

Documentation Checklist**Comments**

- ___ Wide area network (WAN) diagrams showing all network locations including WAN transmission methods used (X.25, frame-relay, T-1, dial-up, etc.)

- ___ Detailed network diagrams for all local area networks within the audit scope, including all significant nodes such as routers, firewalls, gateways, file servers, host processing systems (Unix, mainframe, etc.), with network and node IP addresses and link transmission methods (ethernet, token ring, etc.)

- ___ Narrative descriptions of significant applications in use, along with descriptions of TCP/IP services (telnet, ftp, nfs, tftp, etc.) necessary to support these applications

- ___ Printouts of network control files for significant systems in audit scope (/etc/inetd.conf, /etc/hosts.equiv, /etc/exports, etc.)

- ___ Printout of router configuration files for routers which connect to external networks or are used to segment server networks from the user networks

- ___ Printout of firewall configuration files and log files

- ___ Organizational charts and job descriptions for personnel supporting the networks

- ___ Network operations and security policies and procedures

Index to Audit Procedures

- I. Physical Security—Overview
Page: ____
Coverage/Remarks:
- II. TCP/IP Link Layer Security
Page: ____
Coverage/Remarks:
- III. Network Layer Security
Page: ____
Coverage/Remarks:
- IV. Transport Layer Security
Page: ____
Coverage/Remarks:
- V. Application Layer Security
Page: ____
Coverage/Remarks:
- VI. Internet and Firewall Configuration Security
Page: ____
Coverage/Remarks:
- VII. Web Services Security
Page: ____
Coverage/Remarks:

Audit Procedures

I. Physical Security—Overview

Purpose: To determine that adequate physical security is in place over network transmission media and network devices to prevent unauthorized access and/or modifications to systems and data.

- A. Review WAN diagrams to identify networks and locations with significant host systems. Assess security of these operations centers.

Remarks:

- B. Obtain floor plan diagrams of the wiring and connectivity of networks within the scope of the review and perform the following:

1. Review workstation wiring diagrams. Observe wiring used to determine that workstations are protected from interference from other systems or devices which may degrade the transmission quality.

Remarks:

2. Determine that wiring hubs and concentrators are located in secured areas accessible only by network support personnel.

Remarks:

3. Observe the network and systems operations center to determine that physical access is granted on an as-needed basis and is well controlled.

Remarks:

4. Determine whether network management software is used throughout the network to monitor the network's physical connections and traffic load proactively.

Remarks:

5. Observe and assess physical access controls over satellite and microwave transmission antenna to determine that access is restricted.

Remarks:

- C. Review wiring diagrams and compare them to a physical observation of hub connection labeling, multiplexor link labeling, modem labels, etc., to ensure that all physical connections are authorized and documented.

Remarks:

II. TCP/IP Link Layer Security

Purpose: To determine that the security objectives of the link layer are being adequately met.

A. Using the network diagrams, identify the LAN link protocols (such as ethernet or token ring) and WAN link protocols (such as X.25, Frame-relay, and T-1) in use:

1. Assess the need for bridge security filtering on link addresses to protect confidential portions of the network.

Remarks:

2. Determine whether link-level encryption is needed and is being properly used to protect transmissions across LANs and public WAN links.

Remarks:

B. Identify all dial-up links and dial-up protocols in use (SLIP, PPP).

1. For SLIP links, determine that the PAP authentication method is supplemented by procedures which ensure that passwords are changed regularly; formats are secure; SLIP connections are logged in the dial-up, access server log; and the log is reviewed regularly.

Remarks:

2. For PPP links, determine that CHAP authentication is being used effectively.

Remarks:

3. If Tacacs authentication is being used to support remote access security, review effectiveness of Tacacs configuration and physical and logical access controls over the Tacacs security server.

Remarks:

III. Network Layer Security

Purpose: To determine that network transmissions are properly and securely forwarded to their authorized destinations through authorized network routes.

