



Nessus Scan Report

02/Dec/2016:11:26:41

Nessus Home: Commercial use of the report is prohibited

Any time Nessus is used in a commercial environment you MUST maintain an active subscription to the Nessus Feed in order to be compliant with our license agreement. <http://www.tenable.com/products/nessus>

Table Of Contents

[Hosts Summary \(Executive\)](#)

[192.168.134.131](#)

[Vulnerabilities By Host](#)

■ [192.168.134.131](#)

[Vulnerabilities By Plugin](#)

- [58435 \(1\) - MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution \(2671387\) \(uncredentialed check\)](#)
- [18405 \(1\) - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness](#)
- [51192 \(1\) - SSL Certificate Cannot Be Trusted](#)
- [57582 \(1\) - SSL Self-Signed Certificate](#)
- [57608 \(1\) - SMB Signing Required](#)
- [57690 \(1\) - Terminal Services Encryption Level is Medium or Low](#)
- [58453 \(1\) - Terminal Services Doesn't Use Network Level Authentication \(NLA\)](#)
- [30218 \(1\) - Terminal Services Encryption Level is not FIPS-140 Compliant](#)
- [65821 \(1\) - SSL RC4 Cipher Suites Supported](#)
- [10736 \(8\) - DCE Services Enumeration](#)
- [11219 \(4\) - Nessus SYN scanner](#)
- [11011 \(2\) - Microsoft Windows SMB Service Detection](#)

- [10114 \(1\) - ICMP Timestamp Request Remote Date Disclosure](#)
- [10150 \(1\) - Windows NetBIOS / SMB Remote Host Information Disclosure](#)
- [10287 \(1\) - Traceroute Information](#)
- [10394 \(1\) - Microsoft Windows SMB Log In Possible](#)
- [10397 \(1\) - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure](#)
- [10785 \(1\) - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure](#)
- [10863 \(1\) - SSL Certificate Information](#)
- [11153 \(1\) - Service Detection \(HELP Request\)](#)
- [11936 \(1\) - OS Identification](#)
- [12053 \(1\) - Host Fully Qualified Domain Name \(FQDN\) Resolution](#)
- [19506 \(1\) - Nessus Scan Information](#)
- [20094 \(1\) - VMware Virtual Machine Detection](#)
- [21643 \(1\) - SSL Cipher Suites Supported](#)
- [24786 \(1\) - Nessus Windows Scan Not Performed with Admin Privileges](#)
- [25220 \(1\) - TCP/IP Timestamps Supported](#)
- [26917 \(1\) - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry](#)
- [35716 \(1\) - Ethernet Card Manufacturer Detection](#)
- [45590 \(1\) - Common Platform Enumeration \(CPE\)](#)
- [46215 \(1\) - Inconsistent Hostname and IP Address](#)
- [51891 \(1\) - SSL Session Resume Supported](#)
- [53513 \(1\) - Link-Local Multicast Name Resolution \(LLMNR\) Detection](#)
- [54615 \(1\) - Device Type](#)
- [56984 \(1\) - SSL / TLS Versions Supported](#)
- [57041 \(1\) - SSL Perfect Forward Secrecy Cipher Suites Supported](#)
- [62563 \(1\) - SSL Compression Methods Supported](#)
- [64814 \(1\) - Terminal Services Use SSL/TLS](#)
- [66173 \(1\) - RDP Screenshot](#)
- [66334 \(1\) - Patch Report](#)
- [70544 \(1\) - SSL Cipher Block Chaining Cipher Suites Supported](#)

Hosts Summary (Executive)

192.168.134.131					
Summary					
Critical	High	Medium	Low	Info	Total
0	1	6	2	32	41
Details					
Severity	Plugin Id	Name			
High (9.3)	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)			
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted			
Medium (6.4)	57582	SSL Self-Signed Certificate			
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness			
Medium (5.0)	57608	SMB Signing Required			
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low			
Medium (4.3)	58453	Terminal Services Doesn't Use Network Level Authentication (NLA)			
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant			
Low (2.6)	65821	SSL RC4 Cipher Suites Supported			
Info	10114	ICMP Timestamp Request Remote Date Disclosure			

Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	46215	Inconsistent Hostname and IP Address
Info	51891	SSL Session Resume Supported
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	64814	Terminal Services Use SSL/TLS
Info	66173	RDP Screenshot
Info	66334	Patch Report
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

Vulnerabilities By Host

[-] Collapse All

[+] Expand All

192.168.134.131

Scan Information

Start time: Fri Dec 02 11:26:42 2016

End time: Fri Dec 02 11:57:59 2016

Host Information

DNS Name: WIN-F36N0716668

Netbios: WIN-F36N0716668

Name:

IP: 192.168.134.131

MAC Address: 00:0c:29:50:b1:67

OS: Microsoft Windows 7 Ultimate

Results Summary


Critical	High	Medium	Low	Info	Total
0	1	6	2	43	52

Results Details

0/icmp


	10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
---	---	-------

0/tcp

	24786 - Nessus Windows Scan Not Performed with Admin Privileges	[-/+]
---	---	-------


	12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
---	--	-------


	25220 - TCP/IP Timestamps Supported	[-/+]
---	-------------------------------------	-------

	46215 - Inconsistent Hostname and IP Address	[-/+]
---	--	-------


	20094 - VMware Virtual Machine Detection	[-/+]
---	--	-------

	35716 - Ethernet Card Manufacturer Detection	[-/+]
---	--	-------

	11936 - OS Identification	[-/+]
---	---------------------------	-------


	54615 - Device Type	[-/+]
---	---------------------	-------

	45590 - Common Platform Enumeration (CPE)	[-/+]
---	---	-------

	66334 - Patch Report	[-/+]
---	----------------------	-------


	19506 - Nessus Scan Information	[-/+]
---	---------------------------------	-------

0/udp


	10287 - Traceroute Information	[-/+]
---	--------------------------------	-------

135/tcp

	10736 - DCE Services Enumeration	[-/+]
---	----------------------------------	-------

	11219 - Nessus SYN scanner	[-/+]
---	----------------------------	-------

137/udp

	10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
---	--	-------

139/tcp

	11011 - Microsoft Windows SMB Service Detection	[-/+]
445/tcp		
	57608 - SMB Signing Required	[-/+]
	11011 - Microsoft Windows SMB Service Detection	[-/+]
	10736 - DCE Services Enumeration	[-/+]
	10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
	10394 - Microsoft Windows SMB Log In Possible	[-/+]
	26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	[-/+]
	10397 - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure	[-/+]
554/tcp		
	11219 - Nessus SYN scanner	[-/+]
2869/tcp		
	11219 - Nessus SYN scanner	[-/+]
	11153 - Service Detection (HELP Request)	[-/+]
3389/tcp		
	58435 - MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	[-/+]
	57582 - SSL Self-Signed Certificate	[-/+]
	51192 - SSL Certificate Cannot Be Trusted	[-/+]
	58453 - Terminal Services Doesn't Use Network Level Authentication (NLA)	[-/+]
	57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
	18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
	30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
	65821 - SSL RC4 Cipher Suites Supported	[-/+]
	11219 - Nessus SYN scanner	[-/+]
	64814 - Terminal Services Use SSL/TLS	[-/+]
	66173 - RDP Screenshot	[-/+]
	56984 - SSL / TLS Versions Supported	[-/+]

	62563 - SSL Compression Methods Supported	[-/+]
	10863 - SSL Certificate Information	[-/+]
	21643 - SSL Cipher Suites Supported	[-/+]
	57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
	70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
	51891 - SSL Session Resume Supported	[-/+]
5355/udp		
	53513 - Link-Local Multicast Name Resolution (LLMNR) Detection	[-/+]
49152/tcp		
	10736 - DCE Services Enumeration	[-/+]
49153/tcp		
	10736 - DCE Services Enumeration	[-/+]
49154/tcp		
	10736 - DCE Services Enumeration	[-/+]
49155/tcp		
	10736 - DCE Services Enumeration	[-/+]
49156/tcp		
	10736 - DCE Services Enumeration	[-/+]
49157/tcp		
	10736 - DCE Services Enumeration	[-/+]

Vulnerabilities By Plugin

[-] Collapse All

[+] Expand All

58435 (1) - MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)

Synopsis

The remote Windows host could allow arbitrary code execution.

