Auditing a Syslog Server Running on Fedora Core 1

Chris Sawall, GSEC
GSNA Practical Version 3.0 Option 1
An Auditor's Perspective
23 June 2004

Abstract

This paper will cover the steps necessary to audit a syslog server running on Linux/Fedora Core 1. The target syslog server is used to log and store syslog data from critical network security devices, including Cisco PIX firewalls, Cisco VPN and Dialup servers. The syslog information includes failed login attempts, unauthorized network access, configuration changes and device failures. This paper will give some background on how a syslog server works, followed by the steps needed to create an audit checklist, perform the audit and generate the audit report. This report will detail all findings and then make recommendations, as well as provide a high level summary for executives.

Table of Contents

Index of Tables

Index of Graphs

Introduction

The purpose of this paper is to perform an audit on an existing syslog server. It will verify that the server has been properly configured and secured for the purpose of storing log data from various critical network devices. The target syslog server is running Fedora Core 1 as the operating system, but the standard syslogd service has been replaced with syslog-ng (http://www.balabit.com/products/syslog_ng/). The results of this audit should ensure that the syslog solution currently in place meets the following criteria:

- Ensure data integrity
- Ensure that unnecessary services are not running or can be accessed
- Ensure data storage/backup
- Only allow authorized devices to send syslogs
- Only allow authorized personal to administrate the syslog server

If the above criteria are not met, recommendations will be made to reach the stated objectives.

What is Syslog?

Syslog is short for System Logger. Traditionally, it is a service that runs on a Unix device and provides the capability to log events from both local and remote sources. The syslog service or daemon is a process that waits and listens for event notifications to be sent to it over an IP network, by default, on UDP port 514. Devices that send events to the syslog server are known as syslog clients. The use of syslog to send events to a centralized syslog server has expanded to other (non-Unix) devices like firewalls and routers. Depending on the device where a syslog client is running, it will log a variety of events from kernel messages to all network traffic. It has even been implemented for the Microsoft Windows platforms.

The Syslog Server

Hardware:

- HP LP2000r
- Dual 1.2 GHz Processors
- 4 GB RAM
- Hardware Mirrored 36 GB Drives for System
- Hardware Mirrored 72 GB Drives for Logs

Software:

- Fedora Core 1 (http://fedora.redhat.com/)
- Syslog-ng version 1.6.4 (http://www.balabit.com/products/syslog_ng/)

- Simple Event Correlator (SEC) version 2.2.4 (http://kodu.neti.ee/~risto/sec/)

Syslog-ng was chosen because it is more flexible than the standard GNU syslog service that comes with Fedora Core 1. It scales better, provides better security and has a highly modifiable configuration. SEC was chosen to perform real-time monitoring. SEC can be set up as a service to monitor a file as it is being written to; in this environment it is the syslog log file. SEC can watch for specific strings by using regular expressions, a way to perform pattern matching.

Evaluating the Threats

Definitions

Before potential threats are identified, a few definitions of basic terminology will be explained:

Risk[1]
A threat that exploits a vulnerability that may cause harm to one or more assets.

Threat[1]
A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, data modification, and/or Denial of Service (DoS).

Vunerability[1]
A (universal) vulnerability is a state in a computing system (or set of systems) which either:

- Allows an attacker to execute commands as another user
- Allows an attacker to access data that is contrary to the specified access restrictions for that data
- Allows an attacker to pose as another entity
- Allows an attacker to conduct a denial of service

Exposure[1]
An exposure is a state in a computing system (or set of systems) which is not a universal vulnerability, but either:

- Allows an attacker to conduct information gathering activities
- Allows an attacker to hide activities
- Includes a capability that behaves as expected, but can be easily compromised

[1] http://securityresponse.symantec.com/avcenter/refa.html

- Is a primary point of entry that an attacker may attempt to use to gain access to the system or data
- Is considered a problem according to some reasonable security policy

Analysis of Possible Threats

Based on the definition provided above, a threat can be any circumstance, event or person that could possibly cause harm to a system. Table 1 illustrates several possible threats that could exist on the syslog server and their potential results.

Threat	Result
Unknown devices sending logs to server	A misconfigured device could inadvertently cause a Denial of Service by sending too much data to the syslog server.
Failure to connect to the Internet to keep time	It is vital that a syslog server maintains accurate time so that it can timestamp each log entry appropriately. Non-accurate timestamps make parsing log data nearly impossible to match up with real world events that may have taken place.
Unauthorized access	If an unauthorized user accesses the server, data could be compromised.
Hardware Failure	Loss of ability to receive and monitor syslog data.

Table 1 Threat Analysis

Role of the Syslog Server

Securing the syslog server is vital because of the importance of the data that it gathers and stores. The syslog server receives valuable data from many network devices including firewalls and remote access devices. This data is important to a company because it details all connectivity allowed and denied through firewalls and other remote access devices. The syslog data must retain its integrity in the case of any legal disputes over alleged malicious activity. Table 2 illustrates the major information assets of the syslog server.

Role of Syslog Server	Asset Affected
To gather and store syslog data from critical network infrastructure such as routers, firewalls, VPN and dialup servers.	The integrity of the syslog data must be maintained in the case of any legal dispute. Accurate and reliable syslog data is invaluable for day-to-day troubleshooting of network issues.

Table 2 Information Assets of the Syslog Server

Analysis of Possible Vulnerabilities

As identified and taught in the SANS track: “Auditing Networks, Perimeters & Systems”, vulnerability + threat = exposure. Allowing those exposures to exist is a risk. Table 3 identifies possible vulnerabilities and illustrates the outcome if a successful exploitation were to take place.

Vulnerability	Impact	Exposure
Extraneous services running	Unauthorized users could attempt to exploit vulnerable services that do not otherwise need to be running.	HIGH
Root not restricted to console login	If logging in via an insecure medium, such as telnet, root's password can be compromised. Allowing remote logins with the root account also provides no accountability or tracking of who is using it.	HIGH
Access control	If access control mechanisms are not in place, malicious users could gain control of the system. Privileged users, those who have access to the device, could gain more privileges than those actually given.	HIGH
Physical Security	All security measures and access control mechanisms could be in place, however, if the syslog server is not in a physically secured location, all other security measures could be overridden.	HIGH

Table 3 Vulnerability Analysis

Current State of Practice

The Linux operating system has been in use for quite some time and therefore there is a relatively large amount of information available on how to properly secure a Linux server. Unfortunately there is not as much information available for the specific task of properly setting up and securing a centralized syslog server.

Ref ID	Reference
RID01	Real World Linux Security[2] by Bob Toxen is a must have book for all administrators. This book covers almost every security issue imaginable from physical security to application and service security.
RID02	CIS Level-1 Benchmark Document for Linux[3] details the steps necessary to implement CIS Level-1 security. This document was written by team members from the Center for Internet Security, a non-profit organization. According to CIS[3], the Level-1 Benchmark provides "the prudent level of minimum due care for operating system security".
RID03	Locking Down Your Linux Box - A Checklist Approach[4] is a website that has a basic, but adequate checklist of items to help secure a Linux device. The topics are even classified as "must do" and "should do".
RID04	Auditing a Fedora Core 1 Linux[5] is a GSNA paper on the GIAC website. Since the target syslog server of this audit is running on Fedora, it is appropriate to include a paper that is so directly related.
RID05	The IETF's document on the Syslog Protocol[6] is the Internet-Draft that describes the syslog protocol.
RID06	Managing logging and other data collection mechanisms[7] is an older document written by members of the CERT team in 2000. Although this document is now four years old, it is still an excellent document that pertains to the security of log files today.
RID07	Advanced Log Processing[8] by Anton Chuvakin delves deeper in to log collection, rotation and security.

Table 4 Current State of Practice

Audit Checklist

The following section will layout an audit checklist that can be used to perform an audit against a centralized syslog server. This audit will help administrators determine if they can trust the security of their server and the integrity of their data.

Server Oriented Audit Items

[2] Real World Linux Security, Bob Toxen
[3] http://www.cisecurity.org/bench_linux.html
[4] http://georgetoft.com/linux/security/locking/checklist.shtml
[5] http://www.giac.org/practical/GSNA/Jorge_Ortiz_GSNA.pdf
[6] http://www.ietf.org/internet-drafts/draft-ietf-syslog-protocol-04.txt
[7] http://www.cert.org/security-improvement/practices/p092.html
[8] http://www.securityfocus.com/infocus/1613

VID01	**Basic Vulnerability Check**
References	RID03 - http://georgetoft.com/linux/security/locking/checklist.shtml
Risk: **MEDIUM**	Applications and services that are running may not be at the appropriate patch level, leaving the system vulnerable to exploitation.
Testing Procedure	Run Nessus[9] to check system for vulnerabilities. There are a couple of ways to run Nessus. The first would be to install it on a Linux machine. The binaries can be downloaded from www.nessus.org. The second option is to download a Live CD distribution of Linux with Nessus already compiled on it. This will allow a machine to be booted into Linux without having to install Linux or Nessus. The Nessus server would then be used to scan any target system for vulnerabilities. Knoppix is an excellent Live CD distribution and can be found at www.knoppix.net. Refer to Appendix A for screenshots of Nessus.
Compliance Criteria	Keep current with system and application patches.
Test Nature	**Objective**
Evidence	Space intentionally left blank.
Findings	Space intentionally left blank.

