Vulnerability Scanning with OpenVAS

Laboratory Report in EDA263/DAT641 Computer Security

Dominique Komander
Simon Weber

Group 44

Version no: 0

February 18, 2018

Contents

1 Introduction

The third Assignment of the course DIT641GU Computer Security is about vulnerability scanning. For this the OpenVAS vulnerability scanning tool is used. With this tool it is possible to get information about the system and the used software on the one hand, but also known security issues for the used software on the other hand. Therefore it is a good tool to measure the security of a setup.

This elaboration will firstly describe the OpenVAS tool and its functionality. Then the test-network will be described briefly to give the reader an overview over the setup. Moreover the single steps of the vulnerability analysis will be described in section two. Section three will describe the results of the analysis. The order of steps will be the same as in section two, so the inclined reader is able to jump between the sections to directly view the findings of a step. In the last section the findings will be discussed and a conclusion of the assignment will be drawn. The appendix at the end of the elaboration will contain the vulnerability scan report automatically generated by OpenVAS.

2 Description of OpenVAS Setup

OpenVAS (Open Vulnerability Assessment System) is a combination of different services and tools. Together these tools are a good solution for vulnerability scanning and vulnerability management.

The scanner is supported by daily updated NVTs (Network Vulnerability Tests). Meanwhile there are over 50000. All components are free and under GNU General Public License (GNU GPL). The user interface is either a web-browser, a desktop-application or a CLI. All these interfaces use the same backend services [1]. If vulnerabilities are found, OpenVAS supports with helpful descriptions and links to further details. Scans are repeatable and planable. Additionally OpenVAS offers an alert function, if a thread is found.

The laboratory network setup was the following and can also be seen in Figure 1: The student connects to the OpenVAS-client (on theoden.ce.chalmers.se). The Greenbone Security Assistant there will manage requests from the student and redirect them to the right endpoint in the /24 subnet security network with the domain secnet. This network has three sub-domains: rome.secnet (192.168.1.10), newyork.secnet (192.168.1.11) and farm.secnet (192.168.1.12). Each student had to choose one of the hosts as target. We have chosen farm.secnet for our scans.

Following we will describe the used methods to determine the security of the remote host farm.secnet.

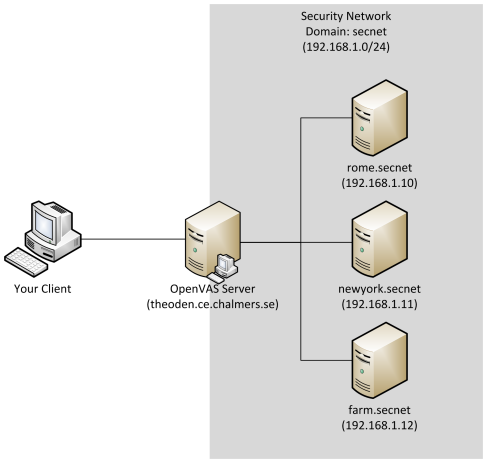

Figure 1: The laboratory network setup

2.1 Port Scanning

At first we scanned the host for open ports. Scanning is a useful method to find out if applications listen on ports and which ones are listening. This is necessary, because open ports may imply weaknesses because they are gateways to the system.

The first 1024 ports are called well-known ports, the ports from 1024-49151 are called User Ports and the last ports are called Dynamic Ports [2]. The most standard services are associated with the well-known ports. For example webbrowsers mostly try to connect to web servers using port 80, if they want to send a http request. Still most ports are not connected to a special service, protocol or application and can therefore be chosen freely. Thats why an automatic port scan is so helpful. One could also do the scanning by hand but since there are 65535 possibly open ports, using a port scanner is a handy method.

The proceeding of the scanning for open ports is quite easy: The scanner sends a request to every port and writes down which ports responded. The aim is to get an overview which ports are open and might be interesting for a deeper search. For this assignment we used the OpenVAS default port list, that scans 4481 of often used ports [1].

2.2 Fingerprinting

Fingerprinting is the next step of the analysis. After we got the information which ports are open we looked at the response and tried to find out which services and applications could be listening on the open ports. This is called Service Fingerprinting.

2.2.1 Service Fingerprinting

Based on the port number and the "Service Name and Transport Protocol Port Number Registry" [3] we were able to make a first guess, what we would find, if a given port is open. For example it is likely, that, if port 22 is open, we will find a application based on the Secure Shell Protocol [3]. The next step is to look at the respond to validate the guess or to gather more information. Every application answers in a different way. After finding out which service is running on the port, the next step is to figure out more about this service. Especially the version of an application is of interest, because known vulnerabilities are always associated with a software version. As soon as the developers get the information of a vulnerability in their software, they will most likely start and fix the security breach. As soon as they fix it, they will release a new version of their product. But if an old version of the software is still running on the tested web server, the vulnerability will probably still be there. Therefore it is the aim in this step, to get to know as much information about the running service including especially the running version. Here again one can look at the given response. Many applications do not only respond the kind of service, but also divulge the information of their version number [4].

2.2.2 Remote Host Fingerprinting

The next step in the analysis is to get to know as much from the host as possible. As described in the last section, many security breaches are equally dependent on the OS version. Furthermore an attacker might need the information of the system, to adjust the shell code he needs to apply after he managed to abused a vulnerability in a software. Sometimes the attacker has only one possibility, because some demons will crash at a failed attempt.

To gain the wanted knowledge about the system, it is necessary to combine the prior results.

2.3 Vulnerability Scanning

Now the real vulnerability scanning takes place. Outgoing from the previously gathered results, it is now possible to check, how vulnerable the system is. As mentioned OpenVAS has many sources that will tell us about known vulnerabilities for the running applications and their versions. The remaining NVTs can be seen as a big database with vulnerabilities in the software and the versions. That means that after OpenVAS found out the above mentioned information, it will search in the database for known vulnerabilities for exactly the version of the services, that are actually running. Then it goes another step further and tries with simple methods to abuse these vulnerabilities. The aim is to find automatically as many vulnerabilities of the host as possible. In the end, OpenVAS produces a report with the found problems and advisory how to deal with them.

The benefits besides the simplicity of the use of OpenVAS are on the one hand the possibility of early detection and on the other hand the advantage that it provides in security management and tracking.

3 Results

In this section we describe the results of the scanning. As said in section two, we will go through the findings in the same way we presented the single steps there.

3.1 Port Scanning

As mentioned before, we focused our research on the host farm.secnet. The OpenVAS port scan revealed 24 ports open in the scanned area. These ports can be seen in Table 1.

Table 1: Information about open ports

Port Number	**Service Name**	**Service Task**	**Suggestions**
21	ftp	File transfer protocol	keep
22	ssh	SSH	keep
23	telnet	Telnet	disable
25	smtp	Simple Mail Transfer Protocol	keep
53	domain	Domain Name System	keep
80	http	hypertext transfer protocol	keep
111	sunrpc	SUN Remote Procedure Call	keep
139	netbios-ssn	NETBIOS Session Service	keep
445	microsoft-ds	Microsoft Directory Services	keep
512	exec	remote process execution	disable
513	login	remote login	disable
514	shell	Remote Shell	disable
1099	rmiregistry	Java Remote Object Registry	keep
1524	ingreslock	ingres database	disable
2049	nfs	Network File System	keep
2121	scientia-ssdb	SCIENTIA-SSDB	keep
3306	mysql	MySQL	keep
3632	distcc	distributed compiler	disable
5432	postgresql	PostgreSQL	keep
5900	vnc	Virtual Network Computing	keep
6000	x11	X Window System	keep
6667	ircd	internet relay chat	keep
8009	ajp13	forgotten tomcat port?	disable
8787	msgsrvr	Message Server	keep

3.2 Fingerprinting

Through the portnumber and the given response we were able to make a good guess, which software would be behind a given port. Therefore we used the Service Name and Transport Protocol Port Number Registry [3]. Our guesses can be seen in Table 1 in column three. Just through the information of the process name and the open port we were able to identify some applications and thereby ports, that should not be used anymore. For example this is telnet on port 23. Then there are exec, rsh, remote login and ssh. They mostly do the same thing, but for exec it is recommended to uninstall it and to use rsh instead. Meanwhile for rsh it is recommended to use ssh instead. Also login is called deprecated and one should use ssh instead. Therefore exec, remote login and rsh are not necessary and a possible vulnerability to the server. Furthermore there is ingreslock, that is sometimes used as a backdoor and should be disabled therefore. Then there is ajp13 on port 8009 running. There are some articles about it, that it is the "forgotten tomcat port" and might be disabled as well. [5]

3.2.1 Services

In Table 2 you can find information about some chosen discovered services. On port 21 and 2121 are two different ftp clients running. On port 21 it is vsFTPd in version 2.3.4 and on port 2121 it is ProFTPD in version 1.3.1 On port 22 it seems like there is OpenSSH in version 4.7p1 running. On port 23 we found telnet, but we were not able to find a version number. That does not matter at all, because, as we will see later, it is recommended to turn telnet off no matter what version is running. On port 25 we probably found an SMTP server. OpenSSH said, that it is probably Postfix, but could not name a version. And on port 80 an Apache Server with the version 2.2.8 is listening. PHP is installed in version 5.2.4.

Table 2: Service fingerprint

Service	**Version**
Telnet	no information
FTP	ProFTPD 1.3.1 on Port 2121
	vsFTPd 2.3.4 on Port 21
SSH	SSH-2.0-OpenSSH_4.7p1
	Debian-8ubuntu1
SMTP	probably: Postfix but Postfix
	version: unknown
WWW	Apache/2.2.8 (Ubuntu)
	PHP version: 5.2.4

3.2.2 Remote Host

The remote host "farm.secnet" with the IP 192.168.1.12 has a Linux Kernel. This follows from the TCP based remote OS fingerprint results. Furthermore it was possible to extract the OS from the Session Setup. The detected OS is a UNIX System. Probably the OS is Ubuntu, as an Apache server and an OpenSSH server for ubuntu are running on it. The host has 24 open ports. It was possible to find out the name of the computer "FARM" and the currently logged in user: "FARM" using NetBIOS. The SMB server seems to be a SAMBA Server (it claims to have a null MAC address).

3.3 Vulnerability Scan

The vulnerability scan revealed many of the above described things. OpenVAS, as you can see in the OpenVAS report in the appendix, firstly weighted the results by severeness. The problems with the highest risk for the host are the first in the report. The Host has 36 vulnerabilities marked with the severity high, 14 marked with medium and 7 with severity low.

Mostly the advice given by OpenVAS is to update the running service. For example vsftp has in the running version a backdoor vulnerability, proFTPD has a SQL Injection vulnerability. Sometimes there is more than one thread coming from the same source. For example the old PHP version alone causes nine of the 36 high severity issues.

For some threads OpenVAS says, that there is no update available and it recommends, that the service should be replaced by another service. That is for example the case with rexec and rsh. Other services are just marked as unsave and OpenVAS does not have a recommendation. That is the case with distcc and ingreslock for instance.

After the version check, OpenVAS checks for some more known issues. For example it recommends to adjust the config file of the apache web server. Furthermore it tries to brute force some services to get access. It uses a list with easy, but often chosen username-password-combinations such as *user:user* or similar. In the scan of host farm two guesses of OpenVAS turned out to be valid and granted access. OpenVAS recommends to change the credentials for ssh (at the moment it is *user:user*) and to change the credentials of postgres (at the moment *postgres:postgres*).

All in all OpenVAS found many vulnerabilities, including some really serious ones, in a short time. We were able to find some of the issues as well after the port checking, but OpenVAS was much faster and much more concrete.

4 Discussion

There are some services, we want to discuss further - These services can be seen in Table 3. The first service is telnet. Computer security experts recommend to disable it, because telnet has access to many points in the network, but is not encrypting sent information (not even passwords). Furthermore there are several vulnerabilities found in the commonly used telnet daemons. Therefore we follow the advice and recommend to disable telnet.

