Global Information Assurance Certification Paper

Marvin Yee
Auditing Networks, Perimeters, and Systems
GSNA Practical Assignment
Version 1.2 (amended October 26, 2001)
Auditing Cisco Perimeter Routers

Table of Contents

Part 1 – Research in Audit, Measurement Practice, and Control

The device that I will be auditing is a Cisco router that is used as the perimeter router. The Cisco router is a 7206 with IOS version 12.2. The specifications if the router is shown below.

```
Cisco Internetwork Operating System Software
IOS (tm) RSP Software (RSP-PV-M), Version 12.2(2)T1,  RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 18-Jul-01 05:20 by ccai
Image text-base: 0x600109C8, data-base: 0x611D0000

ROM: System Bootstrap, Version 11.1(8)CA1, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
BOOTFLASH: RSP Software (RSP-BOOT-M), Version 12.2(2)T1,  RELEASE SOFTWARE (fc2)

Sprintgate uptime is 5 weeks, 3 days, 12 hours, 11 minutes
System returned to ROM by reload at 17:59:20 PDT Thu May 17 2001
System restarted at 11:39:29 PST Fri Nov 16 2001
System image file is "slot0:rsp-pv-mz.122-2.T1.bin"

cisco RSP4 (R5000) processor with 262144K/2072K bytes of memory.
R5000 CPU at 200Mhz, Implementation 35, Rev 2.1, 512KB L2 Cache
Last reset from power-on
G.703/E1 software, Version 1.0.
G.703/JT2 software, Version 1.0.
X.25 software, Version 3.0.0.
Primary Rate ISDN software, Version 1.1.
Chassis Interface.
1 HIP controller (1 HSSI).
1 FSIP controller (8 Serial).
1 MIP controller (2 T1).
1 VIP2 controller (2 FastEthernet)(8 Serial).
1 FEIP controller (2 FastEthernet).
4 FastEthernet/IEEE 802.3 interface(s)
16 Serial network interface(s)
1 HSSI network interface(s)
2 Channelized T1/PRI port(s)
123K bytes of non-volatile configuration memory.

20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
16384K bytes of Flash PCMCIA card at slot 1 (Sector size 128K).
8192K bytes of Flash internal SIMM (Sector size 256K).

Slave in slot 2 is running Cisco Internetwork Operating System Software
IOS (tm) RSP Software (RSP-DW-M), Version 12.2(2)T1,  RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 18-Jul-01 05:22 by ccai
Slave: Loaded from system
Slave: cisco RSP4 (R5000) processor with 262144K bytes of memory.

Configuration register is 0x102
```

In order to satisfy the requirement, I address the following questions as outlined in the "Auditing Networks, Perimeters, and Systems GSNA Practical Assignment Version 1.2 (amended October 26, 2001)

The questions include:

- What is the current state of practice, if any?
    - Why are current methods and techniques in need of improvement?
    - What can be measured objectively?
    - What must be measured subjectively
    - For each objective or subjective test in your checklist or procedure, how do you know when a system is out of spec?

In addressing these questions I will use the format provided by Ruangkrai Rangsiphol in his GSNA Version 1.2 document (http://www.giac.org/practical/Ruangkrai_Rangsiphol_GSNA.zip)

In respond to the above questions, it can be classified into four criteria.

1. Improvement Needed
2. Objective Measurement
3. Subjective Measurement
4. Criteria

Current State of the Practice

The current state of the auditing practice is shown by Justin Snyder 1/10/2001 at http://www.auditnet.org/docs/Cisco%20Router%20Audit%20Program.txt. This audit checklist pertains to routers in general. My focus will be specifically on perimeter routers. However I will use the Snyder router audit document as the basis for comparison. I will also be taking for extensive amount of information on how to secure a Cisco router to add and improve upon the audit tasks shown in the Snyder document. Much of the other information available on the Internet and in publications consists of recommendations on how to configure a router to improve its security. However, there much less information available on how to audit a Cisco router. There is even less information on how to audit a perimeter router.

The following address the additions to the Snyder router audit document. The original is used as the standard. Below each standard are my modifications.

Overview

Standard: Determine personnel responsible for the Cisco Routers.

Improvement Needed:

- Identify the applications that used to monitor the routers.
- Determine personnel not responsible for the routers. Personnel handling the internal network routers may not be the same personnel handling the perimeter routers.

Objective Measurement:

Personnel can be determined by looking in the router configuration.

AAA Authentication

```
NOV7206-1#show configuration | begin aaa
aaa new-model
aaa authentication login default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
```

The above shows that the users are located on a tacacs server. Use the following command to find the tacacs server.

```
NOV7206-1#show tacacs
Server: 10.12.100.25/49: opens=423 closes=422 aborts=34 errors=62
        packets in=6388 packets out=6847 timeout=10 connection_fails=0
expected replies=0
        connection 633FE76C state=CLOSEWAIT

Server: 10.12.100.27/49: opens=8 closes=7 aborts=0 errors=45
        packets in=64 packets out=74 timeout=8 connection_fails=0 expected
replies=0
        connection 6344BB4C state=CLOSEWAIT
```

Obtain access to the AAA server to determine the personnel who have access to the routers.

Subjective Measurement:

Confirm that each account and authorization level matches up with the personnel and their responsibility area.

Criteria:

- Each account with authorization to access the router must be unique and assigned to a single real user or application.
- Group user or application accounts are not permitted.
- Unnecessary accounts must be removed.
- The personnel who manage AAA servers do not implicitly have access to the routers.

Standard: Obtain population of Cisco routers (including numbers and types)
Improvement Needed:

Objective Measurement:

- The traceroute command can reveal the address of the perimeter router. Another option is to telnet into a router on the inside network and search for the next hop address associated with the default route. Repeating the same process will lead to the perimeter router.
- Use nmap to scan the Cisco router

```
nmap -sS -O 10.1.1.0/24
```

Choose the network nearest to the exit points of the internal network.

Subjective Measurement:

Documentation obtained from personnel may not be up to date or accurate.

Criteria:

Telnet to each perimeter router and check for a connection to the internal network and the external network.

Standard: Obtain the router configuration file for each router.
Improvement Needed:

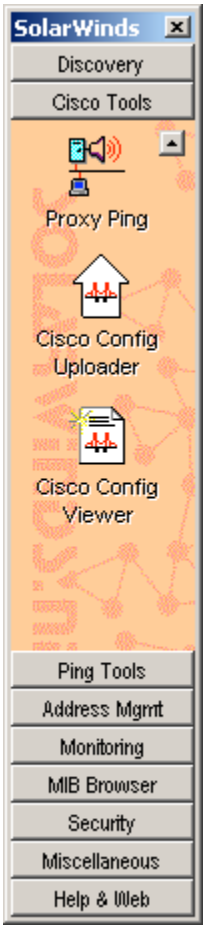
Get the running configuration for each router.

Objective Measurement:

- Telnet into each router and perform the following command.

```
NOV7206-1#show running configuration
```

- Use Solarwinds Cisco Config Viewer to pull the configuration. The IP address and the RW Community string are needed.



Subjective Measurement:

If the configurations are obtained from personnel

Criteria:

The configurations must be the actual active configurations.

Authentication

Standard: Determine the types of accounts that were used to access the routers. A user account can be defined with **enable** privileges with this entry in the configuration file: username **user-ID** privilege 15 password 7 **encryptyed_hash**.

Improvement Needed:

Also determine the accounts that may be located on an AAA server.

Objective Measurement:

```
NOV7206-1#show configuration | begin aaa
aaa new-model
aaa authentication login default group tacacs+ enable
```

aaa authorization exec default group tacacs+ if-authenticated

Subjective Measurement:

Privilege levels must match the level of access required to perform their duties.

Criteria:

Users and their privilege levels must be documented. Privilege levels and roles must be defined. The commands associated with each privilege level must also be documented.

Standard: Determine what users had access to these accounts.

Improvement Needed:

Objective Measurement:

Subjective Measurement:

Interviews with personnel should validate that user accounts and passwords are not being shared. Also personnel must be checked to validate that no one is using system accounts to access the router

Criteria:

A user account policy must be in place that states that the sharing of account information and password information is not allowed.

Standard: Were access attempts to the routers logged?

Improvement Needed:

Attempted access must be logged on a separate logging server.

Objective Measurement

```
NOV7206-1#show logg
Syslog logging: enabled (0 messages dropped, 950 messages rate-limited, 0
flushes, 0 overruns)
    Console logging: disabled
    Monitor logging: level debugging, 3329 messages logged
    Buffer logging: level debugging, 35292 messages logged
    Logging Exception size (8192 bytes)
    Trap logging: level debugging, 8290 message lines logged
        Logging to 10.12.100.27, 8290 message lines logged
        Logging to 10.12.100.245, 8290 message lines logged
```

Check for “Trap logging: level debugging”. Verify the logs for access attempts on the logging servers. The servers are indicated on the last two lines show as “logging to”.

Subjective Measurement

Determine if the syslog server is adequately secured and that the appropriate personnel are reviewing the logs.

Criteria

The logging level must be at either at least 2 (critical) to log telnet and console access. Logging must be to syslog servers no located on the router.

Standard: Determine if all accounts had passwords and determine the strength of the passwords.

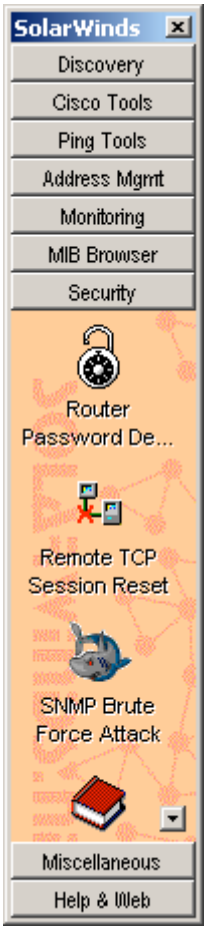
Improvement Needed:

The enable password must use strong encryption.
Passwords must be encrypted on the router configuration.

