Summary

This document reports on the results of an automatic security scan. 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.

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 92 results selected by the filtering described above. Before filtering there were 96 results.

Scan started:	**Fri Sep 13 22:32:32 2013**
Scan ended:	Fri Sep 13 22:45:13 2013

Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
10.10.10.10 (www.world-wide-wait.fi)	Sep 13, 22:32:50	Sep 13, 22:45:13	2	8	15	67	0
Total: 1			2	8	15	67	0

Results per Host

Host 10.10.10.10

Scanning of this host started at:	2013-09-13T22:32:50Z
Number of results:	92

Port Summary for Host 10.10.10.10

Service (Port)	Threat Level
http (80/tcp)	High
https (443/tcp)	High
eli (2087/tcp)	Medium
general/tcp	Medium
ssh (22/tcp)	Medium
ftp (21/tcp)	Low
nbx-dir (2096/tcp)	Low
radsec (2083/tcp)	Low

submission (587/tcp)	Low
urd (465/tcp)	Low
general/CPE-T	Log
general/HOST-T	Log
general/icmp	Log
gnunet (2086/tcp)	Log
imap (143/tcp)	Log
imaps (993/tcp)	Log
infowave (2082/tcp)	Log
mysql (3306/tcp)	Log
nbx-ser (2095/tcp)	Log
pop3 (110/tcp)	Log
pop3s (995/tcp)	Log
sunrpc (111/tcp)	Log
trellisagt (2077/tcp)	Log
trellissvr (2078/tcp)	Log

Security Issues for Host 10.10.10.10

http (80/tcp)

High (CVSS: 5.8)

NVT: http TRACE XSS attack (OID: 1.3.6.1.4.1.25623.1.0.11213)

```
 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]
```

References

CVE:	CVE-2004-2320, CVE-2003-1567
BID:	9506, 9561, 11604
Other:	
	URL:http://www.kb.cert.org/vuls/id/867593

https (443/tcp)

High (CVSS: 5.8)

NVT: http TRACE XSS attack (OID: 1.3.6.1.4.1.25623.1.0.11213)

```
 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]
```

References

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

BID: 9506, 9561, 11604

Other:

URL:http://www.kb.cert.org/vuls/id/867593

eli (2087/tcp)

Medium (CVSS: 4.3)

NVT: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)

```
Server supports SSLv2 ciphers.
Server supports SSLv3 ciphers.
Server supports TLSv1 ciphers.
Weak Ciphers
  SSL3_RSA_WITH_SEED_SHA : SSL_NOT_EXP
  TLS1_RSA_WITH_SEED_SHA : SSL_NOT_EXP
```

general/tcp

Medium (CVSS: 5.0)

NVT: TCP Sequence Number Approximation Reset Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902815)

References

CVE: CVE-2004-0230

BID: 10183

Other:

URL:http://www.osvdb.org/4030

URL:http://xforce.iss.net/xforce/xfdb/15886

URL:http://www.us-cert.gov/cas/techalerts/TA04-111A.html

URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55949

URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55950

URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY62006

URL:http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx

URL:http://www.microsoft.com/technet/security/bulletin/ms06-064.mspx

URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html

URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html

general/tcp

Medium (CVSS: 2.6)

NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Paket 1: 341651444
Paket 2: 341652495
```

References

Other:

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

http (80/tcp)

Medium (CVSS: 5.0)

NVT: Apache UserDir Sensitive Information Disclosure (OID: 1.3.6.1.4.1.25623.1.0.10766)

```
An information leak occurs on Apache based web servers
whenever the UserDir module is enabled. The vulnerability allows an external
attacker to enumerate existing accounts by requesting access to their home
directory and monitoring the response.
 Solution:
 1) Disable this feature by changing 'UserDir public_html' (or whatever) to
'UserDir  disabled'.
Or
2) Use a RedirectMatch rewrite rule under Apache -- this works even if there
is no such  entry in the password file, e.g.:
RedirectMatch ^/~(.*)$ http://my-target-webserver.somewhere.org/$1
Or
3) Add into httpd.conf:
ErrorDocument 404 http://localhost/sample.html
ErrorDocument 403 http://localhost/sample.html
(NOTE: You need to use a FQDN inside the URL for it to work properly).
Additional Information:
http://www.securiteam.com/unixfocus/5WP0C1F5FI.html
```

References

CVE: CVE-2001-1013

BID: 3335

http (80/tcp)

Medium (CVSS: 4.3)

NVT: Apache Web Server ETag Header Information Disclosure Weakness (OID: 1.3.6.1.4.1.25623.1.0.103122)