A. Obtain detailed diagrams of the networks, including network and node IP addresses and authorized host names (DNS names), and perform the following:

1. Determine whether legal IP addresses and DNS names are being used and whether the organization is following a well-organized naming and IP-addressing and subnetworking scheme to prevent duplicate network and host IP addresses.

Remarks:

2. From a network workstation on each significant network, use the traceroute utility (tracert in Windows 95) to document the network path from the workstation to several of the network nodes listed in the documentation tracert (host name or IP address). Compare the output from the tracert command to the network documentation to ensure that it accurately documents routers and systems in the network path. Investigate any undocumented routes or intermediate nodes which are not routers.

Remarks:

3. Also using the traceroute utility, traceroute to an unreachable host system to determine that the maximum hops feature is active (maximum is usually 30).

Remarks:

4. Use the ping utility to test the accuracy of IP addresses and host names of systems listed in the systems diagrams and documentation ping (host name or IP address). Investigate and resolve any unresponding systems.

Remarks:

5. Obtain a log-in account on the significant host systems. Log in and execute the commands netstat, -rn, and netstat -r to list out the routing table for that node by system name (-n) and by IP address (-r). Compare

the output of these commands to the network documentation to ensure that the documentation is accurate.

Remarks:

- B. Identify all routers which connect the network to an external network, or a network managed by another organization, and routers which connect the host systems and server networks to the user networks and external networks. Obtain printouts of the network configuration files and perform the following:
1. Determine that routing table update packets—IGP and EGP (used for dynamic routing)—are filtered and dropped to prevent them from entering the internal network.

Remarks:
 2. Determine that IGP and EGP updates are deactivated and that effective procedures are in place to ensure that accurate static routing tables are maintained for routers.

Remarks:
 3. Determine whether routers have defined static paths to allow traffic to pass from only a specified router on the connected external network (often the case when connecting to vendor networks, affiliated businesses, etc.).

Remarks:
 4. Review the configuration to ensure that packets using the loose source routing option are filtered and dropped to prevent them from entering the internal network.

Remarks:
 5. Also review the router configuration file to ensure that the router ignores ICMP redirect messages which could be used to modify the routing table.

Remarks:

6. Ensure that a filter rule has been implemented to detect packets on the external interface that have a source IP address claiming to originate on the internal network (detects IP address spoofing).

Remarks:

- C. Review and assess router management and access controls for all routers, especially routers which connect the network to an external network or one managed by another organization, and routers which connect the host systems and server networks to the user networks and external networks. Obtain a printout of the router configuration file and perform the following:

1. Review and assess administrative controls over user access and maintenance to routers (work requests, operating system upgrades, sign-offs, etc.).

Remarks:

2. Review configuration backup procedures to ensure that the configuration is backed up securely and is reinstalled subsequent to operating system upgrades.

Remarks:

3. Determine that all telnet and console access ports are password protected by router passwords or Tacacs authentication methods.

Remarks:

4. Ensure that all router passwords are stored in encrypted form, using a secure encryption algorithm.

Remarks:

5. Determine whether telnet access to the router has been completely disabled on routers which connect to external networks. (In most cases it should be disabled to lessen the risk of telnet access from the external network.)

Remarks:

6. Assess the appropriateness of granting privileged access to modify the router configuration file.

Remarks:

7. If Tacacs is used, review operating system security over the Tacacs server; also ensure that administrative controls and backup controls over the Tacacs authentication database are adequate.

Remarks:

8. Review snmp access to the router to ensure that snmp sets are restricted to authorized control workstations and that the default community string passwords have been changed from their default values to more secure, confidential formats.

Remarks:

9. Assess the need and use of access lists to restrict telnet and snmp access to the router.

Remarks:

10. Review for logging of router access and access violations; determine that logs are reviewed and followed up in a timely manner.

Remarks:

11. Using telnet, attempt to connect to a sample of routers to ensure that access is properly restricted with passwords. Verify that a warning banner is in effect to inform users that access to the router is restricted and that their actions are being monitored.

Remarks:

- D. Obtain the network start-up scripts for the significant host systems (Unix: /etc/rc.tcpip, rc.local, or rc.net) and review them to ensure that the gated and

routed daemon programs are not activated. (Routing on host systems is not recommended for operational and security reasons.)

