CHAPTER 21

Security Audit

Security Audit is a feature that examines your existing router configurations and then updates your router in order to make your router and network more secure. Security Audit is based on the Cisco IOS AutoSecure feature; it performs checks on and assists in configuration of almost all of the AutoSecure functions. For a complete list of the functions that Security Audit checks for, and for a list of the few AutoSecure features unsupported by Security Audit, see the topic Cisco SDM and Cisco IOS AutoSecure.

Security Audit operates in one of two modes—the Security Audit wizard, which lets you choose which potential security-related configuration changes to implement on your router, and One-Step Lockdown, which automatically makes all recommended security-related configuration changes.

Perform Security Audit

This option starts the Security Audit wizard. The Security Audit wizard tests your router configuration to determine if any potential security problems exist in the configuration, and then presents you with a screen that lets you determine which of those security problems you want to fix. Once determined, the Security Audit wizard will make the necessary changes to the router configuration to fix those problems.

To have Cisco SDM perform a security audit and then fix the problems it has found:

Step 1 In the left frame, select **Security Audit**.

Step 2 Click **Perform Security Audit**.

The Welcome page of the Security Audit wizard appears.

Step 3 Click **Next>**.

The Security Audit Interface Configuration page appears.

Step 4 The Security Audit wizard needs to know which of your router interfaces connect to your inside network and which connect outside of your network. For each interface listed, check either the **Inside** or **Outside** check box to indicate where the interface connects.

Step 5 Click **Next>**.

The Security Audit wizard tests your router configuration to determine which possible security problems may exist. A screen showing the progress of this action appears, listing all of the configuration options being tested for, and whether or not the current router configuration passes those tests.

If you want to save this report to a file, click **Save Report**.

Step 6 Click **Close**.

The Security Audit Report Card screen appears, showing a list of possible security problems.

Step 7 Check the **Fix it** boxes next to any problems that you want Cisco Router and Security Device Manager (Cisco SDM) to fix. For a description of the problem and a list of the Cisco IOS commands that will be added to your configuration, click the problem description to display a help page about that problem.

Step 8 Click **Next>**.

Step 9 The Security Audit wizard may display one or more screens requiring you to enter information to fix certain problems. Enter the information as required and click **Next>** for each of those screens.

Step 10 The Summary page of the wizard shows a list of all the configuration changes that Security Audit will make. Click **Finish** to deliver those changes to your router.

One-Step Lockdown

This option tests you router configuration for any potential security problems and automatically makes any necessary configuration changes to correct any problems found. The conditions checked for and, if needed, corrected are as follows:

- Disable Finger Service

- Disable PAD Service
- Disable TCP Small Servers Service
- Disable UDP Small Servers Service
- Disable IP BOOTP Server Service
- Disable IP Identification Service
- Disable CDP
- Disable IP Source Route
- Enable Password Encryption Service
- Enable TCP Keepalives for Inbound Telnet Sessions
- Enable TCP Keepalives for Outbound Telnet Sessions
- Enable Sequence Numbers and Time Stamps on Debugs
- Enable IP CEF
- Disable IP Gratuitous ARPs
- Set Minimum Password Length to Less Than 6 Characters
- Set Authentication Failure Rate to Less Than 3 Retries
- Set TCP Synwait Time
- Set Banner
- Enable Logging
- Set Enable Secret Password
- Disable SNMP
- Set Scheduler Interval
- Set Scheduler Allocate
- Set Users
- Enable Telnet Settings
- Enable NetFlow Switching
- Disable IP Redirects
- Disable IP Proxy ARP
- Disable IP Directed Broadcast
- Disable MOP Service

- Disable IP Unreachables
- Disable IP Mask Reply
- Disable IP Unreachables on NULL Interface
- Enable Unicast RPF on Outside Interfaces
- Enable Firewall on All of the Outside Interfaces
- Set Access Class on HTTP Server Service
- Set Access Class on VTY Lines
- Enable SSH for Access to the Router

Welcome Page

This screen describes the Security Audit wizard and the changes the wizard will attempt to make to your router configuration.

Interface Selection Page

This screen displays a list of all interfaces and requires you to identify which router interfaces are “outside” interfaces, that is, interfaces that connect to unsecure networks such as the Internet. By identifying which interfaces are outside interfaces, Security Configuration knows on which interfaces to configure firewall security features.

Interface Column

This column lists each of the router interfaces.

Outside Column

This column displays a check box for each interface listed in the Interface column. Check the check box for each interface that connects to a network outside of your network, such as the Internet.

Inside Column

This column displays a check box for each interface listed in the Interface column. Check the check box for each interface that connects directly to your local network and is thus protected from the Internet by your firewall.

Report Card Page

The Report Card popup page displays a list of recommended configuration changes that, if made, make the network more secure. The **Save** button, enabled after all checks are made, lets you save the report card to a file that you can print or email. Clicking **Close** displays a dialog that lists the reported security problems, and that can list security configurations that Cisco SDM can undo.

