CompTIA Linux+ Outline

Domain 1.0: General Security Concepts

1.1 Recognize and be able to differentiate and explain the following access control models: MAC, DAC, RBAC.

1.2 Recognize and be able to differentiate and explain the following methods of authentication: Kerberos, CHAP (Challenge Handshake Authentication Protocol), Certificates, Username / Password, Tokens, Multi-factor, Mutual, Biometrics.

1.3 Identify non-essential services and protocols and know what actions to take to reduce the risks of those services and protocols.

1.4 Recognize various attacks and specify the appropriate actions to take to mitigate vulnerability and risk.

1.5 Recognize the following types of malicious code and specify the appropriate actions to take to mitigate vulnerability and risk: Viruses, Trojan Horses, Logic Bombs, and Worms.

1.6 Understand the concept of and know how reduce the risks of social engineering.

1.7 Understand the concept and significance of auditing, logging and system scanning.

Domain 2.0: Communication Security

2.1 Recognize and understand the administration of the following types of remote access: 802.1x, VPN (Virtual Private Network)>, RADIUS (Remote Authentication Dial-In User Service), TACACS (Terminal Access Controller Access Control System), L2TP / PPTP (Layer Two Tunneling Protocol / Point to Point Tunneling Protocol), SSH (Secure Shell), IPSEC (Internet Protocol Security), Vulnerabilities.

2.2 Recognize and understand the administration of the following email security concepts: S/MIME (Secure Multipurpose Internet Mail Extensions), PGP (Pretty Good Privacy) like technologies, Vulnerabilities (SPAM and Hoaxes).

2.3 Recognize and understand the administration of the following Internet security concepts: SSL / TLS (Secure Sockets Layer / Transport Layer Security), HTTP/S (Hypertext Transfer Protocol / Hypertext Transfer Protocol over Secure Sockets Layer), Instant Messaging (Vulnerabilities, Packet Sniffing, Privacy), Vulnerabilities (Java Script, ActiveX, Buffer Overflows, Cookies, Signed Applets, CGI (Common Gateway Interface), SMTP (Simple Mail Transfer Protocol) Relay.

Domain 2.0: Communication Security Contd.

2.1 Recognize and understand the administration of the following directory security concepts: SSL / TLS (Secure Sockets Layer / Transport Layer Security), LDAP (Lightweight Directory Access Protocol).

2.2 Recognize and understand the administration of the following file transfer protocols and concepts: S/FTP (File Transfer Protocol), Blind FTP (File Transfer Protocol) / Anonymous, File Sharing, Vulnerabilities (Packet sniffing, 8.3 Naming Conventions).

2.3 Recognize and understand the administration of the following wireless technologies and concepts: WTLS (Wireless Transport Layer Security), 802.11 and 802.11x, WEP / WAP (Wired Equivalent Privacy / Wireless Application Protocol), Vulnerabilities (Site Surveys).

Domain 3.0: Infrastructure Security

3.1 Understand security concerns and concepts of the following types of devices: Firewalls, Routers, Switches, Wireless, Modems, RAS, Telecom/PBX, VPN, IDS, Network Monitoring/Diagnostic, Workstations, Servers, and Mobile Devices.

3.2 Understand the security concerns for the following types of media: Coax, UTP/STP, Fiber, Removable media (tape, CDR, Hard drives, diskettes, flashcards, smartcards).

3.3 Understand the concepts behind the following kinds of security topologies: Security Zones (DMZ, Intranet, Extranet), VLANs (Virtual Local Area Network), NAT (Network Address Translation), Tunneling.

3.4 Differentiate the following types of intrusion detection, be able to explain the concepts of each type, and understand the implementation and configuration of each kind of intrusion detection system: Network Based (Active Detection, Passive Detection), Host Based (Active Detection, Passive Detection), Honey Pots, Incident Response.

3.5 Understand the following concepts of security baselines, be able to explain what a security baseline is, and understand the implementation and configuration of each kind of intrusion detection system: OS / NOS (Operating System / Network Operating System) Hardening (File System, Updates (hotfixes, service packs, patches)), Network Hardening, Application Hardening, Updates (Hotfixes, Service Packs, Patches), Web Servers, E-mail Servers, FTP (File Transfer Protocol) Servers, DNS (Domain Name Service) Servers, NNTP (Network News Transfer Protocol) Servers, File / Print Servers, DHCP (Dynamic Host Configuration Protocol) Servers, Data Repositories.

