doubts.

Streak : 122 ?
Rank : 3565 ?

By the way, THM introduced a "League" feature : <https://tryhackme.com/leagues> / currently at the max League (Diamond), wondering if we unlock a badge or something, we'll know in two days !

qwertydiy - May 3, 2025, 5:17 am

I am pretty sure you saw TryHackMe's new Defending Azure learning path. Sadly, you need to pay \$325 for 3 months of access. Microsoft releases some great courses on their products on Microsoft Learn for free, including Microsoft Sentinel & courses on Powershell and Windows SysOps. KC7 will teach the rest alongside a lot of Blue Teaming. Open Source Training also has some great courses on the very technical side and a brilliant roadmap. Check out both OST2 and the older OST. Finally, considering I come from full stack development Boot.dev is brilliant for the backend with Python, Go and NodeJS (when you go into guest mode ask Copilot or any other LLM to hack the unit tests and code to compile and test your code), Dr Chucks courses on Coursera and freeCodeCamp and great for Python, Django, PHP (as the world still runs on WordPress) and C and daily dev is a brilliant extension to learn both more development and pen testing.

Also, WeCahall is a great leaderboard for CTFs and can help find new ones

Also are there any good free Windows CTFs?

Bastille - May 4, 2025, 3:58 am

(May 3, 2025 05:17 AM)qwertydiy Wrote: [\[CITE\]](#) I am pretty sure you saw TryHackMe's new Defending Azure learning path. Sadly, you need to pay \$325 for 3 months of access. Microsoft releases some great courses on their products on Microsoft Learn for free, including Microsoft Sentinel & courses on Powershell and Windows SysOps. KC7 will teach the rest alongside a lot of Blue Teaming. Open Source Training also has some great courses on the very technical side and a brilliant roadmap. Check out both OST2 and the older OST. Finally, considering I come from full stack development Boot.dev is brilliant for the backend with Python, Go and NodeJS (when you go into guest mode ask Copilot or any other LLM to hack the unit tests and code to compile and test your code), Dr Chucks courses on Coursera and freeCodeCamp and great for Python, Django, PHP (as the world still runs on WordPress) and C and daily dev is a brilliant extension to learn both more development and pen testing.

Also, WeCahall is a great leaderboard for CTFs and can help find new ones

Also are there any good free Windows CTFs?

Yeah saw it, I passed the MS-500 cert but I'm not really interested in Microsoft solutions for cybersecurity, I don't think I'll go with them, like Sentinel and so on. I've learn a lot for free through their website <https://learn.microsoft.com>

Thanks for <https://p.ost2.fyi/> , the site seems to add new content regularly, that's good, there is a lot of content about RE which I'm interested into, I'll take a look at it if I don't have anything interesting on tryhackme regarding this field haha

Regarding the CTFs I've always found interesting those made by organisms such as gov cybersecurity departments. In France it's called "ANSSI" (National Agency of Security Information Systems), and they release CTFs every years. I think it's interesting to get an idea of a "gov level" CTF. Maybe you could try to check if in your country there is something similar, otherwise for the US : NSA with the "Codebreaker Challenge", US CYber Command with "Cyber Stakes", and DoE [Department of Energy] with CyberForce Competition (but maybe more blue team oriented)

It's good to talk with knowledgeable, hope to see you around !

Dystortion - May 4, 2025, 12:41 pm

(May 3, 2025 01:00 AM) Bastille Wrote: [\[CITE\]](#) It's been a while since I've posted last time, I've been focused on my Security+ exam. I've worked a lot on it, but I had doubts, so just to be sure to not fail (and not loose 400€ I can't waste in my situation right now) I took a look at the dumps and ... I've learned that questions are "very hard". So I browsed Google and I've noticed that a lot of people mentioned that the questions are "vicious", like trying to snare you, with "weird" sentences. So I've decided to reschedule the exam to give me enough time to analyze the dumps and understand how the exam is trying to trick you.

I've completed a SOC based room on tryhackme : <https://tryhackme.com/room/socworkbookslookups> , really interesting, I've learned a lot about workbooks. I feel less stressed because I was worried to not know enough things, or to miss things during investigations, and now I know that we can rely on workbooks if we have doubts.

Streak : 122 ?

Rank : 3565 ?

By the way, THM introduced a "League" feature : <https://tryhackme.com/leagues> / currently at the max League (Diamond), wondering if we unlock a badge or something, we'll know in two days !

Definitely solidify your chances at smashing the exam. I guess you'll always feel you're not prepared but I have also heard that they pose the questions awfully in some situations so as long as you can break it down to lehmman's terms you should be all good.

Well done on being at the top league lad!

Bastille - May 5, 2025, 5:24 am

Just completed a room on Splunk, as I'll soon start my SOC-Based homelab it's good going back to the basics : <https://tryhackme.com/room/splunklab>

Hope to do more today, I also need to work on my Security+ cert. Hope you're doing good and that you keep going guys !

Streak : 124 ?

Rank : 3557 ?

qwertydiy - May 5, 2025, 7:41 am

Going to start with Burp Suite today with Hackrsploit's Video on setting it up, the burp suite essential playlist, InsiderPHD's Burp Suite Playlist, Bugcrowd's Introduction to Burp Suite, TryHackMes repeater room and then start WebSec Academy if there is time.

funnywolf - May 5, 2025, 10:15 pm

TryHackMe is great !

Bastille - May 6, 2025, 10:01 am

Just completed the following room to continue with Splunk :

<https://tryhackme.com/room/splunkexploringspl>

Streak : 125 ?

Rank : 3553 ? (I'm starting struggling to improve my rank with just one room per day, gained only 4 ranks from yesterday haha)

I'm focused on my Security+ cert right now, don't have enough time to do more on THM, maybe next week !

qwertydiy - May 6, 2025, 1:05 pm

OK, CompTia seems a bit simple but essential (as in if you do not know it you are going to have a rough time). I am finally getting to the Burp Suite

Bastille - May 6, 2025, 1:12 pm

(May 6, 2025 01:05 PM)qwertydiy Wrote: [\[CITE\]](#) OK, CompTia seems a bit simple but essential (as in if you do not know it you are going to have a rough time). I am finally getting to the Burp Suite

I'm quite comfortable regarding cybersecurity but sometimes I give the wrong answer because there are different valid options, some are better than others and sometimes some information / context are missing. Or sometimes the sentence is a bit confusing. I think that I just need to read carefully, take my time and don't rush even if I think I know the answer.

Nice to see you going on Burp, how do you practice ? THM ?

padrino - May 6, 2025, 2:35 pm

Been a little bit since my last post as I've been away over the weekend. Today I finally completed the Linux Fundamentals Part 3 room on THM. I've actually really enjoyed going back over the basics of linux and improving my knowledge - it's something I have no exposure to in my professional life so this has been a good refresher from my uni days - and since it's such an important part of info sec it needed to be done. Anyway, some of the things covered in part 3 are usage of nano and vim, viewing processes, scheduled tasks, package management, and log files (again).

