How to Learn Hacking? My Path!

sparsh jazz
Sep 13·10 min read

So you want to Learn Real Hacking.If so, you are in the right place.The Reason why i have written this article is Because a lot of people randomly approach me and i have to spend at least 10 minutes on every person trying to explain them how to learn hacking and giving the some good resources to learn from.If you are serious to learn hacking or perhaps make a carreer in cybersecurity as a hacker/penetration tester,i highly recommend you to read the full article careully.This article about is my personal path.The things i have learnt and the resources that helped me gain knowledge.

SO lets get started.Before you advance any further,i want you to watch this video by a really skilled hacker called live overflow.Half of your questions will be answered by watching it.

> https://www.youtube.com/watch?v=2TofunAI6fU

Now lets get started.I assume you are a beginner and a script kiddie(if you dont know what this word is,use google).Firstly stay curious and clear your very basics about computer hardwares,how os works,basic networking and get yourself familiar with using linux commands.Just clear your very basics.

STEP 1

Now lets start with the real deal.Finish this youtube playlist by Hackersploit.It has 145+ videos in total and this channel is probably the best for beginners.

> https://www.youtube.com/playlist?list=PLBf0hzazHTGOEuhPQSnq-Ej8jRyXxfYvl

If you face any error,use google and youtube.Troubleshoot the problem by yourself.Remember that NO ONE CAN TEACH YOU COMPLETE HACKING.No one will spoon feed you or teach you.Always avoid paying money.Money can never give you knowledge.It is earned by researching,falling into troubles and researching.Most of the hackers are self learned.Take as much time as you want,but clear your concepts and finish the playlist.Research as much as you can.You are your own Mentor.

STEP 2

1]plsstudy the books which is in the oscp folder

3]do bufferover flow

4]do programing tools

2]After finshing this,Try to gain knowledge of the CEH certification.NOTE:avoid buying the ceh certification as it is no longer demanded in the industry.What i want you to do is finish this syllabus of CEH from an institute i had studied in.Research on the topics and practice them.

Chapter 1 — Introduction to Ethical Hacking

What is Hacking
What is Ethical Hacking
Types of Hackers
White Hat Hacker

Black Hat Hackers
Gray Hat Hackers
Script Kiddies
Hacktivists
Spy Hackers
Cyber Terrorists
Vulnerability
Exploit
Remote Exploit
Local Exploit
Zero-day
Zero-day vulnerability
Zero-day Exploit
Brute force attack
Phishing
Remote access
Payload

Chapter 2 — Steps of Ethical Hacking Information Gathering

Active Information Gathering
Passive Information Gathering
Scanning
Gaining Access
Maintaining Access
Covering Tracks

Chapter 3 — Types of Malicious files

Viruses
Worms
Trojan Horse
Spyware

Adware
Backdoor
Rootkits
Ransomware

Chapter 4 — Penetration Testing

What is Penetration Testing
Types of Penetration Testing
What is white box Penetration Testing
What is Black Box Penetration testing
Introduction to Linux OS
Social Engineering

Chapter 5 — Google Hacking Using Dorks Demo
Lab Setup

What is Virtual Machine
What is VMware
What is Virtual Box
Install VMware
Install Parrot OS
Install Windows XP
Install Windows 7
Install Add on in Mozila
Tamper Data
Burp Suite
No-Redirect
Install Nessus

Chapter 6 — System Hacking

System Hacking using Kon-Boot
Network Scanning

Port Scanning
Service Scanning
What is Nmap
Scanning With Nmap
Nmap Various Command

Firewall Bypass Using Nmap(learn in depth)

Chapter 7 — Scanning With Nessus Hacking With Metasploit

What is Metasploit?
Xp Remote Exploit using Metasploit
Msfvenom
Windows7 UAC Bypass

Chapter 8 — What is SE-Toolkit

SE-Toolkit Usages
Create Phishing page with SE-Toolkit
Hacking Facebook & Gmail password

Chapter 9 — What is Remote Administration Tool

What is RAT
Exploit With RAT
Protect System from RAT

Chapter 10 — What is Sniffing

Types of Sniffing
Network Sniffing with Wireshark
Get FTP Login Details Using Wireshark

Chapter 11 — What is DOS

Details of DOS
What is DDOS, Installation and use of Xerxes tool

Chapter 12 — Wireless Network Hacking

Wireless Encryption
Hacking WPA 2

Chapter 13 — Web Application Pen-testing

How Web Application Works
Request and Response
Installing Scanner (Acunetix,Netsparker)
Scanning Website

Chapter 14 — OWASP Top 10

What is Sql-Injection?
Types of Sql-Injection
Live Demo on Sql-Injection

Chapter 15 — What is XSS

Types of XSS
Live Demo on XSS All types

Chapter 16 — What is CSRF

Live Demo On CSRF What is HTML Injection
Live Demo on HTML Injection

Chapter 17 — What is Directory Listing

Live Demo on Directory Listing What is Broken Auth
Live Demo on Broken Auth What is Tamper data?
Live Demo on Tamper Data on Ecommerce site
Session Hijacking

Chapter 18 — What is Phishing?

