Lab 5 Nessus Vulnerability Scan Report

This handout is a printout of the results of a Nessus vulnerability scan. The scan was performed on the mock IT infrastructure in the lab environment for the Jones & Bartlett Learning *Managing Risk in Information Systems* course.

Source: Lab environment

Content Last Verified: 2014-7-25

List of hosts

172.16.20.1	Low Severity problem(s) found
172.17.20.1	High Severity problem(s) found
172.18.20.1	High Severity problem(s) found
172.19.20.1	Low Severity problem(s) found
172.20.20.1	High Severity problem(s) found
172.30.0.10	High Severity problem(s) found
172.30.0.66	High Severity problem(s) found

[^] Back

172.16.20.1

Scan Time

Start time :	Thu Aug 05 11:34:38 2010
End time :	Thu Aug 05 11:36:50 2010

Number of vulnerabilities

Open ports :	2
High :	0
Medium :	0
Low :	2

Remote host information

Operating System :
NetBIOS name :
DNS name :

[^] Back to 172.16.20.1

Port general (0/icmp) [-/+]

ICMP Timestamp Request Remote Date Disclosure

Synopsis:
It is possible to determine the exact time set on the remote host.

Description:
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols.

Risk factor:
None

Solution:
Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Plugin output:
This host returns non-standard timestamps (high bit is set)

Plugin ID:
10114

CVE:
CVE-1999-0524

Other references:
OSVDB:94

Nessus Scan Information

Information about this scan : Nessus version : 4.2.2 (Build 9129) Plugin feed version : 201007191034 Type of plugin feed : HomeFeed (Non-commercial use only) Scanner IP : 172.30.0.67 Port scanner(s) : nessus_syn_scanner Port range : default Thorough tests : no Experimental tests : no Paranoia level : 1 Report Verbosity : 1 Safe checks : no Optimize the test : yes CGI scanning : disabled Web application tests : disabled Max hosts : 80 Max checks : 5 Recv timeout : 5 Backports : None Scan Start Date : 2010/8/5 11:34 Scan duration : 132 sec

Plugin ID:
19506

[^] Back to 172.16.20.1

[^] Back

172.17.20.1

Scan Time

Start time :	Thu Aug 05 11:34:38 2010
End time :	Thu Aug 05 11:37:36 2010

Number of vulnerabilities

Open ports :	5
High :	1
Medium :	0
Low :	8

Remote host information

Operating System :	KYOCERA Printer
NetBIOS name :	
DNS name :	

[^] Back to 172.17.20.1

Port general (0/icmp) [-/+]

ICMP Timestamp Request Remote Date Disclosure

Synopsis:
It is possible to determine the exact time set on the remote host.

Description:
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols.

Risk factor:
None

Solution:

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Plugin output:
This host returns non-standard timestamps (high bit is set)

Plugin ID:
10114

CVE:
CVE-1999-0524

Other references:
OSVDB:94

OS Identification

Remote operating system : KYOCERA Printer Confidence Level : 65 Method : SinFP Not all fingerprints could give a match - please email the following to os-signatures@nessus.org : NTP:!:UNIX SinFP: P1:B11013:F0x12:W4128:O0204ffff:M536: P2:B11013:F0x12:W4128:O0204ffff:M536: P3:B01023:F0x14:W5840:O0:M0 P4:4202_7_p=23R The remote host is running KYOCERA Printer

Plugin ID:
11936

Nessus Scan Information

Information about this scan : Nessus version : 4.2.2 (Build 9129) Plugin feed version : 201007191034 Type of plugin feed : HomeFeed (Non-commercial use only) Scanner IP : 172.30.0.67 Port scanner(s) : nessus_syn_scanner Port range : default Thorough tests : no Experimental tests : no Paranoia level : 1 Report Verbosity : 1 Safe checks : no Optimize the test : yes CGI scanning : disabled Web application tests : disabled Max hosts : 80 Max checks : 5 Recv timeout : 5 Backports : None Scan Start Date : 2010/8/5 11:34 Scan duration : 178 sec

Plugin ID:
19506

Traceroute Information

Synopsis:
It was possible to obtain traceroute information.

Description:
Makes a traceroute to the remote host.

Risk factor:
None

Solution:
n/a

Plugin output:
For your information, here is the traceroute from 172.30.0.67 to 172.17.20.1 : 172.30.0.67 172.20.20.1 172.20.0.2 172.17.20.1

Plugin ID:
10287

Port ntp (123/udp) [-/+]

Network Time Protocol (NTP) Server Detection

Synopsis:
An NTP server is listening on the remote host.

Description:
An NTP (Network Time Protocol) server is listening on this port. It provides information about the current date and time of the remote system and may provide system information.

Risk factor:
None

Solution:
n/a

Plugin output:
It was possible to gather the following information from the remote NTP host : version='4', processor='unknown', system='UNIX', leap=3, stratum=16, precision=-24, rootdelay=0.000, rootdispersion=44898.809, peer=0, refid=INIT, reftime=0x00000000.00000000, poll=6, clock=0xD00558E5.B0D6A347, state=1, offset=0.000, frequency=0.000, jitter=0.000, noise=0.000, stability=0.000

Plugin ID:
10884

Port telnet (23/tcp) [-/+]

Cisco Device Default Password

Synopsis:
The remote device has a factory password set.

Description:
The remote CISCO router has a default password set. This allows an attacker to get a lot information about the network, and possibly to shut it down if the 'enable' password is not set either or is also a default password.

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:
Access this device and set a password using 'enable secret'

Plugin output:
Plugin Output : It was possible to log in as 'cisco'/'cisco'

Plugin ID:
23938

CVE:
CVE-1999-0508

Service Detection

A telnet server is running on this port.

Plugin ID:
22964

Unencrypted Telnet Server

Synopsis:
The remote Telnet server transmits traffic in cleartext.

Description:
The remote host is running a Telnet server over an unencrypted channel. Using Telnet over an unencrypted channel is not recommended as logins, passwords and commands are transferred in cleartext. An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information. Use of SSH is prefered nowadays as it protects credentials from eavesdropping and can tunnel additional data streams such as the X11 session.

Risk factor:
Low

CVSS Base Score:2.6
CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Solution:
Disable this service and use SSH instead.

Plugin ID:
42263

Telnet Server Detection

Synopsis:
A Telnet server is listening on the remote port.

Description:
The remote host is running a Telnet server, a remote terminal server.

Risk factor:
None

Solution:
Disable this service if you do not use it.

Plugin output:
Here is the banner from the remote Telnet server : ---------- snip ----------
--- User Access Verification Username: ---------- snip ----------

Plugin ID:
10281

[^] Back to 172.17.20.1

[^] Back

172.18.20.1

Scan Time

Start time :	Thu Aug 05 11:34:38 2010
End time :	Thu Aug 05 11:37:35 2010

Number of vulnerabilities

Open ports :	5
High :	1
Medium :	0
Low :	8

Remote host information

Operating System :	KYOCERA Printer
NetBIOS name :	
DNS name :	

[^] Back to 172.18.20.1

Port general (0/icmp) [-/+]

ICMP Timestamp Request Remote Date Disclosure

Synopsis:
It is possible to determine the exact time set on the remote host.

Description:
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols.

Risk factor:
None

Solution:
Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Plugin output:
This host returns non-standard timestamps (high bit is set)

Plugin ID:
10114

CVE:
CVE-1999-0524

Other references:
OSVDB:94

OS Identification

Remote operating system : KYOCERA Printer Confidence Level : 65 Method : SinFP Not all fingerprints could give a match - please email the following to os-signatures@nessus.org : NTP:!:UNIX SinFP: P1:B11013:F0x12:W4128:O0204ffff:M536: P2:B11013:F0x12:W4128:O0204ffff:M536: P3:B01023:F0x14:W5840:O0:M0 P4:4202_7_p=23R The remote host is running KYOCERA Printer

Plugin ID:
11936

Nessus Scan Information

Information about this scan : Nessus version : 4.2.2 (Build 9129) Plugin feed version : 201007191034 Type of plugin feed : HomeFeed (Non-commercial use only) Scanner IP : 172.30.0.67 Port scanner(s) : nessus_syn_scanner Port range : default Thorough tests : no Experimental tests : no Paranoia level : 1 Report Verbosity : 1 Safe checks : no Optimize the test : yes CGI scanning : disabled Web application tests : disabled Max hosts : 80 Max checks : 5 Recv timeout : 5 Backports : None Scan Start Date :

2010/8/5 11:34 Scan duration : 177 sec

Plugin ID:
19506

Traceroute Information

Synopsis:
It was possible to obtain traceroute information.

Description:
Makes a traceroute to the remote host.

Risk factor:
None

Solution:
n/a

Plugin output:
For your information, here is the traceroute from 172.30.0.67 to 172.18.20.1 : 172.30.0.67 172.20.20.1 172.19.0.1 172.18.20.1

Plugin ID:
10287

Port ntp (123/udp) [-/+]

Network Time Protocol (NTP) Server Detection

Synopsis:
An NTP server is listening on the remote host.

Description:
An NTP (Network Time Protocol) server is listening on this port. It provides information about the current date and time of the remote system and may provide system information.

Risk factor:
None

Solution:
n/a

Plugin output:
It was possible to gather the following information from the remote NTP host : version='4', processor='unknown', system='UNIX', leap=3, stratum=16, precision=-24, rootdelay=0.000, rootdispersion=45905.189, peer=0, refid=INIT, reftime=0x00000000.00000000, poll=6, clock=0xD00558EA.EFBD9427, state=1, offset=0.000, frequency=0.000, jitter=0.000, noise=0.000, stability=0.000

Plugin ID:
10884

Port telnet (23/tcp) [-/+]

Cisco Device Default Password

Synopsis:
The remote device has a factory password set.

Description:
The remote CISCO router has a default password set. This allows an attacker to get a lot information about the network, and possibly to shut it down if the 'enable' password is not set either or is also a default password.

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:
Access this device and set a password using 'enable secret'

Plugin output:
Plugin Output : It was possible to log in as 'cisco'/'cisco'

Plugin ID:
23938

CVE:
CVE-1999-0508

Service Detection

A telnet server is running on this port.

Plugin ID:
22964

Unencrypted Telnet Server

Synopsis:
The remote Telnet server transmits traffic in cleartext.

Description:
The remote host is running a Telnet server over an unencrypted channel. Using Telnet over an unencrypted channel is not recommended as logins, passwords and commands are transferred in cleartext. An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information. Use of SSH is prefered nowadays as it protects credentials from eavesdropping and can tunnel additional data streams such as the X11 session.

Risk factor:
Low

CVSS Base Score:2.6
CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Solution:
Disable this service and use SSH instead.

Plugin ID:
42263

Telnet Server Detection

Synopsis:
A Telnet server is listening on the remote port.

Description:
The remote host is running a Telnet server, a remote terminal server.

Risk factor:
None

Solution:
Disable this service if you do not use it.

Plugin output:
Here is the banner from the remote Telnet server : ---------- snip ----------
--- User Access Verification Username: ---------- snip ----------

Plugin ID:
10281

[^] Back to 172.18.20.1

[^] Back

172.19.20.1

Scan Time

Start time :	Thu Aug 05 11:34:38 2010
End time :	Thu Aug 05 11:37:04 2010

Number of vulnerabilities

Open ports :	5
High :	0
Medium :	0
Low :	9

Remote host information

Operating System :	CISCO IOS 12 CISCO PIX
NetBIOS name :	
DNS name :	

[^] Back to 172.19.20.1

Port general (0/icmp) [-/+]

ICMP Timestamp Request Remote Date Disclosure

Synopsis:
It is possible to determine the exact time set on the remote host.

Description:
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols.

Risk factor:
None

Solution:
Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Plugin output:
This host returns non-standard timestamps (high bit is set)

Plugin ID:
10114

CVE:
CVE-1999-0524

Other references:
OSVDB:94

OS Identification

Remote operating system : CISCO IOS 12 CISCO PIX Confidence Level : 69 Method : SSH Not all fingerprints could give a match - please email the following to os-signatures@nessus.org : NTP:!:UNIX SinFP: P1:B11013:F0x12:W4128:O0204ffff:M536: P2:B11013:F0x12:W4128:O0204ffff:M536: P3:B01023:F0x14:W5840:O0:M0 P4:4202_7_p=22R SSH:SSH-2.0-Cisco-1.25 The remote host is running one of these operating systems : CISCO IOS 12 CISCO PIX

Plugin ID:
11936

Common Platform Enumeration (CPE)

Synopsis:
It is possible to enumerate CPE names that matched on the remote system.

Description:
By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host. Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

Risk factor:
None

See also:
http://cpe.mitre.org/

Solution:
n/a

Plugin output:
The remote operating system matched the following CPEs : cpe:/o:cisco:ios:12 cpe:/o:cisco:pix_firewall

Plugin ID:
45590

Nessus Scan Information

Information about this scan : Nessus version : 4.2.2 (Build 9129) Plugin feed version : 201007191034 Type of plugin feed : HomeFeed (Non-commercial use only) Scanner IP : 172.30.0.67 Port scanner(s) : nessus_syn_scanner Port range : default Thorough tests : no Experimental tests : no Paranoia level : 1 Report Verbosity : 1 Safe checks : no Optimize the test : yes CGI scanning : disabled Web application tests : disabled Max hosts : 80 Max checks : 5 Recv timeout : 5 Backports : None Scan Start Date :

2010/8/5 11:34 Scan duration : 146 sec

Plugin ID:
19506

Traceroute Information

Synopsis:
It was possible to obtain traceroute information.

