

Vulnerability Scanning with OpenVAS

Laboratory Report in EDA263 Computer Security

Olof Magnusson
Yu Husan Liao

Group 51

Version no: 1

August 11, 2025

Contents

1	Introduction	1
2	Description of OpenVAS Setup	2
2.1	Port Scanning	3
2.1.1	Service Fingerprinting	4
2.1.2	Remote Host Fingerprinting	5
2.2	Vulnerability Scanning	5
3	Results	7
3.1	Port Scanning	7
3.2	Fingerprinting	7
3.2.1	Services	7
3.2.2	Remote Host	7
3.3	Vulnerability Scan	8
4	Discussion	11
5	Conclusion	12
	References	13
A	Report from OpenVAS Vulnerability Scanning	15

1 Introduction

The role of technology represents a vital part of our human lives. Considering the technological change concerning the earlier years of computers, we face new challenges to overcome in protecting digital information. Security concerns the protection against malicious intent in different ways. That concludes methods to achieve confidentiality, integrity, authentication, and non-repudiation in the communication protocol. To protect against malicious intent, we need to take security into consideration when implementing systems.

This report will investigate how OpenVAS, a vulnerability scanning tool, could help scan systems for vulnerabilities of TravelBiscuit AB Company. The purpose of this report is to analyze the company's current status regarding security and improve the business more securely.

The report structure is as follows; Section 2 will describe how the OpenVAS works and the useful properties, a more detailed explanation of what scanning is, and the specific setup for this particular scan. Section 3 will provide the result from the port scanning findings; Section 4 will discuss methods to improve security and a comparison of recommendations. Finally, in Section 5, we will provide a conclusion regarding the findings.

2 Description of OpenVAS Setup

OpenVAS - Open Vulnerability Assessment Scanner is an architecture built upon many different capabilities such as unauthenticated testing, authenticated testing. Thus, the architecture integrates multiple services and tools (57.000 plugins) to perform a vulnerability scan to catch more sophisticated security errors [1]. Some examples of features could be checking network services on a target system for vulnerable ports that should not be open or fingerprinting the host to analyse which operating system is running. Other examples are to discover exploits for buffer overflow, man-in-the-middle and malware. OpenVAS classifies threats in different severity levels from high to low risk based on the Common Vulnerability Scoring System (CVSS) [2]. The high (red) indicates critical vulnerabilities in the system, such as multiple security vulnerabilities in Apache, Man-in-the-middle vulnerabilities in OpenSSL. The medium (yellow) severity level could provide both critical and non-critical security vulnerabilities. Some examples could be header information disclosure weakness, weak SSL ciphers, and some non-critical could be TCP timestamps. The low (blue) severity level could provide some small errors such that the DNS server bind allows for remote users to query for version and type information. However, these must be carefully checked (medium and low), although they could turn into critical vulnerabilities. Figure 1 can visualise the setup of this project. Thus, we are remotely interconnected to the OpenVAS server through our desktop client, where the host target is *rome.secnet*.

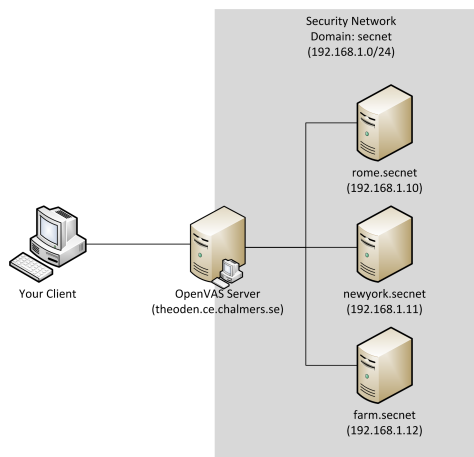


Figure 1: The laboratory network setup

Scanning a specific host is a reconnaissance technique primarily used to diagnose the connectivity on which ports are open (sending packets to the host) on a system and could be viewed as an entry point to a more powerful attack [3]. There are 65535 different and usable port numbers and are labelled as $1, \dots, 65535$, but all the ports are not necessary to be scanned in most cases. It is instead a smarter way to understand what the standard ports are used in the system and perform a specified port sweep. Thus, fewer resources

need to be used to find a successful result. For our report, we have given the task to find out vulnerabilities of the IP address: 192.168.1.10. By analysing the system using a port-scanning technique, the result of the scan could end up in three different ways:

1. Open or accepted
2. Filtered, Dropped or Blocked
3. Closed or denied or Not Listening

The most common ports such as HTTP (80), HTTPS (443), POP3 (110), IMAP (143), SSH(22) are ports that we use for our daily tasks. For example, this could be used accessing websites (both plaintext and encrypted), communicating through email and accessing the remote system through SSH. These are open and accepted ports for users to access (i.e. the port responds to the requests). Filtered ports could be that ports are not listening to inbound traffic due to firewall policy to create a more isolated environment. FTP (20,21) is a closed or denied protocol since it is an insecure protocol that does not provide encryption with data distribution. Telnet (23) is also a legacy protocol that was used for remote connection. These two protocols are closed or denied or not Listening will not even respond to requests on these ports [4].

However, in our case with the OpenVAS, the scans can be categorised into three domains: port scan, service fingerprinting, and network vulnerability scanning. With our result, we hope that we can gather enough information about the systems architecture to determine measures that are needed to implement a more secure system. There are certain things that we need to take into consideration before doing the scans. We need to find a good scanning model that does not take so many resources for the users (and the other groups), and that can be completed in a reasonable time. Therefore, we choose to use *OpenVAS Default*, which covers the most commonly used ports in a system.

2.1 Port Scanning

For port scanning, there were already a set of tests predefined in the OpenVAS. Firstly, we need to create our scan configuration and choose which task we want to perform. One configuration in regards to Port Scanning can be visualised in Figure 2.

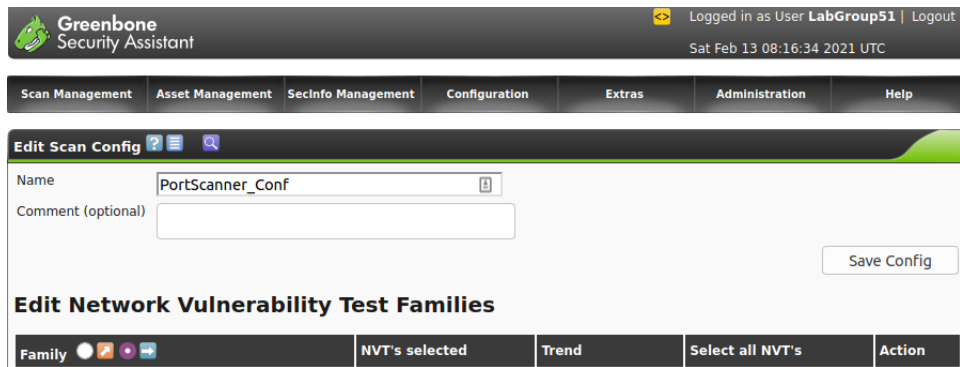


Figure 2: Setup configuration in the Network Vulnerability Test (NVT)

In our case, we want to perform port scanning. The Network Vulnerability Test (NVT) family can be visualised in Figure 3 and the tests were used in order to find open ports on the target host.

Port scanners	0 of 16	<input type="radio"/>	<input checked="" type="checkbox"/>	
Privilege escalation	0 of 49	<input type="radio"/>	<input type="checkbox"/>	
Product detection	0 of 395	<input type="radio"/>	<input type="checkbox"/>	

Figure 3: Port Scanners in Network Vulnerability Test (NVT)

2.1.1 Service Fingerprinting

To analyse which services are currently running on the system, we need to create a new configuration to gain information. Therefore, we choose service detection and useless services in such a way we can detect all the services currently running. This can be visualised in Figure 4

