3 Year Cybersecurity Roadmap

How to get started with a career in Cybersecurity in <=3 years

Why?

- Lack of a structured approach to learning core concepts and the fundamentals required to operate successfully in the Cybersecurity industry.
- It can be daunting to find a starting point.
- Demonstrate the importance of discipline and setting goals.
- Demystify Cybersecurity as a career.

Target Audience

- High school and college/university students interested in getting into the Cybersecurity field.
- Technology Professionals looking to pivot into Cybersecurity.
- Cybersecurity professionals looking to identify knowledge gaps and level up their skills.
- Anyone looking to get started in Cybersecurity.

Year 1

Y1 - Operating Systems

Windows

- Learn how to install, configure and administer Windows.
- Learn how Windows works and the various components that make up the operating system.
- Learn how to secure and harden Windows.
  - CIS Benchmarks.
- Get an understanding of how Windows passwords are hashes and stored.
- Become comfortable with the Windows command line.
- Learn how to setup and configure and Active Directory environment.

Y1 - Operating Systems

Linux

- Learn how to install, configure and administer Linux.
- Learn how Linux works and the various components that make up the operating system.
- Learn how to secure and harden Linux.
  - CIS Benchmarks.
- Become comfortable with the terminal.
- Learn how to install and utilize various Linux distributions.
- Vim, sed, awk and regex!
- Please learn Git…

Y1 - Scripting

Scripting

- Learn how to utilize PowerShell and write PS scripts.
- Learn how to automate tasks on Linux by leveraging shell scripts.
- Python! – Start simple and move on to developing what interests you.

Y1 - Networking

- Understand the OSI model and the various layers that make up the model.
- Get an understanding of how TCP/IP and UDP works.
- Understand the common ports used by various services.
- Learn how common protocols like HTTP, SSH, FTP, SMB etc work.
- Learn how to analyze traffic, more specifically, how to analyze packets with tools like TCPDump and Wireshark.
- Get some gear (routers, switches etc) and setup your own home network!
- Learn how firewalls work. (Pfsense)

Y1 – Security Fundamentals

- Security Concepts
  - Attacks, threats, vulnerabilities, risk etc.
  - CIA Triad
  - GRC
  - Infosec Terminology
- Security Standards
  - CIS
  - NIST

Year 2

Y2 – Pentesting Methodologies & Frameworks

- PTES (Penetration Testing Execution Standard)
- MITRE ATT&CK
- Cyber Kill Chain
- OWASP Top 10
- OWASP Security Testing Guide

Understand the industry standard methodologies used for pentests.

Analyze open source pentesting reports.

Y2 – Home Lab

- Virtualization
  - VirtualBox
  - VMWare
- DevOps
  - Docker & Kubernetes
- Setup your own hacking lab.
  - Kali/Parrot Box.
  - VH Boxes – Get your hands dirty with some basic CTF challenges.

Y2 – Pentesting Fundamentals

- Kali Linux Essentials – Kali Linux Revealed.
- Netcat, SOCAT etc.
- File transfers with Linux & Windows.
- Passive Information Gathering & OSINT.
- Active Information Gathering
- Network & Port Scanning.
- Enumeration.
- Vulnerability Scanning.

Y2 – Exploitation & Post-Exploitation

- Exploitation & Post-Exploitation Frameworks - Metasploit, PowerShell-Empire.
- Searching for and modifying exploits.
- Client-side attacks.
- Buffer Overflows.
- Windows & Linux Exploitation (Services & CVEs).
- Post-Exploitation Techniques.
- Privilege Escalation.
- Password cracking.

Y2 – Practice Like Hell!

- CTFs – participate in older and current CTFs.
- Research – Videos, books, blogs and writeups.
- Practice on platforms like HTB, THM etc.
  - Identify your weak spots and level up!
- Write your own pentesting reports for the CTF/boxes you pwn.
- Start your own blog/channel.
- Document and keep notes. (Build a personal knowledge base)

Y2 – Web App Pentesting & Bug Bounties

- Pwn vulnerable web apps.
- Develop your own web app.
- Watch everything from Jason Haddix & Nahamsec.
- Web proxies (OWASP ZAP & Burp Suite).
- Recon!
- OWASP Top 10
- Get started with Bug Bounties.
- Read reports and blogs.

Year 3

Y3 – Pentesting & Red Teaming

- AV & EDR Evasion.
- AD Penetration Testing.
- Red Teaming TTPs.
- Port Forwarding & Pivoting.
- C2 Frameworks.
- Phishing & Initial Access TTPs.
- Resource Development.

Y3 – Adversary Emulation

- Adversary Emulation.
- Analyze APT/Threat Group Ops.
- Learn how to use EDRs and SIEMs to detect your attacks and understand the defender's perspective.
- Manually & Automatically emulate APTs/Threat Groups.

Y3 – Reverse Engineering

- Assembly – x86 & x64 (oh yeah!)
- C, C++ & C#.
- Binary Exploitation.
- Debugging (IDA, Immunity, GDB)

Thank You

CYBERSECURITY TRAINING SIMPLIFIED

HACKERSPLOIT.ORG // HACKERSPLOIT.ACADEMY

$HACKERSPLOIT_