Objective Measurement

```
ROUTER#show configuration
…
service password-encryption

enable secret 5 <removed>
enable password 7 <removed> ← this should not be present
…
line con 0
 exec-timeout 5 0
 password 7 <removed>
 logging synchronous
line aux 0
line vty 0 4
 exec-timeout 20 0
 password 7 <removed>
 logging synchronous
 transport input telnet
line vty 5 15
 exec-timeout 20 0
 password 7 <removed>
 logging synchronous
 transport input telnet
```

Use solarwinds to decrypt password 7 passwords.



Subjective Measurement

Interview personnel to validate that their user passwords to not match the routers local enable password.

Criteria

Check for the line “service password-encryption”
Check the configuration of the router. Check for the presence of only an enable secret password. Make sure there is not an enable password. The enable password 7 can be decrypted with tools such as solarwinds. Verify that those passwords follow the minimum length and special character requirements. Attempted to log into privileged mode with the decrypted password 7 passwords. Make sure that they do not match.

Standard: Determine if there was a mechanism for periodically changing passwords.

Improvement Needed

Objective Measurement

```
NOV7206-1#show conf
Using 22114 out of 129016 bytes
!
! Last configuration change at 20:49:57 PST Fri Dec 14 2001 by richter
```

```
! NVRAM config last updated at 20:51:57 PST Fri Dec 14 2001 by richter
```

Subjective Measurement

Interview the personnel to determine the last password change. Determine if their understanding of the password change policy matches the documented policy. Determine the process and the tools used.

Criteria

In the router configuration, verify that the date of the last change is either the last date of the scheduled password change or after. Verify that the requirements for changing the password are documented. Verify that the process for changing the passwords is documented. Verity with syslog log files that the password has changed.

If tools are used for scheduling password changes, check for the existence of templates or jobs for the activity.

Standard: No standard exists to warn users that unauthorized access is not permitted

Improvement Needed

A login banner must be presented to warn users that only authorized access is permitted.

Objective Measurement

Telnet to the router to view banner or check the configuration for the following.

```
! Banner to discourage unauthorized access

banner motd ^CCC

 +---------------------------------------------------------------------+
 |                                                                     |
 |  Warning **** Warning **** Warning **** Warning **** Warning **** Warning  |
 |                                                                     |
 |                              City of Metropolis                     |
 |                                                                     |
 | This system is for authorized network administrators only!          |
 |                All activities are recorded and monitored!           |
 |                                                                     |
 | Any unauthorized access, attempted access, or Illegal use may be a felony  |
 |    offense punishable under section 502 of the California Penal Code and   |
 |                              applicable Federal Law.                |
 |                                                                     |
 +---------------------------------------------------------------------+

^C
```

Subjective Measurement

Criteria

The configuration should contain the statement shown above in the objective measurement section.

SNMP - The simple network management protocol (SNMP) is a protocol used to manage a network. The protocol allows the viewing and changing of router settings. An SNMP community name can have either read or read/write access. The community names act as passwords.

Standard: Was simple network management protocol (SNMP) used to configure the network?
Improvement Needed: The statement should be rephrased to question if SNMP is currently used to configure the network.

Objective Measurement

```
NOV7206-1#show snmp
Chassis: 23688085
1402829 SNMP packets input
    0 Bad SNMP version errors
    24 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    15185156 Number of requested variables
    17 Number of altered variables
    952675 Get-request PDUs
    449402 Get-next PDUs
    20 Set-request PDUs
1431241 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    73 No such name errors
    0 Bad values errors
    0 General errors
    1402805 Response PDUs
    28436 Trap PDUs

SNMP logging: enabled
    Logging to 10.12.100.25.162, 0/10, 8008 sent, 419 dropped.
    Logging to 10.12.100.27.162, 0/10, 8008 sent, 419 dropped.
    Logging to 10.8.64.53.162, 0/10, 7982 sent, 445 dropped.
    Logging to 10.12.100.245.162, 0/10, 3134 sent, 15 dropped.
```

Subjective Measurement:

Determine how snmp is used. Is it necessary to have snmp enabled?

Criteria

Check the “show snmp” output. Check for the presence out snmp output response PDU’s. If the number is positive then snmp is enabled. Also check for the presence of “SNMP logging: enabled”. From interviews with personnel, check if management tools need or

users actually need snmp enabled. Documentation of the need must be present in policy or operations manuals.

Standard: Determine the version of SNMP employed by the Company. Version one stores community names in clear-text format. Version two adds encryption of community names.

Improvement Needed:

The standard should be restated to used snmp v2 with encrypted community names where possible.

Objective Measurement

```
NOV7206-1#show snmp group
groupname: ILMI                           security model:v1
readview :*ilmi                           writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                           security model:v2c
readview :*ilmi                           writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: kiwi                           security model:v1
readview :<no readview specified>         writeview: <no writeview
specified>
notifyview: *tv.FFFFFFFF.FFFFFFFF
row status: active

groupname: kiwi                           security model:v2c
readview :<no readview specified>         writeview: <no writeview
specified>
notifyview: *tv.FFFFFFFF.FFFFFFFF
row status: active

groupname: elgin3b                        security model:v1
readview :v1default                       writeview: <no writeview
specified>
notifyview: *tv.FFFFFFFF.FFFFFFFF
row status: active

groupname: elgin3b                        security model:v2c
readview :v1default                       writeview: <no writeview
specified>
notifyview: <no notifyview specified>
row status: active

groupname: gtfoomr4r                      security model:v1
readview :v1default                       writeview: v1default
notifyview: <no notifyview specified>
row status: active

groupname: gtfoomr4r                      security model:v2c
readview :v1default                       writeview: v1default
notifyview: <no notifyview specified>
row status: active
```

Subjective Measurement:

Interview personnel to determine the management platforms using snmp. Determine if snmp v2 or v3 is supported.

Criteria

Determine if the management tools using snmp will support version 2 or version 3. If snmp v2 or v3 us supported then the routers should be using snmp v2 or v3. Determine the version that the router is using by the evaluating the output of the "show snmp group" command under security model.

Standard: Determine the SNMP community names. This could be determined by looking at the configuration file. Cisco routers had two default SNMP community strings (used as passwords): *public* for read access and *private* for read/write access.
Improvement Needed

Objective Measurement

```
NOV7206-1#show snmp group
groupname: ILMI                           security model:v1
readview :*ilmi                           writeview: *ilmi
notifyview: <no notifyview specified>
row status: active
```

Subjective Measurement

Criteria

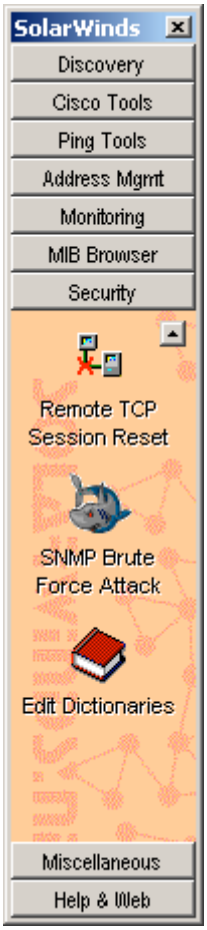
The community names are shown in the "show snmp group" output. The readview is the RO string the writeview is the RW string.

Standard: Determine if the routers incorporate strong SNMP community names. Were they changed from the defaults?
Improvement Needed

Objective Measurement

```
NOV7206-1#show snmp group
groupname: ILMI                           security model:v1
readview :*ilmi                           writeview: *ilmi
notifyview: <no notifyview specified>
row status: active
```

Solarwinds can be used to perform an snmp brute force attack.



Subjective Measurement

Criteria

Verify that the readview and writeview string is not public or private. Verify that the strings are not dictionary words and contain at least one special character.

Standard: Determine which sites were able to use the given SNMP community names. Cisco routers could restrict SNMP access to *set* operations, which change router variables, to certain IP addresses.

Improvement Needed

Objective Measurement

```
ROUTER#show configuration
…
! This list is applied under the vty (telnet) and SNMP commands

access-list 88 permit 10.129.4.254
access-list 88 permit 10.129.5.8
access-list 88 permit 10.129.5.9
access-list 88 deny   any
```

```
! Access list applied to SNMP limiting the addresses that have  ReadWrite
and who has ReadOnly access

snmp-server community <removed> RW 88
snmp-server community <removed> RO 88
```

Subjective Measurement

Criteria

Verify that an access-list is defined and applied to the “snmp-server community” command.

Standard: Determine if SNMP community names could be obtained though the configuration file. The configuration file was used to store most of the configuration settings of the router. Even though this file is binary, the setting (including SNMP community names) was stored as clear-text.

Improvement Needed

Objective Measurement

Subjective Measurement

Determine where the configurations are stored. Verify that only authorized personnel have access to configuration files.

Criteria

Accesses to configuration files are located in protected shares. Access to these shares is limited to authorized personnel.

Standard: Determine whether the Company implemented encryption for set requests from SNMP read/write community names.

Improvement Needed

Objective Measurement

```
NOV7206-1#show snmp group
groupname: ILMI                          security model:v1
readview :*ilmi                          writeview: *ilmi
notifyview: <no notifyview specified>
row status: active
```

Subjective Measurement

Obtain a list of management platforms and their version. Determine if the platforms will support snmp v3 or v2.

Criteria

If the management platforms support snmp v3 or v2 then the routers should be configured for either v3 or v2. Use a sniffer to capture snmp data and verify that the snmp community cannot be read.

Standard: Determine the frequency of SNMP community name changes.

Improvement Needed

Objective Measurement

Subjective Measurement

Interview personnel to determine the frequency of snmp community name changes.

Criteria

Verify in syslog files the change of snmp community strings. Verify that the change frequency matches that specified in a policy document.

Standard: Cisco provides support for an old MIB called OLD-CISCO-SYS-MIB that allows anyone with the read/write community name to TFTP download the configuration file. Determine if the Company's Cisco routers are vulnerable.

