COURSE: SECURITY+ SY0-401

MODULE 4: APPLICATION, DATA AND HOST SECURITY

Overview

- Given a scenario, select the appropriate solution to establish host security
- Implement the appropriate controls to ensure data security
- Compare and contrast alternative methods to mitigate security risks in static environments

Host Security

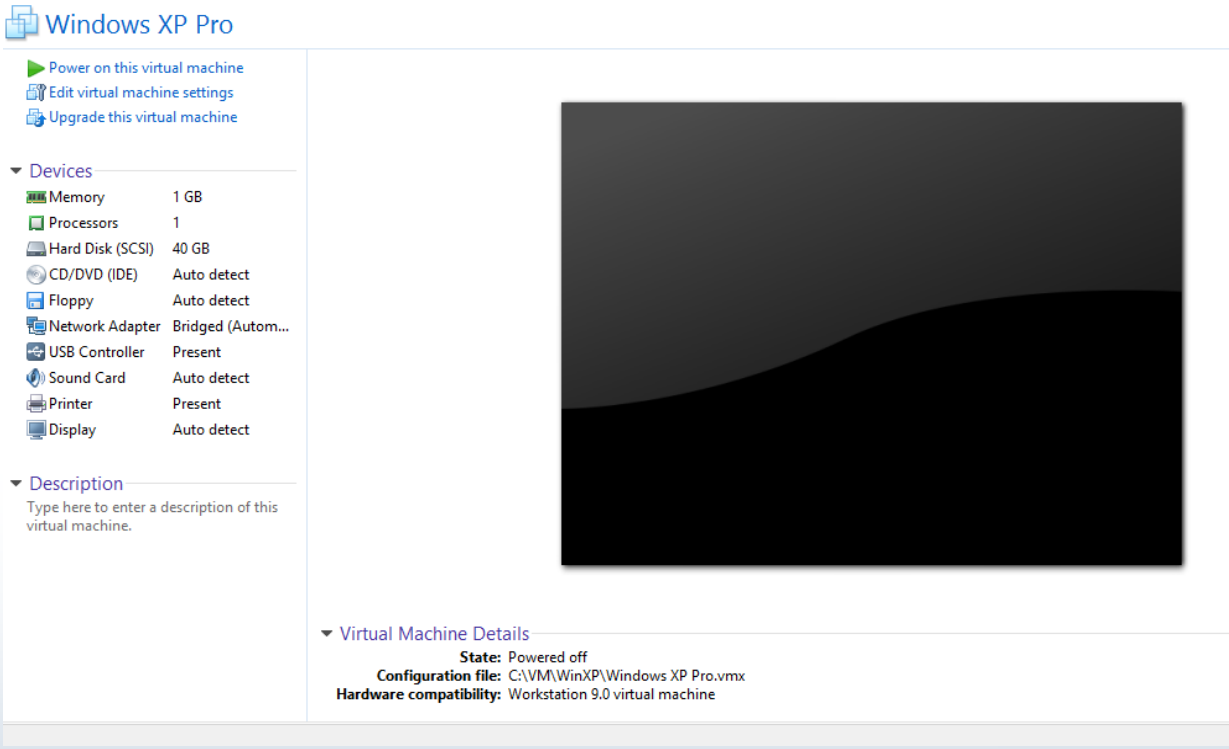
- Operating system security and settings
- OS hardening
  - Anti-malware
  - Antivirus
  - Anti-spam
  - Anti-spyware
  - Pop-up blockers
- Patch management
- White listing vs. black listing applications

Host Security

- Trusted OS
- Host-based firewalls
- Host-based intrusion detection
- Hardware security
- Cable locks
- Safe
- Locking cabinets
- Host software baselining

Host Security

- Virtualization
  - Patch compatibility
  - Host availability/elasticity
  - Security control testing
  - Snapshots
  - Sandboxing



Data Security

- Cloud storage
- SAN
- Handling Big Data
- Data encryption
  - Full disk
  - Database
  - Individual files
  - Removable media
  - Mobile devices

Data Security

- Hardware based encryption devices
  - TPM
  - HSM
  - USB encryption
  - Hard drive
- Data in-transit, Data at-rest, Data in-use
- Permissions/ACL
- Data policies
  - Wiping
  - Disposing
  - Retention
  - Storage

Static Environments

Environments

- SCADA
- Embedded (Printer, Smart TV, HVAC control)
- Android
- iOS
- Mainframe
- Game consoles
- In-vehicle computing systems

Static Environments

- Methods
  - Network segmentation
  - Security layers
  - Application firewalls
  - Manual updates
  - Firmware version control
  - Wrappers
  - Control redundancy and diversity

THANK YOU