Ultimate Guide to Cyber Security: Beginner to Pro

# Introduction to Cyber Security

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access...

Example Command/Syntax:

nmap -A 192.168.1.0/24

--------------------------------------------------

# Cyber Threat Landscape

Types of threats: Malware, Phishing, Ransomware, Insider Threats, APTs...

Example Command/Syntax:

nmap -A 192.168.1.0/24

--------------------------------------------------

# Network Security Fundamentals

Network Components: Routers, Switches, Firewalls. Security Mechanisms: IDS/IPS, VPN, NAC...

Example Command/Syntax:

nmap -A 192.168.1.0/24

--------------------------------------------------

# System Security

Operating System Hardening: Disable unnecessary services, Apply patches regularly...

Example Command/Syntax:

nmap -A 192.168.1.0/24

--------------------------------------------------

# Web Application Security

Common Vulnerabilities (OWASP Top 10): Injection, Broken Authentication, Sensitive Data Exposure...

Example Command/Syntax:

nmap -A 192.168.1.0/24

--------------------------------------------------

# Cloud Security

Key Concepts: Shared Responsibility Model, Data Encryption, Identity and Access Management (IAM)...

Example Command/Syntax:

nmap -A 192.168.1.0/24

--------------------------------------------------

# Cryptography

Encryption Methods: Symmetric (AES), Asymmetric (RSA)...

Example Command/Syntax:

nmap -A 192.168.1.0/24

--------------------------------------------------

# Penetration Testing

Phases: Planning and Reconnaissance, Scanning, Gaining Access, Maintaining Access, Analysis...

Example Command/Syntax:

nmap -A 192.168.1.0/24

--------------------------------------------------

# Malware Analysis

Types of Malware: Virus, Worm, Trojan, Spyware...

Example Command/Syntax:

nmap -A 192.168.1.0/24

--------------------------------------------------

# Digital Forensics

Phases: Identification, Preservation, Analysis, Documentation, Presentation...

Example Command/Syntax:

nmap -A 192.168.1.0/24

--------------------------------------------------

# Security Operations Center (SOC)

Functions: Continuous Monitoring, Incident Response, Threat Intelligence...

Example Command/Syntax:

nmap -A 192.168.1.0/24

--------------------------------------------------

# Governance, Risk, and Compliance (GRC)

Frameworks: ISO 27001, NIST, GDPR...

Example Command/Syntax:

nmap -A 192.168.1.0/24

--------------------------------------------------

# Important Cyber Security Tools

Tools: Wireshark, Nmap, Burp Suite, Nikto, Hydra, Metasploit, sqlmap, Aircrack-ng, John the Ripper, OpenVAS...

Example Command/Syntax:

nmap -A 192.168.1.0/24

--------------------------------------------------

# Interview Preparation

Top Questions: Difference between IDS and IPS, Explain SSL/TLS, How does a VPN work...

Example Command/Syntax:

nmap -A 192.168.1.0/24

--------------------------------------------------

# Final Notes

Cyber security is a vast and evolving field. Practical labs, certifications like CEH, CISSP, OSCP help to advance...

Example Command/Syntax:

nmap -A 192.168.1.0/24

--------------------------------------------------