VID02	**Disable Insecure Network Services**
References	RID02 - CIS Level-1 Benchmark Document for Linux
Risk: **HIGH**	Leaving insecure network services running could put the system at risk for compromise. Unencrypted communications to the target server could be monitored. Administrative connections/sessions could be captured and passwords could be compromised.
Testing Procedure	Services that should be disabled (if installed) are telnet, FTP, rlogin, rsh, rexec and TFTP, IMAP and POP3. To verify if the service is running at any given run-level, do the following: **chkconfig --list <service name>** It will produce the results similar to the following: **<service> 0:off 1:off 2:off 3:on 4:on 5:on 6:off** To disable the service, do either of the following commands: **chkconfig <service> off**

[9] http://www.nessus.org/

	chkconfig --level 345 <service> off
Compliance Criteria	Administration and/or file transfers take place over encrypted communications.
Test Nature	**Objective**
Evidence	Space intentionally left blank.
Findings	Space intentionally left blank.

VID03	**Preventing Root from Logging in Remotely**
References	RID03 - http://georgetoft.com/linux/security/locking/checklist.shtml
Risk: **HIGH**	Allowing root to log in remotely could compromise the account if logging in over an insecure transport. Allowing root to log in remotely does not allow for the proper tracking of the use of the Root account.
Testing Procedure	Telnet - Remove or disable the telnet service. See VID02.
	SSH - Edit the /etc/ssh/sshd_config file. There are two ways this can be accomplished with OpenSSH, which is the SSH server installed with Fedora. Use either the keyword *DenyUsers* or *PermitRootLogin*.[10] The syntax to disable Root access for each is: **DenyUsers root** **PermitRootLogin no**
	FTP - If this service is needed and not disabled per VID02 then edit the /etc/ftpusers file and/or the /etc/vsftpd.ftpusers file. All users listed in this file are NOT allowed to log into the FTP server. Add "root".
Compliance Criteria	The root account cannot log in remotely.
Test Nature	**Objective**
Evidence	Space intentionally left blank.
Findings	Space intentionally left blank.

VID04	**Disable File System Sharing**
References	RID01 - Real World Linux Security RID02 - CIS Level-1 Benchmark Document for Linux
Risk: **HIGH**	There have been several documented vulnerabilities in the Samba implementation on Linux and NFS is frequently exploited, therefore both should be disabled. If proper security controls are not in place, file shares can be accessed and data compromised.

[10] http://www.openbsd.org/cgi-bin/man.cgi?query=sshd_config&sektion=5&arch=&apropos=0&manpath=OpenBSD+Current

Testing Procedure	Disable smbd, nmbd, nfs, nfslock, autofs, netfs and portmap (used by NFS). Samba usually installs itself into the system PATH. So, to determine if Samba is installed, issue the following commands: **which smbd** and **which nmbd** To determine if the service is running at any given run-level, do the following: **chkconfig --list <service name>** It will produce results similar to the following: **<service> 0:off 1:off 2:off 3:on 4:on 5:on 6:off** To disable the service, issue either of the following commands: **chkconfig <service> off** **chkconfig --level 345 <service> off**
	Delete the /etc/exports file.
Compliance Criteria	All Samba and NFS services are disabled.
Test Nature	**Objective**
Evidence	Space intentionally left blank.
Findings	Space intentionally left blank.

VID05	**Remove Current Working Directory from Path**
References	RID03 - http://georgetoft.com/linux/security/locking/checklist.shtml RID04 - Auditing a Fedora Core 1 Linux
Risk: **HIGH**	Defend against accidental execution of program that may be a Trojan horse.
Testing Procedure	From the prompt, type: **echo $PATH** Ensure that dot (.) is not in the $PATH variable.
Compliance Criteria	The current working directory is not in the path.
Test Nature	**Objective**
Evidence	Space intentionally left blank.
Findings	Space intentionally left blank.

VID06	**Login Banner**
References	RID02 - CIS Level-1 Benchmark Document for Linux RID03 - http://georgetoft.com/linux/security/locking/checklist.shtml
Risk: **Medium**	It may hinder prosecution if a proper warning banner is not displayed at login.

Testing Procedure	The primary files containing "warnings" are: /etc/issue, /etc/issue.net and /etc/motd. View the current contents of the files by running: **cat <file>** To change the contents to have appropriate warning banners, do the following: **echo “Authorized Use Only!” > /etc/issue** **echo “Authorized Use Only!” > /etc/issue.net** **echo “Authorized Use Only!” > /etc/motd** Note that the actual text can change, but should be approved by the legal department.
	To ensure that SSH connections provide a banner, modify the /etc/ssh/sshd_config file and add the following line: **Banner /etc/issue**
	By default, vsftpd should have the following line in the /etc/vsftpd/vsftpd.conf file: **ftpd_banner=Unauthorized access is prohibited.**
Compliance Criteria	System should display banner upon every login attempt, either remotely or locally.
Test Nature	**Objective**
Evidence	Space intentionally left blank.
Findings	Space intentionally left blank.

VID07	**Remove “Host” Authentication Files**
References	RID01 - Real World Linux Security RID02 - CIS Level-1 Benchmark Document for Linux
Risk: **HIGH**	Allowing files like .rhosts or /etc/hosts.equiv enable a very weak form of access control.

Testing Procedure	Run the following to create symlinks to the “host” authentication files. Anything written to these files will be immediately discarded.
	
	for file in /root/.rhosts /root/.shosts /etc/hosts.equiv \
	/etc/shosts.equiv ;
	do
	    /bin/rm -f $file
	    ln -s /dev/null $file
	done

Compliance Criteria	“Host” authentication files like .rhosts and /etc/hosts.equiv are not allowed on any systems.
Test Nature	**Objective**
Evidence	Space intentionally left blank.
Findings	Space intentionally left blank.

VID08	**Only Root is UID 0**
References	RID02 - CIS Level-1 Benchmark Document for Linux
Risk: **HIGH**	Any ID other than root with a UID of 0 would have superuser privileges without the need to su to root.
Testing Procedure	Running **awk -F: ‘($3 == 0) { print $1 }’ /etc/passwd** should only return “root”.
Compliance Criteria	Only root has a UID of 0.
Test Nature	**Objective**
Evidence	Space intentionally left blank.
Findings	Space intentionally left blank.

VID09	**iptables**
References	RID01 - Real World Linux Security
Risk: **MEDIUM**	Not protecting the individual host can leave it vulnerable on the network.
Testing Procedure	Check firewall status: **/etc/init.d/iptables status** If firewall is disabled, results will be: **Firewall is stopped.** If firewall is running, a short list of rules may appear, the most basic being the following (which is wide open): **Table: filter** **Chain INPUT (policy ACCEPT)** **target prot opt source destination** **Chain FORWARD (policy ACCEPT)** **target prot opt source destination** **Chain OUTPUT (policy ACCEPT)** target prot opt source destination
Compliance Criteria	Iptables or local firewall should be running to further protect log data and server.
Test Nature	**Objectives**
Evidence	Space intentionally left blank.
Findings	Space intentionally left blank.

Syslog Oriented Audit Items

VID10	**Authorized Syslog Devices**

References	RID05 - http://www.ietf.org/internet-drafts/draft-ietf-syslog-protocol-04.txt
Risk: **MEDIUM**	Allowing unauthorized devices to send syslog data to the syslog server could overwhelm the server's resources, hard disk space or cause a Denial of Service.
Testing Procedure	Check the current rules in iptables to verify that only authorized devices are sending syslog data (generally on UDP port 514) to the syslog server. **iptables -L** The result will be a complete list of the current rules running in iptables.
Compliance Criteria	Only authorized devices should be allowed to send syslogs to the syslog server.
Test Nature	**Objective**
Evidence	Space intentionally left blank.
Findings	Space intentionally left blank.

VID11	**Log Rotation**
References	RID07 - http://www.securityfocus.com/infocus/1613
Risk: **HIGH**	Log files grow too large to work with.