```
 Summary:
 A weakness has been discovered in Apache web servers that are
configured to use the FileETag directive. Due to the way in which
Apache generates ETag response headers, it may be possible for an
attacker to obtain sensitive information regarding server files.
```

```
Specifically, ETag header fields returned to a client contain the
file's inode number.
Exploitation of this issue may provide an attacker with information
that may be used to launch further attacks against a target network.
OpenBSD has released a patch that addresses this issue. Inode numbers
returned from the server are now encoded using a private hash to avoid
the release of sensitive information.
 Solution:
 OpenBSD has released a patch to address this issue.
Novell has released TID10090670 to advise users to apply the available
workaround of disabling the directive in the configuration file for
Apache releases on NetWare. Please see the attached Technical
Information Document for further details.
Information that was gathered:
Inode: 14553109
Size: 111
```

References

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

https (443/tcp)

Medium (CVSS: 5.0)

NVT: Apache UserDir Sensitive Information Disclosure (OID: 1.3.6.1.4.1.25623.1.0.10766)

```
An information leak occurs on Apache based web servers
whenever the UserDir module is enabled. The vulnerability allows an external
attacker to enumerate existing accounts by requesting access to their home
directory and monitoring the response.
 Solution:
 1) Disable this feature by changing 'UserDir public_html' (or whatever) to
'UserDir  disabled'.
Or
2) Use a RedirectMatch rewrite rule under Apache -- this works even if there
is no such  entry in the password file, e.g.:
RedirectMatch ^/~(.*)$ http://my-target-webserver.somewhere.org/$1
Or
3) Add into httpd.conf:
ErrorDocument 404 http://localhost/sample.html
ErrorDocument 403 http://localhost/sample.html
(NOTE: You need to use a FQDN inside the URL for it to work properly).
Additional Information:
http://www.securiteam.com/unixfocus/5WP0C1F5FI.html
```

References

CVE-2001-1013

3335

https (443/tcp)

Medium (CVSS: 4.3)

NVT: Apache Web Server ETag Header Information Disclosure Weakness (OID: 1.3.6.1.4.1.25623.1.0.103122)

```
 Summary:
 A weakness has been discovered in Apache web servers that are
configured to use the FileETag directive. Due to the way in which
Apache generates ETag response headers, it may be possible for an
attacker to obtain sensitive information regarding server files.
Specifically, ETag header fields returned to a client contain the
file's inode number.
Exploitation of this issue may provide an attacker with information
that may be used to launch further attacks against a target network.
OpenBSD has released a patch that addresses this issue. Inode numbers
returned from the server are now encoded using a private hash to avoid
the release of sensitive information.
 Solution:
 OpenBSD has released a patch to address this issue.
Novell has released TID10090670 to advise users to apply the available
workaround of disabling the directive in the configuration file for
Apache releases on NetWare. Please see the attached Technical
Information Document for further details.
Information that was gathered:
Inode: 14553109
Size: 111
```

References

CVE: CVE-2003-1418

BID: 6939

Other:

URL:https://www.securityfocus.com/bid/6939

URL:http://httpd.apache.org/docs/mod/core.html#fileetag

URL:http://www.openbsd.org/errata32.html

URL:http://support.novell.com/docs/Tids/Solutions/10090670.html

ssh (22/tcp)

Medium (CVSS: 3.5)

NVT: openssh-server Forced Command Handling Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103503)

```
According to its banner, the version of OpenSSH installed on the remote
host is older than 5.7:
 ssh-2.0-openssh_5.3
 Summary:
 The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7
provides debug messages containing authorized_keys command options, which allows
remote authenticated users to obtain potentially sensitive information by
reading these messages, as demonstrated by the shared user account required by
Gitolite. NOTE: this can cross privilege boundaries because a user account may
intentionally have no shell or filesystem access, and therefore may have no
supported way to read an authorized_keys file in its own home directory.
OpenSSH before 5.7 is affected;
 Solution:
 Updates are available. Please see the references for more information.
```

References

CVE: CVE-2012-0814

BID: 51702

Other:

URL:http://www.securityfocus.com/bid/51702

URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445

URL:http://packages.debian.org/squeeze/openssh-server

URL:https://downloads.avaya.com/css/P8/documents/100161262

eli (2087/tcp)

Low (CVSS: 0.0)

NVT: No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)