Description

An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted.

If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it.

This plugin also checks for a denial of service vulnerability in Microsoft Terminal Server.

Note that this script does not detect the vulnerability if the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting is enabled or the security layer is set to 'SSL (TLS 1.0)' on the remote host.

See Also

<http://technet.microsoft.com/en-us/security/bulletin/ms12-020>

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Note that an extended support contract with Microsoft is required to obtain the patch for this vulnerability for Windows 2000.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

STIG Severity

I

References

BID	52353
BID	52354
CVE	CVE-2012-0002
CVE	CVE-2012-0152
XREF	OSVDB:80000
XREF	OSVDB:80004
XREF	EDB-ID:18606
XREF	IAVA:2012-A-0039
XREF	MSFT:MS12-020

Exploitable with

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

Plugin Information:

Publication date: 2012/03/22, Modification date: 2014/01/07

Hosts

192.168.134.131 (tcp/3389)

18405 (1) - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

Synopsis

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

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

See Also

<http://www.oxid.it/downloads/rdp-gbu.pdf>

<http://www.nessus.org/u?e2628096>

<http://technet.microsoft.com/en-us/library/cc782610.aspx>

Solution

- Force the use of SSL as a transport layer for this service if supported, or/and
- Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

4.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

References

BID	13818
CVE	CVE-2005-1794
XREF	OSVDB:17131

Plugin Information:

Publication date: 2005/06/01, Modification date: 2014/03/04

Hosts

192.168.134.131 (tcp/3389)

51192 (1) - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.

First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

Second, the certificate chain may contain a certificate that is not valid at the time of the

scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Publication date: 2010/12/15, Modification date: 2014/02/27

Hosts

192.168.134.131 (tcp/3389)

The following certificate was at the top of the certificate chain sent by the remote host, but is signed by an unknown certificate authority :

```
| -Subject : CN=WIN-F36N0716668  
| -Issuer : CN=WIN-F36N0716668
```

57582 (1) - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Publication date: 2012/01/17, Modification date: 2012/10/25

Hosts

192.168.134.131 (tcp/3389)

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

|-Subject : CN=WIN-F36N0716668

57608 (1) - SMB Signing Required

Synopsis

Signing is not required on the remote SMB server.

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/cc731957.aspx>

<http://www.nessus.org/u?74b80723>

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

<http://www.nessus.org/u?a3cac4ea>

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server:

Digitally sign communications (always)'. On Samba, the setting is called 'server signing'.

See the 'see also' links for further details.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Publication date: 2012/01/19, Modification date: 2014/05/08

Hosts

192.168.134.131 (tcp/445)

57690 (1) - Terminal Services Encryption Level is Medium or Low

Synopsis

The remote host is using weak cryptography.

Description

The remote Terminal Services service is not configured to use strong cryptography.

Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.

Solution

Change RDP encryption level to one of :

3. High

4. FIPS Compliant

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Publication date: 2012/01/25, Modification date: 2014/01/07

Hosts**192.168.134.131 (tcp/3389)**

The terminal services encryption level is set to :

2. Medium

58453 (1) - Terminal Services Doesn't Use Network Level Authentication (NLA)**Synopsis**

The remote Terminal Services doesn't use Network Level Authentication.

Description

The remote Terminal Services is not configured to use Network Level Authentication (NLA). NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

See Also

<http://technet.microsoft.com/en-us/library/cc732713.aspx>

<http://www.nessus.org/u?e2628096>

Solution

Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Publication date: 2012/03/23, Modification date: 2013/08/05

Hosts**192.168.134.131 (tcp/3389)****30218 (1) - Terminal Services Encryption Level is not FIPS-140 Compliant****Synopsis**

The remote host is not FIPS-140 compliant.

