

Forum:[Hack Forums](#)

Thread: [Beginner Guide to Hacking](#)

PurpleMoss - April 13, 2023, 2:14 am

I've known about this forum for many many years but only decided to become a member recently. In the short time I've been here I've seen this section flooded in the same silly 'I want to be a hacker, teach me' type posts.

Being completely new to something is completely fine and asking more knowledgeable people is part of learning, but most of the time these people haven't done any learning at all before asking. Rather than saying the same thing over and over again, I've decided to make a small thread with the information needed for someone to get started in this industry. Hacking and Cyber Security are very broad terms so the below is going to be relating to Penetration Testing. So here goes:

A Few Notes Before We Start:

Before we start, lets just go over a few things that you need to consider if you want to get into this world.

Hacking is not something you'll learn in a few hours to 'hack into your gfs account' or 'hack someone who made you cry on Discord'.

Hacking takes years to learn, years to master and a constant hunger for improvement.

Hacking requires you to actually look for things. If you've come on here stating you want to learn hacking but can't find any information, then this isn't the industry for you. No one feeds you the location of the vulnerabilities, it's your job to hunt for them and find them.

No you can't just 'hack Facebook' or 'hack Snapchat'. A lot of infrastructure/web applications are built of pre-existing frameworks that can be fairly secure. Websites like Facebook and Snapchat have built up their defences over the years, you aren't going to be able to 'hack' them after watching a YouTube video. Someone may get lucky and find a 0 day exploit but unlikely by the average person. Social engineering is now something that is used with almost every attack. Look into some of the biggest hacks performed recently in the real world, most of them involve some sort of social engineering.

Despite what anyone tells you, I'm afraid there is no magic button or program that you can use to hack anything you want, sad I know.

The Different Hats

It seems that on this forum, people love talking about the different hat colours, not really something I've experienced much discussion about elsewhere. Essentially they are all the same, you are performing the same actions, doing the same things, it's what you do after that determines what 'hat colour' you are, basically it's based on your morals.

White Hat (Legal if all paperwork is correct) - Finds security issues/vulnerabilities in a system and reports them to the owner/developers for them to fix. This is done with written permission and the scope of the test verified. This type of action does tend to have more options within, such as:

White Box Testing Approach - Full access is given to the testers, credentials, source code, applications etc and a full check is done.

Grey Box Testing Approach - Some access is given, for example a website with admin credentials

into the admin panel.

Black Box Testing Approach - You are given nothing other than a URL or IP addresses.

Grey Hat (Illegal) - Finds security issues/vulnerabilities in a system and reports them to the owner/developers for them to fix. This is done without written permission. This method is still illegal, regardless if your intention is to tell the owner/developers of the issues. With this type of action, you typically work under a 'Black Box' approach.

Black Hat (Illegal) - Finds security issues/vulnerabilities in a system and uses them for their own benefit. This is done without written permission. This could include things like selling the access you have obtained, stealing sensitive information, financial gains etc.

Learning

In order to try to break into something, first you must learn how it works. You need to spend time learning how websites work, how browsers retrieve the website you are requesting, how DNS works. You also need to learn how networks work, how a company's infrastructure works. Below are some of the resources that can help:

Learn about networks - Jason Dion's CompTIA Network+ (N10-007) Full Course on Udemy (warez disallowed)

Learn how websites/web servers work - No one in particular, search 'How do web servers work' on YouTube

Learn how anything else works - Use the method above

Learn how to pen test websites - Look into zSecurity's courses online

Learn about WiFi networks - Look into zSecurity's courses online

Learn about external infrastructure pen tests, along with Linux/Windows priv esc - Look into TheCyberMentor's courses online

The above should get you started but you can never have too many resources for learning. I found the above very helpful when I started years ago but their teaching methods may not be your style. There are plenty of other instructors out there, you just need to look for them.

There are other things that you should also learn along the way such as Linux (not necessarily Kali) and a language such as Python.

Python Basics - 100 days of code: Completely Python course by Dr. Angela Yu from Udemy (warez disallowed)

Python Pen Testing Tools - Look at zSecurity's Python course or TheCyberMentors Python course, but I'd suggest learning the basics first

Linux - Various YouTube searches and mainly just install Linux and look up commands as you go

I would also advice against using Kali, mainly because you won't actually learn how to use Linux properly. Kali is just a Debian based Linux distro that has been tailored to have penetration testing tools on it pre-installed. If you really want to learn how to use Linux, install Ubuntu as a VM and create your 'own version of Kali'. Install the tools that you need when you need them, customise it as you please. You'll encounter lots of errors along the way, but Google as the answer for most errors and you'll learn a huge amount from doing that.

Practice Areas

The three main ones that I would consider are TryHackMe, HackTheBox, and Portswigger Academy.

