Global Information Assurance Certification Paper

SECURITY AUDIT REPORT

FOR YOURDOMAIN SERVERS
By ZARINA MUSA
AUGUST 2000

TABLE OF CONTENTS

SECTION 1

Executive Summary

This security audit review was conducted against two servers at "YourDomain" network. The review included analysis on operating system vulnerabilities, configuration vulnerabilities, risks from installed third-party software, administrative practices, backup policies, disaster preparedness. It also provides a prioritized list of recommended fixes to be performed on both servers.

Details of servers audited :

Item#	Server name	OS	Service Running	Primary function
1	**abcd.yourdomain.com**	RedHat Linux 6.0	Stronghold 2.4.2/ Apache 1.3.6	Web-based email server
2	**efgh.yordomain.com**	BSDI 4.1	Stronghold 2.4/ Apache 1.3.6	Web server

Findings

- A total of 2 servers were audited and both of them are identified as vulnerable.
- 9 vulnerabilities were found, 5 on abcd.yourdomain.com and 4 on efgh.yourdomain.com .
- The operating systems of both servers were not hardened.
- One misconfiguration on access control was found.
- A total of 6 potential vulnerabilities were identified. These vulnerabilities can be exploited in order to gain access to the server. The identified services are sendmail, mountd and fingerd.
- There is a total of two services running which were classified as dangerous. Root access attempts during the audit was succesful. They are linuxconf and printer services.

SECTION 2

Operating System Vulnerabilities

Operating system vulnerabilities include problems that involve file permissions, the file system of the host, system start-up files, and daemons and services running on the system.

Scan Details
Tools used in this security audit :
For scanning – nmap, ISS and rpcinfo.
For locating potential problems in system configuration - Tiger.

A run of Tiger gives a lot of warning messages regarding file permissions on both servers. However, no messages indicating serious problems.
Recommendation : harden both servers. Run Tiger, and see whether you need to perform rectifications based on the output.

Port scan result using nmap for **abcd.yourdomain.com**
#nmap scan initiated Fri July xxxx as : ./nmap –sS –O –v –P0 –oN abcd.yourdomain.com.log abcd.yourdomain.com
Intersting ports on (xxxx):

Port	State	Protocol	Service
21	open	tcp	ftp
23	open	tcp	telnet
25	open	tcp	smtp
79	open	tcp	finger
80	open	tcp	http
98	open	tcp	linuxconf
111	open	tcp	sunrpc
113	open	tcp	auth
443	open	tcp	https
513	open	tcp	login
514	open	tcp	shell
515	open	tcp	printer
604	open	tcp	unknown
609	open	tcp	npmp-trap
1002	open	tcp	unknown
1023	open	tcp	unknown
1024	open	tcp	unknown
6000	open	tcp	X11

TCP sequence Prediction: Class=random positive increments
Difficulty=3391251(Good Luck!)

Sequence numbers:36A38B07 369F749E 364698B5 3688D123 35EAAB13 36618E86
Remote operating system guess:Linux 2.1.122 – 2.2.13

RPC Info for **abcd.yourdomain.com**
#/usr/sbin/rpcinfo –p abcd.yourdomain.com

program	**vers**	**proto**	**port**	**service**
100000	2	tcp	111	portmapper
100000	2	udp	111	portmapper
100024	1	udp	1000	status
100011	1	udp	1011	rquotad
100011	2	udp	1011	rquotad
100005	1	udp	1021	mountd
100005	1	tcp	1023	mountd
100005	2	udp	602	mountd
100005	2	tcp	604	mountd
100005	3	udp	607	mountd
100005	3	tcp	609	mountd
100003	2	udp	2049	nfs
100021	1	udp	1024	nlockmgr
100021	3	udp	1024	nlockmgr
100021	1	tcp	1024	nlockmgr
100021	3	tcp	1024	nlockmgr

Port scan result using ISS 5.8 for **efgh.yourdomain.com**

Service Name	**Description**	**Port#**	**Type**
Chargen	Character Generator	19	TCP
Daytime	Daytime	13	TCP
Discard	Discard	9	TCP
Echo	Echo	7	TCP
Exec	remote procedure execution	512	TCP
Finger	finger	79	TCP
ftp	File Transfer [Control]	21	TCP
httpd	World Wide Web HTTP	80	TCP
https	https Mcom	443	TCP
ident	Authentication Service	113	TCP
imap	Interim Mail Acess Protocol v2	143	TCP
kpop	kpop	1109	TCP
login	remote login a la telnet;	513	TCP
pop3	Post Office Protocol – Version 3	110	TCP
printer	spooler	515	TCP
shell	like exec but automatic	514	TCP
smtp	Simple Mail Transfer	25	TCP
sunrpc	SUN Remote Procedure Call	111	TCP
tcp-mux	TCP Port Service Multiplexer	1	TCP

telnet	Telnet	23	TCP
time	Time	37	TCP

RPC Info for **efgh.yourdomain.com**
#rpcinfo –p yourdomain.com

program	**vers**	**proto**	**port**	**service**
100000	2	tcp	111	rpcbind
100000	2	udp	111	rpcbind
100024	1	udp	921	status
100024	1	udp	923	status
100021	1	udp	925	nlockmgr
100021	3	udp	925	nlockmgr
100021	4	udp	925	nlockmgr
100021	1	tcp	929	nlockmgr
100021	3	tcp	929	nlockmgr
100021	4	tcp	929	nlockmgr
100021	3	tcp	929	nlockmgr

Service matrix as gathered from the scanning activity.

