Cybersecurity

Candidates for this exam are starting their journey in the cybersecurity field. This exam assesses their understanding of key security paradigms, terminology, and mindset. Successful candidates will have a keen awareness of the importance of security and the threats to a business when security procedures are not followed. They are willing to teach others about security concerns. They are developing the investigative and implementation skills necessary to succeed in the field and have an aptitude and desire to learn more. They are familiar with the toolset at a fundamental level and can assist in threat mitigation and incident response. Candidates should have at least 150 hours of instruction or hands-on experience with cybersecurity.

To be successful on the test, the candidate is also expected to have the following prerequisite knowledge and skills:

- 8th grade reading, writing, and communication skills
- Algebra 1
- Critical thinking and problem-solving skills
- General operating system knowledge (Windows, MacOS, Linux)
- Familiarity with connecting to a wireless network with common commercial components
- Familiarity with setting up a simple home network

1. Essential Security Principles

1.1 Define essential security principles

- Vulnerabilities, threats, exploits, and risks; attack vectors; hardening; defense-in-depth; confidentiality, integrity, and availability (CIA); types of attackers; reasons for attacks; code of ethics

1.2 Explain common threats and vulnerabilities

- Malware, ransomware, denial of service, botnets, social engineering attacks (tailgating, spear phishing, phishing, vishing, smishing, etc.), physical attacks, man in the middle, IoT vulnerabilities, insider threats, Advanced Persistent Threat (APT)

1.3 Explain access management principles

- Authentication, authorization, and accounting (AAA); RADIUS; multifactor authentication (MFA); password policies

1.4 Explain encryption methods and applications

- Types of encryption, hashing, certificates, public key infrastructure (PKI); strong vs. weak encryption algorithms; states of data and appropriate encryption (data in transit, data at rest, data in use); protocols that use encryption

2. Basic Network Security Concepts

2.1 Describe TCP/IP protocol vulnerabilities

- TCP, UDP, HTTP, ARP, ICMP, DHCP, DNS

2.2 Explain how network addresses impact network security

- IPv4 and IPv6 addresses, MAC addresses, network segmentation, CIDR notation, NAT, public vs. private networks

2.3 Describe network infrastructure and technologies

- Network security architecture, DMZ, virtualization, cloud, honeypot, proxy server, IDS, IPS

2.4 Set up a secure wireless SoHo network

- MAC address filtering, encryption standards and protocols, SSID

2.5 Implement secure access technologies

- ACL, firewall, VPN, NAC

3. Endpoint Security Concepts

3.1 Describe operating system security concepts

- Windows, macOS, and Linux; security features, including Windows Defender and host-based firewalls; CLI and PowerShell; file and directory permissions; privilege escalation

3.2 Demonstrate familiarity with appropriate endpoint tools that gather security assessment information

- netstat, nslookup, tcpdump

3.3 Verify that endpoint systems meet security policies and standards

- Hardware inventory (asset management), software inventory, program deployment, data backups, regulatory compliance (PCI DSS, HIPAA, GDPR), BYOD (device management, data encryption, app distribution, configuration management)

3.4 Implement software and hardware updates

- Windows Update, application updates, device drivers, firmware, patching

3.5 Interpret system logs

- Event Viewer, audit logs, system and application logs, syslog, identification of anomalies

3.6 Demonstrate familiarity with malware removal

- Scanning systems, reviewing scan logs, malware remediation

4. Vulnerability Assessment and Risk Management

4.1 Explain vulnerability management

- Vulnerability identification, management, and mitigation; active and passive reconnaissance; testing (port scanning, automation)

4.2 Use threat intelligence techniques to identify potential network vulnerabilities

- Uses and limitations of vulnerability databases; industry-standard tools used to assess vulnerabilities and make recommendations, policies, and reports; Common Vulnerabilities and Exposures (CVEs), cybersecurity reports, cybersecurity news, subscription services, and collective intelligence; ad hoc and automated threat intelligence; the importance of updating documentation and other forms of communication proactively before, during, and after cybersecurity incidents; how to secure, share and update documentation

4.3 Explain risk management

- Vulnerability vs. risk, ranking risks, approaches to risk management, risk mitigation strategies, levels of risk (low, medium, high, extremely high), risks associated with specific types of data and data classifications, security assessments of IT systems (information security, change management, computer operations, information assurance)

4.4 Explain the importance of disaster recovery and business continuity planning

- Natural and human-caused disasters, features of disaster recovery plans (DRP) and business continuity plans (BCP), backup, disaster recovery controls (detective, preventive, and corrective)

5. Incident Handling

5.1 Monitor security events and know when escalation is required

- Role of SIEM and SOAR, monitoring network data to identify security incidents (packet captures, various log file entries, etc.), identifying suspicious events as they occur

5.2 Explain digital forensics and attack attribution processes

- Cyber Kill Chain, MITRE ATT&CK Matrix, and Diamond Model; Tactics, Techniques, and Procedures (TTP); sources of evidence (artifacts); evidence handling (preserving digital evidence, chain of custody)

5.3 Explain the impact of compliance frameworks on incident handling

- Compliance frameworks (GDPR, HIPAA, PCI-DSS, FERPA, FISMA), reporting and notification requirements

5.4 Describe the elements of cybersecurity incident response

- Policy, plan, and procedure elements; incident response lifecycle stages (NIST Special Publication 800-61 sections 2.3, 3.1-3.4)