Global Information Assurance Certification Paper

GSNA Practical v4.0 Option 1

Auditing an Apache Server on a FreeBSD System

Chihyao Lin
January 10, 2005

Table of Contents

Abstract

This paper contains an audit of an Apache Server on a FreeBSD System. The system works as the only Web server of an organization. It is said that the Web server is a means of the organization to share public information and provide an environment for members of the organization to register courses provided by the organization. Since prevention is always better than cure, the system is audited by an auditor in order to find potential vulnerabilities and remove them. In this paper, an audit of the system is discussed from the background to impacts that might exist on the system. It is also performed the potential vulnerabilities that might cause the impacts and the way to test them. After that, the result about findings during the tests is also presented to provide a reference for solving problems.

Section I: Identification

1.1 Background of the system being audited

A successful audit comes from a clear scope. According to SANS Audit track material, it is suitable to audit the target from a small and clear scope. That is, it is essential to discuss the system you want to audit carefully and clearly and it is practically good to audit it as simple as possible if the scope is hard to define. For this reason, the identification of an audit process comes before other parts. In this paper, an audit of a Web server on a FreeBSD system is discussed. The organization name of this auditor is supposed as a fake name as ECI for keeping privacy. In this section, the identification of this system is shown from hardware architecture to software installation. It is intended to provide a basic but clear view of this system.

The following part is the specification of this Web server and its role in ECI.

Hardware

Acer Altos 1200LP server
CPU: P III 1GHz X2
Memory: 2G SDRAM
Hard drive: SEAGATE, ST336605LC 40G SCSI hard drive X2
Network interface: Intel 82557 NIC

Software

Operating system: FreeBSD 5.3.
Web server version: Apache 2.0.52.
CGI language version: PHP 4.3.10.
Database software: MySQL 4.0.22.

The purpose of this system:

This system works as the only Web server of ECI which has about forty employees. This Web server is used to provide public information to the public and an environment for people to register activities held by ECI on line. This Web server also has a database server running on the same system. The database is used to store members' information. A customer has to join as a member before he or she is able to register courses. In addition, the auditor is told by the system administrator that this Web server is placed on a different network next to the internal network where employees' computers are connected. There are two firewalls used to protect this Web server: one is used to control access from the internal network, and another one is used to prevent it from being accessed unexpectedly from the outside world. The Web server is intended to be accessed from the Internet via port 80 and port 443. The system administrator of this system is the only person who has the right to access the system remotely or physically. The mechanism for access the system remotely is through SSH which is used to manage the system or update web pages remotely. Beside that, there is a Web interface administrative web page of ECI for the system administrator to log into to manage members' data of ECI. Since Ports collection is used by FreeBSD or other BSD system like OpenBSD or NetBSD to install or manage ported applications easily, the system administrator thinks that it is easy to manage packages by installing them from the Ports collection of FreeBSD system. All packages installed on the system are via Ports collection because of this reason. The architecture of those devices or systems is shown in Figure 1

for a better understanding.

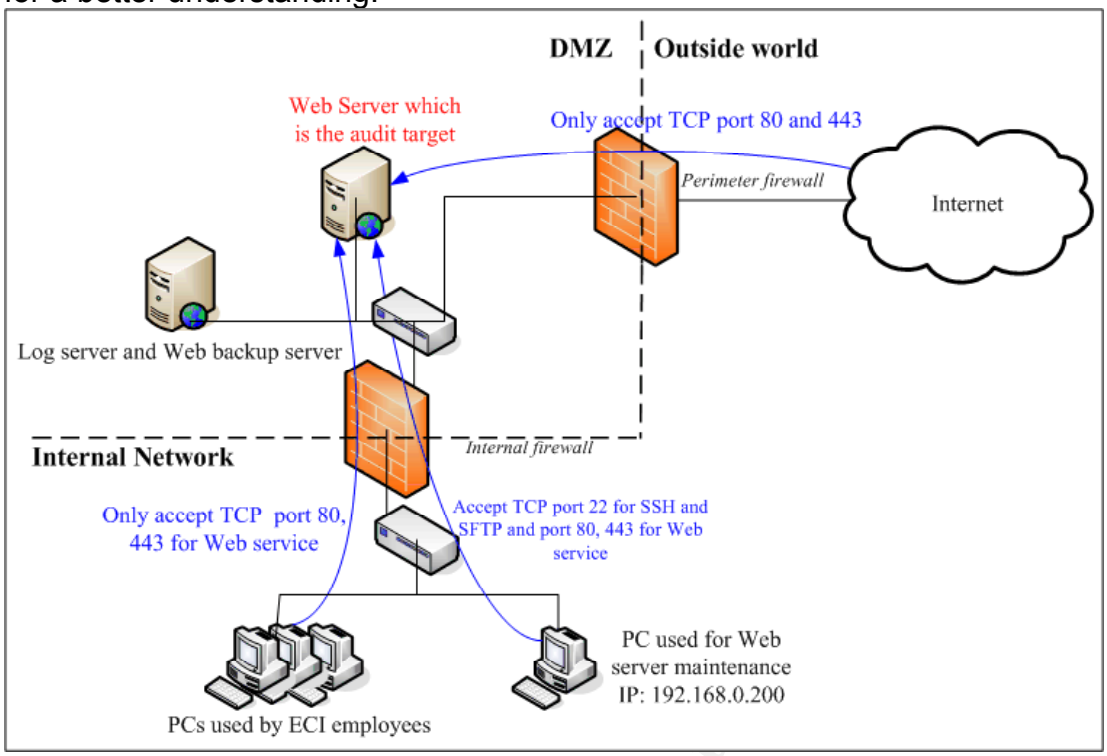

Figure 1. ECI Web service architecture

The information which is useful and is realized by the auditor at this time is as follows.

1. Information about software used to provide Web service and its related versions is realized.
2. There are packet filtering devices in front of this Web server to provide additional protection.
3. It is told that the system administrator is the only one who has the right to change web pages of this system and maintain the system.
4. It is unclear that if the physical restriction to this system works fine.

1.2 The reason to check this system

It is shown that this Web server is one means of ECI to do their business. It is much important to make sure this system is secure enough by removing the "low hanging fruit" part. The low hanging fruit means the system is not protected well that it is easy for crackers to compromise it. Although there is no 100 percent security, it is still necessary and worthwhile to audit the system and solve problems found during the audit. This is a kind of prevention and should be taken regularly since prevention is always better than cure.

1.3 Reference of best practices

It is necessary to refer to industry best practice for providing suitable control and measure practice. The reason is that it is always good to check others' advices and suggestions to maintain a secure system. By reading the best practice, benchmarks or guidelines, some things shown in the materials might bring us new ideas and the reasons for them to do that might persuade us or not. No matter whether we would agree with them or not,

some thing new comes to our mind. For this reason of checking the best practice, the auditor has referred to some of them which are related to the system. For example, the FreeBSD and Apache benchmarks are the main resources used by the auditor. Here is the list.

- The Center for Internet Security (CIS) -- "FreeBSD_benchmark_v1.0.4" [1]
  The benchmark discusses how to make your FreeBSD system more secure.
- The Center for Internet Security (CIS) -- "CIS_Apache_Benchmark_v1.0" [1]
  The guideline discusses the way to configure a more secure Apache server.
- The Open Web Application Security Project (OWASP) -- "OWASPGuideV1.1" and "OWASPGuideV1.1.1" [2]
  The guideline discusses how to build secure web applications and web services.

---

1. http://www.cisecurity.org/
2. http://www.owasp.org/

Section II: Risk Analysis

2.1 The basic concept of a risk

In this section, a risk analysis about the system introduced in the previous section is discussed. In the beginning, it is suitable to show the concept of relationships between threat, vulnerability, consequence and risk. That is:

Risk = Threat x Vulnerability x Consequence. [3]

To be able to understand the relationships of those items, let's discuss each item one by one. First, threat can be considered as the factors that can negatively affect the system availability, integrity and confidentiality. Next, vulnerability can be considered as the weakness which can be used to decrease the value of the system. Finally, the consequence presents the impact of a successful attack. Here is an easy example to demonstrate this idea. Image a situation that there is a thief wants to break into a great mansion to steal money or jewelry. The thief could be thought as the threat and an unlocked window of the house could be considered as vulnerability. Both of threat and vulnerability need to be existed together to bring a risk. If one of them is missed, there is no risk. For example, if there is a system which has a remote security hole. It would still have no risk if it is unplugged though. Since not all attacks would make the same impact, it is necessary to discuss if it is critical or not. That is why the consequence is also an important factor to consider a risk. In other words, the mansion that has valuable things inside it could be thought as a computer system which has valuable information or data. A thief could be thought as a potential attack launched by crackers to negatively affect the computer system. The unlocked window could be thought as a vulnerable application running on the system since both of them could be abused by the attackers (thieves or crackers) in order to break into the house or compromise the system. Finally, no all attacks would bring the same impact is also useful when discussing cyberspace security.

After having a basic concept of a risk, it is suitable to use this concept to audit the Web server introduced in Section I. As the target of the audit is a public server, it is asked to comply with a very secure level. To be able to satisfy this, many requirements might be needed. Although it is a good thing to list those requirements as many as possible, it is not going to be done in this paper. Actually, only three most important testing items for improving the ----------

3. ISO 17799

system security will be discussed here. The three items are introduced to address three of the most serious impacts related to the system. That is, the three items would be used to audit the system in order to find if the system could pass the test or not. The audit result would also be used as the reference for solving problems. All jobs are aimed to improve the security of the system. As it is the most important goal of audits.

2.2 The three most serious impacts

In this part, three most serious impacts related to the system are discussed. Only three impacts listed here do not mean there are only three impacts to consider, it just gives a basic example to demonstrate the procedure of audit. There are also several possible vulnerabilities related to each impact since more than one of them might cause the same impact. The following part shows the information as tables for giving a better understanding.

1. The service is unavailable

Description	This Web server is unable to provide a reliable service all the time. In this impact, only hardware and environment situations are talked here. Software issues are discussed in other part.
Reason of Checking	As a production server, the most basic ability is to provide a twenty-four hour and seven days a week service. If there is no service, it doesn't have to consider the security at all. The Web server of ECI is aimed to provide a lot of public information and an environment for customers to register courses held by ECI. It is really important to provide a reliable service in case of business loss.
Impact level	High
Possible vulnerabilities (impact level)	● Hardware crash. (High) ● Electronic problems. (High) ● Physical security problem. (High) ● Backup mechanism failure. (High)

2. Firewall protection is not working right

Description	The firewalls used to protect the Web server are not configured well. The Web server would be exposed on a wild world, which is too dangerous to face it. Another impact is that the Web server might not be accessed as expectation. For example, a wrong configuration of the firewall might block all packets to the Web server. That might produce a DoS situation.

Reason of Checking	In spite of the hardware or environment situations, the protection comes from other systems or devices like firewalls is also important to check. Consider the principle of "Defense of Depth", the important value like members' information could be thought as the jewelry in a castle. The system itself could be thought as the castle and the protection comes from the firewall could be thought as walls around the castle. It is always good to have more layers of protection since it is safer when some layers are broken but other layers still have the ability to protect the "jewelry".
Impact level	Medium to High
Possible vulnerabilities (impact level)	● The perimeter firewall in front of the Web server is configured wrong. (High) ● The internal firewall in front of the Web server is configured wrong. (Medium)

3. Protection offered by the system itself doesn't work correctly

Description	Protection on the system itself is not only considered as packages used to provide additional protection but also includes correct setting of the system and latest patches installed on the system. If not all requirements are satisfied, impacts from sensitive information disclosed to system compromised by attackers would happen.
Reason of Checking	The system itself is the last line of defense. It is necessary to check the system itself to find potential vulnerabilities before being abused by crackers. Since most attacks and automatic attacking software like worms or robots focus on known vulnerabilities. It would be better to fill the security holes on the system before bad things happen. As the risk equation shown in Section 2.1, risk is the function of vulnerability and threats. Both of vulnerability and threats are needed to be presented to cause a risk. Since there are not many things that we can do to decrease the threats around us, it would be better to decrease the risk of the system by removing potential vulnerabilities instead.
Impact level	Medium to High
Possible vulnerabilities (impact level)	● Latest patches of OS are not applied. (High) ● All packages used for the Web server to work fine and securely are either installed or latest. (High) ● Apache settings are not correctly configured. (Medium to High) ● The password of administrator of Web administrative web page of ECI is not well set. (High)

Section III: Testing

In this section, three testing ways to identify the three most serious impacts discussed in the previous section are shown. It is intended to provide details about how to test those impacts. It is important to provide a clear and complete information about each test since it would make the audit procedure much easier. Not all people would know clearly what the auditor wants to do. Because of that, a clear written procedure would make them feel comfortable especially for the person being audited. In order to make the effect of auditing process much lower, all tests are performed on weekends.

3.1 Test for checking "The service is unavailable" impact

There are several vulnerabilities that might cause this impact. That is, hardware crash, electronic problems, physical security and backup mechanism failure. All tests of those vulnerabilities are discussed individually.

3.1.1 Hardware crash:

It is unable to predict when a hardware problem would happen. We will not spend time on determine the time of hardware failure but check whether there is a backup server with up to date data can be used to take over the original system. The test is to shut down the Web server intentionally to produce a hardware crash situation and change the IP address of the backup server to the Web server. If the Web content provided by the backup server is the same as the original Web server, it passes the test.

3.1.2 Electronic problems:

It is unable to predict when an electronic problem would happen like the one in the hardware crash problem. Instead this test checks if the UPS would take responsibility for providing power when there is an electronic problem and the power generator would start to run automatically after 5 minutes. The power generator is not configured to start right after an electronic problem is because that most of electronic problems would recover within 5 minutes. This can reduce the times to use the power generator. The way to check is to ensure that the power cord of the Web server is plugged into a socket of a UPS. Then the switch of the main power is turned off intentionally. After 5 minutes, check if the UPS still has the ability to provide power and the power generator starts to run automatically. Finally, change to use the main power again and see if the power generator would stop to run automatically. If the Web server works as usual during the whole process, it passes the test.

Note: This time value (5 minutes) is defined according to the policy.

3.1.3 Physical security problem:

The way to check if there is a physical security problem is to try to access the Web server physically and shut down the system by the auditor himself. Since the auditor has no right to access the server remotely or physically. It is expected that the auditor won't shut down the system eventually and this expected result means the system passes this test.

3.1.4 Backup mechanism failure:

The way to check if the backup mechanism works fine is the same way shown in the hardware crash part. Shut down the Web server and change

the IP address of the backup server to the Web server. If the Web content is the same as the original Web server, it passes the test. In other words, this test is not needed after completing hardware crash test.

3.2 Test for "Firewall protection is not working right" impact

3.2.1 The perimeter firewall in front of the Web server is configured wrong.

In this test, Nmap[4] is used to check the open ports from the Internet to the Web server. Nmap is a powerful port scanning tool used to verify the port status of a system. It is used here to make sure that only port 80 and 443 are open. The command and its options enabled in this test are as follow:

 # nmap –P0 –sS –sV –p 1-65535

In the command, the option *P0* asks Nmap not to ICMP ping host before the scan; this is helpful for checking hosts behind the firewall. Since the Web server behind the perimeter might not be able to be pinged, it is better to turn on this option. Next, the option *sS* ask Nmap to do TCP SYN scan against the target. Then, the options *sV* asks Nmap to do the version detection. This is helpful to ensure that open ports are actually owned by the expected services but not something unusual. Finally, all ports from 1 to 65535 are checked by using the option *–p 1-65535*.

At the same time of launching Nmap, Tcpdump[5] which is a common used sniffing tool is used on the Web server to check the only packets seen by the system are the packets which has the port 80 or port 443 set on their destination port filed. The command is as follows:

 # tcpdump –n host IP_of_host_doing_scan > target_file

---

4. http://www.insecure.org/
5. http://www.tcpdump.org/

In the command, the option *n* asks Tcpdump not to convert address to name for providing a pure IP result. The remaining options used in the command ask Tcpdump to show only information with the host which scans the Web server.

If the result shows that the only open ports to the Internet are port 80 and port 443, the system passes this test.

3.2.2 The internal firewall in front of the Web server is configured wrong:

Nmap is also used to check the open ports which can be accessed from the internal network to the Web server. Since there is a computer used to maintain the contents of the Web server and remote management, another port checking process related to its IP address is performed too. The command is as follows:

 # nmap –P0 –sS –sV –p 1-65535

This command is launched twice; one is on the machine whose IP set to the one as the computer used to maintain the Web server, and another one is on the machine whose IP set to another IP address. For example, the first one is set to 192.168.0.200, and the second one is set to 192.168.0.2.

In addition, Tcpdump is run again on the Web server to check packets seen by the system. The command is as follows:

 # tcpdump –n host IP_of_host_doing_scan > target_file

If the result shows that the only open ports to the internal net are port 80

and port 443, it is the expected result.

If the result shows that the open ports to the computer whose IP address is used for Web maintaining are port 80, 443 and 22, it is the expected result.

If the above expected results are shown during the test, the system passes this test.

3.3 Test for "Protection offered by the system itself doesn't work correctly" impact

There are several potential vulnerabilities related to this impact. That is, latest patches of OS are not applied; all packages used for the Web server to work fine and securely are either installed or latest; Apache settings are not correctly configured; the password of administrator of Web administrative web page of ECI is not well set. The ways to check those potential vulnerabilities are discussed individually.

3.3.1 Latest patches of OS are not applied:

Check if CVSup package is installed on the system, and the configuration of CVSup is correct. The correct configuration file of CVSup should be something similar to this:

```
*default host=cvsupXX.freebsd.org
*default base=/usr
*default prefix=/usr
*default release=cvs
*default tag=RELENG_5_3
*default delete usr-rel-suffix
*default compress

src-all
*default tag=.
ports-all
```

If the value of default tag is not RELENG_5_3, or there is no src-all or ports-all entries, it is considered that the configuration is not right. Next, it is necessary to check if source codes fetch by CVSup is up to date. This could be done by verifying if there is an automatic mechanism to launch CVSup regularly or if the UPDATING file which is a clue for verifying if the source codes on the system is latest of the source codes (a file usually placed in the /usr/src directory, and used to contain updated information of FreeBSD system) on the system is the newest. If the source codes on the system are up to date, then the auditor will discuss with the system administrator to ensure that he has applied all patches and use the following command to find the system information.

#uname –a

The result of the above command should contains *5.3-RELEASE-P4*.

Only if all above checks are successful, the system is considered passing the test.

3.3.2 All packages used for the Web server to work fine and securely are either installed or latest:

Since all packages needed to provide Web service on the system are installed from "Ports collection", the information of installed packages can be

checked by using *pkg_version* command. Before launching those commands, make sure that the Ports collection files on the system are up to date. This can be done by launching CVSup command again before doing the following checks.

Note: If the system could pass "Check if the latest OS patches are applied" test, the Ports collection files should be up to date since the ports-all appears in the CVSup file stands for fetching all new Ports collection.

As it is shown in Section I, the latest Apache 2, PHP 4, MySQL 4.0 are as follows: Apache 2.0.52, PHP 4.3.10 and MySQL 4.0.22. The following is the expected result of those checks.

Apache:
 # pkg_version –v | grep apache
apache-2.0.52_4 = up-to-date with port
PHP:
 # pkg_version –v | grep php4
php4-4.3.10 = up-to-date with port
MySQL
 # pkg_version –v | grep mysql
mysql-server-4.0.22 = up-to-date with port

In other words, if the version information of the Apache, PHP and MySQL is lower than this or the up-to-date with port information is not shown, it fails the test. Since there are two Apache modules (Mod_security[6] and Mod_dosevasive[7]) used to provide further protection, they need checking too.

Mod_security:
 # pkg_version –v | grep mod_security
mod_security-1.8.6 = up-to-date with port
Mod_dosevasive:
 # pkg_version –v | grep mod_dosvasive
mod_dosevasive20-1.9 = up-to-date with port

The way to check the modules are the same as checking Apache, PHP or MySQL. That is, if the up-to-date with port information is not shown, it fails the test.

3.3.3 Apache settings are not correctly configured:

In this part, there are several things need checking. They would be discussed separately. It is impossible to mention all settings about Apace here. For the sake of completeness, it is recommended to refer to "CIS Apache Benchmark" provided by CIS or Apache modules documents[8].

All tests here for checking Apache settings are chosen by the auditor based on the importance and will be used to audit the Web server.

---

6. http://www.modsecurity.org/
7. http://www.nuclearelephant.com/projects/dosevasive/
8. http://httpd.apache.org/docs/mod/

1. Check if Apache is run as root privilege.

Description	Apache is run as root privilege.
Impact	If attackers could compromise Apache process, they might get root privilege.

Impact Level	High
The way to test it	Check if the following setting existing in the httpd.conf user: WWW Group: WWW If the above settings are presented, it passes the test.

2. Check if directories of the Web server could be listed.

Description	Directory is able to list.
Impact	Attackers might know better of data on the Web site. This might help them prepare other attacks or know of directory structures.
Impact Level	Medium
The way to test it	1. Check if the default setting: *Options Indexes* has been changed to *Options –Indexes* 2. Try to access a sub directory that doesn't have a default web page to see if it replays a HTTP 403 forbidden message. If this setting has changed to Options –indexes and the HTTP 403 forbidden is returned when the auditor is accessing the directory with no default web page, it passes the test.

3. Check if there is a DoS evasion mechanism set on the system.

Description	DoS evasion is not set.
Impact	If there is no DoS evasion mechanism, the Web site might be affected by DoS attacks badly.
Impact Level	Medium
The way to test it	Check the httpd.conf to find if there is a loaded module: *LoadModule dosevasive20_module* If the above settings are presented, it passes the test.

4. Check if the server information could be disclosed.

Description	Server Information disclosed.
Impact	If attackers could know the type of the Web server, it might help them prepare further attacks.
Impact Level	Medium
The way to test it	1. Check *if ServerSignature Off* is set in the httpd.conf file 2. Check if *<IfModule mod_security.c>* *SecServerSignature "fake server"* *</IfModule>* is set in the httpd.conf file. 3. Check if *expose_php = Off* is set in the php.ini file If all above settings are presented, it passes the test.

3.3.4 The password of administrator of Web administrative web page of ECI is not well set:

A tool named Brutus is used to guess the username/password of the Web administrator web page. I order to make the checking efficiently, the

mod_dosvasive of Apache will be disabled during the test if it is installed and enabled. As the name implies, this tool has the ability to perform brute-force username/password guessing against the administrative web page of ECI. If the attacker could find the username/password to an administrative account, then data on the database could be collected, added or deleted. This is a potential vulnerability that is needed to be identified. If the auditor could not find an account with administrative privilege, it passes the test.

---

9. http://www.hoobie.net/brutus/

Section IV: Auditing

In this section, the three tests listed in the previous section are used to audit the Web system. Before taking the procedure, the auditor had requested a written permission and had it signed by the boss of ECI. The difference between an audit and an attack is the permission. It is always necessary to keep this in mind in case of trouble.

4.1 Audit of "The service is unavailable" test

Test items	Pass/Fail	Findings
Test if hardware crash	Pass	After modifying the IP address of the backup server, the backup server severed the same web page to customers. *Ref: Section 3.1.1*
Test if electronic problems	Pass	At 5 minutes later than turning off the main power, the power generator started to run, and the UPS has about 70 % remaining capacity. When the main power was turned on again after another 5 minutes later, the power generator stopped. *Ref: Section 3.1.2*
Test if physical security problem	Pass	The auditor tried to access the Web server physically. Since there is a restriction on computer room to disallow the auditor's entering and the rack which contains the Web server is always locked, it is not unable to shut down the Web server. *Ref: Section 3.1.3*
Test if backup mechanism failure	Pass	The method used to test the one is the same as the hardware crash test. That is, the result of this one is the same as the one of the hardware crash. *Ref: Section 3.1.4*

4.2 Audit of "Firewall protection is not working right" test

Test items	Pass/Fail	Findings
Test if the perimeter firewall in front of the Web server is configured wrong.	Pass	The result of the test complied with the expected result. It passed the test. *Ref: Section 3.2.1.*

Snapshots

1. The result of Nmap scanned from the Internet to the Web server.

```
home# nmap -PO -sS -sV -p 1-65535 [redacted]

Starting nmap 3.77 ( http://www.insecure.org/nmap/ ) at 2005-01-08 11:42 CST
Interesting ports on [redacted]:
(The 65533 ports scanned but not shown below are in state: filtered)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd
443/tcp open  ssl/http Apache httpd


Nmap run completed -- 1 IP address (1 host up) scanned in 324.819 seconds
```

2. The result of Tcpdump listening on the Web Sever while the above scan was running.

Because of the data of this one is more than 200 lines; the following command is used to check what ports of the Web server are shown in the file. This command *prints* the content of the Tcpdump file, selects the fifth filed data (the destination IP address plus destination port) of each line by using "*awk '{print $5}'*" command, *greps* only the wanted IP address of the Web Sever from the data, *sorts* them and merges all same data to just one line (*uniq*).

 # cat tcpdump_file | awk '{print $5}' | grep IP_of_Web_server | sort | uniq

IP_of_Web_server.443:

IP_of_Web_server.80:

The result of the command shows the only accessed ports to the scanning host is port 80 and 443.

Test items	Pass/Fail	Findings
Test if the internal firewall in front of the Web server is configured wrong.	Pass	The result of the test complied with the expected result. It passed the test. *Ref: Section 3.2.2.*

Snapshots

1. The result of Nmap scanned from the Internet to the Web server.

a. The scanning result from a normal computer on the internal net.

```
home# nmap -PO -sS -sV -p 1-65535 [redacted]

Starting nmap 3.77 ( http://www.insecure.org/nmap/ ) at 2005-01-10 15:47 CST
Interesting ports on [redacted]:
(The 65533 ports scanned but not shown below are in state: filtered)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd
443/tcp open  ssl/http Apache httpd


Nmap run completed -- 1 IP address (1 host up) scanned in 315.601 seconds
```

b. The scanning result from the computer whose IP address set to 192.168.0.200 which is able to access the Web server port 22, 80 and 443 on the internal net.

```
home# nmap -PO -sS -sV -p 1-65535 [redacted]

Starting nmap 3.77 ( http://www.insecure.org/nmap/ ) at 2005-01-10 15:57 CST
Interesting ports on [redacted]:
(The 65532 ports scanned but not shown below are in state: filtered)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 3.8.1p1 (protocol 2.0)
80/tcp  open  http     Apache httpd
443/tcp open  ssl/http Apache httpd


Nmap run completed -- 1 IP address (1 host up) scanned in 309.299 seconds
```

2. The result of Tcpdump listened on the Web Sever while the above scan was running.

a. The Tcpdump data related to 1.a., and the data is extracted by the same command. That is,

 # cat tcpdump_file | awk '{print $5}' | grep IP_of_Web_server | sort | uniq

IP_of_Web_server.443:
IP_of_Web_server.80:

b. The Tcpdump data related to 1.b., and the data is extracted too.

IP_of_Web_server.22:
IP_of_Web_server.443:
IP_of_Web_server.80:

This result shows that the result complies with the expected result.

4.3 Audit of "Protection offered by the system itself doesn't work correctly" test

Test items	Pass/Fail	Findings
Test if latest patches of OS are not applied.	Pass	1. The package CVSup is installed on the system. 2. There is a CVSup configuration file with the content the same as the one in Section 3.3.1 named cvsupfile in the /etc directory. 3. There is a file named 160.cvsupfile with executive attribute placed in the /etc/periodically/daily directory. That means the file will be launched every day. The content of this file is as follows: *#!/bin/sh* */usr/local/bin/cvsup –g –L 2 /etc/cvsupfile* With this mechanism, the source codes would not be older than one day. 4. There is an UPDATING file in the /usr/src directory with the following information in the top of this file [see snapshots below]. This means this file is latest. 5. Using *# uname –a* command returns 5.3-RELEASE-P4. *Ref: Section 3.3.1.*

Snapshots

1. The sample content of the UPDATING file. This file shows the latest content at the time of writing this paper.

```
Updating Information for FreeBSD stable users

This file is maintained and copyrighted by M. Warner Losh
<imp@village.org>.  See end of file for further details.  For commonly
done items, please see the COMMON ITEMS: section later in the file.

Items affecting the ports and packages system can be found in
/usr/ports/UPDATING.  Please read that file before running
portupgrade.  Important recent entries: 20040724 (default X changes).

20050106:       p4      FreeBSD-EN-05:02.sk
        Correct bugs in the sk(4) network driver that could result in
        data corruption and system crashes on SMP systems.

20050103:       p3      FreeBSD-EN-05:01.nfs
```

	Pass/Fail	Findings
Test if all packages used for the Web server to work fine and securely are either installed or latest.	Fail	1. Apache, PHP, and MySQL, are the latest version. 2. Mod_security and Mod_dosvasive. are not installed on the system. *Ref: Section 3.3.2*

Test items	Pass/Fail	Findings
Test if Apache settings are not correctly configured.	Fail	Not all tests in this part succeed. The details about each test are as follows: ● Check if Apache is run as root privilege: Pass ● Check if directories of the Web server could be listed: Pass There is an *Options –Indexes* entry in the httpd.conf file, and it returns a 403 forbidden message when the auditor tried to access a directory without default web page. ● Check if there is a DoS evasion mechanism set on the system. Fail There is no *LoadModule dosevasive20_module* entry in the httpd.conf file. ● Check if the server information could be disclosed: Fail. There is no *<IfModule mod_security.c>* *SecServerSignature "fake server"* *</IfModule>* in the httpd.conf file and *ServerSignature* is set to *On* Ref: Section 3.3.3.

Test items	Pass/Fail	Findings

Test if the password of administrator of Web administrative web page of ECI is not well set.	Pass	There is no account with administrative privilege could be find on the system. [see snapshots below] *Ref: Section 3.3.4.*

Snapshots

1. It is unable to identify the username/password.

4.4 Recommendations

After performing the whole audit, it is shown that the Web server passes most of the tests. Failing some tests means there are some things could be done to make the system more secure. In addition, it is also found that the administrative web page could be used to log in via HTTP protocol or HTTPS protocol. For the sake of completeness, here are some recommendations related to the Web server.

1. It is highly recommended that the system administrator refers to the audit result and the test methods to install packages or configure settings to solve potential vulnerabilities in order to provide a more secure system.
2. It is highly recommended that the administrative web page should be accessed via HTTPS connection only in case of sniffing attacks.
3. It is recommended that the audit of the system is performed regularly, and the tests against to different impacts should be reviewed and updated to be able to audit the system successfully and effectively.

References

[1] Steve Mancini, *"Auditing a Squid Web Proxy Server: An Auditor's Report"* Available at: http://www.giac.org/practical/GSNA/Steven_Mancini_GSNA.pdf

[2] Herschel Gelman, *"Audit of a Small LAMP (Linux, Apache, MySQL and PHP) Web Application"* Available at: http://www.giac.org/practical/GSNA/Herschel_Gelman_GSNA.pdf

[3] Tony Yao, *"Auditing an Apache for Windows Web Server: An Auditor's Perspective"* Available at: http://www.giac.org/practical/GSNA/Tony_Yao_GSNA.pdf

[4] Kelly Hertel, *"Auditing Apache Secure Reverse Proxy On HP-UX in a Large Scale Production Environment: An Auditor Perspective"* Available at: http://www.giac.org/practical/GSNA/Kelly_Tully_GSNA.pdf

[5] The Center for INTERNET SECURITY. *FreeBSD Benchmark.* http://www.cisecurity.org/bench_freebsd.html

[6] The Center for INTERNET SECURITY. *Apache Server Benchmark.* http://www.cisecurity.org/bench_apache.html

[7] The Open Web Application Security Project. *OWASP Guide to Building Secure Web Applications version 1.1.1.* http://prdownloads.sourceforge.net/owasp/OWASPGuideV1.1.1.pdf?download

Last Updated: May 29th, 2017

Upcoming Training

SANS Secure Europe 2017	**Amsterdam, Netherlands**	**Jun 12, 2017 - Jun 20, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**