Expanded Audit Checklist

Center for Internet Security

Gold Standard Benchmark for Cisco IOS

Version 2.1September 2, 2003

Device Name: _____
Local Configuration File: _____
IOS Version: _____
Auditor Name: _____
Date: _____

Use this form to record the data required to configure the audit tool. For yes/no questions, the default answer is shown in upper case and you can circle the value you wish to use. For variable data, the default value is shown and a blank is provided for the value you wish to use. Mandatory items are shown with their required setting. The numbers shown after each question indicate the section number in the benchmark where more information can be found.

1 Level-1

Check rules and data related to system management? (3.1.1) ..... YES

Use local authentication? (3.1.2) ..... (YES/no)

Create new AAA model using local usernames and passwords? (3.1.3) ..... YES

Create local usernames? (3.1.4) ..... YES

Username of user for local authentication? (3.1.5) ..... (username1/_____)

Apply standard SNMP checks? (3.1.6) ..... YES

Disable SNMP server? (3.1.7) ..... (YES/no)

Forbid SNMP read-write? (3.1.8) ..... (YES/no)

Forbid SNMP community string 'public'? (3.1.9) ..... YES

Forbid SNMP community string 'private'? (3.1.10) ..... YES

Require an ACL to be applied for all SNMP access? (3.1.11) ..... (yes/NO)

Specify ACL number to be used for filtering SNMP requests? (3.1.12) .... (99/_____)

Define SNMP ACL? (3.1.13) ..... (yes/NO)

Address block and mask for SNMP access? (3.1.14) .. (192.168.1.0 0.0.0.255/_____)

Apply standard checks to control access to the router? (3.1.15) ..... (YES/no)

Allow Telnet access for remote administration? (3.1.16) ..... (YES/no)

Allow only telnet access for remote login? (3.1.17) ..... YES

Specify maximum allowed exec timeout? (3.1.18) ..... YES

Exec timeout value? (3.1.19) ..... (10 0/_____)

Disable the aux port? (3.1.20) ..... (YES/no)

Use default AAA login authentication on each line? (3.1.21) ..... (YES/no)

Use explicit named AAA login authentication on each line? (3.1.22) ..... (yes/NO)

Name for login AAA list? (3.1.23) ..... (default/_____)

require line passwords? (3.1.24) ..... (YES/no)

Require an enable secret? (3.1.25) ..... YES

Check line password quality? (3.1.26) ..... (YES/no)

Check user password quality? (3.1.27) ..... (YES/no)

Require VTY ACL to be applied? (3.1.28) ..... YES

Specify ACL number to be used for telnet or ssh? (3.1.29) ..... (182/_____)

Define simple (one netblock + one host) VTY ACL? (3.1.30) ..... (YES/no)

Address block and mask for administrative hosts? (3.1.31) ..... (192.168.1.0 0.0.0.255/_____)

Address for administrative host? (3.1.32) ..... (192.168.1.254/_____)

Disable unneeded management services? (3.1.33) ..... (YES/no)

Forbid finger service (on IOS 11)? (3.1.34) ..... YES

Forbid identd service (on IOS 11)? (3.1.35) ..... YES

Forbid finger service (on IOS 12)? (3.1.36) ..... YES

Forbid finger service (on IOS 12)? (3.1.37) ..... YES

Forbid http service? (3.1.38) ..... YES

Encrypt passwords in the configuration? (3.1.39) ..... YES

Check rules and data related to system control? (3.1.40) ..... YES

Synchronize router time via NTP? (3.1.41) ..... (YES/no)

Designate an NTP time server? (3.1.42) ..... YES

Address of first NTP server? (3.1.43) ..... (1.2.3.4/_____)

Designate a second NTP time server? (3.1.44) ..... (YES/no)

Address of second NTP server? (3.1.45) ..... (5.6.7.8/_____)

Designate a third NTP time server? (3.1.46) ..... (YES/no)
Address of third NTP server? (3.1.47) ..... (9.10.11.12/_____)
Apply standard logging rules? (3.1.48) ..... (YES/no)
Use GMT for logging instead of localtime? (3.1.49) ..... (YES/no)
Check timezone and offset? (3.1.50) ..... YES
Forbid summertime clock changes? (3.1.51) ..... YES
Timestamp log messages? (3.1.52) ..... YES
Timestamp debug messages? (3.1.53) ..... YES
enable logging? (3.1.54) ..... YES
Designate syslog server? (3.1.55) ..... YES
Address of syslog server? (3.1.56) ..... (13.14.15.16/_____)
Designate local logging buffer size? (3.1.57) ..... YES
Local log buffer size? (3.1.58) ..... (16000/_____)
Require console logging of critical messages? (3.1.59) ..... YES
Require remote logging of level info or higher? (3.1.60) ..... YES
Disable unneeded control services? (3.1.61) ..... (YES/no)
Forbid small TCP services (on IOS 11)? (3.1.62) ..... YES
Forbid small UDP services (on IOS 11)? (3.1.63) ..... YES
Forbid small TCP services (on IOS 12)? (3.1.64) ..... YES
Forbid small UDP services (on IOS 12)? (3.1.65) ..... YES
Forbid bootp service? (3.1.66) ..... YES
Disable CDP service? (3.1.67) ..... (YES/no)
Forbid config service? (3.1.68) ..... (YES/no)
Use tcp-keepalive-in service to kill stale connections? (3.1.69) ..... YES
Forbid tftp service? (3.1.70) ..... (YES/no)
Check rules and data related to data flow? (3.1.71) ..... YES
Apply standard routing protections? (3.1.72) ..... (YES/no)
Forbid directed broadcasts (on IOS 11)? (3.1.73) ..... YES
Forbid directed broadcasts (on IOS 12)? (3.1.74) ..... YES