Create a Phishing Page What is Web Shell
Hack Web-Server Using Web-Shell

Chapter 19 — Hacking Android Phone using Metasploit and FatRat tool

Chapter 20 — Solve full DVWA (full solution on youtube)

— -

IF you have completed STEP 1 and 2(the Hackersploit video playlist and the CEH syllabus given above),Now you have a decent knowledge of what hacking and penetraton testing is and you can explore things on your own.(Bonus:Solve Over the wire Bandit Challenge.Its very easy and fun.)The link below contains solution to the bandit challenge and some bonus videos- https://www.youtube.com/playlist?list=PLBf0hzazHTGMh2fe2MFf3lCgk0rKmS2by

STEP 3

Start SOLVING CTF And Boot to root machines on Vulnhub or HTB.If you want to learn real practical hacking,The time has come.

> https://www.youtube.com/watch?v=Lus7aNf2xDg

Start solving CTF which is the most fun way to learn hacking.It feels like a game.I consider CTF the best resource to learn hacking.Try to start with some easy boxes from Vulnhub(such as metasploitable 2 and mr robot ctf) and move on to some hard ones.In CTF you will be applying all the knowledge you have gained.Personally i spent 3–4 months and solved 15 CTFs from vulnhub.IF you are comfortable with very easy level CTFs,I highly recommend you to solve this list of 17 vulnhub ctfs.It gets harder as you proceed but you will learn something new and unique in every machine.If you get stuck,watch the walkthrough(solution) on youtube or read it on google.

— — — — — — — — — — — — — -

metasploitable2
bulldog
bulldog2
Matrix
Kuya
Matrix2
Android 4
Mercy
Bravery
Development
Goldeneye
Nullbyte
Pinkeys palace v4
Matrix3
Moonraker
Prime 1
Pegasus (reqires buffer overflow knowledge and C)

Note: Solve them one by one and follow the list.Some machines may need Programming/exploit development knowledge and you can skip them but try your best to solve as many as you can.(Watch the walkthrough ONLY when you are stuck for many many hours).This is the best material to learn real hacking.Solve ctf!!! MANY OF THE MACHINES ARE OSCP LIKE.And are hard too but you can get a touch of oscp by solving them and hone up your skills!

Privilege Escalation is a technique tricky to master so i am sharing the BEST resources to learn them.This will prepare your privilige escalation skills beyond OSCP and is considered the best course in the community-

https://github.com/sagishahar/lpeworkshop
https://www.youtube.com/playlist?list=PLjG9EfEtwbvIrGFTx4XctK8IxkUJkAEqP
https://www.udemy.com/course/windows-privilege-escalation/
https://www.udemy.com/course/linux-privilege-escalation/

NOTE:The last 2 udemy courses by Tib3rius is considered THE BEST in the community till date and has helped many hackers crack oscp.If you have money,do buy it if not, you can get it for free in some websites.

————————————————————————

Now you have a pretty good knowledge and can call yourself as a Penetration Tester/Hacker.Follow the further steps to keep getting better.

STEP 4

Solve OTW Natas Web challenges.This will improve you knowledge of web hacking.I highly highly recommend you to go to youtube and watch CHRIS DALE's Solutions on OTW Natas web challenges.The challenges will be tough but feel free to see the solutions by Chris Dale and try to learn the skills.Watch and follow him.Also check out his other videos.He is a Pro Seasoned Hacker for 17 years with insane knowledge in hacking and is one of my role models.

https://www.youtube.com/playlist?list=PLag7W-lJE2Aw8hzezQl17ZlE6CfNS3nYu

—————————————————————————————-

NOTE: if you have done STEP 3 and 4(CTF and NATAS) you will see that you require programming or scripting knowledge.Dont be disheartened now.Its time i break the Truth that Programming is important.A real hacker makes his own tools and knows how to write scripts and exploits.I suggest you to learn C programming.Yes its a bit hard and old but its really good when you will be learning advanced topics like buffer overflow in future.Learn basic C programming.What you should highly focus on is PYTHON.The Language HACKERS USE to write exploits and scripts.

STEP 5

THE TIME HAS COME!….LEARN PYTHON.It might be a bit boring but trust me its VERY important.I learnt python by reading this book called- Beginning python from novice to professional by magnus lie hetland(read it till ch 15) and see the python3 video playlist on youtube by TheNewBoston.Reading documentation helps a lot when you are stuck in python. https://www.youtube.com/playlist?list=PL6gx4Cwl9DGAcbMi1sH6oAMk4JHw91mC_

After learning python, finish a book like BlackHat python or Violent python or Greyhat python which will teach you how real hackers leverage python for offensive hacking by writing your scripts and tools so you will no longer be a script kiddie.This will take time but will take you to the next level!