Next up I'm going to be looking at some red-team stuff purely because I know I've got some stuff in that area coming up at work so I need to brush up on certain bits.

In professional news I also plucked the courage to speak to the company CTO and asked him about movement from development into a full cyber security job - and he's starting to push more work in that area my way with the potential for a job change into the security team on the cards later this year - so excited to see where that leads if anywhere.

qwertydiy - May 7, 2025, 12:30 am

It's going OK, there is not that much Fred on TryHackMe so I am mostly going to learn from great YouTube series and their academy.

carbonstrike - May 7, 2025, 6:40 am

I've been working my way through the Cyber Security 101 path on THM, It's been about a month and a half of me doing it, and I'm 87% of the way through. I think the roadmaps offered on THM are a pretty solid way to start dipping your toes into Cyber Security.

However, I think like many others might find - It's very difficult to actually retain all the information you're taking in. I can already feel information from previous rooms slipping away from me as I move down the path, I think it's important to try and really take your time with your learning, if you feel there are things slipping away from your knowledge, go back over them (there isn't really a reason not to). Make sure you're doing some form of note taking, even if it's not in depth notes, something you can go back to and glance at to refresh your memory is better than nothing.

And I'm not sure if this is a more personal thing for me, but I think it's such a large field that there are almost certainly going to be parts that you enjoy a lot LESS than others; however, it's important to remember that every part is just as important, even if it might feel more on the tedious side when learning. Something like the OSI Model for example - I didn't find it incredibly invigorating to learn about, but it is crucial to understand. So, I looked online for an acronym to help me memorize it, there are plenty people have came up with online and the one I found that helps me is:

People Don't Need Those Stupid Packets Anyway

That's layer 1 - 7: Physical, Data, Network, Transport, Session, Presentation, and Application. And again if that doesn't work for you it's just an example but there are plenty of creative ways you can find to make the information stick in your head!

Recently I've been introducing myself to SIEM, learning the fundamentals of firewalls and IDS as well as learning about vulnerability scanners and why they are used. And today I'll be learning more about Defensive Security and having a think more about what path exactly I want to go down.

Wishing everyone luck on their learning journey, don't focus too hard on the destination. Try to enjoy the process of learning as much as you can, and really let yourself get involved, stay focused, good luck. :)

qwertydiy - May 7, 2025, 12:02 pm

I was just thinking but anyone who learn cybersecurity should take a Psychology 101 class and a criminology 101 class. Hacking is one of the only crimes to be going up and to help reverse this trend we are going to learn why black hats hack. Clearly it is not peace of mind and in a lot of cases money (technical black hats seem to earn similar figures on the white markt and much higher figures for 0 days on the grey market). It can make red and blue teaming a lot easier once you know what the enemy thinks and social engineering can be defended against.

Bastille - May 9, 2025, 2:26 am

I didn't post for few days but I continued to complete THM rooms, the last one is :

<https://tryhackme.com/room/socmetricsobjectives>

Still focused on SOC, I've also completed two other rooms based on Splunk. Can't wait to start configuring my SOC-based homelab.

Still studying for Security+, wish me luck ..

Streak : 128 ?

Rank : 3521 ?

Robert Rouge - May 9, 2025, 8:21 am

Long time cause sidetracked. Had to go to hospital for heat but back at it.

Lost streak, but have been working hard on trying to get method purchased to work.

old and dated, but maybe elbow grease and effort will fix. Need to set up payment gateway to

replace sellix within a website template I get. Lots to learn.

I upgrade. Looking at web design and asp.net as next learning project, but unsure because very busy season.

Bastille - May 9, 2025, 8:58 am

(May 9, 2025 08:21 AM)Robert Rouge Wrote: [\[CITE\]](#) Long time cause sidetracked. Had to go to hospital for heat but back at it.

Lost streak, but have been working hard on trying to get method purchased to work. old and dated, but maybe elbow grease and effort will fix. Need to set up payment gateway to replace sellix within a website template I get. Lots to learn.

I upgrade. Looking at web design and asp.net as next learning project, but unsure because very busy season.

Hope you're doing better now !

Congrats for the upgrade mate, enjoy the new parks ;) I saw your thread about the payment gateway and sellix but I'm not into that unfortunately, can't help, hope someone will be able to bring some info

qwertydiy - May 9, 2025, 1:22 pm

I can not do much in the next 3-4 days due to preparation for an upcoming RE GCSE. I will try and keep updated.

Andy Walker - May 9, 2025, 8:25 pm

I just started my first room and completed it. It was only pre-security but at least I got it done.

As far as retaining information, i had this problem with python for a while. But one trick I am doing is to give myself a goal I care about.

With python, I am going to make a program with it, not for practice, a real program that people can use. Its helped with motivation and I am remembering stuff better because I have attached value to this code I am writing, it's going to be the foundation for this dream program I will make.

Right now I don't have any big goal for cyber security, but I'm sure it will come to me.

P???sonl?af - May 10, 2025, 3:54 am

Hey everyone! Just posting here to follow the thread. After working 17 years as a restaurant chef (with an interest in hacking/network/coding hence the old account) I finally had the opportunity to make a career switch into Networking & Cyber Security.

I'm currently doing my graduate starting with the basics in networking, systems, OS and security.

Happy learning/training everyone!

Edit: Maybe I should add what I've already done/learned.

It's been 2 weeks with 8 full days of school. (First week was half a week cuz of a holiday)

So far I've done: Networking basics, Hardware Basics, Cyber Security Basics, Operating Systems Basics, Introduction to IoT, Crash-Course Cyber Security (By The Master Channel), Programming Logics & Some excercises in Cisco packet tracer.

Currently working on CCNA-1 & Networking Devices and Initial Configuration.

Exam scores so far:
Networking Basics: 95%
Cyber Security Basics: 86%

Bastille - May 10, 2025, 6:23 am

(May 9, 2025 01:22 PM)qwertydiy Wrote: [\[CITE\]](#) I can not do much in the next 3-4 days due to preparation for an upcoming RE GCSE. I will try and keep updated.
Good luck with your exams !

(May 9, 2025 08:25 PM)Andy Walker Wrote: [\[CITE\]](#) I just started my first room and completed it. It was only pre-security but at least I got it done.

As far as retaining information, i had this problem with python for a while. But one trick I am doing is to give myself a goal I care about.

With python, I am going to make a program with it, not for practice, a real program that people can use. Its helped with motivation and I am remembering stuff better because I have attached value to this code I am writing, it's going to be the foundation for this dream program I will make.