There are two ftp services running on the server. Each of them has one found vulnerability. Vsftp has a backdoor vulnerability, proFTPD has a SQL Injection Vulnerability. Both vulnerabilities can be cleared by an update. But in this case we dont't want just to follow the advice of OpenVAS to update, but also recommend to disable one of the services, since they are mostly used for the same thing. It is not necessary to keep both running, but it increases the risk of future vulnerabilities.

The ssh service should also get an update. Furthermore the used credentials *user:user* should be changed. Here is not even a vulnerability in the service needed to get into the system. A good guess is sufficient. In the same step, the services exec, rsh and remote login should be disabled, since they are doing the same thing as the ssh server.

The smtp server answers to VRFY requests. An attacker could be able to gather information from this (for example if an user account exists on the system). This means a significant assistance to a brute-force attack. Therefore VRFY should be disabled. In the same step it should be checked, if EXPN is already disabled. If it's not, it should be disabled, too.

The apache server has several vulnerabilities. At first, the service and php should be updated. Furthermore the debug HTTP methods TRACE and TRACK should be disabled, since they could be used for cross-site-scripting attacks. Then there should be some changes in the config of the webserver - further information in the OpenVAS report.

The services distcc and ingreslock should be disabled as soon as possible. Ingreslock is marked as possible backdoor and distcc can be used to remotely execute code on the server.

The last recommendation is another password change. This time for the postgres database, because the used credentials "postgres:postgres" are not save.

If we compare the recommendations to the ones we made after the port checking, we can see, that we were able to find some of the issues as well. OpenVAS was much faster and had more details. But still it was necessary to view the recommendations by hand, because not always an update for a service is enough. We were able to see the bigger context and combine some of the recommendations of OpenVAS.

Table 3: Summary of vulnerability scan recommendations

Service Name	**Problems**	**Suggestions**
telnet	Experts in computer security recommend to discontinue the use	disable the service
ftp	backdoor vulnerability	update
	SQL Injection Vulnerability	update
ssh	weak credentials used	change credentials
	old version	update
smtp	'VRFY root' produces an valid answer	Disable VRFY and/or EXPN
www	several PHP issues	update to latest version
	TRACE and TRACK methods activated	disable methods
	server type detection possible	limit directive ServerTokens Prod
	cookie information disclosure vulnerability	update
	doc directory browsable	change config
distcc	Remote Code Execution Vulnerability	disable
ingreslock	Possible Backdoor	disable
postgres	weak credentials used	change credentials

5 Conclusion

OpenVAS is a helpful tool to gather as much information as possible in a short amount of time. Through the possibility of scheduled scans, the frequently updated NVTs and the alert function, OpenVAS can be used to periodically give an overview over a network and to monitor its security state. This way, known vulnerabilities can be discovered soon and the results already come with suggestions. Nevertheless it is necessary, that the administrator checks the reports by hand and keeps the bigger context in mind.

To extend this first idea of a more secure future system, there should be regular update sessions. One could see, that the used services on the farm server were outdated for quite a long time and there were several important updates available. Furthermore old and deprecated services should be disabled completely instead of just installing new services and forgetting the old ones. If old services are forgotten and a vulnerability is discovered, attackers can still use it, even if nobody else uses the services any more. Also there should not be more services than necessary to do the same thing. More services mean, that there are more chances to find a vulnerability. For example it is not needed to have more than one ftp server on a system.

The last recommendation for a more secure system is to use a firewall. In this way, only the ports that the administrator wants are exposed to the internet. Since there are constantly various threads in the internet and not only publicly known threats, this is a way to add an extra layer of security.

References

[1] *OpenVAS Website*. URL: http://openvas.org/software.html.

[2] M. Cotton, L. Eggert, J. Touch, M. Westerlund, and S. Cheshire. *RFC 6335 - Internet assigned numbers authority (IANA) procedures for the management of the service name and transport protocol port number registry*. Tech. rep. 2011.

[3] *Service Name and Transport Protocol Port Number Registry*. Feb. 2018. URL: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

[4] K. Houghton. *Vulnerabilities & Vulnerability Scanning*. 2003. URL: https://www.sans.org/reading-room/whitepapers/threats/vulnerabilities-vulnerability-scanning-1195.

[5] *8009, the forgotten Tomcat port*. Oct. 2011. URL: https://diablohorn.com/2011/10/19/8009-the-forgotten-tomcat-port/.

A Report from OpenVAS Vulnerability Scanning

Scan Report

February 11, 2018

Summary

This document reports on the results of an automatic security scan. The scan started at Sun Feb 11 10:37:22 2018 UTC and ended at Sun Feb 11 11:00:58 2018 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
192.168.1.12 (farm.secnet)	Severity: High	36	14	7	79	0
Total: 1		36	14	7	79	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 136 results selected by the filtering described above. Before filtering there were 137 results.

2 Results per Host

2.1 192.168.1.12

Host scan start	Sun Feb 11 10:37:27 2018 UTC
Host scan end	Sun Feb 11 11:00:58 2018 UTC

Service (Port)	Threat Level
clm_pts (6200/tcp)	High
distcc (3632/tcp)	High
ftp (21/tcp)	High
http (80/tcp)	High
ingreslock (1524/tcp)	High
ircd (6667/tcp)	High
nfs (2049/udp)	High
postgresql (5432/tcp)	High
scientia-ssdb (2121/tcp)	High
ssh (22/tcp)	High
x11 (6000/tcp)	High
http (80/tcp)	Medium
postgresql (5432/tcp)	Medium
ssh (22/tcp)	Medium
exec (512/tcp)	Medium
general/tcp	Medium
netbios-ssn (139/tcp)	Medium
shell (514/tcp)	Medium
smtp (25/tcp)	Medium
ircd (6667/tcp)	Low

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
general/tcp	Low
domain (53/tcp)	Low
telnet (23/tcp)	Low
tftp (69/udp)	Low
vnc (5900/tcp)	Low
distcc (3632/tcp)	Log
ftp (21/tcp)	Log
http (80/tcp)	Log
ingreslock (1524/tcp)	Log
ircd (6667/tcp)	Log
postgresql (5432/tcp)	Log
scientia-ssdb (2121/tcp)	Log
ssh (22/tcp)	Log
x11 (6000/tcp)	Log
exec (512/tcp)	Log
general/tcp	Log
netbios-ssn (139/tcp)	Log
shell (514/tcp)	Log
smtp (25/tcp)	Log
domain (53/tcp)	Log
telnet (23/tcp)	Log
vnc (5900/tcp)	Log
ajp13 (8009/tcp)	Log
domain (53/udp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/SMBClient	Log
general/icmp	Log
login (513/tcp)	Log
microsoft-ds (445/tcp)	Log
msgsrvr (8787/tcp)	Log
mysql (3306/tcp)	Log
netbios-ns (137/udp)	Log
nfs (2049/tcp)	Log
rmiregistry (1099/tcp)	Log
sunrpc (111/tcp)	Log

2.1.1 High clm_pts (6200/tcp)

High (CVSS: 7.5)
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

```
Summary:
vsftpd is prone to a backdoor vulnerability.
```

... continues on next page ...

... continued from previous page ...

Attackers can exploit this issue to execute arbitrary commands in the
context of the application. Successful attacks will compromise the
affected application.
The vsftpd 2.3.4 source package is affected.
Solution:
The repaired package can be downloaded from
https://security.appspot.com/vsftpd.html. Please validate the package
with its signature.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103185

References

BID:48539
Other:
URL:http://www.securityfocus.com/bid/48539
URL:http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-back
↪doored.html
URL:https://security.appspot.com/vsftpd.html
URL:http://vsftpd.beasts.org/

[return to 192.168.1.12]

2.1.2 High distcc (3632/tcp)

High (CVSS: 9.3)
NVT: distcc Remote Code Execution Vulnerability

Summary:
distcc 2.x, as used in XCode 1.5 and others, when not configured to restrict
access to the server port, allows remote attackers to execute arbitrary
commands via compilation jobs, which are executed by the server without
authorization checks.
Solution:
Vendor updates are available. Please see the references for more
information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103553

References

CVE: CVE-2004-2687

... continues on next page ...

... continued from previous page ...

```
Other:
  URL:http://distcc.samba.org/security.html
   URL:http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2687
   URL:http://www.osvdb.org/13378
   URL:http://archives.neohapsis.com/archives/bugtraq/2005-03/0183.html
```

High (CVSS: 8.5)
NVT: DistCC Detection

```
 Summary:
 distcc is a program to distribute builds of C, C++, Objective C or
Objective C++ code across several machines on a network.
distcc should always generate the same results as a local build, is simple
to install and use, and is often two or more times faster than a local compile.
distcc by default trusts its clients completely that in turn could
allow a malicious client to execute arbitrary commands on the server.
For more information about DistCC's security see:
http://distcc.samba.org/security.html
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.12638

[return to 192.168.1.12]

2.1.3 High ftp (21/tcp)

High (CVSS: 7.5)
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

```
 Summary:
 vsftpd is prone to a backdoor vulnerability.
Attackers can exploit this issue to execute arbitrary commands in the
context of the application. Successful attacks will compromise the
affected application.
The vsftpd 2.3.4 source package is affected.
 Solution:
 The repaired package can be downloaded from
https://security.appspot.com/vsftpd.html. Please validate the package
with its signature.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103185

... continues on next page ...

. . . continued from previous page . . .

References

BID:48539
Other:
URL:http://www.securityfocus.com/bid/48539
URL:http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
URL:https://security.appspot.com/vsftpd.html
URL:http://vsftpd.beasts.org/

High (CVSS: 7.5)
NVT: ProFTPD Server SQL Injection Vulnerability

Summary:
This host is running ProFTPD Server and is prone to remote
SQL Injection vulnerability.
Vulnerability Insight:
This flaw occurs because the server performs improper input sanitising,
- when a %(percent) character is passed in the username, a single quote
(') gets introduced during variable substitution by mod_sql and this
eventually allows for an SQL injection during login.
- when NLS support is enabled, a flaw in variable substition feature in
mod_sql_mysql and mod_sql_postgres may allow an attacker to bypass
SQL injection protection mechanisms via invalid, encoded multibyte
characters.
Impact:
Successful exploitation will allow remote attackers to execute arbitrary
SQL commands, thus gaining access to random user accounts.
Affected Software/OS:
ProFTPD Server version 1.3.1 through 1.3.2rc2
Solution:
Upgrade to the latest version 1.3.2rc3,
http://www.proftpd.org/

OID of test routine: 1.3.6.1.4.1.25623.1.0.900507

References

CVE: CVE-2009-0542, CVE-2009-0543
BID:33722
Other:
URL:http://www.milw0rm.com/exploits/8037
URL:http://www.securityfocus.com/archive/1/archive/1/500833/100/0/threaded
URL:http://www.securityfocus.com/archive/1/archive/1/500851/100/0/threaded

High (CVSS: 5.8)
NVT: ProFTPD mod_tls Module NULL Character CA SSL Certificate Validation Security Bypass Vulnerability

```
 Summary:
 ProFTPD is prone to a security-bypass vulnerability because the
application fails to properly validate the domain name in a signed CA
certificate, allowing attackers to substitute malicious SSL
certificates for trusted ones.
Successful exploits allows attackers to perform man-in-the-
middle attacks or impersonate trusted servers, which will aid in
further attacks.
Versions prior to ProFTPD 1.3.2b and 1.3.3 to 1.3.3.rc1 are vulnerable.
 Solution:
 Updates are available. Please see the references for details.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100316

References

```
CVE: CVE-2009-3639
BID:36804
Other:
  URL:http://www.securityfocus.com/bid/36804
   URL:http://bugs.proftpd.org/show_bug.cgi?id=3275
   URL:http://www.proftpd.org
```

[return to 192.168.1.12]

2.1.4 High http (80/tcp)

High (CVSS: 10.0)
NVT: PHP version smaller than 5.2.7

```
  Summary:
  PHP version smaller than 5.2.7 suffers vulnerability.
  Solution:
  Update PHP to version 5.2.7 or later.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.110172

References

. . . continues on next page . . .