Description

The encryption setting used by the remote Terminal Services 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 Information:

Publication date: 2008/02/11, Modification date: 2014/01/07

Hosts**192.168.134.131 (tcp/3389)**

The terminal services encryption level is set to :

2. Medium (Client Compatible)

65821 (1) - SSL RC4 Cipher Suites Supported**Synopsis**

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g. HTTP cookies), and an attacker is able to obtain many (i.e. tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

<http://www.nessus.org/u?217a3666>

<http://cr.yp.to/talks/2013.03.12/slides.pdf>

<http://www.isg.rhul.ac.uk/tls/>

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.3 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

BID [58796](#)

CVE [CVE-2013-2566](#)

XREF [OSVDB:91162](#)

Plugin Information:

Publication date: 2013/04/05, Modification date: 2014/02/27

Hosts**192.168.134.131 (tcp/3389)**

Here is the list of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

TLSv1

RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5

RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}

Kx={key exchange}

Au={authentication}

Enc={symmetric encryption method}

Mac={message authentication code}

{export flag}

10736 (8) - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Hosts

192.168.134.131 (tcp/135)

The following DCERPC services are available locally :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
 UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0
 Description : Unknown RPC service
 Type : Local RPC service
 Named pipe : WindowsShutdown

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
 UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0
 Description : Unknown RPC service
 Type : Local RPC service
 Named pipe : WMsgKRpc097DC0

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
 UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
 Description : Unknown RPC service
 Type : Local RPC service
 Named pipe : WindowsShutdown

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
 UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
 Description : Unknown RPC service
 Type : Local RPC service

Named pipe : WMsgKRpc097DC0

Object UUID : 6d726574-7273-0076-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-772aee7d58e8ea8dba

Object UUID : 52ef130c-08fd-4388-86b3-6edf00000001
UUID : 12e65dd8-887f-41ef-91bf-8d816c42c2e7, version 1.0
Description : Unknown RPC service
Annotation : Secure Desktop LRPC interface
Type : Local RPC service
Named pipe : WMsgKRpc097F21

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000001
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc097F21

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4b112204-0e19-11d3-b42b-0000f81feb9f, version 1.0
Description : SSDP service
Windows process : unknow
Type : Local RPC service
Named pipe : LRPC-6e6285dc3e89763af6

Object UUID : c9a47e12-e999-4e73-9008-3082c99e07cb
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-340dc825aa693b681e

Object UUID : 0a1b1724-cb04-4715-aff8-76ec9a3c2e64
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-340dc825aa693b681e

Object UUID : 46a9b761-e17d-45a2-8c3b-4b4cbb6c17f5
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-340dc825aa693b681e

Object UUID : b6f778fc-5c81-432f-8db4-f5732e3ab458
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-340dc825aa693b681e

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 : LRPC-0da4c7875cee6dc448

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 : LRPC-c3772f9ef0b1d18784

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 : LSARPC_ENDPOINT

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 : lsapolicylookup

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 : lsasspirpc

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 : samss_lpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0767a036-0d22-48aa-ba69-b619480f38cb, version 1.0
Description : Unknown RPC service
Annotation : PcaSvc
Type : Local RPC service
Named pipe : OLE83830492534F4CCD8FD42ADD7326

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0767a036-0d22-48aa-ba69-b619480f38cb, version 1.0
Description : Unknown RPC service
Annotation : PcaSvc
Type : Local RPC service
Named pipe : LRPC-ce74f76ca8f8921990

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : dd490425-5325-4565-b774-7e27d6c09c24, version 1.0
Description : Unknown RPC service

Annotation : Base Firewall Engine API
Type : Local RPC service
Named pipe : LRPC-233e614583021e5067

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-233e614583021e5067

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-233e614583021e5067

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfba-4a24-4fc6-8a23-942bleca65d1, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Local RPC service
Named pipe : spoolss

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Annotation : Spooler base remote object endpoint
Type : Local RPC service
Named pipe : spoolss

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Local RPC service
Named pipe : spoolss

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7ea70bcf-48af-4f6a-8968-6a440754d5fa, version 1.0
Description : Unknown RPC service
Annotation : NSI server endpoint
Type : Local RPC service
Named pipe : OLE7804B45D33284F10A3BE99955C36