Description:
Makes a traceroute to the remote host.

Risk factor:
None

Solution:
n/a

Plugin output:
For your information, here is the traceroute from 172.30.0.67 to 172.19.20.1 : 172.30.0.67 172.20.20.1 172.19.20.1

Plugin ID:
10287

Port ntp (123/udp) [-/+]

Network Time Protocol (NTP) Server Detection

Synopsis:
An NTP server is listening on the remote host.

Description:
An NTP (Network Time Protocol) server is listening on this port. It provides information about the current date and time of the remote system and may provide system information.

Risk factor:
None

Solution:
n/a

Plugin output:
It was possible to gather the following information from the remote NTP host : version='4', processor='unknown', system='UNIX', leap=3, stratum=16, precision=-24, rootdelay=0.000, rootdispersion=45894.944, peer=0, refid=INIT, reftime=0x00000000.00000000, poll=6, clock=0xD00558DE.3C2417C4, state=1, offset=0.000, frequency=0.000, jitter=0.000, noise=0.000, stability=0.000

Plugin ID:
10884

Port ssh (22/tcp) [-/+]

Service Detection

An SSH server is running on this port.

Plugin ID:
22964

SSH Server Type and Version Information

Synopsis:
An SSH server is listening on this port.

Description:
It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Risk factor:
None

Solution:
n/a

Plugin output:
SSH version : SSH-2.0-Cisco-1.25 SSH supported authentication : keyboard-interactive,password

Plugin ID:
10267

SSH Protocol Versions Supported

Synopsis:
A SSH server is running on the remote host.

Description:
This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Risk factor:
None

Solution:
n/a

Plugin output:
The remote SSH daemon supports the following versions of the SSH protocol : - 1.99 - 2.0 SSHv2 host key fingerprint : 9b:3d:7c:93:84:73:58:72:a8:b4:67:b4:f7:ea:d0:46

Plugin ID:
10881

[^] Back to 172.19.20.1

[^] Back

172.20.20.1

Scan Time

Start time :	Thu Aug 05 11:34:38 2010
End time :	Thu Aug 05 11:37:31 2010

Number of vulnerabilities

Open ports :	6
High :	1
Medium :	0
Low :	9

Remote host information

Operating System :	KYOCERA Printer
NetBIOS name :	
DNS name :	

[^] Back to 172.20.20.1

Port general (0/icmp) [-/+]

ICMP Timestamp Request Remote Date Disclosure

Synopsis:
It is possible to determine the exact time set on the remote host.

Description:
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols.

Risk factor:
None

Solution:
Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Plugin output:
This host returns non-standard timestamps (high bit is set)

Plugin ID:
10114

CVE:
CVE-1999-0524

Other references:
OSVDB:94

OS Identification

Remote operating system : KYOCERA Printer Confidence Level : 65 Method : SinFP Not all fingerprints could give a match - please email the following to os-signatures@nessus.org : NTP:!:UNIX SinFP: P1:B11013:F0x12:W4128:O0204ffff:M536: P2:B11013:F0x12:W4128:O0204ffff:M536: P3:B11023:F0x14:W5840:O0:M0 P4:4202_7_p=23R The remote host is running KYOCERA Printer

Plugin ID:
11936

Nessus Scan Information

Information about this scan : Nessus version : 4.2.2 (Build 9129) Plugin feed version : 201007191034 Type of plugin feed : HomeFeed (Non-commercial use only) Scanner IP : 172.30.0.67 Port scanner(s) : nessus_syn_scanner Port range : default Thorough tests : no Experimental tests : no Paranoia level : 1 Report Verbosity : 1 Safe checks : no Optimize the test : yes CGI scanning : disabled Web application tests : disabled Max hosts : 80 Max checks : 5 Recv timeout : 5 Backports : None Scan Start Date :

2010/8/5 11:34 Scan duration : 173 sec

Plugin ID:
19506

Traceroute Information

Synopsis:
It was possible to obtain traceroute information.

Description:
Makes a traceroute to the remote host.

Risk factor:
None

Solution:
n/a

Plugin output:
For your information, here is the traceroute from 172.30.0.67 to 172.20.20.1 : 172.30.0.67 172.20.20.1

Plugin ID:
10287

Port ntp (123/udp) [-/+]

Network Time Protocol (NTP) Server Detection

Synopsis:
An NTP server is listening on the remote host.

Description:
An NTP (Network Time Protocol) server is listening on this port. It provides information about the current date and time of the remote system and may provide system information.

Risk factor:
None

Solution:
n/a

Plugin output:
It was possible to gather the following information from the remote NTP host : version='4', processor='unknown', system='UNIX', leap=3, stratum=16, precision=-24, rootdelay=0.000, rootdispersion=45935.174, peer=0, refid=INIT, reftime=0x00000000.00000000, poll=6, clock=0xD0055933.709DBD75, state=1, offset=0.000, frequency=0.000, jitter=0.000, noise=0.000, stability=0.000

Plugin ID:
10884

Port telnet (23/tcp) [-/+]

Cisco Device Default Password

Synopsis:

The remote device has a factory password set.

Description:
The remote CISCO router has a default password set. This allows an attacker to get a lot information about the network, and possibly to shut it down if the 'enable' password is not set either or is also a default password.

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:
Access this device and set a password using 'enable secret'

Plugin output:
Plugin Output : It was possible to log in as 'cisco'/'cisco'

Plugin ID:
23938

CVE:
CVE-1999-0508

Service Detection

A telnet server is running on this port.

Plugin ID:
22964

Unencrypted Telnet Server

Synopsis:
The remote Telnet server transmits traffic in cleartext.

Description:
The remote host is running a Telnet server over an unencrypted channel. Using Telnet over an unencrypted channel is not recommended as logins, passwords and commands are transferred in cleartext. An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information. Use of SSH is prefered nowadays as it protects credentials from eavesdropping and can tunnel additional data streams such as the X11 session.

Risk factor:
Low

CVSS Base Score:2.6
CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Solution:
Disable this service and use SSH instead.

Plugin ID:
42263

Telnet Server Detection

Synopsis:

A Telnet server is listening on the remote port.

Description:
The remote host is running a Telnet server, a remote terminal server.

Risk factor:
None

Solution:
Disable this service if you do not use it.

Plugin output:
Here is the banner from the remote Telnet server : ---------- snip ----------
--- User Access Verification Username: ---------- snip ----------

Plugin ID:
10281

Port tftp (69/udp) [-/+]

TFTP Daemon Detection

Synopsis:
A TFTP server is listening on the remote port.

Description:
The remote host is running a TFTP (Trivial File Transfer Protocol) daemon. TFTP is often used by routers and diskless hosts to retrieve their configuration. It is also used by worms to propagate.

Risk factor:
None

Solution:
Disable this service if you do not use it.

Plugin ID:
11819

[^] Back to 172.20.20.1

[^] Back

172.30.0.10

Scan Time

Start time :	Thu Aug 05 11:34:38 2010
End time :	Thu Aug 05 11:37:13 2010

Number of vulnerabilities

Open ports :	22
High :	5
Medium :	2
Low :	37

Remote host information

Operating System :	Microsoft Windows Server 2003 Service Pack 1
NetBIOS name :	WINDOWS01
DNS name :	

[^] Back to 172.30.0.10

Port general (0/icmp) [-/+]

MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)

Synopsis:
Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description:
The remote host is vulnerable to a buffer overrun in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:
Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 :
http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx

Plugin ID:
34477

CVE:
CVE-2008-4250

BID:
31874

Other references:
OSVDB:49243

ICMP Timestamp Request Remote Date Disclosure

Synopsis:
It is possible to determine the exact time set on the remote host.

Description:
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols.

Risk factor:
None

Solution:
Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Plugin output:
This host returns non-standard timestamps (high bit is set) The ICMP timestamps might be in little endian format (not in network format) The remote clock is synchronized with the local clock.

Plugin ID:
10114

CVE:
CVE-1999-0524

Other references:
OSVDB:94

TCP/IP Timestamps Supported

Synopsis:
The remote service implements TCP timestamps.

Description:
The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Risk factor:
None

See also:
http://www.ietf.org/rfc/rfc1323.txt

Solution:
n/a

Plugin ID:
25220

VMware Virtual Machine Detection

Synopsis:
The remote host seems to be a VMware virtual machine.

Description:
According to the MAC address of its network adapter, the remote host is a VMware virtual machine. Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk factor:
None

Solution:
n/a

Plugin ID:
20094

Ethernet card brand

Synopsis:
The manufacturer can be deduced from the Ethernet OUI.

Description:
Each ethernet MAC address starts with a 24-bit 'Organizationally Unique Identifier'. These OUI are registered by IEEE.

Risk factor:
None

See also:
http://standards.ieee.org/faqs/OUI.html

See also:
http://standards.ieee.org/regauth/oui/index.shtml

Solution:
n/a

Plugin output:
The following card manufacturers were identified : 00:0c:29:d8:9d:dc : VMware, Inc.

Plugin ID:
35716

OS Identification

Remote operating system : Microsoft Windows Server 2003 Service Pack 1 Confidence Level : 99 Method : MSRPC The remote host is running Microsoft Windows Server 2003 Service Pack 1

Plugin ID:
11936

Common Platform Enumeration (CPE)

Synopsis:
It is possible to enumerate CPE names that matched on the remote system.

Description:
By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host. Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

Risk factor:
None

See also:
http://cpe.mitre.org/

Solution:
n/a

Plugin output:
The remote operating system matched the following CPE : cpe:/o:microsoft:windows_2003_server::sp1 -> Microsoft Windows 2003 Server Service Pack 1

Plugin ID:
45590

Nessus Scan Information

Information about this scan : Nessus version : 4.2.2 (Build 9129) Plugin feed version : 201007191034 Type of plugin feed : HomeFeed (Non-commercial use only) Scanner IP : 172.30.0.67 Port scanner(s) : nessus_syn_scanner Port range : default Thorough tests : no Experimental tests : no Paranoia level : 1 Report Verbosity : 1 Safe checks : no Optimize the test : yes CGI scanning : disabled Web application tests : disabled Max hosts : 80 Max checks : 5 Recv timeout : 5 Backports : None Scan Start Date : 2010/8/5 11:34 Scan duration : 155 sec

Plugin ID:
19506

Traceroute Information

Synopsis:
It was possible to obtain traceroute information.

Description:
Makes a traceroute to the remote host.

Risk factor:
None

Solution:
n/a

Plugin output:
For your information, here is the traceroute from 172.30.0.67 to 172.30.0.10 : 172.30.0.67 172.30.0.10

Plugin ID:
10287

Port dce-rpc (1025/tcp) [-/+]

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available on TCP port 1025 : Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0 Description : Security Account Manager Windows process : lsass.exe Type : Remote RPC service TCP Port : 1025 IP : 172.30.0.10 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : ecec0d70-a603-11d0-96b1-00a0c91ece30, version 2.0 Description : Active Directory Backup Interface Windows process : unknown Annotation : NTDS Backup Interface Type : Remote RPC service TCP Port : 1025 IP : 172.30.0.10 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 16e0cf3a-a604-11d0-

96b1-00a0c91ece30, version 2.0 Description : Active Directory Restore Interface Windows process : unknown Annotation : NTDS Restore Interface Type : Remote RPC service TCP Port : 1025 IP : 172.30.0.10 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0 Description : Active Directory Replication Interface Windows process : unknown Annotation : MS NT Directory DRS Interface Type : Remote RPC service TCP Port : 1025 IP : 172.30.0.10 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0 Description : Local Security Authority Windows process : lsass.exe Type : Remote RPC service TCP Port : 1025 IP : 172.30.0.10 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0 Description : Network Logon Service Windows process : lsass.exe Type : Remote RPC service TCP Port : 1025 IP : 172.30.0.10 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0 Description : IPsec Services (Windows XP & 2003) Windows process : lsass.exe Annotation : IPSec Policy agent endpoint Type : Remote RPC service TCP Port : 1025 IP : 172.30.0.10

Plugin ID:
10736

Port ncacn_http (1027/tcp) [-/+]

Service Detection

An ncacn_http server is running on this port.

Plugin ID:
22964

COM+ Internet Services (CIS) Server Detection

Synopsis:
A COM+ Internet Services (CIS) server is listening on this port.

Description:
COM+ Internet Services are RPC over HTTP tunneling and require IIS to operate. CIS ports shouldn't be visible on internet but only behind a firewall.

Risk factor:
None

See also:
http://msdn.microsoft.com/library/en-us/dndcom/html/cis.asp

See also:
http://support.microsoft.com/support/kb/articles/Q282/2/61.ASP

Solution:
If you do not use this service, disable it with DCOMCNFG. Otherwise, limit access to this port.