Fix It Page

This page displays the configuration changes recommended in the Report Card page. Use the **Select an Option** list to display the security problems Cisco SDM can fix, or the security configurations Cisco SDM can undo.

Select an Option: Fix the security problems

The Report Card screen displays a list of recommended configuration changes that will make your router and network more secure. The potential security problems in your router configuration are listed in the left column. To get more information about a potential problem, click the problem. Online help will display a more detailed description of the problem and the recommended configuration changes. To correct all of the potential problems, click **Fix All**, and then click **Next>** to continue. To correct individual security issues, check the **Fix It** check box next to the issue or issues that you want to correct, and then click **Next>** to continue the Security Audit Wizard. The Security Audit will correct the problems you selected, collecting further input from you as necessary, and will then display a list of the new configuration commands that will be added to the router configuration.

Fix All

Click this button to place a check mark next to all of the potential security problems listed on the Report Card screen.

Select an option: Undo Security Configurations

When this option is selected, Cisco SDM displays the security configurations that it can undo. To have Cisco SDM undo all the security configurations, click **Undo All**. To specify a security configuration that you want to undo, check the **Undo** box next to it. **Click Next>** after you have specified which security configurations to undo. You must select at least one security configuration to undo.

Undo All

Click the button to place a checkmark next to all the security configurations that Cisco SDM can undo.

To see which security configurations Cisco SDM can undo, click:

Security Configurations Cisco SDM Can Undo

I want Cisco SDM to fix some problems, but undo other security configurations

If you want Cisco SDM to fix some security issues but undo other security configurations that you do not need, you can run the Security Audit wizard once to specify the problems to fix, and then run it again so that you can select the security configurations you want to undo.

Disable Finger Service

Security Audit disables the finger service whenever possible. Finger is used to find out which users are logged into a network device. Although this information is not usually tremendously sensitive, it can sometimes be useful to an attacker.

In addition, the finger service can be used in a specific type of Denial-of-Service (DoS) attack called “Finger of death,” which involves sending a finger request to a specific computer every minute, but never disconnecting.

The configuration that will be delivered to the router to disable the Finger service is as follows:

```
no service finger
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable PAD Service

Security Audit disables all packet assembler/disassembler (PAD) commands and connections between PAD devices and access servers whenever possible.

The configuration that will be delivered to the router to disable PAD is as follows:

```
no service pad
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable TCP Small Servers Service

Security Audit disables small services whenever possible. By default, Cisco devices running Cisco IOS version 11.3 or earlier offer the "small services": echo, chargen, and discard. (Small services are disabled by default in Cisco IOS software version 12.0 and later.) These services, especially their User Datagram Protocol (UDP) versions, are infrequently used for legitimate purposes, but they can be used to launch DoS and other attacks that would otherwise be prevented by packet filtering.

For example, an attacker might send a Domain Name System (DNS) packet, falsifying the source address to be a DNS server that would otherwise be unreachable, and falsifying the source port to be the DNS service port (port 53). If such a packet were sent to the router's UDP echo port, the result would be the router sending a DNS packet to the server in question. No outgoing access list checks would be applied to this packet, since it would be considered to be locally generated by the router itself.

Although most abuses of the small services can be avoided or made less dangerous by anti-spoofing access lists, the services should almost always be disabled in any router which is part of a firewall or lies in a security-critical part of the network. Since the services are rarely used, the best policy is usually to disable them on all routers of any description.

The configuration that will be delivered to the router to disable TCP small servers is as follows:

```
no service tcp-small-servers
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable UDP Small Servers Service

Security Audit disables small services whenever possible. By default, Cisco devices running Cisco IOS version 11.3 or earlier offer the "small services": echo, chargen, and discard. (Small services are disabled by default in Cisco IOS software version 12.0 and later.) These services, especially their UDP versions, are infrequently used for legitimate purposes, but they can be used to launch DoS and other attacks that would otherwise be prevented by packet filtering.

For example, an attacker might send a DNS packet, falsifying the source address to be a DNS server that would otherwise be unreachable, and falsifying the source port to be the DNS service port (port 53). If such a packet were sent to the router's UDP echo port, the result would be the router sending a DNS packet to the server in question. No outgoing access list checks would be applied to this packet, since it would be considered to be locally generated by the router itself.

Although most abuses of the small services can be avoided or made less dangerous by anti-spoofing access lists, the services should almost always be disabled in any router which is part of a firewall or lies in a security-critical part of the network. Since the services are rarely used, the best policy is usually to disable them on all routers of any description.

The configuration that will be delivered to the router to disable UDP small servers is as follows:

```
no service udp-small-servers
```

Disable IP BOOTP Server Service

Security Audit disables the Bootstrap Protocol (BOOTP) service whenever possible. BOOTP allows both routers and computers to automatically configure necessary Internet information from a centrally maintained server upon startup, including downloading Cisco IOS software. As a result, BOOTP can potentially be used by an attacker to download a copy of a router's Cisco IOS software.

In addition, the BOOTP service is vulnerable to DoS attacks; therefore it should be disabled or filtered via a firewall for this reason as well.

The configuration that will be delivered to the router to disable BOOTP is as follows:

```
no ip bootp server
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Identification Service

Security Audit disables identification support whenever possible. Identification support allows you to query a TCP port for identification. This feature enables an unsecure protocol to report the identity of a client initiating a TCP connection and a host responding to the connection. With identification support, you can connect a TCP port on a host, issue a simple text string to request information, and receive a simple text-string reply.

