EXAM CRAM

The Security+ Cram Sheet

This Cram Sheet contains the distilled, key facts about the Security+ exam. Review this information as the last step before you enter the testing center, paying special attention to those areas where you think that you need the most review.

SYSTEM SECURITY

1. Programming errors can result in system compromise, allowing someone to gain unauthorized privileges, known as privilege escalation.
2. Forms of system security threats include the following:
   - *Viruses*—Infect systems and spread copies of themselves
   - *Trojans*—Disguise malicious code within apparently useful applications
   - *Logic bombs*—Trigger on a particular condition
   - *Worms*—Self-replicating forms of other types of malicious code
   - *Bots*—Systems that can be controlled by outside sources
   - *Rootkits*—Pieces of software that can be installed and hidden on a computer mainly for the purpose of compromising the system
   - *Spyware*—Software on your PC that is sending information about you and your surfing habits to a remote location
   - *Spam*—Term that refers to the sending of unsolicited commercial email.

Security Risks Pertaining to System Hardware and Peripherals

3. The BIOS can be compromised in several ways: BIOS password, known vulnerabilities, and bypassing access control.
4. Small, high-capacity, removable storage devices present a concern when it comes to corporate security and protecting proprietary information.

Online Vulnerabilities

5. Web vulnerabilities include the following:
   - Java and JavaScript
   - ActiveX controls
   - Cookies
   - CGI vulnerabilities
   - SMTP relay vulnerabilities
6. Protocol vulnerabilities include the following:
   - TLS
   - LDAP
   - FTP vulnerabilities, including anonymous access and unencrypted authentication
   - Wireless vulnerabilities, including WEP key analysis
7. A site survey is necessary before deploying a WLAN.

NETWORK INFRASTRUCTURE

8. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks involve the disruption of normal network services and include the following types:
   - *Smurf*—An attack based on the ICMP echo reply
   - *Fraggle*—Smurf-like attack based on UDP packets
   - *Ping flood*—Blocks service through repeated pings
   - *SYN flood*—Repeated SYN requests without ACK
   - *Land*—Exploits TCP/IP stacks using spoofed SYNs (where the same source address and port appears in both source and destination elements)
   - *Teardrop*—An attack using overlapping, fragmented UDP packets that can't be reassembled correctly
   - *Bonk*—An attack on port 53 using fragmented UDP packets with bogus reassembly information
   - *Boink*—Bonk-like attack on multiple ports
9. A back door allows access to a system. This can happen inadvertently when programming checks that were created during the development stage are not removed before the software goes into production or through the installation of malware.
10. Spoofing is the process of making data look as if it came from a trusted or legitimate origin.
11. Man-in-the-middle attacks involve the interception of traffic between two systems using a third system pretending to be the others.
12. Replay attacks involve the reposting of captured data.
13. TCP/IP hijacking involves taking control of a TCP/IP session.
14. Mathematical attacks involve cryptographic key cracking.
15. Password-guessing, brute-force, and dictionary attacks involve repeated guessing of logons and passwords.
16. A null session is a connection without specifying a username or password.
17. DNS poisoning allows a perpetrator to redirect traffic by changing the IP record for a specific domain (thus permitting attackers to send legitimate traffic anywhere they choose).
18. In ARP poisoning, the attacker deceives a device on your network, poisoning its table associations of other devices.
19. Domain kiting refers to the practice of taking advantage of the Add Grace Period to monopolize domain names without ever paying for them.

Security Applications

20. Host intrusion detection systems (HIDSs) are implemented to monitor event and applications logs, port access, and other running processes.
21. Antivirus software is used to scan for any malicious code present in the system, whether downloaded or copied from other systems.
22. The main component of antispam software is heuristic filtering. Heuristic filtering has a predefined ruleset that compares incoming email information against the ruleset.
23. Although some pop-ups are helpful, many are more of an annoyance, and others can contain inappropriate content or entice the user to download malware.
24. Virtualization gives the organization more control over the environment because applications can be isolated and hardware resources can be shared.

