

COMPTIA SECURITY+ 2008 EXAM OBJECTIVES COVERED

1.0 Systems Security

1.1 Differentiate among various systems security threats.

- Privilege escalation
- Virus
- Worm
- Trojan
- Spyware
- Spam
- Adware
- Rootkits
- Botnets
- Logic bomb

1.2 Explain the security risks pertaining to system hardware and peripherals.

- BIOS
- USB devices
- Cell phones
- Removable storage
- Network attached storage

1.3 Implement OS hardening practices and procedures to achieve workstation and server security.

- Hotfixes
- Service packs
- Patches
- Patch management
- Group policies
- Security templates
- Configuration baselines

1.4 Carry out the appropriate procedures to establish application security.

- ActiveX
- Java
- Scripting
- Browser
- Buffer overflows
- Cookies
- SMTP open relays
- Instant messaging
- P2P
- Input validation
- Cross-site scripting (XSS)

1.5 Implement security applications.

- HIDS
- Personal software firewalls
- Antivirus
- Anti-spam
- Popup blockers

1.6 Explain the purpose and application of virtualization technology.

2.0 Network Infrastructure

2.1 Differentiate between the different ports & protocols, their respective threats and mitigation techniques.

- Antiquated protocols
- TCP/IP hijacking
- Null sessions
- Spoofing
- Man-in-the-middle
- Replay
- DOS
- DDOS
- Domain Name Kiting
- DNS poisoning
- ARP poisoning

4.0 Assessments & Audits

4.1 Conduct risk assessments and implement risk mitigation.

4.2 Carry out vulnerability assessments using common tools.

- Port scanners
- Vulnerability scanners
- Protocol analyzers
- OVAL
- Password crackers
- Network mappers

4.3 Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning.

4.4 Use monitoring tools on systems and networks and detect security-related anomalies.

- Performance monitor
- Systems monitor
- Performance baseline
- Protocol analyzers

4.5 Compare and contrast various types of monitoring methodologies.

- Behavior-based
- Signature-based
- Anomaly-based

4.6 Execute proper logging procedures and evaluate the results.

- Security application
- DNS
- System
- Performance
- Access
- Firewall
- Antivirus

4.7 Conduct periodic audits of system security settings.

- User access and rights review
- Storage and retention policies
- Group policies

5.0 Cryptography

5.1 Explain general cryptography concepts.

- Key management
- Steganography
- Symmetric key
- Asymmetric key
- Confidentiality
- Integrity and availability
- Non-repudiation
- Comparative strength of algorithms
- Digital signatures
- Whole disk encryption
- Trusted Platform Module (TPM)
- Single vs. Dual sided certificates
- Use of proven technologies

5.2 Explain basic hashing concepts and map various algorithms to appropriate applications.

- SHA
- MD5
- LANMAN
- NTLM

5.3 Explain basic encryption concepts and map various algorithms to appropriate applications.

- DES
- 3DES
- RSA
- PGP

2.2 Distinguish between network design elements and components.

- DMZ
- VLAN
- NAT
- Network interconnections
- NAC
- Subnetting
- Telephony

2.3 Determine the appropriate use of network security tools to facilitate network security.

- NIDS
- NIPS
- Firewalls
- Proxy servers
- Honeypot
- Internet content filters
- Protocol analyzers

2.4 Apply the appropriate network tools to facilitate network security.

- NIDS
- Firewalls
- Proxy servers
- Internet content filters
- Protocol analyzers

2.5 Explain the vulnerabilities and mitigations associated with network devices.

- Privilege escalation
- Weak passwords
- Back doors
- Default accounts
- DOS

2.6 Explain the vulnerabilities and mitigations associated with various transmission media.

- Vampire taps

2.7 Explain the vulnerabilities and implement mitigations associated with wireless networking.

- Data emanation
- War driving
- SSID broadcast
- Blue jacking
- Bluesnarfing
- Rogue access points
- Weak encryption

3.0 Access Control

3.1 Identify and apply industry best practices for access control methods.

- Implicit deny
- Least privilege
- Separation of duties
- Job rotation

3.2 Explain common access control models and the differences between each.

- MAC
- DAC
- Role & Rule based access control

3.3 Organize users and computers into appropriate security groups and roles while distinguishing between appropriate rights and privileges.

3.4 Apply appropriate security controls to file and print resources.

3.5 Compare and implement logical access control methods.

- ACL
- Group policies
- Password policy
- Domain password policy

- Elliptic curve
- AES
- AES256
- One time pad
- Transmission encryption (WEP TKIP, etc)

5.4 Explain and implement protocols.

- SSL/TLS
- S/MIME
- PPTP
- HTTP vs. HTTPS vs. SHTTP
- L2TP
- IPSEC
- SSH

5.5 Explain core concepts of public key cryptography.

- Public Key Infrastructure (PKI)
- Recovery agent
- Public key
- Private keys
- Certificate Authority (CA)
- Registration
- Key escrow
- Certificate Revocation List (CRL)
- Trust models

5.6 Implement PKI and certificate management.

- Public Key Infrastructure (PKI)
- Recovery agent
- Public key
- Private keys
- Certificate Authority (CA)
- Registration
- Key escrow
- Certificate Revocation List (CRL)

6.0 Organizational Security

6.1 Explain redundancy planning and its components.

- Hot site
- Cold site
- Warm site
- Backup generator
- Single point of failure
- RAID
- Spare parts
- Redundant servers
- Redundant ISP
- UPS
- Redundant connections

6.2 Implement disaster recovery procedures.

- Planning
- Disaster recovery exercises
- Backup techniques and practices – storage
- Schemes
- Restoration

6.3 Differentiate between and execute appropriate incident response procedures.

- Forensics
- Chain of custody
- First responders
- Damage and loss control
- Reporting – disclosure of

6.4 Identify and explain applicable legislation and organizational policies.

- Secure disposal of computers
- Acceptable use policies
- Password complexity
- Change management
- Classification of information
- Mandatory vacations
- Personally Identifiable Information (PII)
- Due care
- Due diligence

- User names and passwords
- Time of day restrictions
- Account expiration
- Logical tokens

3.6 Summarize the various authentication models and identify the components of each.

- One, two and three-factor authentication
- Single sign-on

3.7 Deploy various authentication models and identify the components of each.

- Biometric reader
- RADIUS
- RAS
- LDAP
- Remote access policies
- Remote authentication
- VPN
- Kerberos
- CHAP
- PAP
- Mutual
- 802.1x
- TACACS

3.8 Explain the difference between identification and authentication (identity proofing).

3.9 Explain and apply physical access security methods.

- Physical access logs/lists
- Hardware locks
- Physical access control – ID badges
- Door access systems
- Man-trap
- Physical tokens
- Video surveillance – camera types and positioning

- Due process
- SLA
- Security-related HR policy
- User education and awareness training

6.5 Explain the importance of environmental controls.

- Fire suppression
- HVAC
- Shielding

6.6 Explain the concept of and how to reduce the risks of social engineering.

- Phishing
- Hoaxes
- Shoulder surfing
- Dumpster diving
- User education and awareness training