It is dangerous to allow any system on a directly connected segment to learn that the router is a Cisco device and to determine the model number and the Cisco IOS software version being run. This information may be used to design attacks against the router.

The configuration that will be delivered to the router to disable the IP identification service is as follows:

```
no ip identd
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable CDP

Security Audit disables Cisco Discovery Protocol (CDP) whenever possible. CDP is a proprietary protocol that Cisco routers use to identify each other on a LAN segment. This is dangerous in that it allows any system on a directly connected segment to learn that the router is a Cisco device and to determine the model number and the Cisco IOS software version being run. This information may be used to design attacks against the router.

The configuration that will be delivered to the router to disable CDP is as follows:

```
no cdp run
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Source Route

Security Audit disables IP source routing whenever possible. The IP protocol supports source routing options that allow the sender of an IP datagram to control the route that the datagram will take toward its ultimate destination, and generally the route that any reply will take. These options are rarely used for legitimate purposes in networks. Some older IP implementations do not process source-routed packets properly, and it may be possible to crash machines running these implementations by sending them datagrams with source routing options.

Disabling IP source routing will cause a Cisco router to never forward an IP packet that carries a source routing option.

The configuration that will be delivered to the router to disable IP source routing is as follows:

```
no ip source-route
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Enable Password Encryption Service

Security Audit enables password encryption whenever possible. Password encryption directs the Cisco IOS software to encrypt the passwords, Challenge Handshake Authentication Protocol (CHAP) secrets, and similar data that are saved in its configuration file. This is useful for preventing casual observers from reading passwords, for example, when they happen to look at the screen over an administrator's shoulder.

The configuration that will be delivered to the router to enable password encryption is as follows:

```
service password-encryption
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Enable TCP Keepalives for Inbound Telnet Sessions

Security Audit enables TCP keep alive messages for both inbound and outbound Telnet sessions whenever possible. Enabling TCP keep alives causes the router to generate periodic keep alive messages, letting it detect and drop broken Telnet connections.

The configuration that will be delivered to the router to enable TCP keep alives for inbound Telnet sessions is as follows:

```
service tcp-keepalives-in
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Enable TCP Keepalives for Outbound Telnet Sessions

Security Audit enables TCP keep alive messages for both inbound and outbound Telnet sessions whenever possible. Enabling TCP keep alives causes the router to generate periodic keep alive messages, letting it detect and drop broken Telnet connections.

The configuration that will be delivered to the router to enable TCP keep alives for outbound Telnet sessions is as follows:

```
service tcp-keepalives-out
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Enable Sequence Numbers and Time Stamps on Debugs

Security Audit enables sequence numbers and time stamps on all debug and log messages whenever possible. Time stamps on debug and log messages indicate the time and date that the message was generated. Sequence numbers indicate the sequence in which messages that have identical time stamps were generated. Knowing the timing and sequence that messages are generated is an important tool in diagnosing potential attacks.

The configuration that will be delivered to the router to enable time stamps and sequence numbers is as follows:

```
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timeout msec
```

```
service sequence-numbers
```

Enable IP CEF

Security Audit enables Cisco Express Forwarding (CEF) or Distributed Cisco Express Forwarding (DCEF) whenever possible. Because there is no need to build cache entries when traffic starts arriving at new destinations, CEF behaves more predictably than other modes when presented with large volumes of traffic addressed to many destinations. Routes configured for CEF perform better under SYN attacks than routers using the traditional cache.

The configuration that will be delivered to the router to enable CEF is as follows:

```
ip cef
```

Disable IP Gratuitous ARPs

Security Audit disables IP gratuitous Address Resolution Protocol (ARP) requests whenever possible. A gratuitous ARP is an ARP broadcast in which the source and destination IP addresses are the same. It is used primarily by a host to inform the network about its IP address. A spoofed gratuitous ARP message can cause network mapping information to be stored incorrectly, causing network malfunction.