```
This web server is [mis]configured in that it does not return '404 Not Found'
error codes when a non-existent file is requested, perhaps returning
a site map, search page or authentication page instead.
CGI scanning will be disabled for this host.
```

eli (2087/tcp)

Low (CVSS: 0.0)

NVT: Nikto (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.14260)

```
The target server did not return 404 on requests for non-existent pages.
This scan has not been executed since Nikto is prone to reporting many false positives in
↵
this case.
If you wish to force this scan, you can enable it in the Nikto preferences in your client.
```

eli (2087/tcp)

Low (CVSS: 0.0)

NVT: wapiti (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.80110)

```
Here is the wapiti report:
Vulnerabilities report -- Wapiti
  http://wapiti.sourceforge.net/
This report has been generated by Wapiti Web Application Scanner
--- End of report ---
```

ftp (21/tcp)

Low (CVSS: 1.9)

NVT: FTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10092)

```
Remote FTP server banner :
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
```

http (80/tcp)

Low (CVSS: 0.0)

NVT: Mailman Detection (OID: 1.3.6.1.4.1.25623.1.0.16338)

```
Mailman 2.1.15 was detected on the remote host under the path /mailman.
Mailman is a Python-based mailing list management package from the GNU
Project.  See http://www.list.org/ for more information.
```

http (80/tcp)

Low (CVSS: 0.0)

NVT: wapiti (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.80110)

```
Here is the wapiti report:
Vulnerabilities report -- Wapiti
```

```
  http://wapiti.sourceforge.net/
This report has been generated by Wapiti Web Application Scanner
--- End of report ---
```

https (443/tcp)

Low (CVSS: 0.0)

NVT: Mailman Detection (OID: 1.3.6.1.4.1.25623.1.0.16338)

```
Mailman 2.1.15 was detected on the remote host under the path /mailman.
Mailman is a Python-based mailing list management package from the GNU
Project.  See http://www.list.org/ for more information.
```

nbx-dir (2096/tcp)

Low (CVSS: 0.0)

NVT: No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)

```
This web server is [mis]configured in that it does not return '404 Not Found'
error codes when a non-existent file is requested, perhaps returning
a site map, search page or authentication page instead.
CGI scanning will be disabled for this host.
```

nbx-dir (2096/tcp)

Low (CVSS: 0.0)

NVT: Nikto (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.14260)

```
The target server did not return 404 on requests for non-existent pages.
This scan has not been executed since Nikto is prone to reporting many false positives in
↵
this case.
If you wish to force this scan, you can enable it in the Nikto preferences in your client.
```

nbx-dir (2096/tcp)

Low (CVSS: 0.0)

NVT: wapiti (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.80110)

```
Here is the wapiti report:
Vulnerabilities report -- Wapiti
  http://wapiti.sourceforge.net/
This report has been generated by Wapiti Web Application Scanner
--- End of report ---
```

radsec (2083/tcp)

Low (CVSS: 0.0)

NVT: No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)

```
This web server is [mis]configured in that it does not return '404 Not Found'
error codes when a non-existent file is requested, perhaps returning
a site map, search page or authentication page instead.
CGI scanning will be disabled for this host.
```

radsec (2083/tcp)

Low (CVSS: 0.0)

NVT: Nikto (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.14260)

```
The target server did not return 404 on requests for non-existent pages.
```

```
This scan has not been executed since Nikto is prone to reporting many false positives in
↵
this case.
If you wish to force this scan, you can enable it in the Nikto preferences in your client.
```

radsec (2083/tcp)

Low (CVSS: 0.0)

NVT: wapiti (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.80110)

```
Here is the wapiti report:
Vulnerabilities report -- Wapiti
  http://wapiti.sourceforge.net/
This report has been generated by Wapiti Web Application Scanner
--- End of report ---
```

submission (587/tcp)

Low (CVSS: 0.0)

NVT: SMTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10263)

```
Remote SMTP server banner :
220-www.world-wide-wait.fi ESMTP Exim 4.80.1 #2 Sat, 14 Sep 2013 01:33:20 +0300
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
This is probably: Exim version 4.80.1
```

urd (465/tcp)

Low (CVSS: 0.0)

NVT: SMTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10263)

