Nessus Report

Report

24/Feb/2012:17:47:53 GMT

Table Of Contents

Vulnerabilities By Host

192.168.1.205

Scan Information

Start time:	Tue Feb 14 13:18:21 2012
End time:	Tue Feb 14 13:20:40 2012

Host Information

Netbios Name:	WINDOWS2000
IP:	192.168.1.205
MAC Address:	00:0c:29:f7:55:ea
OS:	Microsoft Windows 2000 Service Pack 4

Results Summary

Critical	High	Medium	Low	Info	Total
17	2	10	2	60	91

Results Details

0/icmp

11197 - Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)

Description

The remote host uses a network device driver that pads ethernet frames with data which vary from one packet to another, likely taken from kernel memory, system memory allocated to the device driver, or a hardware buffer on its network interface card.
Known as 'Etherleak', this information disclosure vulnerability may allow an attacker to collect sensitive information from the affected host provided he is on the same physical subnet as that host.

See Also

http://www.nessus.org/u?719c90b4

Risk Factor

Low

CVSS Base Score

3.3 (CVSS2#AV:A/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

2.4 (CVSS2#AV:A/AC:L/Au:N/C:P/I:N/A:N)

References

BID	6535
CVE	CVE-2003-0001
XREF	OSVDB:3873

Ports

icmp/0

```
Padding observed in one frame :

  0x00:  1C 1D CF B0 12 44 70 F0 77 00 00 02 04 05 B4 01    .....Dp.w.......
  0x10:  03                                                 .

Padding observed in another frame :

  0x00:  A0 49 F1 80 18 43 A4 BC A6 00 00 01 01 08 0A 00    .I...C..........
  0x10:  1E                                                 .
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine.
This may help an attacker to defeat all time-based authentication protocols.

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	CWE:200
XREF	OSVDB:94

Ports

icmp/0

```
The ICMP timestamps seem to be in little endian format (not in network format)
The difference between the local and remote clocks is 19975 seconds.
```

0/tcp

47709 - Microsoft Windows 2000 Unsupported Installation Detection

Description

The remote host is running a version of Microsoft Windows 2000.
This operating system is no longer supported by Microsoft. This means not only that there will be no new security patches for it but also that Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities in it.

See Also

http://support.microsoft.com/lifecycle/?p1=7274

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Ports

tcp/0

19506 - Nessus Scan Information

Description

This script displays, for each tested host, information about the scan itself :
- The version of the plugin set
- The type of plugin feed (HomeFeed or ProfessionalFeed)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Risk Factor

None

Ports

tcp/0

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201202132338
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.13
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
```

```
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/2/14 13:18
Scan duration : 139 sec
```

45590 - Common Platform Enumeration (CPE)

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.

See Also

http://cpe.mitre.org/

Risk Factor

None

Ports

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_2000::sp4 -> Microsoft Windows 2000 Service Pack 4

Following application CPE matched on the remote system :

  cpe:/a:microsoft:iis:5.0 -> Microsoft IIS 5.0
```

54615 - Device Type

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Risk Factor

None

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 99
```

11936 - OS Identification

Description

Using a combination of remote probes, (TCP/IP, SMB, HTTP, NTP, SNMP, etc...) it is possible to guess the name of the remote operating system in use, and sometimes its version.

Risk Factor

None

Ports

tcp/0

```
Remote operating system : Microsoft Windows 2000 Service Pack 4
Confidence Level : 99
Method : MSRPC


The remote host is running Microsoft Windows 2000 Service Pack 4
```

35716 - Ethernet Card Manufacturer Detection

Description

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

See Also

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

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

Risk Factor

None

Ports

tcp/0

```
The following card manufacturers were identified :

00:0c:29:f7:55:ea : VMware, Inc.
```

20094 - VMware Virtual Machine Detection

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

Ports

tcp/0

10916 - Microsoft Windows - Local Users Information : Passwords never expire

Description

Using the supplied credentials, it is possible to list local users whose passwords never expire.

