Scan Report

September 17, 2015

Summary

This document reports on the results of an automatic security scan. The scan started at Thu Sep 17 18:26:58 2015 UTC and ended at Thu Sep 17 18:47:15 2015 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
172.30.0.7	Severity: High	1	0	1	12	0
172.30.0.11	Severity: High	1	2	2	23	0
172.30.0.12	Severity: High	1	2	2	23	0
172.30.0.15	Severity: Medium	0	7	13	43	0
172.30.0.17 (WINVUL)	Severity: High	2	3	4	21	0
Total: 5		5	14	22	122	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 163 results selected by the filtering described above. Before filtering there were 165 results.

2 Results per Host

2.1 172.30.0.7

Host scan start	Thu Sep 17 18:27:03 2015 UTC
Host scan end	Thu Sep 17 18:39:43 2015 UTC

Service (Port)	Threat Level
ms-wbt-server (3389/tcp)	High
ms-wbt-server (3389/tcp)	Low
ms-wbt-server (3389/tcp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/tcp	Log
ssh (22/tcp)	Log

2.1.1 High ms-wbt-server (3389/tcp)

High (CVSS: 6.4)
NVT: Microsoft RDP Server Private Key Information Disclosure Vulnerability

```
Summary:
This host is running Remote Desktop Protocol server and is prone
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
to information disclosure vulnerability.
  Vulnerability Insight:
  The flaw is due to RDP server which stores an RSA private key
used for signing a terminal server's public key in the mstlsapi.dll library,
which allows remote attackers to calculate a valid signature and further
perform a man-in-the-middle (MITM) attacks to obtain sensitive information.
  Impact:
  Successful exploitation could allow remote attackers to gain
sensitive information.
Impact Level: System/Application
  Affected Software/OS:
  Microsoft RDP 5.2 and below
  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.
A Workaround is to connect only to terminal services over trusted networks.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.902658

References

```
CVE: CVE-2005-1794
BID:13818
Other:
  URL:http://secunia.com/advisories/15605/
   URL:http://xforce.iss.net/xforce/xfdb/21954
   URL:http://www.oxid.it/downloads/rdp-gbu.pdf
```

[return to 172.30.0.7]

2.1.2 Low ms-wbt-server (3389/tcp)

Low (CVSS: 0.0)
NVT: Microsoft Remote Desktop Protocol Detection

```
Summary:
The Microsoft Remote Desktop Protocol (RDP) is running at this host. Remote
Desktop Services, formerly known as Terminal Services, is one of the components
of Microsoft Windows (both server and client versions) that allows a user to
access applications and data on a remote computer over a network.
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.100062

[return to 172.30.0.7]

2.1.3 Log ms-wbt-server (3389/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: ms-wbt-server
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 172.30.0.7]

2.1.4 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

```
172.30.0.7|cpe:/a:openbsd:openssh:6.0p1
172.30.0.7|cpe:/o:debian:debian_linux
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810002

[return to 172.30.0.7]

2.1.5 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

```
traceroute:172.30.0.7
TCP ports:22,3389
UDP ports:
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810003

[return to 172.30.0.7]

2.1.6 Log general/tcp

Log (CVSS: 0.0)
NVT: OS fingerprinting

```
ICMP based OS fingerprint results: (92% confidence)
Linux Kernel
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.102002

References

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

Log (CVSS: 0.0)
NVT: 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: Traceroute

```
Here is the route from 172.30.0.7 to 172.30.0.7:
172.30.0.7
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.51662

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

```
Open TCP ports: 22, 3389
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900239

[return to 172.30.0.7]

2.1.7 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
```

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_6.0p1 Debian-4
Remote SSH supported authentication: password,publickey
Remote SSH banner:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
(not available)
CPE: cpe:/a:openbsd:openssh:6.0p1
Concluded from remote connection attempt with credentials:
  Login: OpenVAS
  Password: OpenVAS
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10267

Log (CVSS: 0.0)
NVT: Services

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

[return to 172.30.0.7]

2.2 172.30.0.11

Host scan start	Thu Sep 17 18:27:03 2015 UTC
Host scan end	Thu Sep 17 18:47:15 2015 UTC

Service (Port)	Threat Level
ms-wbt-server (3389/tcp)	High
general/tcp	Medium
http (80/tcp)	Medium
ms-wbt-server (3389/tcp)	Low
http (80/tcp)	Low
ms-wbt-server (3389/tcp)	Log
general/tcp	Log
http (80/tcp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/icmp	Log
ssh (22/tcp)	Log
sunrpc (111/tcp)	Log

