Tenable Nessus Security Report

Start Time: *Wed May 07 00:56:57 2008* **Finish Time:** *Wed May 07 01:02:54 2008*

fl_spray2_s1

192.168.2.39 10 Open Ports, 27 Notes, 1 Warnings, 3 Holes.

192.168.2.39

[Return to top]

irdmi (8000/tcp)	Port is open Plugin ID : 11219
netbios-ssn (139/tcp)	Port is open Plugin ID : 11219 An SMB server is running on this port Plugin ID : 11011
epmap (135/tcp)	Port is open Plugin ID : 11219 **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 **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 : 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 : 138160b0-1826-4541-8fdc-568f4f419a4e
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0

Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC0000072c.00000001

Object UUID : 785323a5-0869-4572-8ec7-7a3a5605ae79
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0

Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC00000668.00000001

Object UUID : 1d0711f8-9fb2-42e0-84e6-203bec177726
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0

Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC00000668.00000001

Object UUID : 51919847-3b7c-452d-a4d4-850329728d5f
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0

Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC00000668.00000001

Object UUID : ee4971ba-55eb-4cb3-8071-053da54c50b3
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0

Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC00000668.00000001

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 : OLE029F6A14F5A64AE39F60368CA3C7

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 : OLE029F6A14F5A64AE39F60368CA3C7

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 : OLE029F6A14F5A64AE39F60368CA3C7

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 : OLE029F6A14F5A64AE39F60368CA3C7 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
blackjack (1025/tcp)	Port is open Plugin ID : 11219 **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 **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 : 192.168.2.39 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 : 192.168.2.39 Plugin ID : 10736
microsoft-ds	Port is open

(445/tcp)

Plugin ID : 11219

A CIFS server is running on this port
Plugin ID : 11011

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

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 : \\FL_SPRAY2_S1

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 : \\FL_SPRAY2_S1

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 : \\FL_SPRAY2_S1

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 : \\FL_SPRAY2_S1

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 : \\FL_SPRAY2_S1

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 : \\FL_SPRAY2_S1

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 : \\FL_SPRAY2_S1

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 : \\FL_SPRAY2_S1

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 : \\FL_SPRAY2_S1

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 : \\FL_SPRAY2_S1

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 : \\FL_SPRAY2_S1

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 : \\FL_SPRAY2_S1

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 : \\FL_SPRAY2_S1

Plugin ID : 10736

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

Plugin output :

The remote Operating System is : Windows Server 2003 3790 Service Pack 2
The remote native lan manager is : Windows Server 2003 5.2
The remote SMB Domain Name is : FL_SPRAY2_S1

Plugin ID : 10785

Synopsis :

It is possible to log into the remote host.

Description :

The remote host is running one of the Microsoft Windows operating systems. It was possible to log into it using one of the following account :

- 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

Plugin output :

- NULL sessions are enabled on the remote host

CVE : CVE-1999-0504, CVE-1999-0505, CVE-1999-0506, CVE-2000-0222, CVE-

2002-1117, CVE-2005-3595
BID : 494, 990, 11199
Plugin ID : 10394

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

Plugin output :

Here is the browse list of the remote host :

FL_SPRAY2_S1 (os: 5.2)
FL_SPRAY2_S2 (os: 5.2)

Plugin ID : 10397

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
Plugin ID : 26917

Synopsis :

It is possible to log into the remote host.

Description :

The remote host is running one of the Microsoft Windows operating systems. It was possible to log into it using a NULL session.

A NULL session (no login/password) allows to get information about the remote host.

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
CVE : CVE-2002-1117
BID : 494
Plugin ID : 26920

ms-sql-s (1433/tcp)

The SQL Server has a blank password for the 'sa' account.
CVE : CVE-2000-1209
BID : 4797
Plugin ID : 10673

The remote MS SQL server is vulnerable to the Hello overflow.

An attacker may use this flaw to execute commands against
the remote host as LOCAL/SYSTEM, as well as read your database content.

This alert might be a false positive.

Solution: Install Microsoft Patch Q316333 at
http://support.microsoft.com/default.aspx?scid=kb
en-us;Q316333&sd=tech
or disable the Microsoft SQL Server service or use a firewall to protect the
MS SQL port (1433).

Risk Factor : High
CVE : CVE-2002-1123
BID : 5411
Plugin ID : 11067

Port is open
Plugin ID : 11219

Synopsis :

A SQL server is running on the remote host.

Description :

Microsoft SQL server is running on this port.

You should never let any unauthorized users establish
connections to this service.

