Vulnerability Scanning with OpenVAS

Laboratory report in
EDA263/DIT641 Computer Security

Francesca Ponzetta
Lucas Norman

Group Number: 15

Chalmers University of Technology
Gothenburg, Sweden 2015
Version no.: 1.0
February 19, 2020

1. Introduction

Almost every device that we use nowadays is connected to the internet, which means that the network has a central role in our life because it is at the bases of our work, of our study and also of our free time. As a consequence, malicious people have started to exploit the internet network in order to access information from other people or to use this information in a bad way. Strong protection against this kind of threats has become necessary, and one of the best ways of protecting our systems and our devices is to configure them properly.

Analyzing other systems can help in understanding what are the most common issues to be avoided, that's why specific tools can be used to scan and to report information about systems, networks, servers and web applications.

In this report, the information collected by a vulnerability scanning on the Chalmers laboratory network is reported and analyzed. The scanning has been performed using OpenVAS. Section 2 of this report contains a brief description of openVAS and the way it has been used in order to perform the analysis. Section 3 contains the results collected by the scanning and section 4 contains a discussion about the collected results. Finally, the report is summarized in a conclusion in section 5.

2. Description of OpenVAS setup

OpenVAS is a vulnerability scanner. It is used to scan a system in order to collect information about the services running in that system, the ports used by those services and the security issues that may be caused by those services. This is done by running multiple NVTs (Network Vulnerability Tests).
When you set up openVAS you may decide to run all the NVTs, in order to find all the vulnerabilities of the system, or you may decide to perform a scan focusing on some specific vulnerabilities by selecting which NVTs you want to run. OpenVAS allows scanning networks, servers and web applications.
Once the scanning has finished, the results are delivered as a report. Here it is possible to get information about the running services, their version, their vulnerabilities and some suggestions about how to remove those vulnerabilities [1].

In order to perform a scan, openVAS should be properly configured. In particular, the following steps should be followed:

- Connect to the openVAS client
- Create a **new target** (specifying the IP address of the system you want to scan)
- Create the **scan configuration profile** (where you can select which type of scan you want to perform)
- Create a **new task**
- Start the task and wait for the scan to be completed, then check the scanning report.

Figure 1 shows the setup of a network that has been scanned by openVAS: the openVAS server is in the middle between the network to be scanned and our client.

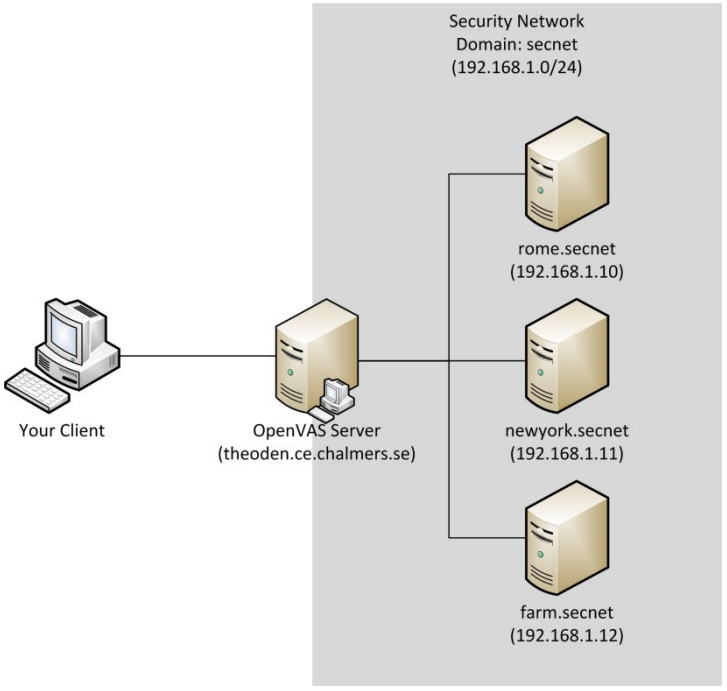

Figure 1: The network setup

The procedure that we followed to scan the laboratory network follows three steps:

- **Port scanning**
- **Service fingerprint**
- **Vulnerability scanning**.