2.2.1 High ms-wbt-server (3389/tcp)

High (CVSS: 6.4)
NVT: Microsoft RDP Server Private Key Information Disclosure Vulnerability

```
  Summary:
  This host is running Remote Desktop Protocol server and is prone
to information disclosure vulnerability.
  Vulnerability Insight:
  The flaw is due to RDP server which stores an RSA private key
used for signing a terminal server's public key in the mstlsapi.dll library,
which allows remote attackers to calculate a valid signature and further
perform a man-in-the-middle (MITM) attacks to obtain sensitive information.
  Impact:
  Successful exploitation could allow remote attackers to gain
sensitive information.
Impact Level: System/Application
  Affected Software/OS:
  Microsoft RDP 5.2 and below
  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.
A Workaround is to connect only to terminal services over trusted networks.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.902658

References

```
CVE: CVE-2005-1794
BID:13818
Other:
  URL:http://secunia.com/advisories/15605/
   URL:http://xforce.iss.net/xforce/xfdb/21954
   URL:http://www.oxid.it/downloads/rdp-gbu.pdf
```

[return to 172.30.0.11]

2.2.2 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: 1287975
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Paket 2: 1288238
```

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 172.30.0.11]

2.2.3 Medium http (80/tcp)

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

```
 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: 808357
Size: 177
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103122

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
```

[return to 172.30.0.11]

2.2.4 Low ms-wbt-server (3389/tcp)

Low (CVSS: 0.0)
NVT: Microsoft Remote Desktop Protocol Detection

```
Summary:
The Microsoft Remote Desktop Protocol (RDP) is running at this host. Remote
Desktop Services, formerly known as Terminal Services, is one of the components
of Microsoft Windows (both server and client versions) that allows a user to
access applications and data on a remote computer over a network.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100062

[return to 172.30.0.11]

2.2.5 Low http (80/tcp)

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

```
Here is the Nikto report:
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          172.30.0.11
+ Target Hostname:    172.30.0.11
+ Target Port:        80
+ Start Time:         2015-09-17 18:28:35 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Debian)
+ Server leaks inodes via ETags, header found with file /, inode: 808357, size:
↪177, mtime: 0x4f44902b5470a
+ The anti-clickjacking X-Frame-Options header is not present.
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-682: /webalizer/: Webalizer may be installed. Versions lower than 2.01-0
↪9 vulnerable to Cross Site Scripting (XSS).
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6544 items checked: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2015-09-17 18:30:03 (GMT0) (88 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.14260

[return to 172.30.0.11]

2.2.6 Log ms-wbt-server (3389/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: ms-wbt-server
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 172.30.0.11]

2.2.7 Log general/tcp

Log (CVSS: 0.0)
NVT: OS fingerprinting

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
Linux Kernel
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.102002

References

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

Log (CVSS: 0.0)
NVT: 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: Traceroute

```
Here is the route from 172.30.0.7 to 172.30.0.11:
172.30.0.7
172.30.0.11
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.51662

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

```
Open TCP ports: 80, 111, 22, 3389
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900239

[return to 172.30.0.11]

2.2.8 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/2.2.22 (Debian)
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: DIRB (NASL wrapper)

```
This are the directories/files found with brute force:
http://172.30.0.11:80/
http://172.30.0.11:80/cgi-bin/
http://172.30.0.11:80/icons/
http://172.30.0.11:80/index
http://172.30.0.11:80/index.html
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.103079

Log (CVSS: 0.0)
NVT: Services

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: Directory Scanner

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.11032

References

```
Other:
  OWASP:OWASP-CM-006
```

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

```
wapiti 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
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80110

Log
NVT:

```
Detected Apache version: 2.2.22
Location: 80/tcp
CPE: cpe:/a:apache:http_server:2.2.22
Concluded from version identification result:
Server: Apache/2.2.22
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900498

[return to 172.30.0.11]

2.2.9 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

```
172.30.0.11|cpe:/a:apache:http_server:2.2.22
172.30.0.11|cpe:/a:openbsd:openssh:6.0p1
172.30.0.11|cpe:/o:debian:debian_linux
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810002

[return to 172.30.0.11]

2.2.10 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

```
traceroute:172.30.0.7,172.30.0.11
TCP ports:80,111,22,3389
UDP ports:
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810003

[return to 172.30.0.11]

2.2.11 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 172.30.0.11]

2.2.12 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
```

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_6.0p1 Debian-4
Remote SSH supported authentication: password,publickey
Remote SSH banner:
(not available)
CPE: cpe:/a:openbsd:openssh:6.0p1
Concluded from remote connection attempt with credentials:
  Login: OpenVAS
  Password: OpenVAS
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10267

Log (CVSS: 0.0)
NVT: Services

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

[return to 172.30.0.11]

2.2.13 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 4 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪TCP
RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) on port 111/
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪TCP
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪TCP
RPC program #100024 version 1 'status' on port 39487/TCP
RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪UDP
RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪UDP
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪UDP
RPC program #100024 version 1 'status' on port 41773/UDP
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11111

[return to 172.30.0.11]

2.3 172.30.0.12

Host scan start	Thu Sep 17 18:27:03 2015 UTC
Host scan end	Thu Sep 17 18:47:14 2015 UTC

Service (Port)	Threat Level
ms-wbt-server (3389/tcp)	High
general/tcp	Medium
http (80/tcp)	Medium
ms-wbt-server (3389/tcp)	Low
http (80/tcp)	Low
ms-wbt-server (3389/tcp)	Log
general/tcp	Log
http (80/tcp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/icmp	Log
ssh (22/tcp)	Log
sunrpc (111/tcp)	Log

2.3.1 High ms-wbt-server (3389/tcp)

High (CVSS: 6.4)
NVT: Microsoft RDP Server Private Key Information Disclosure Vulnerability

Summary:

. . . continues on next page . . .