Improvement Needed

Starting generally from Cisco IOS® software release 12.0 (on some devices, as early as release 11.2P), Cisco has implemented a new means of Simple Network Management Protocol (SNMP) configuration management using the new CISCO-CONFIG-COPY-MIB. This MIB replaces the deprecated configuration section of the OLD-CISCO-SYSTEM-MIB. For details see http://www.cisco.com/warp/customer/477/SNMP/copy_configs_snmp.shtml

Objective Measurement

Perform a show version.

```
Cisco Internetwork Operating System Software
IOS (tm) RSP Software (RSP-PV-M), Version 12.2(2)T1,  RELEASE SOFTWARE
(fc2)
```

Subjective Measurement

Criteria

Modifications to the configuration can be performed if the Ios is 12.0 or greater.

Control of Services

Standard: Determine which services were running on the routers. The key services to evaluate were trivial file transfer protocol (TFTP), simple network management protocol (SNMP), file transfer protocol (FTP), and telnet.

Improvement Needed

Http, ident, bootp, echo, chargen, and discard should also be disabled.

Objective Measurement

The following commands should be found in the configuration file.

Turn off unneeded servers on the router: TCP and UDP small servers include echo, chargen, and discard.

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

Disable async line bootp service

```
no ip bootp server
```

A defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled, browsing to "http://router-ip/anytext?/" is attempted, and the enable password is supplied when requested. This defect can be exploited to produce a denial of service (DoS) attack.

```
no ip http server
```

The ip identd command returns accurate information about the host TCP port; however, no attempt is made to protect against unauthorized queries.

```
no ip identd
```

Disable boot configuration from network.

```
no service-configuration
```

Subjective Measurement

Criteria

The configuration should contain the statement shown above in the objective measurement section.

Standard: There is no standard for source routing.
Improvement Needed:

The standard should state disabling of source routing. IP source routing is almost never used for legitimate purposes and can sometimes be used to transport packets to parts of the network from which they should be blocked

Objective Measurement

```
ROUTER#Show conf
…
no ip source-route
```

Subjective Measurement

Criteria

The configuration should contain the statement shown above in the objective measurement section.

Standard: Determine if open shortest path first (OSPF) was defined on the router. Determined the authentication mechanism that was employed in the Company's implementation of OSPF.
Improvement Needed

The standard should also include the eigrp routing protocol. Eigrp supports MD5 hashed routing updates.

Objective Measurement

Subjective Measurement

Criteria

Standard: Determine whether directed broadcast functionality was enabled on the router. This setting, if enabled, could allow a denial-of-service (DoS) attack of the network (Smurf attack).

Improvement Needed

Objective Measurement

```
ROUTER#show configuration
…
No ip directed-broadcasts
```

Subjective Measurement

Criteria

The configuration should contain the statement shown above in the objective measurement section. Send a directed broadcast to the router and verify with a sniffer that the broadcast is not propagated.

Standard: No standard exists for ad-hoc routing.

Improvement Needed

Disable Ac-Hoc routing.

Objective Measurement

```
ROUTER#show configuration
…
No –ip proxy-arp
```

Subjective Measurement

Criteria

The configuration should contain the statement shown above in the objective measurement section.

Standard: Cisco's finger service will respond with some useless information, which can help an attacker identify the device as a Cisco device. Determine if the Company's routers respond to the finger service with valuable information.

Improvement Needed

Objective Measurement

Finger protocol can be used to gather one half of a username/password combination.

```
ROUTER#show configuration
…
no service finger
```

Subjective Measurement

Criteria

The configuration should contain the statement shown above in the objective measurement section. Use nmap to verify that the services have been disabled.

Standard: No standard exists for Cisco Discovery Protocol.

Improvement Needed

ISP. Cisco Discovery Protocol (CDP) is primarily used to obtain protocol addresses of neighboring devices and discovers the platform of those devices. CDP can also be used to show information about the interfaces your router uses. CDP is media- and protocol-independent, and runs on all Cisco-manufactured equipment including routers, bridges, access servers, and switches. CDP service should be disabled.

Objective Measurement

```
ROUTER#show configuration
...
no cdp enable
```

Subjective Measurement

Criteria

The configuration should contain the statement shown above in the objective measurement section.

Standard: Attackers can connect to Cisco management ports 2001, 4001, and 6001 to help identify the device as a Cisco device. The result of connecting to one of these ports via a browser might look like this: User Access Verification Password: Password: Password: Password: % Bad passwords

Improvement Needed

Access to ports 2001, 4001, and 6001 should only be allowed to be accessed from management stations.

Objective Measurement

```
ROUTER#show access-lists

Access-list 101 permit …
Access-list 101 permit tcp 10.1.1.2 any eq 2001
Access-list 101 permit tcp 10.1.1.2 any eq 4001
Access-list 101 permit tcp 10.1.1.2 any eq 6001
Access-list 101 permit udp 10.1.1.2 any eq 2001
Access-list 101 permit udp 10.1.1.2 any eq 4001
Access-list 101 permit udp 10.1.1.2 any eq 6001

ROUTER#show config
…
Interface Ethernet0
  Access-group 101 in
```

Subjective Measurement

Interview the personnel who manage the routers to determine if any management stations require ports 2001, 4001, 6001.

Criteria

Access Control List must be present to restrict access to ports 2001, 4001, and 6001.

Standard: Another of Cisco's common ports is the XRemote service port (TCP 9001). The XRemote allows systems on your network to start client Xsessions to the router (typically through a dial-up modem). When an attacker connects to the port, the device will send back a common banner, such as: ---Outbound XRemote Service---

Improvement Needed

Access to ports 9001 should only be allowed to be accessed from management stations if necessary.

Objective Measurement

```
ROUTER#show access-lists
Access-list 102 permit …
Access-list 102 permit tcp 10.1.1.2 any eq 9001
Access-list 102 permit udp 10.1.1.2 any eq 9001

ROUTER#show config
…
Interface Ethernet0
  Access-group 102 in
```

Subjective Measurement

Interview the personnel who manage the routers to determine if any management stations require ports 9001.

Criteria

Access Control List must be present to restrict access to ports 9001.

Routing Authorized Traffic

There is no standard defined for passing only authorized traffic.

Standard: No standard exists for filtering unnecessary or malicious traffic.

Improvement Needed

The standard should state that unnecessary or malicious traffic should be dropped.

Objective Measurement

IP extended access list applied to the perimeter router input from the Internet

Block packets that claim to have the same source address as the internal network

```
access-list 101 deny   ip 64.85.238.0 0.0.0.63 any log-input
```

Block packets that are sourced from reserved private addresses

```
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any
```

Block loopback packets

```
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any log-input
```

Block known addresses known to be used for attacks

```
access-list 101 deny   ip 169.254.0.0 0.0.255.255 any log-input
```

Block multicast packets

```
access-list 101 deny   ip 224.0.0.0 31.255.255.255 any log-input
```

Block broadcast

```
access-list 101 deny   ip 0.0.0.0 0.255.255.255 any log-input
```

Block unneeded tcp and udp services

```
access-list 101 deny   tcp any any eq 1
access-list 101 deny   udp any any eq 1
access-list 101 deny   tcp any any eq echo
access-list 101 deny   udp any any eq echo
access-list 101 deny   tcp any any eq discard
access-list 101 deny   udp any any eq discard
access-list 101 deny   tcp any any eq 11
access-list 101 deny   tcp any any eq daytime
access-list 101 deny   udp any any eq 13
access-list 101 deny   tcp any any eq 15
access-list 101 deny   tcp any any eq chargen
access-list 101 deny   udp any any eq 19
access-list 101 deny   tcp any any eq 37
access-list 101 deny   udp any any eq time
access-list 101 deny   tcp any any eq whois
access-list 101 deny   udp any any eq bootps
access-list 101 deny   udp any any eq tftp
access-list 101 deny   tcp any any eq 76
access-list 101 deny   tcp any any eq 93
access-list 101 deny   tcp any any eq sunrpc log-input
access-list 101 deny   udp any any eq sunrpc log-input
access-list 101 deny   tcp any any eq 135
access-list 101 deny   udp any any eq 135
access-list 101 deny   tcp any any eq 137
access-list 101 deny   udp any any eq netbios-ns
access-list 101 deny   tcp any any eq 138
access-list 101 deny   udp any any eq netbios-dgm
access-list 101 deny   tcp any any eq 139
access-list 101 deny   udp any any eq netbios-ss
access-list 101 deny   tcp any any eq login
access-list 101 deny   udp any any eq who
access-list 101 deny   tcp any any eq cmd
access-list 101 deny   udp any any eq syslog
access-list 101 deny   tcp any any eq 550
access-list 101 deny   udp any any eq 550
```

Block incoming telnet

```
access-list 101 deny   tcp any any eq telnet log-input
```

Block DNS zone transfer

```
access-list 101 deny   tcp any any eq domain log-input
```

Allow DNS response

```
access-list 101 permit udp any eq domain 64.85.238.0 0.0.0.63
```

Allow Network Time Protocol (NTP) from only one host

```
access-list 101 permit udp host 192.5.41.209 eq ntp host 64.85.238.26 eq
ntp
access-list 101 deny   udp any any eq ntp
```

Block Simple Network Management Protocol (SNMP) requests and traps

```
access-list 101 deny   udp any any eq snmp log-input
access-list 101 deny   udp any any eq snmptrap
access-list 101 deny   tcp any any eq 161
access-list 101 deny   tcp any any eq 162
! Allow return TCP traffic (established)
access-list 101 permit tcp any 64.85.238.0 0.0.0.63 established
```

Block all ICMP traffic

```
access-list 101 deny   icmp any any
access-list 101 deny   icmp any any redirect log-input
```

Allow any other IP traffic destined the inside network

```
access-list 101 permit ip any 64.85.238.0 0.0.0.63 log-input
```

Subjective Measurement

Criteria

The configuration should contain the statement shown above in the objective measurement section. Use a packet generator such as packet factory to generate packets that should be dropped by the router. Use a sniffer on the inside of the router to verify that the packets have been dropped.

Remote Access

Standard: Were dial-in connections used to access the routers.

Improvement Needed

Dial-in connections to the router should not be active be default. Dial-in access should only be enabled when is support is necessary.

Objective Measurement

```
ROUTER#show configuration
…
line aux 0
transport in all
shutdown
```

Subjective Measurement

Interview personnel to determine if the modems are normally shut down.