2.1 Port scanning

The goal of this first scan is to understand what ports are opened. A port is considered open if there are services running on it. It is important to perform port scanning to become aware of which ports are active and find which services are run on these ports. These services, which rely on the Internet to receive/send packets, can have vulnerabilities and can be exploited to attack the system.

The port scanning was performed selecting the **openVAS default port list**, which contains some well-known ports where the most common services run (like HTTP, IMAP, POP, SSH and Microsoft-ds) and selecting only the **port scanners NVTs**, in order to run only the tests that allow discovering the open ports.

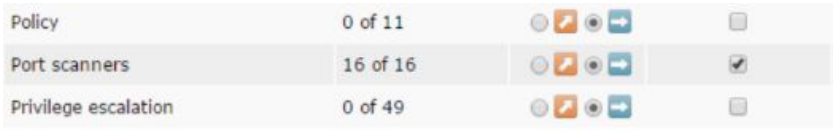

Figure 2: Port scanner SVT selection

2.2 Service fingerprinting

Once the open ports are detected, it is necessary to get more information about the services running on these ports and on the system. This information is provided by the fingerprint of each service, and particular attention should be given to the version of the services because some versions present vulnerabilities that may be targeted by the attackers.

It is useful to focus in particular on services like telnet and SSH (that allows connecting to remote computer), SMTP (that allows sending/receive emails) and www (that allows communicating over the internet), because if they have vulnerabilities they are the first services to be exploited in order to access the system.

2.2.1 Service fingerprinting

For the fingerprint, we have performed a second type of scanning selecting first only the NVTs against the suggested services. As we couldn't find information about the version of these services, we have run another task selecting all the NVTs from the *service detection* and *general* groups.

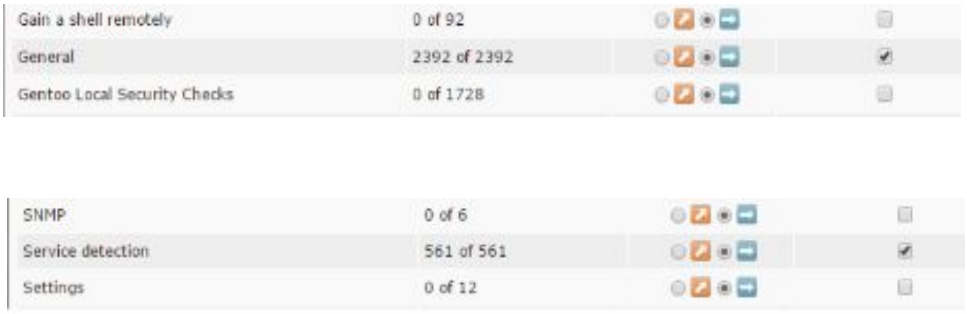

Figure 3: Selection of general NVTs and Service detection NVTs

2.2.2 Remote host fingerprinting

The results provided by the scan have been analyzed better in order to gain more information about the services and the way they reveal information about the remote computer and what information is revealed.

2.3 Vulnerability scanning

The goal of this last step is to discover the potential vulnerabilities of the services running in the system. We have performed a full vulnerability scan by selecting all the NVTs available.

3. Results

The scans revealed several open ports on the network that were using mostly common services as can be seen in Table 1. None of them is an immediate threat but many of them are outdated and have different issues with them. Some of them might also be unused and should, in that case, be disabled, it depends on which services are needed for the host.

The result in the fingerprint scan shown in Table 2 only discovered one service however the full vulnerability scan in Table 3 yielded more results and discovered more information about the different services and the versions of them.

3.1 Port scanning results

The port scan revealed the open ports and the types of services run on them shown in Table 1, all of these are common services that are usually safe. There are two services that are used for file sharing on the operative system Windows, if the server does not use this operative system it is recommended to disable these. The other services are responsible for mail handling, web traffic, and secure connection to remote computers.