Service detection	0 of 561	<input type="radio"/>	<input checked="" type="checkbox"/>	
Settings	0 of 12	<input type="radio"/>	<input type="checkbox"/>	
Slackware Local Security Checks	0 of 534	<input type="radio"/>	<input type="checkbox"/>	
Solaris Local Security Checks	0 of 898	<input type="radio"/>	<input type="checkbox"/>	
SuSE Local Security Checks	0 of 1510	<input type="radio"/>	<input type="checkbox"/>	
Ubuntu Local Security Checks	0 of 2195	<input type="radio"/>	<input type="checkbox"/>	
Useless services	0 of 13	<input type="radio"/>	<input checked="" type="checkbox"/>	

Figure 4: Service detection and useless services in NVT

To get a wider hit-ratio, we choose to include Port scanners in the configuration Figure 5. (This was recommended by Wisam).



Port scanners	0 of 16	<input type="radio"/>   	<input checked="" type="checkbox"/>	
Privilege escalation	0 of 49	<input type="radio"/>   	<input type="checkbox"/>	
Product detection	0 of 395	<input type="radio"/>   	<input type="checkbox"/>	

Figure 5: Port Scanners in NVT

And in order to not miss any important, we choose to enable General family in NVT Figure 6.




General	0 of 2392	<input type="radio"/>   	<input checked="" type="checkbox"/>	
Gentoo Local Security Checks	0 of 1728	<input type="radio"/>   	<input type="checkbox"/>	



Figure 6: General family in NVT


2.1.2 Remote Host Fingerprinting

With remote host fingerprinting, we are trying to discover which operating system the host is using. In particular, the architecture is important, since we could base our penetration testing on that extracted information.

2.2 Vulnerability Scanning

Vulnerability scanning can be performed in several ways. Firstly, we can use the configuration *full and fast*, *Full and fast ultimate*, *Full and very deep*, *Full and very deep ultimate* and our own created configurations. An example of *full and very deep ultimate* test is visualised in Figure 7. Although not recommended, this one takes much resources and takes a long time before getting a result. Thats why it is important to narrow the tests to the purpose of the task.

New Task ?  

Name 

Comment (optional)

Scan Config

Scan Targets

Alerts (optional)

Schedule (optional)

Slave (optional)

Observers (optional)

Add results to Asset Management ☒ yes ☐ no

Scan Intensity

Maximum concurrently executed NVTs per host

Maximum concurrently scanned hosts

Figure 7: Full test

3 Results

3.1 Port Scanning

While running the test, we find the following information in Table 1. Nothing that can be considered deviant from the normal were found.

Table 1: Information about open ports

Port Number	Service Name	Service Task	Suggestions
53	DNS	Domain Name System	Keep
80	TCP	Transmission Control Protocol	Keep
8080	http-alt	HTTP Alternate to port 80	Keep
143/993	IMAP	Internet message access protocol	Keep
445	Microsoft-ds	Server Message Block	Keep
139	netbios-ssn	Datagram distribution service	Keep
110/995	pop3/pop3s	Post Office Protocol	Keep
22	SSH	Secure Shell	Keep

3.2 Fingerprinting

From the scan, we discovered that the remote server type running an Ubuntu as its operating system.

3.2.1 Services

Table 2: Service fingerprint

Service	Version
DNS-server	9.7.0-P1
Apache	apache:tomcat:6.0.24
HTTP	Apache/2.2.14 (Ubuntu)
SSH	ssh-2.0-openssh_5.3p1
SMB	Samba 3.4.7
SMTP	Dovecot