Criteria

A manual process should be documented for connecting or enabling a modem connection when necessary. Identify the modems connected to the perimeter routers and verify that they are shutdown.

Standard: Obtain population of routers with modems and obtain the telephone numbers of the routers.

Improvement Needed

Objective Measurement

Subjective Measurement

Criteria

Standard: Determine if users were properly authenticated when remotely accessing the routers.

Improvement Needed

Objective Measurement

Subjective Measurement
Criteria

Standard: Determine if access attempts were logged.
Improvement Needed
Objective Measurement
Subjective Measurement
Criteria
Connect to a modem and verify that the login attempt is logged.

Standard: Determine if the telephone numbers of the routers were within Company defined telephone prefixes. Hackers commonly poll prefixes to obtain access to a network.
Improvement Needed
Objective Measurement
Subjective Measurement
Interview personnel and obtain phone number list for routers.
Criteria
Verify that phone number list for routers is outside the range of that assigned to the company.

Change Management

Standard: Determine how changes to the router environment were made.
Improvement Needed
Objective Measurement
Subjective Measurement
Interview the personnel to determine if there is a standard process for making changes.
Criteria
Documentation of change process must be available.

Standard: Determine if changes to the router configuration were documented.
Improvement Needed
Objective Measurement
Subjective Measurement
Criteria
A history of changes must be available.

Standard: Were there procedures for changing router configurations?
Improvement Needed
Objective Measurement
Subjective Measurement
Criteria
Documentation of the change process must be available.

Standard: Was there a separation of duties within the change control of the router environment?
Improvement Needed
Objective Measurement
Subjective Measurement
Criteria

Verify that the personnel who make the changes to the router are not the same as those who created the configuration for the change.

Network Monitoring

Standard: Determine the mechanisms for monitoring the network.
Improvement Needed
Objective Measurement
Subjective Measurement

Interview personnel to get a list of monitoring tools.

Criteria

Verify that the perimeter routers are configured in the monitoring tool.

Standard: Determine the personnel that monitor the network.
Improvement Needed
Objective Measurement
Subjective Measurement
Criteria

Standard: Determine the security of the network monitoring tools.
Improvement Needed
Objective Measurement
Subjective Measurement

Interview the personnel responsible for managing the network monitoring tools.

Criteria

At a minimum user access should be restricted to only to authorized personnel.

Part 2 Application of Audit Technique to a Real World System

Item to be audited

I will be auditing a Cisco 7507 Router with IOS version 12.2(2)T1. The router acts as a perimeter router between the Internet and the outside interface of the enterprise firewall. The router will act as the first line of defense. It should be configured to filter unwanted packets from entering the enterprise network. The router should also be configured to reduce the number of events on the IDS system. The router itself should also be hardened to prevent it from being compromised.

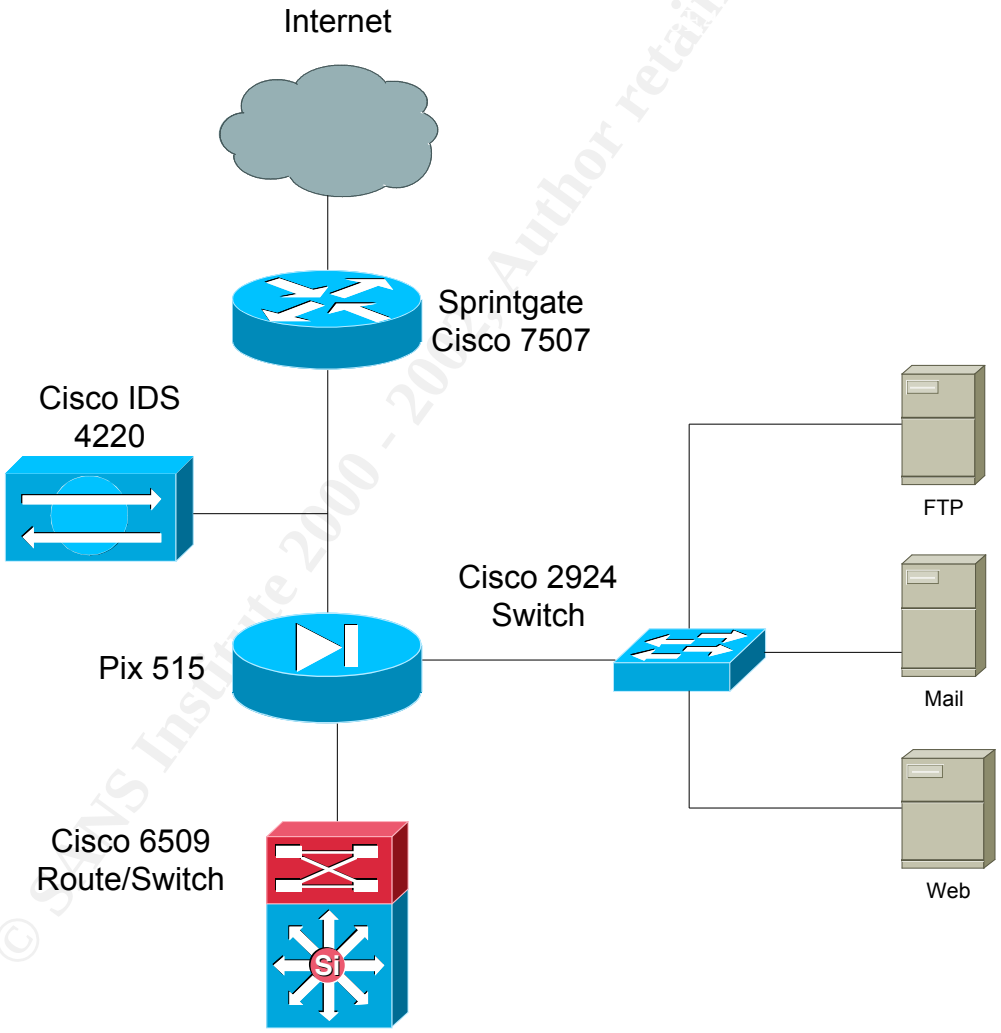
The version output for the router is show below.

```
Sprintgate#show ver
Cisco Internetwork Operating System Software
IOS (tm) RSP Software (RSP-PV-M), Version 12.2(2)T1,  RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 18-Jul-01 05:20 by ccai
Image text-base: 0x600109C8, data-base: 0x611D0000

ROM: System Bootstrap, Version 11.1(8)CA1, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
BOOTFLASH: RSP Software (RSP-BOOT-M), Version 12.2(2)T1,  RELEASE SOFTWARE (fc2)

Sprintgate uptime is 5 weeks, 6 days, 5 hours, 6 minutes
System returned to ROM by reload at 17:59:20 PDT Thu May 17 2001
System restarted at 11:39:29 PST Fri Nov 16 2001
System image file is "slot0:rsp-pv-mz.122-2.T1.bin"

cisco RSP4 (R5000) processor with 262144K/2072K bytes of memory.
R5000 CPU at 200Mhz, Implementation 35, Rev 2.1, 512KB L2 Cache
Last reset from power-on
G.703/E1 software, Version 1.0.
G.703/JT2 software, Version 1.0.
X.25 software, Version 3.0.0.
Primary Rate ISDN software, Version 1.1.
Chassis Interface.
1 HIP controller (1 HSSI).
1 FSIP controller (8 Serial).
1 MIP controller (2 T1).
1 VIP2 controller (2 FastEthernet)(8 Serial).
1 FEIP controller (2 FastEthernet).
4 FastEthernet/IEEE 802.3 interface(s)
16 Serial network interface(s)
1 HSSI network interface(s)
2 Channelized T1/PRI port(s)
123K bytes of non-volatile configuration memory.

20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
16384K bytes of Flash PCMCIA card at slot 1 (Sector size 128K).
8192K bytes of Flash internal SIMM (Sector size 256K).

Slave in slot 2 is running Cisco Internetwork Operating System Software
IOS (tm) RSP Software (RSP-DW-M), Version 12.2(2)T1,  RELEASE SOFTWARE (fc2)
```

```
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 18-Jul-01 05:22 by ccai
Slave: Loaded from system
Slave: cisco RSP4 (R5000) processor with 262144K bytes of memory.

Configuration register is 0x102
```

Risk to the System

The Sprintgate router acts as the only Internet connection for the enterprise.



Loss of the router would cut off the enterprise from the Internet. I will also stop e-commerce traffic using the ftp server, email server, and web servers. Compromise of the router can lead to rerouting traffic. This could be used in man-in-the-middle type attacks. However because there is an additional firewall, losing the router does not compromise the enterprise perimeter security.

Procedurally, the route must be must be configured for alert management. Availability of the router is critical to the enterprise. The configurations must be saved for recovery and any changes to the system are subject to change control. Any an authorized changes must be detected.

The Audit Items

Items to be audited include the following.

Overview

1. Standard: Determine personnel responsible for the Cisco Routers. Subjective:
2. Standard: Obtain population of Cisco routers (including numbers and types)
3. Standard: Obtain the router configuration file for each router.

Authentication

4. Standard: Determine the types of accounts that were used to access the routers. A user account can be defined with **enable** privileges with this entry in the configuration file: username **user-ID** privilege 15 password 7 Standard: Determine what users had access to these accounts.
5. Standard: Were access attempts to the routers logged?
6. Standard: Determine if all accounts had passwords and determine the strength of the passwords.
7. Standard: Determine if there was a mechanism for periodically changing passwords.
8. Standard: No standard exists to warn users that unauthorized access is not permitted
9. Standard: Was simple network management protocol (SNMP) used to configure the network?
10. Standard: Determine the version of SNMP employed by the Company. Version one stores community names in clear-text format. Version two adds encryption of community names.
11. Standard: Determine the SNMP community names. This could be determined by looking at the configuration file. Cisco routers had two default SNMP community strings (used as passwords): *public* for read access and *private* for read/write access.
12. Standard: Determine if the routers incorporate strong SNMP community names. Were they changed from the defaults?
13. Standard: Determine which sites were able to use the given SNMP community names. Cisco routers could restrict SNMP access to *set* operations, which change router variables, to certain IP addresses.
14. Standard: Determine if SNMP community names could be obtained though the configuration file. The configuration file was used to store most of the configuration settings of the router. Even though this file is binary, the setting (including SNMP community names) was stored as clear-text.