. . . continued from previous page . . .

```
  This host is running Remote Desktop Protocol server and is prone
to information disclosure vulnerability.
  Vulnerability Insight:
  The flaw is due to RDP server which stores an RSA private key
used for signing a terminal server's public key in the mstlsapi.dll library,
which allows remote attackers to calculate a valid signature and further
perform a man-in-the-middle (MITM) attacks to obtain sensitive information.
  Impact:
  Successful exploitation could allow remote attackers to gain
sensitive information.
Impact Level: System/Application
  Affected Software/OS:
  Microsoft RDP 5.2 and below
  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.
A Workaround is to connect only to terminal services over trusted networks.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.902658

References

```
CVE: CVE-2005-1794
BID:13818
Other:
  URL:http://secunia.com/advisories/15605/
   URL:http://xforce.iss.net/xforce/xfdb/21954
   URL:http://www.oxid.it/downloads/rdp-gbu.pdf
```

[return to 172.30.0.12]

2.3.2 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: 1295517
Paket 2: 1295772
```

. . . continues on next page . . .

. . . continued from previous page . . .

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 172.30.0.12]

2.3.3 Medium http (80/tcp)

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

```
 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: 808357
Size: 177
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103122

References

```
CVE: CVE-2003-1418
BID:6939
Other:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
  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
```

[return to 172.30.0.12]

2.3.4 Low ms-wbt-server (3389/tcp)

Low (CVSS: 0.0)
NVT: Microsoft Remote Desktop Protocol Detection

```
 Summary:
 The Microsoft Remote Desktop Protocol (RDP) is running at this host. Remote
 Desktop Services, formerly known as Terminal Services, is one of the components
 of Microsoft Windows (both server and client versions) that allows a user to
 access applications and data on a remote computer over a network.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100062

[return to 172.30.0.12]

2.3.5 Low http (80/tcp)

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

```
Here is the Nikto report:
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          172.30.0.12
+ Target Hostname:    172.30.0.12
+ Target Port:        80
+ Start Time:         2015-09-17 18:28:35 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Debian)
+ Server leaks inodes via ETags, header found with file /, inode: 808357, size:
↪177, mtime: 0x4f44902b5470a
+ The anti-clickjacking X-Frame-Options header is not present.
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6544 items checked: 0 error(s) and 4 item(s) reported on remote host
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
+ End Time:           2015-09-17 18:30:03 (GMT0) (88 seconds)
----------------------------------------------------------------------------
+ 1 host(s) tested
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.14260

[return to 172.30.0.12]

2.3.6 Log ms-wbt-server (3389/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: ms-wbt-server
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 172.30.0.12]

2.3.7 Log general/tcp

Log (CVSS: 0.0)
NVT: OS fingerprinting

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.102002

. . . continues on next page . . .

. . . continued from previous page . . .

References

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

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: Traceroute

```
Here is the route from 172.30.0.7 to 172.30.0.12:
172.30.0.7
172.30.0.12
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.51662

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

```
Open TCP ports: 80, 111, 22, 3389
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.900239

[return to 172.30.0.12]

2.3.8 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/2.2.22 (Debian)
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: DIRB (NASL wrapper)

```
This are the directories/files found with brute force:
http://172.30.0.12:80/
http://172.30.0.12:80/cgi-bin/
http://172.30.0.12:80/icons/
http://172.30.0.12:80/index
http://172.30.0.12:80/index.html
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103079

Log (CVSS: 0.0)
NVT: Services

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: Directory Scanner

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.11032

References

```
Other:
  OWASP:OWASP-CM-006
```

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

```
wapiti 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
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80110

Log
NVT:

```
Detected Apache version: 2.2.22
Location: 80/tcp
CPE: cpe:/a:apache:http_server:2.2.22
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Concluded from version identification result:
Server: Apache/2.2.22
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900498

[return to 172.30.0.12]

2.3.9 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

```
172.30.0.12|cpe:/a:apache:http_server:2.2.22
172.30.0.12|cpe:/a:openbsd:openssh:6.0p1
172.30.0.12|cpe:/o:debian:debian_linux
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810002

[return to 172.30.0.12]

2.3.10 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

```
traceroute:172.30.0.7,172.30.0.12
TCP ports:80,111,22,3389
UDP ports:
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810003

[return to 172.30.0.12]

2.3.11 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 172.30.0.12]