Risk Factor

None

References

XREF OSVDB:755

Ports

tcp/0

```
The following local users have passwords that never expire :

  - Administrator
  - Guest
  - IUSR_WINDOWS2000
  - IWAM_WINDOWS2000
  - nessus


Note that, in addition to the Administrator and Guest accounts, Nessus
has only checked for local users with UIDs 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.
```

10915 - Microsoft Windows - Local Users Information : User has never logged on

Description

Using the supplied credentials, it is possible to list local users who have never logged into their accounts.

Risk Factor

None

References

XREF OSVDB:754

Ports
tcp/0

```
The following local users have never logged in :

  - Guest
  - paul
  - josh
  - mike
  - nessus


Note that, in addition to the Administrator and Guest accounts, Nessus
has only checked for local users with UIDs between 1000 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for 'SMB use host SID to enumerate
local users' setting, and then re-run the scan.
```

10913 - Microsoft Windows - Local Users Information : Disabled accounts

Description
Using the supplied credentials, it is possible to list local user accounts that have been disabled.

Risk Factor
None

References
XREF OSVDB:752

Ports
tcp/0

```
The following local user account has been disabled :

  - Guest


Note that, in addition to the Administrator and Guest accounts, Nessus
has only checked for local users with UIDs between 1000 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for 'SMB use host SID to enumerate
local users' setting, and then re-run the scan.
```

25220 - TCP/IP Timestamps Supported

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.

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

Risk Factor
None

Ports
tcp/0

10904 - Microsoft Windows 'Backup Operators' Group User List

Description
Using the supplied credentials, it is possible to extract the member list of the 'Backup Operators' group. Members of this group can logon to the remote host and perform backup operations (read/write files) but have no administrative rights.

Risk Factor
None

Ports
tcp/0

```
The following user is a member of the 'Backup Operators' group :

  - WINDOWS2000\nessus (User)
```

10902 - Microsoft Windows 'Administrators' Group User List

Description

Using the supplied credentials, it is possible to extract the member list of the 'Administrators' group. Members of this group have complete access to the remote system.

Risk Factor

None

Ports

tcp/0

```
The following users are members of the 'Administrators' group :

  - WINDOWS2000\Administrator (User)
  - WINDOWS2000\paul (User)
  - WINDOWS2000\kevin (User)
  - WINDOWS2000\mike (User)
  - WINDOWS2000\nessus (User)
```

24269 - Windows Management Instrumentation (WMI) Available

Description

The supplied credentials can be used to make WMI (Windows Management Instrumentation) requests against the remote host over DCOM.
These requests can be used to gather information about the remote host such as its current state, network interface configuration, etc.

See Also

http://www.microsoft.com/whdc/system/pnppwr/wmi/default.mspx

Risk Factor

None

Ports

tcp/0

0/udp

10287 - Traceroute Information

Description

Makes a traceroute to the remote host.

Risk Factor

None

Ports

udp/0

```
For your information, here is the traceroute from 192.168.1.13 to 192.168.1.205 :
192.168.1.13
192.168.1.205
```

21/tcp

10079 - Anonymous FTP Enabled

Description

This FTP service allows anonymous logins. Any remote user may connect and authenticate without providing a password or unique credentials. This allows a user to access any files made available on the FTP server.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-1999-0497
XREF	OSVDB:69

Ports
tcp/21

34324 - FTP Supports Clear Text Authentication

Description
The remote FTP server allows the user's name and password to be transmitted in clear text, which could 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)

References
XREF	CWE:523
XREF	CWE:522

Ports
tcp/21

```
This FTP server does not support 'AUTH TLS'.
```

10092 - FTP Server Detection

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

Risk Factor
None

Ports
tcp/21

```
The remote FTP banner is :

220 windows2000 Microsoft FTP Service (Version 5.0).
```

22964 - Service Detection

Description
It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Risk Factor
None

Ports
tcp/21

```
An FTP server is running on this port.
```

11219 - Nessus SYN scanner

Description
This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor
None

Ports
tcp/21

```
Port 21/tcp was found to be open
```

25/tcp

45517 - MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832) (uncredentialed check)

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)

References

BID	39381
CVE	CVE-2010-0025
CVE	CVE-2010-0024
XREF	MSFT:MS10-024
XREF	OSVDB:63739
XREF	OSVDB:63738

Exploitable with

Core Impact (true)

Ports

tcp/25

```
The remote version of the smtpsvc.dll is 5.0.2195.6713 versus 5.0.2195.7381.
```