15. Standard: Determine whether the Company implemented encryption for set requests from SNMP read/write community names.
16. Standard: Determine the frequency of SNMP community name changes.
17. Standard: Cisco provides support for an old MIB called OLD-CISCO-SYS-MIB that allows anyone with the read/write community name to TFTP download the configuration file. Determine if the Company's Cisco routers are vulnerable.

Control of Services

18. Standard: Determine which services were running on the routers. The key services to evaluate were trivial file transfer protocol (TFTP), simple network management protocol (SNMP), file transfer protocol (FTP), and telnet.
19. Standard: There is no standard for source routing.
20. Standard: Determine if open shortest path first (OSPF) was defined on the router. Determined the authentication mechanism that was employed in the Company's implementation of OSPF.
21. Standard: Determine whether directed broadcast functionality was enabled on the router. This setting, if enabled, could allow a denial-of-service (DoS) attack of the network (Smurf attack).
22. Standard: No standard exists for ad-hoc routing.
23. Standard: Cisco's finger service will respond with some useless information, which can help an attacker identify the device as a Cisco device. Determine if the Company's routers respond to the finger service with valuable information.
24. Standard: No standard exists for Cisco Discovery Protocol.
25. Standard: Attackers can connect to Cisco management ports 2001, 4001, and 6001 to help identify the device as a Cisco device. The result of connecting to one of these ports via a browser might look like this: User Access Verification Password: Password: Password: Password: % Bad passwords
26. Standard: Another of Cisco's common ports is the XRemote service port (TCP 9001). The XRemote allows systems on your network to start client Xsessions to the router (typically through a dial-up modem). When an attacker connects to the port, the device will send back a common banner, such as: ---Outbound XRemote Service---

Routing Authorized Traffic

27. There is no standard defined for passing only authorized traffic.
28. Standard: No standard exists for filtering unnecessary or malicious traffic.

Remote Access

29. Standard: Were dial-in connections used to access the routers.
30. Standard: Obtain population of routers with modems and obtain the telephone numbers of the routers.

31. Standard: Determine if users were properly authenticated when remotely accessing the routers.
32. Standard: Determine if access attempts were logged.
33. Standard: Determine if the telephone numbers of the routers were within Company defined telephone prefixes. Hackers commonly poll prefixes to obtain access to a network.

Change Management

34. Standard: Determine how changes to the router environment were made.
35. Standard: Determine if changes to the router configuration were documented.
36. Standard: Were there procedures for changing router configurations?
37. Standard: Was there a separation of duties within the change control of the router environment?

Network Monitoring

38. Standard: Determine the mechanisms for monitoring the network.
39. Standard: Determine the personnel that monitor the network.
40. Standard: Determine the security of the network monitoring tools.

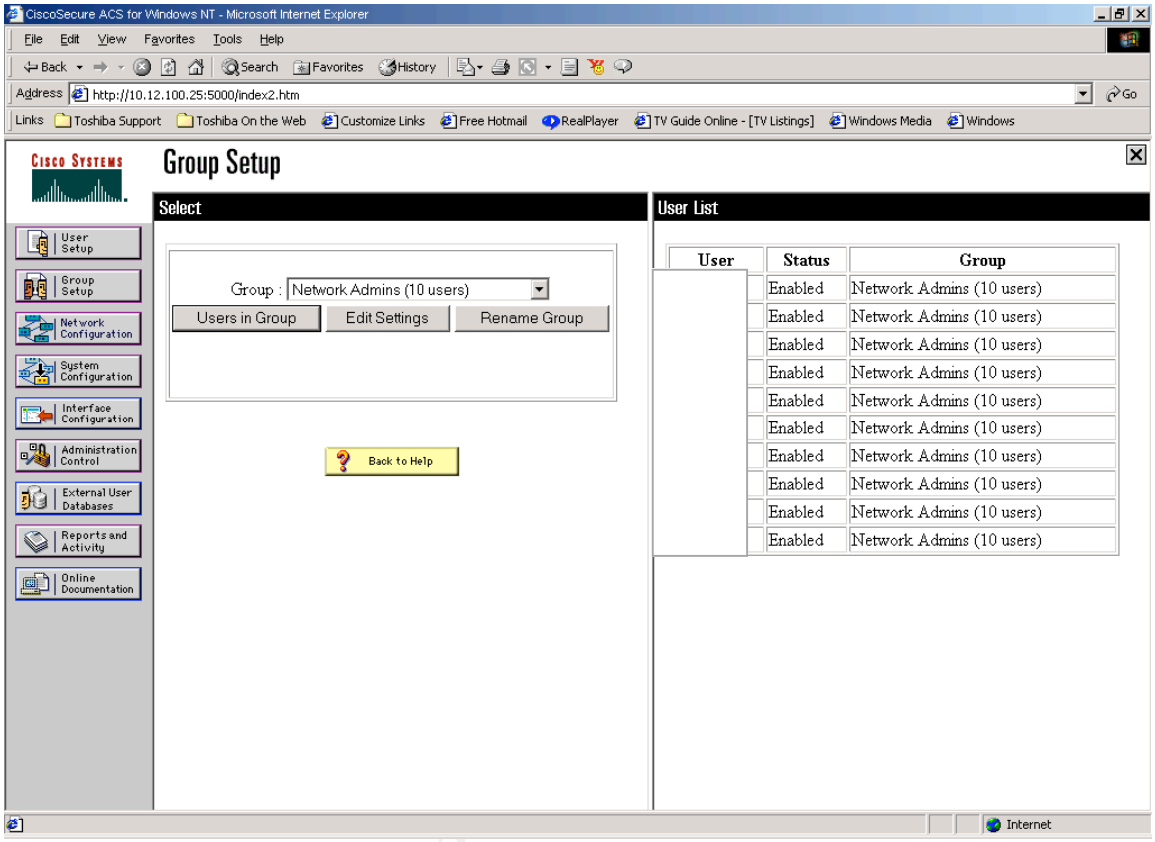
Results of Audit

Overview

1. Standard: Determine personnel responsible for the Cisco Routers.
   Subjective: Interviews with IT manager states that the following personnel should have full access to the perimeter router.
   CR. – VP
   CS. – Manager
   DR – Engineer
   SI – Engineer
   EF. – Engineer
   RW – Engineer
   MY. – Consultant
   Objective: Below shows the router configuration for router login.

```
aaa authentication login default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated

tacacs-server host 207.xx.xx.25 key <removed>
```

   Personnel access is controlled by tacacs. The personnel who have access are show below.



The diagram has been edited to hide the usernames. However, the unedited version shows the existence of a group consulting account and a vendor support account.