(Bonus: Now you can try solving the OTW Natas challenge using python now.Go to JOHN HAMMOND's youtube channel.He has solved the full challenge using python- https://www.youtube.com/playlist?list=PL1H1sBF1VAKWM3wMCn6H5Ql6OrgIivt2V)

John Hammond is the go to guy for CTF and Python and is a pro at it.

STEP 6

Learn Android and IOS Penetration testing.The market is full of developers making android and ios apps and a lot of projects you will recieve as a hacker/pen tester in a company will involve android and ios application and frameworks.Read android hackers handbook and ios hackers handbook as a learning resource.

WHAT NOW?

Now you can do as you wish.Try solving the TJ Null Playlist on youtube which contains OSCP like machines from HTB.Maybe start perparing for OSCP(This is the most demanded and tough exam in the field of hacking.It is the recommended certfication to enter the industry.)The playlist below contains 37 Oscp like HTB machines which every oscp uses as a training ground.Infact the practice machines you will get in pwk labs are pretty similar to it.Ippsec has solved every machine and explained you every possible to Root the machines in great details.HTB membership is paid but its a bang for buck!

- https://www.youtube.com/playlist?list=PLidcsTyj9JXK-fnabFLVEvHinQ14Jy5tf

NOTE:If you had completed The Privilige Escalation courses mentioned in STEP 3, it will be of HUGE help when solving HTB OSCP like machines from ippsec.

MOVING ON…

You should learn REVERSE ENGINEERING.Yes its a tough topic but its a really important one.Read the book “Secrets of Reverse Engeneering” and follow Live overflow on youtube who is a pro in binary exploitation and IOT hacking. Learn topics like Exploit Development OR Malware analysis or IOT hacking or Forensics or Rootkit Analysis.Feel Free to expriment.Maybe Learn web hacking using “web application hackers handbook” and “Portswigger labs” and try doing Bug bounties on platforms like Hackerone,Integriti and bugcrowd.

Hacking is all about learning new things and solving challenges.There are a ton of topics to learn.Its a Journey where you keep learning and meeting new people.Having errors,problems and questions is the part of learning.Hopefully the people in infosec community are very helpful and you learn a lot by talking to them.You can even find a mentor who can guide you and help you out if you face a common problem.Although it has to be you who has to do the work.People can teach you a part or a topic but you have to be your own mentor and teach it to yourself.

ALWAYS REMEMBER THESE THINGS-

Age,race,nationality,educational background doesnt matter in this field.What matters is your hunger and dedecation to learn new things.

Don’t run after money or certs.Run after knowledge.If you have knowledge,cybersecurity is a highly rewarding field.

Avoid people selling courses or asking for money.Everything in free.Avoid buying paid udemy courses or joining institutes.Self Learn is the key.A 4 or 12 hour udemy video can never teach you hacking.

Talking to people is the best secret to get more knowledge.Talk to as many cybersecurity professionals and ethical hackers as you can.You can find the on youtube,linkedin,slack,discord…

There is no x y z path to learn hacking.Every hacker has his own unique path.You learn it by doing it!Just keep learning.

Share Knowledge to those who are dedecated and never charge a single penny for it!

There is no secret forum to learn hacking on Deepweb.You learn it by reading books,blogs,researching,solving CTFs and doing real life projects.

Remember to take breaks.You are human and take care of your body and mind.Dont get BURNOUT take rest and go at your own pace.There is no hurry.IT TAKES TIME.(took me around 1.5 years to finish till STAGE 5).Take your time and enjoy learning everyday.

Stay curious and dedecated and be hungry for knowledge.I have given you a lot of valuable information.Goodluck!!!

HELPFUL YOUTUBE CHANNELS-

Hackersploit(learn from this as a beginner)
Live overflow (advanced)
Dc Cybersec, AskNatoRiley (Great Cybersecurity advise)
Null byte, jsonsec
The cybermentor, , Computerphile
Ippsec, John Hammond (great for ctf)
Stok, XssRat, nahmsec Chris Dale (Great for web and bug bounty)
Crypto the llama, zeus cybersec(MY OWN CHANNEL)

SOME AMAZING BOOKS-(These are some of the most famous and best books every hacker has!)

Penetration testing by georgia weidman(1st book u must read), Hacking the art of exploitation, web applications hackers handbook, The hackers playbook 2 and 3 ,Tribe of Hackers (EASY BOOKS)

Blackhat Python,Serious cryptography, practical malware analysis,shellcoders handbook, secrets of reverse engineering, The Art of Memory Forensics(ADVANCED BOOKS)

————————————

CONCLUSION

If you have come this far,my time and effort has not been in vain.Thank you for reading my article.I am no expert and a learner myself.Wishing you luck on your cybersecurity journey and i would like to thank everyone in the community that has helped me just like i am helping you today .I would always be greatful to my mentor Strike Rider for guiding me and helping me throughout my journey.