To disable gratuitous ARPs, the following configuration will be delivered to the router:

```
no ip gratuitous-arps
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Set Minimum Password Length to Less Than 6 Characters

Security Audit configures your router to require a minimum password length of six characters whenever possible. One method attackers use to crack passwords is to try all possible combinations of characters until the password is discovered. Longer passwords have exponentially more possible combinations of characters, making this method of attack much more difficult.

This configuration change will require every password on the router, including the user, enable, secret, console, AUX, tty, and vty passwords, to be at least six characters in length. This configuration change will be made only if the Cisco IOS version running on your router supports the minimum password length feature.

The configuration that will be delivered to the router is as follows:

```
security passwords min-length <6>
```

Set Authentication Failure Rate to Less Than 3 Retries

Security Audit configures your router to lock access after three unsuccessful login attempts whenever possible. One method of cracking passwords, called the "dictionary" attack, is to use software that attempts to log in using every word in a dictionary. This configuration causes access to the router to be locked for a period of 15 seconds after three unsuccessful login attempts, disabling the dictionary method of attack. In addition to locking access to the router, this configuration causes a log message to be generated after three unsuccessful login attempts, warning the administrator of the unsuccessful login attempts.

The configuration that will be delivered to the router to lock router access after three unsuccessful login attempts is as follows:

```
security authentication failure rate <3>
```

Set TCP Synwait Time

Security Audit sets the TCP synwait time to 10 seconds whenever possible. The TCP synwait time is a value that is useful in defeating SYN flooding attacks, a form of Denial-of-Service (DoS) attack. A TCP connection requires a three-phase handshake to initially establish the connection. A connection request is sent by the originator, an acknowledgement is sent by the receiver, and then an acceptance of that acknowledgement is sent by the originator. Once this three-phase handshake is complete, the connection is complete and data transfer can begin. A SYN flooding attack sends repeated connection requests to a host, but never sends the acceptance of acknowledgements that complete the connections, creating increasingly more incomplete connections at the host. Because the buffer for incomplete connections is usually smaller than the buffer for completed

connections, this can overwhelm and disable the host. Setting the TCP synwait time to 10 seconds causes the router to shut down an incomplete connection after 10 seconds, preventing the buildup of incomplete connections at the host.

The configuration that will be delivered to the router to set the TCP synwait time to 10 seconds is as follows:

```
ip tcp synwait-time <10>
```

Set Banner

Security Audit configures a text banner whenever possible. In some jurisdictions, civil and/or criminal prosecution of crackers who break into your systems is made much easier if you provide a banner informing unauthorized users that their use is in fact unauthorized. In other jurisdictions, you may be forbidden to monitor the activities of even unauthorized users unless you have taken steps to notify them of your intent to do so. The text banner is one method of performing this notification.

The configuration that will be delivered to the router to create a text banner is as follows, replacing <*company name*>, <*administrator email address*>, and <*administrator phone number*> with the appropriate values that you enter into Security Audit:

```
banner ~
Authorized access only
This system is the property of <company name> Enterprise.
Disconnect IMMEDIATELY as you are not an authorized user!
Contact <administrator email address> <administrator phone number>.
~
```

Enable Logging

Security Audit will enable logging with time stamps and sequence numbers whenever possible. Because it gives detailed information about network events, logging is critical in recognizing and responding to security events. Time stamps and sequence numbers provide information about the date and time and sequence in which network events occur.

The configuration that will be delivered to the router to enable and configure logging is as follows, replacing <*log buffer size*> and <*logging server ip address*> with the appropriate values that you enter into Security Audit:

```
logging console critical
logging trap debugging
logging buffered <log buffer size>
logging <logging server ip address>
```

Set Enable Secret Password

Security Audit will configure the **enable secret** Cisco IOS command for more secure password protection whenever possible. The **enable secret** command is used to set the password that grants privileged administrative access to the Cisco IOS system. The **enable secret** command uses a much more secure encryption algorithm (MD5) to protect that password than the older **enable password** command. This stronger encryption is an essential means of protecting the router password, and thus network access.

The configuration that will be delivered to the router to configure the command is as follows:

```
enable secret <>
```

Disable SNMP

Security Audit disables the Simple Network Management Protocol (SNMP) whenever possible. SNMP is a network protocol that provides a facility for retrieving and posting data about network performance and processes. It is very widely used for router monitoring, and frequently for router configuration changes as well. Version 1 of the SNMP protocol, however, which is the most commonly used, is often a security risk for the following reasons:

- It uses authentication strings (passwords) called *community strings* which are stored and sent across the network in plain text.
- Most SNMP implementations send those strings repeatedly as part of periodic polling.
- It is an easily spoofable, datagram-based transaction protocol.

Because SNMP can be used to retrieve a copy of the network routing table, as well as other sensitive network information, Cisco recommends disabling SNMP if your network does not require it. Security Audit will initially request to disable SNMP.

The configuration that will be delivered to the router to disable SNMP is as follows:

```
no snmp-server
```

Set Scheduler Interval

Security Audit configures the scheduler interval on the router whenever possible. When a router is fast-switching a large number of packets, it is possible for the router to spend so much time responding to interrupts from the network interfaces that no other work gets done. Some very fast packet floods can cause this condition. It may stop administrative access to the router, which is very dangerous when the device is under attack. Tuning the scheduler interval ensures that management access to the router is always available by causing the router to run system processes after the specified time interval even when CPU usage is at 100%.

The configuration that will be delivered to the router to tune the scheduler interval is as follows:

```
scheduler interval 500
```

Set Scheduler Allocate

On routers that do not support the command **scheduler interval**, Security Audit configures the **scheduler allocate** command whenever possible. When a router is fast-switching a large number of packets, it is possible for the router to spend so much time responding to interrupts from the network interfaces that no other work gets done. Some very fast packet floods can cause this condition. It may stop administrative access to the router, which is very dangerous when the device is under attack. The **scheduler allocate** command guarantees a percentage of the router CPU processes for activities other than network switching, such as management processes.

The configuration that will be delivered to the router to set the scheduler allocate percentage is as follows:

```
scheduler allocate 4000 1000
```

Set Users

Security Audit secures the console, AUX, vty, and tty lines by configuring Telnet user accounts to authenticate access to these lines whenever possible. Security Audit will display a dialog box that lets you define user accounts and passwords for these lines.

Enable Telnet Settings

Security Audit secures the console, AUX, vty, and tty lines by implementing the following configurations whenever possible:

- Configures **transport input** and **transport output** commands to define which protocols can be used to connect to those lines.
- Sets the exec-timeout value to 10 minutes on the console and AUX lines, causing an administrative user to be logged out from these lines after 10 minutes of no activity.

The configuration that will be delivered to the router to secure the console, AUX, vty, and tty lines is as follows:

```
!
line console 0
transport output telnet
exec-timeout 10
login local
!
line AUX 0
transport output telnet
exec-timeout 10
login local
!
line vty ….
transport input telnet
login local
```

Enable NetFlow Switching

Security Audit enables NetFlow switching whenever possible. NetFlow switching is a Cisco IOS feature that enhances routing performance while using Access Control Lists (ACLs) and other features that create and enhance network security.

NetFlow identifies flows of network packets based on the source and destination IP addresses and TCP port numbers. NetFlow then can use just the initial packet of a flow for comparison to ACLs and for other security checks, rather than having to use every packet in the network flow. This enhances performance, allowing you to make use of all of the router security features.

The configuration that will be delivered to the router to enable NetFlow is as follows:

```
ip route-cache flow
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Redirects

Security Audit disables Internet Message Control Protocol (ICMP) redirect messages whenever possible. ICMP supports IP traffic by relaying information about paths, routes, and network conditions. ICMP redirect messages instruct an end node to use a specific router as its path to a particular destination. In a properly functioning IP network, a router will send redirects only to hosts on its own local subnets, no end node will ever send a redirect, and no redirect will ever be traversed more than one network hop. However, an attacker may violate these rules; some attacks are based on this. Disabling ICMP redirects will cause no operational impact to the network, and it eliminates this possible method of attack.

The configuration that will be delivered to the router to disable ICMP redirect messages is as follows:

```
no ip redirects
```

Disable IP Proxy ARP

Security Audit disables proxy Address Resolution Protocol (ARP) whenever possible. ARP is used by the network to convert IP addresses into MAC addresses. Normally ARP is confined to a single LAN, but a router can act as a proxy for ARP requests, making ARP queries available across multiple LAN segments. Because it breaks the LAN security barrier, proxy ARP should be used only between two LANs with an equal security level, and only when necessary.

The configuration that will be delivered to the router to disable proxy ARP is as follows:

```
no ip proxy-arp
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Directed Broadcast

Security Audit disables IP directed broadcasts whenever possible. An IP directed broadcast is a datagram which is sent to the broadcast address of a subnet to which the sending machine is not directly attached. The directed broadcast is routed through the network as a unicast packet until it arrives at the target subnet, where it is converted into a link-layer broadcast. Because of the nature of the IP addressing architecture, only the last router in the chain, the one that is connected directly to the target subnet, can conclusively identify a directed broadcast. Directed broadcasts are occasionally used for legitimate purposes, but such use is not common outside the financial services industry.

IP directed broadcasts are used in the extremely common and popular “smurf” Denial-of-Service attack, and they can also be used in related attacks. In a “smurf” attack, the attacker sends ICMP echo requests from a falsified source address to a directed broadcast address, causing all the hosts on the target subnet to send replies to the falsified source. By sending a continuous stream of such requests, the attacker can create a much larger stream of replies, which can completely inundate the host whose address is being falsified.

Disabling IP directed broadcasts causes directed broadcasts that would otherwise be “exploded” into link-layer broadcasts at that interface to be dropped instead.

The configuration that will be delivered to the router to disable IP directed broadcasts is as follows:

```
no ip directed-broadcast
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable MOP Service

Security Audit will disable the Maintenance Operations Protocol (MOP) on all Ethernet interfaces whenever possible. MOP is used to provide configuration information to the router when communicating with DECNet networks. MOP is vulnerable to various attacks.

