EC-Council

CND Exam Blueprint v3.0

Domain	Sub Domain	Description	No. Of Questions	Weightage (%)
1. Network Defense Management	Network Attacks and Defense Strategies	• Explain essential terminologies related to network security attacks • Describe the various examples of network-level attack techniques • Describe the various examples of host-level attack techniques • Describe the various examples of application-level attack techniques • Describe the various examples of social engineering attack techniques • Describe the various examples of email attack techniques • Describe the various examples of mobile device-specific attack techniques • Describe the various examples of cloud-specific attack techniques • Describe the various examples of wireless network-specific attack techniques • Describe Attacker's Hacking Methodologies and Frameworks • Understand fundamental goal, benefits, and challenges in network defense • Explain Continual/Adaptive security strategy • Explain defense-in-depth security strategy	7	10%
	Administrative Network Security	• Obtain compliance with regulatory frameworks • Discuss various Regulatory Frameworks, Laws, and Acts • Learn to design and develop security policies • Conduct security awareness training • Discuss other administrative security measures	3	
2. Network Perimeter Protection	Technical Network Security	• Discuss access control principles, terminologies, and models • Redefine Access Control security in Today's Distributed and Mobile Computing World • Discuss Identity and Access Management (IAM) concepts • Discuss cryptographic security techniques • Discuss various cryptographic algorithms • Discuss security benefits of network segmentation techniques • Discuss various essential network security solutions • Discuss various essential network security protocols	6	16%

	Network Perimeter Security	• Understand firewall security concerns, capabilities, and limitations • Understand different types of firewall technologies and their usage • Understand firewall topologies and their usage • Distinguish between hardware, software, host, network, internal, and external firewalls • Select firewalls based on its deep traffic inspection capability • Discuss firewall implementation and deployment process • Discuss recommendations and best practices for secure firewall Implementation and deployment • Discuss firewall administration activities • Understand role, capabilities, limitations, and concerns in IDS deployment • Discuss IDS/IPS classification • Discuss various components of IDS • Discuss effective deployment of network and host-based IDS • Learn to how to deal with false positive and false negative IDS alerts • Discuss the selection of appropriate IDS solutions • Discuss various NIDS and HIDS Solutions with their intrusion detection capabilities • Discuss router and switch security measures, recommendations, and best practices • Leverage Zero Trust Model Security using Software-Defined Perimeter (SDP)	10	
3. Endpoint Protection	Endpoint Security-Windows Systems	• Understand Window OS and Security Concerns • Discuss Windows Security Components • Discuss Various Windows Security Features • Discuss Windows security baseline configurations • Discuss Windows User Account and Password Management • Discuss Windows Patch Management • Discuss User Access Management • Discuss Windows OS Security Hardening Techniques • Discuss Windows Active Directory Security Best Practices • Discuss Windows Network Services and Protocol Security	5	15%
	Endpoint Security-Linux Systems	• Understand Linux OS and Security Concerns • Discuss Linux Installation and Patching • Discuss Linux OS Hardening Techniques • Discuss Linux User Access and Password Management • Discuss Linux Network and Remote Access Security • Discuss Various Linux Security Tools and Frameworks	4	

	Endpoint Security-Mobile Devices	• Discuss Common Mobile Usage Policies in Enterprises • Discuss the Security Risk and challenges associated with Enterprises mobile usage policies • Discuss security guidelines to mitigate risk associated with enterprise mobile usage policies • Discuss and implement various enterprise-level mobile security management Solutions • Discuss and implement general security guidelines and best practices on Mobile platforms • Discuss Security guidelines and tools for Android devices • Discuss Security guidelines and tools for iOS devices	3	
	Endpoint Security-IoT Devices	• Understand IoT Devices, their need, and Application Areas • Understand IoT Ecosystem and Communication models • Understand Security Challenges and risks associated with IoT-enabled environments • Discuss the security in IoT-enabled Environments • Discuss Security Measures for IoT-enabled Environments • Discuss IoT Security Tools and Best Practices • Discuss and refer various standards, Initiatives and Efforts for IoT Security	3	
4. Application and Data Protection	Administrative Application Security	• Discuss and implement Application Whitelisting and Blacklisting • Discuss and implement application Sandboxing • Discuss and implement Application Patch Management • Discuss and implement Web Application Firewall (WAF)	4	13%
	Data Security	• Understand Data Security and its Importance • Discuss the implementation of data access controls • Discuss the implementation of encryption of "Data at rest" • Discuss the implementation of Encryption of "Data at transit" • Discuss the implementation of Encryption of "Data at transit" between browser and web server • Discuss the implementation of Encryption of "Data at transit" between database server and web server • Discuss the implementation of Encryption of "Data at transit" in Email Delivery • Discuss Data Masking ConceptsDiscuss data backup and retention • Discuss Data Destruction Concepts • Data Loss Prevention(DLP) Concepts	9	

