Tenable Nessus Security Report

Start Time: *Wed May 07 01:16:56 2008* **Finish Time:** *Wed May 07 01:36:54 2008*

fl_spray2_s2

192.168.2.38 7 Open Ports, 21 Notes, 1 Warnings, 1 Holes.

192.168.2.38 [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 : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0

Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : W32TIME_ALT

Object UUID : 74ebb514-ea6d-4f6c-94b1-e23a04733cf0
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0

Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC00000950.00000001

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 : d51ff6b5-3f62-4b93-bb2d-27e51d24e27d
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0

Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC00000400.00000001

Object UUID : 3eb4f83e-88b8-4939-8f08-5a6d25d2f43e
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0

Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC00000400.00000001

Object UUID : a15e6247-8826-4c0f-a2da-bfe95b133234
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0

Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC00000400.00000001

Object UUID : 88645783-4750-4420-8ac3-da2afd25c0cb
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0

Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC00000400.00000001

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 : OLE7FB116CA2CB3475082058DF83D60

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 : OLE7FB116CA2CB3475082058DF83D60

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 : OLE7FB116CA2CB3475082058DF83D60

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 : OLE7FB116CA2CB3475082058DF83D60

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

microsoft-ds (445/tcp)

Port is open
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_S2

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_S2

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_S2

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_S2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0

Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Remote RPC service
Named pipe : \PIPE\W32TIME_ALT
Netbios name : \\FL_SPRAY2_S2

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_S2

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_S2

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_S2

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_S2

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_S2

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_S2

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_S2

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_S2

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_S2

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_S2

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-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/udp

For your information, here is the traceroute from 192.168.2.3 to 192.168.2.38 :
192.168.2.3
192.168.2.38

Plugin ID : 10287

blackjack (1025/tcp)

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 : 192.168.2.38

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 : 192.168.2.38

Plugin ID : 10736

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 4 NetBIOS names have been gathered :

FL_SPRAY2_S2 = Computer name
WORKGROUP = Workgroup / Domain name
FL_SPRAY2_S2 = File Server Service
WORKGROUP = Browser Service Elections

The remote host has the following MAC address on its adapter :
00:17:a4:99:e3:4b
CVE : CVE-1999-0621, CVE-1999-0621
Other references : OSVDB:13577
Plugin ID : 10150

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

192.168.2.38 resolves as FL_SPRAY2_S2.
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