Tenable Nessus Security Report

Start Time: *Wed Mar 19 07:37:48 2008* **Finish Time:** *Wed Mar 19 08:12:49 2008*

FL_WEI_S2

192.168.2.37 8 Open Ports, 24 Notes, 1 Warnings, 2 Holes.

192.168.2.37 [Return to top]

vnc-http (5800/tcp)

The remote server is running VNC.
VNC permits a console to be displayed remotely.

Solution Disable VNC access from the network by using a firewall, or stop VNC service if not needed.

Risk Factor : Medium
Plugin ID : 10758

Port is open
Plugin ID : 11219

A web server is running on this port
Plugin ID : 10330

Synopsis :

HMAP fingerprints the remote HTTP server.

Description :

By sending several valid and invalid HTTP requests, it may be possible to identify the remote web server type. In some cases, its version can also be approximated, as well as some options.

An attacker may use this tool to identify the kind of the remote web server and gain further knowledge about this host.

Suggestions for defense against fingerprinting are presented in http://acsac.org/2002/abstracts/96.html

See Also :

http://ujeni.murkyroc.com/hmap/
http://seclab.cs.ucdavis.edu/papers/hmap-thesis.pdf

Risk Factor :

Low

Plugin output :

This web server was fingerprinted as: VNC HTTPD (RFB 003.003)
Plugin ID : 11919

Synopsis :

Some information about the remote HTTP configuration can be extracted.

Description :

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem

Solution:

None.

Risk Factor :

None

Plugin output :

Protocol version : HTTP/1.0
SSL : no
Pipelining : no
Keep-Alive : no
Headers :

<HTML>
<HEAD><TITLE> [fl_wei_s2] </TITLE></HEAD>
<BODY>
<SPAN style='position: absolute; top:0px;left:0px'>
<OBJECT
ID='VncViewer'
classid = 'clsid:8AD9C840-044E-11D1-B3E9-00805F499D93'
codebase = 'http://java.sun.com/update/1.4.2/jinstall-1_4-windows-i586.cab#Version=1,4,0,0'
WIDTH = 1280 HEIGHT = 1056 >
<PARAM NAME = CODE VALUE = VncViewer.class >
<PARAM NAME = ARCHIVE VALUE = VncViewer.jar >
<PARAM NAME = 'type' VALUE = 'application/x-java-applet;version=1.4'>
<PARAM NAME = 'scriptable' VALUE = 'false'>
<PARAM NAME = PORT VALUE=5900>
<PARAM NAME = ENCODING VALUE=Tight>
<PARAM NAME = 'Open New Window' VALUE='Yes'>
<COMMENT>
<EMBED
type = 'application/x-java-applet;version=1.4' \
CODE = VncViewer.class \
ARCHIVE = VncViewer.jar \
WIDTH = 1280 \
HEIGHT = 1056 \
PORT =5900 \
ENCODING =Tight \
scriptable = false \
pluginspage ='http://java.sun.com/products/plugin/index.html#download'>

<NOEMBED>
</NOEMBED>
</EMBED>
</COMMENT>
</OBJECT>
</SPAN>
</BODY>
</HTML>

	Plugin ID : 24260
irdmi (8000/tcp)	Port is open Plugin ID : 11219
vnc (5900/tcp)	**Synopsis** : The remote VNC server does not require authentication. **Description** : The VNC server installed on the remote host allows an attacker to connect to the remote host as no authentication is required to access this service. **Solution**: Disable the No Authentication security type. **Risk Factor** : High / CVSS Base Score : 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) Plugin ID : 26925 Port is open Plugin ID : 11219 **Synopsis** : The remote host is running a remote display software (VNC). **Description** : The remote server is running VNC, a software which permits a console to be displayed remotely. This allows users to control the host remotely. **Solution**: Make sure the use of this software is done in accordance with your corporate security policy and filter incoming traffic to this port. **Risk Factor** : None **Plugin output** : The version of the VNC protocol is : RFB 003.004 Plugin ID : 10342
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 : a3a797d4-2a51-46bc-8b7c-912dfef24d59
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0

Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC000007a0.00000001

Object UUID : 2b2206f0-6eb8-40d1-a772-83ae95e1b995
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0

Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC00000408.00000001

Object UUID : 3a6ea2ab-7b82-4a8a-bb34-4ccacc1033d8
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0

Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC00000408.00000001

Object UUID : 34ff82ae-a3e2-42f1-8167-7ba0af2b3b3d
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0

Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC00000408.00000001

Object UUID : fa12d724-6b28-483d-8a15-0a2fa2672470
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0

Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC00000408.00000001

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 : OLE8DE078CEACC644F38AA457F3BB9A

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 : OLE8DE078CEACC644F38AA457F3BB9A

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 : OLE8DE078CEACC644F38AA457F3BB9A

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 : OLE8DE078CEACC644F38AA457F3BB9A

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 :

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_WEI_S2

Plugin ID : 10785

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\ROUTER
Netbios name : \\FL_WEI_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\msgsvc

Netbios name : \\FL_WEI_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\trkwks
Netbios name : \\FL_WEI_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_WEI_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_WEI_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_WEI_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_WEI_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_WEI_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_WEI_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_WEI_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_WEI_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_WEI_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_WEI_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_WEI_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_WEI_S2

Plugin ID : 10736

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_WEI_S1 (os: 5.2)
FL_WEI_S2 (os: 5.2) - FactoryLink Server 2 Weiketen

Other references : OSVDB:300
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

general/udp

For your information, here is the traceroute from 192.168.2.3 to 192.168.2.37 :
192.168.2.3
192.168.2.37

Plugin ID : 10287

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 5 NetBIOS names have been gathered :

FL_WEI_S2 = Computer name
WORKGROUP = Workgroup / Domain name
FL_WEI_S2 = File Server Service
FL_WEI_S2 = Messenger Service
WORKGROUP = Browser Service Elections

The remote host has the following MAC address on its adapter :
00:17:a4:99:d3:82
CVE : CVE-1999-0621
Other references : OSVDB:13577
Plugin ID : 10150

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 : 192.168.2.37

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 : 192.168.2.37

Plugin ID : 10736

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

192.168.2.37 resolves as FL_WEI_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