Port	**abcd.yourdomain.com**	**efgh.yourdomain.com**
7		•
9		•
13		•
19		•
21	•	•
23	•	•
25	•	•
37	•	•
79	•	•
80	•	•
111	•	•
113	•	•
143		•
443	•	•
512		•
513	•	•
514	•	•
515	•	•
593	•	•
609	•	•
1109		•
6000	•	

Note:
- Port Open

Vulnerabilities found :
1. Problems with sendmail services.

   Sendmail command EXPN and VRF at both **abcd.yourdomain.com** and **efgh.yourdomain.com**

   By exploiting the sendmail vulnerability, a malicious user may be able to gather information, such as usernames, and about user accounts located on the system on which sendmail resides. Using this information, it would then be a relatively simple task for the malicious user to gain access to the system.

2. Problems with daemon services

   a) Finger at both **abcd.yourdomain.com** and **efgh.yourdomain.com**

   Some finger daemons release information about the user's shell, home directory and group membership. This information may be used by hackers to attack the system. Some of the information can also be used to compromise the user account. For example, information such as the last time the user logged into the system could be used to build a table of usage patterns. Another example is that by knowing the user's home directory and exploiting a vulnerabillity in the mail system, a hacker could create an entrance into the system.

   b) RPC nlockmgr services at **efgh.yourdomain.com**

   The RPC nlockmgr service has been detected as running. The nlockmgr is part of the file locking manager system for NFS. It forwards local file locking requests to the lock manager on the server system. The nlockmgr service registers with the RPC portmapper as program 100021.

   c) Mountd at **abcd.yourdomain.com**

   A vulnerability in mountd could allow a remote attacker to cause a buffer overflow, and to use the resulting condition to execute arbitrary code with root privileges.

3. Dangerous services

   These are classified as dangerous services sincer it was able to gain root access and totally take over the servers via these services.

   a) Linuxconf at **abcd.yourdomain.com**
   It was possible to gain root access through the linuxconf services.

b) Printer services at **abcd.yourdomain.com**
It was possible to gain root access through the printer services

Configuration vulnerabilities

Access Control Configuration

Trusted host at **efgh.yourdomain.com**
A trusted host relationship between two hosts allows an intruder to use one host to gain access to a second host.

SECTION 3

Risks from installed third-party software

Both **abcd.yourdomain.com** and **efgh.yourdomain.com** has a Stronghold Secure Web Server (Stronghold 2.4.2/Apache 1.3.6) installed. These two web servers are running http and https(secure) connections.

- They are run as a non-privileged user.
- Proper access control is already being implemented using directives in config files.
- Secure connections require client certificates.
- Common web server compromises are through CGI exploits.
  Refer to this guideline, taken from
  "How To Eliminate The Ten Most Critical Internet Security Threats The Experts' Consensus" Version 1.25 July 12, 2000 Copyright 2000, The SANS Institute

  a) Do not run web servers as root

  b) Get rid of CGI script interpreters in bin directories:
  http://www.cert.org/advisories/CA-96.11.interpreters_in_cgi_bin_dir.html

  c) Remove unsafe CGI scripts

  http://www.cert.org/advisories/CA-97.07.nph-test-cgi_script.html

  http://www.cert.org/advisories/CA-96.06.cgi_example_code.html

  http://www.cert.org/advisories/CA-97.12.webdist.html

  d) Write safer CGI programs:

http://www-4.ibm.com/software/developer/library/secure-cgi/

http://www.cert.org/tech_tips/cgi_metacharacters.html

http://www.cert.org/advisories/CA-97.24.Count_cgi.html

e) Don't configure CGI support on Web servers that don't need it.

f) Run your Web server in a chroot()ed environment to protect the machine against yet to be discovered exploits.

SECTION 4

Administrative Practices

- The management of these two servers are done remotely using standard UNIX password and in clear-text.
  Recommendation : use SSH or VPN

- Access is allowed to all ports and from all machines. No access control is implemented.
  Recommendation : use TCPwrapper

- No backup policies are in place.
  Recommendation : Define a proper backup procedure and plan as a fallback for any kind of discrepancies. Regularly test your backups by restoring files. If possible, avoid doing network backups.

- Equipment inventory is really minimal.
  Recommendation : Put serialized tag on all equipment. Build a database for this.

Other recommendations :

- Install appropriate tools to facilitate automation of security monitoring and intrusion detection.
- Define a standard operational procedure and policy to effectively manage the servers and the services.

SECTION 5

Prioritized List of Security Vulnerabilities

Prioritized list of security vulnerabilities for abcd.yourdomain.com

1. Linuxconf
2. Printer services
3. Mountd
4. Sunrpc services
5. Sendmail service
6. Finger service
7. Disable all other unnecessary services : login, shell, X11
8. Host not hardened
9. Allows access from all machines and for all services.
10. Using standard UNIX password in clear-text.

Prioritized list of security vulnerabilities for efgh.yourdomain.com

1. Trusted host relationship
2. The RPC nlockmgr service as been detected as running. The nlockmgr is part of the file locking manager system for NFS. It forwards local file locking requests to the lock manager on the server system. The nlockmgr service registers with the RPC portmapper as program 100021.
3. Sendmail service
4. Finger service
5. Disable all other unnecessary services : chargen, daytime, discard, echo, exec, imap, kpop, login, pop3, printer, shell, sunrpc, tcp-mux, time
6. Host not hardened.
7. Allows access from all machines and for all services.
8. Using standard UNIX password in clear-text.

SECTION 6

Prioritized list of recommended fixes

Prioritized list of recommended fixes for abcd.yourdomain.com

1. Disable linuxconf service in /etc/inetd.conf. If linuxconf service is required, restrict to local network and apply patch.
   http://www.redhat.com/support/errata/RHEA1999060-1.6.0.html

2. Disable printer service in /etc/inetd.conf. If printer service is required, restrict to local network and apply patch.
   http://www.redhat.com/support/errata/RHSA2000002-01.6.0.html

3. If the system is not being used as an NFS server, then disable the mountd. Otherwise, install a patch for the vulnerability. Check CERT advisory 98.12 for informatiom about obtaining patches for your particular version of Linux.
   http://www.cert.org/CA-98.12.mountd.html
   http://www.redhat.com/support/errata/RHSA1999032_01.html.

4. Disable sunrpc services

5. Make sure the sendmail command EXPN and VRFY is off. To eliminate this vulnerability, you will need to modify the sendmail configuration file(sendmail.cf). The example below shows how to do this:
   #privacy flags
   O PrivacyOptions=authwarning
   O PrivacyOptions=noexpn
   O PrivacyOptions=novrfy

6. Finger service. Comment out fingerd in /etc/inetd.conf
   #finger stream tcp nowait nobody /usr/sbin/tcpd in.fingerd
   then restart inetd

7. Disable all unnecessary services. Services can be disabled by either :
   a) editing /etc/inetd.conf
   b) using Linuxconf
   c) using /usr/sbin/setup.
   d) Using chkconfig
   e) Removing the links in /etc/rc?.d directory

8. Perform host hardening on **abcd.yourdomain.com.** Update all necessary rpm files for Redhat 6.0 http://www.redhat.com.support/errata/rh60-errata-general.html

9. Enable tcp_wrapper especially for telnetd and ftp.

10. Use SSH or VPN for remote access to do remote management on the server instead of telnet and ftp. It also recommended to use dual factor authentication which is password and certificate.

Prioritized list of recommended fixes for efgh.yourdomain.com

1. A trusted host relationship between two hosts allows an intruder to gain access to a second host. Remove the trusted relationship and use a more secure authentication mechanism. Trusted relationships are often controlled by the contents of the /etc/hosts.equiv file and users' .rhosts files. These files should be sanity checked and/or removed.

2. This service should be disabled if your system is not acting as either an NFS client or server.

3. Make sure the sendmail command EXPN and VRFY is off. To eliminate this vulnerability, you will need to modify the sendmail configuration file(sendmail.cf). The example below shows how to do this:
   #privacy flags
   O PrivacyOptions=authwarning
   O PrivacyOptions=noexpn
   O PrivacyOptions=novrfy

4. Finger service. Comment out fingerd in /etc/inetd.conf
   #finger stream tcp nowait nobody /usr/sbin/tcpd in.fingerd
   then restart inetd

5. Disable all unnecessary services.

6. Perform host hardening on **efgh.yourdomain.com.**

7. Enable tcp_wrapper especially for telnetd and ftp.

8. Use SSH or VPN for remote access to do remote management on the server instead of telnet and ftp. It also recommended to use dual factor authentication which is password and certificate.

References

"How To Eliminate The Ten Most Critical Internet Security Threats The Experts' Consensus" Version 1.25 July 12, 2000 Copyright 2000,

Lee Brotzman , "Running UNIX Applications Securely"

Lee Brotzman, "Linux Practicum"

Hal Pomeranz, "Common Issues and Vulnerabilities in Unix Security"

Matt Bishop, "Unix Security Tools and Their Uses"

Last Updated: April 21st, 2018

Upcoming Training

SANSFIRE 2018	**Washington, DC**	**Jul 14, 2018 - Jul 21, 2018**	**Live Event**
SANS Network Security 2018	**Las Vegas, NV**	**Sep 23, 2018 - Sep 30, 2018**	**Live Event**
SANS London October 2018	**London, United Kingdom**	**Oct 15, 2018 - Oct 20, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**