Solution
Block this port from outside communication

Risk Factor :

None
CVE : CVE-1999-0652, CVE-1999-0652
Plugin ID : 10144

ms-wbt-server (3389/tcp)

Synopsis :

It may be possible to get access to the remote host.

Description :

The remote version of Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man in the middle attack.

An attacker may exploit this flaw to decrypt communications between client and server and obtain sensitive information (passwords, ...).

Solution:

Force the use of SSL as a transport layer for this service.

See Also :

http://www.oxid.it/downloads/rdp-gbu.pdf
http://www.nessus.org/u?c544b1fa

Risk Factor :

Medium / CVSS Base Score : 6
(AV:R/AC:H/Au:NR/C:P/A:P/I:P/B:N)
CVE : CVE-2005-1794
BID : 13818
Plugin ID : 18405


Port is open
Plugin ID : 11219

Synopsis :

The remote Windows host has Terminal Services enabled.

Description :

Terminal Services allows a Windows user to remotely obtain a graphical login (and therefore act as a local user on the remote host).

If an attacker gains a valid login and password, he may be able to use this service to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.

Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.

Solution:

Disable Terminal Services if you do not use it, and do not allow this service to run across the Internet.

Risk Factor :

None
Plugin ID : 10940

Synopsis :

The remote host is not FIPS-140 compliant.

Description :

The remote host is running Terminal Services Server. The encryption settings used by the remote service is not FIPS-140 compliant.

Solution:

Change RDP encryption level to :
4. FIPS Compliant

Risk Factor :

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

Plugin output :
The terminal services encryption level is set to:
2. Medium (Client Compatbile)
Plugin ID : 30218

general/icmp

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.

Solution:

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

Risk Factor :

None

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 difference between the local and remote clocks is 4 seconds

CVE : CVE-1999-0524
Plugin ID : 10114

general/udp

For your information, here is the traceroute from 192.168.2.3 to 192.168.2.39 :
192.168.2.3
192.168.2.39

Plugin ID : 10287

ms-sql-m (1434/udp)

Synopsis :

It is possible to determine the remote SQL server version.

Description :

Microsoft SQL server has a function wherein remote users can
query the database server for the version that is being run.
The query takes place over the same UDP port which handles the
mapping of multiple SQL server instances on the same machine.

CAVEAT: It is important to note that, after Version 8.00.194,
Microsoft decided not to update this function. This means that
the data returned by the SQL ping is inaccurate for newer releases
of SQL Server.

Solution:

filter incoming traffic to this port

Risk Factor :

None

Plugin output :

Nessus sent an MS SQL 'ping' request. The results were :
ServerName FL_SPRAY2_S1 InstanceName MSSQLSERVER IsClustered No Version
8.00.194 tcp 1433 np \\FL_SPRAY2_S1\pipe\sql\query

If you are not running multiple instances of Microsoft SQL Server
on the same machine, It is suggested you filter incoming traffic to this port
Plugin ID : 10674

general/tcp

It was possible to
crash either the remote host or the firewall
in between us and the remote host by sending
an UDP packet going to port 0.

This flaw may allow an attacker to shut down
your network.

Solution: contact your firewall vendor if
it was the firewall which crashed, or filter
incoming UDP traffic if the remote host crashed.

Risk Factor : High
CVE : CVE-1999-0675
BID : 576
Plugin ID : 10074

192.168.2.39 resolves as FL_SPRAY2_S1.
Plugin ID : 12053

Remote operating system : Microsoft Windows Server 2003 Service Pack 2
Confidence Level : 99
Method : MSRPC

The remote host is running Microsoft Windows Server 2003 Service Pack 2
Plugin ID : 11936

ntp (123/udp)

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
Plugin ID : 10884

netbios-ns (137/udp)

Synopsis :

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

Description :

The remote host listens on udp port 137 and replies to NetBIOS nbtscan
requests. By sending a wildcard request it is possible to obtain the
name of the remote system and the name of its domain.

Risk Factor :

None

Plugin output :

The following 6 NetBIOS names have been gathered :

FL_SPRAY2_S1 = Computer name
WORKGROUP = Workgroup / Domain name
FL_SPRAY2_S1 = File Server Service
WORKGROUP = Browser Service Elections
WORKGROUP = Master Browser
__MSBROWSE__ = Master Browser

The remote host has the following MAC address on its adapter :
00:17:a4:99:e3:44
CVE : CVE-1999-0621, CVE-1999-0621
Other references : OSVDB:13577
Plugin ID : 10150