CompTIA®

Security+

Exam SY0-501

#1 Threats, Attacks and Vulnerabilities

1.1. Given a scenario, analyze indicators of compromise and determine the type of malware.

- Viruses
- Worm
- Trojan
- Crypto-Malware
- Ransomware
- Rootkit
- Keylogger
- Adware
- Spyware
- Bots (Botnets)
- RAT (Remote Access Trojan)
- Logic Bomb
- Backdoor

Viruses *vs* Worms *vs* Trojans

● Common 1 ● Common 2 ● Common 3	● Common 1 ● Common 2 ● Common 3	● Common 1 ● Common 2 ● Common 3
● Diff 1 ● Diff 2 ● Diff 3	● Diff 1 ● Diff 2 ● Diff 3	● Diff 1 ● Diff 2 ● Diff 3

https://techdifferences.com/difference-between-virus-worm-and-trojan-horse.html

1.2. Compare and contrast types of attacks.

Social Engineering

- Phishing
- Spear Phishing
- Whaling
- Vishing
- Tailgating
- Impersonation
- Dumpster diving
- Shoulder surfing
- Hoax
- Watering hole attack
- Principles (reasons)
  - Authority
  - Intimidation
  - Consensus
  - Scarcity
  - Familiarity
  - Trust
  - Urgency

1.2. Compare and contrast types of attacks.

Application / Service Attacks

- DoS
- DDoS
- Man-In-The-Middle
- Buffer Overflow
- Injection
- IP Spoofing
- MAC Spoofing
- Cross-site Scripting (XSS)
- Cross-site request forgery
- ARP Poisoning
- Amplification
- DNS Poisoning
- Domain Hijacking
- Man-In-The-Browser
- Zero-Day
- Replay
- Pass the hash
- Hijacking and related attacks
  - Clickjacking
  - Session Hijacking
  - URL Hijacking
  - Typo Hijacking
- Driver manipulation
  - Shimming
  - Refactoring

1.2. Compare and contrast types of attacks.

Wireless Attacking

- Replay
- IV
- Evil Twin
- Rogue AP
- Jamming
- WPS
- Bluejacking
- Bluesnarfing
- RFID
- NFC
- Disassociation

1.2. Compare and contrast types of attacks.

Cryptographic Attacks

- Birthday
- Known Plain Text / Cipher Text
- Rainbow Tables
- Dictionary
- Brute Force
  - Online vs Offline
- Collision
- Downgrade
- Replay
- Weak Implementations

1.3. Explain threat actor types and attributes.

Type of actors

- Script Kiddies
- Hacktivist
- Organized Crime
- Nation States / APT
- Insiders
- Competitors

Attribute of Actors

- Internal / External
- Level of sophistication
- Resources / Founding
- Intent / Motivation

Use of open-source engineering

1.4. Explain penetration testing concepts.

- Active reconnaissance
- Passive reconnaissance
- Pivot
- Initial Exploitation
- Persistence
- Privilege Escalation
- Black Box
- White Box
- Gray Box
- Penetration Testing *vs* Vulnerability Scanning

1.5. Explain vulnerability scanning concepts.

- Passively test security controls
- Identify Vulnerability
- Identify lack of security controls
- Identify common misconfigurations
- Intrusive vs non-intrusive
- Credentialed vs non-credentialed
- False positive

1.6. Explain the impact associated with types of vulnerabilities.

- Race conditions
- Vulnerabilities due to:
  - End-of-life systems
  - Embedded systems
  - Lack of vendor support
- Improper input handling
- Improper error handling
- Misconfigurations / weak configuration
- Default configuration
- Resource Exhaustion
- Untrained users
- Improper configured accounts
- Vulnerable business process
- Weak cipher suites and implementations
- Memory / Buffer Vulnerabilities
  - Memory leak
  - Integer overflow
  - Buffer Overflow
  - Pointer Dereference
  - DLL Injection
- System spraw / Undocumented Assets

#2 Technologies and Tools

2.1. Install and configure network components, both hardware- and software-based, to support organizational security.

- Firewall
  - ACL
  - Application-based vs Network-based
  - Stateful vs stateless
  - Implicit deny
- VPN concentrator
  - Remote access vs. site-to-site
  - IPSec
    - Tunnel mode
    - Transport mode
    - AH
    - ESP
- NIPS / NIDS
  - Signature-based
  - Heuristic / behavioral
  - Anomaly
  - Inline vs passive
  - In-band vs out-of-band
  - Rules
  - Analytics
    - False positive
    - False negative
- Router
  - ACLs
  - Antispoofing