Plugin output:
Server banner : ncacn_http/1.0

Plugin ID:
10761

Port dce-rpc (1037/tcp) [-/+]

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available on TCP port 1037 : Object UUID : 00000000-0000-0000-000000000000 UUID : f5cc59b4-4264-101a-8c59-08002b2f8426, version 1.0 Description : File Replication Service Windows process : ntfrs.exe Annotation : NtFrs Service Type : Remote RPC service TCP Port : 1037 IP : 172.30.0.10 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : d049b186-814f-11d1-9a3c-00c04fc9b232, version 1.0 Description : File Replication Service Windows process : ntfrs.exe Annotation : NtFrs API Type : Remote RPC service TCP Port : 1037 IP : 172.30.0.10 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : a00c021c-2be2-11d2-b678-0000f87a8f8e, version 1.0 Description : File Replication Service Windows process : ntfrs.exe Annotation : PERFMON SERVICE Type : Remote RPC service TCP Port : 1037 IP : 172.30.0.10

Plugin ID:
10736

Port dce-rpc (1040/tcp) [-/+]

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available on TCP port 1040 : Object UUID : 00000000-0000-0000-000000000000 UUID : 6bffd098-a112-3610-9833-46c3f874532d, version 1.0 Description : DHCP Server Service Windows process : unknown Type : Remote RPC service TCP Port : 1040 IP : 172.30.0.10 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 5b821720-f63b-11d0-aad2-00c04fc324db, version 1.0 Description : DHCP Server Service Windows process : unknown Type : Remote RPC service TCP Port : 1040 IP : 172.30.0.10

Plugin ID:
10736

Port dce-rpc (1048/tcp) [-/+]

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available on TCP port 1048 : Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5.0 Description : DNS Server Windows process : dns.exe Type : Remote RPC service TCP Port : 1048 IP : 172.30.0.10

Plugin ID:
10736

Port ntp (123/udp) [-/+]

Network Time Protocol (NTP) Server Detection

Synopsis:
An NTP server is listening on the remote host.

Description:
An NTP (Network Time Protocol) server is listening on this port. It provides information about the current date and time of the remote system and may provide system information.

Risk factor:
None

Solution:
n/a

Plugin ID:
10884

Port epmap (135/tcp) [-/+]

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available locally : Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0 Description : DHCP Client Service Windows process : svchost.exe Annotation : DHCP Client LRPC Endpoint Type : Local RPC service Named pipe : dhcpcsvc Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0 Description : DHCP Client Service Windows process : svchost.exe Annotation : DHCP Client LRPC Endpoint Type : Local RPC service Named pipe : DNSResolver Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Local RPC service Named pipe : OLE435A12E49955410AACF00D7B1AC2 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Local RPC service Named pipe : wzcsvc Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Local RPC service Named pipe : OLE435A12E49955410AACF00D7B1AC2 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Local RPC service Named pipe : wzcsvc Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Local RPC service Named pipe : OLE435A12E49955410AACF00D7B1AC2 Object UUID : edcfcc6c-3feb-406a-a134-65526ec0e44b UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0 Description : Distributed Transaction Coordinator Windows process : msdtc.exe Type : Local RPC service Named pipe : OLE52BE1243D8CB4BD393F45CAB3605 Object UUID : edcfcc6c-3feb-406a-a134-65526ec0e44b UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0 Description : Distributed Transaction Coordinator Windows process : msdtc.exe Type : Local RPC service Named pipe : LRPC000000f8.00000001 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 6bffd098-a112-3610-9833-46c3f874532d, version 1.0 Description : DHCP Server Service Windows process : unknown Type : Local RPC service Named pipe : OLE9F42D7DEF0294F7EA727FF147CC6 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 6bffd098-a112-3610-9833-46c3f874532d, version 1.0 Description : DHCP Server Service Windows process : unknown Type : Local RPC service Named pipe : DHCPSERVERLPC Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 5b821720-f63b-11d0-aad2-00c04fc324db, version 1.0 Description : DHCP Server Service Windows process : unknown Type : Local RPC service Named pipe : OLE9F42D7DEF0294F7EA727FF147CC6 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 5b821720-f63b-11d0-aad2-00c04fc324db, version 1.0 Description : DHCP Server Service Windows process : unknown Type : Local RPC service Named pipe : DHCPSERVERLPC Object UUID : 00000000-0000-0000-0000-000000000000 UUID : f5cc59b4-4264-101a-8c59-08002b2f8426, version 1.0 Description : File Replication Service Windows process : ntfrs.exe Annotation : NtFrs Service Type : Local RPC service Named pipe : OLEDA5F6CA1F3F54C3EB5FCC42796C1 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : f5cc59b4-4264-101a-8c59-08002b2f8426, version 1.0 Description : File Replication Service Windows process : ntfrs.exe Annotation : NtFrs Service Type : Local RPC service Named pipe : LRPC00000328.00000001 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : d049b186-814f-11d1-9a3c-00c04fc9b232, version 1.0 Description : File Replication Service Windows process : ntfrs.exe Annotation : NtFrs API Type : Local RPC service Named pipe : OLEDA5F6CA1F3F54C3EB5FCC42796C1 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : d049b186-814f-11d1-9a3c-00c04fc9b232, version 1.0 Description : File Replication Service Windows process : ntfrs.exe Annotation : NtFrs API Type : Local RPC service Named pipe :

LRPC00000328.00000001 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : a00c021c-2be2-11d2-b678-0000f87a8f8e, version 1.0 Description : File Replication Service Windows process : ntfrs.exe Annotation : PERFMON SERVICE Type : Local RPC service Named pipe : OLEDA5F6CA1F3F54C3EB5FCC42796C1 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : a00c021c-2be2-11d2-b678-0000f87a8f8e, version 1.0 Description : File Replication Service Windows process : ntfrs.exe Annotation : PERFMON SERVICE Type : Local RPC service Named pipe : LRPC00000328.00000001 Object UUID : 046c5d0d-e349-4fb7-a1cf-655b3ec26515 UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0 Description : Distributed Transaction Coordinator Windows process : msdtc.exe Type : Local RPC service Named pipe : LRPC0000015c.00000001 Object UUID : ec5a5803-49d8-4aad-8b91-8969db2a0710 UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0 Description : Distributed Transaction Coordinator Windows process : msdtc.exe Type : Local RPC service Named pipe : LRPC0000015c.00000001 Object UUID : 0a557f20-bea4-40d6-a11c-24d8d2e5eb92 UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0 Description : Distributed Transaction Coordinator Windows process : msdtc.exe Type : Local RPC service Named pipe : LRPC0000015c.00000001 Object UUID : 70b58eb6-94b4-4dec-b909-2a73c86fb057 UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0 Description : Distributed Transaction Coordinator Windows process : msdtc.exe Type : Local RPC service Named pipe : LRPC0000015c.00000001 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0 Description : Security Account Manager Windows process : lsass.exe Type : Local RPC service Named pipe : audit Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0 Description : Security Account Manager Windows process : lsass.exe Type : Local RPC service Named pipe : securityevent Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0 Description : Security Account Manager Windows process : lsass.exe Type : Local RPC service Named pipe : protected_storage Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0 Description : Security Account Manager Windows process : lsass.exe Type : Local RPC service Named pipe : dsrole Object UUID : 00000000-0000-0000-0000-000000000000 UUID : ecec0d70-a603-11d0-96b1-00a0c91ece30, version 2.0 Description : Active Directory Backup Interface Windows process : unknown Annotation : NTDS Backup Interface Type : Local RPC service Named pipe : audit Object UUID : 00000000-0000-0000-0000-000000000000 UUID : ecec0d70-a603-11d0-96b1-00a0c91ece30, version 2.0 Description : Active Directory Backup Interface Windows process : unknown Annotation : NTDS Backup Interface Type : Local RPC service Named pipe : securityevent Object UUID : 00000000-0000-0000-0000-000000000000 UUID : ecec0d70-a603-11d0-96b1-00a0c91ece30, version 2.0 Description : Active Directory Backup Interface Windows process : unknown Annotation : NTDS Backup Interface Type : Local RPC service Named pipe : protected_storage Object UUID : 00000000-0000-0000-0000-000000000000 UUID : ecec0d70-a603-11d0-96b1-00a0c91ece30, version 2.0 Description : Active Directory Backup Interface Windows process : unknown Annotation : NTDS Backup Interface Type : Local RPC service Named pipe : dsrole Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 16e0cf3a-a604-11d0-96b1-00a0c91ece30, version 2.0 Description : Active Directory Restore Interface Windows process : unknown Annotation : NTDS Restore Interface Type : Local RPC service Named pipe : audit Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 16e0cf3a-a604-11d0-96b1-00a0c91ece30, version 2.0 Description : Active Directory Restore Interface Windows process : unknown Annotation : NTDS Restore Interface Type : Local RPC service Named pipe : securityevent Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 16e0cf3a-a604-11d0-96b1-00a0c91ece30, version 2.0 Description : Active Directory Restore Interface Windows process : unknown Annotation : NTDS Restore Interface Type : Local RPC service Named pipe : protected_storage Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 16e0cf3a-a604-11d0-96b1-00a0c91ece30, version 2.0 Description : Active Directory Restore Interface Windows process : unknown Annotation : NTDS Restore Interface Type : Local RPC service Named pipe : dsrole Object UUID : 00000000-0000-0000-0000-000000000000 UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0 Description : Active Directory Replication Interface Windows process : unknown Annotation : MS NT Directory DRS Interface Type : Local RPC service Named pipe : audit Object UUID : 00000000-0000-0000-0000-000000000000 UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0 Description : Active Directory Replication Interface Windows process : unknown Annotation : MS NT Directory DRS Interface Type : Local RPC service Named pipe : securityevent Object UUID : 00000000-0000-0000-0000-000000000000 UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0 Description : Active Directory Replication Interface Windows process : unknown Annotation : MS NT Directory DRS Interface Type : Local RPC service Named pipe :

protected_storage Object UUID : 00000000-0000-0000-0000-000000000000 UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0 Description : Active Directory Replication Interface Windows process : unknown Annotation : MS NT Directory DRS Interface Type : Local RPC service Named pipe : dsrole Object UUID : 00000000-0000-0000-0000-000000000000 UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0 Description : Active Directory Replication Interface Windows process : unknown Annotation : MS NT Directory DRS Interface Type : Local RPC service Named pipe : NTDS_LPC Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0 Description : Local Security Authority Windows process : lsass.exe Type : Local RPC service Named pipe : audit Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0 Description : Local Security Authority Windows process : lsass.exe Type : Local RPC service Named pipe : securityevent Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0 Description : Local Security Authority Windows process : lsass.exe Type : Local RPC service Named pipe : protected_storage Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0 Description : Local Security Authority Windows process : lsass.exe Type : Local RPC service Named pipe : dsrole Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0 Description : Local Security Authority Windows process : lsass.exe Type : Local RPC service Named pipe : NTDS_LPC Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0 Description : Network Logon Service Windows process : lsass.exe Type : Local RPC service Named pipe : audit Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0 Description : Network Logon Service Windows process : lsass.exe Type : Local RPC service Named pipe : securityevent Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0 Description : Network Logon Service Windows process : lsass.exe Type : Local RPC service Named pipe : protected_storage Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0 Description : Network Logon Service Windows process : lsass.exe Type : Local RPC service Named pipe : dsrole Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0 Description : Network Logon Service Windows process : lsass.exe Type : Local RPC service Named pipe : NTDS_LPC Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0 Description : IPsec Services (Windows XP & 2003) Windows process : lsass.exe Annotation : IPSec Policy agent endpoint Type : Local RPC service Named pipe : audit Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0 Description : IPsec Services (Windows XP & 2003) Windows process : lsass.exe Annotation : IPSec Policy agent endpoint Type : Local RPC service Named pipe : securityevent Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0 Description : IPsec Services (Windows XP & 2003) Windows process : lsass.exe Annotation : IPSec Policy agent endpoint Type : Local RPC service Named pipe : protected_storage Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0 Description : IPsec Services (Windows XP & 2003) Windows process : lsass.exe Annotation : IPSec Policy agent endpoint Type : Local RPC service Named pipe : dsrole Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0 Description : IPsec Services (Windows XP & 2003) Windows process : lsass.exe Annotation : IPSec Policy agent endpoint Type : Local RPC service Named pipe : NTDS_LPC Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0 Description : IPsec Services (Windows XP & 2003) Windows process : lsass.exe Annotation : IPSec Policy agent endpoint Type : Local RPC service Named pipe : OLECE4771DD8343415CA907BDFCC79A Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Local RPC service Named pipe : wzcsvc

Plugin ID:
10736

Port netbios-ns (137/udp) [-/+]

Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis:
It is possible to obtain the network name of the remote host.

Description:
The remote host listens on UDP port 137 or TCP port 445 and replies to NetBIOS nbtscan or SMB requests. Note that this plugin gathers information to be used in other plugins but does not itself generate a report.

Risk factor:
None

Solution:
n/a

Plugin output:
The following 8 NetBIOS names have been gathered : WINDOWS01 = Computer name VLABS = Workgroup / Domain name VLABS = Domain Controllers WINDOWS01 = File Server Service VLABS = Domain Master Browser VLABS = Browser Service Elections VLABS = Master Browser __MSBROWSE__ = Master Browser The remote host has the following MAC address on its adapter : 00:0c:29:d8:9d:dc

Plugin ID:
10150

Port smb (139/tcp) [-/+]

SMB Service Detection

Synopsis:
A file / print sharing service is listening on the remote host.

