Microsoft MTA Security Fundamentals Training

Course Outline:

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 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 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-ofservice (DoS) attacks; common attack methods **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)