Right now I don't have any big goal for cyber security, but I'm sure it will come to me.
Congrats for your first room ! How do you find TryHackMe ? I really like the fact that it's not only reading courses, but there are also interactive virtual machines, servers to hack, and so on.

(May 10, 2025 03:54 AM)P??sonl?af Wrote: [\[CITE\]](#) Hey everyone! Just posting here to follow the thread. After working 17 years as a restaurant chef (with an interest in hacking/network/coding hence the old account) I finally had the opportunity to make a career switch into Networking & Cyber Security.

I'm currently doing my graduate starting with the basics in networking, systems, OS and security.

Happy learning/training everyone!

Edit: Maybe I should add what I've already done/learned.

It's been 2 weeks with 8 full days of school. (First week was half a week cuz of a holiday)

So far I've done: Networking basics, Hardware Basics, Cyber Security Basics, Operating Systems Basics, Introduction to IoT, Crash-Course Cyber Security (By The Master Channel), Programming Logics & Some excercises in Cisco packet tracer.

Currently working on CCNA-1 & Networking Devices and Initial Configuration.

Exam scores so far:
Networking Basics: 95%
Cyber Security Basics: 86%
Hey man, glad to see you back on HF :)

Damn, pretty good scores for a "beginner" ? hope you'll get graduated. How many months / years will you go through to get graduated ? Do you know what job you'll do after that ?

P??sonl?af - May 10, 2025, 6:27 am

(May 10, 2025 06:23 AM)Bastille Wrote: [\[CITE\]](#) Good luck with your exams !

Congrats for your first room ! How do you find TryHackMe ? I really like the fact that it's not only reading courses, but there are also interactive virtual machines, servers to hack, and so on.

Hey man, glad to see you back on HF :)

Damn, pretty good scores for a "beginner" ? hope you'll get graduated. How many months / years will you go through to get graduated ? Do you know what job you'll do after that ?

It's a 2 year graduate done in 9 months. So it's pretty intensive.

After 9 months there will be an intern stage that would hopefully land you a job into networking.

After that there is additional learning to progress into Cyber Security, either OTJ or in evening lessons.

Bastille - May 10, 2025, 6:34 am

(May 10, 2025 06:27 AM)P??sonl?af Wrote: [\[CITE\]](#) It's a 2 year graduate done in 9 months. So it's pretty intensive.

After 9 months there will be an intern stage that would hopefully land you a job into networking.

After that there is additional learning to progress into Cyber Security, either OTJ or in evening lessons.

Nice ! I did something similar in France when I went back to school few years ago, it was a 9 months program to get a 2 years grade more tech/admin oriented (but I think that most of us ended up working as tech / helpdesk tech).

When you go back to school as an adult I feel it's "easier" than when you're younger, because you're more focused and you know why you wake up every morning and go back to school to study (to get a better future).

I wish you good luck man, but sounds you already took a good start and you don't need luck ?

P??sonl?af - May 10, 2025, 6:42 am

(May 10, 2025 06:34 AM)Bastille Wrote: [\[CITE\]](#) Nice ! I did something similar in France when I went back to school few years ago, it was a 9 months program to get a 2 years grade more tech/admin oriented (but I think that most of us ended up working as tech / helpdesk tech).

When you go back to school as an adult I feel it's "easier" than when you're younger, because you're more focused and you know why you wake up every morning and go back to school to study (to get a better future).

I wish you good luck man, but sounds you already took a good start and you don't need luck ?

Thank you! Yeah the motivation is pretty high to do this so that makes it easier.

Andy Walker - May 10, 2025, 8:59 am

(May 10, 2025 06:23 AM)Bastille Wrote: [\[CITE\]](#) Congrats for your first room ! How do you find TryHackMe ? I really like the fact that it's not only reading courses, but there are also interactive virtual machines, servers to hack, and so on.

Yes. I didn't expect it but it was refreshing to interact with.

McClubbin - May 10, 2025, 11:55 pm

Great resources! For budget certs Coursera is legit as well.

Andy Walker - May 11, 2025, 9:14 pm

I completed the room involving defence, essentially blue team. About malware analysis, is it a strong

path to go into as a professional?

I'm interested in that.

The other roles seem more holistic while malware analysis seems niche. Though my lack of experience might be blinding me.

Do people hire those guys specifically or would they just expect the average network administrator to be able to do that to some extent?

Bastille - May 14, 2025, 2:19 am

(May 11, 2025 09:14 PM)Andy Walker Wrote: [\[CITE\]](#) I completed the room involving defence, essentially blue team. About malware analysis, is it a strong path to go into as a professional?

I'm interested in that.

The other roles seem more holistic while malware analysis seems niche. Though my lack of experience might be blinding me.

Do people hire those guys specifically or would they just expect the average network administrator to be able to do that to some extent?

The study path you choose should depend on the job you're aiming for. If you want to work as a malware analyst, SOC analyst, or do incident response, then malware analysis is relevant. On the other hand, if you want to work as a pentester, it's less relevant (you won't often use or develop malware during pentest operations).

Regarding the market and this skill, if you want to do only malware analysis and work specifically as a malware analyst, you should keep in mind that it's a very advanced field. It requires deep knowledge, especially about how malware and systems work, but also in cryptography, programming, reverse engineering, and low-level languages like assembly.

I couldn't say for sure if malware analysis at that level is highly in demand — it's often more of a "component" of a broader role (like a SOC analyst or forensic analyst). The best thing to do is check on Indeed or LinkedIn to see if it's in demand in your area.

When it comes to sysadmins, it depends on the size of the company. In small companies, you often have to do a bit of everything, so having malware analysis skills can be useful for incident response (understanding what the malware does, its impact, its goal, etc., in order to eradicate it and make sure it doesn't come back). But in larger companies, an admin usually sticks to admin tasks and will only handle security if there are predefined procedures from the security team.

Bastille - May 16, 2025, 8:09 am

Hey guys, it's been a while, I was focused on my Security+ that I just passed ! So I'm back with TryHackMe, just completed the following room : <https://tryhackme.com/room/apt28inceptiontheory>

Quite interesting as, for SOC analysts, it's important to be comfortable with the MITRE ATT&CK matrice.

I'll get back to my SOC-based homelab too, I should move to a new place soon, and I'll have everything necessary for this.

Streak : 135 ?

Rank : 3470 ?

Hope you keep going guys !

P??sonl?af - May 16, 2025, 9:30 am

(May 16, 2025 08:09 AM)Bastille Wrote: [\[CITE\]](#) Hey guys, it's been a while, I was focused on my Security+ that I just passed ! So I'm back with TryHackMe, just completed the following room : <https://tryhackme.com/room/apt28inceptiontheory>

Quite interesting as, for SOC analysts, it's important to be comfortable with the MITRE ATT&CK matrice.

I'll get back to my SOC-based homelab too, I should move to a new place soon, and I'll have everything necessary for this.

Streak : 135 ?