2. Standard: Obtain population of Cisco routers (including numbers and types)
   Objective: The is only one router one border router. This was done by physical verification of the Pix connection and the Sprintnet connection to the Internet.
3. Standard: Obtain the router configuration file for each router.
   Objective: The configuration was obtained locally through show run.

```
Sprintgate#show run
Using 8441 out of 126968 bytes
!
! Last configuration change at 16:19:34 PST Sat Dec 22 2001 by ingraham
! NVRAM config last updated at 16:19:35 PST Sat Dec 22 2001 by ingraham
!
version 12.2
no parser cache
no service single-slot-reload-enable
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service udp-small-servers
service tcp-small-servers
!
```

```
hostname Sprintgate
!
boot system flash slot0:rsp-pv-mz.122-2.T1.bin
logging buffered informational
logging rate-limit console 10 except errors
logging console notifications
aaa new-model
aaa authentication login default group tacacs+ enable
aaa authentication ppp default local group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa authorization network default group tacacs+
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting network default start-stop group tacacs+
enable secret 5 <revoved>
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
ip cef distributed
no ip domain-lookup
ip host net2-nt 207.xx.xx.27
ip host net-nt 207.xx.xx.25
!
no ip dhcp-client network-discovery
isdn voice-call-failure 0
!
controller T1 4/0
 shutdown
 framing esf
 linecode b8zs
!
controller T1 4/1
 shutdown
 framing esf
 linecode b8zs
!
!
interface Loopback0
 ip address 192.168.254.2 255.255.255.255
!
interface Hssi0/0
 bandwidth 45000
 no ip address
 no keepalive
 shutdown
 fair-queue
!
interface Serial1/0/0
 bandwidth 1536
 no ip address
 no ip mroute-cache
 shutdown
 no fair-queue
!
interface Serial1/0/1
 no ip address
 encapsulation frame-relay IETF
 ip route-cache flow
 no ip mroute-cache
 shutdown
 no fair-queue
 no arp frame-relay
```

```
 frame-relay lmi-type cisco
!
interface Serial1/0/2
 no ip address
 encapsulation frame-relay
 ip route-cache flow
 no ip mroute-cache
 shutdown
 no fair-queue
 no arp frame-relay
!
interface Serial1/0/3
 no ip address
 encapsulation frame-relay
 ip route-cache flow
 no ip mroute-cache
 shutdown
 no fair-queue
 no arp frame-relay
!
interface Serial1/0/4
 no ip address
 encapsulation frame-relay
 ip route-cache flow
 no ip mroute-cache
 shutdown
 no fair-queue
 no arp frame-relay
!
interface Serial1/0/5
 no ip address
 ip route-cache flow
 no ip mroute-cache
 shutdown
 no fair-queue
!
interface Serial1/0/6
 bandwidth 1544
 no ip address
 ip route-cache flow
 no ip mroute-cache
 shutdown
 no fair-queue
!
interface Serial1/0/7
 no ip address
 encapsulation frame-relay
 ip route-cache flow
 no ip mroute-cache
 shutdown
 no fair-queue
!
interface FastEthernet1/1/0
 ip address 192.168.254.6 255.255.255.252
 no ip redirects
 full-duplex
!
interface FastEthernet1/1/1
 no ip address
 no ip redirects
 shutdown
 full-duplex
!
```

```
interface FastEthernet5/0
 description To XXX SprintNet segment
 ip address 207.xx.xx.2 255.255.255.0
 no ip redirects
 full-duplex
 no cdp enable
!
!
interface FastEthernet5/1
 ip address 208.xx.xx.3 255.255.255.0
 no ip redirects
 full-duplex
!
interface Serial6/0
 description To Sprintlink (Prvt. Line# 376242) T-1 circuit ID: _______________
 bandwidth 1536
 ip address 144.223.57.2 255.255.255.252
 ip access-group border in
 no ip mroute-cache
 no fair-queue
!
interface Serial6/1
 bandwidth 1544
 no ip address
 no ip mroute-cache
 shutdown
!
interface Serial6/2
 no ip address
 no ip mroute-cache
 shutdown
!
interface Serial6/3
 no ip address
 no ip mroute-cache
 shutdown
!
interface Serial6/4
 no ip address
 no ip mroute-cache
 shutdown
!
interface Serial6/5
 no ip address
 no ip mroute-cache
 shutdown
!
interface Serial6/6
 no ip address
 no ip mroute-cache
 shutdown
!
interface Serial6/7
 no ip address
 no ip mroute-cache
 shutdown
!
router bgp 2xxxx
 no synchronization
 bgp log-neighbor-changes
 network 207.xx.xx.0
 network 208.xx.xx.0
 neighbor 144.xx.xx.1 remote-as xxxx
```

```
 neighbor 144.xx.xx.1 route-map asxxxx-incoming in
 neighbor 144.xx.xx.1 route-map asxxxx-outgoing out
no auto-summary
!
ip classless
no ip forward-protocol udp netbios-ns
no ip forward-protocol udp netbios-dgm
ip route 0.0.0.0 0.0.0.0 Serial6/0
ip route 192.168.254.1 255.255.255.255 192.168.254.5
no ip http server
ip as-path access-list 1 permit ^1239_
ip as-path access-list 2 permit ^701_
!
!
ip access-list extended border
 permit ip host 64.xx.xx.67 any
 permit icmp host 144.xxx.xx.1 host 144.xxx.xx.2
 permit tcp host 144.xxx.xx.1 host 144.xxx.xx.2 eq bgp
 permit tcp host 144.xxx.xx.1 eq bgp host 144.xx.xx.2
 deny   ip 207.xx.xxx.0 0.0.0.255 any log-input
 deny   ip any 10.0.0.0 0.255.255.255 log-input
 deny   ip any 192.168.0.0 0.0.255.255 log-input
 deny   ip any 172.16.0.0 0.15.255.255 log-input
 permit ahp any host 208.xxx.xxx.60
 permit esp any host 208.xxx.xxx.60
 permit tcp any host 208.xxx.xxx.60 eq 500
 permit udp any host 208.xxx.xxx.60 eq isakmp
 permit tcp any host 208.xxx.xxx.60 eq 50
 permit udp any host 208.xxx.xxx.60 eq 50
 deny   ip any host 208.xxx.xxx.60 log-input
 permit ip any 208.xxx.xxx.0 0.0.0.255
 permit ip any 207.xx.xxx.0 0.0.0.255
 permit udp host 192.5.5.250 host 144.xxx.xx.2 eq ntp
 deny   ip any any log-input
logging history size 300
logging trap warnings
logging 207.xx.xx.25
logging 207.xx.xx.245
access-list 10 permit 208.xx.xx.0 0.0.0.255
access-list 20 permit 207.xx.xx.0 0.0.0.255
access-list 110 permit ip host 64.xx.xx.67 any
access-list 110 permit tcp 207.xx.xx.0 0.0.0.255 host 0.0.0.0 eq telnet log-input
access-list 110 deny   ip any any log-input
!
!
route-map as21xx-incoming permit 10
 match as-path 2
 set local-preference 150
!
route-map as21xx-incoming permit 20
 match ip address 10
 set local-preference 210
!
route-map as12xx-incoming permit 10
 match as-path 1
 set local-preference 200
!
route-map as12xx-outgoing permit 10
 match ip address 10
 set metric 20
 set as-path prepend 21xx 21xxx
!
route-map as12xx-outgoing permit 20
```

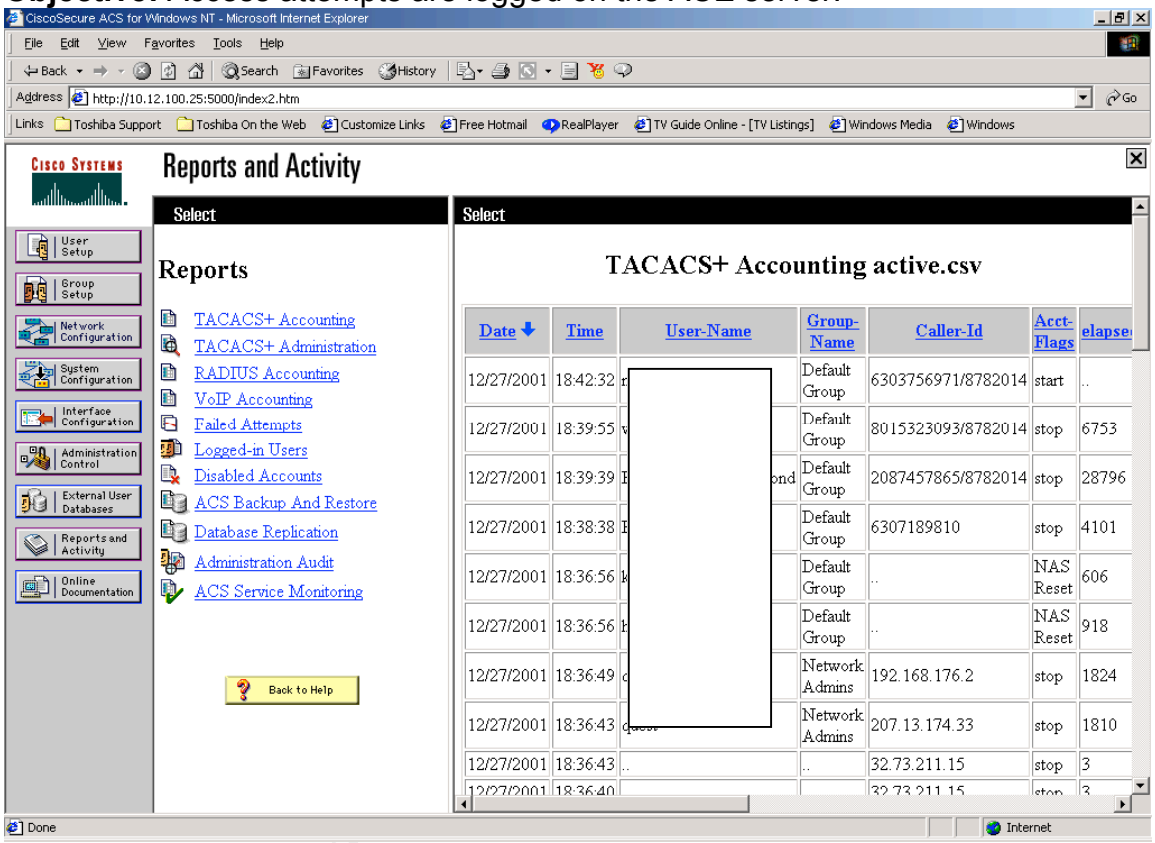
```
 match ip address 20
 set metric 10
!
snmp-server engineID local 000000090200001079358820

!
tacacs-server host 207.xx.xx.25 key <removed>
banner motd ^C


                L E G A L   N O T I C E
               ---------------------------------------


>>>>>>>>>>>>>>> This system is restricted to private use.
               All others log out NOW!
**************************************************************************
*                                                                        *
*                                                                        *
*               This network is protected by a security system.          *
*               Criminal law prohibits unauthorized use.                 *
*               Violators will be prosecuted.                            *
*                                                                        *
*                                                                        *
*                                                                        *
**************************************************************************

^C
!
line con 0
line aux 0
 password 7 <removed>
line vty 0 1
 access-class 110 in
 exec-timeout 30 0
 password 7 <removed>
 length 20
 transport input telnet
line vty 2 4
 access-class 110 in
 exec-timeout 30 0
 password 7 <removed>
 transport input telnet
line vty 5 9
 access-class 110 in
 transport input telnet
!
ntp clock-period 17180167
ntp update-calendar
ntp server 192.5.5.250
!
end

Sprintgate#
```

Authentication

4. Standard: Determine the types of accounts that were used to access the routers. A user account can be defined with **enable** privileges with this entry in the configuration file: username **user-ID** privilege 15 password 7
   Standard: Determine what users had access to these accounts.

Objective: The privilege level is set in Tacacs at 1. Personnel must know the enable password to enter privilege mode.

