EC-Council

CND Exam Blueprint v2.0

Domains	Objectives	Weightage	Number of Questions
1. Computer Network and Defense Fundamentals	• Understanding computer network • Describing OSI and TCP/IP network Models • Comparing OSI and TCP/IP network Models • Understanding different types of networks • Describing various network topologies • Understanding various network components • Explaining various protocols in TCP/IP protocol stack • Explaining IP addressing concept • Understanding Computer Network Defense(CND) • Describing fundamental CND attributes • Describing CND elements • Describing CND process and Approaches	5%	5
2. Network Security Threats, Vulnerabilities, and Attacks	• Understanding threat, attack, and vulnerability • Discussing network security concerns • Reasons behind network security concerns • Effect of network security breach on business continuity • Understanding different types of network threats • Understanding different types of network security vulnerabilities • Understanding different types of network attacks • Describing various network attacks	5%	5
3. Network Security Controls, Protocols, and Devices	• Understanding fundamental elements of network security • Explaining network access control mechanism • Understanding different types of access controls • Explaining network Authentication, Authorization and Auditing (AAA) mechanism • Explaining network data encryption mechanism • Describing Public Key Infrastructure (PKI) • Describing various network security protocols • Describing various network security devices	8%	8
4. Network Security Policy Design and Implementation	• Understanding security policy • Need of security policies • Describing the hierarchy of security policy • Describing the characteristics of a good security policy • Describing typical content of security policy • Understanding policy statement • Describing steps for creating and implementing security policy • Designing of security policy • Implementation of security policy • Describing various types of security policy • Designing of various security policies • Discussing various information security related standards, laws and acts	6%	6

5. Physical Security	• Understanding physical security • Need of physical security • Factors affecting physical security • Describing various physical security controls • Understanding choosing Fire Fighting Systems • Describing various access control authentication techniques • Understanding workplace security • Understanding personnel security • Describing Environmental Controls • Importance of physical security awareness and training	6%	6
6. Host Security	• Understanding host security • Understanding need of securing individual hosts • Understanding threats specific to hosts • Identifying paths to host threats • Purpose of host before assessment • Describing host security baselining • Describing OS security baselining • Understanding and describing security requirements for different types of servers • Understanding security requirements for hardening of routers • Understanding security requirements for hardening of switches • Understanding data security at rest, motion and use • Understanding virtualization security	7%	7
7. Secure Firewall Configuration and Management	• Understanding firewalls • Understanding firewall security concerns • Describing various firewall technologies • Describing firewall topologies • Appropriate selection of firewall topologies • Designing and configuring firewall ruleset • Implementation of firewall policies • Explaining the deployment and implementation of firewall • Factors to considers before purchasing any firewall solution • Describing the configuring, testing and deploying of firewalls • Describing the managing, maintaining, administrating firewall implementation • Understanding firewall logging • Measures for avoiding firewall evasion • Understanding firewall security best practices	8%	8

8. Secure IDS Configuration and Management	• Understanding different types of intrusions and their indications • Understanding IDPS • Importance of implementing IDPS • Describing role of IDPS in network defense • Describing functions, components, and working of IDPS • Explaining various types of IDS implementation • Describing staged deployment of NIDS and HIDS • Describing fine-tuning of IDS by minimizing false positive and false negative rate • Discussing characteristics of good IDS implementation • Discussing common IDS implementation mistakes and their remedies • Explaining various types of IPS implementation • Discussing requirements for selecting appropriate IDSP product • Technologies complementing IDS functionality	8%	8
9. Secure VPN Configuration and Management	• Understanding Virtual Private Network (VPN) and its working • Importance of establishing VPN • Describing various VPN components • Describing implementation of VPN concentrators and its functions • Explaining different types of VPN technologies • Discussing components for selecting appropriate VPN technology • Explaining core functions of VPN • Explaining various topologies for implementation of VPN • Discussing various VPN security concerns • Discussing various security implications for to ensure VPN security and performance	6%	6
10. Wireless Network Defense	• Understanding wireless network • Discussing various wireless standards • Describing various wireless network topologies • Describing possible use of wireless networks • Explaining various wireless network components • Explaining wireless encryption (WEP, WPA,WPA2) technologies • Describing various authentication methods for wireless networks • Discussing various types of threats on wireless networks • Creation of inventory for wireless network components • Appropriate placement of wireless AP • Appropriate placement of wireless antenna • Monitoring of wireless network traffic • Detection and locating of rogue access points • Prevention of wireless network from RF interference • Describing various security implications for wireless network	6%	6

11. Network Traffic Monitoring and Analysis	• Understanding network traffic monitoring • Importance of network traffic monitoring • Discussing techniques used for network monitoring and analysis • Appropriate position for network monitoring • Connection of network monitoring system with managed switch • Understanding network traffic signatures • Baselining for normal traffic • Disusing the various categories of suspicious traffic signatures • Various techniques for attack signature analysis • Understanding Wireshark components, working and features • Demonstrating the use of various Wireshark filters • Demonstrating the monitoring LAN traffic against policy violation • Demonstrating the security monitoring of network traffic • Demonstrating the detection of various attacks using Wireshark • Discussing network bandwidth monitoring and performance improvement	9%	9
12. Network Risk and Vulnerability Management	• Understanding risk and risk management • Key roles and responsibilities in risk management • Understanding Key Risk Indicators (KRI) in risk management • Explaining phase involves in risk management • Understanding enterprise network risk management • Describing various risk management frameworks • Discussing best practices for effective implementation of risk management • Understanding vulnerability management • Explaining various phases involve in vulnerability management • Understanding vulnerability assessment and its importance • Discussing requirements for effective network vulnerability assessment • Discussing internal and external vulnerability assessment • Discussing steps for effective external vulnerability assessment • Describing various phases involve in vulnerability assessment • Selection of appropriate vulnerability assessment tool • Discussing best practices and precautions for deploying vulnerability assessment tool • Describing vulnerability reporting, mitigation, remediation and verification	9%	9

13. Data Backup and Recovery	• Understanding data backup • Describing the data backup plan • Describing the identification of data to backup • Determining the appropriate backup medium for data backup • Understanding RAID backup technology and its advantages • Describing RAID architecture • Describing various RAID levels and their use • Selection of appropriate RAID level • Understanding Storage Area Network (SAN) backup technology and its advantages • Best practices of using SAN • Understanding Network Attached Storage (NAS) backup technology and its advantages • Describing various types of NAS implementation	9%	9
14. Network Incident Response and Management	• Understanding Incident Handling and Response (IH&R) • Roles and responsibilities of Incident Response Team (IRT) • Describing role of first responder • Describing first response activities for network administrators • Describing Incident Handling and Response (IH&R) process • Understanding forensic investigation • People involved in forensics investigation • Describing forensics investigation • methodology	8%	8