Description:
The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Risk factor:
None

Solution:
n/a

Plugin output:
An SMB server is running on this port.

Plugin ID:
11011

Port msft-gc? (3268/tcp) [-/+]

Port msft-gc-ssl? (3269/tcp) [-/+]

Service Detection

The service closed the connection without sending any data. It might be protected by some sort of TCP wrapper.

Plugin ID:
22964

Port ldap (389/tcp) [-/+]

LDAP Server NULL Bind Connection Information Disclosure

Synopsis:
The remote LDAP server allows anonymous access.

Description:
The LDAP server on the remote host is currently configured such that a user can connect to it without authentication - via a 'NULL BIND' - and query it for information. Although the queries that are allowed are likely to be fairly restricted, this may result in disclosure of information that an attacker could find useful. Note that version 3 of the LDAP protocol requires that a server allow anonymous access -- a 'NULL BIND' -- to the root DSA-Specific Entry (DSE) even though it may still require authentication to perform other queries. As such, this finding may be a false-positive.

Risk factor:
Medium

CVSS Base Score:5.0
CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Solution:
Unless the remote LDAP server supports LDAP v3, configure it to disallow NULL BINDs.

Plugin ID:
10723

Other references:
OSVDB:9723

LDAP NULL BASE Search Access

Synopsis:
The remote LDAP server may disclose sensitive information.

Description:
The remote LDAP server supports search requests with a null, or empty, base object. This allows information to be retrieved without any prior knowledge of the directory structure. Coupled with a NULL BIND, an anonymous user may be able to query your LDAP server using a tool such as 'LdapMiner'. Note that there are valid reasons to allow queries with a null base. For example, it is required in version 3 of the LDAP protocol to provide access to the root DSA-Specific Entry (DSE), with information about the supported naming context, authentication types, and the like. It also means that legitimate users can find information in the directory without any a priori knowledge of its structure. As such, this finding may be a false-positive.

Risk factor:
Medium

CVSS Base Score:5.0
CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Solution:
If the remote LDAP server supports a version of the LDAP protocol before v3, consider whether to disable NULL BASE queries on your LDAP server.

Plugin ID:
10722

LDAP Server Detection

Synopsis:
There is an LDAP server active on the remote host.

Description:
The remote host is running a Lightweight Directory Access Protocol, or LDAP, server. LDAP is a protocol for providing access to directory services over TCP/IP.

Risk factor:
None

See also:
http://en.wikipedia.org/wiki/LDAP

Solution:
n/a

Plugin ID:
20870

LDAP Crafted Search Request Server Information Disclosure

Synopsis:
It is possible to discover information about the remote LDAP server.

Description:
By sending a search request with a filter set to 'objectClass=*', it is possible to extract information about the remote LDAP server.

Risk factor:
None

Solution:
n/a

Plugin output:
[+]-namingContexts: | DC=vlabs,DC=local | CN=Configuration,DC=vlabs,DC=local | CN=Schema,CN=Configuration,DC=vlabs,DC=local | DC=DomainDnsZones,DC=vlabs,DC=local | DC=ForestDnsZones,DC=vlabs,DC=local

Plugin ID:
25701

Port cifs (445/tcp) [-/+]

MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)

Synopsis:
Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description:
The remote host is vulnerable to a buffer overrun in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges.

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:
Microsoft has released a set of patches for Windows 2000, XP and 2003 :
http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx

Plugin ID:
22194

CVE:
CVE-2006-3439

BID:
19409

Other references:
OSVDB:27845

MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)

Synopsis:
It is possible to crash the remote host due to a flaw in SMB.

Description:
The remote host is affected by a memory corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host.

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:
Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 :
http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx

Plugin ID:
35362

CVE:
CVE-2008-4834, CVE-2008-4835, CVE-2008-4114

BID:
31179, 33121, 33122

Other references:
OSVDB:48153, OSVDB:52691, OSVDB:52692

MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)

Synopsis:
Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description:
The remote host is vulnerable to heap overflow in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges. In addition to this, the remote host is also affected by an information disclosure vulnerability in SMB that may allow an attacker to obtain portions of the memory of the remote host.

Risk factor:
High

CVSS Base Score:7.5
CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Solution:
Microsoft has released a set of patches for Windows 2000, XP and 2003 :
http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx

Plugin ID:
22034

CVE:
CVE-2006-1314, CVE-2006-1315

BID:
18863, 18891

Other references:
OSVDB:27154, OSVDB:27155

MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)

Synopsis:
Arbitrary code can be executed on the remote host due to a flaw in the SMB implementation.

Description:
The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation that may allow an attacker to execute arbitrary code on the remote host. An attacker does not need to be authenticated to exploit this flaw.

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:
Microsoft has released a set of patches for Windows 2000, XP and 2003 :
http://www.microsoft.com/technet/security/bulletin/ms05-027.mspx

Plugin ID:
18502

CVE:
CVE-2005-1206

BID:
13942

Other references:
IAVA:2005-t-0019, OSVDB:17308

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available remotely : Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Remote RPC service Named pipe : \PIPE\atsvc Netbios name : \\WINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Remote RPC service Named pipe : \PIPE\atsvc Netbios name : \\WINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Remote RPC service Named pipe : \PIPE\atsvc Netbios name : \\WINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0 Description : Security Account Manager Windows process : lsass.exe Type : Remote RPC service Named pipe : \PIPE\lsass Netbios name : \\WINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0 Description : Security Account Manager Windows process : lsass.exe Type : Remote RPC service Named pipe : \PIPE\protected_storage Netbios name : \\WINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : ecec0d70-a603-11d0-96b1-00a0c91ece30, version 2.0 Description : Active Directory Backup Interface Windows process : unknown Annotation : NTDS Backup Interface Type : Remote RPC service Named pipe : \PIPE\lsass Netbios name : \\WINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : ecec0d70-a603-11d0-96b1-00a0c91ece30, version 2.0 Description : Active Directory Backup Interface Windows process : unknown Annotation : NTDS Backup Interface Type : Remote RPC service Named pipe : \PIPE\protected_storage Netbios name : \\WINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 16e0cf3a-a604-11d0-96b1-00a0c91ece30, version 2.0 Description : Active Directory Restore Interface Windows process : unknown Annotation : NTDS Restore Interface Type : Remote RPC service Named pipe : \PIPE\lsass Netbios name : \\WINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 16e0cf3a-a604-11d0-96b1-00a0c91ece30, version 2.0 Description : Active Directory Restore Interface Windows process : unknown Annotation : NTDS Restore Interface Type : Remote RPC service Named pipe : \PIPE\protected_storage Netbios name : \\WINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0 Description : Active Directory Replication Interface Windows process : unknown Annotation : MS NT Directory DRS Interface Type : Remote RPC service Named pipe : \PIPE\lsass Netbios name : \\WINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0 Description : Active Directory Replication Interface Windows process : unknown Annotation : MS NT

Directory DRS Interface Type : Remote RPC service Named pipe : \PIPE\protected_storage Netbios name : \\WINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0 Description : Local Security Authority Windows process : lsass.exe Type : Remote RPC service Named pipe : \PIPE\lsass Netbios name : \\WINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0 Description : Local Security Authority Windows process : lsass.exe Type : Remote RPC service Named pipe : \PIPE\protected_storage Netbios name : \\WINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0 Description : Network Logon Service Windows process : lsass.exe Type : Remote RPC service Named pipe : \PIPE\lsass Netbios name : \\WINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0 Description : Network Logon Service Windows process : lsass.exe Type : Remote RPC service Named pipe : \PIPE\protected_storage Netbios name : \\WINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0 Description : IPsec Services (Windows XP & 2003) Windows process : lsass.exe Annotation : IPSec Policy agent endpoint Type : Remote RPC service Named pipe : \PIPE\lsass Netbios name : \\WINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0 Description : IPsec Services (Windows XP & 2003) Windows process : lsass.exe Annotation : IPSec Policy agent endpoint Type : Remote RPC service Named pipe : \PIPE\protected_storage Netbios name : \\WINDOWS01

Plugin ID:
10736

SMB Service Detection

Synopsis:
A file / print sharing service is listening on the remote host.

Description:
The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Risk factor:
None

Solution:
n/a

Plugin output:
A CIFS server is running on this port.

Plugin ID:
11011

SMB NativeLanManager Remote System Information Disclosure

Synopsis:
It is possible to obtain information about the remote operating system.

Description:
It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445.

Risk factor:
None

Solution:

n/a

Plugin output:
The remote Operating System is : Windows Server 2003 3790 Service Pack 1 The remote native lan manager is : Windows Server 2003 5.2 The remote SMB Domain Name is : VLABS

Plugin ID:
10785

SMB Log In Possible

Synopsis:
It is possible to log into the remote host.

Description:
The remote host is running Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following account : - NULL session - Guest account - Given Credentials

Risk factor:
None

See also:
http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP

See also:
http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

Solution:
n/a

Plugin output:
- NULL sessions are enabled on the remote host

Plugin ID:
10394

CVE:
CVE-1999-0504, CVE-1999-0505, CVE-1999-0506, CVE-2000-0222, CVE-2002-1117, CVE-2005-3595

BID:
494, 990, 11199

Other references:
OSVDB:297, OSVDB:3106, OSVDB:8230, OSVDB:10050

SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration

Synopsis:
It is possible to obtain the domain SID.

Description:
By emulating the call to LsaQueryInformationPolicy() it was possible to obtain the domain SID (Security Identifier). The domain SID can then be used to get the list of users of the domain

Risk factor:
None

Solution:
n/a

Plugin output:
The remote domain SID value is : 1-5-21-1152684087-3219919749-3993949398

Plugin ID:
10398

CVE:
CVE-2000-1200

BID:
959

Other references:
OSVDB:715

SMB use domain SID to enumerate users

Synopsis:
It is possible to enumerate domain users.

Description:
Using the host SID, it is possible to enumerate the domain users on the remote Windows system.

Risk factor:
None

Solution:
n/a

Plugin output:
- Administrator (id 500, Administrator account) - Guest (id 501, Guest account) - krbtgt (id 502, Kerberos account) - HelpServicesGroup (id 1000) - SUPPORT_388945a0 (id 1001) - TelnetClients (id 1002) - WINDOWS01$ (id 1003) - DnsAdmins (id 1104) - DnsUpdateProxy (id 1105) - DHCP Users (id 1106) - DHCP Administrators (id 1107) - XPSTUDENT$ (id 1108) - XPTEACHER$ (id 1109) - instructor (id 1117) - student (id 1118) Note that, in addition to the Administrator, Guest, and Kerberos accounts, Nessus has enumerated only those domain users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

Plugin ID:
10399

CVE:
CVE-2000-1200

BID:
959

Other references:
OSVDB:714

SMB Registry : Nessus Cannot Access the Windows Registry

Synopsis:
Nessus is not able to access the remote Windows Registry.

Description:
It was not possible to connect to PIPE\winreg on the remote host. If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access' service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Risk factor:
None

Solution:
n/a

Plugin ID:
26917

Windows SMB NULL Session Authentication

Synopsis:
It is possible to log into the remote Windows host with a NULL session.

Description:
The remote host is running Microsoft Windows, and it was possible to log into it using a NULL session (i.e., with no login or password). An unauthenticated remote attacker can leverage this issue to get information about the remote host.

Risk factor:
None

See also:
http://support.microsoft.com/kb/q143474/

See also:
http://support.microsoft.com/kb/q246261/

Solution:
n/a

Plugin ID:
26920

CVE:
CVE-1999-0519, CVE-1999-0520, CVE-2002-1117

BID:
494

Other references:
OSVDB:299

SMB LanMan Pipe Server Listing Disclosure

Synopsis:
It is possible to obtain network information.

Description:
It was possible to obtain the browse list of the remote Windows system by send a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

Risk factor:
None

Solution:
n/a

Plugin output:
Here is the browse list of the remote host : WINDOWS01 (os : 5.2)

Plugin ID:
10397

Other references:
OSVDB:300

SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis:
It is possible to obtain the host SID for the remote host.

Description:
By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier). The host SID can then be used to get the list of local users.

Risk factor:
None

See also:
http://technet.microsoft.com/en-us/library/bb418944.aspx

Solution:
You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value. Refer to the 'See also' section for guidance.

Plugin output:
The remote host SID value is : 1-5-21-1152684087-3219919749-3993949398 The value of 'RestrictAnonymous' setting is : unknown

Plugin ID:
10859

CVE:
CVE-2000-1200

BID:
959

Other references:
OSVDB:715

SMB use host SID to enumerate local users

Synopsis:
It is possible to enumerate local users.

Description:
Using the host SID, it is possible to enumerate local users on the remote Windows system.