Remarks:

IV. Transport Layer Security

Purpose: To determine that application port numbers are assigned and controlled in a secure manner and that applications utilize the transmission integrity and acknowledgment controls of the transport layer.

- A. Obtain a printout of the services file (Unix—/etc/services) and review it to ensure that no in-house-developed applications are assigned to port numbers less than or equal to TCP or UDP port number 1023. For any in-house-developed or third-party applications that use UDP, determine whether effective application program controls are in place to perform transmission integrity and acknowledgment controls.

Remarks:

- B. Review the contents of start-up scripts (Unix—/etc/rc or /etc/inetd.conf) on significant servers and host systems:

1. Identify high-risk, active applications along with their TCP or UDP port number assignments (NFS, rsh, rlogin, tftp, etc.).

Remarks:

2. Obtain the configuration file for the router or routers which connect these systems and networks to the user networks and wide area networks. Determine that the router(s) is configured to detect and drop high-risk network traffic based on TCP or UDP port numbers. This check ensures that an unauthorized user cannot take advantage of security exposures inherent in these applications.

Remarks:

3. Determine whether router port number filters are properly set to read the status flag on packets to allow return packets on connections initiated from the internal network to pass through. Make sure the filters block packets trying to initiate a connection from an external network to the internal network.

Remarks:

4. Examine the router configuration file for routers that connect server and user networks to external networks. Ensure that filter rules are established to filter and drop incoming and outgoing application packets based on their UDP and TCP port numbers. The following types of traffic are often filtered and dropped on external routers. Additional filters should be used based on the types of traffic and applications prevalent on the network:
 - a. udp 42 DNS name server
Remarks:
 - b. udp and tcp 53 DNS zone transfers
Remarks:
 - c. udp 67 bootp
Remarks:
 - d. udp 69 tftp
Remarks:
 - e. ucp 79 finger
Remarks:
 - f. tcp 87 link
Remarks:
 - g. tcp 95 supdup (super-duper telnet)
Remarks:
 - h. udp and tcp 111 portmapper for Remote Procedure Call (RPC)
Remarks:

i. udp 161 snmp (get, get-next, and set)

Remarks:

j. udp 162 snmp (traps)

Remarks:

k. tcp 512 rexec

Remarks:

l. tcp 513 rlogin

Remarks:

m. tcp 514 rsh

Remarks:

n. udp 514 syslog

Remarks:

o. tcp 515 lpd

Remarks:

p. udp 2049 NFS

Remarks:

q. tcp 6000+n X Windows

Remarks:

5. Review TCP connection monitoring procedures. While logged in to a host system, use the netstat -a command to review active connections to host systems. Conduct this review with the system administrator.

Remarks:

6. If Remote Procedure Call (RPC) programs are used, review network control procedures to monitor and control RPC program numbers and monitoring techniques.

Remarks:

V. Application Layer Security

Purpose: To ensure that proper controls have been implemented to secure the active TCP/IP applications.

A. Obtain the system start-up scripts and server program control files (Unix: /etc/rc.tcpip, or /etc/rc.local and /etc/inetd.conf) for the significant systems and servers. Review them to determine which applications are active. (Inactive applications are commented out by placing a # sign in front of their entry.) Also, use the ps command to list all active processes to detect any applications that were started manually from the command line rather than from a start-up script. For each application, perform the following procedures:

1. Terminal Emulation Programs

a. telnet—Determine whether all telnet users are assigned well-controlled passwords and IDs. Ascertain that any telnet access from external networks, such as the Internet, is supplemented by additional security, such as smart-cards or challenge-response authentication (to overcome the cleartext transmission of telnet passwords and IDs). Cross-reference to the host operating system and log-in security workpapers. Assess whether telnet should be completely deactivated on sensitive network nodes—such as firewalls, gateways, and routers—that connect to external networks. Cross-reference to Tacacs security workpapers as appropriate.

