Scan Report

February 21, 2018

Summary

This document reports on the results of an automatic security scan. The scan started at Wed Feb 21 09:31:11 2018 UTC and ended at Wed Feb 21 09:48:15 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
192.168.1.10 (rome.secnet)	Severity: High	4	9	1	77	0
Total: 1		4	9	1	77	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 91 results selected by the filtering described above. Before filtering there were 92 results.

2 Results per Host

2.1 192.168.1.10

Host scan start Wed Feb 21 09:31:17 2018 UTC
Host scan end Wed Feb 21 09:48:15 2018 UTC

Service (Port)	Threat Level
http-alt (8080/tcp)	High
imap (143/tcp)	High
pop3 (110/tcp)	High
http-alt (8080/tcp)	Medium
general/tcp	Medium
http (80/tcp)	Medium
imaps (993/tcp)	Medium
microsoft-ds (445/tcp)	Medium
pop3s (995/tcp)	Medium
domain (53/tcp)	Low
http-alt (8080/tcp)	Log
imap (143/tcp)	Log
pop3 (110/tcp)	Log
general/tcp	Log
http (80/tcp)	Log
imaps (993/tcp)	Log
microsoft-ds (445/tcp)	Log
pop3s (995/tcp)	Log
domain (53/tcp)	Log
domain (53/udp)	Log

. . . (continues) . . .

. . . (continued) . . .

Service (Port)	Threat Level
general/CPE-T	Log
general/HOST-T	Log
general/SMBClient	Log
general/icmp	Log
netbios-ns (137/udp)	Log
netbios-ssn (139/tcp)	Log
ssh (22/tcp)	Log

2.1.1 High http-alt (8080/tcp)

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.12085

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

Product detection result

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

```
 Summary:
 Apache Tomcat is prone to multiple remote vulnerabilities including
information-disclosure and denial-of-service issues.
Remote attackers can exploit these issues to cause denial-of-service
conditions or gain access to potentially sensitive information;
information obtained may lead to further attacks.
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
The following versions are affected:
Tomcat 5.5.0 to 5.5.29 Tomcat 6.0.0 to 6.0.27 Tomcat 7.0.0
Tomcat 3.x, 4.x, and 5.0.x may also be affected.
 Solution:
 The vendor released updates. Please see the references for more
information.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100712

References

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

[return to 192.168.1.10]

2.1.2 High imap (143/tcp)

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.105043

References

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

[return to 192.168.1.10]

2.1.3 High pop3 (110/tcp)

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.105043

References

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

[return to 192.168.1.10]

2.1.4 Medium http-alt (8080/tcp)

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

Product detection result

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.103032

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2010-4172
BID:45015
Other:
  URL:https://www.securityfocus.com/bid/45015
   URL:http://tomcat.apache.org/security-6.html
   URL:http://tomcat.apache.org/security-7.html
   URL:http://tomcat.apache.org/security-6.html
   URL:http://tomcat.apache.org/security-7.html
   URL:http://jakarta.apache.org/tomcat/
   URL:http://www.securityfocus.com/archive/1/514866
```

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

Product detection result

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.100598

References

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
    URL:http://www.securityfocus.com/archive/1/510879
```

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

Product detection result

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.901114

References

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

[return to 192.168.1.10]

2.1.5 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: 370915249
Paket 2: 370915357
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80091

References

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

[return to 192.168.1.10]

2.1.6 Medium http (80/tcp)

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.103122

References

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

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

```
  Summary:
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.902830

References

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

[return to 192.168.1.10]