```
Remote SMTP server banner :
220-www.world-wide-wait.fi ESMTP Exim 4.80.1 #2 Sat, 14 Sep 2013 01:33:20 +0300
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
This is probably: Exim version 4.80.1
```

eli (2087/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

eli (2087/tcp)

Log (CVSS: 0.0)

NVT: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

```
The remote web server type is :
cpsrvd/11.38.2.6
```

eli (2087/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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

ftp (21/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

ftp (21/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

```
An FTP server is running on this port.
Here is its banner :
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
```

general/CPE-T

Log (CVSS: 0.0)

NVT: CPE Inventory (OID: 1.3.6.1.4.1.25623.1.0.810002)

```
10.10.10.10|cpe:/a:mysql:mysql:5.5.32-cll
10.10.10.10|cpe:/a:apache:http_server:2.2.24
10.10.10.10|cpe:/a:openbsd:openssh:5.3
10.10.10.10|cpe:/o:linux:kernel
```

general/HOST-T

Log (CVSS: 0.0)

NVT: Host Summary (OID: 1.3.6.1.4.1.25623.1.0.810003)

```
traceroute:192.168.10.236,192.168.10.1,10.10.10.10
TCP
ports:587,2086,80,2087,443,465,110,21,111,993,22,995,2095,2096,2077,2078,3306,2082,143↵
,2083
UDP ports:
```

general/icmp

Log (CVSS: 0.0)

NVT: ICMP Timestamp Detection (OID: 1.3.6.1.4.1.25623.1.0.103190)

```
 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.
```

References

CVE: CVE-1999-0524

Other:

URL:http://www.ietf.org/rfc/rfc0792.txt

general/tcp

Log (CVSS: 0.0)

NVT: OS fingerprinting (OID: 1.3.6.1.4.1.25623.1.0.102002)

```
ICMP based OS fingerprint results: (91% confidence)
Linux Kernel
```

References

Other:

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

general/tcp

Log (CVSS: 0.0)

NVT: Checks for open udp ports (OID: 1.3.6.1.4.1.25623.1.0.103978)

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

general/tcp

Log (CVSS: 0.0)

NVT: arachni (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.110001)

```
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.
```

general/tcp

Log (CVSS: 0.0)

NVT: Traceroute (OID: 1.3.6.1.4.1.25623.1.0.51662)

```
Here is the route from 192.168.10.236 to 10.10.10.10:
192.168.10.236
192.168.10.1
10.10.10.10
```

general/tcp

Log (CVSS: 0.0)

NVT: Checks for open tcp ports (OID: 1.3.6.1.4.1.25623.1.0.900239)

```
Open TCP ports: 587, 2086, 80, 2087, 443, 465, 110, 21, 111, 993, 22, 995, 2095, 2096,
207↵
7, 2078, 3306, 2082, 143, 2083
```

gnunet (2086/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

gnunet (2086/tcp)

Log (CVSS: 0.0)

NVT: Identify unknown services with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)

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

http (80/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

http (80/tcp)

Log (CVSS: 0.0)

NVT: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

```
The remote web server type is :
Apache/2.2.24 (Unix) mod_ssl/2.2.24 OpenSSL/1.0.0-fips mod_bwlimited/1.4
Solution : You can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.
```

http (80/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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

http (80/tcp)

Log (CVSS: 0.0)

NVT: Directory Scanner (OID: 1.3.6.1.4.1.25623.1.0.11032)

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

References

Other:

OWASP:OWASP-CM-006

http (80/tcp)

Log (CVSS: 0.0)

NVT: Apache Web ServerVersion Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)

```
Detected Apache Tomcat version: 2.2.24
Location: 80/tcp
CPE: cpe:/a:apache:http_server:2.2.24
Concluded from version identification result:
Server: Apache/2.2.24
```

https (443/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

https (443/tcp)

Log (CVSS: 0.0)

NVT: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

```
The remote web server type is :
Apache/2.2.24 (Unix) mod_ssl/2.2.24 OpenSSL/1.0.0-fips mod_bwlimited/1.4
Solution : You can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.
```

https (443/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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

https (443/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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

https (443/tcp)

Log (CVSS: 0.0)

NVT: SSL Certificate Expiry (OID: 1.3.6.1.4.1.25623.1.0.15901)

```
The SSL certificate of the remote service is valid between 2011-06-07 00:00:00 and 2014-
09↵
-25 12:00:00 UTC.
```

https (443/tcp)

Log (CVSS: 0.0)

NVT: wapiti (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.80110)