Remarks:

b. X-Windows—Using the network configuration diagrams, identify all X workstations in use and perform the following procedures.

i. Review the xdm window manager program start-up script on the X workstation for the xhost entry to determine whether the - activating access control lists or + sign (designating all hosts as trusted) is being used.

Remarks:

ii. After determining if access control has been activated, review the contents of the file /etc/X0.hosts, which lists out

the authorized X client systems. Identify each client system and assess the appropriateness of its authorized X clients.

Remarks:

- iii. Review the xdm configuration file `/usr/lib/X11/xdm-config` for the entry that starts the magic cookie authentication program. If it is active, review and assess procedures used to distribute the magic cookie bit string to X client systems.

Remarks:

2. File Transfer Programs

- a. ftp—Determine whether all ftp users are assigned well-controlled passwords and IDs and whether any ftp access from external networks, such as the Internet, is supplemented by additional security such as smart-cards. Cross-reference to the operating system's, log-in security workpapers.
 - i. Review the ftp entry in `/etc/inetd.conf` for the `-l`, `-e`, `-t`, and `-u` security options.

Remarks:

- ii. Review user home directories for `.netrc` files. Review the contents of this file to ensure that only authorized external users and systems are listed. Determine whether `.netrc` files are owned by the root account and system group with no world-writeable access, and whether all users have a blank `.netrc` file in their home directories, at a minimum.

Remarks:

- iii. Review the contents `/etc/ftpusers` to ensure that it includes all of the system accounts and any user accounts which do not need to use ftp.

Remarks:

b. Anonymous ftp—Ensure that anonymous ftp is not being used on systems which provide “mission critical” processing. If anonymous ftp is being used, review the following:

i. A log-in-disabled account called ftp is in the /etc/passwd file, and its home directory is /users/home/ftp. This should be owned by the root account and system group with 555 permissions. Its shell program is /bin/false, and it cannot be listed in /etc/ftpusers.

Remarks:

ii. The /users/home/ftp directory should include the subdirectories /etc, with a false password and group file owned by the root account and system group with 444 permissions and /bin, which should normally include only the ls command file owned by the root account with 111 permissions.

Remarks:

iii. The /pub directory should contain the data to be provided as the anonymous service and should be owned by the root account and system group with 555 permissions.

Remarks:

iv. Test the security of anonymous ftp by logging in under anonymous ftp and attempting to download the true /etc/passwd file.

Remarks:

c. tftp—Review the tftp entry in /etc/inetd.conf to determine whether tftp is started with the -s secure flag to limit it to the boot directory noted (usually /tftpboot), or whether chroot mode is used with a log-in-disabled account, called tftp, with the /tftpboot directory located in /users/tftp home directory. Review the contents of the /users/tftp home directory to ensure that it has only necessary system boot files. If tftp is active, cross-reference the workpapers to a review of routers which connect to external networks, to

ensure that filter rules are implemented to drop incoming or outgoing tftp packets.

Remarks:

- d. bootp—If bootp is active, cross-reference the workpapers to a review of routers which connect to external networks to ensure that filter rules are implemented to drop incoming or outgoing bootp packets.

Remarks:

- e. NFS—Review the network start-up scripts (/etc/rc.tcpip or /etc/rc.local) to determine whether NFS is active. Obtain a copy of the NFS control file /etc/exports and perform the following:
 - i. Determine whether any file system listed as a mounted directory is authorized for this purpose.

Remarks:

- ii. Determine whether access entries are used to restrict each mounted file system to an authorized client system.

Remarks:

- iii. Review and assess use of the root option, granting client systems' root users root access to the mounted file system.

Remarks:

- iv. Determine whether the RO (read-only option) is used and that executables and setuid and setgid programs are not located in mounted directories.

Remarks:

- v. On networks using NFS, cross-reference the workpapers to a review of routers which connect to external networks to

ensure that filter rules are implemented to drop incoming or outgoing NFS packets.