Rank : 3470 ?

Hope you keep going guys !

Nice man! When I have some more basic knowledge I wanne try some TryHackMe rooms too!

For now, I'm half-way in CCNA-1 with checkpoint exams of 85%/85%/92%/88%

I've progressed a bit Networking Devices and Initial Configuration but since I do that on the side as addition to my graduate and free time has been a bit limited I haven't done so much there yet.
One checkpoint exam there of 100%

Keep learning everyone!

Bastille - May 17, 2025, 2:47 am

(May 16, 2025 09:30 AM)P??sonl?af Wrote: [\[CITE\]](#) Nice man! When I have some more basic knowledge I wanne try some TryHackMe rooms too!

For now, I'm half-way in CCNA-1 with checkpoint exams of 85%/85%/92%/88%

I've progressed a bit Networking Devices and Initial Configuration but since I do that on the side as addition to my graduate and free time has been a bit limited I haven't done so much there yet.
One checkpoint exam there of 100%

Keep learning everyone!

Nice buddy ! Do you go with netacad ? Back in the days I remember I was learning and practicing with this platform. You'll definitely enjoy TryHackMe, the basics can be kinda annoying, but when you master them, hacking is reaaaally cool. But they are vital, most people want to dive straight to hacking but they don't understand what they do, so most of the time they give up.

I've just completed the following room on THM : <https://tryhackme.com/room/voltttyphoon> which brought me 450 points as it was a new room (less than a day old). Really really cool room, I've been able to practice on Splunk, it was an incident response simulation and I had to investigate the attack, I've learned few things, I used a write-up for only 1 answer, because I was looking for an

encoded powershell command, so I used the basic terms but forgot about the option "-E" to encode.

Streak : 136 ?

Rank : 3373 ?

As I've completed my daily TryHackMe room, now I'll go with some malware analysis for the forum, and then maybe continue my VirusTotal guide for beginner malware analysts

Hope you keep going guys !

Andy Walker - May 17, 2025, 3:44 am

I just completed Intro to Networking on Tryhackme. I'm going to see if I can get Ubuntu installed on one of my laptops and get started testing different things.

(May 14, 2025 02:19 AM)Bastille Wrote: [\[CITE\]](#) The study path you choose should depend on the job you're aiming for. If you want to work as a malware analyst, SOC analyst, or do incident response, then malware analysis is relevant. On the other hand, if you want to work as a pentester, it's less relevant (you won't often use or develop malware during pentest operations).

Regarding the market and this skill, if you want to do only malware analysis and work specifically as a malware analyst, you should keep in mind that it's a very advanced field. It requires deep knowledge, especially about how malware and systems work, but also in cryptography, programming, reverse engineering, and low-level languages like assembly.

I couldn't say for sure if malware analysis at that level is highly in demand — it's often more of a "component" of a broader role (like a SOC analyst or forensic analyst). The best thing to do is check on Indeed or LinkedIn to see if it's in demand in your area.

When it comes to sysadmins, it depends on the size of the company. In small companies, you often have to do a bit of everything, so having malware analysis skills can be useful for incident response (understanding what the malware does, its impact, its goal, etc., in order to eradicate it and make sure it doesn't come back). But in larger companies, an admin usually sticks to admin tasks and will only handle security if there are predefined procedures from the security team.

Thanks Bastille for the info. I mostly found systems administrative jobs in my country of Jamaica. There isn't any specific reference to malware analysis or incident response.

Maybe companies seem to be more invested in preventing the hack rather than investigating it, which makes sense.

Since I'm going mostly into programming, I think malware analysis suits that route. I'm probably going to have to see if I can get opportunities online when the time comes.

StinkButt420 - May 17, 2025, 7:25 am

May 17th, I started early at work. I spun up a VM while I was at work, and tried to work through a HTB "sherlock", the easiest one.

I was interrupted, but considering I'm actively pursuing certificates in the BLUE side of CS, any time looking through logs, and learning about DFIR is time well spent. I also plan to learn something new in Python, what it will be, I do not know. Then I'm gonna finish up a module, and learn something about wireshark. And also grabbing Kali Linux instead of ParrotOS. I like Parrot, but I'm gonna interchange between them and see if I like one more than the other.

The sherlock I worked on involved looking through a log to see when a Bruteforce attempt was

successful, then using a WTMP file to figure out when they started issuing commands from a terminal, what IP it was coming from, what accounts they were creating, etc. It took me a moment to actually figure out the format of the auth.log file, but I figured it out after a closer inspection of the IPs. I was entering the wrong one. (I was entering the destination IP and not the source one LOL)

So yeah, gonna be a good one.

P??sonl?af - May 18, 2025, 4:43 am

(May 17, 2025 02:47 AM)Bastille Wrote: [\[CITE\]](#) Nice buddy ! Do you go with netacad ? Back in the days I remember I was learning and practicing with this platform. You'll definitely enjoy TryHackMe, the basics can be kinda annoying, but when you master them, hacking is reaaaaally cool. But they are vital, most people want to dive straight to hacking but they don't understand what they do, so most of the time they give up.

I've just completed the following room on THM : <https://tryhackme.com/room/volttyphoon> which brought me 450 points as it was a new room (less than a day old). Really really cool room, I've been able to practice on Splunk, it was an incident response simulation and I had to investigate the attack, I've learned few things, I used a write-up for only 1 answer, because I was looking for an encoded powershell command, so I used the basic terms but forgot about the option "-E" to encode.

Streak : 136 ?

Rank : 3373 ?

As I've completed my daily TryHackMe room, now I'll go with some malware analysis for the forum, and then maybe continue my VirusTotal guide for beginner malware analysts

Hope you keep going guys !

Yeah we're learning the basics with Cisco/Netacad for the CCNA certification

On the side I'm also going for the CCST certification, then next on my list is CompTIA Tech+

Since I'm missing the field experience for any related job I want to arm myself with a wide arrange of credentials.

I'm exited to try THM but want to wait a bit more to master the bascis so I don't get overrun & discouraged in the beginning. Like you said, I want to know & understand what i'm doing before I attempt to actually do it.

Bastille - May 18, 2025, 5:18 am

Just completed few easy rooms on THM to keep my streak and my rank in the league.

Yesterday I've completed a malware analysis and provided a thread :

<https://hackforums.net/showthread.php?tid=6298353>

Streak : 137 ?

Rank : 3336 ?

I'll try to make one more malware analysis today, could be nice to publish at least 3 malware analysis per week so people who want to learn could have real-life example

Hope you keep going guys, but it's Sunday so don't forget to rest too !

Bastille - May 19, 2025, 10:59 pm

Didn't post yesterday but I've completed many rooms, just completed this one this morning :
<https://tryhackme.com/room/adbasicenumeration>

I think that I actually love AD pentesting, I'll do more soon. As I worked as a sysadmin I'm familiar with this environment and I had no idea how easy it was to compromise an AD. I've hardened some over the years but looks like it was not enough haha

Streak : 139 ?