10263 - SMTP Server Detection

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

Ports

tcp/25

```
Remote SMTP server banner :

220 windows2000 Microsoft ESMTP MAIL Service, Version: 5.0.2195.6713 ready at  Fri, 10 Feb 2012
 07:46:03 -0500
```

22964 - Service Detection

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Risk Factor

None

Ports

tcp/25

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

11219 - Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Ports

tcp/25

```
Port 25/tcp was found to be open
```

80/tcp

34460 - Obsolete Web Server Detection

Description

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.
A lack of support implies that no new security patches are being released for it.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

Ports

tcp/80

```
Product                : Microsoft IIS 5.0
Server response header : Microsoft-IIS/5.0
Support ended          : 2010-07-13
Supported versions     : Microsoft IIS 7.5 / 7.0 / 6.0 / 5.1
Additional information : http://support.microsoft.com/lifecycle/?p1=2095
```

11213 - HTTP TRACE / TRACK Methods Allowed

Description

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

http://www.kb.cert.org/vuls/id/288308

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

http://download.oracle.com/sunalerts/1000718.1.html

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.9 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

BID 37995

BID	33374
BID	11604
BID	9561
BID	9506
CVE	CVE-2010-0386
CVE	CVE-2004-2320
CVE	CVE-2003-1567
XREF	CWE:16
XREF	OSVDB:50485
XREF	OSVDB:5648
XREF	OSVDB:3726
XREF	OSVDB:877

Ports
tcp/80

```
Use the URLScan tool to deny HTTP TRACE requests or to permit only the
methods needed to meet site requirements and policy.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus215712166.html HTTP/1.1
Connection: Close
Host: 192.168.1.205
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Fri, 10 Feb 2012 12:46:57 GMT
Content-Type: message/http
Content-Length: 314


TRACE /Nessus215712166.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.1.205
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trid [...]
```

10956 - Microsoft IIS / Site Server codebrws.asp Arbitrary Source Disclosure

Description

Microsoft's IIS 5.0 web server is shipped with a set of sample files to demonstrate different features of the ASP language. One of these sample files allows a remote user to view the source of any file in the web root with the extension .asp, .inc, .htm, or .html.

See Also

http://www.microsoft.com/technet/security/bulletin/MS99-013.mspx

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

BID	167
CVE	CVE-1999-0739
XREF	MSFT:MS99-013
XREF	OSVDB:782

Ports

tcp/80

10661 - Microsoft IIS 5 .printer ISAPI Filter Enabled

Description

IIS 5 has support for the Internet Printing Protocol(IPP), which is enabled in a default install. The protocol is implemented in IIS5 as an ISAPI extension. At least one security problem (a buffer overflow) has been found with that extension in the past, so we recommend you disable it if you do not use this functionality.

See Also

http://www.cert.org/advisories/CA-2001-10.html

Risk Factor

None

Ports

tcp/80

11874 - Microsoft IIS 404 Response Service Pack Signature

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

Ports

tcp/80

```
The remote IIS server *seems* to be Microsoft IIS 5 - SP3 or SP4
```

10077 - Microsoft FrontPage Extensions Check

Description

The remote web server appears to be running with the FrontPage extensions.
FrontPage allows remote web developers and administrators to modify web content from a remote location. While this is a fairly typical scenario on an internal local area network, the FrontPage extensions should not be available to anonymous users via the Internet (or any other untrusted 3rd party network).

Risk Factor

None

References

CVE	CVE-2000-0114
XREF	OSVDB:67

Ports
tcp/80

```
The remote frontpage server leaks information regarding the name of the anonymous user.
By knowing the name of the anonymous user, more sophisticated attacks may be launched.
We could gather that the name of the anonymous user is : IUSR_WINDOWS2000
```

11424 - WebDAV Detection

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

Ports
tcp/80

24260 - HyperText Transfer Protocol (HTTP) Information

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

Ports
tcp/80

```
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 :

  Server: Microsoft-IIS/5.0
  Date: Fri, 10 Feb 2012 12:46:52 GMT
  Content-Length: 1270
  Content-Type: text/html
  Cache-control: private
```

10107 - HTTP Server Type and Version

Description

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

Risk Factor

None

Ports
tcp/80

```
The remote web server type is :

Microsoft-IIS/5.0
```

43111 - HTTP Methods Allowed (per directory)

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

Ports
tcp/80

```
Based on the response to an OPTIONS request :

  - HTTP methods  COPY  GET  HEAD  LOCK  PROPFIND  SEARCH  TRACE
    UNLOCK OPTIONS are allowed on :

    /
```

11422 - Web Server Unconfigured - Default Install Page Present

Description

The remote web server uses its default welcome page. It probably means that this server is not used at all or is serving content that is meant to be hidden.