Testing Procedure	Check the /etc/logrotate.conf file and /etc/logrotate.d/ directory. The logrotate.conf file sets the global parameters for logrotate. The keyword **daily** should be near the top of the file. This tells logrotate when to rotate the log files. Verify that logrotate is running daily by checking Crontab: **cat /etc/crontab** It should return something similar to the following: **SHELL=/bin/bash** **PATH=/sbin:/bin:/usr/sbin:/usr/bin** **MAILTO=root** **HOME=/** **# run-parts** **01 * * * * root run-parts /etc/cron.hourly** **02 4 * * * root run-parts /etc/cron.daily** **22 4 * * 0 root run-parts /etc/cron.weekly** **42 4 1 * * root run-parts /etc/cron.monthly** Then verify that the /etc/cron.daily folder contains the **logrotate** script. Ensure that either the /etc/logrotate.conf or one of the files within the /etc/logrotate.d folder contains information on rotating the primary syslog file.
Compliance Criteria	Log files are rotated daily.
Test Nature	**Objective**
Evidence	Space intentionally left blank.
Findings	Space intentionally left blank.

VID12	**Apply Checksum Algorithm**
References	RID07 - http://www.securityfocus.com/infocus/1613
Risk: **MEDIUM**	The integrity of the syslog data is lost if the files are tampered with.
Testing Procedure	Talk to the administrator responsible for maintaining the syslog server and discuss file integrity. • Are the log files being encrypted? • Is a hashing algorithm being applied to the log files?
Compliance Criteria	Checksum algorithms must be applied to rotated log files.
Test Nature	**Subjective**
Evidence	Space intentionally left blank.
Findings	Space intentionally left blank.

VID13	Log Data Stored on Write-Once/Read-Many Media
References	RID06 - http://www.cert.org/security-improvement/practices/p092.html
Risk: **HIGH**	Data integrity could be compromised if data is not stored on write-once media.
Testing Procedure	Talk to the administrator responsible for maintaining the syslog server and discuss syslog storage. • How are the log files stored? • How many log files are maintained? • How long are the log files maintained? • Where are the log files physically stored?
Compliance Criteria	Syslog data must be stored on write-once media such as a CD/DVD-ROM.
Test Nature	**Subjective**
Evidence	Space intentionally left blank.
Findings	Space intentionally left blank.

VID14	Log File Disposal
References	RID06 - http://www.cert.org/security-improvement/practices/p092.html
Risk: **MEDIUM**	Old log information is not needed past any policy's stated retention period. Logs may still contain sensitive information that could be used inappropriately if data is not destroyed.
Testing Procedure	Talk to administrator responsible for maintaining the syslog server and discuss log file/media disposal. • How long are log files stored? • How is the storage media destroyed?
Compliance Criteria	Outdated log information must be destroyed after retention period has ended.
Test Nature	**Subjective**
Evidence	Space intentionally left blank.
Findings	Space intentionally left blank.

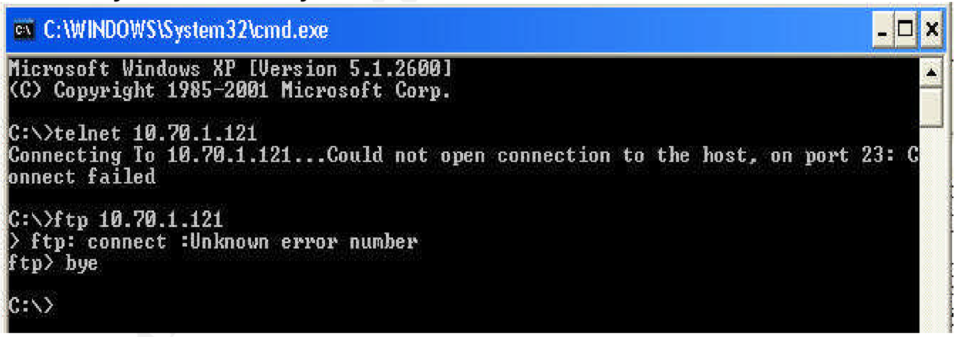
Conducting the Audit

All of the audit items are defined in detail in the previous section. This section, Conducting the Audit, will only contain the Evidence and Findings of each of the individual audit items.

Server Oriented Audit Items

VID01	Basic Vulnerability Check

<table>
<tr><td>Evidence</td><td>See Nessus results in Appendix B.</td></tr>
<tr><td>Findings</td><td><b>Failed Compliance Criteria.</b> Nessus found the following items of concern:
• The running version of SSH (3.6.1p2) is older than the current release of 3.8.1p1[11]. There is a flaw in the buffer management functions on versions older than 3.7.1.
• SSH allows older versions of the SSH protocol to connect to the server.
• The Apache web server is running.
  o The web server accepts several weaker ciphers when connecting via HTTPS.
  o Apache is allowing TRACE and TRACK methods.
• The server does not discard TCP packets that have the FIN flag set.
On the positive side, Nessus was only able to show that three ports are listening, TCP 22, 80 and 443.</td></tr>
</table>

<table>
<tr><th>VID02</th><th>Disable Insecure Network Services</th></tr>
<tr><td>Evidence</td><td>Manually tested ability to telnet or FTP.


Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>telnet 10.70.1.121
Connecting To 10.70.1.121...Could not open connection to the host, on port 23: Connect failed

C:\>ftp 10.70.1.121
> ftp: connect :Unknown error number
ftp> bye

C:\>

chkconfig --list telnet
error reading information on service telnet: No such file or directory

chkconfig --list vsftpd
vsftpd   0:off   1:off   2:off   3:off   4:off   5:off   6:off

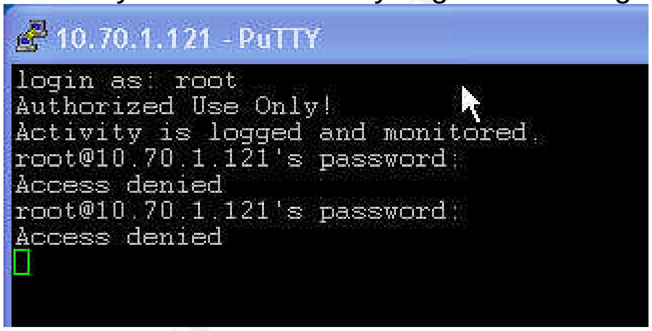
chkconfig --list rlogin
error reading information on service rlogin: No such file or directory

chkconfig --list rsh
error reading information on service rsh: No such file or directory

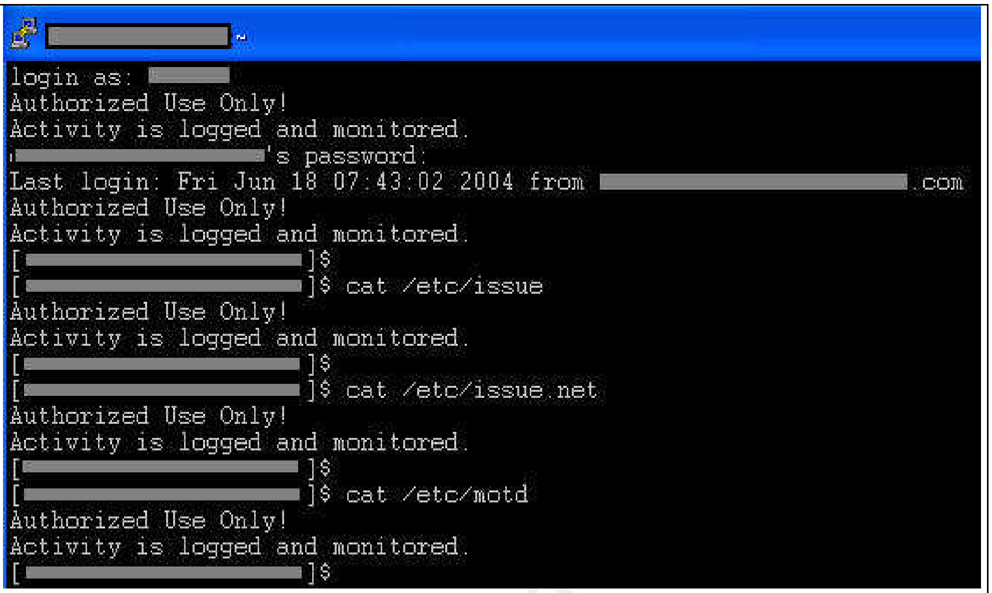
chkconfig --list shell</td></tr>
</table>