If you want to learn web application pen testing, Portswigger Academy is the way forwards, completely free and very helpful.

If you are new to it all and want to learn a bit of everything, TryHackMe is very beginner friendly.

If you are more advanced and like 'game style' practice then HackTheBox is your go to.

Do I Need To Know How To Code?

The answer is yes and no. Do we need to be able to code to the same level as a developer? No. I would recommend learning one language fairly well, such as Python. Python is a very easy beginner language and it'll teach you the structure of coding, such as functions, loops, if statements, OOP etc. Once you understand all this, picking up other languages won't be as hard.

I'd also suggest learning a bit of everything, again, you don't need to be able to code anything complex, but you need (at the very least) to be able to understand what the code is doing when you see it. Learning HTML, JS, PHP, very basic C, Python will help you in your career.

So being able to read through code is fine, but don't get hung up on the fact that you need to be a developer level coder.

If I Can't Code, Does That Make Me A Skid?

Absolutely not! We all have different skills and abilities, if someone trustworthy has made a program that we have a use for, what's the point in writing a program that already exists and works? If it works well and does what we need, make the most of it and use it! What makes someone a 'skid' is when they use a program with no knowledge of what it is doing or how it works.

Using a pre-made program doesn't make you a skid if you understand what it is doing, if you can look through the code (open source) and understand what's happening behind the scenes, even to a basic level.

Let's look at an example, a car manufacturer is making a new petrol engine car, they have designed the body but they have used the engine from another manufacturer because it's an established, stable, and reliable engine. This is quite common in the motor industry and doesn't make the manufacturer any less credible. The thing to consider is that whilst they are using another manufactured engine, the techs understand how that engine works, and have probably made slight modifications to it. It's very rare they just grab an engine and dump it in their car with no alterations and no knowledge of it's internal workings.

So aimlessly using pre-made programs with no understanding of how they work makes you a 'skid'. Using pre-made programs that you've understood, researched, even modified doesn't make you a 'skid'.

I Can't Remember It All, Is That Bad?

Not at all, and it's very common. The average person can't be expected to remember everything they learn, specially if they don't use it that much. The important thing is to understand it and know about it. Don't try to remember everything, it won't work and you'll just exhaust yourself trying. There is a huge amount of things you need to learn to be successful at this. Even if you want to focus on web application pen testing, you still need to learn some social engineering, some networking/infrastructure methods, some programming languages, some tools on Linux.

What's important is the fact you know what can be done, and where to find out more about it. For example, if I wanted to try to practice hacking a WiFi network, I can't remember the exact commands needed to do each and every step, but I know that most of what will be needed is the Aircrack-ng suite, so I'd bring up the guide for that and look through what commands I need.

Another example is if I'm writing something in Python and wanted to use flags as a user's input, I can't remember the exact structure and syntax for doing that, but I know I can use the argparse library so I'd get the documentation up for that.

When Will I Know Enough?

You won't, this is one of those industries where you'll never know enough and will always be learning. I self studied for 2 years and have been working as a full time employed pen tester for another 2 years. I'm still learning, there's still things I don't know and if I'm honest, still things I don't understand.

The information I've given you above, along with the learning material should keep you occupied for at least a year.

My inbox and Discord (PurpleMoss#0801) is always open to people needing help or advice, but please at least look into the basics on your own first.

fredfuchs - April 13, 2023, 4:38 pm

Why on earth does this post lack any good comments?! Well done on the amazing and detailed write up OP. I love it.

PurpleMoss - April 13, 2023, 4:57 pm

(Apr 13, 2023 04:38 PM)fredfuchs Wrote: [\[CITE\]](#) Why on earth does this post lack any good comments?! Well done on the amazing and detailed write up OP. I love it.

Thank you. Hopefully it helps some people out ?

dirtyjohn9283 - April 14, 2023, 4:46 am

Thank you for the information, can I contact you on discord and ask a few questions about certs?

PurpleMoss - April 14, 2023, 4:53 am

(Apr 14, 2023 04:46 AM)dirtyjohn9283 Wrote: [\[CITE\]](#) Thank you for the information, can I contact you on discord and ask a few questions about certs?

Feel free to. My Discord is at the bottom of the thread.

RetiredTrash - April 14, 2023, 10:04 pm

Comprehensive post. Appreciate such good knowledge as a beginner myself.

ALEDIO - April 15, 2023, 10:12 am

I really appreciate this thread, from now on when I am forced to answer the usual questions of new members I will redirect them here. Congratulations on the quality of the post, it contains the answer to the existential questions of every person who comes here to ask.

continentbender - April 15, 2023, 10:55 am

This is a good thread for beginners could use a section for reverse engineering as well

ice13 - April 15, 2023, 11:24 am

Really nice and encouraging thread good job!