2.1.7 Medium imaps (993/tcp)

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

```
Weak ciphers offered by this service:
  SSL3_RSA_RC4_40_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_RSA_RC2_40_MD5
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
  SSL3_RSA_DES_40_CBC_SHA
  SSL3_EDH_RSA_DES_40_CBC_SHA
  SSL3_ADH_RC4_40_MD5
  SSL3_ADH_RC4_128_MD5
  SSL3_ADH_DES_40_CBC_SHA
  TLS1_RSA_RC4_40_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
  TLS1_RSA_RC2_40_MD5
  TLS1_RSA_DES_40_CBC_SHA
  TLS1_EDH_RSA_DES_40_CBC_SHA
  TLS1_ADH_RC4_40_MD5
  TLS1_ADH_RC4_128_MD5
  TLS1_ADH_DES_40_CBC_SHA
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103440

[return to 192.168.1.10]

2.1.8 Medium microsoft-ds (445/tcp)

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

```
 Summary:
 Samba is prone to multiple remote denial-of-service vulnerabilities.
An attacker can exploit these issues to crash the application, denying
service to legitimate users.
Versions prior to Samba 3.4.8 and 3.5.2 are vulnerable.
 Solution:
 Updates are available. Please see the references for more information.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100644

References

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
    URL:http://samba.org/samba/history/samba-3.5.2.html
    URL:http://www.samba.org
```

[return to 192.168.1.10]

2.1.9 Medium pop3s (995/tcp)

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.103440

[return to 192.168.1.10]

2.1.10 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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
to query for version and type information.  The query of the CHAOS
TXT record 'version.bind', will typically prompt the server to send
the information back to the querying source.
The remote bind version is : 9.7.0-P1
Solution :
Using the 'version' directive in the 'options' section will block
the 'version.bind' query, but it will not log such attempts.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10028

[return to 192.168.1.10]

2.1.11 Log http-alt (8080/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.800371

[return to 192.168.1.10]

2.1.12 Log imap (143/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: IMAP STARTTLS Detection

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.105007

[return to 192.168.1.10]

2.1.13 Log pop3 (110/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

. . . continues on next page . . .

. . . continued from previous page . . .

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: POP3 STARTTLS Detection

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.105008

[return to 192.168.1.10]

2.1.14 Log general/tcp

Log (CVSS: 0.0)
NVT: OS fingerprinting

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

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.102002

References

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

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.103079

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.103978

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.110001

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.14260

Log (CVSS: 0.0)
NVT: Traceroute

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.51662

Log (CVSS: 0.0)
NVT: Simple TCP portscan in NASL

```
Host have 10 TCP port(s) open in given port range.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80112

Log (CVSS: 0.0)
NVT: Simple TCP portscan in NASL

```
This portscanner is EXPERIMENTAL and you should NOT RELY ON it if you don’t know
↪ what you’re doing. If you are sure what you’re doing - you should turn on exp
↪erimental_scripts option in preferences in order to turn off this warning.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80112

Log (CVSS: 0.0)
NVT: Microsoft SMB Signing Disabled

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.802726

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.900239

[return to 192.168.1.10]

2.1.15 Log http (80/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.10107

Log (CVSS: 0.0)
NVT: Directory Scanner

```
The following directories were discovered:
/cgi-bin, /icons
While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11032

References

Other:
  OWASP:OWASP-CM-006

Log (CVSS: 0.0)
NVT: w3af (NASL wrapper)

```
w3af could not be found in your system path.
OpenVAS was unable to execute w3af and to perform the scan you
requested.
Please make sure that w3af is installed and that w3af_console is
available in the PATH variable defined for your environment.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80109

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.80110

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.900498

[return to 192.168.1.10]

2.1.16 Log imaps (993/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

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