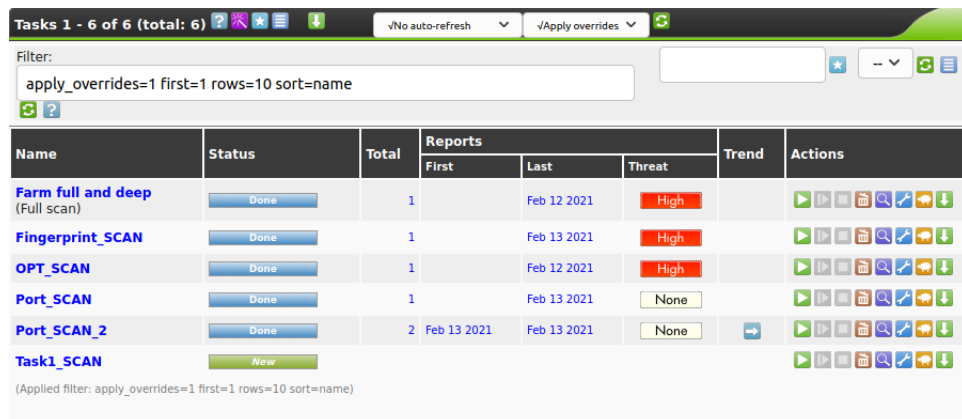
3.2.2 Remote Host

From analysing the data, we found the following information: the operating system was classified by ICMP based OS fingerprint by 91% confidence to be a Linux Kernel. Thus,

looking deeper into the log file, we could see that the operating system was the Linux distribution Ubuntu. To be precise with the specific version, we need to understand the information in Table 2. The DNS-server provides valuable information about the version since 9.7.0-P1 was used in the Ubuntu 10.04 LTS version [5]. Another interesting found was that we detected a SMB workgroup: WORKGROUP.

3.3 Vulnerability Scan

Following previous tests with OpenVAS, we know the systems have many vulnerabilities that needs to be fixed. With outdated software, some errors and bugs could provides weakness in the protocol. One of them is the outdated apache server of version 2.2.15. Thus, with Vulnerability Scan, OpenVAS classify vulnerability results from high to low and provide alerts for potential threats to the user. Different scans that was performed are visualised in Figure 8.



Name	Status	Total	Reports			Trend	Actions
			First	Last	Threat		
Farm full and deep (Full scan)	Done	1		Feb 12 2021	High		[Icons]
Fingerprint_SCAN	Done	1		Feb 13 2021	High		[Icons]
OPT_SCAN	Done	1		Feb 12 2021	High		[Icons]
Port_SCAN	Done	1		Feb 13 2021	None		[Icons]
Port_SCAN_2	Done	2	Feb 13 2021	Feb 13 2021	None	[Icon]	[Icons]
Task1_SCAN	New						[Icons]

(Applied filter: apply_overrides=1 first=1 rows=10 sort=name)

Figure 8: Different tests that can be used: from general to specific scanning

An overview of Farm full and deep scan (Full Scan) is visualised in Figure 9. The results show that there are 5 High risks, 11 Medium risks and 2 Low risks.

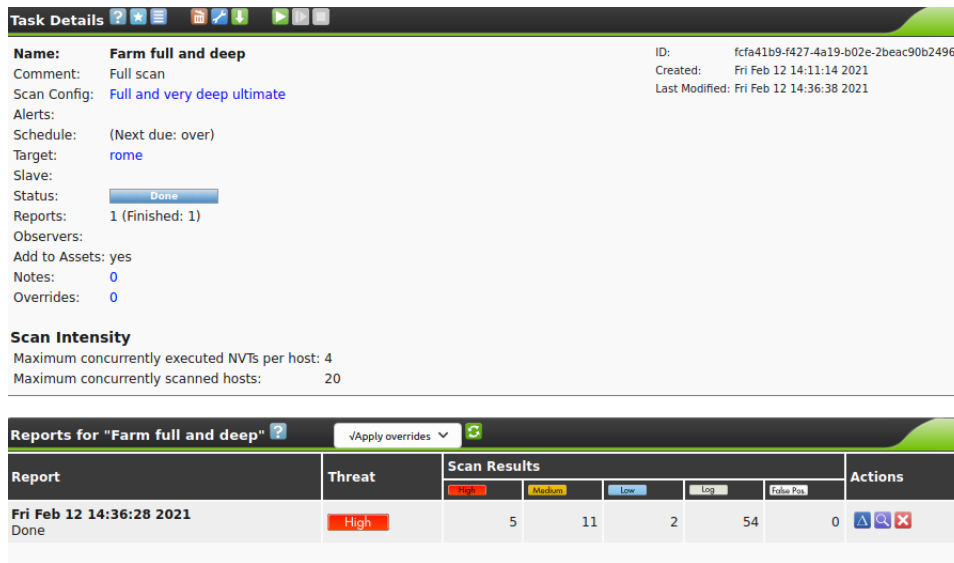


Figure 9: Farm full and deep (computational intensive) to get a overview of the system

