MHT HACKERS EMPOWER HACKERS

MYHACKERTECH.COM

CONTACT INFORMATION

@MyHackerTech
E. sales@myhackertech.com

Want to become an ethical hacker and secure systems and networks?

This checklist covers key steps and resources to start ethical hacking.

ETHICAL HACKING: ESSENTIAL STEPS AND RESOURCES

>_BASICS
>_TECHNIQUES
>_PRACTICE
>_MASTER TOOLS
>_EXPERIENCE
>_SMALL BOARD COMPUTERS
>_COMMUNITY
>_ETHICAL
>_UPDATE
>_CERTIFICATION

UNDERSTAND THE BASICS

STEPS

- **Computer Fundamentals:** Familiarize yourself with computer hardware, software, and operating systems.
- **Networking Basics:** Learn about TCP/IP, network protocols, and how data flows over the internet.
- **Learn Microsoft Windows -** Love it or hate it, it is the core of business computing worldwide. You need to learn desktop and server versions. Learn how to use Windows 11 as a user. Then delve into Windows Server. Learn Active Directory - how Windows creates users and the security it uses behind the scenes. Learn how file sharing and networking works. Learn about the different network services that are available in Windows and how to use them.
- **Learn Linux -** On the contrary many internet systems use a flavor of Linux. Pick one and begin learning. Ubuntu is a good place to start. Linux mint is perfect to start if you are used to using Windows. You will find it very familiar. After you are familiar with using it as a user, begin to learn how to create users, and file sharing, then learn network services, setup simple file sharing, then setup internet-based network services.

RESOURCES

Windows 11 All-in-One For Dummies, 2nd Edition
https://www.amazon.com/Windows-All-One-Dummies-2nd-dp-1394276885/dp/1394276885
Linux for Dummies, book -
https://www.amazon.com/Linux-All-One-Dummies-Richard/dp/1119901928
How to get started with Linux: A beginner's guide -
https://www.pcworld.com/article/427298/how-to-get-started-with-linux-a-beginners-guide.html

BASICS_ _ _ _ _ _

STUDY ETHICAL HACKING TECHNIQUES

STEPS

- Begin to learn Ethical Hacking using a platform like **Kali Linux** or **ParrotOS**. Kali is geared more for professional Pentesting use and Parrot is geared more for a security user. Try both and see which you like more. Once you become proficient, build your own! You can add the tools you want to **Ubuntu** or **PiOS**, or build your own Kali even. But it is good to start with a generic platform like Kali Linux or ParrotOS when starting.
- **Ethical Hacking Courses:** Enroll in online courses or attend in-person classes to learn the fundamentals of ethical hacking.
- **Books:** Read books like "Hacking: The Art of Exploitation" by Jon Erickson and "Metasploit: The Penetration Tester's Guide" by David Kennedy. ”Basic Security Testing with Kali Linux, 4th Edition” & ”Advanced Security Testing with Kali Linux” by Daniel W. Dieterle.
- **Online Tutorials:** Explore websites like Hack The Box, TryHackMe, and OverTheWire for hands-on practice.
- **Operating Systems:** Gain expertise in Linux and Windows, which are commonly targeted by hackers. Learn how to create and add users, and shares.
- **Programming Languages:** Learn Python, a versatile language used for scripting and automation. C/C++ is good to know for Windows targets. Also, web application languages like Javascript and PHP. Golang is also growing in popularity.
- **Cybersecurity Fundamentals:** Study concepts like encryption, authentication, and security models.

RESOURCES

MyHackerTech Courses -
https://myhackertech.com/pages/ethical-hacking-courses-and-tutorials
Udemy: Ethical Hacking courses by various instructors.
Coursera: Ethical Hacking Specialization.
Offensive Security: Certified Ethical Hacker (CEH) training.
ParrotOS - https://parrotsec.org/
Kali Linux - https://kali.org