```
Service supports SSLv2 ciphers.
Service supports SSLv3 ciphers.
Service supports TLSv1 ciphers.
Medium ciphers offered by this service:
  SSL3_RSA_DES_192_CBC3_SHA
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
  SSL3_EDH_RSA_DES_192_CBC3_SHA
  SSL3_ADH_DES_192_CBC_SHA
  SSL3_DHE_RSA_WITH_AES_128_SHA
  SSL3_ADH_WITH_AES_128_SHA
  TLS1_RSA_DES_192_CBC3_SHA
  TLS1_EDH_RSA_DES_192_CBC3_SHA
  TLS1_ADH_DES_192_CBC_SHA
  TLS1_DHE_RSA_WITH_AES_128_SHA
  TLS1_ADH_WITH_AES_128_SHA
Weak ciphers offered by this service:
  SSL3_RSA_RC4_40_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_DES_40_CBC_SHA
  SSL3_EDH_RSA_DES_40_CBC_SHA
  SSL3_ADH_RC4_40_MD5
  SSL3_ADH_RC4_128_MD5
  SSL3_ADH_DES_40_CBC_SHA
  TLS1_RSA_RC4_40_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
  TLS1_RSA_RC2_40_MD5
  TLS1_RSA_DES_40_CBC_SHA
  TLS1_EDH_RSA_DES_40_CBC_SHA
  TLS1_ADH_RC4_40_MD5
  TLS1_ADH_RC4_128_MD5
  TLS1_ADH_DES_40_CBC_SHA
No non-ciphers are supported by this service
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.802067

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

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
  TLS1_ADH_WITH_AES_128_SHA
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.902816

[return to 192.168.1.10]

2.1.17 Log microsoft-ds (445/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 0

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.102011

Log (CVSS: 0.0)
NVT: SMB log in

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.10394

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.11011

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.804449

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.804449

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.902425

[return to 192.168.1.10]

2.1.18 Log pop3s (995/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

. . . continues on next page . . .

. . . continued from previous page . . .

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

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

```
Service supports SSLv2 ciphers.
Service supports SSLv3 ciphers.
Service supports TLSv1 ciphers.
Medium ciphers offered by this service:
  SSL3_RSA_DES_192_CBC3_SHA
  SSL3_EDH_RSA_DES_192_CBC3_SHA
  SSL3_ADH_DES_192_CBC_SHA
  SSL3_DHE_RSA_WITH_AES_128_SHA
  SSL3_ADH_WITH_AES_128_SHA
  TLS1_RSA_DES_192_CBC3_SHA
  TLS1_EDH_RSA_DES_192_CBC3_SHA
  TLS1_ADH_DES_192_CBC_SHA
  TLS1_DHE_RSA_WITH_AES_128_SHA
  TLS1_ADH_WITH_AES_128_SHA
Weak ciphers offered by this service:
  SSL3_RSA_RC4_40_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_DES_40_CBC_SHA
  SSL3_EDH_RSA_DES_40_CBC_SHA
  SSL3_ADH_RC4_40_MD5
  SSL3_ADH_RC4_128_MD5
  SSL3_ADH_DES_40_CBC_SHA
  TLS1_RSA_RC4_40_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.802067

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.902816

[return to 192.168.1.10]

2.1.19 Log domain (53/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.100069

[return to 192.168.1.10]

2.1.20 Log domain (53/udp)

Log (CVSS: 0.0)
NVT: DNS Server Detection

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.100069

[return to 192.168.1.10]

2.1.21 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

```
192.168.1.10|cpe:/a:samba:samba:3.4.7
192.168.1.10|cpe:/a:apache:tomcat:6.0.24
192.168.1.10|cpe:/a:apache:http_server:2.2.14
192.168.1.10|cpe:/o:linux:kernel
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810002

[return to 192.168.1.10]

2.1.22 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.810003

[return to 192.168.1.10]

2.1.23 Log general/SMBClient

Log (CVSS: 0.0)
NVT: SMB Test

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.90011

[return to 192.168.1.10]

2.1.24 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.103190

References

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

[return to 192.168.1.10]

2.1.25 Log netbios-ns (137/udp)

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

```
The following 7 NetBIOS names have been gathered :
 ROME            = This is the computer name registered for workstation services
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.10150

[return to 192.168.1.10]

2.1.26 Log netbios-ssn (139/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.11011

[return to 192.168.1.10]

2.1.27 Log ssh (22/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.100259

[return to 192.168.1.10]