Table 1: Information about open ports

Port number	Service name	Service task	Suggestions
53	Domain	Domain Name System	Keep
80	HTTP	Hypertext Transfer protocol used for web traffic	Keep
8080	HTTP-alt	HTTP alternative	Keep
143	IMAP	Internet Mail Access Protocol used for mail services	Keep unless there are safer mail protocols
993	IMAPS	IMAP-SSL	Keep
445	Microsoft-ds	Used for file sharing	Keep if the server relies on file sharing
139	Netbios-ssn	Used for File and print sharing	Keep if configured properly, otherwise disable
110	POP3	Post Office Protocol 3 Used for mail services	Keep, unless there are safer mail protocols
995	POP3S	POP3-SSL	Keep
22	SSH	Secure Shell	Keep

3.2 Fingerprinting results

3.2.1 Service fingerprinting

The result that was discovered from the service fingerprint scan reported only one service that can be seen in Table 2. This service is a DNS server that is responsible for translating domain names into IP addresses. This lets a user access a website by typing in the name of the website instead of its IP address. The type of the DNS server is called BIND (Berkeley Internet Name Domain) which is the most commonly used today and the version of it is 9.7.0-P1.

Table 2: Service fingerprint

Service	Version
Domain Name System (DNS)	9.7.0-P1

3.2.2 Remote host fingerprinting

As the fingerprint scan only discovered one service it wasn't possible to gather much information from that, however, the full vulnerability scan gave out more information regarding the system as a whole. Several services give information about the operating system being Linux-based and the SSH service even leaks information about the exact version of the operating system in its banner. By finding out that the current version of the SSH server is SSH-2.0-OpenSSH_5.3p1 it is possible to find out that the version of the operating system is Linux Ubuntu 10.04.3.

By also looking at the scan results for the Samba SMB server it is possible to find out the workgroup the computer belongs to, which is a shared Windows/Linux workgroup named "WORKGROUP" and also the name of the computer which is "ROME".

3.3 Vulnerability scanning results

From the vulnerability scanning we have found out more information about the services running; these results are listed in Table 3. All of the different services seen in the table are outdated in some way and need to be updated to newer versions.

Apache Tomcat is a servlet/JSP container server used for handling the lifecycle of servlets and processing requests regarding them. The version (6.0.24) using the port is an outdated version with vulnerabilities and needs to be updated.

The Apache HTTP server is a remote web server used for the Ubuntu operating system with the purpose to deliver web content over the internet in a secure manner. The version used on this port (2.2.14) is outdated and needs to be updated to protect vulnerabilities.

Dovecot is an open software POP3 & IMAP server that is used for UNIX - based operating systems. Its main purpose is as a mail storage server but it can also be used to forward connections to other servers or retrieve mail on remote servers. The version of the service could not be found during the scan and it is recommended to check for updates for it to be on the safe side.

Samba is an SMB (Server Message Block) server used to share files and printers between computers in a network. Samba is open software and is commonly used in a Linux/Unix system to share files and printers in a Windows network. The version used is 3.4.7 and is outdated.

SSH (Secure Shell) is a protocol used to safely connect to other computers over the internet or on a network. The current version has information disclosure issues and needs to be updated.

Table 3: Vulnerability scan

Service	Version
http-alt: servlet/JSP container	**Apache Tomcat:** version 6.0.24
HTTP server	**Apache:** version 2.2.14 (ubuntu)
Mail server	**Dovecot**
SMB server	**samba**: 3.4.7
SSH server	SSH-2.0-OpenSSH_5.3p1

4. Discussion

The first scan performed (the port scan) revealed the most commonly used services in almost every system. Although some issues were found in the services running on those ports, these issues can be fixed by properly updating the services, without the need to disable them.

The second scan performed was about reading the fingerprint of the services running on these ports. The only issue found was related to the DNS server, but in this case as well, it doesn't represent a big threat to the system. Looking at the report provided by openVAS, no additional information about the operating system is provided by the services.

Reading the report of the vulnerability scan we have detected several issues. Among the services, different vulnerabilities can be exploited to perform DoS attacks or to gain information about the system. To see a summarized version of the threats, read Table 4.

The vulnerabilities found can be divided into 3 threat levels:

- **High threat**: for the Apache Tomcat the issue is related to information disclosure. This was caused by the default files remaining in the servlet container which could give attackers sensitive information about the system, which could lead to further attacks. As a solution to this problem, these files should be removed. In addition, the current version of the Tomcat can be exploited for a DoS attack and further information disclosure, so an update to a newer version would be required.

  Concerning the mail services, like IMAP(S) and POP3(S), they can be exploited to perform Man In The Middle security bypass. In particular earlier versions of OpenSSL did not properly restrict the processing of ChangeChiperSpec messages, causing MITM and consequently message hijacking to obtain sensitive information [2]. An update of OpenSSL is required to solve these problems.