2.3.12 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
```

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_6.0p1 Debian-4
Remote SSH supported authentication: password,publickey
Remote SSH banner:
(not available)
CPE: cpe:/a:openbsd:openssh:6.0p1
Concluded from remote connection attempt with credentials:
  Login: OpenVAS
  Password: OpenVAS
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10267

Log (CVSS: 0.0)
NVT: Services

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

[return to 172.30.0.12]

2.3.13 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 4 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪TCP
RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) on port 111/
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪TCP
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪TCP
RPC program #100024 version 1 'status' on port 58181/TCP
RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪UDP
RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪UDP
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪UDP
RPC program #100024 version 1 'status' on port 56059/UDP
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11111

[return to 172.30.0.12]

2.4 172.30.0.15

Host scan start	Thu Sep 17 18:27:03 2015 UTC
Host scan end	Thu Sep 17 18:39:55 2015 UTC

Service (Port)	Threat Level
epmap (135/tcp)	Medium
general/tcp	Medium
ldap (389/tcp)	Medium
msft-gc (3268/tcp)	Medium
general/tcp	Low
ldap (389/tcp)	Low
msft-gc (3268/tcp)	Low
domain (53/tcp)	Low
ftp (21/tcp)	Low
general/SMBClient	Low
msft-gc-ssl (3269/tcp)	Low
ntp (123/udp)	Low
unknown (5985/tcp)	Low
epmap (135/tcp)	Log
general/tcp	Log
ldap (389/tcp)	Log
msft-gc (3268/tcp)	Log
domain (53/tcp)	Log
ftp (21/tcp)	Log
msft-gc-ssl (3269/tcp)	Log
unknown (5985/tcp)	Log
domain (53/udp)	Log

. . . (continues) . . .

. . . (continued) . . .

Service (Port)	Threat Level
general/CPE-T	Log
general/HOST-T	Log
general/icmp	Log
http-rpc-epmap (593/tcp)	Log
kerberos (88/tcp)	Log
kerberos (88/udp)	Log
kpasswd (464/tcp)	Log
ldaps (636/tcp)	Log
microsoft-ds (445/tcp)	Log
ms-wbt-server (3389/tcp)	Log
unknown (47001/tcp)	Log
unknown (9389/tcp)	Log

2.4.1 Medium epmap (135/tcp)

Medium (CVSS: 5.0)
NVT: DCE Services Enumeration

```
  Summary:
  Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.
An attacker may use this fact to gain more knowledge
about the remote host.
  Solution:
  filter incoming traffic to this port.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10736

Medium (CVSS: 5.0)
NVT: DCE Services Enumeration

```
Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.
An attacker may use this fact to gain more knowledge
about the remote host.
Here is the list of DCE services running on this host:
Port: 49152/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49152]
Port: 49153/tcp
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49153]
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     Annotation: Event log TCPIP
     UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49153]
     Annotation: NRP server endpoint
     UUID: abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49153]
     Annotation: Wcm Service
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49153]
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49153]
     Annotation: DHCP Client LRPC Endpoint
Port: 49154/tcp
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49154]
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49154]
     UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49154]
     Annotation: XactSrv service
     UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49154]
     Annotation: IdSegSrv service
     UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49154]
     Annotation: IKE/Authip API
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49154]
     Annotation: IP Transition Configuration endpoint
     UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49154]
     Annotation: Proxy Manager provider server endpoint
     UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49154]
     Annotation: Proxy Manager client server endpoint
     UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49154]
     Annotation: Adh APIs
     UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49154]
     Annotation: Impl friendly name
     UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49154]
Port: 49155/tcp
     UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49155]
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     Annotation: Impl friendly name
     UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
     Endpoint: ncacn_ip_tcp:172.30.0.15[49155]
     Annotation: MS NT Directory DRS Interface
     UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
     Endpoint: ncacn_ip_tcp:172.30.0.15[49155]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : LSA access
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49155]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_ip_tcp:172.30.0.15[49155]
     Annotation: RemoteAccessCheck
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_ip_tcp:172.30.0.15[49155]
     Annotation: RemoteAccessCheck
     UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49155]
     Named pipe : lsass
     Win32 service or process : Netlogon
     Description : Net Logon service
Port: 49157/tcp
     UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
     Endpoint: ncacn_http:172.30.0.15[49157]
     Annotation: MS NT Directory DRS Interface
     UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
     Endpoint: ncacn_http:172.30.0.15[49157]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : LSA access
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_http:172.30.0.15[49157]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_http:172.30.0.15[49157]
     Annotation: RemoteAccessCheck
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_http:172.30.0.15[49157]
     Annotation: RemoteAccessCheck
     UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
     Endpoint: ncacn_http:172.30.0.15[49157]
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     Named pipe : lsass
     Win32 service or process : Netlogon
     Description : Net Logon service
Port: 49158/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49158]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_ip_tcp:172.30.0.15[49158]
     Annotation: RemoteAccessCheck
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_ip_tcp:172.30.0.15[49158]
     Annotation: RemoteAccessCheck
     UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49158]
     Named pipe : lsass
     Win32 service or process : Netlogon
     Description : Net Logon service
Port: 49159/tcp
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49159]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49159]
     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49159]
     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49159]
     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49159]
Port: 49174/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:172.30.0.15[49174]
Port: 49180/tcp
     UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49180]
     Annotation: Remote Fw APIs
Port: 49184/tcp
     UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5
     Endpoint: ncacn_ip_tcp:172.30.0.15[49184]
     Named pipe : dnsserver
     Win32 service or process : dns.exe
     Description : DNS Server
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Port: 49200/tcp
     UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.15[49200]
     Annotation: Frs2 Service
Solution : filter incoming traffic to this port(s).
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10736

[return to 172.30.0.15]

2.4.2 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: 552927
Paket 2: 553031
```