... continued from previous page ...

CVE: CVE-2008-2371, CVE-2008-2665, CVE-2008-2666, CVE-2008-2829, CVE-2008-3658,
↪CVE-2008-3659, CVE-2008-3660, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE
↪-2008-5658
BID:29796, 29797, 29829, 30087, 30649, 31612, 32383, 32625, 32688, 32948

High (CVSS: 10.0)
NVT: PHP version smaller than 5.2.6

Summary:
PHP version smaller than 5.2.6 suffers vulnerability.
Solution:
Update PHP to version 5.2.6 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110183

References

CVE: CVE-2007-4850, CVE-2007-6039, CVE-2008-0599, CVE-2008-1384, CVE-2008-2050,
↪CVE-2008-2051
BID:27413, 28392, 29009

High (CVSS: 9.3)
NVT: PHP version smaller than 5.2.14

Summary:
PHP version smaller than 5.2.14 suffers vulnerability.
Solution:
Update PHP to version 5.2.14 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110171

References

CVE: CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864,
↪CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE
↪-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3065
BID:38708, 40948, 41991

... continues on next page ...

. . . continued from previous page . . .

High (CVSS: 9.3)
NVT: PHP version smaller than 5.2.5

Summary:
PHP version smaller than 5.2.5 suffers vulnerability.
Solution:
Update PHP to version 5.2.5 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110179

References

CVE: CVE-2007-3996, CVE-2007-4782, CVE-2007-4783, CVE-2007-4784, CVE-2007-4825,
↪CVE-2007-4840, CVE-2007-4887, CVE-2007-4889, CVE-2007-5447, CVE-2007-5653, CVE
↪-2007-5898, CVE-2007-5899, CVE-2007-5900, CVE-2008-2107, CVE-2008-2108, CVE-20
↪08-4107
BID:26403

High (CVSS: 9.3)
NVT: PHP version smaller than 5.3.3

Summary:
PHP version smaller than 5.3.3 suffers vulnerability.
Solution:
Update PHP to version 5.3.3 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110182

References

CVE: CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864,
↪CVE-2010-1917, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE
↪-2010-2191, CVE-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3062, CVE-20
↪10-3063, CVE-2010-3064, CVE-2010-3065
BID:38708, 40461, 40948, 41991

High (CVSS: 7.5)
NVT: TikiWiki Versions Prior to 4.2 Multiple Unspecified Vulnerabilities

Product detection result

. . . continues on next page . . .

... continued from previous page ...

cpe:/a:tikiwiki:tikiwiki:1.9.5
Detected by TikiWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

Summary:
TikiWiki is prone to multiple unspecified vulnerabilities, including:
- An unspecified SQL-injection vulnerability
- An unspecified authentication-bypass vulnerability
- An unspecified vulnerability
Exploiting these issues could allow an attacker to compromise the application, access or modify data, exploit latent vulnerabilities in the underlying database, and gain unauthorized access to the affected application. Other attacks are also possible.
Versions prior to TikiWiki 4.2 are vulnerable.
Solution:
The vendor has released an advisory and fixes. Please see the references for details.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100537

References
CVE: CVE-2010-1135, CVE-2010-1134, CVE-2010-1133, CVE-2010-1136
BID:38608
Other:
URL:http://www.securityfocus.com/bid/38608
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision
↪=24734
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision
↪=25046
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision
↪=25424
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision
↪=25435
URL:http://info.tikiwiki.org/article86-Tiki-Announces-3-5-and-4-2-Releases
URL:http://info.tikiwiki.org/tiki-index.php?page=homepage

High (CVSS: 7.5)
NVT: PHP-CGI-based setups vulnerability when parsing query string parameters from php files.

Summary:
When PHP is used in a CGI-based setup (such as Apache's mod_cgid), the php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the php-cgi binary, which can be exploited to disclose source

... continues on next page ...

... continued from previous page ...

code and obtain arbitrary code execution.
An example of the -s command, allowing an attacker to view the source code
of index.php is below:
http://localhost/index.php?-s

OID of test routine: 1.3.6.1.4.1.25623.1.0.103482

References

CVE: CVE-2012-1823, CVE-2012-2311, CVE-2012-2336, CVE-2012-2335
BID:53388
Other:
URL:http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-r
↪isks-Update-1567532.html
URL:http://www.kb.cert.org/vuls/id/520827
URL:http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
URL:https://bugs.php.net/bug.php?id=61910
URL:http://www.php.net/manual/en/security.cgi-bin.php

High (CVSS: 7.5)
NVT: PHP version smaller than 5.2.11

Summary:
PHP version smaller than 5.2.11 suffers vulnerability.
Solution:
Update PHP to version 5.2.11 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110176

References

CVE: CVE-2009-3291, CVE-2009-3292, CVE-2009-3293, CVE-2009-3294, CVE-2009-4018,
↪CVE-2009-5016
BID:36449, 44889

High (CVSS: 7.5)
NVT: PHP version smaller than 5.3.1

Summary:
PHP version smaller than 5.3.1 suffers vulnerability.
Solution:

... continues on next page ...

... continued from previous page ...

Update PHP to version 5.3.1 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110178

References
CVE: CVE-2009-3557, CVE-2009-3559, CVE-2009-4017, CVE-2009-4018, CVE-2010-1128
BID:36554, 36555, 37079, 37138

High (CVSS: 7.5)
NVT: PHP version smaller than 5.2.8

Summary:
PHP version smaller than 5.2.8 suffers vulnerability.
Solution:
Update PHP to version 5.2.8 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110180

References
CVE: CVE-2008-5814, CVE-2008-5844
BID:32673

High (CVSS: 7.5)
NVT: phpinfo() output accessible

The following files are calling the function phpinfo() which
disclose potentially sensitive information to the remote attacker :
/phpinfo.php
Solution: Delete them or restrict access to them

OID of test routine: 1.3.6.1.4.1.25623.1.0.11229

High (CVSS: 6.8)
NVT: PHP version smaller than 5.3.4

Summary:

... continues on next page ...

... continued from previous page ...

PHP version smaller than 5.3.4 suffers vulnerability.
Solution:
Update PHP to version 5.3.4 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110181

References

CVE: CVE-2006-7243, CVE-2010-2094, CVE-2010-2950, CVE-2010-3436, CVE-2010-3709, ↪CVE-2010-3710, CVE-2010-3870, CVE-2010-4150, CVE-2010-4156, CVE-2010-4409, CVE ↪-2010-4697, CVE-2010-4698, CVE-2010-4699, CVE-2010-4700, CVE-2011-0753, CVE-20 ↪11-0754, CVE-2011-0755
BID:40173, 43926, 44605, 44718, 44723, 44951, 44980, 45119, 45335, 45338, 45339, ↪ 45952, 45954, 46056, 46168

High (CVSS: 5.8)
NVT: http TRACE XSS attack

Summary:
Debugging functions are enabled on the remote HTTP server.
Description :
The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.
It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.
An attacker may use this flaw to trick your legitimate web users to give him their credentials.
Solution:
Disable these methods.
Plugin output :
Solution:
Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

See also http://httpd.apache.org/docs/current/de/mod/core.html#traceenable

OID of test routine: 1.3.6.1.4.1.25623.1.0.11213

References

CVE: CVE-2004-2320, CVE-2003-1567

... continues on next page ...

... continued from previous page ...

```
BID:9506, 9561, 11604
Other:
  URL:http://www.kb.cert.org/vuls/id/867593
```

[return to 192.168.1.12]

2.1.5 High ingreslock (1524/tcp)

High (CVSS: 10.0)
NVT: Possible Backdoor: Ingreslock

```
 Summary:
 A backdoor is installed on the remote host
Attackers can exploit this issue to execute arbitrary commands in the
context of the application. Successful attacks will compromise the
affected isystem.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103549

[return to 192.168.1.12]

2.1.6 High ircd (6667/tcp)

High (CVSS: 7.5)
NVT: Check for Backdoor in unrealircd

```
 Summary:
 Detection of backdoor in unrealircd.
 Vulnerability Insight:
 Remote attackers can exploit this issue to execute arbitrary system
commands within the context of the affected application.
The issue affects Unreal 3.2.8.1 for Linux. Reportedly package
Unreal3.2.8.1.tar.gz downloaded in November 2009 and later is
affected. The MD5 sum of the affected file is
752e46f2d873c1679fa99de3f52a274d. Files with MD5 sum of
7b741e94e867c0a7370553fd01506c66 are not affected.
 Solution:
 Install latest version of unrealircd and check signatures of software
you're installing.
```

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.80111

References

```
CVE: CVE-2010-2075
BID:40820
Other:
  URL:http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt
   URL:http://seclists.org/fulldisclosure/2010/Jun/277
   URL:http://www.securityfocus.com/bid/40820
```

[return to 192.168.1.12]

2.1.7 High nfs (2049/udp)

High (CVSS: 10.0)
NVT: NFS export

```
Here is the export list of farm.secnet :
/ *
Please check the permissions of this exports.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.102014

References

```
CVE: CVE-1999-0554, CVE-1999-0548
```

[return to 192.168.1.12]

2.1.8 High postgresql (5432/tcp)

High (CVSS: 9.0)
NVT: PostgreSQL weak password

Product detection result

```
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
```

```
Summary:
It was possible to login into the remote PostgreSQL as user postgres using weak
```

... continues on next page ...

... continued from previous page ...

```
↪ credentials.
 Solution:
 Change the password as soon as possible.
It was possible to login as user postgres with password "postgres".
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103552

High (CVSS: 8.5)
NVT: PostgreSQL Multiple Security Vulnerabilities

Product detection result

```
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
```

```
 Summary:
 PostgreSQL is prone to multiple security vulnerabilities.
Attackers can exploit these issues to bypass certain security
restrictions and execute arbitrary Perl or Tcl code.
These issues affect versions prior to the following PostgreSQL
versions:
8.4.4
8.3.11
8.2.17
8.1.21
8.0.25
7.4.29
 Solution:
 Updates are available. Please see the references for more information.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100645

References

```
CVE: CVE-2010-1169, CVE-2010-1170, CVE-2010-1447
BID:40215
Other:
  URL:http://www.securityfocus.com/bid/40215
   URL:http://www.postgresql.org/about/news.1203
   URL:http://www.postgresql.org/
   URL:http://www.postgresql.org/support/security
```

High (CVSS: 6.8)
NVT: PostgreSQL Multiple Security Vulnerabilities

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary:
PostgreSQL is prone to multiple security vulnerabilities, including a denial-of-service issue, a privilege-escalation issue, and an authentication-bypass issue.
Attackers can exploit these issues to shut down affected servers, perform certain actions with elevated privileges, and bypass authentication mechanisms to perform unauthorized actions. Other attacks may also be possible.
Solution:
Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100273

References
CVE: CVE-2009-3229, CVE-2009-3230, CVE-2009-3231
BID:36314
Other:
URL:http://www.securityfocus.com/bid/36314
URL:https://bugzilla.redhat.com/show_bug.cgi?id=522085#c1
URL:http://www.postgresql.org/
URL:http://www.postgresql.org/support/security
URL:http://permalink.gmane.org/gmane.comp.security.oss.general/2088

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:

. . . continues on next page . . .

... continued from previous page ...