Risk factor:
None

Solution:
n/a

Plugin output:
- Administrator (id 500, Administrator account) - Guest (id 501, Guest account) - HelpServicesGroup (id 1000) - SUPPORT_388945a0 (id 1001) - TelnetClients (id 1002) - WINDOWS01$ (id 1003) - DnsAdmins (id 1104) - DnsUpdateProxy (id 1105) - DHCP Users (id 1106) - DHCP Administrators (id 1107) - XPSTUDENT$ (id 1108) - XPTEACHER$ (id 1109) - instructor (id 1117) - student (id 1118) Note that, in addition to the Administrator and Guest accounts, Nessus has enumerated only those local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

Plugin ID:
10860

CVE:
CVE-2000-1200

BID:
959

Other references:
OSVDB:714

Port kpasswd? (464/tcp) [-/+]

Port dns (53/tcp) [-/+]

DNS Server Detection

Synopsis:
A DNS server is listening on the remote host.

Description:
The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

Risk factor:
None

See also:
http://en.wikipedia.org/wiki/Domain_Name_System

Solution:
Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Plugin ID:
11002

DNS Server Detection

Synopsis:

A DNS server is listening on the remote host.

Description:
The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

Risk factor:
None

See also:
http://en.wikipedia.org/wiki/Domain_Name_System

Solution:
Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Plugin ID:
11002

Port http-rpc-epmap (593/tcp) [-/+]

Service Detection

An http-rpc-epmap is running on this port.

Plugin ID:
22964

Port ldaps? (636/tcp) [-/+]

Service Detection

The service closed the connection without sending any data. It might be protected by some sort of TCP wrapper.

Plugin ID:
22964

Port kerberos? (88/tcp) [-/+]

Kerberos Information Disclosure

Synopsis:
The remote Kerberos server is leaking information.

Description:
Nessus was able to retrieve the realm name and/or server time of the remote Kerberos server.

Risk factor:
None

Solution:
n/a

Plugin output:
Nessus gathered the following information : Server time : 2010-08-05 15:35:23 UTC Realm : VLABS.LOCAL

Plugin ID:
43829

[^] Back to 172.30.0.10

[^] Back

172.30.0.66

Scan Time

Start time :	Thu Aug 05 11:34:38 2010
End time :	Thu Aug 05 11:43:07 2010

Number of vulnerabilities

Open ports :	44
High :	6
Medium :	1
Low :	70

Remote host information

Operating System :	Microsoft Windows Server 2003 Service Pack 1
NetBIOS name :	TARGETWINDOWS01
DNS name :	

[^] Back to 172.30.0.66

Port general (0/icmp) [-/+]

MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)

Synopsis:
Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description:
The remote host is vulnerable to a buffer overrun in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:
Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 :
http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx

Plugin ID:
34477

CVE:
CVE-2008-4250

BID:
31874

Other references:
OSVDB:49243

ICMP Timestamp Request Remote Date Disclosure

Synopsis:
It is possible to determine the exact time set on the remote host.

Description:
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols.

Risk factor:
None

Solution:
Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Plugin output:
The ICMP timestamps seem to be in little endian format (not in network format) The remote clock is synchronized with the local clock.

Plugin ID:
10114

CVE:
CVE-1999-0524

Other references:
OSVDB:94

TCP/IP Timestamps Supported

Synopsis:
The remote service implements TCP timestamps.

Description:
The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Risk factor:
None

See also:
http://www.ietf.org/rfc/rfc1323.txt

Solution:
n/a

Plugin ID:
25220

VMware Virtual Machine Detection

Synopsis:

The remote host seems to be a VMware virtual machine.

Description:
According to the MAC address of its network adapter, the remote host is a VMware virtual machine. Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk factor:
None

Solution:
n/a

Plugin ID:
20094

Ethernet card brand

Synopsis:
The manufacturer can be deduced from the Ethernet OUI.

Description:
Each ethernet MAC address starts with a 24-bit 'Organizationally Unique Identifier'. These OUI are registered by IEEE.

Risk factor:
None

See also:
http://standards.ieee.org/faqs/OUI.html

See also:
http://standards.ieee.org/regauth/oui/index.shtml

Solution:
n/a

Plugin output:
The following card manufacturers were identified : 00:0c:29:d6:61:16 : VMware, Inc.

Plugin ID:
35716

Additional DNS Hostnames

Synopsis:
Potential virtual hosts have been detected.

Description:
Hostnames different from the current hostname have been collected by miscellaneous plugins. Different web servers may be hosted on name- based virtual hosts.

Risk factor:
None

See also:
http://en.wikipedia.org/wiki/Virtual_hosting

Solution:
If you want to test them, re-scan using the special vhost syntax, such as : www.example.com [192.0.32.10]

Plugin output:
- targetwindows01

Plugin ID:
46180

OS Identification

Remote operating system : Microsoft Windows Server 2003 Service Pack 1 Confidence Level : 99 Method : MSRPC The remote host is running Microsoft Windows Server 2003 Service Pack 1

Plugin ID:
11936

Common Platform Enumeration (CPE)

Synopsis:
It is possible to enumerate CPE names that matched on the remote system.

Description:
By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host. Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

Risk factor:
None

See also:
http://cpe.mitre.org/

Solution:
n/a

Plugin output:
The remote operating system matched the following CPE : cpe:/o:microsoft:windows_2003_server::sp1 -> Microsoft Windows 2003 Server Service Pack 1 Here is the list of application CPE IDs that matched on the remote system : cpe:/a:microsoft:iis:6.0 -> Microsoft IIS 6.0 cpe:/a:microsoft:iis:6.0 -> Microsoft IIS 6.0 cpe:/a:microsoft:iis:6.0 -> Microsoft IIS 6.0

Plugin ID:
45590

Nessus Scan Information

Information about this scan : Nessus version : 4.2.2 (Build 9129) Plugin feed version : 201007191034 Type of plugin feed : HomeFeed (Non-commercial use only) Scanner IP : 172.30.0.67 Port scanner(s) : nessus_syn_scanner Port range : default Thorough tests : no Experimental tests : no Paranoia level : 1 Report Verbosity : 1 Safe checks : no Optimize the test : yes CGI scanning : disabled Web application tests : disabled Max hosts : 80 Max checks : 5 Recv timeout : 5 Backports : None Scan Start Date : 2010/8/5 11:34 Scan duration : 509 sec

Plugin ID:
19506

Web Application Tests Disabled

Synopsis:
Web application tests were not enabled during the scan.

Description:
One or several web servers were detected by Nessus, but neither the CGI tests nor the Web Application Tests were enabled. If you want to get a more complete report, you should enable one of these features, or both. Please note that the scan might take significantly longer with these tests, which is why they are disabled by default.

Risk factor:
None

See also:
http://blog.tenablesecurity.com/web-app-auditing/

Solution:
To enable specific CGI tests, go to the 'Advanced' tab, select 'Global variable settings' and set 'Enable CGI scanning'. To generic enable web application tests, go to the 'Advanced' tab, select 'Web Application Tests Settings' and set 'Enable web applications tests'. You may configure other options, for example HTTP credentials in 'Login configurations', or form-based authentication in 'HTTP login page'.

Plugin ID:
43067

Open Port Re-check

Synopsis:
Previously open ports are now closed.

Description:
One of several ports that were previously open are now closed or unresponsive. There are numerous possible causes for this failure : - The scan may have caused a service to freeze or stop running. - An administrator may have stopped a particular service during the scanning process. This might be an availability problem related to the following reasons : - A network outage has been experienced during the scan, and the remote network cannot be reached from the Vulnerability Scanner any more. - This Vulnerability Scanner has been blacklisted by the system administrator or by automatic intrusion detection/prevention systems which have detected the vulnerability assessment. - The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective. In any case, the audit of the remote host might be incomplete and may need to be done again

Risk factor:
None

Solution:
- increase checks_read_timeout and/or reduce max_checks - disable your IPS during the Nessus scan

Plugin output:
Port 1994 was detected as being open but is now closed

Plugin ID:
10919

Traceroute Information

Synopsis:
It was possible to obtain traceroute information.

Description:
Makes a traceroute to the remote host.

Risk factor:
None

Solution:
n/a

Plugin output:
For your information, here is the traceroute from 172.30.0.67 to 172.30.0.66 : 172.30.0.67 172.30.0.66

Plugin ID:
10287

Port dce-rpc (1025/tcp) [-/+]

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available on TCP port 1025 : Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0 Description : Security Account Manager Windows process : lsass.exe Type : Remote RPC service TCP Port : 1025 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0 Description : IPsec Services (Windows XP & 2003) Windows process : lsass.exe Annotation : IPSec Policy agent endpoint Type : Remote RPC service TCP Port : 1025 IP : 172.30.0.66

Plugin ID:
10736

Port dce-rpc (1026/tcp) [-/+]

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using

this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available on TCP port 1026 : Object UUID : 07d0d68a-fecc-4ccc-a540-b7fbb40e0a74 UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0 Description : Distributed Transaction Coordinator Windows process : msdtc.exe Type : Remote RPC service TCP Port : 1026 IP : 172.30.0.66 Object UUID : 91f4314a-ffa9-410f-b292-db2e3cf7f472 UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0 Description : Distributed Transaction Coordinator Windows process : msdtc.exe Type : Remote RPC service TCP Port : 1026 IP : 172.30.0.66 Object UUID : 296c459f-9a7c-4286-9457-3f8bea99a7a5 UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0 Description : Distributed Transaction Coordinator Windows process : msdtc.exe Type : Remote RPC service TCP Port : 1026 IP : 172.30.0.66 Object UUID : 9d9c253b-be1e-4a41-bc9f-cd2b443e5ab6 UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0 Description : Distributed Transaction Coordinator Windows process : msdtc.exe Type : Remote RPC service TCP Port : 1026 IP : 172.30.0.66

Plugin ID:
10736

Port dce-rpc (1031/tcp) [-/+]

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available on TCP port 1031 : Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5.0 Description : DNS Server Windows process : dns.exe Type : Remote RPC service TCP Port : 1031 IP : 172.30.0.66

Plugin ID:
10736

Port dce-rpc (1032/tcp) [-/+]

DCE Services Enumeration

Synopsis:

A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available on TCP port 1032 : Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 82ad4280-036b-11cf-972c-00aa006887b0, version 2.0 Description : Internet Information Service (IISAdmin) Windows process : inetinfo.exe Type : Remote RPC service TCP Port : 1032 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 8cfb5d70-31a4-11cf-a7d8-00805f48a135, version 3.0 Description : Internet Information Service (SMTP) Windows process : inetinfo.exe Type : Remote RPC service TCP Port : 1032 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1.0 Description : Unknown RPC service Type : Remote RPC service TCP Port : 1032 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 4f82f460-0e21-11cf-909e-00805f48a135, version 4.0 Description : Internet Information Service (NNTP) Windows process : inetinfo.exe Type : Remote RPC service TCP Port : 1032 IP : 172.30.0.66

Plugin ID:
10736

Port dce-rpc (1033/tcp) [-/+]

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available on TCP port 1033 : Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 8cfb5d70-31a4-11cf-a7d8-00805f48a135, version 3.0 Description : Internet Information Service (SMTP) Windows process : inetinfo.exe Type : Remote RPC service TCP Port : 1033 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1.0 Description : Unknown RPC service Type : Remote RPC service TCP Port : 1033 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 4f82f460-0e21-11cf-909e-00805f48a135, version 4.0 Description : Internet Information Service (NNTP) Windows

process : inetinfo.exe Type : Remote RPC service TCP Port : 1033 IP : 172.30.0.66

Plugin ID:
10736

Port dce-rpc (1034/tcp) [-/+]

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available on TCP port 1034 : Object UUID : 00000000-0000-0000-000000000000 UUID : bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1.0 Description : Unknown RPC service Type : Remote RPC service TCP Port : 1034 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 4f82f460-0e21-11cf-909e-00805f48a135, version 4.0 Description : Internet Information Service (NNTP) Windows process : inetinfo.exe Type : Remote RPC service TCP Port : 1034 IP : 172.30.0.66

Plugin ID:
10736

Port dce-rpc (1041/tcp) [-/+]

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available on TCP port 1041 : Object UUID : 00000000-0000-0000-000000000000 UUID : 45f52c28-7f9f-101a-b52b-08002b2efabe, version 1.0 Description : Wins

Service Windows process : wins.exe Type : Remote RPC service TCP Port : 1041 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 811109bf-a4e1-11d1-ab54-00a0c91e9b45, version 1.0 Description : Wins Service Windows process : wins.exe Type : Remote RPC service TCP Port : 1041 IP : 172.30.0.66

Plugin ID:
10736

Port dce-rpc (1042/tcp) [-/+]

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available on TCP port 1042 : Object UUID : 00000000-0000-0000-0000-000000000000 UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QMRT V1 Type : Remote RPC service TCP Port : 1042 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QMRT V2 Type : Remote RPC service TCP Port : 1042 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QM2QM V1 Type : Remote RPC service TCP Port : 1042 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0 Description : Unknown RPC service Annotation : Message Queuing - RemoteRead V1 Type : Remote RPC service TCP Port : 1042 IP : 172.30.0.66

Plugin ID:
10736

Port dce-rpc (1043/tcp) [-/+]

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available on TCP port 1043 : Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 6bffd098-a112-3610-9833-46c3f874532d, version 1.0 Description : DHCP Server Service Windows process : unknown Type : Remote RPC service TCP Port : 1043 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 5b821720-f63b-11d0-aad2-00c04fc324db, version 1.0 Description : DHCP Server Service Windows process : unknown Type : Remote RPC service TCP Port : 1043 IP : 172.30.0.66

Plugin ID:
10736

Port nntp (119/tcp) [-/+]

Service Detection

An NNTP server is running on this port.