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 172.30.0.15]

2.4.3 Medium ldap (389/tcp)

Medium (CVSS: 5.0)
NVT: LDAP allows null bases

```
  Summary:
  It is possible to disclose LDAP information.
Description :
Improperly configured LDAP servers will allow the directory BASE
to be set to NULL.  This allows information to be culled without
any prior knowledge of the directory structure.  Coupled with a
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
NULL BIND, an anonymous user can query your LDAP server using a
tool such as 'LdapMiner'
  Solution:
  Disable NULL BASE queries on your LDAP server
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10722

Medium (CVSS: 5.0)
NVT: Use LDAP search request to retrieve information from NT Directory Services

```
 Summary:
 It is possible to disclose LDAP information.
Description :
The directory base of the remote server is set to NULL. This allows information
to be enumerated without any prior knowledge of the directory structure.
 Solution:
 If pre-Windows 2000 compatibility is not required, remove
pre-Windows 2000 compatibility as follows :
- start cmd.exe
- execute the command :
  net localgroup  'Pre-Windows 2000 Compatible Access' everyone /delete
- restart the remote host
Plugin output :
The following information was pulled from the server via a LDAP request:
NTDS Settings,CN=TARWIN2012DC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=
↪Configuration,DC=securelabsondemand,DC=com
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.12105

[return to 172.30.0.15]

2.4.4 Medium msft-gc (3268/tcp)

Medium (CVSS: 5.0)
NVT: LDAP allows null bases

```
  Summary:
  It is possible to disclose LDAP information.
Description :
Improperly configured LDAP servers will allow the directory BASE
to be set to NULL.  This allows information to be culled without
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
any prior knowledge of the directory structure.  Coupled with a
NULL BIND, an anonymous user can query your LDAP server using a
tool such as 'LdapMiner'
  Solution:
  Disable NULL BASE queries on your LDAP server
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10722

Medium (CVSS: 5.0)
NVT: Use LDAP search request to retrieve information from NT Directory Services

```
 Summary:
 It is possible to disclose LDAP information.
Description :
The directory base of the remote server is set to NULL. This allows information
to be enumerated without any prior knowledge of the directory structure.
 Solution:
 If pre-Windows 2000 compatibility is not required, remove
pre-Windows 2000 compatibility as follows :
- start cmd.exe
- execute the command :
  net localgroup  'Pre-Windows 2000 Compatible Access' everyone /delete
- restart the remote host
Plugin output :
The following information was pulled from the server via a LDAP request:
NTDS Settings,CN=TARWIN2012DC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=
↪Configuration,DC=securelabsondemand,DC=com
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.12105

[return to 172.30.0.15]

2.4.5 Low general/tcp

Low (CVSS: 0.0)
NVT: FileZilla Server Version Detection

```
FileZilla Server version 0.9.43 was detected on the host
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.900518

[return to 172.30.0.15]

2.4.6 Low ldap (389/tcp)

Low
NVT:

```
Summary:
A LDAP Server is running at this host.
 The Lightweight Directory Access Protocol, or LDAP is an application
 protocol for querying and modifying directory services running over
 TCP/IP.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100082

[return to 172.30.0.15]

2.4.7 Low msft-gc (3268/tcp)

Low
NVT:

```
Summary:
A LDAP Server is running at this host.
 The Lightweight Directory Access Protocol, or LDAP is an application
 protocol for querying and modifying directory services running over
 TCP/IP.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100082

[return to 172.30.0.15]

2.4.8 Low domain (53/tcp)

Low (CVSS: 0.0)
NVT: Microsoft DNS server internal hostname disclosure detection

. . . continues on next page . . .

. . . continued from previous page . . .

```
Microsoft DNS server seems to be running on this port.