Risk Factor

None

References

XREF OSVDB:2117

Ports
tcp/80

```
The default welcome page is from IIS.
```

22964 - Service Detection

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Risk Factor

None

Ports
tcp/80

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

11219 - Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Ports
tcp/80

```
Port 80/tcp was found to be open
```

135/tcp

21655 - MS04-012: Cumulative Update for Microsoft RPC/DCOM (828741) (uncredentialed check)

Description

The remote host has multiple bugs in its RPC/DCOM implementation (828741).
An attacker may exploit one of these flaws to execute arbitrary code on the remote system.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.4 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	8811
BID	10127
BID	10123
BID	10121
CVE	CVE-2004-0124
CVE	CVE-2003-0807
CVE	CVE-2004-0116
CVE	CVE-2003-0813
XREF	MSFT:MS04-012
XREF	IAVA:2004-A-0005
XREF	OSVDB:5247
XREF	OSVDB:5246
XREF	OSVDB:5245
XREF	OSVDB:2670

Ports

tcp/135

11219 - Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Ports

tcp/135

```
Port 135/tcp was found to be open
```

10736 - DCE Services Enumeration

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

Ports

tcp/135

```
The following DCERPC services are available locally :
```

```
Object UUID : 91bd414f-5bd4-4f23-9870-718c93344194
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC000003e8.00000001

Object UUID : b095229a-a4f9-4f8c-9399-f77185c1f26d
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC000003e8.00000001

Object UUID : b8141b76-4631-4612-9bc7-8b04c0f009b2
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC000003e8.00000001

Object UUID : edc19f44-389c-40df-8e42-c15127914c9d
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC [...]
```

135/udp

11890 - MS03-043: Buffer Overrun in Messenger Service (828035) (uncredentialed check)

Description

A security vulnerability exists in the Messenger Service that could allow arbitrary code execution on an affected system. An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system or could cause the Messenger Service to fail.
Disabling the Messenger Service will prevent the possibility of attack.
This plugin actually tests for the presence of this flaw.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	8826
CVE	CVE-2003-0717
XREF	MSFT:MS03-043
XREF	IAVA:2003-A-0017
XREF	OSVDB:10936

Exploitable with

CANVAS (true)

Ports

udp/135

137/udp

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

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

Ports

udp/137

```
The following 11 NetBIOS names have been gathered :

 INet~Services    = Domain Controllers (IIS)
 IS~WINDOWS2000   = Computer name (IIS)
 WINDOWS2000      = Computer name
 WINDOWS2000      = Messenger Service
 ADMINISTRATOR    = Messenger Username
 WORKGROUP        = Workgroup / Domain name
 WINDOWS2000      = File Server Service
 WORKGROUP        = Browser Service Elections
 IWAM_WINDOWS200  = Messenger Username
 WORKGROUP        = Master Browser
 __MSBROWSE__     = Master Browser

The remote host has the following MAC address on its adapter :
   00:0c:29:f7:55:ea
```

139/tcp

11219 - Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Ports

tcp/139

```
Port 139/tcp was found to be open
```

11011 - Microsoft Windows SMB Service Detection

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

Ports

tcp/139

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

443/tcp

11219 - Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Ports

tcp/443

```
Port 443/tcp was found to be open
```

445/tcp

34477 - MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)

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)

CVSS Temporal Score

8.7 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	31874
CVE	CVE-2008-4250
XREF	CWE:94
XREF	MSFT:MS08-067
XREF	IAVA:2008-A-0081
XREF	OSVDB:49243

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

11808 - MS03-026: Microsoft RPC Interface Buffer Overrun (823980)

