CompTIA Security + 3.0 Architecture and Design

Filename: comptia-secplussy0501-3-3-secure_system_design
Title: Secure System Design
Subtitle: CompTIA Security+ (SY0-501)

3.3 Secure System Design

- 3.3 Given a scenario, implement secure systems design.
    - Hardware/firmware security
        - FDE/SED
            - FDE
                - BitLocker
                - Intel(McAfee) Complete Endpoint Protection
                - Sophos SafeGuard Enterprise
                - Symantec Endpoint Encryption
            - SED
                - Seagate Constellation, Dell, HP, Samsung, Toshiba
                - Internal/External
                - Hotswappsble
                - Mechanical, Solid State
                - SATA, SAS
        - TPM
            - Contains identifiers for trusted routines
            - Contains information on trusted operational state
            - Stores cryptographic data such as encryption keys
            - Helps to assist UEFI Secure Boot
        - HSM
        - UEFI/BIOS
        - Secure boot and attestation
            - Trusted bootloaders
            - Measured Boot (type of attestation)
        - Supply chain
            - NIST 800-161
            - NIST 18227
        - Hardware root of trust
            - A set of trusted routines that are "rooted" in or begin in the hardware
            - TPM/KNOX
        - EMI/EMP
    - Operating systems
        - Types
            - Network
            - Server
            - Workstation
            - Appliance
            - Kiosk
            - Mobile OS
    - Patch management
        - Resources
            - SANS
            - http://bit.ly/2o7hTgj
    - Disabling unnecessary ports and services
        - Show netstat -a -n on Windows Server
        - Show nmap -v 10.10.10.100 (\note SMTP port)
    - Least functionality
    - Secure configurations
        - Are the current processes on the system
    - Trusted operating system
        - An operating systems that provided multiple layers of security
        - The ability of the OS security mechanisms to achieve security standards compliances
    - Application whitelisting/blacklisting
    - Disable default accounts/passwords
    - Peripherals
        - Wireless keyboards
        - Wireless mice
        - Displays
        - WiFi-enabled MicroSD cards
            - Eyefi - http://www.eyefi.com/
            - EZ Share
        - Printers/MFDs

- External storage devices
- Digital cameras