The configuration that will be delivered to the router to disable the MOP service on Ethernet interfaces is as follows:

```
no mop enabled
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Unreachables

Security Audit disables Internet Message Control Protocol (ICMP) host unreachable messages whenever possible. ICMP supports IP traffic by relaying information about paths, routes, and network conditions. ICMP host unreachable messages are sent out if a router receives a nonbroadcast packet that uses an unknown protocol, or if the router receives a packet that it is unable to deliver to the ultimate destination because it knows of no route to the destination address. These messages can be used by an attacker to gain network mapping information.

The configuration that will be delivered to the router to disable ICMP host unreachable messages is as follows:

```
int <all-interfaces>
no ip unreachables
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Mask Reply

Security Audit disables Internet Message Control Protocol (ICMP) mask reply messages whenever possible. ICMP supports IP traffic by relaying information about paths, routes, and network conditions. ICMP mask reply messages are sent when a network devices must know the subnet mask for a particular subnetwork

in the internetwork. ICMP mask reply messages are sent to the device requesting the information by devices that have the requested information. These messages can be used by an attacker to gain network mapping information.

The configuration that will be delivered to the router to disable ICMP mask reply messages is as follows:

```
no ip mask-reply
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Unreachables on NULL Interface

Security Audit disables Internet Message Control Protocol (ICMP) host unreachable messages whenever possible. ICMP supports IP traffic by relaying information about paths, routes, and network conditions. ICMP host unreachable messages are sent out if a router receives a nonbroadcast packet that uses an unknown protocol, or if the router receives a packet that it is unable to deliver to the ultimate destination because it knows of no route to the destination address. Because the null interface is a packet sink, packets forwarded there will always be discarded and, unless disabled, will generate host unreachable messages. In that case, if the null interface is being used to block a Denial-of-Service attack, these messages flood the local network with these messages. Disabling these messages prevents this situation. In addition, because all blocked packets are forwarded to the null interface, an attacker receiving host unreachable messages could use those messages to determine Access Control List (ACL) configuration.

If the “null 0” interface is configured on your router, Security Audit will deliver the following configuration to the router to disable ICMP host unreachable messages for discarded packets or packets routed to the null interface is as follows:

```
int null 0
no ip unreachables
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Enable Unicast RPF on Outside Interfaces

Security Audit enables unicast Reverse Path Forwarding (RPF) on all interfaces that connect to the Internet whenever possible. RPF is a feature that causes the router to check the source address of any packet against the interface through which the packet entered the router. If the input interface is not a feasible path to the source address according to the routing table, the packet will be dropped. This source address verification is used to defeat IP spoofing.

This works only when routing is symmetric. If the network is designed in such a way that traffic from host A to host B may normally take a different path than traffic from host B to host A, the check will always fail, and communication between the two hosts will be impossible. This sort of asymmetric routing is common in the Internet core. Ensure that your network does not use asymmetric routing before enabling this feature.

In addition, unicast RPF can be enabled only when IP Cisco Express Forwarding (CEF) is enabled. Security Audit will check the router configuration to see if IP CEF is enabled. If IP CEF is not enabled, Security Audit will recommend that IP CEF be enabled and will enable it if the recommendation is approved. If IP CEF is not enabled, by Security Audit or otherwise, unicast RPF will not be enabled.

To enable unicast RPF, the following configuration will be delivered to the router for each interface that connects outside of the private network, replacing <*outside interface*> with the interface identifier:

```
interface <outside interface>
ip verify unicast reverse-path
```

Enable Firewall on All of the Outside Interfaces

If the Cisco IOS image running on the router includes the Firewall feature set, then Security Audit will enable Context-Based Access Control (CBAC) on the router whenever possible. CBAC, a component of the Cisco IOS Firewall feature set, filters packets based on application-layer information, such as what kinds of commands are being executed within the session. For example, if a command that is not supported is discovered in a session, the packet can be denied access.

CBAC enhances security for TCP and User Datagram Protocol (UDP) applications that use well-known ports, such as port 80 for HTTP or port 443 for Secure Sockets Layer (SSL). It does this by scrutinizing source and destination

addresses. Without CBAC, advanced application traffic is permitted only by writing Access Control Lists (ACLs). This approach leaves firewall doors open, so most administrators tend to deny all such application traffic. With CBAC enabled, however, you can securely permit multimedia and other application traffic by opening the firewall as needed and closing it all other times.

To enable CBAC, Security Audit will use Cisco SDM's Create Firewall screens to generate a firewall configuration.

Set Access Class on HTTP Server Service

Security Audit enables the HTTP service on the router with an access class whenever possible. The HTTP service permits remote configuration and monitoring using a web browser, but is limited in its security because it sends a clear-text password over the network during the authentication process. Security Audit therefore limits access to the HTTP service by configuring an access class that permits access only from directly connected network nodes.

