

RE: Cisco Config Files?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-07/0039.html>

From: mht@clark.net

Date: 07/25/01

Message-Id: <5.1.0.14.2.20010724223456.00abcd0@pop3.clark.net>

Date: Tue, 24 Jul 2001 22:56:00 -0700

To: "Skinner, Tim L." <Tskinner@larsonallen.com>, "'pen-test@securityfocus.com'" <pen-test@securityfocus.com>

From: mht@clark.net

Subject: RE: Cisco Config Files?

"Configuring IP Services" chapter in the Network Protocols Configuration Guide, Part 1.

From the typical Cisco IOS Essential course(s).. (I keep on forgetting, I actually took notes when I took this course..)

```
service password-encryption
enable secret <removed>
no enable password
no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
no ip bootp server
no ip redirect
no ip direct broadcast
no ip proxy-arp
no cdp enable
service nagle
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
service tcp-keepalives-in
no ip source-route
ip spd enable
logging buffered 16384
logging trap debugging
logging x.x.x.x
ip subnet-zero
ip classless
! access-list 150 to deny RFC1918 addresses
access-list 150 deny ip 0.0.0.0 0.255.255.255 255.0.0.0 0.255.255.255
access-list 150 deny ip 10.0.0.0 0.255.255.255 255.0.0.0 0.255.255.255
access-list 150 deny ip 127.0.0.0 0.255.255.255 255.0.0.0 0.255.255.255
access-list 150 deny ip 169.254.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

RE: Cisco Config Files?

SecurityFocus Penetration: RE: Cisco Config Files?

```

access-list 150 deny ip 172.16.0.0 0.15.255.255 255.240.0.0 0.15.255.255
access-list 150 deny ip 192.0.2.0 0.0.0.255 255.255.255.0 0.0.0.255
access-list 150 deny ip 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255
access-list 150 deny ip 224.0.0.0 31.255.255.255 224.0.0.0 31.255.255.255
access-list 150 deny ip any 255.255.255.128 0.0.0.127
access-list 150 permit ip any any
snmp-server community hardToGuessString RO 4
snmp-server community hardToGuessString RW 5
snmp-server system-shutdown
snmp-server host trap-host hardToGuessString
snmp-server tftp-server-list 5
snmp-server enable traps config
snmp-server enable traps snmp
snmp-server enable traps link-status
snmp-server enable traps config
snmp-server enable traps envmon
snmp-server enable traps bgp
snmp-server enable traps frame-relay
snmp-server trap-source Ethernet0
snmp-server contact someone@whocares.com
banner motd ^C
#####
# This system is for the use of authorized users only. #
# Individuals using this computer system without authority, or in #
# excess of their authority, are subject to having all of their #
# activities on this system monitored and recorded by system #
# personnel. #
# #
# In the course of monitoring individuals improperly using this #
# system, or in the course of system maintenance, the activities #
# of authorized users may also be monitored. #
# #
# Anyone using this system expressly consents to such monitoring #
# and is advised that if such monitoring reveals possible #
# evidence of criminal activity, system personnel may provide the #
# evidence of such monitoring to law enforcement officials. #
#####
^C

```

blah, blah

All the Cisco SNMP MIBs are publicly available. If you have commercial SNMP management packets and/or shareware-freeware packets, you may need to go and grab the MIB. Here is the FTP site:
<ftp://ftp.cisco.com/pub/mibs/>

At 03:19 PM 07/23/2001 -0500, Skinner, Tim L. wrote:
 >Cisco provides some good
 >guidelines on secure
 >configuration.
 >Check out

SecurityFocus Penetration: RE: Cisco Config Files?

><http://www.cisco.com/warp/public/707/21.html>
>
>
>
>By chance does anyone have a copy of a secure cisco config file? It's for
>our
>main company's main border router. I'm in serious need of something to
>compare
>mine too. I haven't been able to find a link too a good one.
>If someone has a good link for reference I'd be so appreciative.
>
>Thanks again,
>
>Alexander

>This list is provided by the SecurityFocus Security Intelligence Alert (SIA)
>Service For more information on SecurityFocus' SIA service which
>automatically alerts you to the latest security vulnerabilities please see:
><https://alerts.securityfocus.com/>

>This list is provided by the SecurityFocus Security Intelligence Alert (SIA)
>Service. For more information on SecurityFocus' SIA service which
>automatically alerts you to the latest security vulnerabilities please see:
><https://alerts.securityfocus.com/>

This list is provided by the SecurityFocus Security Intelligence Alert (SIA)
Service. For more information on SecurityFocus' SIA service which
automatically alerts you to the latest security vulnerabilities please see:
<https://alerts.securityfocus.com/>

-
- **Previous message:** [Vladimir Parkhaev: "IIS/Unicode and authentication box"](#)
 - **In reply to:** [Skinner, Tim L.: "RE: Cisco Config Files?"](#)
 - **Next in thread:** [Dave Ryan: "Re: Cisco Config Files?"](#)
 - **Reply:** [Dave Ryan: "Re: Cisco Config Files?"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)