TECHNIQUES__

HANDS-ON PRACTICE

STEPS

- The best way to learn is hands on! Getting theory and knowledge is good, but the only way to really learn security is to do it! Setup a safe lab using **Virtual Machines** in **VMWare** or **Virtualbox**. Learn **WiFi Pentesting** and client based attacks. Learn about password cracking. Learn about USB based attacks like **BadUSB**.
- Check out tutorial YouTube channels like **WebPwnized**. The YouTube author walks you through many hacking techniques and software tools. **Capture the Flag** type websites will also help you learn new techniques and try them out. If you get stuck you can always find good walkthroughs of the CTF you are working on.
- **Create a Lab:** Set up a safe, isolated environment for practice. Use virtual machines, such as **VirtualBox** or **VMware**, to simulate networks and systems.
- **Capture the Flag (CTF) Challenges:** Participate in CTF challenges to test your skills. Websites like Hack The Box and CTFTime offer various challenges for all skill levels.

RESOURCES

Basic Security Testing with Kali Linux, 4th Edition - https://www.amazon.com/Basic-Security-Testing-Linux-Fourth/dp/B0C47PXVDJ
Penetration Testing: A Hands-On Introduction to Hacking - https://www.amazon.com/Penetration-Testing-Hands-Introduction-Hacking/dp/1593275641
WebPwnized - https://www.youtube.com/@webpwnized/videos
Hack The Box - CTFs - https://www.hackthebox.com/hacker/ctf
CTFTime - https://ctftime.org
VirtualBox - https://www.virtualbox.org/wiki/Downloads
VMware - https://support.broadcom.com/group/ecx/downloads

PRACTICE___

MASTER TOOLS AND TECHNIQUES

STEPS

- After you have the basics down good, it’s time to dig deeper. Begin to learn **WebApp Pentesting** and **Active Directory (AD)** testing.
- These techniques are a little more involved, but you can do it! Begin to learn how webapp Pentesting works, looking for vulnerabilities like the **OWASP Top 10**. These usually require a much deeper understanding of Linux and how webapp software and programming languages works. You will learn things like **SQL injection, Broken Access controls and forgery attacks**.
- **Active Directory** testing is definitely a more advanced topic, but so rewarding when you get it. Learn how to map out AD and how misconfigured settings in users and accounts could let an attacker move from user to user until they get Domain Admin control.
- A lot of the more advanced security certifications include AD testing and WebApp testing training.
- Also, learning documentation and report writing skills are imperative.
- **Penetration Testing Tools:** Familiarize yourself with tools like **Wireshark**, **Nmap, Burp Suite, and Metasploit.**
- **Vulnerability Scanning:** Learn how to identify and exploit vulnerabilities in systems and applications. Apps like **Nessus, Qualys, Rapid7** and many more.

RESOURCES

Metasploit The Penetration Tester’s Guide
https://www.amazon.com/Metasploit-2nd-David-Kennedy-dp-1718502982/dp/1718502982
Advanced Security Testing with Kali Linux -
https://www.amazon.com/Advanced-Security-Testing-Kali-Linux/dp/B09RPTFK1S
Wireshark - https://www.wireshark.org/download.html
NMAP - https://nmap.org/download
Burp Suite - https://portswigger.net/burp/communitydownload
Metasploit - https://www.metasploit.com/download
OWASP Top Ten - https://owasp.org/www-project-top-ten/

TOOLS______

GAIN PRACTICAL EXPERIENCE

STEPS

- It wouldn't hurt to start your career in IT Support. How better to learn basic windows, Linux, network usage and troubleshooting than to do it! From there increase your networking knowledge - learn about **routers** and **switches** and **VLANs**. **Cisco** has many great classes to learn and increase these skills. Move to server support, again, seeing how users and security are handled in a real environment is great experience.
- Also, learning how basic server problems are corrected will give you experience that will come in handy in the security field. Many people jump from **IT Support** into basic security defense positions, many times in the same company. Once you have solid security defense skills, jumping to **Red Team** is a natural progression.
- **Internships or Freelancing:** Seek internships or freelance opportunities to gain real-world experience in ethical hacking.