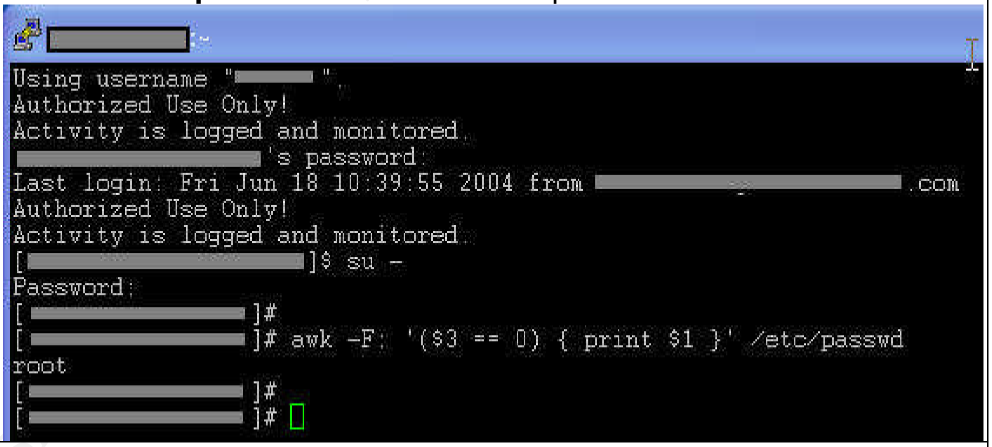
[11] The latest version of OpenSSH (http://www.openssh.org/) as of 6/18/04 was 3.8.1p1.

	error reading information on service shell: No such file or directory chkconfig --list login error reading information on service login: No such file or directory chkconfig --list tftp tftp off chkconfig --list imaps error reading information on service imaps: No such file or directory chkconfig --list pop3s error reading information on service pop3s: No such file or directory
Findings	**Passes Compliance Criteria.** The tested insecure services were either not installed or were not running.

VID03	**Preventing Root from Logging in Remotely**
Evidence	Manually tried to SSH to syslog server using root to login.  10.70.1.121 - PuTTY login as: root Authorized Use Only! Activity is logged and monitored. root@10.70.1.121's password: Access denied root@10.70.1.121's password: Access denied See Appendix C to view the entire sshd_config file.
Findings	**Passes Compliance Criteria.** The keyword **PermitRootLogin** is set to **no**.

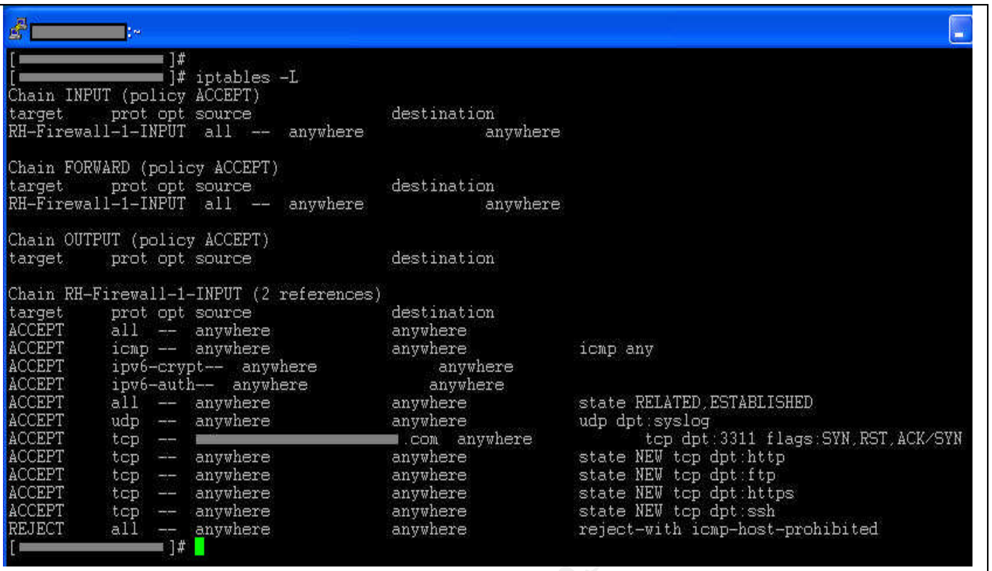
VID06	**Login Banner**
Evidence	Reviewing the contents of /etc/issue, /etc/issue.net and /etc/motd showed they all contained the same warning banner:

	 login as: [redacted] Authorized Use Only! Activity is logged and monitored. [redacted]'s password: Last login: Fri Jun 18 07:43:02 2004 from [redacted].com Authorized Use Only! Activity is logged and monitored. [[redacted]]$ [[redacted]]$ cat /etc/issue Authorized Use Only! Activity is logged and monitored. [[redacted]]$ [[redacted]]$ cat /etc/issue.net Authorized Use Only! Activity is logged and monitored. [[redacted]]$ [[redacted]]$ cat /etc/motd Authorized Use Only! Activity is logged and monitored. [[redacted]]$ See Appendix C for the /etc/ssh/sshd_config file. See Appendix D for the /etc/vsftpd/vsftpd.conf file.
Findings	**Passes Compliance Criteria.** Reviewing the stated files showed that an adequate warning banner is being used for remote logins.

VID08	**Only Root is UID 0**
Evidence	**Passes Compliance Criteria.** Check passwd file for UID 0:  Using username "[redacted]". Authorized Use Only! Activity is logged and monitored. [redacted]'s password: Last login: Fri Jun 18 10:39:55 2004 from [redacted].com Authorized Use Only! Activity is logged and monitored. [[redacted]]$ su - Password: [[redacted]]# [[redacted]]# awk -F: '($3 == 0) { print $1 }' /etc/passwd root [[redacted]]# [[redacted]]#
Findings	**Passes Compliance Criteria.** Only user with a UID of 0 is root.

Syslog Oriented Audit Items

VID10	**Authorized Syslog Devices**
Evidence	The current configuration of the iptables firewall is:



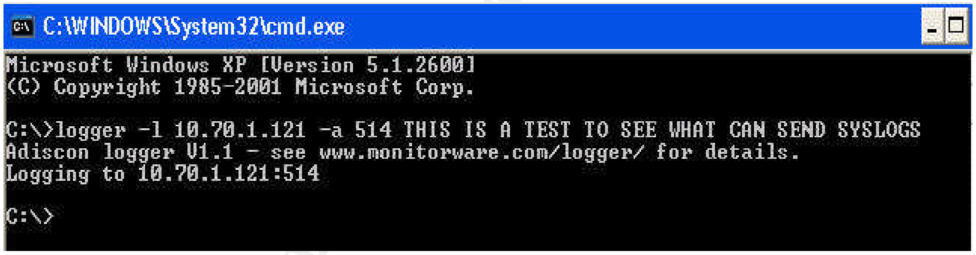
```
[redacted]:~
[[redacted]]#
[[redacted]]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere            icmp any
ACCEPT     ipv6-crypt--  anywhere             anywhere
ACCEPT     ipv6-auth--  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
ACCEPT     udp  --  anywhere             anywhere            udp dpt:syslog
ACCEPT     tcp  --  [redacted].com  anywhere           tcp dpt:3311 flags:SYN,RST,ACK/SYN
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:ftp
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:ssh
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-prohibited
[[redacted]]#
```

Test sending a syslog message from a “unauthorized” Windows XP workstation:

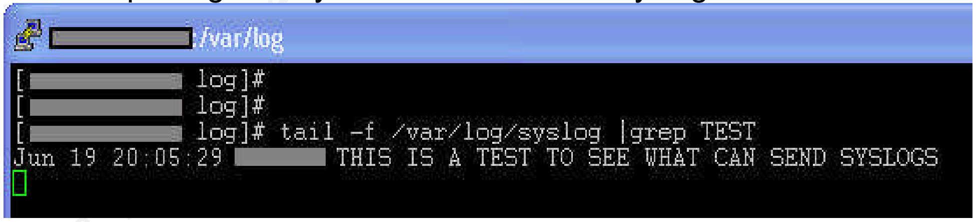


```
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>logger -l 10.70.1.121 -a 514 THIS IS A TEST TO SEE WHAT CAN SEND SYSLOGS
Adiscon logger V1.1 - see www.monitorware.com/logger/ for details.
Logging to 10.70.1.121:514

C:\>
```

While capturing for keyword “TEST” on the syslog server:

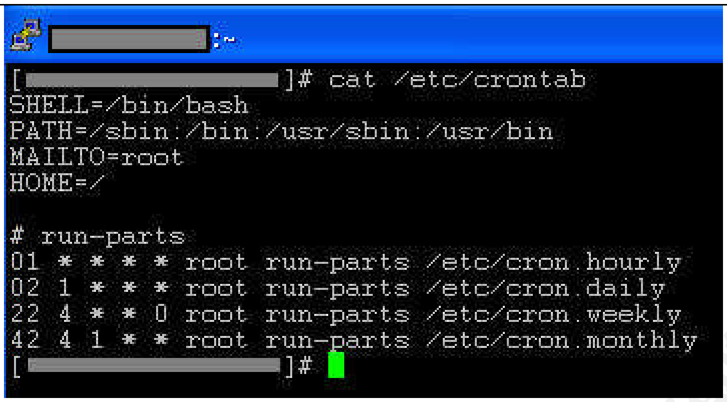


```
[redacted]:/var/log
[[redacted] log]#
[[redacted] log]#
[[redacted] log]# tail -f /var/log/syslog |grep TEST
Jun 19 20:05:29 [redacted] THIS IS A TEST TO SEE WHAT CAN SEND SYSLOGS
```

Logger for windows was obtained from www.monitorware.com.