Also, an overview of FingerprintScan is visualised in Figure 10 showing that the systems have 2 High risks, 3 Medium risks and 1 Low risk.

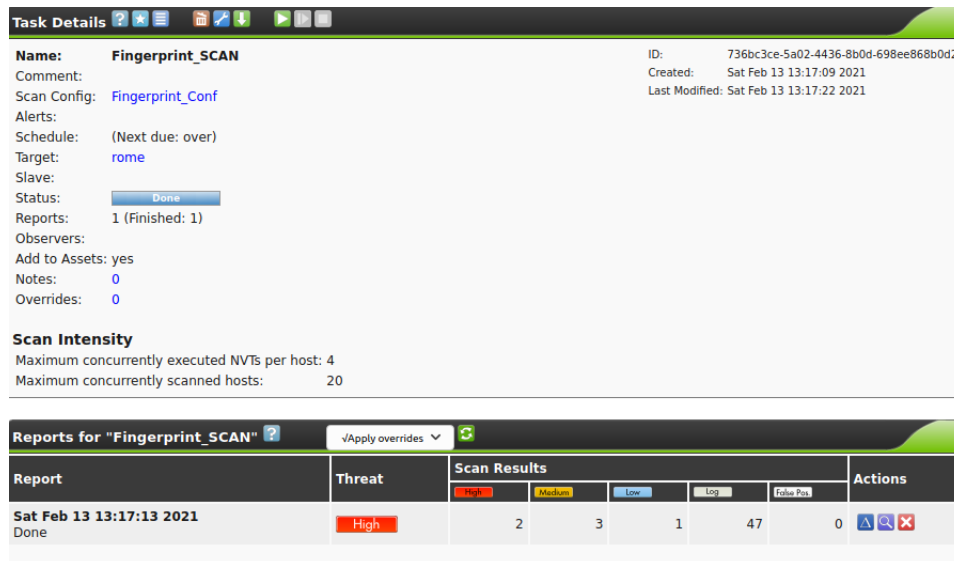


Figure 10: Fingerprint scan used to collect information about the host

As we discussed previously, Apache is prone to multiple vulnerabilities. There are seven risk vulnerabilities associated with this protocol, where two are marked as High and five as Medium. These issues open up for more information to disclose or attacks. For example, Apache HTTP Server is prone to cookie information disclosure. Thus it is vital

to fix those issues as soon as possible. In OpenSSL, we found four risk vulnerabilities marked as High and five marked as Medium. The most dangerous threat in OpenSSL is the Man-in-the-middle bypass vulnerabilities, thus successfully exploiting this issue to disclose sensitive information. The remaining threats such as TCP timestamps, CBC ciphers Information Disclosure Vulnerability, Samba Multiple Remote Denial of Service Vulnerabilities could provide openings for a denial of service attack. We only discovered one that was classified as a low threat, and that was the DNS server bind which allows for remote users to query for version and type information. This is mainly related to the Denial-of-service attack, where a rogue actor potentially can make the server crash by exhausting the service by sending requests.

