HURBAD
Institute of Technology

CompTIA

Security+ 01

Attacks, Threats, and Vulnerabilities

STUDY PLAN

MAALINKA 1AAD

INFORMATION SECURITY ROLES

1. Information Security
2. Cybersecurity Framework
3. Information Security Competencies
4. Information Security Roles and Responsibilities
5. Information Security Business Units
6. Questions 01: Security Roles and Security Controls

MAALINKA 2AAD

SECURITY CONTROL AND FRAMEWORK TYPES

1. Security Control Categories
2. Security Control Functional Types
3. NIST Cybersecurity Framework
4. ISO and Cloud Frameworks
5. Benchmarks and Secure Configuration Guides
6. Regulations, Standards, and Legislation

MAALINKA 3AAD

THREAT ACTOR TYPES AND ATTACK VECTORS

1. Vulnerability, Threat, and Risk
2. Attributes of Threat Actors
3. Hackers, Script Kiddies, and Hacktivists
4. State Actors and Advanced Persistent Threats
5. Criminal Syndicates and Competitors
6. Insider Threat Actors

7. Attack Surface and Vectors
8. Question 02: Threat Actors and Threat Intelligence

MAALINKA 4AAD

THREAT INTELLIGENCE SOURCES

1. Threat Research Sources
2. Threat Intelligence Providers
3. TTPs and Indicators of Compromise
4. Threat Data Feeds
5. Artificial Intelligence and Predictive Analysis

MAALINKA 5AAD

BUILD CYBERSECURITY LAB

1. Building Cybersecurity Lab
2. VMware Workstation Pro – Download, Install, and Configure
3. DC1 – Installing Windows Server 2016
4. DC1 – Installing DC and DNS
5. MS1 – Installing Windows Server 2016
6. DC1 – Install Certification Authority (CA)
7. MS1 – Installing and Configure DHCP
8. MS1 – Installing and Configure IIS Server
9. LP1 – Graphical User Interface of Kali Linux
10. LP1 – Kali Linux Terminal
11. LP1 – Basics Linux Commands
12. LX1 – Download and Install CentOS
13. PT1 – Download and Install Kali Linux
14. RT1-LOCAL, RT2-ISP, RT3-INT VMs – VyOS Linux

MAALINKA 6AAD

NETWORK RECONNAISSANCE TOOLS

1. Ipconfig, ping, and arp
2. Route and traceroute
3. Use nmap to discover hosts
4. Netstat and nslookup
5. Reconnaissance and Discovery Tools
6. Packet Capture and tcpdump
7. Packet Analysis and Wireshark
8. Packet Injection and Replay
9. Exploitation Frameworks

MAALINKA 7AAD

GENERAL VULNERABILITY TYPES

1. Software Vulnerabilities and Patch Management
2. Zero-day and Legacy Platform Vulnerabilities
3. Weak Host Configurations
4. Weak Network Configurations
5. Impacts from Vulnerabilities
6. Third-Party Risks

MAALINKA 8AAD

VULNERABILITY SCANNING TECHNIQUES

1. Security Assessment Frameworks
2. Vulnerability Scan Types

3. Common Vulnerabilities and Exposures
4. Intrusive versus Non-intrusive Scanning
5. Credentialed versus Non-credentialed Scanning
6. False Positives, False Negatives, and Log Review
7. Configuration Review
8. Threat Hunting

MAALINKA 9AAD

PENETRATION TESTING CONCEPTS

1. Penetration Testing
2. Rules of Engagement
3. Exercise Team Types
4. Passive and Active Reconnaissance
5. Pen Test Attack Life Cycle

MAALINKA 10AAD

SOCIAL ENGINEERING TECHNIQUES

1. Social Engineering
2. Social Engineering Principles
3. Impersonation and Trust
4. Dumpster Diving and Tailgating
5. Identity Fraud and Invoice Scams
6. Phishing, Whaling, and Vishing
7. Spam, Hoaxes, and Prepending
8. Pharming and Credential Harvesting
9. Influence Campaigns

MAALINKA 11AAD

MALWARE-BASED ATTACKS

1. Malware Classification
2. Computer Viruses
3. Computer Worms and Fileless Malware
4. Spyware, Adware, and Keyloggers
5. Backdoors and Remote Access Trojans
6. Rootkits
7. Ransomware, Crypto-Malware, and Logic Bombs
8. Malware Indicators
9. Process Analysis