2.1. Install and configure network components, both hardware- and software-based, to support organizational security.

- Switch
  - Port security
  - Layer 2 vs. Layer 3
  - Loop prevention
  - Flood Guard
- Load balancer
  - Scheduling
    - Affinity
    - Round-robin
  - Active-Passive
  - Active-Active
  - Virtual IP
- Proxy
  - Forward and reverse proxy
  - Transparent
  - Application / Multipurpose
- Access Point
  - SSID
  - MAC filtering
  - Signal strength
  - Band selection/width
  - Antenna types and placement
  - Fat vs. thin
  - Controller-based vs. standalone

2.1. Install and configure network components, both hardware- and software-based, to support organizational security.

- SIEM
  - Aggregation
  - Correlation
  - Automated alerting and triggers
  - Time synchronization
  - Event deduplication
  - Logs / WORM
- DLP
  - USB blocking
  - Cloud-based
  - Email
- Bridge
- NAC
  - Dissolvable vs permanent
  - Host health checks
  - Agent vs agentless
- Mail gateway
  - Spam filter
  - DLP
  - Encryption
- SSL/TLS accelerators
- SSL descriptors
- Media gateway
- Hardware security module

2.2. Given a scenario, use appropriate software tools to assess the security posture of an organization.

- Protocol analyzer
- Network scanners
  - Rogue system detection
  - Network mapping
- Wireless scanners/cracker
- Password cracker
- Vulnerability scanner
- Configuration compliance scanner
- Exploitation frameworks
- Data sanitization tools
- Steganography tools
- Honeypot
- Backup utilities
- Banner grabbing
- Passive vs active
- Command tools
  - ping
  - netstat
  - tracert
  - nslookup/dig
  - arp
  - ipconfig/ip/ifconfig
  - tcpdump
  - nmap
  - netcat

2.3. Given a scenario, troubleshoot common security issues.

- Unencrypted credentials/clear text
- Logs and events anomalies
- Permission issues
- Access violations
- Certificate issues
- Data exfiltration
- Misconfigured devices
  - Firewall
  - Content filter
  - Access points
- Weak security configurations
- Personnel issues
  - Policy violation
  - Insider threat
  - Social engineering
  - Social media
  - Personal email
- Unauthorization software
- Baseline deviation
- License compliance violation (Availability/integrity)
- Asset management
- Authentication issues

2.4. Given a scenario, analyze and interpret output from security technologies.

- HIDS / HIPS
- Antivirus
- File security check
- Host-based firewall
- Application whitelisting
- Removable media control
- Advanced malware tools
- Patch management tools
- UTM
- DLP
- Data execution prevention
- Web application firewall

2.5. Given a scenario, deploy mobile devices securely.

- Connection methods
  - Cellular
  - WiFi
  - SATCOM
  - Bluetooth
  - NFC
  - ANT
  - Infrared
  - USB

- Mobile device management concepts
  - Application management
  - Content management
  - Remote wipe
  - Geofencing
  - Geolocation
  - Screen locks
  - Push notification services
  - Passwords and pins
  - Biometrics
  - Context-aware authentication
  - Containerization
  - Storage segmentation
  - Full device encryption

2.5. Given a scenario, deploy mobile devices securely.

- Enforcement and monitoring for:
    - Third-party app stores
    - Rooting / jailbreaking
    - sideloading
    - Custom firmware
    - Carrier unlocking
    - Firmware OTA updates
    - Camera use
    - SMS/MMS
    - External media
    - USB OTG
    - Recording microphone
    - GPS tagging
    - WiFi direct / ad hoc
    - Tathering
    - Payment methods

- Deployment models
    - BYOD
    - COPE
    - CYOD
    - Corporate-owned
    - VDI

2.6. Given a scenario, implement secure protocols.

- Protocols
  - DNSSEC
  - SSH
  - S/MIME
  - SRTP
  - LDAPS
  - FTPS
  - SFTP
  - SNMPv3
  - SSL/TLS
  - HTTPS
  - Secure POP.IMAP

- Use cases
  - Voice and video
  - Time synchronization
  - Email and web
  - File transfer
  - Directory services
  - Remote access
  - Domain name resolution
  - Routing and switching
  - Network address allocation
  - Subscription services

FTPS vs SFTP

https://www.smartfile.com/blog/sftp-vs-ftps-the-secure-file-transfer-methods-battle-it-out/

#3 Architecture and Design

3.1. Explain use cases and purpose for frameworks, best practices and secure configuration guides.

- Industry standard frameworks and reference architectures.
  - Regulatory
  - Non-regulatory
  - National vs International
  - Industry specific frameworks
- Defense in depth / Layered security
  - Vendor diversity
  - Control diversity
    - Administrative
    - Technical
  - User training
- Benchmarks / secure configuration guides
  - Platform/vendor specific guides
    - Web Servers
    - Operating system
    - Application Server
    - Network infrastructure devices

