# Table of Contents

Introduction to Cyber Security

Cyber Threat Landscape

Network Security Fundamentals

System Security

Web Application Security

Cloud Security

Cryptography

Penetration Testing

Malware Analysis

Digital Forensics

Security Operations Center (SOC)

Governance, Risk, and Compliance (GRC)

Important Cyber Security Tools

Interview Preparation

Final Notes

# Introduction to Cyber Security

Cyber Security is the discipline dedicated to protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Effective cybersecurity measures are particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

Cybersecurity domains include information security, network security, application security, operational security, disaster recovery, and end-user education.

Examples of real-world attacks include the WannaCry ransomware attack and the Equifax data breach.

Security can be enforced by implementing multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe.

# Cyber Threat Landscape

The cyber threat landscape refers to the dynamic and evolving nature of threats that exist in the digital world.

Common Threats:

- Malware: Viruses, worms, Trojans, ransomware, and spyware.

- Phishing: Social engineering tactics to trick individuals into revealing sensitive information.

- Man-in-the-Middle (MitM) Attacks: Intercepting communications between two parties.

- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks: Overloading systems with traffic to cause failures.

Emerging Threats:

- IoT vulnerabilities: Smart devices often lack robust security.

- AI-powered attacks: Using machine learning to automate sophisticated cyber attacks.

# Network Security Fundamentals

Network security protects the integrity, confidentiality, and accessibility of computer networks and data.

Key Components:

- Firewalls: Act as barriers between trusted and untrusted networks.

- Intrusion Detection and Prevention Systems (IDPS): Detect and prevent attacks.

- VPNs: Secure remote access to networks.

- Network Access Control (NAC): Enforces security policies on devices accessing the network.

# System Security

System security ensures that individual devices (desktops, laptops, mobile devices) are protected.

- Hardening the system: Minimizing vulnerabilities by disabling unnecessary services, applying patches, and configuring securely.

- Antivirus and Anti-malware software.

- Secure configurations and baseline settings.

- Mobile device management (MDM) systems to secure mobile environments.

# Web Application Security

Web application security focuses on websites and online services against different security threats that exploit vulnerabilities in an application's code.

Common Attacks:

- Cross-Site Scripting (XSS)

- SQL Injection

- Cross-Site Request Forgery (CSRF)

Best Practices:

- Secure Coding Standards

- Regular Code Reviews

- Application Security Testing

# Cloud Security

Cloud security involves the technologies and processes that protect cloud computing environments.

Considerations include:

- Data security (encryption and backup)

- Identity and access management (IAM)

- Compliance with regulations (e.g., GDPR, HIPAA)

- Vendor security assessments

- Logging and monitoring

# Cryptography

Cryptography is the practice and study of techniques for securing communication and data from adversaries.

Types:

- Symmetric Key Cryptography

- Asymmetric Key Cryptography

- Hash Functions

Applications:

- SSL/TLS encryption for web traffic

- Data encryption at rest and in transit

- Digital signatures for verification

# Penetration Testing

Penetration testing simulates cyberattacks against systems to discover exploitable vulnerabilities.

Stages:

- Reconnaissance

- Scanning

- Gaining Access

- Maintaining Access

- Analysis and Reporting

Tools:

- Metasploit

- Burp Suite

- Nmap

- Nessus

# Malware Analysis

Malware analysis involves examining malicious software to understand its origin, functionality, and potential impact.

Techniques:

- Static Analysis: Analyzing the code without running it.

- Dynamic Analysis: Executing malware in a safe environment to observe behavior.

- Hybrid Analysis: Combining static and dynamic methods.

# Digital Forensics

Digital forensics is the process of uncovering and interpreting electronic data.

Phases:

- Identification

- Preservation

- Analysis

- Documentation

- Presentation

Tools:

- Autopsy

- FTK

- EnCase

- Volatility (Memory Forensics)

# Security Operations Center (SOC)

SOC is a centralized function employing people, processes, and technology to continuously monitor and improve an organization’s security posture.

Key Functions:

- Threat Detection

- Incident Response

- Compliance Monitoring

- Risk Assessment

# Governance, Risk, and Compliance (GRC)

GRC is the umbrella term covering an organization's approach to governance, risk management, and compliance with regulations.

- Governance: Aligning security with business goals.

- Risk Management: Identifying, assessing, and mitigating risks.

- Compliance: Adhering to laws, regulations, and internal policies.

# Important Cyber Security Tools

A strong cybersecurity toolkit includes:

- Wireshark (Network Traffic Analysis)

- Nmap (Port Scanning)

- Nessus (Vulnerability Scanning)

- Burp Suite (Web Security Testing)

- Splunk (Security Information and Event Management - SIEM)

- OSSEC (Host-based Intrusion Detection)

# Interview Preparation

Preparation Strategies:

- Master Networking fundamentals.

- Understand Operating Systems (Linux and Windows).

- Hands-on with security tools (Wireshark, Nmap, Metasploit).

- Study common attack methods and defenses.

- Certifications: CompTIA Security+, CEH, CISSP, OSCP.

# Final Notes

Becoming proficient in cybersecurity is a journey that requires continuous learning, hands-on practice, and adapting to an ever-evolving threat landscape.

Networking, community involvement (conferences, online forums), and consistent skill upgrades are vital.