5. Standard: Were access attempts to the routers logged?
   Objective: Access attempts are logged on the ACE server.



6. Standard: Determine if all accounts had passwords and determine the strength of the passwords.
   Subjective: Users are defined in NT. I was unable to determine the password requirement settings on NT. The policy does state the use of complex passwords.
7. Standard: Determine if there was a mechanism for periodically changing passwords.
   Subjective: Users are required to change their NT passwords every three months. The policy states changing passwords every 3 months.
8. Standard: No standard exists to warn users that unauthorized access is not permitted
   Objective: The router does contain a banner.

```
Trying sprintgate.xxxxx.com (207.xx.xxx.1)... Open
```

L E G A L N O T I C E

```
>>>>>>>>>>>>>>> This system is restricted to private use.
               All others log out NOW!
**************************************************************************
*                                                                        *
*                                                                        *
*              This network is protected by a security system.           *
*              Criminal law prohibits unauthorized use.                  *
*              Violators will be prosecuted.                             *
*                                                                        *
*                                                                        *
*                                                                        *
**************************************************************************


User Access Verification

Username:
```

9. Standard: Was simple network management protocol (SNMP) used to configure the network?
   Objective:

```
Sprintgate#show snmp
0 SNMP packets input
    0 Bad SNMP version errors
    2028 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    927627 Number of requested variables
    0 Number of altered variables
    54111 Get-request PDUs
    238 Get-next PDUs
    2 Set-request PDUs
    0 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs

SNMP logging: disabled
```

   SNMP is disabled.
10. Standard: Determine the version of SNMP employed by the Company. Version one stores community names in clear-text format. Version two adds encryption of community names.
    N/A
11. Standard: Determine the SNMP community names. This could be determined by looking at the configuration file. Cisco routers had two default SNMP community strings (used as passwords): *public* for read access and *private* for read/write access.
    N/A
12. Standard: Determine if the routers incorporate strong SNMP community names. Were they changed from the defaults?
    N/A

13. Standard: Determine which sites were able to use the given SNMP community names. Cisco routers could restrict SNMP access to *set* operations, which change router variables, to certain IP addresses.
    N/A
14. Standard: Determine if SNMP community names could be obtained though the configuration file. The configuration file was used to store most of the configuration settings of the router. Even though this file is binary, the setting (including SNMP community names) was stored as clear-text.
    N/A
15. Standard: Determine whether the Company implemented encryption for set requests from SNMP read/write community names.
    N/A
16. Standard: Determine the frequency of SNMP community name changes.
    N/A
17. Standard: Cisco provides support for an old MIB called OLD-CISCO-SYS-MIB that allows anyone with the read/write community name to TFTP download the configuration file. Determine if the Company's Cisco routers are vulnerable.
    N/A

Control of Services

18. Standard: Determine which services were running on the routers. The key services to evaluate were trivial file transfer protocol (TFTP), simple network management protocol (SNMP), file transfer protocol (FTP), and telnet.
    Objective:

```
Sprintgate#show proc cpu
CPU utilization for five seconds: 0%/0%; one minute: 5%; five minutes: 5%
 PID  Runtime(ms)   Invoked  uSecs    5Sec   1Min   5Min TTY Process
   1         492    713030      0   0.00%  0.00%  0.00%   0 Load Meter
   2          20     28168      0   0.00%  0.00%  0.00%   0 BGP Open
   3    14741380    822396  17924   0.00%  0.49%  0.49%   0 Check heaps
   4           0         1      0   0.00%  0.00%  0.00%   0 Chunk Manager
   5           0         1      0   0.00%  0.00%  0.00%   0 Pool Manager
   6           0         2      0   0.00%  0.00%  0.00%   0 Timers
   7           4         2   2000   0.00%  0.00%  0.00%   0 Serial Backgroun
   8           0         1      0   0.00%  0.00%  0.00%   0 OIR Handler
   9          76    712853      0   0.00%  0.00%  0.00%   0 ALARM_TRIGGER_SC
  10           0         1      0   0.00%  0.00%  0.00%   0 IPC Zone Manager
  11         304   3557201      0   0.00%  0.00%  0.00%   0 IPC Periodic Tim
  12       48132   2564398     18   0.00%  0.00%  0.00%   0 IPC Seat Manager
  13        6388    113554     56   0.00%  0.00%  0.00%   0 ARP Input
  14       11188    871400     12   0.00%  0.00%  0.00%   0 HC Counter Timer
  15           0         7      0   0.00%  0.00%  0.00%   0 DDR Timers
  16           0         2      0   0.00%  0.00%  0.00%   0 Dialer event
  17           0         1      0   0.00%  0.00%  0.00%   0 Entity MIB API
  18           0         1      0   0.00%  0.00%  0.00%   0 SERIAL A'detect
  19           0         1      0   0.00%  0.00%  0.00%   0 Microcode Loader
  20           0         1      0   0.00%  0.00%  0.00%   0 Critical Bkgnd
  21       29160    392695     74   0.00%  0.00%  0.00%   0 Net Background
  22          16      4891      3   0.00%  0.00%  0.00%   0 Logger
  23         504   3557196      0   0.00%  0.00%  0.00%   0 TTY Background
  24        1044   3557232      0   0.00%  0.00%  0.00%   0 Per-Second Jobs
  25           0         1      0   0.00%  0.00%  0.00%   0 Inode Table Dest
```

26	0	1	0	0.00%	0.00%	0.00%	0	Inode Table Refr
27	0	1	0	0.00%	0.00%	0.00%	0	IP Crashinfo Inp
28	0	1	0	0.00%	0.00%	0.00%	0	DSX3MIB ll handl
29	0	2	0	0.00%	0.00%	0.00%	0	VSI Master
30	2152	3557200	0	0.00%	0.00%	0.00%	0	RSP Background
31	0	1	0	0.00%	0.00%	0.00%	0	Memory Scanner
32	7864	118831	66	0.00%	0.00%	0.00%	0	Slave Time
33	0	1	0	0.00%	0.00%	0.00%	0	Slave IPC OIR
34	5996	5178440	1	0.00%	0.00%	0.00%	0	CEF process
35	1444	1008834	1	0.00%	0.00%	0.00%	0	Chassis Daemon
36	2548	59430	42	0.00%	0.00%	0.00%	0	RSP Chassis Back
37	0	2	0	0.00%	0.00%	0.00%	0	MIP Mailbox
38	0	1	0	0.00%	0.00%	0.00%	0	vcq_proc
39	0	1	0	0.00%	0.00%	0.00%	0	CT3 Mailbox
40	0	1	0	0.00%	0.00%	0.00%	0	CE3 Mailbox
41	0	1	0	0.00%	0.00%	0.00%	0	SRP Event Proc
42	150040	3712855	40	0.00%	0.00%	0.00%	0	IPC CBus process
43	0	2	0	0.00%	0.00%	0.00%	0	ATM OAM Input
44	0	2	0	0.00%	0.00%	0.00%	0	ATM OAM TIMER
45	0	93	0	0.00%	0.00%	0.00%	0	TurboACL
46	0	2	0	0.00%	0.00%	0.00%	0	AAA Dictionary R
PID	Runtime(ms)	Invoked	uSecs	5Sec	1Min	5Min	TTY	Process
47	295472	2012839	146	0.08%	0.01%	0.00%	0	IP Input
48	0	1	0	0.00%	0.00%	0.00%	0	ICMP event handl
49	40264	388824	103	0.00%	0.00%	0.00%	0	CDP Protocol
50	0	2	0	0.00%	0.00%	0.00%	0	PASVC create VA
51	0	1	0	0.00%	0.00%	0.00%	0	X.25 Encaps Mana
52	0	1	0	0.00%	0.00%	0.00%	0	frr_tunnel
53	0	3	0	0.00%	0.00%	0.00%	0	IP Hdr Comp Proc
54	3197824	60911	52499	0.00%	0.07%	0.05%	0	IP Background
55	0	1	0	0.00%	0.00%	0.00%	0	SNMP Timers
56	0	1	0	0.00%	0.00%	0.00%	0	PPP IP Add Route
57	20264	59433	340	0.00%	0.00%	0.00%	0	Adj Manager
58	12	29736	0	0.00%	0.00%	0.00%	0	DHCPD Timer
59	2288	17750648	0	0.00%	0.00%	0.00%	0	MDFS RP process
60	220	315914	0	0.00%	0.00%	0.00%	0	TCP Timer
61	36	136	264	0.00%	0.00%	0.00%	0	TCP Protocols
62	0	1	0	0.00%	0.00%	0.00%	0	Probe Input
63	0	1	0	0.00%	0.00%	0.00%	0	RARP Input
64	0	1	0	0.00%	0.00%	0.00%	0	HTTP Timer
65	0	1	0	0.00%	0.00%	0.00%	0	Socket Timers
66	40	171	233	0.00%	0.00%	0.00%	0	DHCPD Receive
67	968	59418	16	0.00%	0.00%	0.00%	0	IP Cache Ager
68	0	1	0	0.00%	0.00%	0.00%	0	COPS
69	0	1	0	0.00%	0.00%	0.00%	0	PAD InCall
70	0	2	0	0.00%	0.00%	0.00%	0	X.25 Background
71	2536	59430	42	0.00%	0.00%	0.00%	0	TCP Intercept Ti
72	0	2	0	0.00%	0.00%	0.00%	0	TC-ATM Proc
73	0	2	0	0.00%	0.00%	0.00%	0	Tag Input
74	20	56432	0	0.00%	0.00%	0.00%	0	IPC LC Message H
75	56	335	167	0.00%	0.00%	0.00%	0	AAA Accounting
76	0	6	0	0.00%	0.00%	0.00%	0	Router Autoconf
77	0	1	0	0.00%	0.00%	0.00%	0	SYSMGT Events
78	1268	7072558	0	0.00%	0.00%	0.00%	0	cbus utilization
79	11708	374870	31	0.00%	0.00%	0.00%	0	Net Input
80	1360	713030	1	0.00%	0.00%	0.00%	0	Compute load avg
81	650636	59491	10936	0.00%	0.00%	0.00%	0	Per-minute Jobs
82	0	1	0	0.00%	0.00%	0.00%	0	FR LMI
83	7760	34853065	0	0.00%	0.00%	0.00%	0	FR Broadcast Out
84	0	1	0	0.00%	0.00%	0.00%	0	FR ARP
85	24	178423	0	0.00%	0.00%	0.00%	0	FR TUNNEL
86	0	1	0	0.00%	0.00%	0.00%	0	FRF9 manager
87	0	1	0	0.00%	0.00%	0.00%	0	FRF9 timed event

```
 88           0         2      0   0.00%  0.00%  0.00%   0 IP Flow Backgrou
 90       21644     29000    746   0.00%  0.00%  0.00%   0 PDU DISPATCHER
 94        1512   3583509      0   0.00%  0.00%  0.00%   0 NTP
PID  Runtime(ms)   Invoked  uSecs    5Sec   1Min   5Min TTY Process
 95        1464    187841      7   0.00%  0.00%  0.00%   0 CEF Scanner
 96        5508   1010057      5   0.00%  0.00%  0.00%   0 DHCPD Database
 97        2764  13952655      0   0.00%  0.00%  0.00%   0 CEF IPC Backgrou
 98           0         1      0   0.00%  0.00%  0.00%   0 DSS Process
 99           4        47     85   0.00%  0.00%  0.00%   0 TCP Listener
100     5643824   9071387    622   0.00%  0.84%  0.89%   0 BGP Router
101      268912   3616436     74   0.00%  0.01%  0.00%   0 BGP I/O
102   142508564    879840 161976   0.00%  3.42%  3.63%   0 BGP Scanner
103           0      1900      0   0.00%  0.00%  0.00%   0 TACACS+
104       10512   1057546      9   0.00%  0.00%  0.00%   0 Standby
105         340     14143     24   0.00%  0.00%  0.03%   2 Virtual Exec
```

Small services were found in the configuration.

```
service udp-small-servers
service tcp-small-servers
```

Nmap also confirms the presence of the small-services.

