Exam 98-367: Security Fundamentals

This exam validates that a candidate has fundamental security knowledge and skills. It can serve as a stepping stone to the Microsoft Certified Solutions Associate (MCSA) exams. 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

Microsoft
Technology Associate

Understand Operating System Security

- **Understand User Authentication.**
  - Multifactor authentication; physical and virtual smart cards; Remote Authentication Dial-In User Service (RADIUS); biometrics; use Run As to perform administrative tasks
- **Understand Permissions.**
  - File system permissions; share permissions; registry; Active Directory; enable or disable inheritance; behavior when moving or copying files within the same disk or on another disk; multiple groups with different permissions; basic permissions and advanced permissions; take ownership; delegation; inheritance
- **Understand Password Policies.**
  - Password complexity; account lockout; password length; password history; time between password changes; enforce by using Group Policies; common attack methods; password reset procedures; protect domain user account passwords
- **Understand Audit Policies.**
  - Types of auditing; what can be audited; enable auditing; what to audit for specific purposes; where to save audit information; how to secure audit information
- **Understand Encryption.**
  - Encrypting file system (EFS); how EFS- encrypted folders impact moving/copying files; BitLocker (To Go); TPM; software-based encryption; MAIL encryption and signing and other uses; virtual private network (VPN); public key/ private key; encryption algorithms; certificate properties; certificate services; PKI/certificate services infrastructure; token devices; lock down devices to run only trusted applications
- **Understand Malware.**
  - Buffer overflow; viruses, polymorphic viruses; worms; Trojan horses; spyware; ransomware; adware; rootkits; backdoors; zero day attacks

Exam 98-367: Security Fundamentals

Understand Security Layers

- **Understand Core Security Principles.**
  - Confidentiality; integrity; availability; how threat and risk impact principles; principle of least privilege; social engineering; attack surface analysis; threat modelling
- **Understand Physical Security.**
  - Site security; computer security; removable devices and drives; access control; mobile device security; keyloggers
- **Understand Internet Security.**
  - Browser security settings; secure websites
- **Understand Wireless Security.**
  - Advantages and disadvantages of specific security types; keys; service set identifiers (SSIDs); MAC filters

Understand Network Security

- **Understand Dedicated Firewalls.**
  - Types of hardware firewalls and their characteristics; when to use a hardware firewall instead of a software firewall; stateful vs. stateless firewall inspection; Security Compliance Manager; security baselines
- **Understand Network Isolation.**
  - Routing; honeypot; perimeter networks; network address translation (NAT); VPN; IPsec; server and domain isolation
- **Understand Protocol Security.**
  - Protocol spoofing; IPsec; tunnelling; DNSsec; network sniffing; denial-of-service (DoS) attacks; common attack methods

Understand Security Software

- **Understand Client Protection.**
  - Antivirus; protect against unwanted software installations; User Account Control (UAC); keep client operating system and software updated; encrypt offline folders; software restriction policies; principal of least privilege
- **Understand Email Protection.**
  - Antispam, antivirus, spoofing, phishing, and pharming; client vs. server protection; Sender Policy Framework (SPF) records; PTR records
- **Understand Server Protection.**
  - Separation of services; hardening; keep servers updated; secure dynamic Domain Name System (DNS) updates; disable unsecure authentication protocols; Read-Only Domain Controllers (RODC)