Internal hostname disclosed (0.in-addr.arpa/SOA/IN): tarwin2012dc.securelabsonde
↪mand.com
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100950

References

```
Other:
  URL:http://www.openvas.org/blog.php?id=31
```

Low (CVSS: 0.0)
NVT: Microsoft DNS server internal hostname disclosure detection

```
Microsoft DNS server seems to be running on this port.

Internal hostname disclosed (255.in-addr.arpa/SOA/IN): tarwin2012dc.securelabson
↪demand.com
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100950

References

```
Other:
  URL:http://www.openvas.org/blog.php?id=31
```

[return to 172.30.0.15]

2.4.9 Low ftp (21/tcp)

Low (CVSS: 1.9)
NVT: FTP Server type and version

```
Remote FTP server banner :
220-FileZilla Server version 0.9.43 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit http://sourceforge.net/projects/filezilla/
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.10092

[return to 172.30.0.15]

2.4.10 Low general/SMBClient

Low (CVSS: 0.0)
NVT: SMB Test

```
OS Version = WINDOWS SERVER 2012 R2 STANDARD 9600
Domain = SECURELABSONDEM
SMB Serverversion = WINDOWS SERVER 2012 R2 STANDARD 6.3
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.90011

Low (CVSS: 0.0)
NVT: SMB Test

```
OS Version = WINDOWS SERVER 2012 R2 STANDARD 9600
Domain = SECURELABSONDEM
SMB Serverversion = Windows Server 2012 R2 Standard 6.3
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.90011

Low (CVSS: 0.0)
NVT: SMB Test

```
OS Version = Windows Server 2012 R2 Standard 9600
Domain = SECURELABSONDEM
SMB Serverversion = WINDOWS SERVER 2012 R2 STANDARD 6.3
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.90011

Low (CVSS: 0.0)
NVT: SMB Test

```
OS Version = Windows Server 2012 R2 Standard 9600
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Domain = SECURELABSONDEM
SMB Serverversion = Windows Server 2012 R2 Standard 6.3
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.90011

[return to 172.30.0.15]

2.4.11 Low msft-gc-ssl (3269/tcp)

Low (CVSS: 0.0)
NVT: Check open ports

```
This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by a plugin
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10919

[return to 172.30.0.15]

2.4.12 Low ntp (123/udp)

Low (CVSS: 0.0)
NVT: NTP read variables

```
  Summary:
  A NTP (Network Time Protocol) server is listening on this port.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10884

[return to 172.30.0.15]

2.4.13 Low unknown (5985/tcp)

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

```
Here is the Nikto report:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          172.30.0.15
+ Target Hostname:    172.30.0.15
+ Target Port:        5985
+ Start Time:         2015-09-17 18:29:08 (GMT0)
---------------------------------------------------------------------------
+ Server: Microsoft-HTTPAPI/2.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 6544 items checked: 0 error(s) and 1 item(s) reported on remote host
+ End Time:           2015-09-17 18:30:26 (GMT0) (78 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.14260

[return to 172.30.0.15]

2.4.14 Log epmap (135/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 172.30.0.15]

2.4.15 Log general/tcp

Log (CVSS: 0.0)
NVT: OS fingerprinting

```
ICMP based OS fingerprint results: (83% confidence)
Microsoft Windows
```

. . . 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: 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: Traceroute

```
Here is the route from 172.30.0.7 to 172.30.0.15:
172.30.0.7
172.30.0.15
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.51662

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
Open TCP ports: 3269, 464, 5985, 445, 593, 21, 9389, 636, 135, 47001, 88, 389, 3
↪389, 53, 3268
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900239

[return to 172.30.0.15]

2.4.16 Log ldap (389/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 172.30.0.15]

2.4.17 Log msft-gc (3268/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: ldap
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 172.30.0.15]

2.4.18 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.
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 172.30.0.15]

2.4.19 Log ftp (21/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Services

```
An FTP 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 172.30.0.15]

2.4.20 Log msft-gc-ssl (3269/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: tcpwrapped
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 172.30.0.15]

2.4.21 Log unknown (5985/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 :
Microsoft-HTTPAPI/2.0
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.10107

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

```
This are the directories/files found with brute force:
http://172.30.0.15:5985/
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103079

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: wapiti (NASL wrapper)

```
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
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80110

[return to 172.30.0.15]

2.4.22 Log domain (53/udp)

Log (CVSS: 0.0)
NVT: DNS Server Detection

. . . continues on next page . . .

. . . continued from previous page . . .

```
 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 172.30.0.15]

2.4.23 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

```
172.30.0.15|cpe:/a:filezilla:filezilla_server:0.9.43
172.30.0.15|cpe:/o:microsoft:windows
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810002

[return to 172.30.0.15]

2.4.24 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

```
traceroute:172.30.0.7,172.30.0.15
TCP ports:3269,464,5985,445,593,21,9389,636,135,47001,88,389,3389,53,3268
UDP ports:
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810003

[return to 172.30.0.15]

2.4.25 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 172.30.0.15]

2.4.26 Log http-rpc-epmap (593/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 172.30.0.15]

2.4.27 Log kerberos (88/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Kerberos Detection

```
A Kerberos Server is running at this port.
Realm: SECURELABSONDEMAND.COM
Server time: 2015-09-17 18:29:14
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103854

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

```
Nmap service detection result for this port: kerberos-sec
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 172.30.0.15]

2.4.28 Log kerberos (88/udp)

Log (CVSS: 0.0)
NVT: Kerberos Detection

```
A Kerberos Server is running at this port.
Server time: 2015-09-17 18:29:14
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103854

[return to 172.30.0.15]

2.4.29 Log kpasswd (464/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: kpasswd5
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 172.30.0.15]

2.4.30 Log ldaps (636/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 172.30.0.15]

2.4.31 Log microsoft-ds (445/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

. . . continues on next page . . .

. . . continued from previous page . . .