Apply Network Tools

25. Firewalls separate external and internal networks and include the following types:
   - Packet-filtering firewalls (network layer, Layer 3)
   - Proxy-service firewalls, including circuit-level (session layer, Layer 5) and application-level (application layer, Layer 7) gateways
   - Stateful-inspection firewalls (application layer, Layer 7)
26. Network intrusion detection systems (NIDSs) designed to catch attacks in progress within the network, not just on individual machines or the boundary between private and public networks.
27. Proxy servers can be placed between the private network and the Internet for Internet connectivity or internally for web content caching.
28. Protocol analyzers can be placed in-line or in between the devices from which you want to capture the traffic.

Common Access Control Models

29. Access control includes considerations of direct access, network access, facilities, and the environment supporting a system.
30. Print and file sharing increases the risk of intruders being able to access any of the files on a computer's hard drive.
31. Every operating system object created has a security attribute that matches it to an access control list.
32. Identity proofing is an organizational process that binds users to authentication methods.

ACCESS CONTROL

33. Authentication involves determining the identity of the account attempting access to resources. Here are some key points:
   - Kerberos authentication is a ticket-based, symmetric key authentication system involving a KDC. Kerberos 5 supports mutual authentication.
   - CHAP involves the exchange of hashed values for authentication.
   - Certificates are used within a PKI to provide an asymmetric key solution.
   - Username and password combinations are the most common form of authentication.
   - Token-based authentication is a strong form requiring possession of the token item.
   - Biometric authentication uses parts of the human body (hand, finger, iris, and so on) for authentication.

Remote Access

34. Remote access includes these items:
    - 802.11x wireless networking (Wi-Fi)
    - Virtual private network (VPN) connections
    - Dial-up using RADIUS, TACACS, or TACACS+
    - SSL connections
    - Packet-level authentication via IPsec in the network layer (Layer 3) of the OSI model
35. VPN connections use PPTP or L2TP connectivity.
36. SSH functions as a secure Telnet.
37. RAS allows remote dial-up (Telecom/PBX) or VPN connections.

Securing Connectivity

38. Email can be secured using the S/MIME or PGP protocols.
39. Email and instant messaging suffer from undesired messages (spam) and hoaxes.
40. Web connectivity can be secured using HTTPS, SSL, and TLS.
41. Access control includes MAC, DAC, and RBAC (rule-based access control or role-based access control).

ASSESSMENTS AND AUDITS

Intrusion Detection

42. Intrusion detection may be managed by two basic methods: knowledge-based and behavior-based detection.
43. An IDS monitors packet data using behavior-based or knowledge-based methods, operating in network-based or host-based configurations.
44. Honeypots and honeynets are used to study the actions of hackers and to distract them from more valuable data.
45. Incident handling may include detection, deflection, or countermeasures.
46. A security baseline is a measure of normal network activity against which behavior-based IDSs measure network traffic to detect anomalies.
47. Hardening is the process of securing a host, network, or application to resist attacks. Some key services that should be considered during hardening are Web, email, FTP, DNS, NNTP, DHCP, file, print, and data repository servers.

Monitoring Tools

48. Useful network diagnostic tools include the following:
    - Ping
    - Tracert/traceroute
    - Nslookup
    - Netstat
    - IPconfig/IFconfig
    - Telnet
    - SNMP
49. Workstations, servers, and mobile devices (such as PDAs) require configuration to improve security beyond the default.

CRYPTOGRAPHY

Algorithms

50. Symmetric key algorithms depend on a shared single key for encryption and decryption. Examples include DES, 3DES, AES, Blowfish, IDEA, and the Rivest ciphers (RC2, RC4, RC5, and RC6).
51. Asymmetric key algorithms use a public key for encryption and a private key for decryption. Examples include the RSA, Diffie-Hellman, El Gamal, and elliptic curve cryptography standards.
52. A hashing algorithm uses a mathematical formula to verify data integrity. Examples include the SHA and the Message Digest series algorithms (MD2, MD4, and MD5).