The Http server was properly disabled on the router.

```
no ip http server
```

Ident should be removed from the router. The command "`no ip identd`" was not found on the router.

19. Standard: There is no standard for source routing.
    Objective: `no ip source route` is not present in the configuration. It should be added.
20. Standard: Determine if open shortest path first (OSPF) was defined on the router. Determined the authentication mechanism that was employed in the Company's implementation of OSPF.
    N/A
21. Standard: Determine whether directed broadcast functionality was enabled on the router. This setting, if enabled, could allow a denial-of-service (DoS) attack of the network (Smurf attack).
    Objective: `no ip directed-broadcast` was not found in the configuration
22. Standard: No standard exists for ad-hoc routing.
    Objective: `no proxy-arp` was not found in the configuration. It needs to be added.
23. Standard: Cisco's finger service will respond with some useless information, which can help an attacker identify the device as a Cisco device. Determine if the Company's routers respond to the finger service with valuable information.
    Objective: `no service finger` was not found in the configuration. Nmap also found the finger service enabled. Finger service should be disabled.
24. Standard: No standard exists for Cisco Discovery Protocol.

Objective: The finger service is enabled and needs to be disabled.

```
Sprintgate#show cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
OUTSIDE1         Fas 5/1           146         T S       WS-C2924-XFas 0/24
```

25. Standard: Attackers can connect to Cisco management ports 2001, 4001, and 6001 to help identify the device as a Cisco device. The result of

connecting to one of these ports via a browser might look like this: User Access Verification Password: Password: Password: Password: % Bad passwords

Objective: No access-list exists for blocking ports 2001,4001,6001.

```
Standard IP access list 10
    permit 208.xxx.xxx.0, wildcard bits 0.0.0.255 (43 matches) check=853791
Standard IP access list 20
    permit 207.xxx.xxx.0, wildcard bits 0.0.0.255 (9 matches) check=516813
Extended IP access list 110
    permit ip host 64.xxx.xxx.67 any (2 matches)
    permit tcp 207.xx.xx.0 0.0.0.255 host 0.0.0.0 eq telnet log-input (66 matches)
    deny ip any any log-input (7 matches)
Extended IP access list border
    permit ip host 64.xx.xx.67 any
    permit icmp host 144.xx.xx.1 host 144.xx.xx.2 (9 matches)
    permit tcp host 144.xx.xx.1 host 144.xx.xx.2 eq bgp
    permit tcp host 144.xx.xx.1 eq bgp host 144.xx.xx.2 (68578 matches)
    deny ip 207.xx.xxx.0 0.0.0.255 any log-input (11 matches)
    deny ip any 10.0.0.0 0.255.255.255 log-input
    deny ip any 192.168.0.0 0.0.255.255 log-input
    deny ip any 172.16.0.0 0.15.255.255 log-input
    permit ahp any host 208.253.246.60
    permit esp any host 208.xx.xx.60 (403441 matches)
    permit tcp any host 208.xx.xx.60 eq 500
    permit udp any host 208.xxx.xx.60 eq isakmp (3302 matches)
    permit tcp any host 208.xx.xx.60 eq 50
    permit udp any host 208.xx.xx.60 eq 50
    deny ip any host 208.xxx.xxx.60 log-input (15 matches)
    permit ip any 208xx.xx.0 0.0.0.255 (11909 matches)
    permit ip any 207.xx.xx.0 0.0.0.255 (18631603 matches)
    permit udp host 192.5.5.250 host 144.xx.xxx.2 eq ntp (6528 matches)
    deny ip any any log-input (50 matches)
```

26. Standard: Another of Cisco's common ports is the XRemote service port (TCP 9001). The XRemote allows sytems on your network to start client Xsessions to the router (typically through a dial-up modem). When an attacker connects to the port, the device will send back a common banner, such as: ---Outbound XRemote Service---
    Objective: no access-list blocks port 9001

Routing Authorized Traffic

27. There is no standard defined for passing only authorized traffic.
    Subjective: There was no outbound access list specifically permitting authorized traffic. Unless all traffic is authorized outbound acls should be added.
28. Standard: No standard exists for filtering unnecessary or malicious traffic.
    Objective: The access lists protect for spoofing but icmp and other protocols should also be blocked based on the following reference.
    http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf

Remote Access

29. Standard: Were dial-in connections used to access the routers.
    N/A
30. Standard: Obtain population of routers with modems and obtain the telephone numbers of the routers.
    N/A

31. Standard: Determine if users were properly authenticated when remotely accessing the routers.
    N/A
32. Standard: Determine if access attempts were logged.
    N/A
33. Standard: Determine if the telephone numbers of the routers were within Company defined telephone prefixes. Hackers commonly poll prefixes to obtain access to a network.
    N/A

Change Management

34. Standard: Determine how changes to the router environment were made.
    Subjective: Through interview the staff says that changes can be made via a telnet session or via CiscoWorks through scheduled jobs. There is a change control process however there are no measures to prevent ad hoc changes.
35. Standard: Determine if changes to the router configuration were documented.
    Objective: Changes on the routers are captured by CiscoWorks and ACE Server.
36. Standard: Were there procedures for changing router configurations?
    Subjective: Documented procedures were not available. However conversation with engineers indicate a standard procedure.
37. Standard: Was there a separation of duties within the change control of the router environment?
    Subjective: There was no separation of duties due to the limited resources of the staff. Everyone does everything.

Network Monitoring

38. Standard: Determine the mechanisms for monitoring the network.
    Objective: IPSwitch What's up Gold is used for monitoring. The perimeter router was verified in the configuration.
39. Standard: Determine the personnel that monitor the network.
    Subjective: The personnel monitoring the network consisted of one engineer. A back up should be identified.
40. Standard: Determine the security of the network monitoring tools.
    Subjective: The access to monitoring tools contains all the NT domain administrators. This should be changed to only allow the appropriate personnel.

Evaluation of the System

The overall evaluation of the system resulted in a fair configuration. The primary issues pertain to the need to remove unnecessary services on the router.

Access Control Lists also need to be improved to block unwanted traffic and to specifically allow authorized traffic.

Tools such as CiscoWorks are available and were adequately used to log access, track configurations. More should be done to move change control to batch processes on the CiscoWorks. Ace server did an appropriate job of user authentication, authorization, and accounting.

Below is a list of items that require actions to address or correct.

Item 1) 2 accounts existed that are shared. One for a consulting company and the other for vendor support. It is recommended that unique accounts be created for accountability.
Item 18) Smaller services, identd, service-configuration need to be removed.
Item 19) Source routing needs to be disabled.
Item 21) Directed broadcasts should be disabled. The system is vulnerable to smurf attacks.
Item 22) Ad Hoc routing is enabled and it should be disabled.
Item 23) The finger service should be removed.
Item 24) CDP should be disabled
Item 25) An access list is needed to block 2001,4001, and 6001
Item 26) An access list is needed to block 9001
Item 27) Outbound acl should be added to only permit authorized traffic.
Item 28) Additional blocking should be incorporated to block unwanted traffic.
Item 34) Changes on the routers should be moved to using CiscoWorks only. A change window should be implemented to allow for easier detection of unauthorized changes.
Item 36) Procedures need to be documented for change control.
Item 37) Separation of duties is limited by availability of staff.
Item 39) Back up personnel should be identified for network monitoring.
Item 40) Access to Monitoring Servers need to be limited to only the authorized personnel instead of all domain admins.

The costs associated with the addressing each item should be low. Most items can be corrected with configuration changes. Only items 39 and 40 present some staffing issues because they deal with separation of duties.

Histories should be kept to support a documented change process, password update etc. Items that do not show up in logs on network management systems should be noted in a operations folder.

A follow up audit should be repeated once the items have been address to verify that improvements have been implemented.

Evaluation of the Audit

Overall the audit process is thorough. It uncovers areas that require improvement as well as areas that are properly configured. Some formatting into a checklist will help its usability.

The tools required for the audit is minimal. It primarily relies on looking at the configuration of the router and the configuration of the management tools. NMAP is used to verify proper behavior of the configuration. However this can only be done with a properly configured router. It does detect an improperly configured router.

The audit was sufficient in identifying areas of weakness on the perimeter router. Better definition could be provided into the specific commands and the interpretations of their output. The current audit requires an experience router engineer to interpret command line output. The audit could be more efficient if certain sections are combined into a single check box or item.

References

"Building a Perimeter Security Solution with the Cisco Secure Integrated Software," June 13, 2001, http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/tech/firew_wp.htm

"Increasing Security on Cisco Routers" http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm

"Improving Security on Cisco Routers," http://www.cisco.com/warp/public/707/21.html

"Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks," February 17, 2000, http://www.cisco.com/warp/public/707/newsflash.html

Techniques for blocking Nimda
Cisco CCO Web site
http://www.cisco.com/warp/public/63/nimda.shtml

Mike Wenstrom, "Managing Cisco Network Security," January 2001

National Security Agency, Ft Meade, Maryland "Cisco Router Security Recommendation Guides," September 21, 2001, http://nsa2.www.conxion.com/cisco/guides/cis-1.pdf, http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf

Justin Snyder, January 10, 2001, "Data Communications - Cisco Routers" http://www.auditnet.org/docs/Cisco%20Router%20Audit%20Program.txt http://www.auditnet.org/docs/Cisco%20Router%20Audit%20Program.doc.

Last Updated: July 24th, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS AUD507 (GSNA) @ Canberra 2017	**Canberra, Australia**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**