Rank : 3174 ?

EDIT : Just completed another room about AD exploitation :
<https://tryhackme.com/room/adauthenticatedenumeration>

qwertydiy - May 21, 2025, 1:38 pm

Finally finished exams today: plan to do a lot over the coming weeks like do some web hacking, learn spring boot and go, do some docker, learn sudo in depth (more on that later) and if there is time some kernel development. Also learn Burp Suite Basics today. Hopling to learn repeater

Bastille - May 22, 2025, 2:20 am

(May 21, 2025 01:38 PM)qwertydiy Wrote: [\[CITE\]](#) Finally finished exams today: plan to do a lot over the coming weeks like do some web hacking, learn spring boot and go, do some docker, learn sudo in depth (more on that later) and if there is time some kernel development. Also learn Burp Suite Basics today. Hopling to learn repeater

Hope the exams went well, feel free to share your next achievements regarding the topics you've mentioned !

Didn't do a lot those 2 previous days, I'm busy with IRL stuff, I will be more free this week-end, I saw an Android Analysis room that I really want to complete :
<https://tryhackme.com/room/androidanalysis>

Hope you keep going guys !

Streak : 141 ?

Rank : 3185 ?

P??sonl?af - May 22, 2025, 2:30 am

I've finished CCNA-1 yesterday and started with CCNA-2 today.

Out of CCNA-1 the only thing that doesn't stick is the data-link layer subdivision MAC & LLC. Who does what.

Everything else I'm pretty confident in.

I also did my CCNA-1 theoretical & practical (Logical) exams yesterday. Results below.
Wednesday will be my CCNA-1 practical physical exam.

Happy Learning & Stay Awesome people!

Bastille - May 23, 2025, 5:52 am

(May 22, 2025 02:30 AM)P??sonl?af Wrote: [\[CITE\]](#) I've finished CCNA-1 yesterday and started with CCNA-2 today.

Out of CCNA-1 the only thing that doesn't stick is the data-link layer subdivision MAC & LLC. Who does what.

Everything else I'm pretty confident in.

I also did my CCNA-1 theoretical & practical (Logical) exams yesterday. Results below.
Wednesday will be my CCNA-1 practical physical exam.

Happy Learning & Stay Awesome people!

Nice results ! Wish you good luck for the practical part, keep us updated !

Just completed a new room on THM : <https://tryhackme.com/room/apt28inthesnare> , it was interesting, but don't have a lot about it to say.

Yesterday I've started my SOC-based homelab, I'll continue today, I'll also work on some tutorials for HF, and I should dive into CySA+ studies to pass the exam.

Hope you keep going guys !

Streak : 142 ?

Rank : 3150 ?

qwertydiy - May 24, 2025, 5:46 am

Looked at your thread and some other videos so now I have a long term cyber security roadmap that should last at least till 2026 if not 2027. Done Burp Suite Intruder. I should go to Bug Crowd's Video on it soon. Completed some C and Java. Hopefully, I should do KC7 Solvi Systems too.

Bastille - May 24, 2025, 12:06 pm

I've made this thread yesterday : <https://hackforums.net/showthread.php?tid=6298815>

Completed 2 rooms on TryHackMe

Continued to work on my SOC-based homelab today

It was a good day ?

Streak : 143 ?

Rank : 3136 ?

JHK010 - May 24, 2025, 6:07 pm

nice hack training like it so nicely ! ! !!

Bastille - May 25, 2025, 3:26 am

(May 24, 2025 06:07 PM)JHK010 Wrote: [\[CITE\]](#) nice hack training like it so nicely !!!

Feel free to join us and share your daily achievements, what you've studied, learned, and so on

I've just completed an easy room about DFIR and ethic on THM to keep my streak :

<https://tryhackme.com/room/irphilosophyethics>

I'll spend more time on my SOC-based homelab, and I should devote time to study CySA+

Hope you keep going guys !

Streak : 144 ?

Rank : 3121 ?

Bastille - May 26, 2025, 5:22 am

Didn't sleep well, so it will be a lazy day :

Just completed an easy and quick room to keep my streak : <https://tryhackme.com/room/md2pdf>

I've made this thread <https://hackforums.net/showthread.php?tid=6298988> to wait until I could release the advanced version (work in progress)

I don't think I'll work on my homelab today, work on it yesterday already, Splunk is very interesting but I now understand why people are dedicated to it in companies, there are so many things to setup and adjust.

Streak : 145 ?

Rank : 3125 ?

Now I think I'll take a nap, see you later

EDIT : completed an easy second room to unlock the league :

<https://tryhackme.com/room/neighbour>

Bastille - May 28, 2025, 1:27 am

Just completed the following room on THM : <https://tryhackme.com/room/contiransomwarehgh> really interesting, it was an investigation through Splunk about Conti Ransomware on an Exchange server, but I need to get more familiar with SOC things such as EventIDs and so on. I'll work on flashcards and cheat sheets.

I've worked a lot of my SOC-based homelab yesterday, especially on the Splunk server, I've encountered many issues, I've fixed all of them, and that allowed me to get more familiar with it.

Today, I would like to :

- Continue my advanced VirusTotal guide for HF
- Continue my SOC-based homelab (maybe add more data from my Windows machines, such as with Sysmon, dashboards, and maybe add more machines)

I'll also share my SOC cheat sheets on HF when it's ready

Streak : 147 ?

Rank : 3073 ?

Hope you keep going guys !

P??sonl?af - May 28, 2025, 8:52 am

My CCNA-1 Practical Physical exam today went really well. I remembered all the commands expect 'show cpd n d'

Finished with a 97% score so I'm really happy with that.
Bringing the total of the CCNA-1 exams to 90%

The 3 first theory exams on CCNA-2 are going good as well. I just find that they are going over the commands you need to remember quite fast with not enough exercises imo. Will mostlikely look for more exercises, if anyone knows a good practice site/method that is relevant LMK.

Now I have a long 4 day weekend where I want to progress in Networking Devices and Initial Configuration some more for that CCST

Bastille - May 29, 2025, 3:11 am

(May 28, 2025 08:52 AM)P??sonl?af Wrote: [\[CITE\]](#) My CCNA-1 Practical Physical exam today went really well. I remembered all the commands expect 'show cpd n d'

Finished with a 97% score so I'm really happy with that.
Bringing the total of the CCNA-1 exams to 90%

The 3 first theory exams on CCNA-2 are going good as well. I just find that they are going over the commands you need to remember quite fast with not enough exercises imo. Will mostlikely look for more exercises, if anyone knows a good practice site/method that is relevant LMK.

Now I have a long 4 day weekend where I want to progress in Networking Devices and Initial Configuration some more for that CCST
Congrats man, you're going really fast !

