Cyber Security: Complete Learning Guide

1. Background of Cyber Security

Cyber security emerged as computer networks expanded in the 1980s and 1990s. Early security focused on basic access control and antivirus protection.

With the rise of the internet, cloud computing, and digital transformation, cyber threats evolved into sophisticated attacks such as ransomware, phishing, and advanced persistent threats (APT).

2. Core Domains of Cyber Security

Network Security: Firewalls, IDS/IPS, VPNs.

Application Security: Secure coding, vulnerability scanning.

Cloud Security: IAM, encryption, compliance.

Security Operations (SOC): Incident response and monitoring.

Governance, Risk & Compliance (GRC).

3. How to Learn Cyber Security

Step 1: Master networking and Linux fundamentals.

Step 2: Understand common attack types and vulnerabilities.

Step 3: Practice in labs (TryHackMe, Hack The Box).

Step 4: Learn security tools and scanning techniques.

Step 5: Study security frameworks (NIST, ISO 27001).

Step 6: Practice incident response and threat analysis.

4. Skill Levels

Beginner: Basic security concepts and tools.

Intermediate: Vulnerability assessment, SIEM, firewall configuration.

Advanced: Penetration testing, red/blue team operations.

Architect: Enterprise security design and zero-trust architecture.

5. Certifications

CompTIA Security+.

CEH (Certified Ethical Hacker).

CISSP (Certified Information Systems Security Professional).

CISM / CISA.

Cloud Security Certifications (AWS, Azure, GCP).

6. Tools for Learning and Practice

Network Tools: Wireshark, Nmap.

Penetration Testing: Metasploit, Burp Suite.

SIEM: Splunk, ELK Stack.

Cloud Security: IAM tools, security scanners.

Operating Systems: Kali Linux.

Conclusion

Cyber security is critical for protecting digital infrastructure. Mastery requires technical foundations, hands-on labs, and continuous learning.