```
 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: SECURELABSONDEM
Detected SMB server: Windows Server 2012 R2 Standard 6.3
Detected OS: Windows Server 2012 R2 Standard 9600
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.102011

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

[return to 172.30.0.15]

2.4.32 Log ms-wbt-server (3389/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Services

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

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

```
No medium ciphers are supported by this service
No weak ciphers are supported by this service
No non-ciphers are supported by this service
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103441

Log (CVSS: 0.0)
NVT: SSL Certificate Expiry

```
The SSL certificate of the remote service is valid between 2015-09-16 16:56:25 a
↪nd 2016-03-17 16:56:25 UTC.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.15901

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

```
Nmap service detection result for this port: ms-wbt-server
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

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

```
No medium ciphers are supported by this service
No weak ciphers are supported by this service
No non-ciphers are supported by this service
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.802067

[return to 172.30.0.15]

2.4.33 Log unknown (47001/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 172.30.0.15]

2.4.34 Log unknown (9389/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 172.30.0.15]

2.5 172.30.0.17

Host scan start	Thu Sep 17 18:27:03 2015 UTC
Host scan end	Thu Sep 17 18:35:00 2015 UTC

Service (Port)	Threat Level
microsoft-ds (445/tcp)	High
epmap (135/tcp)	Medium
general/tcp	Medium
general/SMBClient	Low
microsoft-ds (445/tcp)	Log
epmap (135/tcp)	Log
general/tcp	Log
general/CPE-T	Log
general/HOST-T	Log
general/icmp	Log
ms-wbt-server (3389/tcp)	Log
netbios-ns (137/udp)	Log
netbios-ssn (139/tcp)	Log

2.5.1 High microsoft-ds (445/tcp)

High (CVSS: 10.0)
NVT: Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability

```
  Summary:
  This host is missing a critical security update according to
  Microsoft Bulletin MS09-050.
  Vulnerability Insight:
  Multiple vulnerabilities exists,
  - A denial of service vulnerability exists in the way that Microsoft Server
    Message Block (SMB) Protocol software handles specially crafted SMB version
    2 (SMBv2) packets.
  - Unauthenticated remote code execution vulnerability exists in the way
    that Microsoft Server Message Block (SMB) Protocol software handles
    specially crafted SMB packets.
  Impact:
  An attacker can exploit this issue to execute code with SYSTEM-level
  privileges; failed exploit attempts will likely cause denial-of-service
  conditions.
  Impact Level: System
  Affected Software/OS:
  - Windows 7 RC
  - Windows Vista and
  - Windows 2008 Server
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900965

References

```
CVE: CVE-2009-2526, CVE-2009-2532, CVE-2009-3103
BID:36299
Other:
  URL:http://www.microsoft.com/technet/security/bulletin/MS09-050.mspx
```

High (CVSS: 10.0)
NVT: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)

```
  Summary:
  This host is missing a critical security update according to
  Microsoft Bulletin MS10-012.
  Vulnerability Insight:
  - An input validation error exists while processing SMB requests and can
    be exploited to cause a buffer overflow via a specially crafted SMB packet.
  - An error exists in the SMB implementation while parsing SMB packets during
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
    the Negotiate phase causing memory corruption via a specially crafted SMB
    packet.
  - NULL pointer dereference error exists in SMB while verifying the 'share'
    and 'servername' fields in SMB packets causing denial of service.
  - A lack of cryptographic entropy when the SMB server generates challenges
    during SMB NTLM authentication and can be exploited to bypass the
    authentication mechanism.
  Impact:
  Successful exploitation will allow remote attackers to execute arbitrary
  code or cause a denial of service or bypass the authentication mechanism
  via brute force technique.
  Impact Level: System/Application
  Affected Software/OS:
  Microsoft Windows 7
  Microsoft Windows 2000 Service Pack and prior
  Microsoft Windows XP Service Pack 3 and prior
  Microsoft Windows Vista Service Pack 2 and prior
  Microsoft Windows Server 2003 Service Pack 2 and prior
  Microsoft Windows Server 2008 Service Pack 2 and prior
  Solution:
  Run Windows Update and update the listed hotfixes or download and
  update mentioned hotfixes in the advisory from the below link,
  http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.902269

References

```
CVE: CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, CVE-2010-0231
Other:
  URL:http://secunia.com/advisories/38510/
   URL:http://support.microsoft.com/kb/971468
   URL:http://www.vupen.com/english/advisories/2010/0345
   URL:http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx
```

[return to 172.30.0.17]