Concepts of Using Cryptography

53. Cryptographic encryption improves confidentiality.
54. Error checking within encryption/decryption schemes ensures data integrity. Digital signatures are used to sign data so that the recipient can verify the data's origin.
55. Cryptographic routines can perform user authentication and provide for nonrepudiation of data origin.
56. Cryptographic methods may be used for access control.

Public Key Infrastructure

57. PKI relies on asymmetric key cryptography using certificates issued by an authentication certificate authority (CA) such as VeriSign.
58. Certificates are digitally signed blocks of data that may be used within a PKI setting. Some things to remember about certificates include the following:
    - Certificate policies specify the uses for a certificate and additional technical data.
    - A certificate practice statement (CPS) is a legal document that details the purpose of conveying information using a certificate.
    - Certificates can be revoked before their expiration date.
    - A CRL is used when verification of digital certificate takes place to ensure the validity of a digital certificate.
    - A newer mechanism for identifying revoked certificates is the Online Certificate Status Protocol (OCSP).
59. Certificate authorities may be grouped into several trust models, including the following:
    - S*ingle CA*—Uses a single CA
    - *Hierarchical CA*—Uses a root CA and subordinate CAs
    - *Bridge CA*—Uses a bridge CA and principal CAs
60. IPsec consists of AH, ESP, IPComp, and IKE.

Key Management and Certificate Life Cycle

61. Key management and the certificate life cycle support PKI solutions through the process of creating, using, and then destroying public keys and the digital certificates they are associated with. The life cycle includes the following parts:
    - *Key generation*—A public key pair is created and held by the CA.
    - *Identity submission*—The requesting entity submits its identity to the CA.
    - *Registration*—The CA registers the request and verifies the submission identity.
    - *Certification*—The CA creates a certificate signed by its own digital certificate.
    - *Distribution*—The CA publishes the generated certificate.
    - *Usage*—The receiving entity is authorized to use the certificate only for its intended use.
    - *Revocation and expiration*—The certificate will expire or may be revoked earlier if needed.
    - *Renewal*—If needed, a new key pair can be generated and the certificate renewed.
    - *Recovery*—Recovery is possible if a certifying key is compromised but the holder is still valid and trusted.
    - *Archiving*—The certificates and their uses are stored.
62. Key management may be centralized or decentralized.
63. Key escrow occurs when a CA or other entity maintains a copy of the private key associated with the public key signed by the CA.
64. Multiple key pairs require multiple certificates.

ORGANIZATIONAL SECURITY

Redundancy Planning

65. A disaster recovery plan (DRP) details considerations for backup and restoration, including secure recovery methods. Some of the items within the DRP are impact and risk assessments and service level agreements (SLAs) with suppliers and vendors.
66. A business continuity plan details the procedures to follow to reestablish proper connectivity and the facilities needed to restore data in the event of a catastrophic loss. Items of consideration include network connectivity, facilities, clustering, and fault tolerance.
67. Backups may be full, incremental, differential, daily, or copy.
68. RAID organizes multiple disks into a large, high-performance logical disk.
    - *RAID 0*—Striped disk array without fault tolerance
    - *RAID 1*—Mirroring and duplexing
    - *RAID 5*—Independent data disks with distributed parity blocks

Security Policies and Procedures

69. Security policies define guidelines and specifications for general types of security considerations. Policies include risk assessment, security, acceptable use, and compliance. Procedures are step-by-step items defined within each policy that specify the responsible agents, actions to be taken, and methods for proper reporting.
70. Risk identification includes asset identification, risk assessment, threat identification and classification, and identification of vulnerabilities.
71. Education is required to ensure that users are aware of required and recommended security guidelines.
72. All aspects of security must be documented, including security policies, architecture documentation, and retention and disposal procedures for each form of documentation.
73. Computer forensic analysis includes the need to establish a clear chain of custody, properly collect the evidence, correctly perform the investigation, document all actions and findings, preserve all evidence and documentation, and prepare to provide expert testimony or consultation if required.