98-367
Security Fundamentals

Target Audience

Candidates for this exam are seeking to prove fundamental security knowledge and skills. Before taking this exam, candidates should have a solid foundational knowledge of the topics outlined in this preparation guide. It is recommended that candidates become familiar with the concepts and the technologies described here by taking relevant training courses. Candidates are expected to have some hands-on experience with Windows Server, Windows based networking, Active Directory, Anti-Malware products, firewalls, network topologies and devices, and network ports.

Objective Domain

1. Understanding Security Layers

1.1. Understand core security principles.
This objective may include but is not limited to: confidentiality; integrity; availability; how threat and risk impact principles; principle of least privilege; social engineering; attack surface

1.2. Understand physical security.
This objective may include but is not limited to: site security; computer security; removeable devices and drives; access control; mobile device security; disable Log On Locally; keyloggers

1.3. Understand Internet security.
This objective may include but is not limited to: browser settings; zones; secure Web sites

1.4. Understand wireless security.
This objective may include but is not limited to: advantages and disadvantages of specific security types; keys; SSID; MAC filters

2. Understanding Operating System Security

2.1. Understand user authentication.
This objective may include but is not limited to: multifactor; smart cards; RADIUS; Public Key Infrastructure (PKI); understand the certificate chain; biometrics; Kerberos and time skew; using Run As to perform administrative tasks; password reset procedures

2.2. Understand permissions.
This objective may include but is not limited to: file; share; registry; Active Directory; NTFS vs. FAT; enabling or disabling inheritance; behavior when moving or copying files within the

same disk or onto another disk; multiple groups with different permissions; basic permissions and advanced permissions; take ownership; delegation

2.3. Understand password policies.
This objective may include but is not limited to: password complexity; account lockout; password length; password history; time between password changes; enforce by using group policies; common attack methods

2.4. Understand audit policies.
This objective may include but is not limited to: types of auditing; what can be audited; enabling auditing; what to audit for specific purposes; where to save audit information; how to secure audit information

2.5. Understand encryption.
This objective may include but is not limited to: EFS; how EFS-encrypted folders impact moving and copying files; BitLocker (To Go); Trusted Platform Module (TPM); software-based encryption; MAIL encryption and signing and other uses; VPN; public key and private key; encryption algorithms; certificate properties; certificate services; PKI/certificate services infrastructure; token devices

2.6. Understand malware.
This objective may include but is not limited to: buffer overflow; worms; Trojans; spyware

3. Understanding Network Security

3.1. Understand dedicated firewalls.
This objective may include but is not limited to: types of hardware firewalls and their characteristics; when to use a hardware firewall instead of a software firewall; stateful vs. stateless inspection

3.2. Understand Network Access Protection (NAP).
This objective may include but is not limited to: purpose of NAP; requirements for NAP

3.3. Understand network isolation.
This objective may include but is not limited to: VLANs; routing; honeypot; DMZ; NAT; VPN; IPsec; Server and Domain Isolation

3.4. Understand protocol security.
This objective may include but is not limited to: protocol spoofing; IPsec; tunneling; DNSsec; network sniffing; common attack methods

4. Understanding Security Software

4.1. Understand client protection.
This objective may include but is not limited to: anti-virus; User Account Control (UAC); keeping client operating system and software updated; encrypting offline folders; software restriction policies

4.2. Understand e-mail protection.
This objective may include but is not limited to: anti-spam; anti-virus; spoofing, phishing, and pharming; client vs. server protection; SPF records; PTR records

4.3. Understand server protection.

This objective may include but is not limited to: separation of services; hardening; keeping server updated; secure dynamic DNS updates; disabling unsecure authentication protocols; Read-Only Domain Controllers; separate management VLAN; Microsoft Baseline Security Analyzer (MBSA)