The configuration that will be delivered to the router to enable the HTTP service with an access class is as follows:

```
ip http server
ip http access-class <std-acl-num>
!
!HTTP Access-class:Allow initial access to direct connected subnets !
!only
access-list <std-acl-num> permit <inside-network>
access-list <std-acl-num> deny any
```

Set Access Class on VTY Lines

Security Audit configures an access class for vty lines whenever possible. Because vty connections permit remote access to your router, they should be limited only to known network nodes.

The configuration that will be delivered to the router to configure an access class for vty lines is as follows:

```
access-list <std-acl-num> permit <inside-network>
access-list <std-acl-num> deny any
```

In addition, the following configuration will be applied to each vty line:

```
access-class <std-acl-num>
```

Enable SSH for Access to the Router

If the Cisco IOS image running on the router is a crypto image (an image that uses 56-bit Data Encryption Standard (DES) encryption and is subject to export restrictions), then Security Audit will implement the following configurations to secure Telnet access whenever possible:

- Enable Secure Shell (SSH) for Telnet access. SSH makes Telnet access much more secure.
- Set the SSH timeout value to 60 seconds, causing incomplete SSH connections to shut down after 60 seconds.
- Set the maximum number of unsuccessful SSH login attempts to two before locking access to the router.

The configuration that will be delivered to the router to secure access and file transfer functions is as follows:

```
ip ssh time-out 60
ip ssh authentication-retries 2
!
line vty 0 4
transport input ssh
!
```

Note After making the configuration changes above, you must specify the SSH modulus key size and generate a key. Use the SSH page to do so.

Enable AAA

Cisco IOS Authentication, Authorization, and Accounting (AAA) is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing authentication, authorization, and accounting services.

Cisco SDM will perform the following precautionary tasks while enabling AAA to prevent loss of access to the router:

- Configure authentication and authorization for VTY lines

  The local database will be used for both authentication and authorization.
- Configure authentication for a console line

  The local database will be used for authentication.
- Modify HTTP authentication to use the local database

Configuration Summary Screen

This screen displays a list of all the configuration changes that will be delivered to the router configuration, based on the security problems that you selected to fix in the Report Card screen.

Cisco SDM and Cisco IOS AutoSecure

AutoSecure is a Cisco IOS feature that, like Cisco SDM, lets you more easily configure security features on your router, so that your network is better protected. Cisco SDM implements almost all of the configurations that AutoSecure affords.

AutoSecure Features Implemented in Cisco SDM

The following AutoSecure features are implemented in this version of Cisco SDM. For an explanation of these services and features, click the links below:

- Disable SNMP
- Disable Finger Service
- Disable PAD Service
- Disable TCP Small Servers Service
- Disable IP BOOTP Server Service
- Disable IP Identification Service
- Disable CDP
- Disable IP Source Route

- Disable IP Redirects
- Disable IP Proxy ARP
- Disable IP Directed Broadcast
- Disable MOP Service
- Disable IP Unreachables
- Disable IP Unreachables on NULL Interface
- Disable IP Mask Reply
- Enable Password Encryption Service
- Disable IP Unreachables on NULL Interface
- Disable IP Unreachables on NULL Interface
- Set Minimum Password Length to Less Than 6 Characters
- Enable IP CEF
- Enable Firewall on All of the Outside Interfaces
- Set Users
- Enable Logging
- Enable Firewall on All of the Outside Interfaces
- Set Minimum Password Length to Less Than 6 Characters
- Enable Firewall on All of the Outside Interfaces
- Set Users
- Set Users
- Set Users
- Enable Unicast RPF on Outside Interfaces
- Enable Firewall on All of the Outside Interfaces

AutoSecure Features Not Implemented in Cisco SDM

The following AutoSecure features are not implemented in this version of Cisco SDM:

- Disabling NTP—Based on input, AutoSecure will disable the Network Time Protocol (NTP) if it is not necessary. Otherwise, NTP will be configured with MD5 authentication. Cisco SDM does not support disabling NTP.

- Configuring AAA—If the Authentication, Authorization, and Accounting (AAA) service is not configured, AutoSecure configures local AAA and prompts for configuration of a local username and password database on the router. Cisco SDM does not support AAA configuration.
- Setting SPD Values—Cisco SDM does not set Selective Packet Discard (SPD) values.
- Enabling TCP Intercepts—Cisco SDM does not enable TCP intercepts.
- Configuring anti-spoofing ACLs on outside interfaces—AutoSecure creates three named access lists used to prevent anti-spoofing source addresses. Cisco SDM does not configure these ACLs.

AutoSecure Features Implemented Differently in Cisco SDM

- Disable SNMP—Cisco SDM will disable SNMP, but unlike AutoSecure, it does not provide an option for configuring SNMP version 3.
- Enable SSH for Access to the Router—Cisco SDM will enable and configure SSH on crypto Cisco IOS images, but unlike AutoSecure, it will not enable Service Control Point (SCP) or disable other access and file transfer services, such as FTP.