Findings	**Fails Compliance Criteria.** While iptables appears to limit the services to only TCP 3311, HTTP, HTTPS, FTP, SSH and syslog; syslog is allowed from any host. This is also proven by manually sending a syslog message from an “unauthorized” device.

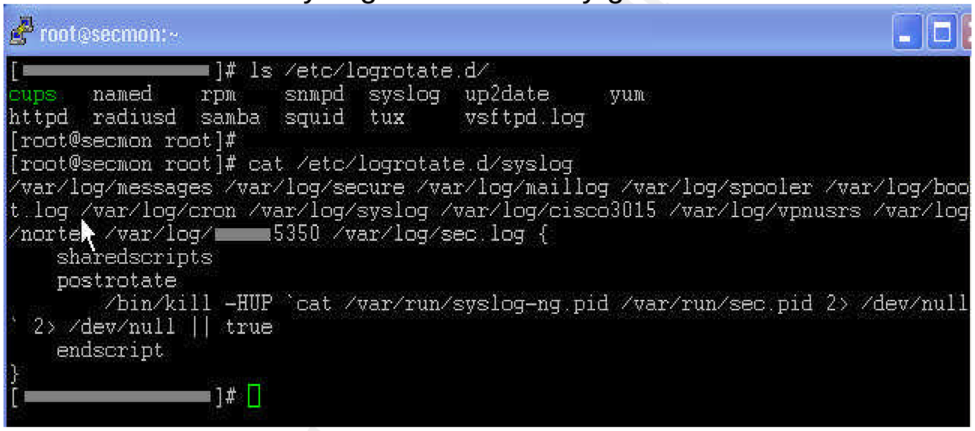
VID11	**Log Rotation**
Evidence	Checked the contents of /etc/crontab:

<table>
<tr>
<td></td>
<td>


<pre>
[redacted]:~
[[redacted]]# cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

run-parts
01 * * * * root run-parts /etc/cron.hourly
02 1 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
[[redacted]]#
</pre>

Verification that the syslog file will actually get rotated:



<pre>
root@secmon:~
[[redacted]]# ls /etc/logrotate.d/
cups   named   rpm   snmpd syslog up2date   yum
httpd   radiusd samba squid tux   vsftpd.log
[root@secmon root]#
[root@secmon root]# cat /etc/logrotate.d/syslog
/var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/boo
t.log /var/log/cron /var/log/syslog /var/log/cisco3015 /var/log/vpnusrs /var/log
/nortel /var/log/[redacted]5350 /var/log/sec.log {
    sharedscripts
    postrotate
        /bin/kill -HUP `cat /var/run/syslog-ng.pid /var/run/sec.pid 2> /dev/null
` 2> /dev/null || true
    endscript
}
[[redacted]]#
</pre>

See Appendix E for the entire configuration file.
</td>
</tr>
<tr>
<td>Findings</td>
<td><b>Passes Compliance Criteria.</b> Crontab is set to run the scripts in cron.daily on a daily basis. Review of /etc/logrotate.d/syslog shows that the actual syslog file is set to be rotated on a daily basis.</td>
</tr>
</table>

VID12	**Apply Checksum Algorithm**
Evidence	Discussed file integrity with the administrator of the syslog server. Currently, there is nothing being done to ensure the integrity of the syslog files.
Findings	**Fails Compliance Criteria.** There is no hashing algorithm being applied nor are the files encrypted.

VID13	**Log Data Stored on Write-Once/Read-Many Media**
Evidence	Discussed log storage with the administrator of the syslog server. Currently, two weeks of log data are stored locally. A script runs every night to send the previous days log files off to another server via FTP. The logs reside on the aggregation server until the total file size is enough to fill a DVD-ROM. After they log files are burned to DVD, they are maintained for a period of three years. All log files are stored onsite in a locked file cabinet.

Findings	**Passes Compliance Criteria with notes.** Log data is stored both on the local syslog server and a remote aggregation server. After enough log files are gathered, a DVD is burned for storage. However, files are transferred to the aggregation server via FTP. A secure protocol such as SFTP or SCP should be used to transfer the log files.

VID14	**Log File Disposal**
References	RID06 - http://www.cert.org/security-improvement/practices/p092.html
Risk: **MEDIUM**	Old log information is not needed past any policy's stated retention period. Logs may still contain sensitive information that could be used inappropriately if data is not destroyed.
Testing Procedure	Talk to administrator responsible for maintaining the syslog server and discuss log file/media disposal. • How long are log files stored? • How is the storage media destroyed?
Compliance Criteria	Outdated log information must be destroyed after retention period has ended.
Test Nature	**Subjective**
Evidence	Discussions with the administrator of the syslog server revealed that all media (CD's and DVD's) is destroyed manually after the data retention period of three years.
Findings	**Passes Compliance Criteria.** The media is physically shattered by hand.

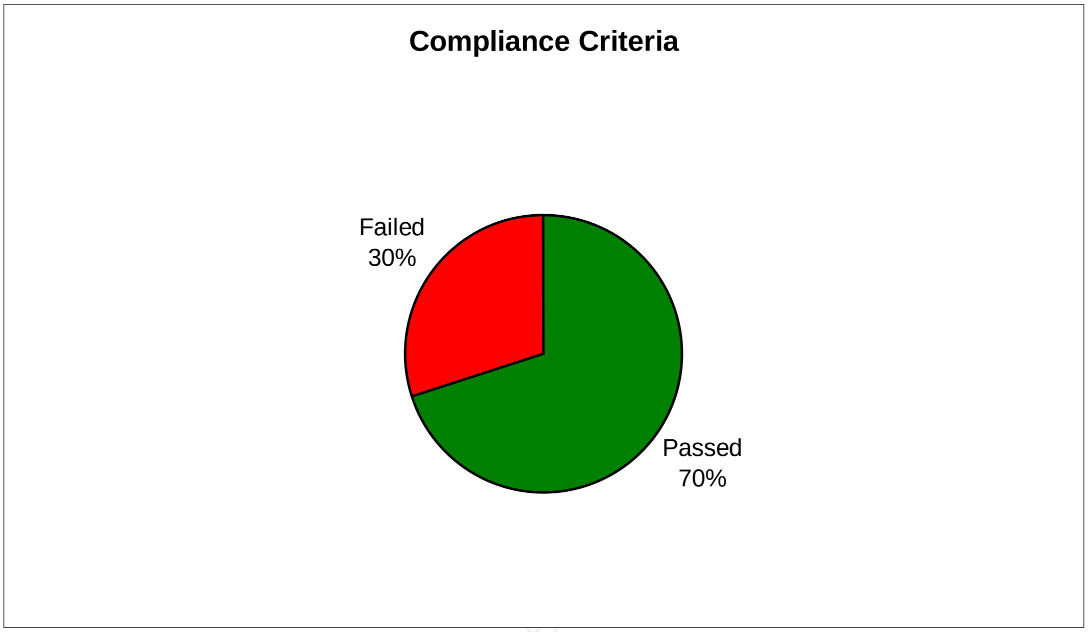
Audit Report

Executive Summary

An audit was conducted to validate the security of a centralized syslog server. The objective of this audit was to determine if any vulnerabilities existed and to ensure that the server was secure enough to store the company’s syslog data from critical network infrastructure.

A variety of tests were conducted on the syslog server to check for known vulnerabilities. These included physical tests with software to look for known holes or exploits as well as interviews with key personnel.

The current state of the syslog server is adequate. Graph 1 shows that 70 percent of the audit items met the Compliance Criteria while 30 percent failed. Although physical security of the server is good and network access is limited, there are still a few high-risk vulnerabilities that should be addressed.



Graph 1 Compliance Criteria

The syslog server could be brought to 100% compliance very easily, with almost no associated costs other than labor. Minor configuration changes will help properly secure the syslog server from any outstanding threats.

Audit Findings

Table 5 summarizes the audit results with a Pass/Fail grade on the Compliance Criteria.

Audit Item	Description	Meets Compliance Criteria
VID01	Basic Vulnerability Check	Failed
VID02	Disable Insecure Network Services	Passed
VID03	Prevent Root from Logging in Remotely	Passed
VID06	Login Banner	Passed
VID08	Only Root is UID 0	Passed
VID10	Authorized Syslog Devices	Failed
VID11	Log Rotation	Passed

VID12	Apply Checksum Algorithm	Failed
VID13	Log Data Stored on Write-Once/Read-Many Media	Passed
VID14	Log File Disposal	Passed

Table 5 Audit Findings Summarization

The syslog server met the compliance criteria for most tests. Audit items VID02, VID03 and VID08 showed strong access controls were already in place to guarantee that only authorized personnel were accessing syslog resources. The tests also show proper controls are in place to limit access to the root account of the syslog server.