- **Medium threat:** The current version of Apache Tomcat is vulnerable to several issues. First of all to cross-site scripting caused by improper sanitization of the user inputs. The attacker could exploit these issues to execute arbitrary script code in the browser of an unsuspecting user, steal cookie-based authentication credentials and perform other attacks. The second issue is related to a security bypass vulnerability caused by "realm name" in the "WWW-Authenticate" HTTP header for "BASIC" and "Digest" authentication. When the attacker sends a request for a resource, he could obtain the hostname and the IP address of the server and use them to perform further attacks. An update is required.

  Another issue regarding the mail services used, in this case, IMAPs and POP3s, is that they are using weak ciphers which causes an information vulnerability issue. The solution to this is to change the configurations for this service so it no longer supports the weak ciphers anymore.

  The Apache HTTP server has both an issue with information disclosure from its packages banner and from an error in handling its cookies. The fault in the cookie handling is caused by an error in the default error handling, specifically for the error response to the status code 400 when no custom ErrorDocument is configured. Successful exploitation of these issues can give the attacker sensitive information that may help the attacker in further attacks. To solve this vulnerability, an update to version 2.2.22 or later is required.

The SMB server used for file sharing is vulnerable to multiple remote DoS vulnerabilities that the attacker could use to crash the application. An update is required.

The OpenSSH server is vulnerable to a forced command handling information disclosure. The attacker could receive sensitive information from its banner. An update is required.

- **Low threat:** the DNS server used is a BIND based name server that allows remote users to query for version and type information. As a solution, it would be necessary to use the 'version' directive in the "option" section to block the "version.bind" query.

Table 4: Summary of vulnerability scan recommendations

Service name	Problems	Suggestions
Apache Tomcat 6.0.24	**High threat:** Default files can disclose sensitive information, DoS issues **Medium Threat:** Cross-site scripting vulnerabilities caused by improper sanitization of user input.	Remove default files, update the Apache Tomcat to the latest version.
Apache 2.2.14	**Medium threat:** Information disclosure caused by improper cookie handling	Upgrade the Apache HTTP server to 2.2.22 version or later
OpenSSL	**High threat:** -IMAP/IMAPS/POP3/ POP3S vulnerable to MITM security Bypass Vulnerability. **Medium threat:** IMAPS/POP3S: weak ciphers	-Update to a newer version -Use protocols with stronger ciphers
SMB server	**Medium threat:** vulnerable to multiple remote DoS attacks	Upgrade Samba to a later version than 3.5.2
SSH server	**Medium threat:** Information disclosure vulnerability	Update to a newer version, need to be version 5.7 or higher.
BIND DNS server	**Low threat:** Information disclosure regarding version and type information.	By using the "version" directive in the "options" section the queries about the sensitive information will be blocked.

Dovecot	**Issue:** Unknown version	Check for updates

5. Conclusions

In conclusion, it has been determined that the current state of this computer is not secure, however, updating all the necessary services could lead to it being seen as secure.

For the future a good strategy to ensure its security would be keeping the services up to date with a regular frequency, it would also be good to keep track of the different services regularly and disabling the ones that are not being used.

From the vulnerabilities in the system, we determined that the current operating system was the Linux Ubuntu 10.04.3 which is a very old version of Ubuntu, so a recommendation is updating the operating system to the latest version and then keeping track of the new versions and updating to them more frequently in the future to ensure a safer system.

A suggestion would be to design a to-do list and assign a person to do all the tasks on the list once every decided period (once every month could be suitable).

References:

[1] OpenVAS. *About OpenVAS*. URL: https://www.openvas.org/about.html (visited 21-02-18).

[2] SecuritySpace. *Vulnerability Search. URL: http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.105043* (visited 21-02-19)

Appendix: OpenVAS Vulnerability scan report

Scan Report

February 12, 2021

Summary

This document reports on the results of an automatic security scan. The scan started at Fri Feb 12 12:35:06 2021 UTC and ended at Fri Feb 12 12:53:32 2021 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.secnet)	Severity: High	6	14	1	60	0
Total: 1		6	14	1	60	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 81 results selected by the filtering described above. Before filtering there were 82 results.