You can practice on your own computer with GNS3 or Cisco Packet Tracer, but I think you already know these (at least the second one). You can use an AI to give you exercises based on the CCNA2 cert. I've went through this for my Security+ exam, I've asked ChatGPT questions the same way they're asked in the certification, it helped me.

P??sonl?af - May 29, 2025, 3:28 am

(May 29, 2025 03:11 AM)Bastille Wrote: [\[CITE\]](#) Congrats man, you're going really fast !

You can practice on your own computer with GNS3 or Cisco Packet Tracer, but I think you already know these (at least the second one). You can use an AI to give you exercises based on the CCNA2 cert. I've went through this for my Security+ exam, I've asked ChatGPT questions the same way they're asked in the certification, it helped me.

Thank you! It's funny as you are not the first one to say I'm going really fast. I don't see/feel it tbh. I'm just going for it on my own pace.

As far as CPT goes. Is there a place where I can find exercises for CCNA-2. I'm sure at the end of the course I will be able to do the practice skill exam over & over. Might just be looking at some different situations/setups/scenario's. Perhaps with some trouble-shooting as well.

Bastille - May 30, 2025, 4:40 am

Just completed the following room (still Splunk-based) :

<https://tryhackme.com/room/newhireoldartifacts>

I'm getting more and more comfortable on how to conduct investigations, how to search and find artifacts, how to use the SPL queries

Streak : 149 ?

Rank : 2981 ? (I'm now under 3.000, was like 12.000 when I started, proof that constancy is important, keep going guys !)

I'll work (play) some on my homelab now, need to tune my Splunk SIEM with alerts rules and dashboards, add some VMs to my lab such as DVWA to check what's going on the SIEM when I'm exploiting vulnerabilities on a website.

Reminder

Hope you keep going guys ! It's been a while since I saw you in this thread last time ...

[SIM-5594896](#) Still playing with RPi ? Did you continue THM ?

[capt_nemo](#) How the German Rank Killer is going ? Still on the podium doing rooms on TryHackMe ? How things are going with your Pentest+ path ?

[padrino](#) Last time you've mentioned that you could change your position, from dev to cybersec, any news ? Let's assume you're too busy with your new role so you have less time for HF haha

[Robert Rouge](#) how health is going since ? Hope you're doing better, did you start your web design project ?

[Chorozon](#) Any update regarding the certs ? Security+ and the others ? It's been a while since you posted last time, feel free to let us know !

[RootRXXT](#) How things are going with cybersecurity ?

[M?tt](#) what's new since you got the GIAC ? Working on new things ? Another cert ? :)

[plops](#) It's been a while man ! Did you continue to study on THM ? Or maybe working on something else since ?

[13parliament37](#) Did you sharpened your JS skills ? New projects you worked on ?

[SIM-5614029](#) Still studying on THM ? Hope you keep going buddy !

[qwertydiy](#) Almost a week since last time we got news from you, feel free to keep us up to date :)

[Thul3a](#) if you ever come back, drop a hello !

[Just4kickz](#) How things are going on THM ? Did you continue buddy ?

[Dystortion](#) did you fix the trouble caused by the water on your computer ?

[TENET](#) it's been around 3 months man, hope to see you around, what's new ? Working on new

things related to antivirus ? :)

[Andy Walker](#) How THM and malware analysis are going since ?

[Miracula](#) New malware are coming soon ? ? Cool projects you're working on ?

[s0lo](#) Did you continue to play with your web servers and honey pots ?

padrino - May 30, 2025, 4:49 am

(May 30, 2025 04:40 AM)Bastille Wrote: [\[CITE\]](#) [padrino](#) Last time you've mentioned that you could change your position, from dev to cybersec, any news ? Let's assume you're too busy with your new role so you have less time for HF haha

No news as of yet - although the company has freed up some funds for me to persue training to make the new role a realty so I'm focussing on that at the moment! I'll be reporting here on any training I get haha - looking to book some thing in the next few months!

Most of my free time recently has been focussed on family and big work projects so it's left little time for study and HF updates at the moment - but I try and log in when I can. I actually really love ths community so I'm trying to be as active as I can. I really need to get back to my free time study though - and not just the stuff I get through work.

How're you getting on man, I see you're making great progress on this thread and have been training like a monster - any new roles/goals on the horizon?

Bastille - May 30, 2025, 4:58 am

(May 30, 2025 04:49 AM)padrino Wrote: [\[CITE\]](#) No news as of yet - although the company has freed up some funds for me to persue training to make the new role a realty so I'm focussing on that at the moment! I'll be reporting here on any training I get haha - looking to book some thing in the next few months!

Most of my free time recently has been focussed on family and big work projects so it's left little time for study and HF updates at the moment - but I try and log in when I can. I actually really love ths community so I'm trying to be as active as I can. I really need to get back to my free time study though - and not just the stuff I get through work.

How're you getting on man, I see you're making great progress on this thread and have been training like a monster - any new roles/goals on the horizon?

I'm glad to hear that things are still looking good for your job change and that your company is supporting you. I understand that things can take time in real life — we grow and take on new responsibilities. You've got your priorities straight, that's great! ;)

Haha, well, I've kept up with my daily training on THM, I passed my Security+ certification two weeks ago, I'm thinking of passing CySA+ now, and I've started setting up a homelab focused on the SOC analyst role to get familiar with the tools, methods, and concepts — and to showcase it during job interviews when I start applying for SOC analyst positions in September, if all goes well (finger-crossed ?)

padrino - May 30, 2025, 5:20 am

(May 30, 2025 04:58 AM)Bastille Wrote: [\[CITE\]](#) I'm glad to hear that things are still looking good for your job change and that your company is supporting you. I understand that things can take time in real life — we grow and take on new responsibilities. You've got your priorities straight, that's great! ;)

Haha, well, I've kept up with my daily training on THM, I passed my Security+ certification two weeks ago, I'm thinking of passing CySA+ now, and I've started setting up a homelab focused on the SOC analyst role to get familiar with the tools, methods, and concepts — and to showcase it during job interviews when I start applying for SOC analyst positions in September, if all goes well (finger-crossed ?)

Man that's awesome! Great commitment. Really hope it goes well for you in september - keep us updated!

M?tt - June 2, 2025, 6:08 pm

Pursuing another cert. It kinda counts, but not really. SSAP which revolves around Security Awareness Plans. Pretty dry stuff, but definitely helpful and informative. Taking the exam next week and wrapping up my paper currently.

Honestly as much as I love school, I can't wait to finish so I can explore on my own. I just don't have the time or bandwidth to do both while in school and balancing work and family. I feel so behind and ahead of others at the same time and it's a weird complex.