URL:http://www.securityfocus.com/bid/67899
URL:http://openssl.org/

High (CVSS: 6.5)
NVT: PostgreSQL NULL Character CA SSL Certificate Validation Security Bypass Vulnerability

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary:
PostgreSQL is prone to a security-bypass vulnerability because the application fails to properly validate the domain name in a signed CA certificate, allowing attackers to substitute malicious SSL certificates for trusted ones.
Successfully exploiting this issue allows attackers to perform man-in-the-middle attacks or impersonate trusted servers, which will aid in further attacks.
PostgreSQL is also prone to a local privilege-escalation vulnerability. Exploiting this issue allows local attackers to gain elevated privileges.
PostgreSQL versions prior to 8.4.2, 8.3.9, 8.2.15, 8.1.19, 8.0.23, and 7.4.27 are vulnerable to this issue.
Solution:
Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100400

References
CVE: CVE-2009-4034, CVE-2009-4136
BID:37334, 37333
Other:
URL:http://www.securityfocus.com/bid/37334
URL:http://www.securityfocus.com/bid/37333
URL:http://www.postgresql.org
URL:http://www.postgresql.org/support/security
URL:http://www.postgresql.org/about/news.1170

High (CVSS: 6.5)
NVT: PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary:
PostgreSQL is prone to a buffer-overflow vulnerability because the application fails to perform adequate boundary checks on user-supplied data.
Attackers can exploit this issue to execute arbitrary code with elevated privileges or crash the affected application.
PostgreSQL version 8.0.x, 8.1.x, 8.3.x is vulnerable; other versions may also be affected.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100470

References
CVE: CVE-2010-0442
BID:37973
Other:
URL:http://www.postgresql.org/
URL:http://www.securityfocus.com/bid/37973
URL:http://xforce.iss.net/xforce/xfdb/55902
URL:http://intevydis.blogspot.com/2010/01/postgresql-8023-bitsubstr-overflow.html

High (CVSS: 6.5)
NVT: PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary:
PostgreSQL is prone to a buffer-overflow vulnerability because the application fails to perform adequate boundary checks on user-supplied data. The issue affects the 'intarray' module.
An authenticated attacker can leverage this issue to execute arbitrary code within the context of the vulnerable application. Failed exploit attempts will result in a denial-of-service condition.
The issue affect versions prior to 8.2.20, 8.3.14, 8.4.7, and 9.0.3.
Solution:
Updates are available. Please see the references for more information.

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.103054

References

CVE: CVE-2010-4015
BID:46084
Other:
URL:https://www.securityfocus.com/bid/46084
URL:http://www.postgresql.org/
URL:http://www.postgresql.org/about/news.1289

High (CVSS: 6.0)
NVT: PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability

Product detection result

cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary:
PostgreSQL is prone to a local privilege-escalation vulnerability.
Exploiting this issue allows local attackers to gain elevated
privileges and execute arbitrary commands with the privileges of
the victim.
Versions prior to PostgreSQL 9.0.1 are vulnerable.
Solution:
Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100843

References

CVE: CVE-2010-3433
BID:43747
Other:
URL:https://www.securityfocus.com/bid/43747
URL:http://www.postgresql.org/docs/9.0/static/release-9-0-1.html
URL:http://www.postgresql.org
URL:http://www.postgresql.org/support/security

High (CVSS: 5.5)
NVT: PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary:
PostgreSQL is prone to an unauthorized-access vulnerability.
Attackers can exploit this issue to reset special parameter
settings only a root user should be able to modify. This may aid in
further attacks.
This issue affects versions prior to the following PostgreSQL
versions:
7.4.29,
8.0.25
8.1.21,
8.2.17
8.3.11
8.4.4
Solution:
Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100648

References
CVE: CVE-2010-1975
BID:40304
Other:
URL:http://www.securityfocus.com/bid/40304
URL:http://www.postgresql.org/docs/current/static/release-8-4-4.html
URL:http://www.postgresql.org/docs/current/static/release-8-2-17.html
URL:http://www.postgresql.org/docs/current/static/release-8-1-21.html
URL:http://www.postgresql.org/docs/current/static/release-8-3-11.html
URL:http://www.postgresql.org/
URL:http://www.postgresql.org/docs/current/static/release-8-0-25.html
URL:http://www.postgresql.org/docs/current/static/release-7-4-29.html

[return to 192.168.1.12]

2.1.9 High scientia-ssdb (2121/tcp)

High (CVSS: 7.5)
NVT: ProFTPD Server SQL Injection Vulnerability

```
Summary:
This host is running ProFTPD Server and is prone to remote
SQL Injection vulnerability.
Vulnerability Insight:
This flaw occurs because the server performs improper input sanitising,
- when a %(percent) character is passed in the username, a single quote
  (') gets introduced during variable substitution by mod_sql and this
  eventually allows for an SQL injection during login.
- when NLS support is enabled, a flaw in variable substition feature in
  mod_sql_mysql and mod_sql_postgres may allow an attacker to bypass
  SQL injection protection mechanisms via invalid, encoded multibyte
  characters.
Impact:
Successful exploitation will allow remote attackers to execute arbitrary
SQL commands, thus gaining access to random user accounts.
Affected Software/OS:
ProFTPD Server version 1.3.1 through 1.3.2rc2
Solution:
Upgrade to the latest version 1.3.2rc3,
http://www.proftpd.org/
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900507

References

```
CVE: CVE-2009-0542, CVE-2009-0543
BID:33722
Other:
  URL:http://www.milw0rm.com/exploits/8037
   URL:http://www.securityfocus.com/archive/1/archive/1/500833/100/0/threaded
   URL:http://www.securityfocus.com/archive/1/archive/1/500851/100/0/threaded
```

High (CVSS: 6.8)
NVT: ProFTPD Long Command Handling Security Vulnerability

```
Summary:
The host is running ProFTPD Server, which is prone to cross-site
request forgery vulnerability.
Vulnerability Insight:
The flaw exists due to the application truncating an overly long FTP command,
and improperly interpreting the remainder string as a new FTP command.
Impact:
```

... continues on next page ...

... continued from previous page ...

```
This can be exploited to execute arbitrary FTP commands on another
user's session privileges.
Impact Level : Application
Affected Software/OS:
ProFTPD Project versions 1.2.x on Linux
ProFTPD Project versions 1.3.x on Linux
Solution:
Fixed is available in the SVN repository,
http://www.proftpd.org/cvs.html
*****
NOTE : Ignore this warning, if above mentioned fix is applied already.
*****
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900133

References

```
CVE: CVE-2008-4242
BID:31289
Other:
  URL:http://secunia.com/advisories/31930/
   URL:http://bugs.proftpd.org/show_bug.cgi?id=3115
```

High (CVSS: 5.8)
NVT: ProFTPD mod_tls Module NULL Character CA SSL Certificate Validation Security Bypass Vulnerability

```
 Summary:
 ProFTPD is prone to a security-bypass vulnerability because the
application fails to properly validate the domain name in a signed CA
certificate, allowing attackers to substitute malicious SSL
certificates for trusted ones.
Successful exploits allows attackers to perform man-in-the-
middle attacks or impersonate trusted servers, which will aid in
further attacks.
Versions prior to ProFTPD 1.3.2b and 1.3.3 to 1.3.3.rc1 are vulnerable.
 Solution:
 Updates are available. Please see the references for details.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100316

References

... continues on next page ...

... continued from previous page ...

```
CVE: CVE-2009-3639
BID:36804
Other:
  URL:http://www.securityfocus.com/bid/36804
   URL:http://bugs.proftpd.org/show_bug.cgi?id=3275
   URL:http://www.proftpd.org
```

[return to 192.168.1.12]

2.1.10 High ssh (22/tcp)

High (CVSS: 9.0)
NVT: SSH Brute Force Logins with default Credentials

```
Summary:
A number of known default credentials is tried for log in via SSH protocol.
Solution:
Change the password as soon as possible.
It was possible to login with the following credentials <User>:<Password>
user:user



OID of test routine: 1.3.6.1.4.1.25623.1.0.103239
```

[return to 192.168.1.12]

2.1.11 High x11 (6000/tcp)

High (CVSS: 10.0)
NVT: X Server

```
This X server does *not* allow any client to connect to it
however it is recommended that you filter incoming connections
to this port as attacker may send garbage data and slow down
your X session or even kill the server.
Here is the server version : 11.0
Here is the message we received : Client is not authorized
Solution: filter incoming connections to ports 6000-6009



OID of test routine: 1.3.6.1.4.1.25623.1.0.10407
```

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-1999-0526

[return to 192.168.1.12]

2.1.12 Medium http (80/tcp)

Medium (CVSS: 5.0)
NVT: /doc directory browsable ?

```
 Summary:
 The /doc directory is browsable.
/doc shows the content of the /usr/doc directory and therefore it shows which pr
↪ograms and - important! - the version of the installed programs.
 Solution:
 Use access restrictions for the /doc directory.
If you use Apache you might use this in your access.conf:
 <Directory /usr/doc>
 AllowOverride None
 order deny,allow
 deny from all
 allow from localhost
 </Directory>
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10056

References
CVE: CVE-1999-0678
BID:318

Medium (CVSS: 5.0)
NVT: awiki Multiple Local File Include Vulnerabilities

```
 Summary:
 awiki is prone to multiple local file-include vulnerabilities because
it fails to properly sanitize user-supplied input.
An attacker can exploit this vulnerability to obtain potentially
sensitive information and execute arbitrary local scripts in the
context of the webserver process. This may allow the attacker to
compromise the application and the computer; other attacks are
also possible.
```

... continues on next page ...

... continued from previous page ...

awiki 20100125 is vulnerable; other versions may also be affected.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103210

References

BID:49187
Other:
URL:http://www.securityfocus.com/bid/49187
URL:http://www.kobaonline.com/awiki/

Medium (CVSS: 5.0)
NVT: PHP version smaller than 5.2.9

Summary:
PHP version smaller than 5.2.9 suffers vulnerability.
Solution:
Update PHP to version 5.2.9 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110187

References

CVE: CVE-2008-5498, CVE-2009-1271, CVE-2009-1272
BID:33002, 33927

Medium (CVSS: 4.3)
NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability

Product detection result

cpe:/a:phpmyadmin:phpmyadmin
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary:
The host is running phpMyAdmin and is prone to Cross-Site
Scripting Vulnerability.
Vulnerability Insight:
The flaw is caused by input validation errors in the 'error.php'
script when processing crafted BBcode tags containing '@' characters, which
could allow attackers to inject arbitrary HTML code within the error page

... continues on next page ...

