The Security+ Cram Sheet

GENERAL SECURITY CONCEPTS

1. Access control includes MAC, DAC, and RBAC (Rule-Based Access Control or Role-Based Access Control)
2. 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 v5 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.
3. Nonessential services and protocols should be disabled, which requires an understanding of the following:
   - The role of each server, along with its current configuration
   - Required or critical services, protocols, and applications
   - Configuration changes that should be made to existing servers

ATTACKS

4. 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
5. A back door allows access to a system without normal security checks.
6. Spoofing is the process of making data look as if it came from somewhere other than its origin.
7. Man-in-the-middle attacks involve the interception of traffic between two systems using a third system pretending to be the others.
8. Replay attacks involve the reposting of captured data.
9. TCP/IP hijacking involves taking control of a TCP/IP session.
10. Mathematical attacks involve cryptographic key cracking.
11. Password-guessing, brute-force, and dictionary attacks involve repeated guessing of logons and passwords.
12. Forms of malicious code include the following:
    - *Viruses*—Infect systems and spread copies of themselves
    - *Trojan horses*—Disguise malicious code within apparently useful applications
    - *Logic bombs*—Trigger on a particular condition
    - *Worms*—Self-replicating forms of other types of malicious code
    - *Java and ActiveX controls*—Automatically execute when sent via email
13. Social engineering involves manipulating human psychology to gain access to something of value.

AUDITING

14. Auditing is the process of tracking user actions on the network.
15. System scanning involves probing service ports.

COMMUNICATION SECURITY

REMOTE ACCESS

16. 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
17. VPN connections use PPTP or L2TP connectivity.
18. SSH functions as a secure Telnet.

SECURING CONNECTIVITY

19. Email can be secured using the S/MIME or PGP protocols.
20. Email and Instant Messaging suffer from undesired messages (spam) and hoaxes.
21. Web connectivity can be secured using HTTPS, SSL, and TLS.

ONLINE VULNERABILITIES

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

INFRASTRUCTURE SECURITY

BASIC NETWORK SECURITY DEVICES

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. Routers forward packets between subnets (Network layer, layer 3) using the following:
    - RIP
    - IGRP
    - EIGRP
    - OSPF
    - BGP
    - EGP
    - IS-IS
27. Switches segment broadcast networks (Data Link layer, layer 2).
28. Wireless devices provide broadcast-based connectivity.
29. Modems allow connection through audio telephony.
30. RAS allows remote dial-up (Telecom/PBX) or VPN connections.
31. Useful network diagnostic tools include the following:
    - Ping
    - Tracert/traceroute
    - Nslookup
    - Netstat
    - IPConfig/ifconfig
    - Telnet
    - SNMP
32. Workstations, servers, and mobile devices (such as PDAs) require configuration to improve security beyond the default.

MEDIA

33. The two main types of coaxial cable (coax) are 10Base2 (Thinnet) and 10Base5 (Thicknet).
34. Twisted pair cable is either unshielded (UTP) or shielded (STP). Both come in two speeds: Cat3 (10Mbps) or Cat5 (100Mbps).
35. Fiber-optic cable (fiber) speeds range from 100Mbps to 2Gbps (with higher speeds in the works).
36. Removable media includes tape, recordable compact discs (CD-R), hard drives, diskettes, flashcards, and smartcards.
37. Backups may be full, incremental, differential, or copy.

SECURITY TOPOLOGIES

38. Security zones support the management of a bastion host and screened host or screened subnet gateways.
39. Networks may be divided into intranets, extranets, DMZs, and the Internet.
40. A VLAN allows for computers on the same physical segment to be on different logical segments.
41. Network Address Translation (NAT) devices translate traffic between public and private address schemes.

42. Tunneling is the process of transmitting data encapsulated within a second protocol to prevent direct eavesdropping using a packet sniffer.

INTRUSION 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.

BASICS OF CRYPTOGRAPHY

ALGORITHMS

48. 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).
49. 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).
50. 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.

CONCEPTS OF USING CRYPTOGRAPHY

51. Cryptographic encryption improves confidentiality.
52. 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.
53. Cryptographic routines can perform user authentication and provide for nonrepudiation of data origin.
54. Cryptographic methods may be used for access control.

PUBLIC KEY INFRASTRUCTURE (PKI)

55. PKI relies on asymmetric-key cryptography using certificates issued by an authentication Certificate Authority (CA) such as VeriSign.
56. 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 as well as 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.
57. Certificate Authorities may be grouped into several trust models, including the following:
    - *Single CA*—Uses a single CA
    - *Hierarchical CA*—Uses a root CA and subordinate CAs
    - *Bridge CA*—Uses a bridge CA and principal CAs
58. The IETF Working Group on X.509 standards for PKI is PKIX.
59. IPSec consists of AH, ESP, IPComp, and IKE.

KEY MANAGEMENT AND CERTIFICATE LIFECYCLE

60. Key management and the certificate lifecycle support PKI solutions through the process of creating, using, and then destroying public keys and the digital certificates they are associated with. The lifecycle 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.
61. Key management may be either centralized or decentralized.
62. An escrow agent maintains a copy of the private key signed by the CA.
63. Multiple key pairs will require multiple certificates.

OPERATIONAL/ORGANIZATIONAL SECURITY

PHYSICAL SECURITY

64. Access control includes considerations of direct access, network access, facilities, and the environment supporting a system.
65. Social engineering involves extracting useful information from an authorized user, whereas reverse social engineering involves convincing an authorized user of the attacker's authorization or expertise so that the user will ask for assistance.
66. 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.
67. A business continuity plan details the procedures to follow in order to reestablish proper connectivity as well as the facilities needed to restore data in the event of a catastrophic loss. Items of consideration include network connectivity, facilities, clustering, and fault tolerance.

SECURITY POLICIES AND PROCEDURES

68. Security policies define guidelines and specifications for general types of security considerations. Procedures are step-by-step items defined within each policy that specify the responsible agents, actions to be taken, and methods for proper reporting. Procedures must be followed. Policies include risk assessment, security, acceptable use, and compliance. Focus details may include due care, privacy, separation of duties, need to know, password management, retention, disposal and destruction, incident response, and Human Resources policies.
69. Privilege management may be user based, group based, or role based, reflecting a MAC, DAC, or RBAC configuration.
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, as well as 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.