



Elite Cyber Security Career Roadmap 2026

CYBER SECURITY MASTERY ROADMAP 2026

If you wish to build a professional career in cybersecurity, here is a complete, step-by-step roadmap. Designed by the 'Cyber Police' brand, this guide will show you the entire path—from starting from scratch to becoming an advanced cybersecurity specialist. Cybersecurity is a field where skills and continuous learning matter most; this roadmap is divided into levels ranging from basic to advanced, enabling you to learn in a systematic manner.

Phase 1: IT & Networking Fundamentals

Strengthen your IT and networking fundamentals; before diving into cybersecurity, you need to understand how computers and networks operate. Jumping straight into learning hacking tools is a major mistake. Networking Basics: Understand the OSI Model, TCP/IP, IP Addressing (IPv4/IPv6), Subnetting, DNS, DHCP, and how routers and switches function. Operating Systems: Gain in-depth knowledge of Linux (Ubuntu, Kali Linux) and master the Command Line Interface (CLI); also, learn Windows administration. Hardware & Virtualization: Learn to set up your own lab using VMware or VirtualBox.

CompTIA Network+

CompTIA A+

Linux Essentials

Phase 2: Security Basics & Programming

Core Security Concepts and Automation: In this phase, you will learn fundamental security concepts and how to automate them using programming. Security Fundamentals: CIA Triad (Confidentiality, Integrity, Availability) and Cryptography (Hashing, Encryption, Symmetric vs. Asymmetric keys). Programming: Learn the Python programming language to write security scripts; basic Bash scripting is also essential. Web Application Basics: Understand the fundamentals of HTML, CSS, JavaScript, and databases (SQL) to comprehend web-based attacks.

CompTIA Security+

Python Essentials



Elite Cyber Security Career Roadmap 2026

Phase 3: Ethical Hacking & Defensive Security

Penetration Testing and Core Skills: This is where you begin to learn about actual security assessment and offensive/defensive methodology. Ethical Hacking: Information Gathering, Vulnerability Assessment, System Hacking, Wi-Fi Hacking, and Social Engineering. Tools Mastery: Practical use of industry-standard tools like Nmap, Burp Suite, Metasploit, Wireshark, and John the Ripper. Web Application Security: Learn how to find and fix OWASP Top 10 vulnerabilities (SQL Injection, XSS, CSRF, IDOR). Defensive Basics: How to use Firewalls, IDS/IPS, and basic log analysis. CEH (Certified Ethical

CEH (Certified Ethical Hacker)

eJPT

CompTIA PenTest+

Cyber Wing Tip: Don't just focus on theory. Solve real hands-on labs by practicing on platforms like TryHackMe and Hack The Box.

Phase 4: Specialization & Advanced Levels

Choose your path (Offensive vs Defensive) You must become an expert in one of the core domains of cyber security: Red Teaming / Offensive: Penetration Testing, Bug Bounty, Exploit Development, Privilege Escalation. Blue Teaming / Defensive: SOC (Security Operations Center) Analyst, Incident Response, Digital Forensics, Threat Hunting. Cloud Security: Learn how to secure AWS, Azure, or Google Cloud security architectures.

OSCP (Offensive Security Certified Professional)

CISSP

BTL1 (Blue Team Level 1)

Important Tips for Success: Build a Portfolio: Build Your Personal

- **Build a portfolio:** Showcase your personal projects, write-ups, and GitHub repositories. Stay active on LinkedIn and join cybersecurity communities.
- **Stay Updated:** The cyber threat landscape changes daily. Read security blogs (such as The Hacker News and BleepingComputer) and stay updated on new vulnerabilities.
- **Ethics & Legality:** Always operate within legal frameworks and permissions. Fully comply with cyber laws and ethics.