Domain 4.0: User Management

4.1 Create and delete users.

Domain 5.0: Maintaining a Linux System

5.1 Create and manage local storage devices and file systems (e.g. fsck, fdisk, mkfs).

5.2 Verify user and root cron jobs and understand the function of cron.

5.3 Identify core dumps and remove or forward as appropriate.

5.4 Run and interpret ifconfig.

5.5 Download and install patches and updates (e.g., packages, tgz).

5.6 Differentiate core services from non-critical services (e.g., ps, PID, PPID, init, timer).

5.7 Identify, execute and kill processes (ps, kill, killall).

5.8 Monitor system log files regularly for errors, logins, and unusual activity.

5.9 Document work performed on a system.

5.10 Perform and verify backups and restores.

5.11 Perform and verify security best practices (e.g., passwords, physical environments).

5.12 Assess security risks (e.g., location, sensitive data, file system permissions, remove/disable unused accounts, audit system services/programs).

5.13 Set daemon and process permissions (e.g., SUID - SGID - Owner/groups).

5.14 Identify and locate the problem by determining whether the problem is hardware, operating system, application software, configuration, or the user.

5.15 Describe troubleshooting best practices (i.e., methodology).

5.16 Examine and edit configuration files based on symptoms of a problem using system utilities.

5.17 Examine, start, and stop processes based on the signs and symptoms of a problem.

5.18 Use system status tools to examine system resources and statuses (e.g., fsck, setserial).

5.19 Use systems boot disk(s) and root disk on workstation and server to diagnose and rescue file system.

5.20 Inspect and determine cause of errors from system log files.

5.21 Use disk utilities to solve file system problems (e.g., mount, umount).

5.22 Resolve problems based on user feedback (e.g., rights, unable to login to the system, unable to print, unable to receive or transmit mail).

5.23 Recognize common errors (e.g., package dependencies, library errors, version conflicts).

5.24 Take appropriate action on boot errors (e.g., LILO, bootstrap).

Domain 5.0: Maintaining a Linux System Contd.

5.25 Identify backup and restore errors.

5.26 Identify application failure on server (e.g., Web page, telnet, ftp, pop3, snmp).

5.27 Identify and use trouble shooting commands (e.g., locate, find, grep, ? , <, >, >>, cat, tail).

5.28 Locate troubleshooting resources and update as allowable (e.g., Web, man pages, howtos, infopages, LUGs).

5.29 Use network utilities to identify network and connectivity problems (e.g., ping, route, traceroute, netstat, Isof).

Domain 6.0: Identify, Install, and Maintain System Hardware

6.1 Identify basic terms, concepts, and functions of system components, including how each component should work during normal operation and during the boot process.

6.2 Assure that system hardware is configured correctly prior to installation (e.g., IRQs, BIOS, DMA, SCSI settings, cabling) by identifying proper procedures for installing and configuring ATA devices.

6.3 Assure that system hardware is configured correctly prior to installation (e.g., IRQs, BIOS, DMA, SCSI settings, cabling) by identifying proper procedures for installing and configuring SCSI and IEEE 1394 devices.

6.4 Assure that system hardware is configured correctly prior to installation (e.g., IRQs, BIOS, DMA, SCSI, cabling) settings by identifying proper procedures for installing and configuring peripheral devices.

6.5 Assure that system hardware is configured correctly prior to installation (e.g., IRQs, BIOS, DMA, SCSI, cabling) settings by identifying available IRQs, DMAs, and I/O addresses and procedures for device installation and configuration.

6.6 Remove and replace hardware and accessories (e.g., cables and components) based on symptoms of a problem by identifying basic procedures for adding and removing field replaceable components.

6.7 Remove and replace hardware and accessories (e.g., cables and components) based on symptoms of a problem by identifying common symptoms and problems associated with each component and how to troubleshoot and isolate the problems.

<u>Domain 6.0</u>: <u>Identify, Install, and Maintain System Hardware</u>

6.8 Identify basic networking concepts, including how a network works.

6.9 Identify proper procedures for diagnosing and troubleshooting ATA devices.

6.10 Identify proper procedures for diagnosing and troubleshooting SCSI devices.

6.11 Identify proper procedures for diagnosing and troubleshooting peripheral devices.

6.12 Identify proper procedures for diagnosing and troubleshooting core system hardware.

6.13 Identify and maintain mobile system hardware (e.g., PCMCIA, APM).