Audit item VID06 shows proper due diligence as the syslog server displays a warning banner upon all logins, both local and remote. Although VID01 fails initial compliance tests, it does show that the syslog server is only listening on three ports, TCP 22, 80 and 443.

The failure of several key compliance tests indicate that the syslog server or the data it stores may be vulnerable to compromise. The three failures are highlighted as follows:

- The basic vulnerability scan performed in VID01 shows that the SSH service is out of date and needs to be upgraded. The current running version of 3.6.1p2 has a flaw in the buffer management functions.
- Audit item VID10 shows that any device on the network has the capability to send syslog data to the syslog server. This could prove detrimental to the system. If too many unauthorized devices are sending data to the system, unnecessary processing of that data could result in valid data being dropped. The unwanted data would also consume disk space and extend the length of time needed to backup or search historical data. Whether malicious or accidental, if too many devices are sending syslog data to the server this could result in a Denial of Service.
- Audit item VID12 reveals that checksum algorithms are not applied to the syslog files as they are rotated daily. Without valid checksum data, there is no way to prove that the syslog data has not been modified.

Recommendations

The following section will layout a series of recommendations to improve the security of the syslog server. Based on the audit findings, the syslog server is adequately secured against most threats, but a few key changes would significantly decrease the risk for exposure. All of the following items can be done with almost no associated costs other than the labor involved to perform the tasks.

- SSH
  - Upgrade OpenSSH (www.openssh.org) to the latest version.
  - Only allow SSH protocol 2 to connect to the server.
- Apache
  - Disable weak ciphers.
  - Disable the TRACE and TRACK methods.
- Filter incoming and outgoing ICMP timestamp requests.
- Ensure that iptables is only allowing authorized hosts to send syslog data to the syslog server.
- When sending data to the syslog aggregation server, the data should be sent via an encrypted means such as SFTP or SCP.
- All syslog files should have a checksum generated after they are rotated.

References

[1] Symantec. “Glossary.” URL: http://securityresponse.symantec.com/avcenter/refa.html (14 June 2004).

[2] Toxen, Bob. Real World Linux Security. Upper Saddle River: Prentice Hall, 2003.

[3] The Center for Internet Security. “Benchmarks/Tools.” URL: http://www.cisecurity.org/bench_linux.html (13 June 2004).

[4] George Oft. “Locking Down Your Linux Box - A Checklist Approach.” George’s Web Site. URL: http://georgetoft.com/linux/security/locking/checklist.shtml. (13 June 2004).

[5] Ortiz, Jorge. Auditing a Fedora Core 1 Linux. 17 February 2004. URL: http://www.giac.org/practical/GSNA/Jorge_Ortiz_GSNA.pdf. (15 June 2004).

[6] The Internet Engineering Task Force. “The syslog Protocol.” 29 April 2004. URL: http://www.ietf.org/internet-drafts/draft-ietf-syslog-protocol-04.txt. (15 June 2004).

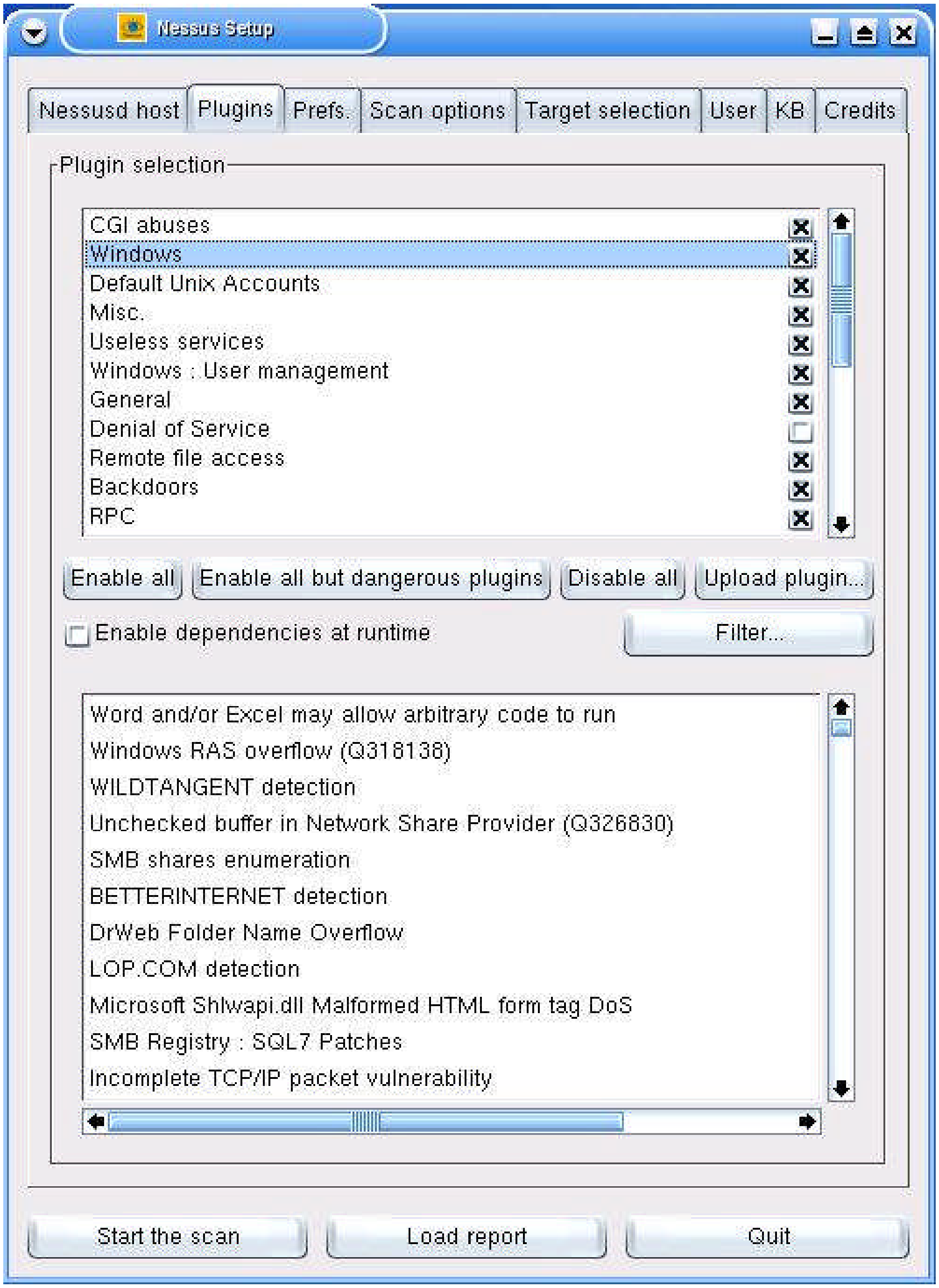
[7] CERT. “Managing logging and other data collection mechanisms.” 1 May 2001. URL: http://www.cert.org/security-improvement/practices/p092.html. (14 June 2004).

[8] Chuvakin, Anton. Advanced Log Processing. 1 August 2002. URL: http://www.securityfocus.com/infocus/1613. (13 June 2004).

[9] OpenBSD. “SSHD_CONFIG.” Manual Pages. 25 September 1999. URL: http://www.openbsd.org/cgi-bin/man.cgi?query=sshd_config&sektion=5&arch=&apropos=0&manpath=OpenBSD+Current. (14 June 2004).

Appendix A - Running Nessus

Choose which scans to run from the Plugins screen. Remember to disable the Denial of Service plugins if prior authorization has not been given, as the plugins will most likely crash at least one system.