Remarks:

- f. PC-NFS—Review the network start-up scripts (/etc/rc.tcpip or /etc/rc.local) to determine whether PC-NFS is active. Review the /etc/exports file for the AUTH UNIX option, which requires a PC-NFS user to have authentication through the Unix log-in process before accessing mounted file systems.

Remarks:

B. Berkeley “r” commands

1. rlogin—Determine whether all rlogin users are assigned well-controlled passwords and IDs. Cross-reference workpapers to a review of the host system’s log-in security. Review the contents of the /etc/hosts.equiv file to ensure that the + sign is not being used (which designates all systems as trusted systems) and that all systems or NIS netgroups listed are authorized systems and users located on the same IP network, under the same control as the system under audit. Review user home directories for .rhosts files. Examine the contents of these files to ensure that all users listed are located on systems on the local IP network. Also determine that, at a minimum, users have empty .rhost files in their home directories owned by the root directory and system group with 750 permissions. Cross-reference the workpapers to a review of routers which connect to external networks to ensure that filter rules are implemented to drop incoming or outgoing rlogin packets.

Remarks:

2. rsh—Repeat rlogin steps.

Remarks:

3. rcp—Repeat rlogin steps.

Remarks:

4. rexec—Should almost always be disabled in /etc/inetd.conf due to security weaknesses. If it is active, determine whether all rexec users are assigned well-controlled passwords and IDs. Cross-reference the workpapers to a review of the host system, log-in security, and routers which connect to external networks, to ensure that filter rules are implemented to drop incoming rexec packets.

Remarks:

C. Others

1. snmp—Review the start-up scripts (Unix: /etc/rc.tcpip or /etc/rc.local) to determine whether the snmp daemon is active. Normally, snmp should be used for network management purposes. If it is not active, inquire about the reason why and determine what other network management procedures are used to monitor the network. Using the network configuration diagram, identify the snmp manager (control workstation) and agents (host systems and network devices) on each network under review. Obtain the control file /etc/snmpd.com for each manager and agent on the network and perform the following:

- a. Determine whether all agent systems listed in the manager's control file are authentic members of the manager's snmp network.

Remarks:

- b. Determine whether only the authorized manager system is listed in the agents' control file.

Remarks:

- c. Observe the format of the community string passwords used, to ensure that the default community strings have been changed to more secure values.

Remarks:

- d. Determine whether special-privilege access is required for sending set commands to snmp agents from the manager. Obtain the /etc/snmp.trap file on the agents and determine whether the managers listed (for the agent to send traps to) are authorized

manager workstations on the local network. Also verify that secure community string passwords are being used.

Remarks:

- e. Cross-reference the workpapers to a review of routers which connect to external networks, to ensure that filter rules are implemented to drop incoming snmp packets to prevent an external system from using the set command to change the configuration of network and host systems on the local network.

Remarks:

2. smtp—Review the network start-up files (Unix: /etc/rc.tcpip or /etc/rc.local) to determine that the sendmail program is not active on internal systems. (It should be restricted to an e-mail gateway.) Review /etc/inetd.conf to ensure that the smtpd server program is not active on internal systems. Determine whether PEM or PGP authentication is used to ensure the authenticity and confidentiality of mail messages transmitted via the Internet.

Remarks:

3. nntp—Review the network start-up files (Unix: /etc/rc.tcpip or /etc/rc.local) to determine that the nntp file is not active on internal systems. (It should be restricted to a news server). Determine that PEM security is used to authenticate nntp clients and servers and that messages are encrypted.

Remarks:

4. DNS—Review network documentation to determine whether networks are using well-organized, registered DNS domains. Determine whether each DNS domain has a primary DNS server as well as a secondary DNS server, and that each has a well-secured operating system and is also physically secured. Review the primary DNS server's configuration to ensure that DNS zone transfers are restricted to the secondary server. Cross-reference the workpapers to a review of router filters on routers which connect to external networks to ensure that DNS zone transfer packets are detected and dropped at the router. Determine whether the

version of DNS in use supports inverse queries to verify host names against IP addresses.