```
wapiti report filename is empty. that could mean that
wrong version of wapiti is used or tmp dir is not accessible.
Make sure to have wapiti 2.x as wapiti 1.x is not supported.
In short: check installation of wapiti and OpenVAS
```

https (443/tcp)

Log (CVSS: 0.0)

NVT: Apache Web ServerVersion Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)

```
Detected Apache Tomcat version: 2.2.24
Location: 443/tcp
CPE: cpe:/a:apache:http_server:2.2.24
Concluded from version identification result:
Server: Apache/2.2.24
```

imap (143/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

imap (143/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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

imap (143/tcp)

Log (CVSS: 0.0)

NVT: IMAP Banner (OID: 1.3.6.1.4.1.25623.1.0.11414)

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

imaps (993/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

imaps (993/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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

imaps (993/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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

imaps (993/tcp)

Log (CVSS: 0.0)

NVT: IMAP Banner (OID: 1.3.6.1.4.1.25623.1.0.11414)

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

imaps (993/tcp)

Log (CVSS: 0.0)

NVT: SSL Certificate Expiry (OID: 1.3.6.1.4.1.25623.1.0.15901)

```
The SSL certificate of the remote service is valid between 2011-06-07 00:00:00 and 2014-
09↵
-25 12:00:00 UTC.
```

infowave (2082/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

mysql (3306/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

mysql (3306/tcp)

Log (CVSS: 0.0)

NVT: MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)

```
Detected MySQL version: 5.5.32-cll
Location: 3306/tcp
CPE: cpe:/a:mysql:mysql:5.5.32-cll
Concluded from version identification result:
5.5.32-cll  «X P\`L;$?P ÿ÷    ▯           U:ccGzO]eb=J mysql_native_password
```

mysql (3306/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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

mysql (3306/tcp)

Log (CVSS: 0.0)

NVT: Database Open Access Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902799)

```
MySQL can be accessed by remote attackers
```

References

Other:

URL:https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf

nbx-dir (2096/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

nbx-dir (2096/tcp)

Log (CVSS: 0.0)

NVT: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

```
The remote web server type is :
cpsrvd/11.38.2.6
```

nbx-dir (2096/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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

nbx-ser (2095/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

pop3 (110/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

pop3 (110/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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

pop3s (995/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

pop3s (995/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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

pop3s (995/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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

pop3s (995/tcp)

Log (CVSS: 0.0)

NVT: SSL Certificate Expiry (OID: 1.3.6.1.4.1.25623.1.0.15901)

```
The SSL certificate of the remote service is valid between 2011-06-07 00:00:00 and 2014-09↵
-25 12:00:00 UTC.
```

radsec (2083/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

radsec (2083/tcp)

Log (CVSS: 0.0)

NVT: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

```
The remote web server type is :
cpsrvd/11.38.2.6
```

radsec (2083/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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

ssh (22/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

ssh (22/tcp)

Log (CVSS: 0.0)

NVT: SSH Protocol Versions Supported (OID: 1.3.6.1.4.1.25623.1.0.100259)

```
The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0
SSHv2 Fingerprint: 99:af:d4:df:f5:4d:be:2f:ac:2a:cb:aa:e1:43:79:07
```

ssh (22/tcp)

Log (CVSS: 0.0)

NVT: SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

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

ssh (22/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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

submission (587/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

submission (587/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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

```
Here is its banner :
220-www.world-wide-wait.fi ESMTP Exim 4.80.1 #2 Sat, 14 Sep 2013 01:33:05 +0300
```

sunrpc (111/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

sunrpc (111/tcp)

Log (CVSS: 0.0)

NVT: Identify unknown services with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)

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

trellisagt (2077/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

trellissvr (2078/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

urd (465/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

urd (465/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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

urd (465/tcp)

Log (CVSS: 0.0)

NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

```
An SMTP server is running on this port through SSL
Here is its banner :
220-www.world-wide-wait.fi ESMTP Exim 4.80.1 #2 Sat, 14 Sep 2013 01:33:04 +0300
```

urd (465/tcp)

Log (CVSS: 0.0)

NVT: SSL Certificate Expiry (OID: 1.3.6.1.4.1.25623.1.0.15901)

```
The SSL certificate of the remote service is valid between 2011-06-07 00:00:00 and 2014-
```

```
09↵
-25 12:00:00 UTC.
```

This file was automatically generated.