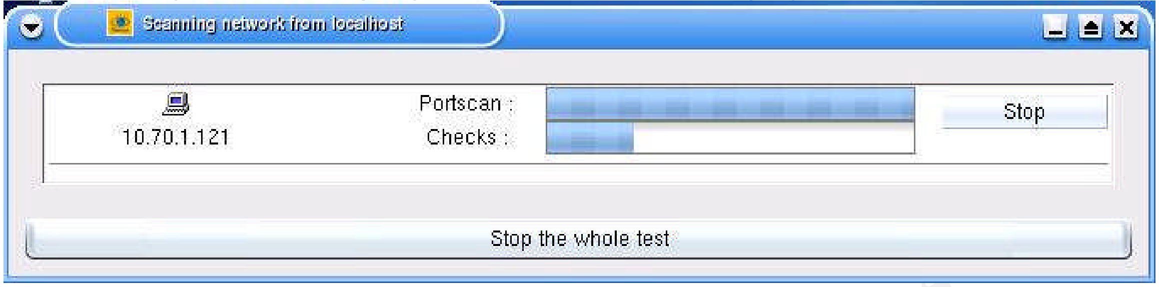


CGI abuses ☒
Windows ☒
Default Unix Accounts ☒
Misc. ☒
Useless services ☒
Windows : User management ☒
General ☒
Denial of Service ☐
Remote file access ☒
Backdoors ☒
RPC ☒

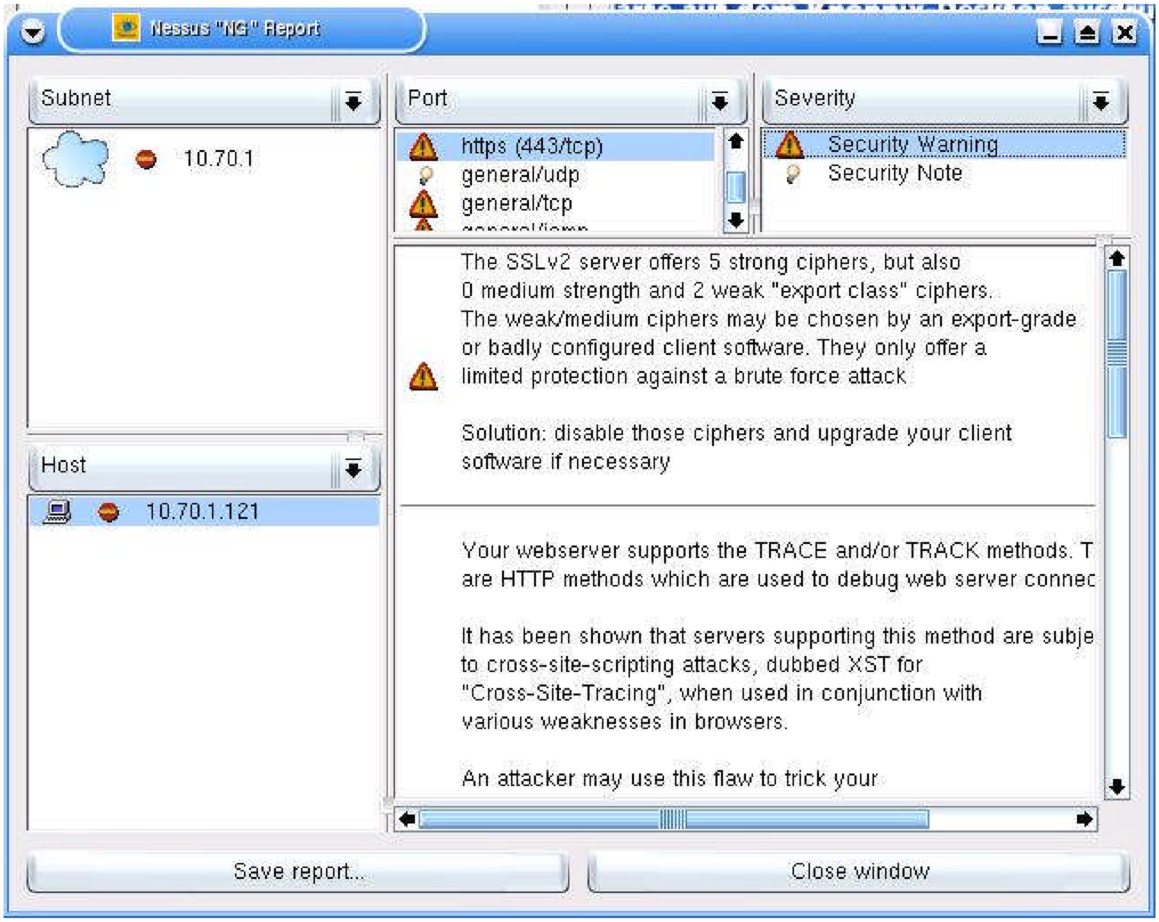
☐ Enable dependencies at runtime

Word and/or Excel may allow arbitrary code to run
Windows RAS overflow (Q318138)
WILDTANGENT detection
Unchecked buffer in Network Share Provider (Q326830)
SMB shares enumeration
BETTERINTERNET detection
DrWeb Folder Name Overflow
LOP.COM detection
Microsoft Shlwapi.dll Malformed HTML form tag DoS
SMB Registry : SQL7 Patches
Incomplete TCP/IP packet vulnerability

After starting the scan, a progress window will be displayed.



After the scan is complete, all vulnerabilities are displayed. Reports can be generated in many formats, such as HTML, ASCII, XML, etc.



The SSLv2 server offers 5 strong ciphers, but also
0 medium strength and 2 weak "export class" ciphers.
The weak/medium ciphers may be chosen by an export-grade
or badly configured client software. They only offer a
limited protection against a brute force attack

Solution: disable those ciphers and upgrade your client
software if necessary

Your webserver supports the TRACE and/or TRACK methods. T
are HTTP methods which are used to debug web server connec

It has been shown that servers supporting this method are subje
to cross-site-scripting attacks, dubbed XST for
"Cross-Site-Tracing", when used in conjunction with
various weaknesses in browsers.

An attacker may use this flaw to trick your

Appendix B - Nessus Results

Nessus Scan Report
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details	
Hosts which were alive and responding during test	1
Number of security holes found	1
Number of security warnings found	5

Host List	
Host(s)	**Possible Issue**
10.70.1.121	Security hole(s) found

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
10.70.1.121	ssh (22/tcp)	Security hole found
10.70.1.121	www (80/tcp)	Security notes found
10.70.1.121	https (443/tcp)	Security warning(s) found
10.70.1.121	general/tcp	Security warning(s) found
10.70.1.121	general/udp	Security notes found
10.70.1.121	general/icmp	Security warning(s) found

Security Issues and Fixes: 10.70.1.121		
Type	**Port**	**Issue and Fix**
Vulnerability	ssh (22/tcp)	You are running a version of OpenSSH which is older than 3.7.1 Versions older than 3.7.1 are vulnerable to a flaw in the buffer management functions which might allow an attacker to execute arbitrary commands on this host. An exploit for this issue is rumored to exist. Note that several distribution patched this hole without changing the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive. If you are running a RedHat host, make sure that the command : rpm -q openssh-server

		Returns : openssh-server-3.1p1-13 (RedHat 7.x) openssh-server-3.4p1-7 (RedHat 8.0) openssh-server-3.5p1-11 (RedHat 9) Solution : Upgrade to OpenSSH 3.7.1 See also : http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375452423794&w=2 http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375456923804&w=2 Risk factor : High CVE : CAN-2003-0682, CAN-2003-0693, CAN-2003-0695 BID : 8628 Other references : RHSA:RHSA-2003:279-02, SuSE:SUSE-SA:2003:039 Nessus ID : 11837
Warning	ssh (22/tcp)	 The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol. These protocols are not completely cryptographically safe so they should not be used. Solution : If you use OpenSSH, set the option 'Protocol' to '2' If you use SSH.com's set the option 'Ssh1Compatibility' to 'no' Risk factor : Low Nessus ID : 10882
Informational	ssh (22/tcp)	An ssh server is running on this port Nessus ID : 10330
Informational	ssh (22/tcp)	Remote SSH version : SSH-1.99-OpenSSH_3.6.1p2 Nessus ID : 10267
Informational	ssh (22/tcp)	The remote SSH daemon supports the following versions of the SSH protocol : . 1.33 . 1.5 . 1.99 . 2.0 Nessus ID : 10881
Informational	www (80/tcp)	A web server is running on this port Nessus ID : 10330
Informational	www (80/tcp)	 The remote web servers is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map or search page instead. Nessus enabled some counter measures for that, however they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate Nessus ID : 10386
Informational	www (80/tcp)	Nessus was not able to reliably identify this server. It might be: Apache/1.3.17 (Win32) The fingerprint differs from these known signatures on 2 point(s) Nessus ID : 11919
Informational	www (80/tcp)	The remote web server type is : Apache/2.0.49 (Fedora) Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers. Nessus ID : 10107
Warning	https (443/tcp)	The SSLv2 server offers 5 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers.