Remarks:

5. Obtain detailed documentation of how the server program is started to gain an understanding of the startup process and how it is executed for third-party or in-house-developed applications for programs such as Oracle, Sybase, SAP R/3, etc. Obtain printouts of the scripts that start up the server and identify all significant control parameters. Compare these parameters to their expected, secure values and assess the appropriateness of the settings.

Remarks:

VI. Internet and Firewall Configuration Security

Purpose: To determine whether the connection to an external network, such as the Internet, is secured with an application gateway firewall and that the firewall is properly configured to secure Internet traffic.

A. Obtain a detailed network diagram of the firewall network configuration (router, DNS server, firewall host system, Web server, other) with host names and IP addresses.

1. Determine whether all of the physical and logical components of the firewall network are managed by the same group, and that the control procedures and policies are well documented and regularly updated.

Remarks:

2. Review firewall network operations and control procedures to ensure that procedures are documented and in place to back up security and configuration files and properly restore these files after system failures, or software or operating system upgrades.

Remarks:

3. Using the network diagram as a guide, observe the physical connections between the various components, noting proper labeling of all physical connections and consistency of physical connections with the diagram. Investigate any connections which link portions of the firewall network to networks or links not documented in the network diagram.

- a. Determine whether the firewall has only two network interfaces—the link to the external network and the link to the internal network.

Remarks:

- b. Determine whether the router which connects to the Internet has only two interfaces—one that connects to the Internet service provider and a second that connects directly to the firewall or one which connects to the sacrificial network outside of the firewall.

Remarks:

- c. For all systems (Web server, DNS server, router, firewall) on the sacrificial network, determine that each component has no links to any other parts of the internal network or to other networks.

Remarks:

- B. Review the router configuration file for the router that connects to the Internet service provider. Determine whether adequate filters are in place to detect and drop incoming services that are not authorized to be used on any of the components located on the sacrificial network (possibly telnet, snmp, bootp, etc.).

Remarks:

- C. Ensure that the application gateway firewall's host operating system (usually Unix) has been properly modified to disable services that could be used to subvert the security of the firewall software program:

1. Review the `/etc/inetd.conf` file and the `/etc/rc` start-up files to ensure that all standard network services have been disabled by commenting out (#) their entries.

Remarks:

2. Execute the command `netstat` at the firewall operating system prompt and review the output (it should show no routes available) to ensure that IP datagram routing has been disabled in the operating system kernel.

Remarks:

3. Review the contents of the `/etc/hosts.equiv`, `$HOME/.rhosts`, and `$HOME/.netrc` files to ensure that they are empty or do not exist on the system.

Remarks:

4. Review the `/etc/passwd` file to ensure that only the root account and one firewall administration account are active (not including log-in-disabled system accounts `bin`, `wheel`, etc.). Assess controls (passwords, logging, and review) over use of these accounts.

Remarks:

5. Review the directory structure to ensure that no other application programs, language compilers, interpreters, or other utilities are loaded on the system.

Remarks:

- D. Review the configuration of the firewall software. Often, a configuration file can be printed out and reviewed.
 1. Identify all supported and active network application proxies along with the indication of where connections may be initiated. (This may be noted as “trusted network” for connections initiated from the internal network and “untrusted network” for connections initiated from the external network—the Internet.) Compare this to the Internet policy description of authorized services. Investigate any deviations from policy.

Remarks:

2. For all proxies that allow network connections to be initiated from the Internet (telnet, ftp, etc.), ensure that strong password authentication controls are implemented (challenge-response, encryption) or that third-party security schemes have been implemented (SecureID, S/key).

Remarks:

3. For all proxies that allow network connections to be initiated from the Internet there should normally be restrictions (based on IP addresses or host names) on the source of such connections and the systems on the internal network that an Internet user may access. Assess the need for these restrictions and review the configuration of such access controls.

Remarks:

4. Review ID and password controls—authorizations for IDs, password format, and aging controls.

Remarks:

5. Review and assess the use of groups to assign services and access capabilities to users.

Remarks:

6. For generic proxy programs that may be in use, review the port number and IP source and destination restrictions to ensure they are correctly designed to restrict this traffic. Assess the need and implementation of compensating controls such as router filters.