2.5.2 Medium epmap (135/tcp)

Medium (CVSS: 5.0)
NVT: DCE Services Enumeration

```
  Summary:
  Distributed Computing Environment (DCE) services running on the remote host
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
can be enumerated by connecting on port 135 and doing the appropriate queries.
An attacker may use this fact to gain more knowledge
about the remote host.
  Solution:
  filter incoming traffic to this port.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10736

Medium (CVSS: 5.0)
NVT: DCE Services Enumeration

```
Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.
An attacker may use this fact to gain more knowledge
about the remote host.
Here is the list of DCE services running on this host:
Port: 49152/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.17[49152]
Port: 49153/tcp
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.17[49153]
     Annotation: Event log TCPIP
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.17[49153]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.17[49153]
     Annotation: DHCPv6 Client LRPC Endpoint
Port: 49154/tcp
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.17[49154]
     UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.17[49154]
     Annotation: IKE/Authip API
     UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.17[49154]
     Annotation: Impl friendly name
     UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.17[49154]
Port: 49155/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.17[49155]
     Named pipe : lsass
     Win32 service or process : lsass.exe
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     Description : SAM access
Port: 49156/tcp
     UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.17[49156]
     Annotation: Remote Fw APIs
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:172.30.0.17[49156]
     Annotation: IPSec Policy agent endpoint
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
Port: 49157/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:172.30.0.17[49157]
Solution : filter incoming traffic to this port(s).
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10736

[return to 172.30.0.17]

2.5.3 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: 551284
Paket 2: 551388
```

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 172.30.0.17]

2.5.4 Low general/SMBClient

Low (CVSS: 0.0)
NVT: SMB Test

```
OS Version = WINDOWS SERVER (R) 2008 STANDARD 6001 SERVICE PACK 1
Domain = WORKGROUP
SMB Serverversion = WINDOWS SERVER (R) 2008 STANDARD 6.0
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.90011

Low (CVSS: 0.0)
NVT: SMB Test

```
OS Version = WINDOWS SERVER (R) 2008 STANDARD 6001 SERVICE PACK 1
Domain = WORKGROUP
SMB Serverversion = Windows Server (R) 2008 Standard 6.0
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.90011

Low (CVSS: 0.0)
NVT: SMB Test

```
OS Version = Windows Server (R) 2008 Standard 6001 Service Pack 1
Domain = WORKGROUP
SMB Serverversion = WINDOWS SERVER (R) 2008 STANDARD 6.0
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.90011

Low (CVSS: 0.0)
NVT: SMB Test

```
OS Version = Windows Server (R) 2008 Standard 6001 Service Pack 1
Domain = WORKGROUP
SMB Serverversion = Windows Server (R) 2008 Standard 6.0
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.90011

[return to 172.30.0.17]

2.5.5 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: Windows Server (R) 2008 Standard 6.0
Detected OS: Windows Server (R) 2008 Standard 6001 Service Pack 1
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.102011

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

[return to 172.30.0.17]

2.5.6 Log epmap (135/tcp)

Log
NVT:

```
Open port.
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 0

[return to 172.30.0.17]

2.5.7 Log general/tcp

Log (CVSS: 0.0)
NVT: OS fingerprinting

```
ICMP based OS fingerprint results: (83% confidence)
Microsoft Windows
```

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: 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: Traceroute

```
Here is the route from 172.30.0.7 to 172.30.0.17:
172.30.0.7
172.30.0.17
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.51662

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.802726

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

```
Open TCP ports: 445, 135, 3389, 139
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900239

[return to 172.30.0.17]

2.5.8 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

```
172.30.0.17|cpe:/o:microsoft:windows
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810002

[return to 172.30.0.17]

2.5.9 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

```
traceroute:172.30.0.7,172.30.0.17
TCP ports:445,135,3389,139
UDP ports:
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810003

[return to 172.30.0.17]

2.5.10 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 172.30.0.17]

2.5.11 Log ms-wbt-server (3389/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Services

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

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

```
No medium ciphers are supported by this service
No weak ciphers are supported by this service
No non-ciphers are supported by this service
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103441

Log (CVSS: 0.0)
NVT: SSL Certificate Expiry

```
The SSL certificate of the remote service is valid between 2015-09-16 16:56:18 a
↪nd 2016-03-17 16:56:18 UTC.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.15901

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

```
Nmap service detection result for this port: ms-wbt-server
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

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

```
No medium ciphers are supported by this service
No weak ciphers are supported by this service
No non-ciphers are supported by this service
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.802067

[return to 172.30.0.17]

2.5.12 Log netbios-ns (137/udp)

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

```
The following 3 NetBIOS names have been gathered :
 WINVUL          = This is the computer name registered for workstation services
↪ by a WINS client.
 WORKGROUP       = Workgroup / Domain name
 WINVUL          = Computer name
The remote host has the following MAC address on its adapter :
   f2:22:82:ac:da:e2
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 172.30.0.17]

2.5.13 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 172.30.0.17]

This file was automatically generated.