RESOURCES

Operator Handbook -
https://www.amazon.com/Operator-Handbook-Team-OSINT-Reference/dp/B085RR67H5/
Blue Team Handbook: Incident Response Edition -
https://www.amazon.com/Blue-Team-Handbook-condensed-Responder/dp/1500734756/
Red Team Field Manual -
https://www.amazon.com/RTFM-Red-Team-Field-Manual/dp/1075091837/
Blue Team Field Manual -
https://www.amazon.com/Blue-Team-Field-Manual-BTFM/dp/154101636X/
Red Team Development and Operations -
https://www.amazon.com/Red-Team-Development-Operations-practical/dp/B083XVG633/
Cisco Courses - https://www.netacad.com/

EXPERIENCE__

SMALL BOARD COMPUTERS (SBC)

STEPS

- **Learn the use of small board computers that are used in hacking.** SBC's are used by both attackers and Red Teams. **Pentest dropboxes**, **wardriving** and **warflying**, and a lot of WiFi attacks/ testing is now down using SBCs. **Drones** are also becoming a hot go to hacking platform for red teams.
- Learn how to use Hak5 devices, Proxmark3, Raspberry Pi based devices, ESP32 devices and **Flipper Zeros**
- **Hak5, Proxmark3, Raspberry Pi based devices** and custom hardware attack devices are used in every Red Team test. Knowing how to use them will increase your value as a Red Team operator.

RESOURCES

Security Testing with Raspberry Pi, Second Addition - https://www.amazon.com/Security-Testing-Raspberry-Pi-Second/dp/B0BHL323C5
Tactical Wireless Security - https://www.amazon.com/Tactical-Wireless-Security-Daniel-Dieterle/dp/B0DR65GG5V
FlipperZero - https://flipperzero.one/
Hak5 - https://shop.hak5.org/
Raspberry Pi - https://www.raspberrypi.com/
Proxmark3 - https://proxmark.com/proxmark-3-hardware/proxmark-3
MyHackerTech Courses - Raspberry Pi Course Chapter
https://myhackertech.com/pages/ethical-hacking-courses-and-tutorials

SBC

JOIN THE ETHICAL HACKING COMMUNITY

STEPS

- **Forums and Communities:** Join online forums like Reddit's r/AskNetsec and communities like HackerOne and Bugcrowd.
- **Networking:** Connect with fellow ethical hackers and cybersecurity professionals through LinkedIn, Social Media (Instagram, X, Mastodon, Threads) and local meetups.

ETHICAL AND LEGAL CONSIDERATIONS

STEPS

- **Compliance:** Familiarize yourself with laws and regulations surrounding cybersecurity and ethical hacking in your region.
- The General Data Protection Regulation (GDPR)
- The Health Insurance Portability and Accountability Act (HIPAA)
- The Payment Card Industry Data Security Standard (PCI DSS)
- **Ethical Guidelines:** Always adhere to ethical standards and avoid any unauthorized or malicious activities.

RESOURCES

MyHackerTech - https://linktr.ee/myhackertech
Cyberv1k1ng - https://linktr.ee/danieldieterle
AskNetsec on Reddit - https://www.reddit.com/r/AskNetsec/
HackerOne - https://www.hackerone.com/
Bugcrowd - https://www.bugcrowd.com/
GDPR - https://gdpr-info.eu/
HIPAA - https://www.hhs.gov/hipaa/for-professionals/index.html

COMMUNITY___

STAY UPDATED

STEPS

- **Follow Security News:** Stay informed about the latest cybersecurity threats and trends by following websites, blogs, and news sources like **KrebsOnSecurity** and **Threatpost**.
- **Conferences and Webinars:** Attend cybersecurity conferences and webinars to network and learn from experts in the field, DEFCOn, BSides, Black Hat
- **Cybersecurity** is a rapidly evolving field. Commit to lifelong learning to stay relevant.

CERTIFICATION

STEPS

- **Cybersecurity Certifications:** Consider certifications like CompTIA Security+, Certified Information Systems Security Professional (CISSP), or Certified Ethical Hacker (CEH).
- **Consider advanced certifications** like Offensive Security Certified Professional (OSCP) or Certified Information Security Manager (CISM) to enhance your career prospects.

RESOURCES

KrebsOnSecurity - https://krebsonsecurity.com
Threatpost - https://threatpost.com
Black Hat Conference - https://www.blackhat.com
OffSec Certification - https://www.offsec.com/courses-and-certifications/
CEH - https://www.eccouncil.org/train-certify/certified-ethical-hacker-ceh/

UPDATE_____