MTA: Security Fundamentals – Skills Measured

NOTE: The bullets that appear below each of the skills measured are intended to illustrate how we are assessing that skill. This list is not definitive or exhaustive.

NOTE: In most cases, exams do NOT cover preview features, and some features will only be added to an exam when they are GA (General Availability).

Exam 98-367: Security Fundamentals

Understand security layers (25–30%)

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 operating system security (35-40%)

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

Understand network security (20–25%)

Understand dedicated firewalls

- types of hardware firewalls and their characteristics; when to use a hardware firewall instead of a software firewall; stateful versus 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; tunneling; DNSsec; network sniffing; denial-of-service (DoS) attacks; common attack methods

Understand security software (15–20%)

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; principle of least privilege

Understand email protection

- antispam, antivirus, spoofing, phishing, and pharming; client versus server protection; Sender Policy Framework (SPF) records; PTR records

Understand server protection

- separation of services; hardening; keep server updated; secure dynamic Domain Name System (DNS) updates; disable unsecure authentication protocols; Read-Only Domain Controllers (RODC)