2 Results per Host

2.1 192.168.1.10

Host scan start Fri Feb 12 12:35:12 2021 UTC
Host scan end Fri Feb 12 12:53:31 2021 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
imaps (993/tcp)	Medium
pop3s (995/tcp)	Medium
general/tcp	Medium
http (80/tcp)	Medium
netbios-ssn (139/tcp)	Medium
ssh (22/tcp)	Medium
domain (53/tcp)	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

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
netbios-ssn (139/tcp)	Log
ssh (22/tcp)	Log
domain (53/tcp)	Log
domain (53/udp)	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.
```

... continues on next page ...

... continued from previous page ...

Remote attackers can exploit these issues to cause denial-of-service 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

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

...continues on next page ...

... continued from previous page ...

Other:
URL:https://www.securityfocus.com/bid/45015
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 imaps (993/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
```

Medium (CVSS: 0.0)
NVT: SSL Certificate Expiry

```
The SSL certificate of the remote service expired 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]

2.1.8 Medium pop3s (995/tcp)

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

```
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

. . . continues on next page . . .

... continued from previous page ...

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
```

Medium (CVSS: 0.0)
NVT: SSL Certificate Expiry

```
The SSL certificate of the remote service expired 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]

2.1.9 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: 213725466
Paket 2: 213725569
```

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]

2.1.10 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

...continues on next page ...

... continued from previous page ...

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]

2.1.11 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.
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]

2.1.12 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]

2.1.13 Low domain (53/tcp)

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]

2.1.14 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.
```

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=1D8473EB3388897CD87E8396143
↪5C1ED (dataname [] datavalue [] )
```

. . . continues on next page . . .

... continued from previous page ...

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.
```

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.80110

[return to 192.168.1.10]

2.1.15 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
```

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.
```

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.11414

[return to 192.168.1.10]

2.1.16 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
```

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.
```

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.11414

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
  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]

2.1.17 Log pop3 (110/tcp)

Log
NVT:

```
Open port.
```

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:
```

...continues on next page ...

... continued from previous page ...

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]

2.1.18 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: Check for SSL Ciphers

Service supports SSLv2 ciphers.
Service supports SSLv3 ciphers.
Service supports TLSv1 ciphers.

... continues on next page ...

... continued from previous page ...

```
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
  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
```

... continues on next page ...

... continued from previous page ...

```
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]

2.1.19 Log general/tcp

Log (CVSS: 0.0)
NVT: OS fingerprinting

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

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&amp;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]
```

... continues on next page ...

... continued from previous page ...

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: Microsoft SMB Signing Disabled

```
SMB signing is disabled on this host
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.802726

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]

2.1.20 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.
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
```

...continues on next page ...

... continued from previous page ...

```
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]

2.1.21 Log netbios-ssn (139/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: SMB on port 445

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.11011

[return to 192.168.1.10]

2.1.22 Log ssh (22/tcp)

Log
NVT:

```
Open port.
```

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]

2.1.23 Log domain (53/tcp)

Log
NVT:

```
Open port.
```

...continues on next page ...

... continued from previous page ...

OID of test routine: 0

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]

2.1.24 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]

2.1.25 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

```
192.168.1.10|cpe:/a:samba:samba:3.4.7
```

... continues on next page ...

... continued from previous page ...

```
192.168.1.10|cpe:/a:apache:tomcat:6.0.24
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]

2.1.26 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]

2.1.27 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]

2.1.28 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]

2.1.29 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

Log (CVSS: 0.0)
NVT: SMB log in

```
It was possible to log into the remote host using the SMB protocol.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10394

Log (CVSS: 0.0)
NVT: SMB on port 445

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.11011

Log (CVSS: 0.0)
NVT: SMB Brute Force Logins With Default Credentials

```
It was possible to log into the remote host using the SMB protocol.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.804449

Log (CVSS: 0.0)
NVT: SMB Brute Force Logins With Default Credentials

```
It was possible to log into the remote host using the SMB protocol.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.804449

Log (CVSS: 0.0)
NVT: Microsoft Windows SMB Accessible Shares

```
The following shares where found
IPC$
```

. . . continues on next page . . .

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.902425

[return to 192.168.1.10]

2.1.30 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]