Bastille - June 3, 2025, 1:13 am

(Jun 2, 2025 06:08 PM)M?tt Wrote: [\[CITE\]](#) Pursuing another cert. It kinda counts, but not really. SSAP which revolves around Security Awareness Plans. Pretty dry stuff, but definitely helpful and informative. Taking the exam next week and wrapping up my paper currently.

Honestly as much as I love school, I can't wait to finish so I can explore on my own. I just don't have the time or bandwidth to do both while in school and balancing work and family. I feel so behind and ahead of others at the same time and it's a weird complex.

Wish you good luck for your paper and the exam man, and yeah I know what you mean, getting older is not easy to keep on track, I feel that the only reason I can progress is because I'm unemployed and single. And I don't want a wife or kids before I know I'll not progress anymore in my career otherwise it will be too much work

Stanley - June 3, 2025, 1:40 am

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

Bastille - June 3, 2025, 1:47 am

[Bumping my thread to not merge my posts]

Yesterday I've completed few rooms, whose the following about Splunk :

<https://tryhackme.com/room/splunkdatamanipulation>

Really informative, feeling more comfortable with Splunk, I need to apply what I've learned in my SOC-based homelab

Will continue Splunk today, conduct a malware analysis, and work on my homelab

Streak : 152 ?
Rank : 2956 ?

Hope you keep going guys

Bastille - June 5, 2025, 2:46 am

It's been few days, but I've continued to learn, completed few Splunk rooms, just completed the following one : <https://tryhackme.com/room/xss> it's nice to go back to basics sometimes

I've worked on my homelab too, will continue today,

Hope you keep going guys !

Streak : 155 ?
Rank : 2939 ?

P??sonl?af - June 5, 2025, 9:12 am

I can finally say I made an exam that was good enough for my standards! xD

All jokes aside, I'm coming to the end of CCNA2 and do feel like I need more practice on the subject/theory to be fully confident. I've made a PDF with all the CCNA2 exam questions, answers & reasoning and been feeding it to chatgtp to test me. At the moment I've been getting a 85%-88% score each questions but I'd like a bigger buffer before requesting to do my final exam. Tomorrow will be a recap day.

[CCNA2_Final_Exam.pdf](#)

Bastille - June 5, 2025, 9:25 am

(Jun 5, 2025 09:12 AM)P??sonl?af Wrote: [\[CITE\]](#) I can finally say I made an exam that was good enough for my standards! xD

All jokes aside, I'm coming to the end of CCNA2 and do feel like I need more practice on the subject/theory to be fully confident. I've made a PDF with all the CCNA2 exam questions, answers & reasoning and been feeding it to chatgtp to test me. At the moment I've been getting a 85%-88% score each questions but I'd like a bigger buffer before requesting to do my final exam. Tomorrow will be a recap day.

[CCNA2_Final_Exam.pdf](#)

100% man that's crazy haha, wish you good luck for the final exam ! What will be the next steps ?

P??sonl?af - June 5, 2025, 9:40 am

(Jun 5, 2025 09:25 AM)Bastille Wrote: [\[CITE\]](#) 100% man that's crazy haha, wish you good luck for the final exam ! What will be the next steps ?

I'll have to do a small course about windows 11 because well who knows xDDD

After that I should be doing the course windows server.

iGaB1 - June 6, 2025, 11:54 pm

Hi, how are you? Thanks so much for the information, you're a genius, my friend. I'm new to all this and I'm trying to learn.

Bastille - June 7, 2025, 12:46 am

(Jun 6, 2025 11:54 PM)iGaB1 Wrote: [\[CITE\]](#) Hi, how are you? Thanks so much for the information, you're a genius, my friend. I'm new to all this and I'm trying to learn.

Hello, welcome to HF, you're welcome ! If you have any question feel free to ask on the forum but don't forget to provide as much details as possible.

If you're new to hacking / cybersecurity I've made this guide for beginners :

<https://hackforums.net/showthread.php?tid=6263412>

Don't forget to read the [Help Docs](#) too, hope to see you around !

qwertydiy - June 7, 2025, 1:11 pm

Sorry, justy more exams I have been learning recon in bug bounty and nmap. I also completed the data analyst tracks for python, r and sql. going to learn nmap really well (how can I pick up obfuscation?).

Bastille - June 8, 2025, 12:09 am

(Jun 7, 2025 01:11 PM)qwertydiy Wrote: [\[CITE\]](#) Sorry, justy more exams I have been learning recon in bug bounty and nmap. I also completed the data analyst tracks for python, r and sql. going to learn nmap really well (how can I pick up obfuscation?).

Nmap is one of the key tool, definitely a must have, mastering it will give you a great benefit for your bug bounties.

Regarding obfuscation, some techniques are "general" and others are applied to specific languages, for example : you don't obfuscate the same way a PowerShell command and a JavaScript code. What kind of code you want to obfuscate, Python ?

SarahQueen - June 8, 2025, 12:58 pm

Hello everyone, Glad to be here!

Skidsuper - June 9, 2025, 1:20 am

Looking for ways to implement AI in security.

P??sonl?af - June 10, 2025, 6:40 am

I studied all weekend to be able to request the CCNA-2 Final exam (Theory) today. Did some recap this morning to freshen up and went for it.

Tomorrow I'll start the preparations for the skills exams. I want to get the DTP, inter-VLAN routing, Arp inspection, BPDUGuard / portfast & port security commands in my fingers before going for it.

Bastille - June 23, 2025, 2:00 pm

It's been a while since I've posted last time here, I've stopped THm to focus on my homelab I need to finish to be able to present it during job interviews.

Hope you keep going guys !

Andy Walker - July 2, 2025, 8:39 pm

It's been a while. I paid for Tryhackme, so I'm dedicated to getting better. So I downloaded Docker and some other containers and virtual machines to figure out how to use them.

Docker for some reason won't start on my newer Windows maybe I should try a different version.

I want to set up a homelab but I only got two working computers, I got a lot of old laptops but no good batteries for them. I still need more stuff like a switch etc.

But I feel good so far with my progress.

P??sonl?af - July 9, 2025, 4:40 am

In the spirit of keeping Senpei [Bastille](#) alive.

In my graduate (Networking & Cyber Security) adventure I'm currently working on Linux. Had little to no experience with that before so I'm taking a bit slower then when I did CCNA 1 & 2

Did my first mid-term exam yesterday and was pleased with the results. Overall the 90% score is something I want to maintain throughout the program.

Up to the next exam!

Observer - August 3, 2025, 1:54 pm

I've currently started getting into cybersec again.

Subbed to THM, currently doing cybersec 101. Today I learned about SQLi and BurpSuite's Repeater Module.

Also doing bandit from overthewire on the side to get my linux knowledge up.

P??sonl?af - August 7, 2025, 5:03 am

Checking in! Today I was finally able to finish Linux.

Not gonna lie this isn't my cup of tea or something I am (still) feel comfortably in.