4 Discussion

We found several vulnerabilities and therefore recommended some actions listed in Table 3. The fingerprint and port-scan provided little results, a good indicator from a security point of view. These results indicate that the open ports are not vulnerable to exploits if they are not misconfigured. Furthermore, it is essential to create port policies such that a rogue user cannot overload the services. This needs to be done at the application level. The fingerprint that the system raised was an outdated DNS server that is not a massive threat to a system. However, we recommend updating this before it could end up with vulnerabilities since it is not up-to-date with the current version. OpenVAS raised several vulnerabilities when we did perform the vulnerability scan – six risks was classified as red and nine as yellow. These are critical issues and needs to be fixed as soon as possible. From our analysis, we discovered that these issues primarily derive from outdated software, as can be seen in Table 3. Furthermore, we did not find any Dovecot version, but after some research the information we got was: `OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS LOGINDISABLED] Dovecot ready`. Dovecot does not introduce any errors or alerts in the OpenVAS, but since most of the system is not up to date, we can conclude that it is neither up to date. The Dovecot is known to have vulnerabilities in its previous versions [6]. Hence, we suggest to update that version as soon as possible.

Table 3: Summary of vulnerability scan recommendations

Service Name	Problems	Suggestions
Dovecot	Unknown version	Update
Apache Tomcat 6.0.24	Legacy version	Update
Apache 2.2.14	Legacy version	Update to 2.2.22 or later
OpenSSL	Legacy version	Update
Samba 3.4.7	Legacy version	Update to 3.4.8 or 3.5.2
OpenSSH 5.3pl	Legacy version	Update

5 Conclusion

The host Rome has significant vulnerabilities that need to be addressed. The first recommendation is always to be up-to-date with software, and there are two primary reasons for that. Firstly, companies are sorting out bugs and vulnerabilities by releasing new software versions to mitigate information disclosure. Secondly, the companies release beneficial updates to the system, i.e., make the application runs faster or binary compatibilities to implement new functionalities. Another problem we found was that the system was running Ubuntu 10.04 LTS version. Hence, we highly recommend that the company hire one or two individuals who have experience in this field and monitor and maintain the system daily. Also, implementing security policies is an integral part of building better systems. It consists of standardized documenting, security awareness training for employees, frequent security meetings, and specifying a hardware-software mapping to provide a clear picture of the network in the company. Moreover, it is utterly important since this is an industry where things happen very quickly, and it is essential to have an incident response system to the actions. With these things in considerations seen in Table 4, the company can create security models to develop a more secure system. Finally, we would like to thank TravelBiscuit AB, which has given us this project, and we look forward to discussing the solutions in more detail in person.

Table 4: Summary of the things to be taken into consideration in order to improve security in TravelBiscuit

Recommendations
Update software
Monitor and maintain OS system
Implement security policies
Build a incident response system

References

- [1] *OpenVAS - Open Vulnerability Assessment Scanner*. URL: <https://www.openvas.org/>.
- [2] *Common Vulnerability Scoring System (CVSS)*. URL: <https://nvd.nist.gov/vuln-metrics/cvss#>.
- [3] M. De Vivo, E. Carrasco, G. Isern, and G. O. de Vivo. “A review of port scanning techniques”. In: *ACM SIGCOMM Computer Communication Review* 29.2 (1999), pp. 41–48.
- [4] *Are open ports a security risk?* URL: <https://lifars.com/2020/10/are-open-ports-a-security-risk/> (visited on 02/10/2021).
- [5] *USN-1910-1: Bind vulnerability*. URL: <https://ubuntu.com/security/notices/USN-1910-1> (visited on 02/13/2021).
- [6] *Dovecot Vulnerabilites*. URL: https://www.cvedetails.com/vulnerability-list/vendor_id-6485/Dovecot.html (visited on 02/17/2021).