Plugin ID:
22964

News Server (NNTP) Information Disclosure

Synopsis:
Information about the remote NNTP server can be collected.

Description:
By probing the remote NNTP server, Nessus is able to collect information about it, such as whether it allows remote connections, the number of newsgroups, etc.

Risk factor:
None

Solution:
Disable this server if it is not used.

Plugin output:
This NNTP server allows unauthenticated connections. For your information, we counted 3 newsgroups on this NNTP server: 0 in the alt hierarchy, 0 in rec, 0 in biz, 0 in sci, 0 in soc, 0 in misc, 0 in news, 0 in comp, 0 in talk, 0 in humanities. Although this server says it allows posting, we were unable to send a message (posted in alt.test).

Plugin ID:
11033

Port daytime (13/tcp) [-/+]

Unknown Service Detection: HELP Request

Daytime is running on this port

Plugin ID:
11153

Daytime Service Detection

Synopsis:
A daytime service is running on the remote host

Description:
The remote host is running a 'daytime' service. This service is designed to give the local time of the day of this host to whoever connects to this port. The date format issued by this service may sometimes help an attacker to guess the operating system type of this host, or to set up timed authentication attacks against the remote host. In addition, if the daytime service is running on a UDP port, an attacker may link it to the echo port of a third-party host using spoofing, thus creating a possible denial of service condition between this host and the third party.

Risk factor:
None

Solution:
- Under Unix systems, comment out the 'daytime' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the following registry keys to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDaytime HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpDaytime Then launch cmd.exe and type : net stop simptcp net start simptcp To restart the service.

Plugin ID:
10052

Daytime Service Detection

Synopsis:
A daytime service is running on the remote host

Description:
The remote host is running a 'daytime' service. This service is designed to give the local time of the day of this host to whoever connects to this port. The date format issued by this service may sometimes help an attacker to guess the operating system type of this host, or to set up timed authentication attacks against the remote host. In addition, if the daytime service is running on a UDP port, an attacker may link it to the echo port of a third-party host using spoofing, thus creating a possible denial of service condition between this host and the third party.

Risk factor:
None

Solution:
- Under Unix systems, comment out the 'daytime' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the following registry keys to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDaytime HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpDaytime Then launch cmd.exe and type : net stop simptcp net start simptcp To restart the service.

Plugin ID:
10052

Port epmap (135/tcp) [-/+]

DCE Services Enumeration

Synopsis:

A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available locally : Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0 Description : DHCP Client Service Windows process : svchost.exe Annotation : DHCP Client LRPC Endpoint Type : Local RPC service Named pipe : dhcpcsvc Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0 Description : DHCP Client Service Windows process : svchost.exe Annotation : DHCP Client LRPC Endpoint Type : Local RPC service Named pipe : DNSResolver Object UUID : 00000000-0000-0000-0000-000000000000 UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0 Description : Unknown RPC service Annotation : ICF+ FW API Type : Local RPC service Named pipe : trkwks Object UUID : 00000000-0000-0000-0000-000000000000 UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0 Description : Unknown RPC service Annotation : ICF+ FW API Type : Local RPC service Named pipe : senssvc Object UUID : 00000000-0000-0000-0000-000000000000 UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0 Description : Unknown RPC service Annotation : ICF+ FW API Type : Local RPC service Named pipe : SECLOGON Object UUID : 00000000-0000-0000-0000-000000000000 UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0 Description : Unknown RPC service Annotation : ICF+ FW API Type : Local RPC service Named pipe : keysvc Object UUID : 8c71f82f-c4b5-445d-bd77-f4df53f25025 UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0 Description : Distributed Transaction Coordinator Windows process : msdtc.exe Type : Local RPC service Named pipe : OLE8C75BFE27468490EA46AB826B6BB Object UUID : 8c71f82f-c4b5-445d-bd77-f4df53f25025 UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0 Description : Distributed Transaction Coordinator Windows process : msdtc.exe Type : Local RPC service Named pipe : LRPC00000e70.00000001 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0 Description : Unknown RPC service Annotation : Unimodem LRPC Endpoint Type : Local RPC service Named pipe : tapsrvlpc Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0 Description : Unknown RPC service Annotation : Unimodem LRPC Endpoint Type : Local RPC service Named pipe : unimdmsvc Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 6bffd098-a112-3610-9833-46c3f874532d, version 1.0 Description : DHCP Server Service Windows process : unknown Type : Local RPC service Named pipe : OLE583FD74FA324462D970C92C1D2CE Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 6bffd098-a112-3610-9833-46c3f874532d, version 1.0 Description : DHCP Server Service Windows process : unknown Type : Local RPC service Named pipe : DHCPSERVERLPC Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 5b821720-f63b-11d0-aad2-00c04fc324db, version 1.0 Description : DHCP Server Service Windows process : unknown Type : Local RPC service Named pipe : OLE583FD74FA324462D970C92C1D2CE Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 5b821720-f63b-11d0-aad2-00c04fc324db, version 1.0 Description : DHCP Server Service Windows process : unknown Type : Local RPC service Named pipe : DHCPSERVERLPC Object UUID : 00000000-0000-0000-0000-000000000000 UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QMRT V1 Type : Local RPC service Named pipe : QMsvc$targetwindows01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QMRT V1 Type : Local RPC service Named pipe : QMMgmtFacility$targetwindows01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3,

version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QMRT V2 Type : Local RPC service Named pipe : QMsvc$targetwindows01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QMRT V2 Type : Local RPC service Named pipe : QMMgmtFacility$targetwindows01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QM2QM V1 Type : Local RPC service Named pipe : QMsvc$targetwindows01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QM2QM V1 Type : Local RPC service Named pipe : QMMgmtFacility$targetwindows01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0 Description : Unknown RPC service Annotation : Message Queuing - RemoteRead V1 Type : Local RPC service Named pipe : QMsvc$targetwindows01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0 Description : Unknown RPC service Annotation : Message Queuing - RemoteRead V1 Type : Local RPC service Named pipe : QMMgmtFacility$targetwindows01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 45f52c28-7f9f-101a-b52b-08002b2efabe, version 1.0 Description : Wins Service Windows process : wins.exe Type : Local RPC service Named pipe : OLE94E42FBD08BE40B1A3DBC6318FE7 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 45f52c28-7f9f-101a-b52b-08002b2efabe, version 1.0 Description : Wins Service Windows process : wins.exe Type : Local RPC service Named pipe : LRPC000003e4.00000001 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 811109bf-a4e1-11d1-ab54-00a0c91e9b45, version 1.0 Description : Wins Service Windows process : wins.exe Type : Local RPC service Named pipe : OLE94E42FBD08BE40B1A3DBC6318FE7 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 811109bf-a4e1-11d1-ab54-00a0c91e9b45, version 1.0 Description : Wins Service Windows process : wins.exe Type : Local RPC service Named pipe : LRPC000003e4.00000001 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 82ad4280-036b-11cf-972c-00aa006887b0, version 2.0 Description : Internet Information Service (IISAdmin) Windows process : inetinfo.exe Type : Local RPC service Named pipe : OLE8F25C46D6AE44A8CA4AF36FBE70B Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 82ad4280-036b-11cf-972c-00aa006887b0, version 2.0 Description : Internet Information Service (IISAdmin) Windows process : inetinfo.exe Type : Local RPC service Named pipe : INETINFO_LPC Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 8cfb5d70-31a4-11cf-a7d8-00805f48a135, version 3.0 Description : Internet Information Service (SMTP) Windows process : inetinfo.exe Type : Local RPC service Named pipe : OLE8F25C46D6AE44A8CA4AF36FBE70B Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 8cfb5d70-31a4-11cf-a7d8-00805f48a135, version 3.0 Description : Internet Information Service (SMTP) Windows process : inetinfo.exe Type : Local RPC service Named pipe : INETINFO_LPC Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 8cfb5d70-31a4-11cf-a7d8-00805f48a135, version 3.0 Description : Internet Information Service (SMTP) Windows process : inetinfo.exe Type : Local RPC service Named pipe : SMTPSVC_LPC Object UUID : 00000000-0000-0000-0000-000000000000 UUID : bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1.0 Description : Unknown RPC service Type : Local RPC service Named pipe : OLE8F25C46D6AE44A8CA4AF36FBE70B Object UUID : 00000000-0000-0000-0000-000000000000 UUID : bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1.0 Description : Unknown RPC service Type : Local RPC service Named pipe : INETINFO_LPC Object UUID : 00000000-0000-0000-0000-000000000000 UUID : bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1.0 Description : Unknown RPC service Type : Local RPC service Named pipe : SMTPSVC_LPC Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 4f82f460-0e21-11cf-909e-00805f48a135, version 4.0 Description : Internet Information Service (NNTP) Windows process : inetinfo.exe Type : Local RPC service Named pipe : OLE8F25C46D6AE44A8CA4AF36FBE70B Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 4f82f460-0e21-11cf-909e-00805f48a135, version 4.0 Description : Internet Information Service (NNTP) Windows process : inetinfo.exe Type : Local RPC service Named pipe : INETINFO_LPC Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 4f82f460-0e21-11cf-909e-00805f48a135, version 4.0 Description : Internet Information Service (NNTP) Windows process : inetinfo.exe Type : Local RPC service Named pipe : SMTPSVC_LPC Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 4f82f460-0e21-11cf-909e-00805f48a135, version 4.0 Description : Internet Information Service (NNTP) Windows process : inetinfo.exe Type : Local RPC service Named pipe : NNTPSVC_LPC Object UUID : 07d0d68a-fecc-4ccc-a540-b7fbb40e0a74 UUID : 906b0ce0-c70b-1067-

b317-00dd010662da, version 1.0 Description : Distributed Transaction Coordinator Windows process : msdtc.exe Type : Local RPC service Named pipe : LRPC000006d0.00000001 Object UUID : 91f4314a-ffa9-410f-b292-db2e3cf7f472 UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0 Description : Distributed Transaction Coordinator Windows process : msdtc.exe Type : Local RPC service Named pipe : LRPC000006d0.00000001 Object UUID : 296c459f-9a7c-4286-9457-3f8bea99a7a5 UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0 Description : Distributed Transaction Coordinator Windows process : msdtc.exe Type : Local RPC service Named pipe : LRPC000006d0.00000001 Object UUID : 9d9c253b-be1e-4a41-bc9f-cd2b443e5ab6 UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0 Description : Distributed Transaction Coordinator Windows process : msdtc.exe Type : Local RPC service Named pipe : LRPC000006d0.00000001 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0 Description : Security Account Manager Windows process : lsass.exe Type : Local RPC service Named pipe : audit Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0 Description : Security Account Manager Windows process : lsass.exe Type : Local RPC service Named pipe : securityevent Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0 Description : Security Account Manager Windows process : lsass.exe Type : Local RPC service Named pipe : protected_storage Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0 Description : Security Account Manager Windows process : lsass.exe Type : Local RPC service Named pipe : dsrole Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0 Description : IPsec Services (Windows XP & 2003) Windows process : lsass.exe Annotation : IPSec Policy agent endpoint Type : Local RPC service Named pipe : audit Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0 Description : IPsec Services (Windows XP & 2003) Windows process : lsass.exe Annotation : IPSec Policy agent endpoint Type : Local RPC service Named pipe : securityevent Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0 Description : IPsec Services (Windows XP & 2003) Windows process : lsass.exe Annotation : IPSec Policy agent endpoint Type : Local RPC service Named pipe : protected_storage Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0 Description : IPsec Services (Windows XP & 2003) Windows process : lsass.exe Annotation : IPSec Policy agent endpoint Type : Local RPC service Named pipe : dsrole Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Local RPC service Named pipe : wzcsvc Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Local RPC service Named pipe : OLE2448CD1D428640C2977609B29D0F Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Local RPC service Named pipe : wzcsvc Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Local RPC service Named pipe : OLE2448CD1D428640C2977609B29D0F Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Local RPC service Named pipe : wzcsvc Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Local RPC service Named pipe : OLE2448CD1D428640C2977609B29D0F Object UUID : 00000000-0000-0000-0000-000000000000 UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0 Description : Unknown RPC service Annotation : ICF+ FW API Type : Local RPC service Named pipe : wzcsvc Object UUID : 00000000-0000-0000-0000-000000000000 UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0 Description : Unknown RPC service Annotation : ICF+ FW API Type : Local RPC service Named pipe : OLE2448CD1D428640C2977609B29D0F Object UUID : 00000000-0000-0000-0000-000000000000 UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0 Description : Unknown RPC service Annotation : ICF+ FW API Type : Local RPC service Named pipe : AudioSrv

Plugin ID:
10736

Port netbios-ns (137/udp) [-/+]

Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis:
It is possible to obtain the network name of the remote host.