... continued from previous page ...

```
and conduct phishing attacks.
  Impact:
  Successful exploitation will allow attackers to inject arbitrary
HTML code within the error page and conduct phishing attacks.
Impact Level: Application
  Affected Software/OS:
  phpMyAdmin version 3.3.8.1 and prior.
  Solution:
  No solution or patch was made available for at least one year
since disclosure of this vulnerability. Likely none will be provided anymore.
General solution options are to upgrade to a newer release, disable respective
features, remove the product or replace the product by another one.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.801660

References

```
CVE: CVE-2010-4480
Other:
  URL:http://www.exploit-db.com/exploits/15699/
   URL:http://www.vupen.com/english/advisories/2010/3133
```

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 192.168.1.12]

2.1.13 Medium postgresql (5432/tcp)

Medium (CVSS: 4.0)
NVT: PostgreSQL Conversion Encoding Remote Denial of Service Vulnerability

Product detection result

```
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
```

```
Summary:
PostgreSQL is prone to a remote denial-of-service vulnerability.
 Exploiting this issue may allow attackers to terminate connections
 to the PostgreSQL server, denying service to legitimate users.
Solution:
Updates are available. Update to newer Version.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100157

References

```
CVE: CVE-2009-0922
BID:34090
Other:
  URL:http://www.securityfocus.com/bid/34090
   URL:http://www.postgresql.org/
```

Medium (CVSS: 3.5)
NVT: PostgreSQL Hash Table Integer Overflow Vulnerability

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

```
  Summary:
  The host is running PostgreSQL and is prone to integer overflow
  vulnerability.
  Vulnerability Insight:
  The flaw is due to an integer overflow error in 'src/backend/executor/nodeHash
↪.c',
  when used to calculate size for the hashtable for joined relations.
  Impact:
  Successful exploitation could allow execution of specially-crafted sql query
  which once processed would lead to denial of service (postgresql daemon crash)
↪.
  Impact Level: Application
  Affected Software/OS:
  PostgreSQL version 8.4.1 and prior and 8.5 through 8.5alpha2
  Solution:
  Apply the patch,
  http://git.postgresql.org/gitweb?p=postgresql.git;a=commitdiff;h=64b057e682365
↪5fb6c5d1f24a28f236b94dd6c54
  ******
  NOTE: Please ignore this warning if the patch is applied.
  ******
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.902139

References
CVE: CVE-2010-0733
Other:
URL:https://bugzilla.redhat.com/show_bug.cgi?id=546621
URL:http://www.openwall.com/lists/oss-security/2010/03/16/10
URL:http://archives.postgresql.org/pgsql-bugs/2009-10/msg00310.php
URL:http://archives.postgresql.org/pgsql-bugs/2009-10/msg00289.php
URL:http://archives.postgresql.org/pgsql-bugs/2009-10/msg00287.php
URL:http://archives.postgresql.org/pgsql-bugs/2009-10/msg00277.php

... continues on next page ...

... continued from previous page ...

Medium (CVSS: 2.1)
NVT: PostgreSQL Low Cost Function Information Disclosure Vulnerability

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary:
PostgreSQL is prone to an information-disclosure vulnerability.
Local attackers can exploit this issue to obtain sensitive
information that may lead to further attacks.
PostgreSQL 8.3.6 is vulnerable; other versions may also be affected.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100158

References
BID:34069
Other:
URL:http://www.securityfocus.com/bid/34069
URL:http://www.postgresql.org/

[return to 192.168.1.12]

2.1.14 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_4.7p1 debian-8ubuntu1

OID of test routine: 1.3.6.1.4.1.25623.1.0.103503

References
CVE: CVE-2012-0814
BID:51702
Other:

... continues on next page ...

... continued from previous page ...

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 192.168.1.12]

2.1.15 Medium exec (512/tcp)

Medium (CVSS: 5.0)
NVT: Check for rexecd Service

Summary:
Rexecd Service is running at this Host.
Rexecd (Remote Process Execution) has the same kind of functionality
that rsh has : you can execute shell commands on a remote computer.
The main difference is that rexecd authenticate by reading the
username and password *unencrypted* from the socket.
Solution:
Disable rexec Service.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100111

[return to 192.168.1.12]

2.1.16 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: 51127999
Paket 2: 51128102

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 192.168.1.12]

2.1.17 Medium netbios-ssn (139/tcp)

Medium (CVSS: 2.1)
NVT: Samba 'client/mount.cifs.c' Remote Denial of Service Vulnerability

```
 Summary:
 Samba is prone to a remote denial-of-service vulnerability.
A remote attacker can exploit this issue to crash the affected
application, denying service to legitimate users.
Samba 3.4.5 and earlier are vulnerable.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100499

References

```
CVE: CVE-2010-0547
BID:38326
Other:
  URL:http://www.securityfocus.com/bid/38326
   URL:http://git.samba.org/?p=samba.git;a=commit;h=a065c177dfc8f968775593ba00df
↪fafeebb2e054
   URL:http://us1.samba.org/samba/
```

[return to 192.168.1.12]

2.1.18 Medium shell (514/tcp)

Medium (CVSS: 0.0)
NVT: Check for rsh Service

```
 Summary:
 rsh Service is running at this Host.
   rsh (remote shell) is a command line computer program which can execute
   shell commands as another user, and on another computer across a computer
   network.
 Solution:
 Disable rsh and use ssh instead.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100080

[return to 192.168.1.12]

2.1.19 Medium smtp (25/tcp)

Medium (CVSS: 5.0)
NVT: Check if Mailserver answer to VRFY and EXPN requests

```
'VRFY root' produces the following answer: 252 2.0.0 root
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100072

References

```
Other:
  URL:http://cr.yp.to/smtp/vrfy.html
```

[return to 192.168.1.12]

2.1.20 Low ircd (6667/tcp)

Low (CVSS: 0.0)
NVT: IRC daemon identification

```
The IRC server version is : Unreal3.2.8.1. FhiXOoE [*=2309]
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11156

[return to 192.168.1.12]

2.1.21 Low general/tcp

Low (CVSS: 0.0)
NVT: ProFTPD Server Remote Version Detection

```
ProFTPD version 1.3.1 was detected on the host
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900815

[return to 192.168.1.12]

2.1.22 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 : 9.4.2
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 192.168.1.12]

2.1.23 Low telnet (23/tcp)

Low (CVSS: 0.0)
NVT: Check for Telnet Server

```
 Summary:
 A telnet Server is running at this host.
   Experts in computer security, such as SANS Institute, and the members of the
   comp.os.linux.security newsgroup recommend that the use of Telnet for remote
   logins should be discontinued under all normal circumstances, for the followi
↪ng
   reasons:
   * Telnet, by default, does not encrypt any data sent over the connection
     (including passwords), and so it is often practical to eavesdrop on the
     communications and use the password later for malicious purposes; anybody w
↪ho
     has access to a router, switch, hub or gateway located on the network betwe
↪en
     the two hosts where Telnet is being used can intercept the packets passing
↪by
     and obtain login and password information (and whatever else is typed) with
↪ any
```

... continues on next page ...

... continued from previous page ...

```
     of several common utilities like tcpdump and Wireshark.

   * Most implementations of Telnet have no authentication that would ensure
     communication is carried out between the two desired hosts and not intercep
↪ted
     in the middle.
   * Commonly used Telnet daemons have several vulnerabilities discovered over
     the years.



OID of test routine: 1.3.6.1.4.1.25623.1.0.100074
```

[return to 192.168.1.12]

2.1.24 Low tftp (69/udp)

Low (CVSS: 0.0)
NVT: TFTP detection

```
 Summary:
 The remote host has TFTP server running.
Description :
The remote host has TFTP server running. TFTP stands
for Trivial File Transfer Protocol.
 Solution:
 Disable TFTP server if not used.



OID of test routine: 1.3.6.1.4.1.25623.1.0.80100
```

[return to 192.168.1.12]

2.1.25 Low vnc (5900/tcp)

Low (CVSS: 5.0)
NVT: VNC security types

```
The remote VNC server chose security type #2 (VNC authentication)



OID of test routine: 1.3.6.1.4.1.25623.1.0.19288
```

Low (CVSS: 0.0)
NVT: Check for VNC

```
 Summary:
 The remote host is running a remote display software (VNC)
Description :
The remote server is running VNC, a software which permits a
console to be displayed remotely.
This allows authenticated users of the remote host to take its
control remotely.
 Solution:
 Make sure the use of this software is done in accordance with your
corporate security policy, filter incoming traffic to this port.
Plugin output :
The version of the VNC protocol is : RFB 003.003
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10342

[return to 192.168.1.12]

2.1.26 Log distcc (3632/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 192.168.1.12]

2.1.27 Log ftp (21/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: FTP Banner Detection

```
Remote FTP server banner :
220 (vsFTPd 2.3.4)
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10092

Log (CVSS: 0.0)
NVT: Services

```
An FTP server is running on this port.
Here is its banner :
220 (vsFTPd 2.3.4)
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

[return to 192.168.1.12]

2.1.28 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/2.2.8 (Ubuntu) DAV/2
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: Web mirroring

```
The following CGI have been discovered :
Syntax : cginame (arguments [default value])
/twiki/bin/edit/Sandbox/TestTopic3 (topicparent [Sandbox.WebHome] )
/twiki/bin/view/Know/WebChanges (topic [] )
/twiki/bin/edit/Know/WebPreferences (t [1518345656] )
/twiki/bin/edit/TWiki/GoodStyle (t [1518345661] )
/twiki/bin/view/Know/WebTopicList (topic [] skin [print] )
/twiki/bin/edit/Know/WebTopicList (t [1518345671] )
/twiki/bin/view/TWiki/TWikiPreferences (topic [] )
/twiki/bin/rdiff/Sandbox/WebIndex (rev1 [1.2] rev2 [1.1] )
/twiki/bin/view/Sandbox/TestTopic1 (unlock [on] )
/twiki/bin/preview/Sandbox/TestTopic1 (formtemplate [] topicparent [] cmd [] )
/twiki/bin/view/Sandbox/WebNotify (topic [] skin [print] rev [1.4] )
/twiki/bin/edit/Sandbox/WebNotify (t [1518345677] )
/twiki/bin/view/Main/TWikiAdminGroup (topic [] skin [print] rev [1.6] )
/twiki/bin/oops/Main/TWikiAdminGroup (template [oopsmore] param1 [1.7] param2 [1
↪.7] )
/twiki/bin/edit/Main/PeterThoeny (t [1518345681] )
/twiki/bin/upload/Main/WebHome (filepath [] filecomment [] filename [] hidefile
↪[] createlink [] )
/twiki/bin/oops/Main/LondonOffice (template [oopsmore] param1 [1.3] param2 [1.3]
↪ )
/twiki/bin/edit/Main/BookView (topicparent [Main.TWikiVariables] )
/twiki/bin/edit/Main/WebTopicViewTemplate (topicparent [Main.TWikiVariables] )
/twiki/bin/edit/Main/UnlockTopic (topicparent [Main.TWikiVariables] )
/twiki/bin/edit/Main/DontNotify (topicparent [Main.TWikiVariables] )
/twiki/bin/oops/Main/KevinKinnell (param1 [1.2] param2 [1.2] template [oopsmore]
↪ )
/phpMyAdmin/phpmyadmin.css.php (token [689e3cdc015be078b06b3e09a8ed5880] js_fram
↪e [right] lang [en-utf-8] nocache [2457687151] convcharset [utf-8] )
/mutillidae/index.php (username [anonymous] do [toggle-hints] page [home.php] )
/mutillidae/ (page [add-to-your-blog.php] )
/mutillidae/styles/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/twiki/bin/edit/Sandbox/TestTopic4 (topicparent [Sandbox.WebHome] )
/twiki/bin/view/Main/WebSearch (topic [] )
```

... continues on next page ...

. . . continued from previous page . . .