A Report from OpenVAS Vulnerability Scanning

Scan Report

February 19, 2021

Summary

This document reports on the results of an automatic security scan. The scan started at Fri Feb 12 14:36:37 2021 UTC and ended at Fri Feb 12 14:59:26 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	2
2	Results per Host	2
2.1	192.168.1.10	2
2.1.1	High http (80/tcp)	3
2.1.2	High imap (143/tcp)	3
2.1.3	High imaps (993/tcp)	4
2.1.4	High pop3 (110/tcp)	4
2.1.5	High pop3s (995/tcp)	5
2.1.6	Medium http (80/tcp)	5
2.1.7	Medium imaps (993/tcp)	7
2.1.8	Medium pop3s (995/tcp)	8
2.1.9	Medium general/tcp	9
2.1.10	Medium netbios-ssn (139/tcp)	10
2.1.11	Medium ssh (22/tcp)	10
2.1.12	Low domain (53/tcp)	11
2.1.13	Low general/icmp	11
2.1.14	Log http (80/tcp)	12
2.1.15	Log imap (143/tcp)	14
2.1.16	Log imaps (993/tcp)	14
2.1.17	Log pop3 (110/tcp)	17
2.1.18	Log pop3s (995/tcp)	17
2.1.19	Log general/tcp	19

2.1.20	Log netbios-ssn (139/tcp)	22
2.1.21	Log ssh (22/tcp)	22
2.1.22	Log domain (53/tcp)	23
2.1.23	Log general/icmp	24
2.1.24	Log domain (53/udp)	25
2.1.25	Log general/CPE-T	25
2.1.26	Log general/HOST-T	25
2.1.27	Log general/SMBClient	26
2.1.28	Log microsoft-ds (445/tcp)	26
2.1.29	Log netbios-ns (137/udp)	28

1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
192.168.1.10 (rome.secnnet)	Severity: High	5	11	2	54	0
Total: 1		5	11	2	54	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 72 results selected by the filtering described above. Before filtering there were 73 results.

2 Results per Host

2.1 192.168.1.10

Host scan start Fri Feb 12 14:36:44 2021 UTC

Host scan end Fri Feb 12 14:59:26 2021 UTC

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

... (continues) ...

... (continued) ...

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

2.1.1 High http (80/tcp)

High (CVSS: 10.0)
NVT: Apache Multiple Security Vulnerabilities

Summary:

Apache is prone to multiple vulnerabilities.
These issues may lead to information disclosure or other attacks.
Apache versions prior to 2.2.15 are affected.

Solution:

Upgrade to Apache 2.2.15 or Later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100514

References

CVE: CVE-2010-0425, CVE-2010-0434, CVE-2010-0408, CVE-2007-6750

BID: 38494, 38491

Other:

URL: <http://www.securityfocus.com/bid/38494>

URL: http://httpd.apache.org/security/vulnerabilities_22.html

URL: <http://httpd.apache.org/>

URL: https://issues.apache.org/bugzilla/show_bug.cgi?id=48359

URL: <http://svn.apache.org/viewvc?view=revision&revision=917870>

[\[return to 192.168.1.10 \]](#)

2.1.2 High imap (143/tcp)

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

... continues on next page ...

...continued from previous page ...
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
...continues on next page ...

...continued from previous page ...

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 (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

... continues on next page ...

...continued from previous page ...

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.htmlURL:<http://svn.apache.org/viewvc?view=revision&revision=1235454>URL:<http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm>

↩1

[\[return to 192.168.1.10 \]](#)

2.1.7 Medium imaps (993/tcp)

Medium (CVSS: 4.3) NVT: Check for SSL Weak Ciphers
<p>Weak ciphers offered by this service:</p> <ul style="list-style-type: none">SSL3_RSA_RC4_40_MD5SSL3_RSA_RC4_128_MD5SSL3_RSA_RC4_128_SHASSL3_RSA_RC2_40_MD5SSL3_RSA_DES_40_CBC_SHASSL3_EDH_RSA_DES_40_CBC_SHASSL3_ADH_RC4_40_MD5SSL3_ADH_RC4_128_MD5SSL3_ADH_DES_40_CBC_SHATLS1_RSA_RC4_40_MD5TLS1_RSA_RC4_128_MD5TLS1_RSA_RC4_128_SHATLS1_RSA_RC2_40_MD5TLS1_RSA_DES_40_CBC_SHATLS1_EDH_RSA_DES_40_CBC_SHATLS1_ADH_RC4_40_MD5TLS1_ADH_RC4_128_MD5TLS1_ADH_DES_40_CBC_SHA <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.103440</p>

Medium (CVSS: 4.3) NVT: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability
<p>OID of test routine: 1.3.6.1.4.1.25623.1.0.802087</p>
<p>References CVE: CVE-2014-3566 BID: 70574 Other: URL: http://osvdb.com/113251 URL: https://www.openssl.org/~bodo/ssl-poodle.pdf</p>
... continues on next page ...

