PRESENTS

Roadmap for Cyber becoming a

Successful Security Engineer

Roadmap for Beginners

Following is the roadmap to learning **Security Engineer** skills for a total beginner. It includes FREE learning resources for technical skills (or tool skills) and soft (or core) skills

Prerequisites: You must have skills or interests to build skills in Coding . Without these two you cannot become an **Security Engineer .**

Total Duration: **3 Months** (**3 hours** of study Every Day) Also,

Week 1: Introduction to Cybersecurity

- Learn what cybersecurity is, why it's important, and the different career paths in cybersecurity.
- Understand common threats such as phishing, malware, and social engineering.

Week 2-3: Networking Basics

- Learn the basics of networking, including IP addresses, subnets, and protocols like TCP/IP and HTTP.
- Understand the OSI model, DNS, and how data flows across networks.

Week 4: Linux Fundamentals

- Learn Linux, as it is the most commonly used operating system for cybersecurity professionals.
- Get familiar with the command line, file management, and basic Linux tools.

Week 5-6: Windows Security

- Understand Windows architecture and the security features available in the Windows operating system.
- Learn about Active Directory, Group Policy, and Windows Defender.

Week 7: Introduction to Cryptography

- Learn the basics of cryptography, including symmetric and asymmetric encryption.
- Understand key concepts like hashing, digital signatures, and SSL/TLS.

Week 8-9: Network Security

- Learn about firewalls, VPNs, IDS/IPS, and network segmentation.
- Understand how to secure networks from external threats and monitor for suspicious activity.

Week 10: Web Application Security

- Understand common web vulnerabilities like SQL injection, XSS, and CSRF.
- Learn how attackers exploit these vulnerabilities and how to protect against them.

Week 11-12: Ethical Hacking and Penetration Testing

- Learn the steps of penetration testing, including reconnaissance, scanning, exploitation, and reporting.
- Understand how to use tools like Nmap, Metasploit, and Burp Suite for penetration testing.

Week 13: Wireshark for Network Analysis
- Learn how to use Wireshark to capture and analyze network traffic.
- Understand how to identify anomalies and suspicious activity.

Week 14: Vulnerability Assessment and Management
- Learn how to identify vulnerabilities in systems using tools like Nessus or OpenVAS.
- Understand vulnerability scanning and how to prioritize patching.

Week 15-16: Incident Response and Forensics
- Learn about the steps of incident response, including preparation, detection, containment, eradication, and recovery.
- Understand digital forensics basics, including acquiring and analyzing evidence.

Week 17: Social Engineering and Human Factors
- Understand social engineering tactics like phishing, baiting, and pretexting.
- Learn how to educate users and prevent social engineering attacks.

Week 18: Security Tools and Automation
- Learn about common security tools like SIEM (Security Information and Event Management).
- Get familiar with scripting languages (like Python) to automate security tasks.

Week 19: Compliance and Governance
- Learn about data protection regulations such as GDPR and compliance standards like ISO 27001.
- Understand why compliance and policy are critical to cybersecurity.

Week 20: Practice with Capture the Flag (CTF) Challenges
- Test your skills with CTF challenges, which provide practical experience in cybersecurity scenarios.
- Participate in platforms like TryHackMe, Hack The Box, or PicoCTF.

General Resources:

Resources for practice

tryhackme - https://tryhackme.com/

hackthebox - https://www.hackthebox.com/

owaspjuicebox - https://demo.owasp-juice.shop/#/

burpsuite - https://portswigger.net/web-security

Youtube video for learning

ippsec - https://www.youtube.com/@ippsec

johnhammod - https://www.youtube.com/@_JohnHammond

networkchuck - https://www.youtube.com/@NetworkChuck

liveoverflow - https://www.youtube.com/@LiveOverflow

lowlevel - https://www.youtube.com/@LowLevel-TV

Online tools for cyber security

cyberchef - https://cyberchef.org

dcode - https://www.dcode.fr

crackstation - https://crackstation.net/

Capture the Flag (CTF):

Capture the Flag (CTF) challenges and bug bounties are great opportunities to enhance your cybersecurity skills. CTF competitions involve solving a variety of challenges, like cryptography, forensics, and web exploitation, to find hidden "flags." Bug bounties involve finding and reporting security vulnerabilities in software or websites, often earning rewards. Participating in CTFs and bug bounties regularly helps improve problem-solving abilities, gain hands-on experience, and explore different aspects of cybersecurity. It’s important to explore various domains rather than sticking to one, and platforms like P2P Hub provide a range of opportunities to gain experience across multiple cybersecurity areas.