RiskLimit - April 16, 2023, 3:19 am

Great guide, definitely helpful for beginners.

> Do I Need To Know How To Code?

Well I'd say you do need to know the fundamentals of Python so you can manipulate requests and automate tasks, or write certain scripts, exploits. You would also need C or C++ if you want to write some sort of malware to infect a server or a target machine. However you can just get one of those tools on Github, but I'd suggest knowing and understanding how they work if you'll use them

PurpleMoss - April 16, 2023, 4:20 am

(Apr 16, 2023 03:19 AM)RiskLimit Wrote: [CITE](#) Great guide, definitely helpful for beginners.

> Do I Need To Know How To Code?

Well I'd say you do need to know the fundamentals of Python so you can manipulate requests and automate tasks, or write certain scripts, exploits. You would also need C or C++ if you want to write some sort of malware to infect a server or a target machine. However you can just get one of those tools on Github, but I'd suggest knowing and understanding how they work if you'll use them

Thanks, I did mention in that section that you should learn Python well enough. Thing I'm trying to get across is that you don't need to know how to code like a developer, no one cares if an exploit is messy code, as long as it works. We aren't trying to sell the code.

jzx100 - April 16, 2023, 8:07 am

Many thanks for your support!! I'll think about it because it's my biggest dream and no university in the world teaches you such interesting things!

B3A - April 17, 2023, 7:31 am

Just gone through your posts.

Pretty decent entries for a new-comer.!

Florin Salam - April 17, 2023, 8:40 am

Thanks mate for the good quality of guidance for starters.

BlscIs05 - April 18, 2023, 3:45 pm

Great post. Not only gives a lot of valuable information but also let's beginners know how much time we put into this in order to be successful at it. I think most people that lookup this type of info think it's something that a quick Google search and 30 minute tutorial is all they need. If you don't want to spend the time and do the work then you should probably just move on because its a never ending task where your skills have to evolve as the technology behind software, websites, and app architecture does. You will never know everything.

padrino - April 18, 2023, 3:56 pm

Brilliant post. Really insightful - nice work man.

RolanSan - April 19, 2023, 5:28 am

Thank you for taking the time to type out that guide, very informative

Sloppy Salami Slapper - April 19, 2023, 10:15 am

Thanks op for providing some insight for beginners like me

EDGETheEAGLE - April 25, 2023, 12:40 pm

This is a fantastic post. Thank you for sharing your hindsight and knowledge.

taipan2000 - April 27, 2023, 2:20 am

Incredibly helpful post, and a very interesting and educational read. Thank you!

skorz - April 27, 2023, 8:23 pm

mind if i shoot you a message on disc? wanted to ask a few career related questions.

Fang - April 28, 2023, 4:09 pm

Thanks mate for the good quality of guidance for starters.

Platinum Stargazer - April 29, 2023, 3:31 am

(Apr 13, 2023 04:57 PM)PurpleMoss Wrote: [\[CITE\]](#) Thank you. Hopefully it helps some people out ? Hi mate. Thanks. Only just read through your beginners 101 guide. I will definitely start on learning how networks work, how websites work, how wifi works etc.

I will start on learning Python and about other hacking tools like Metasploit etc too

I dunno which hat i am. Red hat perhaps? I aim to hack to shut down scammers operations, but i am 70% motivated by justice and 30% motivated by revenge. I do this to make the world a better place. I am not motivated by money. But to serve justice to the world

Best
Platinum Star Gazer

PurpleMoss - April 29, 2023, 8:37 am

(Apr 29, 2023 03:31 AM)Platinum Stargazer Wrote: [\[CITE\]](#) Hi mate. Thanks. Only just read through your beginners 101 guide. I will definitely start on learning how networks work, how websites work, how wifi works etc.

I will start on learning Python and about other hacking tools like Metasploit etc too

I dunno which hat i am. Red hat perhaps? I aim to hack to shut down scammers operations, but i am 70% motivated by justice and 30% motivated by revenge. I do this to make the world a better place. I am not motivated by money. But to serve justice to the world

Best
Platinum Star Gazer
I wouldn't worry too much about what colour hat you are ?.

WalleyCoyote - April 29, 2023, 6:40 pm

Sounds great really interested

Glenn - May 4, 2023, 9:45 am

Thanks man good post.

Ishitmypants2 - May 5, 2023, 5:36 am

Thank you so much! Saving this for reference.

prettyboydd - May 5, 2023, 1:35 pm

awesome man thanks for the help

Dread.Reaper - May 5, 2023, 4:24 pm

(Apr 29, 2023 08:37 AM)PurpleMoss Wrote: [\[CITE\]](#) I wouldn't worry too much about what colour hat you are ?.