The second mid-term was hard. I had to second guess and rethink quite a lot of questions.

Thankfully I was more lucky with the questions on the final exam. With some educated guesses here & there I scored a decent result.

I'm done for today but am quite excited to start my last chapter in CCNA monday!

P??sonl?af - August 14, 2025, 3:00 am

I'm exited to be able to work on my last course for CCNA

2 midterms done & it's going great!

P??sonl?af - September 8, 2025, 4:10 am

This one was for you Senpei [Bastille](#)

CCNA3 done! Next up Window Serv.

Will start the study for the whole CCNA cert & book an appointment asap.

Lowkey - September 8, 2025, 4:13 am

Not a hacker anymore but checking in because I love you papa.

Bastille - September 13, 2025, 12:47 am

(Aug 3, 2025 01:54 PM)Observer Wrote: [\[CITE\]](#) I've currently started getting into cybersec again. Subbed to THM, currently doing cybersec 101. Today I learned about SQLi and BurpSuite's Repeater Module.

Also doing bandit from overthewire on the side to get my linux knowledge up.

Welcome onboard buddy, I'm into cybersec too, if you need something or just want to talk, feel free :)

THM is definitely the best platform to start learning I think, and overthewire is really good to get more comfortable with the basics used with Linux and Hacking

(Sep 8, 2025 04:10 AM)P??sonl?af Wrote: [\[CITE\]](#) This one was for you Senpei [Bastille](#)

CCNA3 done! Next up Window Serv.

Will start the study for the whole CCNA cert & book an appointment asap.

Hey buddy, thanks for keeping this thread alive, I'm really glade to see that you keep going :)

You were a cook chief, now you seem good to become a cybersecurity chief ?

Wish you good luck for the next ones, I'll probably be more active on HF again. Seeing you continuing kinda motivates me

(Sep 8, 2025 04:13 AM)Lowkey Wrote: [\[CITE\]](#) Not a hacker anymore but checking in because I love you papa.

We'll always be hackers at heart, no matter what happens ? love you too son

ttbr0 - September 13, 2025, 2:28 pm

today i started looking into obfuscation and deobfuscation theory. i have always been interested virtualization for years so i was reading into it more seriously about how they work. i started with vmprotect since it was the most common that i have seen in terms of samples and literature.

Andy Walker - October 27, 2025, 10:15 am

Hey guys. Still studying Windows registry and how to get past password and UAC controls on my system. I gotten better at Python, so some basic stuff that confused me don't confuse me as much.

I can look at other people's code and actually understand what's it's trying to do. It's probably going to take more practice to write complex code like that myself. Anyways, happy October.

Observer - October 27, 2025, 11:25 am

(Sep 13, 2025 12:47 AM)Bastille Wrote: [\[CITE\]](#) Welcome onboard buddy, I'm into cybersec too, if you need something or just want to talk, feel free :)

THM is definitely the best platform to start learning I think, and overthewire is really good to get more comfortable with the basics used with Linux and Hacking

STP to OSPF killed my soul a little bit so i fell back a bit on studying but im getting back into it. Do you think i should parallel do CTFs on THM in the meanwhile?

Work and CCNA study is rough lol

Money- - December 14, 2025, 7:44 pm

Yo long time no see. How's everyone here? Any progress in the cyber world?

alaraghinaoi - December 18, 2025, 7:04 pm

Nice one.

I shall look to learn more.

Bastille - December 19, 2025, 5:30 pm

(Dec 14, 2025 08:44 PM)Money- Wrote: [\[CITE\]](#) Yo long time no see. How's everyone here? Any progress in the cyber world?

Still learning. Even if I'm not active on HF anymore, I'm still dedicated to computing, until AI kills it.

Hope you're doing well, man. Thanks for keeping this thread alive for a brief moment.

P??sonl?af - February 4, 2026, 10:17 am

Hey hey,

Been a while since I posted here but I've been busy.

I'm up to 16 certifications atm and reaching the final stage of my OJL.

There is a real chance I'll be offered to stay at the company so we're hoping for the best.

The last 2 certifications I have achieved are
CyberOps Associate & Junior Cybersecurity Analyst

4ynow - February 4, 2026, 10:52 am

(Jan 3, 2025 06:11 AM)Bastille Wrote: [\[CITE\]](#)
2025 Day counter

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158

[/align]

1. PRESENTATION

For many, starting a new year means setting resolutions to achieve their goals. Beyond fitness and health, I want to invite those who are interested—and who sometimes lack a bit of motivation—to join this thread with the following objectives:

- ? Share your daily progress in the field (GitHub contributions, rooms on TryHackMe, etc.).
- ? Exchange ideas and get inspired by others to explore new things and see how others study/practice.
- ? Discuss common or interesting topics.
- ? Share your knowledge with others.

- ? Celebrate your achievements (it's important to feel proud and boost your ego).

2. THE LEARNING PYRAMID

For those who don't know, we retain information differently depending on how we learn. Here's the pyramid:

- ? Passive Reading : 10%
- ? Audio / Visual : 20%
- ? Demonstration : 30%
- ? Group Discussion : 50%
- ? Practice by doing : 75%
- ? Teach Others : 90%?

It's important to practice, but you can even go further by teaching to others in this thread what you did, improve your learning retention rate !

3. SOURCES TO PRACTICE

In my thread : <https://hackforums.net/showthread.php?tid=6263412> I shared many platforms where you can learn for free, I'm joining the list below to give you some ideas :

[If you begin, and you don't want to spend money, I highly recommend you to start with TryHackMe, then you can decide to spend more.]

- o [OverTheWire](#) (interesting if you begin, especially to get comfortable with Linux)
- o [TryHackMe](#) (the one I recommend if you begin)
- o [HackTheBox](#) (more advanced than TryHackMe, you can go on it after being familiar with cybersecurity)
- o [Root-Me](#) (general)
- o [Cryptohack \[url\]](#) (for learning modern cryptography)
- o [VulnHub \[url\]](#) (downloadable vulnerable virtual machines)
- o [TCM Security](#) (from CyberMentorChief mentioned earlier from YouTube's learning section)
- o [Let's Defend](#) (more oriented blue team)
- o [Cyber Defenders](#) (more oriented blue team)

4. HALL OF FAME / LEADERBOARD

I want to implement a leaderboard on this post based on the activity of the participants, let me know what do you think about it. Feel free to share any of useful metrics such as :

Profile

Yearly activity

In your daily post you're free to share :

- Links to rooms you've completed

- Badges you earned
- Streaks
- Contributions
- and any other thing that could be relevant !

I wish you all a good luck, a productive year, do the necessary to achieve your goals and become who you want to be.
thanks

Pr0m3th3us - *May 21, 2026, 5:19 pm*

Started back up again on HTB. Gonna finish the OS fundamentals hopefully within in a couple days.