Description

The remote version of Windows contains a flaw in the function RemoteActivation() in its RPC interface that could allow an attacker to execute arbitrary code on the remote host with the SYSTEM privileges.
A series of worms (Blaster) are known to exploit this vulnerability in the wild.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	8205
CVE	CVE-2003-0352
XREF	MSFT:MS03-026
XREF	IAVA:2003-A-0011
XREF	OSVDB:2100

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

12054 - MS04-007: ASN.1 Vulnerability Could Allow Code Execution (828028) (uncredentialed check)

Description

The remote Windows host has an ASN.1 library that could allow an attacker to execute arbitrary code on this host.
To exploit this flaw, an attacker would need to send a specially crafted ASN.1 encoded packet with improperly advertised lengths.
This particular check sent a malformed NTLM packet and determined that the remote host is not patched.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	13300
BID	9743
BID	9635
BID	9633
CVE	CVE-2003-0818
XREF	MSFT:MS04-007
XREF	IAVA:2004-A-0001
XREF	OSVDB:3902

Exploitable with

CANVAS (true)Metasploit (true)

Ports

tcp/445

18502 - MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)

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)

References

BID	13942
CVE	CVE-2005-1206
XREF	MSFT:MS05-027
XREF	OSVDB:17308

Exploitable with

Core Impact (true)

Ports

tcp/445

12209 - MS04-011: Security Update for Microsoft Windows (835732) (uncredentialed check)

Description

The remote version of Windows contains a flaw in the function 'DsRolerUpgradeDownlevelServer' of the Local Security Authority Server Service (LSASS) that may allow an attacker to execute arbitrary code on the remote host with SYSTEM privileges.
A series of worms (Sasser) are known to exploit this vulnerability in the wild.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	10108
CVE	CVE-2003-0533
XREF	MSFT:MS04-011
XREF	IAVA:2004-A-0006
XREF	OSVDB:5248

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

19407 - MS05-043: Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) (uncredentialed check)

Description

The remote host contains a version of the Print Spooler service that may allow an attacker to execute code on the remote host or crash the spooler service.
An attacker can execute code on the remote host with a NULL session against :
- Windows 2000
An attacker can crash the remote service with a NULL session against :
- Windows 2000
- Windows XP SP1
An attacker needs valid credentials to crash the service against :
- Windows 2003
- Windows XP SP2

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	14514
CVE	CVE-2005-1984
XREF	MSFT:MS05-043
XREF	OSVDB:18607

Exploitable with

CANVAS (true)Core Impact (true)

Ports

tcp/445

11835 - MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed check)

Description

The remote host is running a version of Windows that has a flaw in its RPC interface, which may allow an attacker to execute arbitrary code and gain SYSTEM privileges.
An attacker or a worm could use it to gain the control of this host.
Note that this is NOT the same bug as the one described in MS03-026, which fixes the flaw exploited by the 'MSBlast' (or LoveSan) worm.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	8460
BID	8458
CVE	CVE-2003-0605
CVE	CVE-2003-0528
CVE	CVE-2003-0715
XREF	MSFT:MS03-039
XREF	IAVA:2003-A-0012
XREF	OSVDB:2535
XREF	OSVDB:11797
XREF	OSVDB:11460

Ports

tcp/445

35362 - MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)

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)

References

BID	33122
BID	33121
BID	31179

CVE	CVE-2008-4114
CVE	CVE-2008-4835
CVE	CVE-2008-4834
XREF	MSFT:MS09-001
XREF	OSVDB:52692
XREF	OSVDB:52691
XREF	OSVDB:48153

Ports

tcp/445

22194 - MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)

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)

CVSS Temporal Score

8.7 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	19409
CVE	CVE-2006-3439
XREF	MSFT:MS06-040
XREF	IAVA:2006-A-0036
XREF	OSVDB:27845

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

19408 - MS05-039: Vulnerability in Plug and Play Service Could Allow Remote Code Execution (899588) (uncredentialed check)

Description

The remote version of Windows contains a flaw in the function 'PNP_QueryResConfList()' in the Plug and Play service that may allow an attacker to execute arbitrary code on the remote host with SYSTEM privileges.
A series of worms (Zotob) are known to exploit this vulnerability in the wild.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	14513
CVE	CVE-2005-1983
XREF	MSFT:MS05-039
XREF	IAVA:2005-A-0025
XREF	OSVDB:18605