Remarks:

7. For each proxy, determine that adequate logging mechanisms have been activated and that logs are reviewed on a timely basis.

Remarks:

8. Determine whether audit alerts have been adequately designed to alert management on a real-time basis of security events that require prompt attention (alerts such as snmp traps, e-mail messages, pagers, etc.).

Remarks:

9. Identify and assess the appropriateness of administrators' access to view and modify the firewall configuration. Review the configuration change log (many firewall products support this), and investigate several changes with the administrator to ensure that they are authorized changes.

Remarks:

VII. Web Services Security

Purpose: To ensure that the Web site is secured from unauthorized modifications to data and programs supporting World Wide Web services.

- A. Review the network diagram and also observe the physical configuration of the Web server's location on the network:
1. If the Web server provides public access information services, it should be located outside the firewall on the sacrificial network. Filter rules should be implemented on the router which connects the sacrificial network to the Internet to restrict the types of traffic which may access the Web server (tftp, telnet, snmp, etc.).

Remarks:

2. If the Web server is used for commercial transactions, it should usually be located behind the firewall. A router should be situated between the Web server and the rest of the internal network. This router should be configured with restrictive filter rules to control further the traffic coming from the Web server.

Remarks:

3. Ensure that no public access information services are provided on a commercial Web server that is located on the internal side of the firewall.

Remarks:

- B. Review the operating system security of the Web server platform:

1. Review the `/etc/passwd` file to ensure that there are no unnecessary accounts. Unless telnet is offered as a service, there should only be the root account, log-in-disabled system accounts, log-in-disabled application owner accounts for Web services (www, wais, gopher, etc.), and possibly one administrative account.

Remarks:

2. Review `/etc/rc` start-up scripts and the `/etc/inetd.conf` file to determine whether unnecessary network services such as tftp, NFS, or others have

been deactivated (i.e., it would not be desirable to allow Internet users to use telnet to log in to the Web server's operating system).

Remarks:

3. Review the directory structure to ensure that other programs, compilers, and interpreters have been removed.

Remarks:

4. Ensure that directories have maximum permissions of 755.

Remarks:

- C. Review the Web services policies and procedures to identify the authorized Web services. Review the start-up entries in the /etc/rc scripts or the /etc/inetd.conf file to ensure that only authorized Web services are provided.

Remarks:

- D. If telnet is offered as a Web service, do the following:

1. Review the user entries in the /etc/passwd file to ensure that telnet users are pathed to a secure script program rather than one of the command shells.

Remarks:

2. Review the code of the script program to ensure that it performs its stated function and does not include any system commands or escape characters that would allow a user to exit to the operating system.

Remarks:

3. Ensure that the start-up command entry for telnet in the /etc/inetd.conf file includes the -p option, with a port number other than the standard 23 to start telnet on a nonstandard port.

Remarks:

- E. For the wide area information service (wais), perform the following steps:
1. Review the wais start-up entry in the `/etc/inetd.conf` file or in the `/etc/rc` start-up scripts for these options:
 - a. The `-u` option designates that the process will switch owners from the root account to a specified log-in-disabled owner account such as wais. Cross-reference the workpapers to a review of the `/etc/passwd` file.

Remarks:
 - b. The `-l` option should be used to activate detail logging.

Remarks:
 - c. The `-d` option identifies the public wais directory (usually `/usr/local/wais`).

Remarks:
 2. If it is necessary to specify access control for the program, review the variable `SERVSECURITYFILE` in the `server.h` file. This variable points to the access control file used to specify systems by DNS name and IP address that are authorized to access the server. Review and assess the appropriateness of entries in the access control file.

Remarks:
 3. If it is necessary to specify access control for the wais database, review the variable `DATASECURITYFILE` in the `server.h` file. This variable points to the access control file used to specify systems by DNS name and IP address that are authorized to access data sources. Review and assess the appropriateness of entries in this file to ensure that controlled data sources are adequately protected.