Cool I was starting to worry about this Khaki beige fishing hat Ive been rocking.

PurpleMoss - May 6, 2023, 1:50 am

(May 5, 2023 04:24 PM)Dread.Reaper Wrote: [\[CITE\]](#) Cool I was starting to worry about this Khaki beige fishing hat Ive been rocking.

That means you're elite!

korai - May 6, 2023, 10:42 am

i think this would be where my question fits. im specially interested in web security, i already know about how computers works(not completely, its very extensive) and ip, networking, i also know javascript, html, and a bit of php, is there anything else i should learn? also were i can learn more about this?

(sorry for any typo, im not english)

PD: very nice guide man, very well explained

Dread.Reaper - May 6, 2023, 12:47 pm

(May 6, 2023 10:42 AM)korai Wrote: [\[CITE\]](#) i think this would be where my question fits. im specially interested in web security, i already know about how computers works(not completely, its very extensive) and ip, networking, i also know javascript, html, and a bit of php, is there anything else i should learn? also were i can learn more about this?

(sorry for any typo, im not english)

PD: very nice guide man, very well explained

You are going to want to take a detailed look into this section: [Pentesting and Forensics](#)

korai - May 6, 2023, 1:27 pm

(May 6, 2023 12:47 PM)Dread.Reaper Wrote: [\[CITE\]](#) You are going to want to take a detailed look into this section: (removed this since i cant post links)

Thanks! I'll check it!

pandaemic - May 9, 2023, 9:41 pm

Hadn't heard of zSecurity until now, thank you and thank you for pointing me in the right directions. The hardest part of learning everything is deciding what to learn first.

Ifyg - May 13, 2023, 12:38 am

You couldnt make this simpler. The way i understand this is that no matter how much you study, practise is always the key.

pistachio7 - May 14, 2023, 7:48 am

Thanks for your post

URCB - May 23, 2023, 9:17 pm

Thanks man. I think it's good starting point.

User#Cry - June 22, 2023, 6:53 am

This is the only advice you need as a beginner. Thanks for the effort you put into writing this wonderful post. I wish I could have found this when I was a beginner.

Monyito666 - June 28, 2023, 12:43 am

Thank you for this OP, very informative for a Skid like me..keep up the good work sir

kissfromarose - August 10, 2023, 5:48 pm

Great post , thanks for the information, really helpful

mnt007 - August 10, 2023, 7:23 pm

Great post.Thansk for good guidance.

johannaheinrich - August 13, 2023, 8:37 am

Thank you bro I will look at this very soon.

DartLipt - August 14, 2023, 8:53 am

Really nice and encouraging thread good job!

nimda - August 24, 2023, 3:31 am

Great read, thanks for the post.

lazymrak - November 24, 2023, 6:34 am

It's wonderful.As a beginner,this gives me a lot,thanks!

nibblenbyte - November 24, 2023, 12:26 pm

This may need to be a sticky for all the "I'm new can someone teach me"/"Can I hack XYZ" posts
haha.

Good 101 write up!

Linda_de_cara - November 25, 2023, 2:17 pm

(Apr 13, 2023 02:14 AM)PurpleMoss Wrote: [\[CITE\]](#) I've known about this forum for many many years but only decided to become a member recently. In the short time I've been here I've seen this section flooded in the same silly 'I want to be a hacker, teach me' type posts.

Being completely new to something is completely fine and asking more knowledgeable people is part of learning, but most of the time these people haven't done any learning at all before asking. Rather than saying the same thing over and over again, I've decided to make a small thread with the information needed for someone to get started in this industry. Hacking and Cyber Security are very broad terms so the below is going to be relating to Penetration Testing. So here goes:

This post it's gold for newbies like me. I will contact you in the future if I need some tips. thank you for your time! ?

YoungLoser - November 25, 2023, 2:24 pm

Only other thing i would add is to start doing the Academy at HackTheBox, and doing live machines as well

dls1234 - November 27, 2023, 1:44 am

Comprehensive post. Appreciate such good knowledge as a beginner myself.

KhoNoan - March 28, 2024, 9:08 am

Hello, i'm new to this forum and pretty sure that this post will help not only me but other people who just started hacking. Tysm and have a good day man.

djyloxser - March 29, 2024, 5:21 pm

I post to follow thanks

TheCoz - March 30, 2024, 9:05 am

This is an awesome post. I will add, I've gone through a lot of python courses and one of the best entry level courses was Python for Everybody, done by Michigan professor Charles Severance. You

can find it on multiple platforms, i think i did it on edX.

890jump - *May 1, 2024, 2:28 pm*

Really appreciate you taking the time out to post this. It's helpful to a newcomer like myself. Down the rabbit hole I now go!