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

21193 - MS05-047: Plug and Play Remote Code Execution and Local Privilege Elevation (905749) (uncredentialed check)

Description

The remote host contain a version of the Plug and Play service that contains a vulnerability in the way it handles user-supplied data.
An authenticated attacker may exploit this flaw by sending a malformed RPC request to the remote service and execute code with SYSTEM privileges.
Note that authentication is not required against Windows 2000 if the MS05-039 patch is missing.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	15065
CVE	CVE-2005-2120
XREF	MSFT:MS05-047
XREF	OSVDB:18830

Exploitable with

Core Impact (true)

Ports

tcp/445

22034 - MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)

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)

CVSS Temporal Score

6.2 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	18891

BID	18863
CVE	CVE-2006-1315
CVE	CVE-2006-1314
XREF	MSFT:MS06-035
XREF	OSVDB:27155
XREF	OSVDB:27154

Exploitable with

Core Impact (true)

Ports

tcp/445

56211 - SMB Use Host SID to Enumerate Local Users Without Credentials

Description

Using the host security identifier (SID), it is possible to enumerate local users on the remote Windows system without credentials.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

BID	959
CVE	CVE-2000-1200
XREF	OSVDB:714

Ports

tcp/445

```
- Administrator (id 500, Administrator account)
- Guest (id 501, Guest account)
- IUSR_WINDOWS2000 (id 1000)
- IWAM_WINDOWS2000 (id 1001)
- paul (id 1002)
- kevin (id 1003)
- josh (id 1004)
- mike (id 1005)
- nessus (id 1006)
```

56210 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier), without credentials.
The host SID can then be used to get the list of local users.

See Also

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

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

BID	959
CVE	CVE-2000-1200
XREF	OSVDB:715

Ports

tcp/445

```
The remote host SID value is :

1-5-21-1123561945-1085031214-839522115
```

57608 - SMB Signing Not Required

Description

Signing is not required on the remote SMB server. This can allow man-in-the-middle attacks against the SMB server.

See Also

http://support.microsoft.com/kb/887429

http://technet.microsoft.com/en-us/library/cc786681%28WS.10%29.aspx

http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Ports

tcp/445

26920 - Microsoft Windows SMB NULL Session Authentication

Description

The remote host is running Microsoft Windows. It is possible to log into it using a NULL session (i.e., with no login or password).
Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.

See Also

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

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

http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.2 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

BID	494

CVE	CVE-2002-1117
CVE	CVE-1999-0520
CVE	CVE-1999-0519
XREF	OSVDB:8230
XREF	OSVDB:299

Ports

tcp/445

```
It was possible to bind to the \browser pipe
```

18602 - Microsoft Windows SMB svcctl MSRPC Interface SCM Service Enumeration

Description

It is possible to anonymously read the event logs of the remote Windows 2000 host by connecting to the \srvsvc pipe and binding to the event log service, OpenEventLog().
An attacker may use this flaw to anonymously read the system logs of the remote host. As system logs typically include valuable information, an attacker may use them to perform a better attack against the remote host.

See Also

http://archives.neohapsis.com/archives/fulldisclosure/2005-07/0137.html

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

BID	14178
BID	14093
CVE	CVE-2005-2150
XREF	OSVDB:17860

Ports

tcp/445

18585 - Microsoft Windows SMB Service Enumeration via \srvsvc

Description

This plugins connects to \srvsvc (instead of \svcctl) to enumerate the list of services running on the remote host on top of a NULL session.
An attacker may use this feature to gain better knowledge of the remote host.