3.2. Given a scenario, implement secure network architecture concepts.

- Zones / topologies
  - DMZ
  - Extranet
  - Intranet
  - Wireless
  - Guest
  - Honeypots
  - NAT
  - Ad hocs
- Segregation/Segmentation/Isolation
  - Physical
  - Logical (VLAN)
  - Virtualization
  - Air gaps
- Tunneling / VPN
  - Site-to-site
  - Remote access
- SND

3.2. Explain use cases and purpose for frameworks, best practices and secure configuration guides.

- Security device / Technology placement
  - Sensors
  - Collectors
  - Correlation Engines
  - Filters
  - Proxies
  - Firewalls
  - VPN concentrators
  - SSL accelerators
  - Load balancers
  - DDos mitigator
  - Aggregation switches
  - Taps and port mirrors

3.3. Given a scenario, implement secure systems design.

- Hardware / firmware security
  - FDE/SED
  - TPM
  - HSM
  - UEFI / BIOS
  - Secure boot and attestation
  - Supply chain
  - Hardware root of trust
  - EMI / EMP

- Peripherals
  - Wireless keyboards
  - Wireless mice
  - Displays
  - WiFi-enabled MicroSD cards
  - Printers / MFDs
  - External Storage Devices
  - Digital Cameras

3.3. Given a scenario, implement secure systems design.

- Operating systems
  - Types
    - Network
    - Server
    - Workstation
    - Appliance
    - Kiosk
    - Mobile OS
  - Patch management
  - Disabling unnecessary ports and services
  - Least functionality
  - Secure configurations
  - Trusted Operating System
  - Application whitelisting / blacklisting
  - Disable default accounts / passwords

3.4. Explain the importance of secure staging deployment concepts.

- Sandboxing
- Environment
  - Development
  - Test
  - Staging
  - Production
- Secure baseline
- Integrity measurement

3.5. Explain the security implications of embedded systems.

- SCADA / ICS
- Smart Devices / IoT
  - Wearable technology
  - Home automation
- HVAC
- SoC
- RTOS
- Printers / MFDs
- Camera Systems
- Special purpose
  - Medical devices
  - Vehicles
  - Aircraft / UAV

3.6. Summarize secure application development and deployment concepts.

- Development life-cycle models
  - Waterfall vs Agile
- Secure DevOps
  - Security Automation
  - Continuous Integration
  - Baselining
  - Immutable systems
  - Infrastructure as code
- Version control and change management
- Provisioning and deprovisioning

- Secure coding techniques
  - Proper error handling
  - Proper input validation
  - Normalization
  - Stored procedures
  - Code signing
  - Encryption
  - Obfuscation/camouflage
  - Code reuse / dead code
  - Server-side vs client-side
  - Execution and validation
  - Memory management
  - Use of third-party libraries and SDKs
  - Data exposure

3.6. Summarize secure application development and deployment concepts.

- Code quality and testing
  - Static code analysis
  - Dynamic analysis (e.g. fuzzing)
  - Stress testing
  - Sandboxing
  - Model verification
- Compiled vs Runtime code

3.7. Summarize cloud and virtualization concepts.

- Hypervisor
  - Type I
  - Type II
  - Application cells / containers
- VM sprawl avoidance
- VM escape protection
- Cloud storage
- On-premisse vs hosted vs cloud
- VDI / VDE
- Cloud access security broker
- Security as a Service

- Cloud deployment models
  - SaaS
  - PaaS
  - IaaS
  - Private
  - Public
  - Hybrid
  - Community

3.8. Explain how resiliency and automation strategies reduce risk.

- Automation/scripting
  - Automated courses of action
  - continuous monitoring
  - Configuration validation
- Templates
- Master image
- Non-persistence
  - Snapshots
  - Revert to know state
  - Rollback to known configuration
  - Live boot media

- Elasticity
- Distributive allocation
- Redundancy
- Fault tolerance
- High Availability
- RAID

3.9. Explain the importance of physical security controls.

- Lighting
- Signs
- Fencing / gate / cage
- Security guards
- Alarms
- Safe
- Secure cabinets / enclosures
- Protected distributions / protected cabling
- Airgap
- Mantrap
- Faraday cage
- Lock types
- Biometrics
- Barricades / bollards
- Tokens / cards
- Environmental controls
  - HVAC
  - Hot and cold aisles
  - Fire supression

3.9. Explain the importance of physical security controls.

- Cable locks
- Screen filters
- Cameras
- Motion detection
- Logs
- Infrared detection
- Key management

#4 Identity and Access Management

#5 Risk Management

#6 Cryptography and PKI