Forbid IP source routing? (3.1.75) ..... YES

2 Level-2

Check rules and data related to system management? (4.1.1) ..... (yes/NO)

Use TACACS Plus authentication? (4.1.2) ..... (yes/NO)

Create emergency account? (4.1.3) ..... YES

Check for AAA new-model? (4.1.4) ..... (yes/NO)

Require tacacs authentication for login? (4.1.5) ..... (yes/NO)

Require tacacs authentication for enable? (4.1.6) ..... (yes/NO)

Check for aaa accounting for exec? (4.1.7) ..... (yes/NO)

Check for aaa accounting for commands? (4.1.8) ..... (yes/NO)

Check for aaa accounting for network events? (4.1.9) ..... (yes/NO)

Check for aaa accounting for connections? (4.1.10) ..... (yes/NO)

Check for aaa accounting for system events? (4.1.11) ..... (yes/NO)

Use loopback address as source for TACACS? (4.1.12) ..... (yes/NO)

What is the local loopback interface number? (4.1.13) ..... (0/_____)

Check the existence of the defined loopback interface? (4.1.14) ..... (yes/NO)

What is the local loopback address? (4.1.15) ..... (192.168.1.3/_____)

Apply level 2 checks to control access to the router? (4.1.16) ..... YES

Require use of SSH for remote administration? (4.1.17) ..... (YES/no)

Check for SSH transport only on VTYs? (4.1.18) ..... (YES/no)

Require VTY ACL to be applied? (4.1.19) ..... YES

Define VTY ACL? (4.1.20) ..... (YES/no)

Check rules and data related to system control? (4.1.21) ..... (yes/NO)

Apply non-standard logging rules? (4.1.22) ..... (YES/no)

Use localtime for logging instead of GMT? (4.1.23) ..... (yes/NO)

Local timezone name? (4.1.24) ..... (GMT/_____)

Local timezone offset from GMT? (4.1.25) ..... (0/_____)

Check timezone and offset? (4.1.26) ..... (yes/NO)

Require summertime clock changes? (4.1.27) ..... (yes/NO)

Apply loopback checks? (4.1.28) ..... (yes/NO)

Use primary loopback as source address for NTP? (4.1.29) ..... (yes/NO)

Forbid all non-standard loopbacks? (4.1.30) ..... (yes/NO)

Use loopback for tftp source interface? (4.1.31) ..... (yes/NO)

Disable unneeded services? (4.1.32) ..... (yes/NO)

Check rules and data related to data flow? (4.1.33) ..... (yes/NO)

Apply border router filtering rules? (4.1.34) ..... (yes/NO)

What is the primary external interface? (4.1.35) ..... (Ethernet0/_____)

Does this border router have a second external interface? (4.1.36) ..... (yes/NO)

What is the secondary external interface? (4.1.37) ..... (Ethernet1/_____)

Apply ingress filter to second external interface? (4.1.38) ..... (yes/NO)

What ACL number (100-199) should be used for ingress filtering? (4.1.39) (180/_____)

Apply egress filter to second external interface? (4.1.40) ..... (yes/NO)

What ACL number (100-199) should be used for egress filtering? (4.1.41) (181/_____)

Test for existence of 2nd external interface? (4.1.42) ..... (yes/NO)

Define egress filter? (4.1.43) ..... (yes/NO)

What is the the internal netblock and mask? (4.1.44) .. (192.168.1.0 0.0.0.255/_____)

Apply ingress filter to external interface? (4.1.45) ..... (yes/NO)

Define ingress filter? (4.1.46) ..... (yes/NO)

Apply egress filter to first external interface? (4.1.47) ..... (yes/NO)

Test for existence of external interface? (4.1.48) ..... (yes/NO)

Apply extra routing protections? (4.1.49) ..... (yes/NO)

Use Unicast RPF for filtering? (4.1.50) ..... (yes/NO)

Forbid proxy arp? (4.1.52) ..... (YES/no)

Forbid tunnel interfaces? (4.1.53) ..... (yes/NO)