Security Configurations Cisco SDM Can Undo

This table lists the security configurations that Cisco SDM can undo.

Security Configuration	Equivalent CLI
Disable Finger Service	No service finger
Disable PAD Service	No service pad
Disable TCP Small Servers Service	No service tcp-small-servers no service udp-small-servers
Disable IP BOOTP Server Service	No ip bootp server
Disable IP Identification Service	No ip identd
Disable CDP	No cdp run
Disable IP Source Route	No ip source-route

Security Configuration	Equivalent CLI
Enable NetFlow Switching	ip route-cache flow
Disable IP Redirects	no ip redirects
Disable IP Proxy ARP	no ip proxy-arp
Disable IP Directed Broadcast	no ip directed-broadcast
Disable MOP Service	No mop enabled
Disable IP Unreachables	int <all-interfaces> no ip unreachables
Disable IP Mask Reply	no ip mask-reply
Disable IP Unreachables on NULL Interface	int null 0 no ip unreachables
Enable Password Encryption Service	service password-encryption
Enable TCP Keepalives for Inbound Telnet Sessions	service tcp-keepalives-in
Enable TCP Keepalives for Outbound Telnet Sessions	service tcp-keepalives-out
Disable IP Gratuitous ARPs	no ip gratuitous arps

Undoing Security Audit Fixes

Cisco SDM can undo this security fix. If you want Cisco SDM to remove this security configuration, run the Security Audit wizard. In the Report Card window, select the option **Undo Security Configurations**, place a check mark next to this configuration and other configurations that you want to undo, and click **Next>**.

Add or Edit Telnet/SSH Account Screen

This screen lets you add a new user account or edit an existing user account for Telnet and SSH access to your router.

User Name

Enter the username for the new account in this field.

Password

Enter the password for the new account in this field.

Confirm Password

Reenter the new account password in this field for confirmation. The entry in this field must match the entry in the password field.

Configure User Accounts for Telnet/SSH Page

This screen lets you manage the user accounts that have Telnet or Secure Shell (SSH) access to your router. The table in this screen shows each Telnet user account, listing the account username and displaying asterisks to represent the account password. Note that this screen appears only if you have not already configured any user accounts; therefore, the table on this screen is always empty when it is initially displayed.

Enable Authorization for Telnet Check Box

Check this box to enable Telnet and SSH access to your router. Clear this box to disable Telnet and SSH access to your router.

Add... Button

Click this button to display the Add a User Account screen, letting you add an account by assigning the account a username and password.

Edit... Button

Click a user account in the table to select it, and click this button to display the Edit a User Account screen, letting you edit the username and password of the selected account.

Delete Button

Click a user account in the table to select it, and click this button to delete the selected account.

Enable Secret and Banner Page

This screen lets you enter a new enable secret and a text banner for the router.

The enable secret is an encrypted password that provides administrator-level access to all functions of the router. It is vital that the secret be secure and difficult to crack. Your secret must be a minimum of six characters long, and it is recommended that you include both alphabetic and numeric characters and that you do not use a word that can be found in a dictionary, or that might be personal information about yourself that someone might be able to guess.

The text banner will be displayed whenever anyone connects to your router using Telnet or SSH. The text banner is an important security consideration because it is a method of notifying unauthorized individuals that access to your router is prohibited. in some jurisdictions, this is a requirement for civil and/or criminal prosecution.

New Password

Enter the new enable secret in this field.

Re-enter New Password

Re-enter the new enable secret in this field for verification.

Login Banner

Enter the text banner that you want configured on your router.

Logging Page

This screen lets you configure the router log by creating a list of syslog servers where log messages will be forwarded, and by setting the logging level, which determines the minimum severity a log message must have in order for it to be captured.

IP Address/Hostname Table

This table displays a list of hosts to where the router log messages will be forwarded. These hosts should be syslog servers that can trap and manage the router log messages.

Add... Button

Click this button to display the IP Address/Host Name screen, letting you add a syslog server to the list by entering either its IP address or host name.

Edit... Button

Click a syslog server in the table to select it, and click this button to display the IP Address/Host Name screen, letting you edit the IP address or host name of the selected syslog server.

Delete Button

Click a syslog server in the table to select it, and click this button to delete the selected syslog server from the table.

Set logging level Field

In this field, select the minimum severity level that a router log message must have in order for it to be trapped and forwarded to the syslog server(s) in the table on this screen. A log message severity level is shown as a number from 1 through 7, with lower numbers indicating more severe events. The descriptions of each of the severity levels are as follows:

- 0 - emergencies

  System unusable
- 1- alerts

Immediate action needed

- 2 - critical

  Critical conditions

- 3 - errors

  Error conditions

- 4 - warnings

  Warning conditions

- 5 - notifications

  Normal but significant condition

- 6 - informational

  Informational messages only

- 7 - debugging

  Debugging messages