```
/twiki/bin/search/Main/ (showlock [] search [] web [] scope [topic] nosearch []
↪reverse [] regex [] order [] nototal [] limit [all] bookview [] nosummary [] c
↪asesensitive [] )
/twiki/bin/view/TWiki/TWikiTopics (topic [] )
/twiki/bin/view/TWiki/TWikiVariables (topic [] )
/twiki/bin/view/TWiki/InstantEnhancements (topic [] )
/twiki/bin/view/TWiki/WikiName (topic [] skin [print] rev [1.2] )
/twiki/bin/view/Sandbox/TestTopic2 (unlock [on] )
/twiki/bin/preview/Sandbox/TestTopic2 (formtemplate [] topicparent [] cmd [] )
/twiki/bin/upload/Main/TWikiGroups (filename [] filepath [] filecomment [] creat
↪elink [] hidefile [] )
/twiki/bin/view/Main/WebStatistics (topic [] rev [r1.117] )
/twiki/bin/edit/Main/CoreTeam (topicparent [Main.AndreaSterbini] )
/twiki/bin/view/TWiki/WikiSyntax (topic [] skin [print] rev [1.14] )
/twiki/bin/edit/Sandbox/TestTopic5 (topicparent [Sandbox.WebHome] )
/twiki/bin/edit/Main/WebPreferences (t [1518345651] )
/twiki/bin/view/TWiki/WebChanges (topic [] )
/twiki/bin/view/TWiki/GoodStyle (topic [] skin [print] rev [1.5] )
/twiki/bin/oops/TWiki/DefaultPlugin (template [oopsmore] param1 [1.5] param2 [1.
↪5] )
/twiki/bin/view/TWiki/InterwikiPlugin (topic [] )
/twiki/bin/oops/Know/ReadmeFirst (template [oopsmore] param1 [1.6] param2 [1.6]
↪)
/twiki/bin/view/Sandbox/TestTopic3 (unlock [on] )
/twiki/bin/preview/Sandbox/TestTopic3 (formtemplate [] topicparent [] cmd [] )
/twiki/bin/rdiff/Sandbox/WebNotify (rev1 [1.5] rev2 [1.4] )
/twiki/bin/oops/TWiki/WikiCulture (template [oopsmore] param1 [1.8] param2 [1.8]
↪ )
/twiki/bin/edit/Main/TWikiGuest (t [1518345689] )
/twiki/bin/oops/Main/JohnTalintyre (template [oopsmore] param1 [1.3] param2 [1.3
↪] )
/twiki/bin/view/Main/TWikiVariables (topic [] skin [print] rev [1.2] )
/twiki/bin/view/TWiki/WikiWord (topic [] skin [print] rev [1.3] )
/twiki/bin/upload/Main/WebPreferences (filename [] filepath [] filecomment [] cr
↪eatelink [] hidefile [] )
/twiki/bin/edit/Sandbox/TestTopic6 (topicparent [Sandbox.WebHome] )
/twiki/bin/edit/Main/SupportGroup (topicparent [Main.TWikiGroups] )
/twiki/bin/view/TWiki/WebTopicList (topic [] )
/twiki/bin/edit/TWiki/TWikiShorthand (t [1518345662] )
/twiki/bin/rdiff/TWiki/TWikiGlossary (rev1 [1.2] rev2 [1.1] )
/twiki/bin/edit/TWiki/WikiStyleWord (topicparent [TWiki.TextFormattingFAQ] )
/twiki/bin/view/TWiki/InterWikis (topic [] )
/twiki/bin/view/TWiki/TWikiAdminCookBook (topic [] )
/twiki/bin/view/Main/SupportGroup (unlock [on] )
/twiki/bin/preview/Main/SupportGroup (formtemplate [] topicparent [] cmd [] )
/twiki/bin/oops/Main/SanJoseOffice (template [oopsmore] param1 [1.3] param2 [1.3
↪] )
```

. . . continues on next page . . .

... continued from previous page ...

```
/twiki/bin/view/Main/TokyoOffice (topic [] skin [print] rev [1.2] )
/twiki/bin/rdiff/Main/WebNotify (rev1 [1.7] rev2 [1.6] )
/twiki/bin/oops/Main/WebNotify (template [oopsmore] param1 [1.7] param2 [1.7] )
/twiki/bin/rdiff/Main/NobodyGroup (rev1 [1.2] rev2 [1.1] )
/twiki/bin/edit/Main/JohnTalintyre (t [1518345694] )
/twiki/bin/rdiff/Main/AndreaSterbini (rev1 [1.2] rev2 [1.1] )
/twiki/bin/edit/TWiki/WikiSyntax (t [1518345706] )
/twiki/bin/upload/TWiki/WebHome (filepath [] filecomment [] filename [] hidefile
↪ [] createlink [] )
/twiki/bin/edit/Sandbox/TestTopic7 (topicparent [Sandbox.WebHome] )
/twiki/bin/view/Main/TWikiGroups (topic [] skin [print] rev [1.2] )
/twiki/bin/edit/Main/EngineeringGroup (topicparent [Main.TWikiGroups] )
/twiki/bin/search/Main/SearchResult (search [TWiki%20*Groups%5B%5EA-Za-z%5D] sco
↪pe [text] regex [on] )
/twiki/bin/register/Main/WebHome (Twk1Name [] Twk1WikiName [] Twk1LoginName [] T
↪wk1Email [] Twk0Phone [] Twk0Department [] Twk1Location [] TopicName [TWikiReg
↪istration] )
/twiki/bin/edit/Sandbox/WebChanges (t [1518345657] )
/twiki/bin/edit/TWiki/TWikiSite (t [1518345660] )
/twiki/bin/view/Sandbox/TestTopic5 (unlock [on] )
/twiki/bin/preview/Sandbox/TestTopic5 (formtemplate [] topicparent [] cmd [] )
/twiki/bin/view/Sandbox/WebTopicList (topic [] skin [print] )
/twiki/bin/oops/Sandbox/WebTopicList (template [oopsmore] param1 [1.1] param2 [1
↪.1] )
/twiki/bin/view/Main/CharleytheHorse (topic [] skin [print] rev [r1.1] )
/twiki/bin/oops/Main/CharleytheHorse (param1 [1.1] param2 [1.1] template [oopsmo
↪re] )
/twiki/bin/view/Main/EngineeringGroup (unlock [on] )
/twiki/bin/preview/Main/EngineeringGroup (formtemplate [] topicparent [] cmd []
↪)
/twiki/bin/rdiff/Main/PeterThoeny (rev1 [1.8] rev2 [1.7] )
/twiki/bin/edit/Main/SanJoseOffice (t [1518345685] )
/twiki/bin/view/Main/TWikiGuest (topic [] skin [print] rev [1.4] )
/twiki/bin/rdiff/Main/JohnTalintyre (rev1 [1.3] rev2 [1.2] )
/twiki/bin/attach/TWiki/FileAttachment (filename [Sample.txt] revInfo [1] )
/twiki/bin/oops/Main/GrantBow (param1 [1.1] param2 [1.1] template [oopsmore] )
/twiki/bin/edit/Sandbox/TestTopic8 (topicparent [Sandbox.WebHome] )
/twiki/bin/search/Sandbox/SearchResult (search [] scope [topic] nosearch [on] re
↪verse [on] regex [on] order [modified] )
/twiki/bin/view/Main/OfficeLocations (topic [] skin [print] rev [1.3] unlock [on
↪] )
/twiki/bin/oops/Main/OfficeLocations (template [oopsmore] param1 [1.4] param2 [1
↪.4] )
/twiki/bin/edit/TWiki/StartingPoints (t [1518345653] )
/twiki/bin/rdiff/TWiki/StartingPoints (rev1 [1.3] rev2 [1.2] )
/twiki/bin/rdiff/Sandbox/WebChanges (rev1 [1.2] rev2 [1.1] )
/phpMyAdmin/themes/original/img/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
```

... continues on next page ...

. . . continued from previous page . . .

```
/twiki/bin/view/TWiki/TWikiTutorial (topic [] )
/twiki/bin/edit/TWiki/MeaningfulTitle (topicparent [TWiki.TextFormattingFAQ] )
/twiki/bin/view/Know/WebIndex (topic [] )
/twiki/bin/view/Know/WebStatistics (topic [] )
/twiki/bin/oops/Sandbox/WebIndex (template [oopsmore] param1 [1.2] param2 [1.2]
↪)
/twiki/bin/edit/TWiki/WikiName (t [1518345673] )
/twiki/bin/view/Sandbox/TestTopic6 (unlock [on] )
/twiki/bin/preview/Sandbox/TestTopic6 (formtemplate [] topicparent [] cmd [] )
/twiki/bin/view/Sandbox/WebStatistics (topic [] )
/twiki/bin/rdiff/Main/SanJoseOffice (rev1 [1.3] rev2 [1.2] )
/twiki/bin/edit/Main/TokyoOffice (t [1518345686] )
/twiki/bin/preview/Main/OfficeLocations (formtemplate [] topicparent [] cmd [] )
/twiki/bin/view/Main/JohnTalintyre (topic [] skin [print] rev [1.2] )
/twiki/bin/edit/Main/TWikiVariables (t [1518345695] )
/twiki/bin/view/TWiki/BookView (topic [] skin [print] rev [1.1] )
/twiki/bin/edit/TWiki/WikiReferences (t [1518345705] )
/twiki/bin/rdiff/TWiki/WikiReferences (rev1 [1.2] rev2 [1.1] )
/twiki/bin/view/TWiki/WebHome (topic [] )
/twiki/bin/search/TWiki/ (showlock [] search [] web [] nosearch [] scope [topic]
↪ reverse [] regex [] limit [all] nototal [] order [] nosummary [] bookview []
↪casesensitive [] )
/twiki/bin/edit/Main/TWikiGroups (t [1518345647] )
/twiki/bin/view/TWiki/WelcomeGuest (topic [] )
/twiki/bin/view/TWiki/TWikiRegistration (topic [] skin [print] rev [1.7] )
/twiki/bin/edit/TWiki/TWikiRegistration (t [1518345652] )
/twiki/bin/rdiff/TWiki/TWikiRegistration (rev1 [1.8] rev2 [1.7] )
/twiki/bin/oops/TWiki/TWikiRegistration (template [oopsmore] param1 [1.8] param2
↪ [1.8] )
/twiki/bin/view/Sandbox/WebChanges (topic [] skin [print] )
/twiki/bin/view/TWiki/TWikiSite (topic [] skin [print] )
/twiki/bin/edit/TWiki/NewTopic (topicparent [TWiki.TWikiShorthand] )
/twiki/bin/oops/TWiki/TWikiGlossary (template [oopsmore] param1 [1.2] param2 [1.
↪2] )
/twiki/bin/view/TWiki/DefaultPlugin (topic [] skin [print] rev [1.4] )
/twiki/bin/edit/TWiki/WikiOrg (topicparent [TWiki.TWikiAdminCookBook] )
/twiki/bin/view/Know/WebNotify (topic [] skin [print] rev [1.6] )
/twiki/bin/view/Sandbox/TestTopic7 (unlock [on] )
/twiki/bin/preview/Sandbox/TestTopic7 (formtemplate [] topicparent [] cmd [] )
/twiki/bin/oops/Sandbox/WebNotify (template [oopsmore] param1 [1.5] param2 [1.5]
↪ )
/twiki/bin/view/Main/SanJoseOffice (topic [] skin [print] rev [1.2] )
/twiki/bin/edit/TWiki/TWikiFormTemplate (topicparent [Main.WebPreferences] )
/twiki/bin/oops/Main/AndreaSterbini (param1 [1.2] param2 [1.2] template [oopsmor
↪e] )
/twiki/bin/edit/TWiki/WikiWord (t [1518345704] )
/twiki/bin/edit/TWiki/StandardColors (t [1518345707] )
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
/twiki/bin/rdiff/TWiki/StandardColors (rev1 [1.4] rev2 [1.3] )
/twiki/bin/rdiff/TWiki/SiteMap (rev1 [1.2] rev2 [1.1] )
/twiki/bin/view/TWiki/WebTopicEditTemplate (topic [] skin [print] rev [1.4] )
/twiki/bin/edit/TWiki/WebTopicEditTemplate (t [1518345709] )
/twiki/bin/rdiff/TWiki/WebTopicEditTemplate (rev1 [1.5] rev2 [1.4] )
/twiki/bin/oops/TWiki/WebTopicEditTemplate (template [oopsmore] param1 [1.5] par
↪am2 [1.5] )
/twiki/bin/upload/TWiki/TWikiRegistration (filename [] filepath [] filecomment [
↪] createlink [] hidefile [] )
/twiki/bin/edit/TWiki/WebPreferences (t [1518345654] )
/twiki/bin/rdiff/Know/WebPreferences (rev1 [1.11] rev2 [1.10] )
/twiki/bin/view/Sandbox/TestTopic8 (unlock [on] )
/twiki/bin/preview/Sandbox/TestTopic8 (formtemplate [] topicparent [] cmd [] )
/twiki/bin/view/Main/GrantBow (topic [] skin [print] rev [r1.1] )
/twiki/bin/rdiff/TWiki/WikiSyntax (rev1 [1.15] rev2 [1.14] )
/twiki/bin/edit/TWiki/SiteMap (t [1518345708] )
/dav/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/mutillidae/styles/ddsmoothmenu/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/twiki/bin/view/TWiki/WebSearch (topic [] )
/twiki/bin/search/Sandbox/ (search [%5C.*] web [] nosearch [on] scope [topic] re
↪verse [on] regex [on] nototal [] limit [100] order [modified] nosummary [] boo
↪kview [] casesensitive [] )
/twiki/bin/view/Sandbox/WebSearch (topic [] )
/twiki/bin/view/TWiki/TextFormattingRules (topic [] )
/twiki/bin/view/TWiki/TextFormattingFAQ (topic [] )
/twiki/bin/view/Know/ReadmeFirst (topic [] skin [print] rev [1.5] )
/twiki/bin/view/Main/CccCcc (topic [] skin [print] rev [r1.1] )
/twiki/bin/edit/Main/TWikiRegistration (topicparent [Main.OfficeLocations] )
/twiki/bin/oops/Main/NobodyGroup (param1 [1.2] param2 [1.2] template [oopsmore]
↪)
/twiki/bin/edit/Main/WebTopicNonWikiTemplate (topicparent [Main.TWikiVariables]
↪)
/twiki/bin/edit/Main/TWikiDocumentation (topicparent [Main.FileAttachment] )
/twiki/bin/edit/TWiki/YearTwoThousand (topicparent [TWiki.WikiWord] )
/twiki/bin/rdiff/Main/WebPreferences (rev1 [1.13] rev2 [1.12] )
/twiki/bin/search/TWiki/SearchResult (search [TWiki%20*Registration%5B%5EA-Za-z%
↪5D] scope [text] regex [on] )
/twiki/bin/search/Know/ (search [%54opicClassification.%2ANoDisclosure] web [] s
↪cope [text] regex [on] bookview [] )
/twiki/bin/edit/TWiki/DefaultPlugin (t [1518345667] )
/twiki/bin/edit/Main/TWikiAdminGroup (t [1518345679] )
/twiki/bin/rdiff/Main/TWikiAdminGroup (rev1 [1.7] rev2 [1.6] )
/twiki/bin/oops/Main/PeterThoeny (template [oopsmore] param1 [1.8] param2 [1.8]
↪)
/twiki/bin/rdiff/Main/TokyoOffice (rev1 [1.3] rev2 [1.2] )
/twiki/bin/edit/Main/IncludeTopicsAndWebPages (topicparent [Main.TWikiVariables]
↪ )
```

. . . continues on next page . . .

... continued from previous page ...