Description:
The remote host listens on UDP port 137 or TCP port 445 and replies to NetBIOS nbtscan or SMB requests. Note that this plugin gathers information to be used in other plugins but does not itself generate a report.

Risk factor:
None

Solution:
n/a

Plugin output:
The following 6 NetBIOS names have been gathered : TARGETWINDOWS01 = Computer name TARGETWINDOWS01 = File Server Service WORKGROUP = Workgroup / Domain name WORKGROUP = Browser Service Elections WORKGROUP = Master Browser __MSBROWSE__ = Master Browser The remote host has the following MAC address on its adapter : 00:0c:29:d6:61:16

Plugin ID:
10150

Port smb (139/tcp) [-/+]

SMB Service Detection

Synopsis:
A file / print sharing service is listening on the remote host.

Description:
The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Risk factor:
None

Solution:
n/a

Plugin output:
An SMB server is running on this port.

Plugin ID:
11011

Port qotd (17/tcp) [-/+]

Unknown Service Detection: GET Request

qotd seems to be running on this port

Plugin ID:
17975

Quote of the Day (QOTD) Service Detection

Synopsis:
The quote service (qotd) is running on this host.

Description:
A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote. Another quote of the day service is defined as a datagram based application on UDP. A server listens for UDP datagrams on UDP port 17. When a datagram is received, an answering datagram is sent containing a quote (the data in the received datagram is ignored). An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Risk factor:
None

Solution:
- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the following registry keys to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd Then launch cmd.exe and type : net stop simptcp net start simptcp To restart the service.

Plugin ID:
10198

CVE:
CVE-1999-0103

Other references:
OSVDB:150

Quote of the Day (QOTD) Service Detection

Synopsis:
The quote service (qotd) is running on this host.

Description:
A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote. Another quote of the day service is defined as a datagram based application on UDP. A server listens for UDP datagrams on UDP port 17. When a datagram is received, an answering datagram is sent containing a quote (the data in the received datagram is ignored). An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Risk factor:
None

Solution:
- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the following registry keys to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd Then launch cmd.exe and type : net stop simptcp net start simptcp To restart the service.

Plugin ID:
10198

CVE:
CVE-1999-0103

Other references:
OSVDB:150

Port ms-streaming (1755/tcp) [-/+]

Windows Media Service Server Detection

Synopsis:
A Windows Media Service server is listening on the remote port.

Description:
The remote host is running a Windows Media Service server a media streaming server.

Risk factor:
None

Solution:
Ensure that use of this software is in agreement with your organization's acceptable use and security policies.

Plugin output:
Version 9.01.01.3814 of Microsoft Media Services is running on this port.

Plugin ID:
46016

Port msmq? (1801/tcp) [-/+]

Port chargen (19/tcp) [-/+]

Service Detection

A chargen server is running on this port.

Plugin ID:
22964

Port stun-port? (1994/tcp) [-/+]

Unknown Service Detection: Banner Retrieval

Synopsis:
There is an unknown service running on the remote host.

Description:
Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Risk factor:
None

Solution:
N/A

Plugin output:
If you know what this service is, please send a description along with the following output to svc-signatures@nessus.org : Port : 1994 Type : spontaneous Banner : 0x00: 00 14 0C 00 00 00 F4 C0 02 3C C0 08 62 B4 D1 AE .....<..b... 0x10: 2D 5B 00 00 00 00 -[....

Plugin ID:
11154

Port ftp (21/tcp) [-/+]

Service Detection

An FTP server is running on this port.

Plugin ID:
22964

FTP Server Detection

Synopsis:
An FTP server is listening on this port.

Description:
It is possible to obtain the banner of the remote FTP server by connecting to the remote port.

Risk factor:
None

Solution:
N/A

Plugin output:
The remote FTP banner is : 220-EXPERIMANTAL BUILD 220-NOT FOR PRODUCTION USE 220- 220 Implementing draft-bryan-ftp-hash-02

Plugin ID:
10092

FTP Supports Clear Text Authentication

Synopsis:
The remote FTP server allows credentials to be transmitted in clear text.

Description:
The remote FTP does not encrypt its data and control connections. The user name and password are transmitted in clear text and may be intercepted by a network sniffer, or a man-in-the-middle attack.

Risk factor:
Low

CVSS Base Score:2.6
CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Solution:
Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server such as data and control connections must be encrypted.

Plugin ID:
34324

Port dce-rpc (2103/tcp) [-/+]

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available on TCP port 2103 : Object UUID : 00000000-0000-0000-0000-000000000000 UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QMRT V1 Type : Remote RPC service TCP Port : 2103 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QMRT V2 Type : Remote RPC service TCP Port : 2103 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QM2QM V1 Type : Remote RPC service TCP Port : 2103 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0 Description : Unknown RPC service Annotation : Message Queuing - RemoteRead V1 Type : Remote RPC service TCP Port : 2103 IP : 172.30.0.66

Plugin ID:
10736

Port dce-rpc (2105/tcp) [-/+]

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available on TCP port 2105 : Object UUID : 00000000-0000-0000-0000-000000000000 UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QMRT V1 Type : Remote RPC service TCP Port : 2105 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QMRT V2 Type : Remote RPC service TCP Port : 2105 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QM2QM V1 Type : Remote RPC service TCP Port : 2105 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0 Description : Unknown RPC service Annotation : Message Queuing - RemoteRead V1 Type : Remote RPC service TCP Port : 2105 IP : 172.30.0.66

Plugin ID:
10736

Port dce-rpc (2107/tcp) [-/+]

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available on TCP port 2107 : Object UUID : 00000000-0000-0000-0000-000000000000 UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QMRT V1 Type : Remote RPC service TCP Port : 2107 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QMRT V2 Type : Remote RPC service TCP Port : 2107 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0 Description : Message Queuing Service Windows process : mqsvc.exe Annotation : Message Queuing - QM2QM V1 Type : Remote RPC service TCP Port : 2107 IP : 172.30.0.66 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0 Description : Unknown RPC service Annotation : Message Queuing - RemoteRead V1 Type : Remote RPC service TCP Port : 2107 IP : 172.30.0.66

Plugin ID:
10736

Port smtp (25/tcp) [-/+]

MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832) (uncredentialed check)

Synopsis:
The remote mail server may be affected by multiple vulnerabilities.

Description:
The installed version of Microsoft Exchange / Windows SMTP Service is affected at least one vulnerability : - Incorrect parsing of DNS Mail Exchanger (MX) resource records could cause the Windows Simple Mail Transfer Protocol (SMTP) component to stop responding until the service is restarted. (CVE-2010-0024) - Improper allocation of memory for interpreting SMTP command responses may allow an attacker to read random e-mail message fragments stored on the affected server. (CVE-2010-0025)

Risk factor:
Medium

CVSS Base Score:5.0
CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P

Solution:
Microsoft has released a set of patches for Windows 2000, XP, 2003, and 2008 as well as Exchange Server 2000, 2003, 2007, and 2010 : http://www.microsoft.com/technet/security/bulletin/ms10-024.mspx

Plugin output:
The remote version of the smtpsvc.dll is 6.0.3790.1830 versus 6.0.3790.4675.

Plugin ID:
45517

CVE:
CVE-2010-0024, CVE-2010-0025

BID:
39381

Service Detection

An SMTP server is running on this port.

Plugin ID:
22964

SMTP Server Detection

Synopsis:
An SMTP server is listening on the remote port.

Description:
The remote host is running a mail (SMTP) server on this port. Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Risk factor:
None

Solution:
Disable this service if you do not use it, or filter incoming traffic to this port.

Plugin output:
Remote SMTP server banner : 220 TargetWindows01 Microsoft ESMTP MAIL Service, Version: 6.0.3790.1830 ready at Thu, 5 Aug 2010 11:35:48 -0400

Plugin ID:
10263

Port name? (42/tcp) [-/+]

MS09-039: Vulnerabilities in WINS Could Allow Remote Code Execution (969883) (uncredentialed check)

Synopsis:
Arbitrary code can be executed on the remote host through the WINS service

Description:
The remote host has a Windows WINS server installed. The remote version of this server has two vulnerabilities that may allow an attacker to execute arbitrary code on the remote system: - One heap overflow vulnerability can be exploited by any attacker - One integer overflow vulnerability can be exploited by a WINS replication partner. An attacker may use these flaws to execute arbitrary code on the remote system with SYSTEM privileges.

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:
Microsoft has released a set of patches for Windows 2000 and 2003 : http://www.microsoft.com/technet/security/Bulletin/MS09-039.mspx

Plugin ID:
40564

CVE:
CVE-2009-1923, CVE-2009-1924

BID:
35980, 35981

Other references:
OSVDB:56899, OSVDB:56900

Port cifs (445/tcp) [-/+]

MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)

Synopsis:
Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description:
The remote host is vulnerable to a buffer overrun in the 'Server' service that may allow an attacker to

execute arbitrary code on the remote host with 'SYSTEM' privileges.

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:
Microsoft has released a set of patches for Windows 2000, XP and 2003 :
http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx

Plugin ID:
22194

CVE:
CVE-2006-3439

BID:
19409

Other references:
OSVDB:27845

MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)

Synopsis:
It is possible to crash the remote host due to a flaw in SMB.

Description:
The remote host is affected by a memory corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host.

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:
Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 :
http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx

Plugin ID:
35362

CVE:
CVE-2008-4834, CVE-2008-4835, CVE-2008-4114

BID:
31179, 33121, 33122

Other references:
OSVDB:48153, OSVDB:52691, OSVDB:52692

MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)

Synopsis:
Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description:
The remote host is vulnerable to heap overflow in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges. In addition to this, the remote host is also affected by an information disclosure vulnerability in SMB that may allow an attacker to obtain portions of the memory of the remote host.

Risk factor:
High

CVSS Base Score:7.5
CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Solution:
Microsoft has released a set of patches for Windows 2000, XP and 2003 :
http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx

Plugin ID:
22034

CVE:
CVE-2006-1314, CVE-2006-1315

BID:
18863, 18891

Other references:
OSVDB:27154, OSVDB:27155

MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)

Synopsis:
Arbitrary code can be executed on the remote host due to a flaw in the SMB implementation.

Description:
The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation that may allow an attacker to execute arbitrary code on the remote host. An attacker does not need to be authenticated to exploit this flaw.

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:
Microsoft has released a set of patches for Windows 2000, XP and 2003 :
http://www.microsoft.com/technet/security/bulletin/ms05-027.mspx

Plugin ID:
18502

CVE:
CVE-2005-1206

BID:
13942

Other references:
IAVA:2005-t-0019, OSVDB:17308

DCE Services Enumeration

Synopsis:
A DCE/RPC service is running on the remote host.

Description:
By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Risk factor:
None

Solution:
N/A

Plugin output:
The following DCERPC services are available remotely : Object UUID : 00000000-0000-0000-0000-000000000000 UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0 Description : Unknown RPC service Annotation : ICF+ FW API Type : Remote RPC service Named pipe : \pipe\trkwks Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0 Description : Unknown RPC service Annotation : ICF+ FW API Type : Remote RPC service Named pipe : \PIPE\srvsvc Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0 Description : Unknown RPC service Annotation : ICF+ FW API Type : Remote RPC service Named pipe : \pipe\keysvc Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0 Description : Unknown RPC service Annotation : ICF+ FW API Type : Remote RPC service Named pipe : \PIPE\wkssvc Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0 Description : Unknown RPC service Annotation : Unimodem LRPC Endpoint Type : Remote RPC service Named pipe : \pipe\tapsrv Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 45f52c28-7f9f-101a-b52b-08002b2efabe, version 1.0 Description : Wins Service Windows process : wins.exe Type : Remote RPC service Named pipe : \pipe\WinsPipe Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 811109bf-a4e1-11d1-ab54-00a0c91e9b45, version 1.0 Description : Wins Service Windows process : wins.exe Type : Remote RPC service Named pipe : \pipe\WinsPipe Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 82ad4280-036b-11cf-972c-00aa006887b0, version 2.0 Description : Internet Information Service (IISAdmin) Windows process : inetinfo.exe Type : Remote RPC service Named pipe : \PIPE\INETINFO Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 8cfb5d70-31a4-11cf-a7d8-00805f48a135, version 3.0 Description : Internet Information Service (SMTP) Windows process : inetinfo.exe Type : Remote RPC service Named pipe : \PIPE\INETINFO Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 8cfb5d70-31a4-11cf-a7d8-00805f48a135, version 3.0 Description : Internet Information Service (SMTP) Windows process : inetinfo.exe Type : Remote RPC service Named pipe : \PIPE\SMTPSVC Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1.0 Description : Unknown RPC service Type : Remote RPC service Named pipe : \PIPE\INETINFO Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1.0

Description : Unknown RPC service Type : Remote RPC service Named pipe : \PIPE\SMTPSVC Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 4f82f460-0e21-11cf-909e-00805f48a135, version 4.0 Description : Internet Information Service (NNTP) Windows process : inetinfo.exe Type : Remote RPC service Named pipe : \PIPE\INETINFO Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 4f82f460-0e21-11cf-909e-00805f48a135, version 4.0 Description : Internet Information Service (NNTP) Windows process : inetinfo.exe Type : Remote RPC service Named pipe : \PIPE\SMTPSVC Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 4f82f460-0e21-11cf-909e-00805f48a135, version 4.0 Description : Internet Information Service (NNTP) Windows process : inetinfo.exe Type : Remote RPC service Named pipe : \PIPE\NNTPSVC Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0 Description : Security Account Manager Windows process : lsass.exe Type : Remote RPC service Named pipe : \PIPE\lsass Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0 Description : Security Account Manager Windows process : lsass.exe Type : Remote RPC service Named pipe : \PIPE\protected_storage Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0 Description : IPsec Services (Windows XP & 2003) Windows process : lsass.exe Annotation : IPSec Policy agent endpoint Type : Remote RPC service Named pipe : \PIPE\lsass Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0 Description : IPsec Services (Windows XP & 2003) Windows process : lsass.exe Annotation : IPSec Policy agent endpoint Type : Remote RPC service Named pipe : \PIPE\protected_storage Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Remote RPC service Named pipe : \PIPE\atsvc Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Remote RPC service Named pipe : \PIPE\atsvc Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0 Description : Scheduler Service Windows process : svchost.exe Type : Remote RPC service Named pipe : \PIPE\atsvc Netbios name : \\TARGETWINDOWS01 Object UUID : 00000000-0000-0000-0000-000000000000 UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0 Description : Unknown RPC service Annotation : ICF+ FW API Type : Remote RPC service Named pipe : \PIPE\atsvc Netbios name : \\TARGETWINDOWS01

Plugin ID:
10736

SMB Service Detection

Synopsis:
A file / print sharing service is listening on the remote host.