...continued from previous page ...

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
<p>OID of test routine: 1.3.6.1.4.1.25623.1.0.802087</p>
<p>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</p>

Medium (CVSS: 0.0) NVT: SSL Certificate Expiry
<p>The SSL certificate of the remote service expired 2015-12-04 15:16:06 GMT!</p>
<p>OID of test routine: 1.3.6.1.4.1.25623.1.0.15901</p>

[\[return to 192.168.1.10 \]](#)

2.1.9 Medium general/tcp

Medium (CVSS: 2.6) NVT: TCP timestamps
<p>It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 214463776 Paket 2: 214463878</p>
<p>OID of test routine: 1.3.6.1.4.1.25623.1.0.80091</p>
<p>... continues on next page ...</p>

...continued from previous page ...

References**Other:**URL:<http://www.ietf.org/rfc/rfc1323.txt>[\[return to 192.168.1.10 \]](#)**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. 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=7254URL:<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:

...continues on next page ...

<p>...continued from previous page ...</p> <p>ssh-2.0-openssh_5.3p1 debian-3ubuntu7</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.103503</p>
<p>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</p>

[\[return to 192.168.1.10 \]](#)

2.1.12 Low domain (53/tcp)

<p>Low (CVSS: 5.0) NVT: Determine which version of BIND name daemon is running</p>
<p>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.</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.10028</p>

[\[return to 192.168.1.10 \]](#)

2.1.13 Low general/icmp

<p>Low (CVSS: 0.0) NVT: Record route</p>
<p>...continues on next page ...</p>

...continued from previous page ...

Here is the route recorded between 192.168.1.1 and 192.168.1.10 :
192.168.1.10.
192.168.1.10.

OID of test routine: 1.3.6.1.4.1.25623.1.0.12264

[\[return to 192.168.1.10 \]](#)

2.1.14 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

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

[\[return to 192.168.1.10 \]](#)

2.1.15 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.
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.

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.

...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

[\[return to 192.168.1.10 \]](#)

2.1.17 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:
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.

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:

...continues on next page ...

...continued from previous page ...

```

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

[\[return to 192.168.1.10 \]](#)

2.1.19 Log general/tcp

Log (CVSS: 7.8)
NVT: 3com switch2hub

Fake IP address not specified. Skipping this check.

OID of test routine: 1.3.6.1.4.1.25623.1.0.80103

Log (CVSS: 0.0)
NVT: OS fingerprinting

ICMP based OS fingerprint results: (91% 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&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: 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, 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 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

[\[return to 192.168.1.10 \]](#)

2.1.21 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

[\[return to 192.168.1.10 \]](#)

2.1.22 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

[\[return to 192.168.1.10 \]](#)

2.1.23 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>

[\[return to 192.168.1.10 \]](#)

2.1.24 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
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:80,110,445,993,22,995,139,53,143
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
<p>The tool "smbclient" is not available for openvasd. Therefore none of the tests using smbclient are executed.</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.90011</p>

[\[return to 192.168.1.10 \]](#)

2.1.28 Log microsoft-ds (445/tcp)

Log NVT:
<p>Open port.</p> <p>OID of test routine: 0</p>

Log (CVSS: 0.0) NVT: SMB NativeLanMan
<p>Summary:</p> <p>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</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.102011</p>

Log (CVSS: 0.0) NVT: SMB log in
... continues on next page ...

...continued from previous page ...

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\$

OID of test routine: 1.3.6.1.4.1.25623.1.0.902425

[\[return to 192.168.1.10 \]](#)

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

[\[return to 192.168.1.10 \]](#)