5. Enterprise Virtual, Cloud, and Wireless Network Protection	Enterprise Virtual Network Security	• Understand Virtualization Essential Concepts • Discus Network Virtualization (NV) Security • Discuss Software-Defined Network (SDN) Security • Discuss Network Function Virtualization (NFV) Security • Discus OS Virtualization Security • Discuss Security Guidelines, recommendations and best practices for Containers • Discuss Security Guidelines, recommendations and best practices for Dockers • Discuss Security Guidelines, recommendations and best practices for Kubernetes	4	12%
	Enterprise Cloud Network Security	• Understand Cloud Computing Fundamentals • Understand the Insights of Cloud Security • Evaluate CSP for Security before Consuming Cloud Service • Discuss security in Amazon Cloud (AWS) • Discuss security in Microsoft Azure Cloud • Discuss Security in Google Cloud Platform (GCP) • Discuss general security best practices and tools for cloud security	3	
	Enterprise Wireless Network Security	• Understand wireless network fundamentals • Understand wireless network encryption mechanisms • Understand wireless network authentication methods • Discuss and implement wireless network security measures	5	
6. Incident Detection	Network Traffic Monitoring and Analysis	• Understand the need and advantages of network traffic monitoring • Setting up the environment for network monitoring • Determine baseline traffic signatures for normal and suspicious network traffic • Perform network monitoring and analysis for suspicious traffic using Wireshark • Discuss network performance and bandwidth monitoring concepts	7	14%
	Network Logs Monitoring and Analysis	• Understand logging concepts • Discuss log monitoring and analysis on Windows systems • Discuss log monitoring and analysis on Linux • Discuss log monitoring and analysis on Mac • Discuss log monitoring and analysis on Firewall • Discuss log monitoring and analysis on Routers • Discuss log monitoring and analysis on Web Servers • Discuss centralized log monitoring and analysis	7	

7. Incident Response	Incident Response and Forensic Investigation	• Understand incident response concept • Understand the role of first responder in incident response • Discuss Do's and Don't in first response • Describe incident handling and response process • Describe forensics investigation process	6	10%
	Business Continuity and Disaster Recovery	• Introduction to Business Continuity (BC) and Disaster Recovery (DR) • Discuss BC/DR Activities • Explain Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) • Discuss various BC/DR Standards	4	
8. Incident Prediction	Risk Anticipation with Risk Management	• Understand risk management concepts • Learn to manage risk though risk management program • Learn different Risk Management Frameworks (RMF) • Learn to manage vulnerabilities through vulnerability management program • Learn vulnerability assessment and scanning	3	10%
	Threat Assessment with Attack Surface Analysis	• Understand the attack surface analysis • Understand and visualize your attack surface • Learn to identify Indicators of Exposures (IoE) • Learn to conduct attack simulation • Learn to reduce the attack surface	4	
	Threat Prediction With Cyber Threat Intelligence	• Understand the role of cyber threat intelligence in network defense • Understand different types of threat Intelligence • Understand the Indicators of Threat Intelligence: Indicators of Compromise (IoCs) and Indicators of Attack (IoA) • Understand the layers of Threat Intelligence • Learn to leverage/consume threat intelligence for proactive defense	3	