```
/twiki/bin/edit/Main/TWikiForms (topicparent [Main.TWikiVariables] )
/twiki/bin/edit/Main/FormattedSearch (topicparent [Main.TWikiVariables] )
/twiki/bin/edit/TWiki/BookView (t [1518345702] )
/twiki/bin/edit/TWiki/AVeryLongWikiTopicNameIsAlsoPossible (topicparent [TWiki.W
↪ikiWord] )
/twiki/bin/rdiff/Main/TWikiGroups (rev1 [1.3] rev2 [1.2] )
/twiki/bin/oops/Know/WebPreferences (template [oopsmore] param1 [1.11] param2 [1
↪.11] )
/twiki/bin/view/TWiki/WebChangesAlert (topic [] skin [print] rev [1.12] )
/twiki/bin/edit/TWiki/WebChangesAlert (t [1518345663] )
/twiki/bin/rdiff/TWiki/WebChangesAlert (rev1 [1.13] rev2 [1.12] )
/twiki/bin/oops/TWiki/WebChangesAlert (template [oopsmore] param1 [1.13] param2
↪[1.13] )
/twiki/bin/rename/TWiki/WebChangesAlert (newweb [TWiki] newtopic [WebChangesNoti
↪fy] confirm [on] )
/twiki/bin/view/TWiki/TWikiGlossary (topic [] skin [print] rev [1.1] )
/twiki/bin/edit/Know/ReadmeFirst (t [1518345670] )
/twiki/bin/edit/Know/WebNotify (t [1518345671] )
/twiki/bin/edit/Main/CccCcc (t [1518345678] )
/twiki/bin/view/Main/WebNotify (topic [] skin [print] rev [1.6] )
/twiki/bin/view/Main/AndreaSterbini (topic [] skin [print] rev [1.1] )
/twiki/bin/oops/TWiki/WikiNotation (template [oopsmore] param1 [1.3] param2 [1.3
↪] )
/twiki/bin/view/Main/TWikiUsers (topic [] rev [r1.16] )
/twiki/bin/view/TWiki/WebIndex (topic [] )
/twiki/bin/view/TWiki/TWikiShorthand (topic [] skin [print] )
/twiki/bin/oops/TWiki/TWikiShorthand (template [oopsmore] param1 [1.1] param2 [1
↪.1] )
/twiki/bin/view/TWiki/TWikiFAQ (topic [] )
/twiki/bin/view/Sandbox/WebIndex (topic [] skin [print] rev [1.1] )
/twiki/bin/rdiff/TWiki/WikiName (rev1 [1.3] rev2 [1.2] )
/twiki/bin/oops/TWiki/WikiName (template [oopsmore] param1 [1.3] param2 [1.3] )
/twiki/bin/view/Main/LondonOffice (topic [] skin [print] rev [1.2] )
/twiki/bin/edit/Main/LondonOffice (t [1518345685] )
/twiki/bin/view/Main/KevinKinnell (topic [] skin [print] rev [1.1] )
/twiki/bin/edit/Main/KevinKinnell (t [1518345697] )
/twiki/bin/view/TWiki/RegularExpression (topic [] skin [print] rev [1.2] )
/twiki/bin/edit/TWiki/RegularExpression (t [1518345703] )
/twiki/bin/rdiff/TWiki/RegularExpression (rev1 [1.3] rev2 [1.2] )
/twiki/bin/oops/TWiki/RegularExpression (template [oopsmore] param1 [1.3] param2
↪ [1.3] )
/twiki/bin/view/TWiki/FormattedSearch (topic [] )
/twiki/bin/edit/TWiki/WikiNotation (t [1518345710] )
/twiki/bin/view/TWiki/FileAttachment (topic [] )
/twiki/bin/rdiff/Main/TWikiVariables (rev1 [1.3] rev2 [1.2] )
/twiki/bin/edit/Main/WikiSyntax (topicparent [Main.TWikiVariables] )
/twiki/bin/viewfile/TWiki/FileAttachment (rev [] filename [Sample.txt] )
```

... continues on next page ...

... continued from previous page ...

```
/twiki/bin/rdiff/TWiki/WikiWord (rev1 [1.4] rev2 [1.3] )
/twiki/bin/oops/TWiki/WikiWord (template [oopsmore] param1 [1.4] param2 [1.4] )
/twiki/bin/oops/TWiki/WikiSyntax (template [oopsmore] param1 [1.15] param2 [1.15
↪] )
/twiki/bin/rdiff/TWiki/WikiNotation (rev1 [1.3] rev2 [1.2] )
/twiki/bin/search/Know/SearchResult (search [] scope [text] regex [on] )
/twiki/bin/view/TWiki/StartingPoints (topic [] skin [print] rev [1.2] )
/twiki/bin/oops/TWiki/StartingPoints (template [oopsmore] param1 [1.3] param2 [1
↪.3] )
/twiki/bin/rdiff/TWiki/GoodStyle (rev1 [1.6] rev2 [1.5] )
/twiki/bin/edit/TWiki/TWikiGlossary (t [1518345664] )
/twiki/bin/edit/Sandbox/WebIndex (t [1518345672] )
/twiki/bin/edit/Sandbox/WebTopicList (t [1518345676] )
/twiki/bin/oops/Main/CccCcc (param1 [1.1] param2 [1.1] template [oopsmore] )
/twiki/bin/edit/Main/CharleytheHorse (t [1518345678] )
/twiki/bin/view/TWiki/WikiCulture (topic [] skin [print] rev [1.7] )
/twiki/bin/edit/TWiki/WikiCulture (t [1518345681] )
/twiki/bin/rdiff/Main/LondonOffice (rev1 [1.3] rev2 [1.2] )
/twiki/bin/view/Main/WebRss (topic [] rev [r1.1] )
/twiki/bin/edit/Main/RegularExpression (topicparent [Main.TWikiVariables] )
/twiki/bin/rdiff/Main/KevinKinnell (rev1 [1.2] rev2 [1.1] )
/twiki/bin/edit/Main/AndreaSterbini (t [1518345698] )
/twiki/bin/view/Main/FileAttachment (topic [] rev [r1.3] )
/twiki/bin/view/TWiki/WikiReferences (topic [] skin [print] rev [1.1] )
/twiki/bin/oops/TWiki/WikiReferences (template [oopsmore] param1 [1.2] param2 [1
↪.2] )
/twiki/bin/view/TWiki/WikiNotation (topic [] skin [print] rev [1.2] )
/twiki/bin/edit/Main/OfficeLocations (t [1518345649] )
/twiki/bin/rdiff/Main/OfficeLocations (rev1 [1.4] rev2 [1.3] )
/twiki/bin/view/Main/WebIndex (topic [] )
/twiki/bin/view/Know/WebSearch (topic [] )
/twiki/bin/view/Know/WebPreferences (topic [] skin [print] rev [1.10] )
/mutillidae/images/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/twiki/bin/edit/TWiki/TWikiTopic (topicparent [TWiki.TWikiTopics] )
/twiki/bin/oops/TWiki/GoodStyle (template [oopsmore] param1 [1.6] param2 [1.6] )
/twiki/bin/rdiff/Know/ReadmeFirst (rev1 [1.6] rev2 [1.5] )
/twiki/bin/oops/Main/TokyoOffice (template [oopsmore] param1 [1.3] param2 [1.3]
↪)
/twiki/bin/upload/Main/OfficeLocations (filename [] filepath [] filecomment [] c
↪reatelink [] hidefile [] )
/twiki/bin/edit/Main/WebNotify (t [1518345692] )
/twiki/bin/view/Main/NobodyGroup (topic [] skin [print] rev [1.1] )
/twiki/bin/view/TWiki/StandardColors (topic [] skin [print] rev [1.3] )
/twiki/bin/oops/TWiki/StandardColors (template [oopsmore] param1 [1.4] param2 [1
↪.4] )
/twiki/bin/view/Main/WebHome (topic [] rev [r1.20] )
/twiki/bin/view/Sandbox/WebHome (topic [] unlock [on] )
```

... continues on next page ...

... continued from previous page ...