See Also

http://www.hsc.fr/ressources/presentations/null_sessions/

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

BID	14177

BID	14093
CVE	CVE-2005-2150
XREF	OSVDB:17859

Ports
tcp/445

```
It was possible to enumerate the list of services running on the remote
host thru a NULL session, by connecting to \srvsvc


Here is the list of services running on the remote host :
Computer Browser [ Browser ]
DHCP Client [ Dhcp ]
Logical Disk Manager [ dmserver ]
DNS Client [ Dnscache ]
Event Log [ Eventlog ]
COM+ Event System [ EventSystem ]
IIS Admin Service [ IISADMIN ]
Server [ lanmanserver ]
Workstation [ lanmanworkstation ]
TCP/IP NetBIOS Helper Service [ LmHosts ]
Messenger [ Messenger ]
Distributed Transaction Coordinator [ MSDTC ]
FTP Publishing Service [ MSFTPSVC ]
Network Connections [ Netman ]
Removable Storage [ NtmsSvc ]
Plug and Play [ PlugPlay ]
IPSEC Policy Agent [ PolicyAgent ]
Protected Storage [ ProtectedStorage ]
Remote Access Connection Manager [ RasMan ]
Remote Registry Service [ RemoteRegistry ]
Remote Procedure Call (RPC) [ RpcSs ]
Security Accounts Manager [ SamSs ]
Task Scheduler [ Schedule ]
RunAs Service [ seclogon ]
System Event Notification [ SENS ]
S [...]
```

10860 - SMB Use Host SID to Enumerate Local Users

Description
Using the host security identifier (SID), it is possible to enumerate local users on the remote Windows system.

Risk Factor
None

Ports
tcp/445

```
  - Administrator (id 500, Administrator account)
  - Guest (id 501, Guest account)
  - IUSR_WINDOWS2000 (id 1000)
  - IWAM_WINDOWS2000 (id 1001)
  - paul (id 1002)
  - kevin (id 1003)
  - josh (id 1004)
  - mike (id 1005)
  - nessus (id 1006)

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.
```

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

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.

See Also

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

Risk Factor

None

Ports

tcp/445

```
The remote host SID value is :

1-5-21-1123561945-1085031214-839522115

The value of 'RestrictAnonymous' setting is : unknown
```

10395 - Microsoft Windows SMB Shares Enumeration

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Risk Factor

None

Ports

tcp/445

```
Here are the SMB shares available on the remote host when logged as a NULL session:

  - IPC$
  - ADMIN$
  - C$
```

17651 - Microsoft Windows SMB : Obtains the Password Policy

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Risk Factor

None

Ports

tcp/445

```
The following password policy is defined on the remote host:

Minimum password len: 0
Password history len: 0
Maximum password age (d): 42
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0
```

10397 - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

Description

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

Risk Factor

None

References

XREF OSVDB:300

Ports

tcp/445

```
Here is the browse list of the remote host :

WINDOWS2000 ( os : 5.0 )
```

26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the 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

Ports

tcp/445

```
Could not connect to the registry because:
Could not connect to \winreg
```

11219 - Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Ports

tcp/445

```
Port 445/tcp was found to be open
```

10394 - Microsoft Windows SMB Log In Possible

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 accounts :
- NULL session
- Guest account
- Given Credentials

See Also

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

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

Risk Factor

None

Exploitable with

Metasploit (true)

Ports

tcp/445

```
- NULL sessions are enabled on the remote host
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

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

Ports
tcp/445

```
The remote Operating System is : Windows 5.0
The remote native lan manager is : Windows 2000 LAN Manager
The remote SMB Domain Name is : WINDOWS2000
```

10736 - DCE Services Enumeration

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

Ports
tcp/445

```
The following DCERPC services are available remotely :

Object UUID : d076374b-02d8-465a-8334-b1a66a47c02e
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Remote RPC service
Named pipe : \pipe\WMIEP_138
Netbios name : \\WINDOWS2000

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 : \\WINDOWS2000

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 : \\WINDOWS2000

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8cfb5d70-31a4-11cf-a7d8-00805f48a135, version 3.0
Description : Internet Information Serv [...]
```

11011 - Microsoft Windows SMB Service Detection

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

Ports
tcp/445

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

1025/tcp

13852 - MS04-022: Microsoft Windows Task Scheduler Remote Overflow (841873)

Description

There is a flaw in the Task Scheduler application which could allow a remote attacker to execute code remotely. There are many attack vectors for this flaw. An attacker, exploiting this flaw, would need to either have the ability to connect to the target machine or be able to coerce a local user to either install a .job file or browse to a malicious website.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	10708
CVE	CVE-2004-0212
XREF	MSFT:MS04-022
XREF	IAVA:2004-A-0013
XREF	OSVDB:7798

Ports

tcp/1025

11219 - Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Ports

tcp/1025