		The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack Solution: disable those ciphers and upgrade your client software if necessary Nessus ID : 10863
Warning	https (443/tcp)	Your webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials. Solution: Disable these methods. If you are using Apache, add the following lines for each virtual host in your configuration file : RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F] If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. If you are using Sun ONE Web Server releases 6.0 SP2 and later, add the following to the default object section in obj.conf: <Client method="TRACE"> AuthTrans fn="set-variable" remove-headers="transfer-encoding" set-headers="content-length: -1" error="501" </Client> If you are using Sun ONE Web Server releases 6.0 SP2 or below, compile the NSAPI plugin located at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603 See http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603 http://www.kb.cert.org/vuls/id/867593 Risk factor : Medium Nessus ID : 11213
Informational	https (443/tcp)	A SSLv2 server answered on this port Nessus ID : 10330
Informational	https (443/tcp)	A web server is running on this port through SSL Nessus ID : 10330
Informational	https (443/tcp)	The following directories were discovered: /cgi-bin, /email, /error, /icons, /manual, /phpSecurePages, /usage, /weblog While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards Nessus ID : 11032

Informational	https (443/tcp)	Here is the SSLv2 server certificate: Certificate: Data: Version: 3 (0x2) Serial Number: 4e:32:f4:a9:00:01:00:00:00:1b Signature Algorithm: sha1WithRSAEncryption Issuer: <REMOVED FOR PAPER> Validity Not Before: May 18 17:27:11 2004 GMT Not After : Jan 20 13:51:59 2005 GMT Subject: emailAddress=<REMOVED FOR PAPER> Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:c0:83:55:10:d5:e9:6b:b6:59:67:ec:d4:f2:f0: a2:20:62:06:a9:24:71:88:84:28:aa:19:31:27:d9: 12:02:f4:19:8c:53:b5:cb:81:c0:c9:10:99:6c:88: da:24:62:95:28:86:d9:f9:bb:28:63:26:49:be:a0: 87:a7:0a:91:09:b7:bb:55:5f:0a:df:05:b1:81:6d: f2:6e:0a:97:2d:94:9d:6b:5c:d0:a4:ea:bd:a2:b4: 93:a1:d4:3f:72:87:7c:32:f3:94:26:6f:d7:a1:1a: 0c:42:f7:bd:6c:71:15:e5:8b:a0:6b:a0:91:7c:98: 68:1a:23:0d:10:9a:6f:c0:8b Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Subject Key Identifier: 15:F5:82:EC:1F:B2:69:72:AC:FD:E1:74:42:CE:4A:7A:FE:E6:52:6D X509v3 Authority Key Identifier: keyid:1E:6E:D1:B1:75:D0:CB:9B:A0:F3:CE:20:60:2F:73:50:DA:21:E1:EA DirName:/emailAddress=<REMOVED FOR PAPER> serial:1D:81:D6:C6:00:01:00:00:00:08 X509v3 CRL Distribution Points: URI: <REMOVED FOR PAPER> URI:file://\\ <REMOVED FOR PAPER> Authority Information Access: CA Issuers - URI: <REMOVED FOR PAPER> CA Issuers - URI:file://\\ <REMOVED FOR PAPER> Signature Algorithm: sha1WithRSAEncryption 18:04:45:8c:f0:51:32:98:9b:85:c3:74:17:3f:4f:11:c2:eb: 3e:8b:02:a4:89:11:a9:dd:c5:49:a8:90:42:e6:f8:00:e8:b1: 8f:9f:21:c8:c0:c9:3b:c2:c7:fb:44:b5:cf:78:7e:bc:22:18: dc:c3:3d:33:e8:58:d6:f5:4c:b8:ad:59:b6:41:b1:fb:e8:30: 24:fd:8f:c7:ef:f8:8e:e7:61:db:55:7a:c9:ff:4f:b7:5c:4f: 40:81:81:ba:13:04:e9:ff:d5:8f:31:82:4d:e8:b6:4b:e7:fb: 24:f8:82:5a:27:ab:bc:72:e6:3f:ec:84:48:ae:fd:7c:45:00: 32:72:c7:b6:fe:07:5d:51:4e:a5:76:e1:57:f5:a0:f8:55:be: b6:a4:ba:86:12:a1:3a:0e:04:6f:83:aa:aa:4e:36:4f:73:cb: 40:55:84:0e:2a:94:c9:8c:30:39:b8:0a:08:5c:e7:ca:0f:0c: dd:13:7e:56:05:76:52:c3:c4:1e:64:c7:86:32:df:4f:cd:f0: 6e:87:76:a1:e1:36:91:6c:24:f8:ea:e1:33:f1:66:71:27:80: 71:21:3c:bc:f9:bc:7f:91:fb:f1:cd:39:1e:e8:e6:67:22:d5: cb:11:26:2f:bd:5b:28:5f:01:55:49:b0:23:e0:33:af:07:25: 1c:c1:01:63 Nessus ID : 10863
Informational	https (443/tcp)	Here is the list of available SSLv2 ciphers: RC4-MD5 EXP-RC4-MD5 RC2-CBC-MD5 EXP-RC2-CBC-MD5 DES-CBC-MD5 DES-CBC3-MD5 RC4-64-MD5 Nessus ID : 10863

Informational	https (443/tcp)	This SSLv2 server also accepts SSLv3 connections. This SSLv2 server also accepts TLSv1 connections. Nessus ID : 10863
Informational	https (443/tcp)	This web server was fingerprinted as: Apache/2.0.4x with DAV/2 on Linux which is not consistent with the displayed banner: Apache/2.0.49 (Fedora) If you think that Nessus was wrong, please send this signature to www-signatures@nessus.org : HTM:200:200:200:200:200:HTM:501:200:200:HTM:HTM:200:400:400:400:400:404:405:405:200:200:405:405:200:FIXME:Apache/2.0.49 (Fedora) Including these headers: ETag: "1ec142-55b-e34bfbc0" Nessus ID : 11919
Informational	https (443/tcp)	The remote web server type is : Apache/2.0.49 (Fedora) Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers. Nessus ID : 10107
Warning	general/tcp	The remote host does not discard TCP SYN packets which have the FIN flag set. Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules. See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html http://www.kb.cert.org/vuls/id/464113 Solution : Contact your vendor for a patch Risk factor : Medium BID : 7487 Nessus ID : 11618
Informational	general/udp	For your information, here is the traceroute to 10.70.1.121 : 10.70.30.190 10.70.1.121 Nessus ID : 10287
Warning	general/icmp	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols. Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). Risk factor : Low CVE : CAN-1999-0524 Nessus ID : 10114

This file was generated by Nessus, the open-sourced security scanner.

Appendix C - SSHD Configuration

```
#	$OpenBSD: sshd_config,v 1.59 2002/09/25 11:17:16 markus Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

#Port 22
#Protocol 2,1
#ListenAddress 0.0.0.0
#ListenAddress ::

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 3600
#ServerKeyBits 768

# Logging
#obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 120
PermitRootLogin no
#StrictModes yes
#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile     .ssh/authorized_keys

# rhosts authentication should not be used
#RhostsAuthentication no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
```

```
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

#AFSTokenPassing no

# Kerberos TGT Passing only works with the AFS kaserver
#KerberosTgtPassing no

# Set this to 'yes' to enable PAM keyboard-interactive authentication
# Warning: enabling this may bypass the setting of 'PasswordAuthentication'
#PAMAuthenticationViaKbdInt no

#X11Forwarding no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PrintMotd yes
#PrintLastLog yes
#KeepAlive yes
#UseLogin no
#UsePrivilegeSeparation yes
#PermitUserEnvironment no
#Compression yes

#MaxStartups 10
# no default banner path
Banner /etc/issue
#VerifyReverseMapping no

# override default of no subsystems
Subsystem       sftp    /usr/libexec/openssh/sftp-server
```

Appendix D - VSFTPD Configuration

The following is the configuration from the /etc/vsftpd/vsftpd.conf file.

```
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
```

```
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown
# below.
#xferlog_file=/var/log/vsftpd.log
#
# If you want, you can have your log file in standard ftpd xferlog format
xferlog_std_format=YES
#
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
#
# You may change the default value for timing out a data connection.
#data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
#async_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode.
# Beware that turning on ascii_download_enable enables malicious remote
parties
# to consume your I/O resources, by issuing the command "SIZE /big/file" in
# ASCII mode.
# These ASCII options are split into upload and download because you may wish
# to enable ASCII uploads (to prevent uploaded scripts etc. from breaking),
# without the DoS risk of SIZE and ASCII downloads. ASCII mangling should be
# on the client anyway..
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
ftpd_banner=Unauthorized access is prohibited.
#
```

```
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd.banned_emails
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES

pam_service_name=vsftpd
userlist_enable=YES
#enable for standalone mode
listen=YES
tcp_wrappers=YES
```

Appendix E - Logrotate

Contents of the /etc/logrotate.conf file:

```
# see "man logrotate" for details
# rotate log files daily
daily

# keep 4 weeks worth of backlogs
rotate 14

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp -- we'll rotate them here
/var/log/wtmp {
    monthly
    create 0664 root utmp
    rotate 1
}

# system-specific logs may be also be configured here.
```

This page intentionally left blank.