```
/twiki/bin/edit/Sandbox/TestTopic1 (topicparent [Sandbox.WebHome] )
/twiki/bin/oops/Main/TWikiGroups (template [oopsmore] param1 [1.3] param2 [1.3]
↪)
/twiki/bin/view/Main/WebChanges (topic [] )
/twiki/bin/edit/Main/WebTopicEditTemplate (topicparent [Main.WebPreferences] )
/twiki/bin/view/TWiki/WebPreferences (topic [] skin [print] )
/twiki/bin/view/TWiki/TWikiForms (topic [] )
/twiki/bin/edit/Sandbox/WebTopicEditTemplate (topicparent [Sandbox.WebPreference
↪s] )
/twiki/bin/view/TWiki/TWikiAccessControl (topic [] )
/twiki/bin/rdiff/TWiki/WikiCulture (rev1 [1.8] rev2 [1.7] )
/twiki/bin/view/Main/PeterThoeny (topic [] skin [print] rev [1.7] )
/twiki/bin/rdiff/Main/TWikiGuest (rev1 [1.5] rev2 [1.4] )
/twiki/bin/edit/Main/WebRss (t [1518345691] )
/twiki/bin/oops/Main/TWikiVariables (template [oopsmore] param1 [1.3] param2 [1.
↪3] )
/twiki/bin/rdiff/TWiki/BookView (rev1 [1.2] rev2 [1.1] )
/twiki/bin/oops/TWiki/BookView (template [oopsmore] param1 [1.2] param2 [1.2] )
/twiki/bin/view/TWiki/SiteMap (topic [] skin [print] rev [1.1] )
/twiki/bin/view/Main/WebTopicEditTemplate (unlock [on] )
/twiki/bin/preview/Main/WebTopicEditTemplate (formtemplate [] topicparent [] cmd
↪ [] )
/phpMyAdmin/index.php (phpMyAdmin [f2c0d1953788da46058606e621f35118023fc6dc] tok
↪en [689e3cdc015be078b06b3e09a8ed5880] pma_username [] table [] lang [] server
↪[1] db [] convcharset [utf-8] pma_password [] )
/twiki/bin/view/Know/WebHome (topic [] )
/twiki/bin/edit/Sandbox/TestTopic2 (topicparent [Sandbox.WebHome] )
/twiki/bin/view/Main/WebPreferences (topic [] skin [print] rev [1.12] )
/twiki/bin/view/Sandbox/WebPreferences (topic [] skin [print] rev [1.9] )
/twiki/bin/edit/Sandbox/WebPreferences (t [1518345658] )
/twiki/bin/rdiff/Sandbox/WebPreferences (rev1 [1.10] rev2 [1.9] )
/twiki/bin/oops/Sandbox/WebPreferences (template [oopsmore] param1 [1.10] param2
↪ [1.10] )
/twiki/bin/rdiff/TWiki/DefaultPlugin (rev1 [1.5] rev2 [1.4] )
/twiki/bin/rdiff/Know/WebNotify (rev1 [1.7] rev2 [1.6] )
/twiki/bin/oops/Know/WebNotify (template [oopsmore] param1 [1.7] param2 [1.7] )
/twiki/bin/oops/Main/TWikiGuest (template [oopsmore] param1 [1.5] param2 [1.5] )
/twiki/bin/edit/Main/NobodyGroup (t [1518345693] )
/twiki/bin/edit/Main/GrantBow (t [1518345701] )
Directory index found at /dav/
Directory index found at /twiki/TWikiDocumentation.html
Directory index found at /phpMyAdmin/themes/original/img/
Directory index found at /mutillidae/styles/
Directory index found at /mutillidae/styles/ddsmoothmenu/
Directory index found at /mutillidae/images/
```

... 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:
/cgi-bin, /doc, /test, /icons, /phpMyAdmin
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: PHP Version Detection

```
Detected PHP version: 5.2.4
Location: tcp/80
CPE: cpe:/a:php:php:5.2.4
Concluded from version identification result:
X-Powered-By: PHP/5.2.4-2ubuntu5.10
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.800109

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

Log (CVSS: 0.0)
NVT: phpMyAdmin Detection

```
Detected phpMyAdmin version: unknown
Location: /phpMyAdmin
CPE: cpe:/a:phpmyadmin:phpmyadmin
Concluded from version identification result:
unknown
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900129

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

```
Detected Apache version: 2.2.8
Location: 80/tcp
CPE: cpe:/a:apache:http_server:2.2.8
Concluded from version identification result:
Server: Apache/2.2.8
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900498

Log (CVSS: 0.0)
NVT: TikiWiki Version Detection

```
Detected TikiWiki version: 1.9.5 under /tikiwiki
Location: /tikiwiki
CPE: cpe:/a:tikiwiki:tikiwiki:1.9.5
Concluded from version identification result:
1.9.5
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.901001

[return to 192.168.1.12]

2.1.29 Log ingreslock (1524/tcp)

Log NVT:
Open port. OID of test routine: 0

[return to 192.168.1.12]

2.1.30 Log ircd (6667/tcp)

Log NVT:
Open port. OID of test routine: 0

Log (CVSS: 0.0) NVT: Identify unknown services with nmap
Nmap service detection result for this port: irc OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 192.168.1.12]

2.1.31 Log postgresql (5432/tcp)

Log NVT:
Open port.

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 0

Log (CVSS: 0.0)
NVT: PostgreSQL Detection

```
Detected PostgreSQL version: 8.3.1
Location: 5432/tcp
CPE: cpe:/a:postgresql:postgresql:8.3.1
Concluded from version identification result:
T versionDg]PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.
↪3 (Ubuntu 4.2.3-2ubuntu4)CSELECTZI
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100151

Log (CVSS: 0.0)
NVT: Services

```
An unknown service is running on this port.
It is usually reserved for Postgres
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: Postgres TLS Detection

```
Summary:
The remote Postgres Server supports TLS.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.105013

Log (CVSS: 0.0)
NVT: Database Open Access Vulnerability

```
Postgresql database can be accessed by remote attackers
```

. . . continues on next page . . .

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.902799

References

```
Other:
  URL:https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_d
↪ss_v1-2.pdf
```

[return to 192.168.1.12]

2.1.32 Log scientia-ssdb (2121/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: FTP Banner Detection

```
Remote FTP server banner :
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.1.12]
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10092

Log (CVSS: 0.0)
NVT: Services

```
An FTP server is running on this port.
Here is its banner :
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.1.12]
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

[return to 192.168.1.12]

2.1.33 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: 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3
```

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_4.7p1 Debian-8ubuntu1
Remote SSH supported authentication: publickey,password
Remote SSH banner:
(not available)
CPE: cpe:/a:openbsd:openssh:4.7p1
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

[return to 192.168.1.12]

2.1.34 Log x11 (6000/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 192.168.1.12]

2.1.35 Log exec (512/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 192.168.1.12]

2.1.36 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

. . . continues on next page . . .

... continued from previous page ...

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)

... continues on next page ...

... continued from previous page ...

```
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 192.168.1.12:
192.168.1.1
192.168.1.12
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.51662

Log (CVSS: 0.0)
NVT: TWiki Version Detection

```
Detected TWiki version: unknown
Location: /twiki
CPE: cpe:/a:twiki:twiki
Concluded from HTTP response.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.800399

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, 3632, 5900, 8009, 8787, 6667, 445, 21, 111, 2049, 22, 6000,
↪23, 512, 513, 25, 514, 1099, 2121, 3306, 139, 1524, 53, 5432
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900239

Log (CVSS: 0.0)
NVT: Anonymous FTP Checking

```
Summary:
This FTP Server allows anonymous logins.
 A host that provides an FTP service may additionally provide Anonymous FTP
 access as well. Under this arrangement, users do not strictly need an account
 on the host. Instead the user typically enters 'anonymous' or 'ftp' when
 prompted for username. Although users are commonly asked to send their email
 address as their password, little to no verification is actually performed on
 the supplied data.
Solution:
If you do not want to share files, you should disable anonymous logins.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900600

References
CVE: CVE-1999-0497

[return to 192.168.1.12]

2.1.37 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 192.168.1.12]

2.1.38 Log shell (514/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 192.168.1.12]

2.1.39 Log smtp (25/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

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

```
Remote SMTP server banner :
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
This is probably: Postfix
Detected Postfix version: unknown
Location: 25/tcp
CPE: cpe:/a:postfix:postfix
```

...continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.10263

Log (CVSS: 0.0)
NVT: SMTP STARTTLS Detection

```
The remote Mailserver supports the STARTTLS command.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103118

Log (CVSS: 0.0)
NVT: Services

```
An SMTP server is running on this port
Here is its banner :
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

[return to 192.168.1.12]

2.1.40 Log domain (53/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: DNS Server Detection

```
Summary:
A DNS Server is running at this Host.
```

... continues on next page ...

... continued from previous page ...

```
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 192.168.1.12]

2.1.41 Log telnet (23/tcp)

Log
NVT:

```
Open port.



OID of test routine: 0
```

Log (CVSS: 0.0)
NVT: Detect Server type and version via Telnet

```
Remote telnet banner :
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


farm login:



OID of test routine: 1.3.6.1.4.1.25623.1.0.10281
```

Log (CVSS: 0.0)
NVT: Services

```
A telnet server seems to be running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

[return to 192.168.1.12]

2.1.42 Log vnc (5900/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 192.168.1.12]

2.1.43 Log ajp13 (8009/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

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

```
Nmap service detection result for this port: ajp13
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 192.168.1.12]

2.1.44 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 192.168.1.12]

2.1.45 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

```
192.168.1.12|cpe:/a:samba:samba:3.0.20
192.168.1.12|cpe:/a:twiki:twiki
192.168.1.12|cpe:/a:postgresql:postgresql:8.3.1
192.168.1.12|cpe:/o:linux:kernel
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810002

[return to 192.168.1.12]

2.1.46 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

```
traceroute:192.168.1.1,192.168.1.12
TCP ports:80,3632,5900,8009,8787,6667,445,21,111,2049,22,6000,23,512,513,25,514,
↪1099,2121,3306,139,1524,53,5432
UDP ports:
```

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.810003

[return to 192.168.1.12]

2.1.47 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 192.168.1.12]

2.1.48 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 192.168.1.12]

2.1.49 Log login (513/tcp)

Log NVT:
Open port. OID of test routine: 0

Log (CVSS: 0.0) NVT: Identify unknown services with nmap
Nmap service detection result for this port: login This is a guess. A confident identification of the service was not possible. OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 192.168.1.12]

2.1.50 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 3.0.20-Debian Detected OS: Unix

. . . continues on next page . . .

. . . continued from previous page . . .

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: 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 192.168.1.12]

2.1.51 Log msgsrvr (8787/tcp)

Log
NVT:

```
Open port.
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 0

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 192.168.1.12]

2.1.52 Log mysql (3306/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Services

```
An unknown service is running on this port.
It is usually reserved for MySQL
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 192.168.1.12]

2.1.53 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 :
 FARM            = This is the computer name registered for workstation services
↪ by a WINS client.
 FARM            = This is the current logged in user registered for this workst
↪ation.
 FARM            = Computer name
 WORKGROUP       = Workgroup / Domain name
 WORKGROUP       = Workgroup / Domain name (part of the Browser elections)
. 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 192.168.1.12]

2.1.54 Log nfs (2049/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 192.168.1.12]

2.1.55 Log rmiregistry (1099/tcp)

Log
NVT:

. . . continues on next page . . .

... continued from previous page ...

```
Open port.


OID of test routine: 0
```

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

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


OID of test routine: 1.3.6.1.4.1.25623.1.0.66286
```

[return to 192.168.1.12]

2.1.56 Log sunrpc (111/tcp)

Log
NVT:

```
Open port.


OID of test routine: 0
```

Log (CVSS: 0.0)
NVT: rpcinfo -p

```
These are the registered RPC programs:
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪TCP
RPC program #100003 version 2 'nfs' (nfsprog) on port 2049/TCP
RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/TCP
RPC program #100003 version 4 'nfs' (nfsprog) on port 2049/TCP
RPC program #100024 version 1 'status' on port 37211/TCP
RPC program #100005 version 1 'mountd' (mount showmount) on port 39574/TCP
RPC program #100005 version 2 'mountd' (mount showmount) on port 39574/TCP
RPC program #100021 version 1 'nlockmgr' on port 42182/TCP
RPC program #100021 version 3 'nlockmgr' on port 42182/TCP
RPC program #100021 version 4 'nlockmgr' on port 42182/TCP
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
```

... continues on next page ...

. . . continued from previous page . . .

```
↪UDP
RPC program #100003 version 2 'nfs' (nfsprog) on port 2049/UDP
RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/UDP
RPC program #100003 version 4 'nfs' (nfsprog) on port 2049/UDP
RPC program #100021 version 1 'nlockmgr' on port 39758/UDP
RPC program #100021 version 3 'nlockmgr' on port 39758/UDP
RPC program #100021 version 4 'nlockmgr' on port 39758/UDP
RPC program #100005 version 1 'mountd' (mount showmount) on port 42563/UDP
RPC program #100005 version 2 'mountd' (mount showmount) on port 42563/UDP
RPC program #100024 version 1 'status' on port 46056/UDP
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11111

[return to 192.168.1.12]