Description:
The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Risk factor:
None

Solution:
n/a

Plugin output:
A CIFS server is running on this port.

Plugin ID:
11011

SMB NativeLanManager Remote System Information Disclosure

Synopsis:
It is possible to obtain information about the remote operating system.

Description:
It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445.

Risk factor:
None

Solution:
n/a

Plugin output:
The remote Operating System is : Windows Server 2003 3790 Service Pack 1 The remote native lan manager is : Windows Server 2003 5.2 The remote SMB Domain Name is : TARGETWINDOWS01

Plugin ID:
10785

SMB Log In Possible

Synopsis:
It is possible to log into the remote host.

Description:
The remote host is running Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following account : - NULL session - Guest account - Given Credentials

Risk factor:
None

See also:
http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP

See also:
http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

Solution:
n/a

Plugin output:
- NULL sessions are enabled on the remote host

Plugin ID:
10394

CVE:
CVE-1999-0504, CVE-1999-0505, CVE-1999-0506, CVE-2000-0222, CVE-2002-1117, CVE-2005-3595

BID:
494, 990, 11199

Other references:
OSVDB:297, OSVDB:3106, OSVDB:8230, OSVDB:10050

SMB Registry : Nessus Cannot Access the Windows Registry

Synopsis:
Nessus is not able to access the remote Windows Registry.

Description:
It was not possible to connect to PIPE\winreg on the remote host. If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access' service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Risk factor:
None

Solution:
n/a

Plugin ID:
26917

Windows SMB NULL Session Authentication

Synopsis:
It is possible to log into the remote Windows host with a NULL session.

Description:
The remote host is running Microsoft Windows, and it was possible to log into it using a NULL session (i.e., with no login or password). An unauthenticated remote attacker can leverage this issue to get information about the remote host.

Risk factor:
None

See also:
http://support.microsoft.com/kb/q143474/

See also:
http://support.microsoft.com/kb/q246261/

Solution:
n/a

Plugin ID:
26920

CVE:
CVE-1999-0519, CVE-1999-0520, CVE-2002-1117

BID:
494

Other references:
OSVDB:299

SMB LanMan Pipe Server Listing Disclosure

Synopsis:
It is possible to obtain network information.

Description:
It was possible to obtain the browse list of the remote Windows system by send a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

Risk factor:
None

Solution:
n/a

Plugin output:
Here is the browse list of the remote host : TARGETWINDOWS01 (os : 5.2)

Plugin ID:
10397

Other references:
OSVDB:300

Port dns (53/tcp) [-/+]

DNS Server Detection

Synopsis:
A DNS server is listening on the remote host.

Description:
The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

Risk factor:
None

See also:
http://en.wikipedia.org/wiki/Domain_Name_System

Solution:
Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Plugin ID:
11002

DNS Server Detection

Synopsis:
A DNS server is listening on the remote host.

Description:
The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

Risk factor:
None

See also:
http://en.wikipedia.org/wiki/Domain_Name_System

Solution:
Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Plugin ID:
11002

Port rtsp (554/tcp) [-/+]

Unknown Service Detection: HELP Request

A streaming server is running on this port.

Plugin ID:
11153

RTSP Server Type / Version Detection

Synopsis:
An RTSP (Real Time Streaming Protocol) server is listening on the remote port.

Description:
The remote server is an RTSP server. RTSP is a client-server multimedia presentation protocol, which is used to stream videos and audio files over an IP network. It is usually possible to obtain the list of capabilities and the server name of the remote RTSP server by sending an OPTIONS request.

Risk factor:
None

See also:
http://en.wikipedia.org/wiki/Rtsp

Solution:
Disable this service if you do not use it.

Plugin output:
Server Type : WMServer/9.1.1.3814 The remote RSTP server responds to an 'OPTIONS *' request as follows : ---------- snip ---------- Public: DESCRIBE, SETUP, PLAY, PAUSE, TEARDOWN, SET_PARAMETER, GET_PARAMETER, OPTIONS Allow: OPTIONS, GET_PARAMETER Supported: com.microsoft.wm.srvppair, com.microsoft.wm.sswitch, com.microsoft.wm.eosmsg, com.microsoft.wm.fastcache, com.microsoft.wm.packetpairssrc, com.microsoft.wm.startupprofile Date: Thu, 05 Aug 2010 15:36:38 GMT CSeq: 1 Server: WMServer/9.1.1.3814 ---------- snip ----------

Plugin ID:
10762

Port nntps? (563/tcp) [-/+]

Port tftp (69/udp) [-/+]

TFTP Daemon Detection

Synopsis:
A TFTP server is listening on the remote port.

Description:
The remote host is running a TFTP (Trivial File Transfer Protocol) daemon. TFTP is often used by routers and diskless hosts to retrieve their configuration. It is also used by worms to propagate.

Risk factor:
None

Solution:
Disable this service if you do not use it.

Plugin ID:
11819

Port echo (7/tcp) [-/+]

Echo Service Detection

Synopsis:
An echo service is running on the remote host.

Description:
The remote host is running the 'echo' service. This service echoes any data which is sent to it. This service is unused these days, so it is strongly advised that you disable it, as it may be used by attackers to set up denial of services attacks against this host.

Risk factor:
None

Solution:
- Under Unix systems, comment out the 'echo' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the following registry key to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpEcho HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpEcho Then launch cmd.exe and type : net stop simptcp net start simptcp To restart the service.

Plugin ID:
10061

CVE:
CVE-1999-0103, CVE-1999-0635

Other references:
OSVDB:150

Service Detection

An echo server is running on this port.

Plugin ID:
22964

Echo Service Detection

Synopsis:
An echo service is running on the remote host.

Description:
The remote host is running the 'echo' service. This service echoes any data which is sent to it. This service is unused these days, so it is strongly advised that you disable it, as it may be used by attackers to set up denial of services attacks against this host.

Risk factor:
None

Solution:
- Under Unix systems, comment out the 'echo' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the following registry key to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpEcho HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpEcho Then launch cmd.exe and type : net stop simptcp net start simptcp To restart the service.

Plugin ID:
10061

CVE:
CVE-1999-0103, CVE-1999-0635

Other references:
OSVDB:150

Port www (80/tcp) [-/+]

Service Detection

A web server is running on this port.

Plugin ID:
22964

HTTP methods per directory

Synopsis:
This plugin determines which HTTP methods are allowed on various CGI directories.

Description:
By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory. As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501. Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Risk factor:
None

Solution:
n/a

Plugin output:
Based on the response to an OPTIONS request : - HTTP methods COPY GET HEAD LOCK PROPFIND SEARCH TRACE UNLOCK OPTIONS are allowed on : /

Plugin ID:
43111

HTTP Server type and version

Synopsis:
A web server is running on the remote host.

Description:
This plugin attempts to determine the type and the version of the remote web server.

Risk factor:
None

Solution:
n/a

Plugin output:
The remote web server type is : Microsoft-IIS/6.0

Plugin ID:
10107

Microsoft IIS 404 Response Service Pack Signature

Synopsis:
The remote web server is running Microsoft IIS.

Description:
The Patch level (Service Pack) of the remote IIS server appears to be lower than the current IIS service pack level. As each service pack typically contains many security patches, the server may be at risk. Note that this test makes assumptions of the remote patch level based on static return values (Content-Length) within a IIS Server's 404 error message. As such, the test can not be totally reliable and should be manually confirmed. Note also that, to determine IIS6 patch levels, a simple test is done based on strict RFC 2616 compliance. It appears as if IIS6-SP1 will accept CR as an end-of-line marker instead of both CR and LF.

Risk factor:
None

Solution:
Ensure that the server is running the latest stable Service Pack.

Plugin output:
The remote IIS server *seems* to be Microsoft IIS 6.0 - SP1

Plugin ID:
11874

HyperText Transfer Protocol (HTTP) Information

Synopsis:
Some information about the remote HTTP configuration can be extracted.

Description:
This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc... This test is informational only and does not denote any security problem.

Risk factor:
None

Solution:
n/a

Plugin output:
Protocol version : HTTP/1.1 SSL : no Keep-Alive : no Options allowed : OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH Headers : Content-Length: 1433 Content-Type: text/html Content-Location: http://172.30.0.66/iisstart.htm Last-Modified: Fri, 21 Feb 2003 22:48:30 GMT Accept-Ranges: bytes ETag: "0339c5afbd9c21:825" Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET Date: Thu, 05 Aug 2010 15:39:22 GMT

Plugin ID:
24260

WebDAV Detection

Synopsis:
The remote server is running with WebDAV enabled.

Description:
WebDAV is an industry standard extension to the HTTP specification. It adds a capability for authorized users to remotely add and manage the content of a web server. If you do not use this extension, you should disable it.

Risk factor:
None

Solution:
http://support.microsoft.com/default.aspx?kbid=241520

Plugin ID:
11424

Port www (8000/tcp) [-/+]

Service Detection

A web server is running on this port.

Plugin ID:
22964

HTTP Server type and version

Synopsis:
A web server is running on the remote host.

Description:
This plugin attempts to determine the type and the version of the remote web server.

Risk factor:
None

Solution:
n/a

Plugin output:
The remote web server type is : CherryPy/3.1.2

Plugin ID:
10107

HyperText Transfer Protocol (HTTP) Information

Synopsis:
Some information about the remote HTTP configuration can be extracted.

Description:
This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc... This test is informational only and does not denote any security problem.

Risk factor:
None

Solution:
n/a

Plugin output:
Protocol version : HTTP/1.1 SSL : no Keep-Alive : no Options allowed : (Not implemented) Headers : Date: Thu, 05 Aug 2010 15:39:23 GMT Content-Length: 96 Content-Type: text/html;charset=utf-8 Location: http://172.30.0.66/en-US/ Server: CherryPy/3.1.2 Set-Cookie: session_id_8000=2923ed0ff187b9d1fca89d12eabbe503304acb6b; expires=Fri, 06 Aug 2010 15:39:23 GMT; Path=/

Plugin ID:
24260

Port www (8080/tcp) [-/+]

Service Detection

A web server is running on this port.

Plugin ID:
22964

HTTP Server type and version

Synopsis:
A web server is running on the remote host.

Description:
This plugin attempts to determine the type and the version of the remote web server.

Risk factor:
None

Solution:
n/a

Plugin output:
The remote web server type is : Microsoft-IIS/6.0

Plugin ID:
10107

HyperText Transfer Protocol (HTTP) Information

Synopsis:
Some information about the remote HTTP configuration can be extracted.

Description:
This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc... This test is informational only and does not denote any security problem.

Risk factor:
None

Solution:
n/a

Plugin output:
Protocol version : HTTP/1.1 SSL : no Keep-Alive : no Options allowed : (Not implemented) Headers : Content-Length: 1656 Content-Type: text/html Server: Microsoft-IIS/6.0 WWW-Authenticate: Negotiate WWW-Authenticate: NTLM X-Powered-By: ASP.NET Date: Thu, 05 Aug 2010 15:39:22 GMT

Plugin ID:
24260

Port apache-administration-server? (8089/tcp) [-/+]

Port vectorchat? (8098/tcp) [-/+]

Port discard (9/tcp) [-/+]

Discard Service Detection

Synopsis:
A discard service is running on the remote host.

Description:
The remote host is running a 'discard' service. This service typically sets up a listening socket and will ignore all the data which it receives. This service is unused these days, so it is advised that you disable it.

Risk factor:
None

Solution:
- Under Unix systems, comment out the 'discard' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the following registry key to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDiscard Then launch cmd.exe and type : net stop simptcp net start simptcp To restart the service.

Plugin ID:
11367

[^] Back to 172.30.0.66