```
Port 1025/tcp was found to be open
```

10736 - DCE Services Enumeration

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

Ports

tcp/1025

```
The following DCERPC services are available on TCP port 1025 :

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
TCP Port : 1025
IP : 192.168.1.205

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
TCP Port : 1025
IP : 192.168.1.205
```

1026/tcp

11219 - Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Ports

tcp/1026

```
Port 1026/tcp was found to be open
```

10736 - DCE Services Enumeration

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

Ports

tcp/1026

```
The following DCERPC services are available on TCP port 1026 :

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 : 1026
IP : 192.168.1.205

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 : 1026
IP : 192.168.1.205

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 : 1026
IP : 192.168.1.205
```

1027/udp

10736 - DCE Services Enumeration

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

Ports

udp/1027

```
The following DCERPC services are available on UDP port 1027 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
UDP Port : 1027
IP : 192.168.1.205
```

1028/udp

10736 - DCE Services Enumeration

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

Ports

udp/1028

```
The following DCERPC services are available on UDP port 1028 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1.0
Description : Messenger Service
Windows process : svchost.exe
Annotation : Messenger Service
Type : Remote RPC service
UDP Port : 1028
IP : 192.168.1.205
```

1093/tcp

22319 - MSRPC Service Detection

Description

The remote host is running a Windows RPC service. This service replies to the RPC Bind Request with a Bind Ack response.
However it is not possible to determine the uuid of this service.

Risk Factor

None

Ports

tcp/1093

11219 - Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Ports

tcp/1093

```
Port 1093/tcp was found to be open
```

1210/tcp

20008 - MS05-051: Vulnerabilities in MSDTC Could Allow Remote Code Execution (902400) (uncredentialed check)

Description

The remote version of Windows contains a version of MSDTC (Microsoft Data Transaction Coordinator) service has several remote code execution, local privilege escalation and denial of service vulnerabilities.
An attacker may exploit these flaws to obtain the complete control of the remote host.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.4 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	15056
BID	15057
BID	15058
BID	15059
CVE	CVE-2005-1980
CVE	CVE-2005-1979
CVE	CVE-2005-1978
CVE	CVE-2005-2119
XREF	MSFT:MS05-051
XREF	IAVA:2005-A-0030
XREF	OSVDB:19904
XREF	OSVDB:19903
XREF	OSVDB:19902
XREF	OSVDB:18828

Ports

tcp/1210

21334 - MS06-018: Vulnerability in Microsoft Distributed Transaction Coordinator Could Allow DoS (913580) (uncredentialed check)

Description

The remote version of Windows contains a version of MSDTC (Microsoft Data Transaction Coordinator) service that is affected by several remote code execution and denial of service vulnerabilities.
An attacker may exploit these flaws to obtain complete control of the remote host (2000, NT4) or to crash the remote service (XP, 2003).

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	17906
BID	17905

CVE	CVE-2006-1184
CVE	CVE-2006-0034
XREF	MSFT:MS06-018
XREF	OSVDB:25336
XREF	OSVDB:25335

Exploitable with

Core Impact (true)

Ports

tcp/1210

11219 - Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Ports

tcp/1210

```
Port 1210/tcp was found to be open
```

10736 - DCE Services Enumeration

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

Ports

tcp/1210

```
The following DCERPC services are available on TCP port 1210 :

Object UUID : 91bd414f-5bd4-4f23-9870-718c93344194
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Remote RPC service
TCP Port : 1210
IP : 192.168.1.205

Object UUID : b095229a-a4f9-4f8c-9399-f77185c1f26d
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Remote RPC service
TCP Port : 1210
IP : 192.168.1.205

Object UUID : b8141b76-4631-4612-9bc7-8b04c0f009b2
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Remote RPC service
TCP Port : 1210
IP : 192.168.1.205
```

```
Object UUID : edc19f44-389c-40df-8e42-c15127914c9d
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Remote RPC service
TCP  [...]
```

3372/tcp

11153 - Service Detection (HELP Request)

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.

Risk Factor

None

Ports

tcp/3372

```
An MSDTC server seems to be running on this port.
```

11219 - Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Ports

tcp/3372

```
Port 3372/tcp was found to be open
```