Remarks:

- F. If the gopher service is provided, perform the following steps:
1. Review the gopher start-up entry in the `/etc/inetd.conf` file or the `/etc/rc` start-up scripts for these options:
 - a. The `-u` option designates that the process will switch owners from the root account to a specified log-in-disabled owner account such as gopher. Cross-reference the workpapers to a review of the `/etc/passwd` file. The `-u` option is necessary for gopher to run in chroot mode. It restricts users to the `/usr/local/etc/gopher` directory. If the server starts as the nobody user, it cannot use chroot mode.

Remarks:
 - b. The `-l` option should be used to activate detail logging.

Remarks:
 2. Test the effectiveness of the chroot setting by attempting to access other portions of the directory structure.

Remarks:
 3. If it is necessary to set up access control for the gopher server, review the configuration file `gopher.conf` and assess the appropriateness of access rules defined for calling systems.

Remarks:

- G. If http services (standard World Wide Web) are provided, perform the following procedures:
1. Review the http start-up entry in the `/etc/inetd.conf` file or the `/etc/rc` start-up scripts for these options:
 - a. The `-u` option designates that the process will switch owners from the root account to a specified log-in-disabled owner account such as www or http. Cross-reference the workpapers to a review of the `/etc/passwd` file.

Remarks:

- b. The -d option designates the server root directory, usually /usr/local/http.

Remarks:

- 2. Review the directory structure to ensure that the standard structure and permissions are used:

- a. /cgi-bin.

Remarks:

- b. /conf.

Remarks:

- c. /icons.

Remarks:

- d. /logs.

Remarks:

- e. /support.

Remarks:

The directories should be owned by the www (log-in- disabled) account and group with permissions of 755 or less. The control files in the /conf file should be owned by the www account and its group with permissions of 750.

Remarks:

- 3. Review the configuration file httpd.conf for the following entries:

- a. The ID and group ID should designate the Unix http (or www) owner account and group.

Remarks:

- b. The ServerAdmin entry should be the e-mail address of the administrator.

Remarks:

- c. All other entries must be consistent with the startup command in /etc/rc scripts or the /etc/inetd.conf file.

Remarks:

4. Review the srm.conf configuration file for the following entries:

- a. The DocumentRoot entry should indicate /usr/local/httpd/httpdocs to restrict users to the documents directory. (This is a key control since httpd does not operate in chroot mode.)

Remarks:

- b. The UserDir entry should normally be disabled.

Remarks:

- c. The Alias entry should reflect any changes to the standard http directory structure.

Remarks:

5. If access control is necessary (unusual on a public access server but possible on a commerce server), review the following parameters in the access.conf file:

- a. AllowOverride should normally be set to none.

Remarks:

- b. Obtain the password file referenced by the AuthUserFile parameter and the group file referenced by the AuthGroupFile parameter. Use these files to assist in a review of the allow and deny access rules for each directory in the access.conf configuration.

Remarks:

- c. Review the following options parameters:

- i. Indexes should be disabled globally or for any directory that may contain CGI programs.

Remarks:

- ii. FollowSymLinks should be disabled.

Remarks:

- iii. SymLinksIfOwnerMatch should be disabled.

Remarks:

- iv. ExeCGI should be disabled.

Remarks:

- v. IncludesNoExec should always be indicated.

Remarks:

- 6. Review the http server logs to ensure that suspicious events are reviewed.

Remarks:

- H. If CGI programs (Common Gateway Interface) are used in conjunction with the Web services, perform the following steps:

1. Ensure that CGI programs are located only in the /usr/local/httpd/cgi-bin directory owned by the www account and group with permissions of 750.

Remarks:

2. Determine that CGI programs are not setuid or setgid.

Remarks:

3. Review program development standards and quality assurance procedures to control the coding of CGI programs.

Remarks:

4. Review the code of the CGI programs for the following:

- a. System commands (should be very restricted).

Remarks:

- b. Escape characters and variables. (These should be trapped in the beginning of the program code to ensure that they cannot be executed from within the program.)

Remarks: