Vulnerability Scanning with OpenVAS

Laboratory Report in EDA263/DAT641 Computer Security

Oskar Åkergren
Pär Svedberg

Group 1

Version no: 1.0

March 17, 2015

Contents

List of Tables

List of Figures

1 Introduction

In this report the details of a vulnerability scan on the host known as "Rome" will be presented. The purpose of conducting this report is to analyse the current security level, and with these analyses recommend the measurements that are needed to provide the host with the highest security possible.

The structure of the report is as follows:
Section 2 provides a description of the vulnerability scanning utility OpenVAS in general and the specific setup of this scan. Section 3 is the section where the results are presented, section 4 is where the discussion of the results is held and lastly, in section 5, the conclusion will be stated.

2 Description of OpenVAS Setup

Open Vulnerability Assessment System is a system that collects multiple services and tools, called "Network Vulnerability Tests" (NVT) and presents them in a single interface, allowing the user to combine them to a thoroughly vulnerability scan [1].

The logical layout of the network scanned for this report is presented in Figure 1, where the target is "rome.secnet". OpenVAS is installed on the intermediate server between the target and our client machine.

Scanning a host is a method to control in which ways a system is open to the outside, and it is one of the methods an attacker might conduct to search for entry points in a system [2]. There are several types of vulnerability scans, such as "port scan", "database scan", "web application security scan" and others [3].

The scans used in this report is in order: "port scan", "service fingerprinting" and "network vulnerability scan". The different scans will produce a list of open ports found on the host, combined with a fingerprint scan that will search through these open ports and generate a fingerprint of what type of services that are behind these ports. The fingerprint will contain the available information, such as the names and versions of services.

In the scans we expect a result in the form of information about open ports and the services behind them, marked with the security risk of each port and/or service.

To perform a scan with OpenVAS, the system needs to be installed on a server. In the interface of OpenVAS, the user choose which types of NVTs should be conducted with each scan, what port range to use and which target in the network the scan is aimed at.

The aim of this report is to detect as many open ports as possible, within reason. The host is not known to have any extraordinary security issues, so the OpenVAS default port range was chosen as a suitable range, as it provides a wide range of well known ports.

2.1 Port Scanning

A set of tests in OpenVAS, called "Port Scanners", were used to perform the port scanning, see Figure 2.

These NVTs where chosen so that a thorough port scan were conducted, and the open ports on the target will be displayed clearly. By doing this, information is gained on which ports on the target there are services listening for incoming connections. This is also similar to what a potential attacker would do.

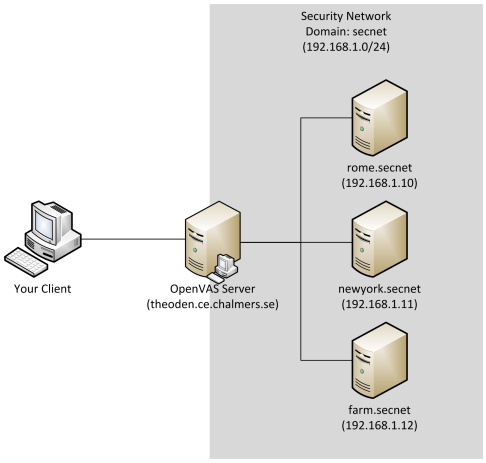

Figure 1: The network setup

Policy	0 of 11			
Port scanners	16 of 16			
Privilege escalation	0 of 49			

Figure 2: Port Scanners NVT

2.2 Service fingerprinting

The settings we used in this section is the ones presented in Figures 3 and 4

2.2.1 Service Fingerprinting

To see which kind of services are running on the target system, OpenVAS was set up to try to get identifying information from them. Here the NVT families used were the ones collected in the NVT families "General" and "Service detection". In addition to the self-explaining "Service detection", "General" was added to broaden the detection possibilities.

Gain a shell remotely	0 of 92			
General	2392 of 2392			
Gentoo Local Security Checks	0 of 1728			

Figure 3: General NVT

SNMP	0 of 6			
Service detection	561 of 561			
Settings	0 of 12			

Figure 4: Service detection NVT

2.2.2 Remote Host Fingerprinting

When doing this fingerprinting we will try to conclude what information is revealed of the system, in form of operative system such as Windows or Linux.

2.3 Vulnerability Scanning

When the vulnerability scan was preformed, the predefined scan "full and fast" was used in order to detect all possible issues, see Figure 5.

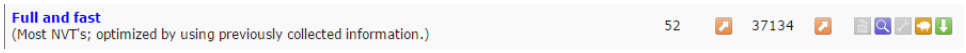

Figure 5: Vulnerability scan

3 Results

As shown in Table 1, there are a number of open ports that belongs to relatively well known services. There is no imminent threat on these ports, although some services might be old and unused, it depends on what services on the host that are actually in use.

The services detected are presented in Table 2, even though there are very few of them.

3.1 Port Scanning

When performing a port scan on the system, the ports found to be open are listed in Table 1. If the server is not part of a Microsoft Windows network, it should be considered to close the Windows related services and ports. Nothing abnormal was found.

Table 1: Information about open ports

Port Number	**Service Name**	**Service Task**	**Suggestion**
53	DNS	Domain Name System	Keep
80/8080	HTTP	Web traffic	Keep
143/993	IMAP/ IMAPS	Email retrieval	Keep
445	Microsoft-DS	Microsoft network services [1]	Keep[2]
139	NetBIOS Session Service	Used by Microsoft-DS	Keep[2]
110/995	POP3/ POP3S	Email retrieval	Keep
22	SSH	Secure data communication	Keep

[1] Includes 'Active Directory: authentication and authorization' and 'SMB: File and printer sharing'
[2] Keep if the network rely on MS services related to this server

3.2 Fingerprinting

3.2.1 Services

As seen in Table 2, one service was identified from the service fingerprinting scan, a Domain Name System (DNS) server called bind with the version number 9.7.0-p1. This version was released in 2010 and is outdated.

However, when performing the vulnerability scan, the fingerprints of the services listed in Table 3 were found.

Of interest here is that all the listed services are old and outdated. Apache Tomcat 6.0.24 is a java servlet/web server that was released in 2010. Being published in 2009, the installed version of Apache HTTP web server is one year older than its java counterpart. The SMB server, Samba, is used for Linux/UNIX program interoperability with Windows and the current version dates back to 2010. Also OpenSSH, used for secure connections between computers, is of a version from 2010. All of the aforementioned services have multiple known security vulnerabilities.

Table 2: Service fingerprint

Service	**Version**
DNS server	bind 9.7.0-p1

Table 3: Vulnerability scan fingerprint

Service	**Version**
Java servlet web server	Apache Tomcat 6.0.24
HTTP web server	Apache 2.2.14
mail server	Dovecot
SMB server	Samba 3.4.7
OpenSSH	OpenSSH 5.3p1

3.2.2 Remote Host

Analysing the information gained by the vulnerability scan, the system's operating system were confirmed to be of the Linux distribution Ubuntu. Combining this knowledge with the information provided in 3.2.1, it is also possible determine that the version of Ubuntu is of the 10.04 LTS [4, 5]. It was also found that the system is part of a SMB/Windows workgroup with the name "WORKGROUP".

3.3 Vulnerability Scan

As mentioned in 3.2.1, the vulnerability scan revealed the version of many of the system's services and that they are outdated. With outdated software it is common that there are publicly known vulnerabilities and weaknesses. OpenVAS classifies the threats found in the vulnerability scan by severity, high, medium and low. In the performed particular scan there were six high threats, ten medium threats and one low threat.

In Apache Tomcat 6.0.24, the java servlet/web server, the vulnerability scan found two high risk and five medium risk vulnerabilities. These security risks include, but are not limited to, that potential attackers can gain access to sensitive data and cause denial-of-service.

OpenSSL, in this case used for secure retrieval of email, were found to have two high risk and two medium risk vulnerabilities. The most critical vulnerability is the possibility of man-in-the-middle attacks; a session can be hijacked or compromised.

Remaining security risks classified as medium threats were a denial-of-service vulnerability in the SMB server Samba, risk of information-disclosure by the OpenSSH server and one vulnerability related to giving away timestamps, which can potentially open the system for denial-of-service attacks.

One threat were classified as low risk, the DNS server bind. The issues related to system's version of bind is mostly related to availability issues, as in cause the DNS server to crash or denial-of-service.

4 Discussion

The first two scans, the ones carried out in section 2.1 and 2.2, yielded very little results, which is a good sign from a security perspective. The most basic entry points to the system is secure as shown in Table 1. This table displays that there were no uncommon ports in use, and those who were could be open for legitimate reasons.

The only item that the fingerprint scan raised as an issue was an outdated DNS–server software, as seen in Table 2, which in itself was not a great threat to the system. From this fingerprint scan we were not able to tell anything about the host operating system.

The vulnerability scan reported, contrary to the other two scans, a number of issues that needs to be addressed. The primary reason for the issues are based on outdated software, so in order to improve the system's security, software updates need to be preformed. OpenVAS raised six (6) high security risks, and ten (10) medium risks and all of them were based on old software and need to be tended to. For specific applications that needs updates, see Table 4.

Of the applications listed in Table 4, the highest priority are 'Tomcat' and 'OpenSSL' because they generate the threat level 'high' from OpenVAS. Dovecot does not generate any issues in OpenVAS, though it is known to have had security threats [6], so an update is recommended if it is as outdated as the rest of the systems software.

Table 4: Summary of vulnerability scan recommendations

Service Name	**Problems**	**Suggestions**
Dovecot	Unknown version	Check for update
Apache Tomcat 6.0.24	Outdated	Software update
Apache 2.2.14	Outdated	Software update
OpenSSL	Outdated	Software update
Samba 3.4.7	Outdated	Software update
OpenSSH 5.3p1	Outdated	Software update

5 Conclusion

Our conclusion of this OpenVAS scan is that the host “Rome” is not secure, because of outdated software. The host could be considered secure if the software were to be updated.

Our first recommendation to secure the host is to implement a routine for software updates and patches. A designated person should be appointed to make sure that the software update routine is followed through, if there are more than one person that administrates the host.

Our second recommendation is to upgrade the operating system. From the vulnerability scan we can conclude that the OS installed on the host is the 'Ubuntu 10.04 LTS' system, which by now is quite old. To make sure that the OS is up to date, a system upgrade should be performed, some months after a new 'Long Time Support' OS is released from the vendor.

References

[1] OpenVAS. *About OpenVAS*. 2015. URL: http://www.openvas.org/about.html (visited on 03/03/2015).

[2] Wikipedia. *Vulnerability scanner*. 2014. URL: http://en.wikipedia.org/wiki/Vulnerability_scanner (visited on 03/03/2015).

[3] The Government of the Hong Kong Special Administrative Region. *AN OVERVIEW OF VULNERABILITY SCANNERS*. 2008. URL: http://www.infosec.gov.hk/english/technical/files/vulnerability.pdf (visited on 03/03/2015).

[4] Canonical Ltd. *Software Packages in "lucid-updates", Subsection net*. 2015. URL: http://packages.ubuntu.com/en/lucid-updates/net/ (visited on 03/03/2015).

[5] E. K. Joseph. "Updates and Security for 10.04, 12.04, 12.10 and 13.10". In: *Ubuntu Weekly Newsletter* (361 2014). URL: https://wiki.ubuntu.com/UbuntuWeeklyNewsletter/Issue361 (visited on 03/03/2015).

[6] Canonical Ltd. *USN-2213-1: Dovecot vulnerability*. 2014. URL: http://www.ubuntu.com/usn/usn-2213-1/ (visited on 03/03/2015).

A Report from OpenVAS Vulnerability Scanning

Scan Report

February 26, 2015

Summary

This document reports on the results of an automatic security scan. The scan started at Thu Feb 26 22:57:18 2015 UTC and ended at Thu Feb 26 23:13:57 2015 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
192.168.1.10 (ROME)	Severity: High	6	10	1	53	0
Total: 1		6	10	1	53	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 70 results selected by the filtering described above. Before filtering there were 71 results.

2 Results per Host

2.1 192.168.1.10

Host scan start	Thu Feb 26 22:57:23 2015 UTC
Host scan end	Thu Feb 26 23:13:57 2015 UTC

Service (Port)	Threat Level
http-alt (8080/tcp)	High
imap (143/tcp)	High
imaps (993/tcp)	High
pop3 (110/tcp)	High
pop3s (995/tcp)	High
http-alt (8080/tcp)	Medium
pop3s (995/tcp)	Medium
general/tcp	Medium
http (80/tcp)	Medium
netbios-ssn (139/tcp)	Medium
ssh (22/tcp)	Medium
domain (53/udp)	Low
http-alt (8080/tcp)	Log
imap (143/tcp)	Log
imaps (993/tcp)	Log
pop3 (110/tcp)	Log
pop3s (995/tcp)	Log
general/tcp	Log
http (80/tcp)	Log
netbios-ssn (139/tcp)	Log

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
ssh (22/tcp)	Log
domain (53/udp)	Log
domain (53/tcp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/SMBClient	Log
general/icmp	Log
microsoft-ds (445/tcp)	Log
netbios-ns (137/udp)	Log

2.1.1 High http-alt (8080/tcp)

High (CVSS: 6.8)
NVT: Apache Tomcat servlet/JSP container default files

```
Default files, such as documentation, default Servlets and JSPs were found on
the Apache Tomcat servlet/JSP container.
Remove default files, example JSPs and Servlets from the Tomcat
Servlet/JSP container.
These files should be removed as they may help an attacker to guess the
exact version of Apache Tomcat which is running on this host and may provide
other useful information.
The following default files were found :
/examples/servlets/index.html
/examples/jsp/snp/snoop.jsp
/examples/jsp/index.html
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.12085

High (CVSS: 6.4)
NVT: Apache Tomcat 'Transfer-Encoding' Information Disclosure and Denial Of Service Vulnerabilities

Product detection result
```
cpe:/a:apache:tomcat:6.0.24
Detected by Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)
```

```
 Summary:
 Apache Tomcat is prone to multiple remote vulnerabilities including
information-disclosure and denial-of-service issues.
Remote attackers can exploit these issues to cause denial-of-service
```

... continues on next page ...

... continued from previous page ...

conditions or gain access to potentially sensitive information;
information obtained may lead to further attacks.
The following versions are affected:
Tomcat 5.5.0 to 5.5.29 Tomcat 6.0.0 to 6.0.27 Tomcat 7.0.0
Tomcat 3.x, 4.x, and 5.0.x may also be affected.
Solution:
The vendor released updates. Please see the references for more
information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100712

References
CVE: CVE-2010-2227
BID:41544
Other:
URL:https://www.securityfocus.com/bid/41544
URL:http://tomcat.apache.org/security-5.html
URL:http://tomcat.apache.org/security-6.html
URL:http://tomcat.apache.org/security-7.html
URL:http://tomcat.apache.org/
URL:http://www.securityfocus.com/archive/1/512272

[return to 192.168.1.10]

2.1.2 High imap (143/tcp)

High (CVSS: 6.8)
NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (STARTTLS Check)

OID of test routine: 1.3.6.1.4.1.25623.1.0.105043

References
CVE: CVE-2014-0224
BID:67899
Other:
URL:http://www.securityfocus.com/bid/67899
URL:http://openssl.org/

[return to 192.168.1.10]

2.1.3 High imaps (993/tcp)

High (CVSS: 6.8) NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability
OID of test routine: 1.3.6.1.4.1.25623.1.0.105042
References CVE: CVE-2014-0224 BID:67899 Other: URL:http://www.securityfocus.com/bid/67899 URL:http://openssl.org/

[return to 192.168.1.10]

2.1.4 High pop3 (110/tcp)

High (CVSS: 6.8) NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (STARTTLS Check)
OID of test routine: 1.3.6.1.4.1.25623.1.0.105043
References CVE: CVE-2014-0224 BID:67899 Other: URL:http://www.securityfocus.com/bid/67899 URL:http://openssl.org/

[return to 192.168.1.10]

2.1.5 High pop3s (995/tcp)

High (CVSS: 6.8) NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability
. . . continues on next page . . .

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.105042

References
CVE: CVE-2014-0224
BID:67899
Other:
URL:http://www.securityfocus.com/bid/67899
URL:http://openssl.org/

[return to 192.168.1.10]

2.1.6 Medium http-alt (8080/tcp)

Medium (CVSS: 4.3)
NVT: Apache Tomcat 'sort' and 'orderBy' Parameters Cross Site Scripting Vulnerabilities

Product detection result
cpe:/a:apache:tomcat:6.0.24
Detected by Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)

Summary:
Apache Tomcat is prone to multiple cross-site scripting
vulnerabilities because it fails to properly sanitize user-
supplied input.
An attacker may leverage these issues to execute arbitrary script code
in the browser of an unsuspecting user in the context of the affected
site. This may let the attacker steal cookie-based authentication
credentials and launch other attacks.
Solution:
Updates are available; please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103032

References
CVE: CVE-2010-4172
BID:45015
Other:
URL:https://www.securityfocus.com/bid/45015

... continues on next page ...

... continued from previous page ...

URL:http://tomcat.apache.org/security-6.html
URL:http://tomcat.apache.org/security-7.html
URL:http://tomcat.apache.org/security-6.html
URL:http://tomcat.apache.org/security-7.html
URL:http://jakarta.apache.org/tomcat/
URL:http://www.securityfocus.com/archive/1/514866

Medium (CVSS: 2.6)
NVT: Apache Tomcat Authentication Header Realm Name Information Disclosure Vulnerability

Product detection result
cpe:/a:apache:tomcat:6.0.24
Detected by Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)

Summary:
Apache Tomcat is prone to a remote information-disclosure
vulnerability.
Remote attackers can exploit this issue to obtain the host name or IP
address of the Tomcat server. Information harvested may lead to
further attacks.
The following versions are affected:
Tomcat 5.5.0 through 5.5.29 Tomcat 6.0.0 through 6.0.26
Tomcat 3.x, 4.0.x, and 5.0.x may also be affected.
Solution:
Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100598

References
CVE: CVE-2010-1157
BID:39635
Other:
URL:http://www.securityfocus.com/bid/39635
URL:http://tomcat.apache.org/security-5.html
URL:http://tomcat.apache.org/security-6.html
URL:http://tomcat.apache.org/
URL:http://svn.apache.org/viewvc?view=revision&revision=936540
URL:http://svn.apache.org/viewvc?view=revision&revision=936541
URL:http://www.securityfocus.com/archive/1/510879

Medium (CVSS: 2.6)
NVT: Apache Tomcat Security bypass vulnerability

Product detection result
cpe:/a:apache:tomcat:6.0.24
Detected by Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)

Summary:
This host is running Apache Tomcat server and is prone to security bypass vulnerability.
Vulnerability Insight:
The flaw is caused by 'realm name' in the 'WWW-Authenticate' HTTP header for 'BASIC' and 'DIGEST' authentication that might allow remote attackers to discover the server's hostname or IP address by sending a request for a resource.
Impact:
Remote attackers can exploit this issue to obtain the host name or IP address of the Tomcat server. Information harvested may aid in further attacks.
Impact Level: Application
Affected Software/OS:
Apache Tomcat version 5.5.0 to 5.5.29
Apache Tomcat version 6.0.0 to 6.0.26
Solution:
Upgrade to the latest version of Apache Tomcat 5.5.30 or 6.0.27 or later,
For updates refer to http://tomcat.apache.org

OID of test routine: 1.3.6.1.4.1.25623.1.0.901114

References
CVE: CVE-2010-1157
BID:39635
Other:
URL:http://tomcat.apache.org/security-5.html
URL:http://tomcat.apache.org/security-6.html
URL:http://www.securityfocus.com/archive/1/510879

[return to 192.168.1.10]

2.1.7 Medium pop3s (995/tcp)

Medium (CVSS: 4.3)
NVT: Check for SSL Weak Ciphers

... continues on next page ...

... continued from previous page ...

```
Weak ciphers offered by this service:
  SSL3_RSA_RC4_40_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_DES_40_CBC_SHA
  SSL3_EDH_RSA_DES_40_CBC_SHA
  SSL3_ADH_RC4_40_MD5
  SSL3_ADH_RC4_128_MD5
  SSL3_ADH_DES_40_CBC_SHA
  TLS1_RSA_RC4_40_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
  TLS1_RSA_RC2_40_MD5
  TLS1_RSA_DES_40_CBC_SHA
  TLS1_EDH_RSA_DES_40_CBC_SHA
  TLS1_ADH_RC4_40_MD5
  TLS1_ADH_RC4_128_MD5
  TLS1_ADH_DES_40_CBC_SHA
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103440

Medium (CVSS: 4.3)
NVT: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

OID of test routine: 1.3.6.1.4.1.25623.1.0.802087

References

```
CVE: CVE-2014-3566
BID:70574
Other:
  URL:http://osvdb.com/113251
   URL:https://www.openssl.org/~bodo/ssl-poodle.pdf
   URL:https://www.imperialviolet.org/2014/10/14/poodle.html
   URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
   URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit
↪ing-ssl-30.html
```

[return to 192.168.1.10]

2.1.8 Medium general/tcp

Medium (CVSS: 2.6)
NVT: TCP timestamps

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Paket 1: 720558107
Paket 2: 720558210
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80091

References

```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
```

[return to 192.168.1.10]

2.1.9 Medium http (80/tcp)

Medium (CVSS: 4.3)
NVT: Apache Web Server ETag Header Information Disclosure Weakness

```
Information that was gathered:
Inode: 152086
Size: 177
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103122

References

```
CVE: CVE-2003-1418
BID:6939
Other:
  URL:https://www.securityfocus.com/bid/6939
   URL:http://httpd.apache.org/docs/mod/core.html#fileetag
   URL:http://www.openbsd.org/errata32.html
   URL:http://support.novell.com/docs/Tids/Solutions/10090670.html
```

Medium (CVSS: 4.3)
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

```
Summary:
This host is running Apache HTTP Server and is prone to cookie
information disclosure vulnerability.
Vulnerability Insight:
The flaw is due to an error within the default error response for
status code 400 when no custom ErrorDocument is configured, which can be
exploited to expose 'httpOnly' cookies.
Impact:
Successful exploitation will allow attackers to obtain sensitive information
that may aid in further attacks.
Impact Level: Application
Affected Software/OS:
Apache HTTP Server versions 2.2.0 through 2.2.21
Solution:
Upgrade to Apache HTTP Server version 2.2.22 or later,
For updates refer to http://httpd.apache.org/
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.902830

References

```
CVE: CVE-2012-0053
BID:51706
Other:
  URL:http://osvdb.org/78556
   URL:http://secunia.com/advisories/47779
   URL:http://www.exploit-db.com/exploits/18442
   URL:http://rhn.redhat.com/errata/RHSA-2012-0128.html
   URL:http://httpd.apache.org/security/vulnerabilities_22.html
   URL:http://svn.apache.org/viewvc?view=revision&amp;revision=1235454
   URL:http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm
↪l
```

[return to 192.168.1.10]

2.1.10 Medium netbios-ssn (139/tcp)

Medium (CVSS: 5.0)
NVT: Samba Multiple Remote Denial of Service Vulnerabilities

```
Summary:
Samba is prone to multiple remote denial-of-service vulnerabilities.
```

... continues on next page ...

... continued from previous page ...

An attacker can exploit these issues to crash the application, denying
service to legitimate users.
Versions prior to Samba 3.4.8 and 3.5.2 are vulnerable.
Solution:
Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100644

References

CVE: CVE-2010-1635
BID:40097
Other:
URL:http://www.securityfocus.com/bid/40097
URL:https://bugzilla.samba.org/show_bug.cgi?id=7254
URL:http://samba.org/samba/history/samba-3.4.8.html
URL:http://samba.org/samba/history/samba-3.5.2.html
URL:http://www.samba.org

[return to 192.168.1.10]

2.1.11 Medium ssh (22/tcp)

Medium (CVSS: 3.5)
NVT: openssh-server Forced Command Handling Information Disclosure Vulnerability

According to its banner, the version of OpenSSH installed on the remote
host is older than 5.7:
ssh-2.0-openssh_5.3p1 debian-3ubuntu7

OID of test routine: 1.3.6.1.4.1.25623.1.0.103503

References

CVE: CVE-2012-0814
BID:51702
Other:
URL:http://www.securityfocus.com/bid/51702
URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445
URL:http://packages.debian.org/squeeze/openssh-server
URL:https://downloads.avaya.com/css/P8/documents/100161262

[return to 192.168.1.10]

2.1.12 Low domain (53/udp)

Low (CVSS: 5.0)
NVT: Determine which version of BIND name daemon is running

```
BIND 'NAMED' is an open-source DNS server from ISC.org.
Many proprietary DNS servers are based on BIND source code.
The BIND based NAMED servers (or DNS servers) allow remote users
to query for version and type information.  The query of the CHAOS
TXT record 'version.bind', will typically prompt the server to send
the information back to the querying source.
The remote bind version is : 9.7.0-P1
Solution :
Using the 'version' directive in the 'options' section will block
the 'version.bind' query, but it will not log such attempts.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10028

[return to 192.168.1.10]

2.1.13 Log http-alt (8080/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: HTTP Server type and version

```
The remote web server type is :
Apache-Coyote/1.1
and the 'ServerTokens' directive is ProductOnly
Apache does not permit to hide the server type.
```

. . . continues on next page . . .

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.10107

Log (CVSS: 0.0)
NVT: Services

```
A web server is running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: Web mirroring

```
The following CGI have been discovered :
Syntax : cginame (arguments [default value])
/examples/servlets/servlet/RequestParamExample (firstname [] lastname [] )
/examples/jsp/jsp2/el/implicit-objects.jsp (foo [bar] )
/examples/jsp/jsp2/el/functions.jsp (foo [JSP+2.0] )
/examples/servlets/servlet/CookieExample (cookiename [] cookievalue [] )
/examples/servlets/servlet/SessionExample;jsessionid=0EF89E75F6776AF767786E3F789
↪B7B54 (dataname [] datavalue [] )
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10662

Log (CVSS: 0.0)
NVT: Directory Scanner

```
The following directories were discovered:
/docs, /examples
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
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11032

References

```
Other:
  OWASP:OWASP-CM-006
```

Log (CVSS: 0.0)
NVT: Apache Tomcat Version Detection

```
Detected Apache Tomcat version: 6.0.24
Location: 8080/tcp
CPE: cpe:/a:apache:tomcat:6.0.24
Concluded from version identification result:
Apache Tomcat/6.0.24
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.800371

Log (CVSS: 0.0)
NVT: wapiti (NASL wrapper)

```
wapiti could not be found in your system path.
OpenVAS was unable to execute wapiti and to perform the scan you
requested.
Please make sure that wapiti is installed and that wapiti is
available in the PATH variable defined for your environment.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80110

[return to 192.168.1.10]

2.1.14 Log imap (143/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Services

```
An IMAP server is running on this port
```

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: IMAP STARTTLS Detection

```
Summary:
The remote IMAP Server supports the STARTTLS command.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.105007

Log (CVSS: 0.0)
NVT: IMAP Banner

```
The remote imap server banner is :
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS L
↪OGINDISABLED] Dovecot ready.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11414

[return to 192.168.1.10]

2.1.15 Log imaps (993/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Services

```
A TLSv1 server answered on this port
```

... continues on next page ...

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: Services

```
An IMAP server is running on this port through SSL
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: IMAP Banner

```
The remote imap server banner is :
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE AUTH=PLAIN
↪] Dovecot ready.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11414

Log (CVSS: 0.0)
NVT: SSL Certificate Expiry

```
The SSL certificate of the remote service is valid between
2014-12-04 15:16:06 GMT and 2015-12-04 15:16:06 GMT.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.15901

[return to 192.168.1.10]

2.1.16 Log pop3 (110/tcp)

Log
NVT:

```
Open port.
```

. . . continues on next page . . .

... continued from previous page ...

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Services

```
A pop3 server is running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: POP3 STARTTLS Detection

```
Summary:
The remote POP3 Server supports the STARTTLS command.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.105008

[return to 192.168.1.10]

2.1.17 Log pop3s (995/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Services

```
A TLSv1 server answered on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: Services

```
A pop3 server is running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: SSL Certificate Expiry

```
The SSL certificate of the remote service is valid between
2014-12-04 15:16:06 GMT and 2015-12-04 15:16:06 GMT.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.15901

Log (CVSS: 0.0)
NVT: Check for SSL Ciphers

```
Service supports SSLv2 ciphers.
Service supports SSLv3 ciphers.
Service supports TLSv1 ciphers.
Medium ciphers offered by this service:
  SSL3_RSA_DES_192_CBC3_SHA
  SSL3_EDH_RSA_DES_192_CBC3_SHA
  SSL3_ADH_DES_192_CBC_SHA
  SSL3_DHE_RSA_WITH_AES_128_SHA
  SSL3_ADH_WITH_AES_128_SHA
  TLS1_RSA_DES_192_CBC3_SHA
  TLS1_EDH_RSA_DES_192_CBC3_SHA
  TLS1_ADH_DES_192_CBC_SHA
  TLS1_DHE_RSA_WITH_AES_128_SHA
  TLS1_ADH_WITH_AES_128_SHA
Weak ciphers offered by this service:
  SSL3_RSA_RC4_40_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_DES_40_CBC_SHA
  SSL3_EDH_RSA_DES_40_CBC_SHA
  SSL3_ADH_RC4_40_MD5
  SSL3_ADH_RC4_128_MD5
  SSL3_ADH_DES_40_CBC_SHA
```

. . . continues on next page . . .

... continued from previous page ...

```
  TLS1_RSA_RC4_40_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
  TLS1_RSA_RC2_40_MD5
  TLS1_RSA_DES_40_CBC_SHA
  TLS1_EDH_RSA_DES_40_CBC_SHA
  TLS1_ADH_RC4_40_MD5
  TLS1_ADH_RC4_128_MD5
  TLS1_ADH_DES_40_CBC_SHA
No non-ciphers are supported by this service
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.802067

Log (CVSS: 0.0)
NVT: Check for SSL Medium Ciphers

```
Medium ciphers offered by this service:
  SSL3_RSA_DES_192_CBC3_SHA
  SSL3_EDH_RSA_DES_192_CBC3_SHA
  SSL3_ADH_DES_192_CBC_SHA
  SSL3_DHE_RSA_WITH_AES_128_SHA
  SSL3_ADH_WITH_AES_128_SHA
  TLS1_RSA_DES_192_CBC3_SHA
  TLS1_EDH_RSA_DES_192_CBC3_SHA
  TLS1_ADH_DES_192_CBC_SHA
  TLS1_DHE_RSA_WITH_AES_128_SHA
  TLS1_ADH_WITH_AES_128_SHA
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.902816

[return to 192.168.1.10]

2.1.18 Log general/tcp

Log (CVSS: 0.0)
NVT: OS fingerprinting

```
ICMP based OS fingerprint results: (100% confidence)
Linux Kernel
```

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.102002

References
Other:
URL:http://www.phrack.org/issues.html?issue=57&id=7#article

Log (CVSS: 0.0)
NVT: DIRB (NASL wrapper)

```
DIRB could not be found in your system path.
OpenVAS was unable to execute DIRB and to perform the scan you
requested.
Please make sure that DIRB is installed and is
available in the PATH variable defined for your environment.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103079

Log (CVSS: 0.0)
NVT: Checks for open udp ports

```
Open UDP ports: [None found]
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103978

Log (CVSS: 0.0)
NVT: arachni (NASL wrapper)

```
Arachni could not be found in your system path.
OpenVAS was unable to execute Arachni and to perform the scan you
requested.
Please make sure that Arachni is installed and that arachni is
available in the PATH variable defined for your environment.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.110001

Log (CVSS: 0.0)
NVT: Nikto (NASL wrapper)

```
Nikto could not be found in your system path.
OpenVAS was unable to execute Nikto and to perform the scan you
requested.
Please make sure that Nikto is installed and that nikto.pl or nikto is
available in the PATH variable defined for your environment.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.14260

Log (CVSS: 0.0)
NVT: Traceroute

```
Here is the route from 192.168.1.1 to 192.168.1.10:
192.168.1.1
192.168.1.10
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.51662

Log (CVSS: 0.0)
NVT: Checks for open tcp ports

```
Open TCP ports: 80, 110, 445, 993, 22, 8080, 995, 139, 53, 143
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900239

[return to 192.168.1.10]

2.1.19 Log http (80/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: HTTP Server type and version

```
The remote web server type is :
Apache/2.2.14 (Ubuntu)
Solution : You can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10107

Log (CVSS: 0.0)
NVT: Services

```
A web server is running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: Directory Scanner

```
The following directories were discovered:
/cgi-bin, /icons
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
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11032

References

```
Other:
  OWASP:OWASP-CM-006
```

Log (CVSS: 0.0)
NVT: wapiti (NASL wrapper)

```
wapiti could not be found in your system path.
OpenVAS was unable to execute wapiti and to perform the scan you
requested.
```

... continues on next page ...

... continued from previous page ...

```
Please make sure that wapiti is installed and that wapiti is
available in the PATH variable defined for your environment.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80110

Log (CVSS: 0.0)
NVT: Apache Web ServerVersion Detection

```
Detected Apache version: 2.2.14
Location: 80/tcp
CPE: cpe:/a:apache:http_server:2.2.14
Concluded from version identification result:
Server: Apache/2.2.14
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900498

[return to 192.168.1.10]

2.1.20 Log netbios-ssn (139/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 192.168.1.10]

2.1.21 Log ssh (22/tcp)

Log
NVT:

```
Open port.
```

... continues on next page ...

. . . continued from previous page . . .

OID of test routine: 0

Log (CVSS: 0.0)
NVT: SSH Protocol Versions Supported

```
The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0
SSHv2 Fingerprint: 0c:d8:26:b3:dd:f0:d4:83:57:95:78:f8:5a:0c:ae:53
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100259

Log (CVSS: 0.0)
NVT: SSH Server type and version

```
Detected SSH server version: SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7
Remote SSH supported authentication: publickey,password
Remote SSH banner:
(not available)
CPE: cpe:/a:openbsd:openssh:5.3p1
Concluded from remote connection attempt with credentials:
  Login: OpenVAS
  Password: OpenVAS
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10267

Log (CVSS: 0.0)
NVT: Services

```
An ssh server is running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

[return to 192.168.1.10]

2.1.22 Log domain (53/udp)

Log (CVSS: 0.0)
NVT: DNS Server Detection

```
 Summary:
 A DNS Server is running at this Host.
A Name Server translates domain names into IP addresses. This makes it
possible for a user to access a website by typing in the domain name instead of
the website's actual IP address.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100069

[return to 192.168.1.10]

2.1.23 Log domain (53/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Identify unknown services with nmap

```
Nmap service detection result for this port: domain
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 192.168.1.10]

2.1.24 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

```
192.168.1.10|cpe:/a:samba:samba:3.4.7
192.168.1.10|cpe:/a:apache:tomcat:6.0.24
```

. . . continues on next page . . .

... continued from previous page ...

```
192.168.1.10|cpe:/a:apache:http_server:2.2.14
192.168.1.10|cpe:/a:openbsd:openssh:5.3p1
192.168.1.10|cpe:/o:canonical:ubuntu_linux
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810002

[return to 192.168.1.10]

2.1.25 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

```
traceroute:192.168.1.1,192.168.1.10
TCP ports:80,110,445,993,22,8080,995,139,53,143
UDP ports:
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810003

[return to 192.168.1.10]

2.1.26 Log general/SMBClient

Log (CVSS: 0.0)
NVT: SMB Test

```
The tool "smbclient" is not available for openvasd.
Therefore none of the tests using smbclient are executed.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.90011

[return to 192.168.1.10]

2.1.27 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

```
 Summary:
 The remote host responded to an ICMP timestamp request. The Timestamp Reply is
an ICMP message which replies to a Timestamp message. It consists of the
originating timestamp sent by the sender of the Timestamp as well as a receive
timestamp and a transmit timestamp. This information could theoretically be used
to exploit weak time-based random number generators in other services.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103190

References

```
CVE: CVE-1999-0524
Other:
  URL:http://www.ietf.org/rfc/rfc0792.txt
```

[return to 192.168.1.10]

2.1.28 Log microsoft-ds (445/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

```
 Summary:
 It is possible to extract OS, domain and SMB server information
from the Session Setup AndX Response packet which is generated
during NTLM authentication.Detected SMB workgroup: WORKGROUP
Detected SMB server: Samba 3.4.7
Detected OS: Unix
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.102011

[return to 192.168.1.10]

2.1.29 Log netbios-ns (137/udp)

Log (CVSS: 0.0)
NVT: Using NetBIOS to retrieve information from a Windows host

```
The following 5 NetBIOS names have been gathered :
 ROME            = This is the computer name registered for workstation services
↪ by a WINS client.
 ROME            = This is the current logged in user registered for this workst
↪ation.
 ROME            = Computer name
 WORKGROUP       = Workgroup / Domain name (part of the Browser elections)
 WORKGROUP       = Workgroup / Domain name
. This SMB server seems to be a SAMBA server (this is not a security
risk, this is for your information). This can be told because this server
claims to have a null MAC address
If you do not want to allow everyone to find the NetBios name
of your computer, you should filter incoming traffic to this port.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10150

[return to 192.168.1.10]