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7ea70bcf-48af-4f6a-8968-6a440754d5fa, version 1.0
Description : Unknown RPC service
Annotation : NSI server endpoint
Type : Local RPC service
Named pipe : LRPC-22fc2b5b05a046f9d1

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 : OLE7804B45D33284F10A3BE99955C36

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 : LRPC-22fc2b5b05a046f9d1

Object UUID : 6c637067-6569-746e-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0

Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 666f7270-6c69-7365-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 24d1f7c7-76af-4f28-9ccd-7f6cb6468601
UUID : 2eb08e3e-639f-4fba-97b1-14f878961076, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 24d1f7c7-76af-4f28-9ccd-7f6cb6468601
UUID : 2eb08e3e-639f-4fba-97b1-14f878961076, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEEA4C0E2541C24E218AC5E6075FE0

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : OLEEA4C0E2541C24E218AC5E6075FE0

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fblcdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fblcdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLEEA4C0E2541C24E218AC5E6075FE0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fblcdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : senssvc

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 : IUserProfile2

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 : OLEEA4C0E2541C24E218AC5E6075FE0

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 : senssvc

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 : IUserProfile2

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 : OLEEA4C0E2541C24E218AC5E6075FE0

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 : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEEA4C0E2541C24E218AC5E6075FE0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Local RPC service

Named pipe : OLEEA4C0E2541C24E218AC5E6075FE0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3cle0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Local RPC service
Named pipe : OLEEA4C0E2541C24E218AC5E6075FE0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : OLEEA4C0E2541C24E218AC5E6075FE0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : senssvc

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : OLEEA4C0E2541C24E218AC5E6075FE0

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name

Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEEA4C0E2541C24E218AC5E6075FE0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Local RPC service
Named pipe : eventlog

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 : eventlog

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 : AudioClientRpc

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 : Audiosrv

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-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0

Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service
Named pipe : AudioClientRpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service
Named pipe : Audiosrv

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc6

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Local RPC service
Named pipe : AudioClientRpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Local RPC service
Named pipe : Audiosrv

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Local RPC service
Named pipe : dhcpcsvc6

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Local RPC service
Named pipe : OLEDC79DED0D766462AAF5B89F94561

Object UUID : 00000000-0000-0000-0000-000000000000

UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : AudioClientRpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : Audiosrv

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : dhcpcsvc6

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : OLEDC79DED0D766462AAF5B89F94561

192.168.134.131 (tcp/445)

The following DCERPC services are available remotely :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\WIN-F36N0716668

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\WIN-F36N0716668

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 : \\WIN-F36N0716668

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 : \WIN-F36N0716668

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 : \WIN-F36N0716668

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 : \WIN-F36N0716668

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \WIN-F36N0716668

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3cle0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \WIN-F36N0716668

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \WIN-F36N0716668

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \WIN-F36N0716668

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \WIN-F36N0716668

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
Named pipe : \PIPE\srsvsvc
Netbios name : \WIN-F36N0716668

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN-F36N0716668

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\srsvsvc
Netbios name : \\WIN-F36N0716668

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\WIN-F36N0716668

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 : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\WIN-F36N0716668

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\WIN-F36N0716668

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\WIN-F36N0716668

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\WIN-F36N0716668

192.168.134.131 (tcp/49152)

The following DCERPC services are available on TCP port 49152 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49152
IP : 192.168.134.131

192.168.134.131 (tcp/49153)

The following DCERPC services are available on TCP port 49153 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.134.131

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 : Remote RPC service
TCP Port : 49153
IP : 192.168.134.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.134.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.134.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.134.131

192.168.134.131 (tcp/49154)

The following DCERPC services are available on TCP port 49154 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.134.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3cle0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.134.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint

Type : Remote RPC service
TCP Port : 49154
IP : 192.168.134.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.134.131

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.134.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.134.131

192.168.134.131 (tcp/49155)

The following DCERPC services are available on TCP port 49155 :

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 : 49155
IP : 192.168.134.131

192.168.134.131 (tcp/49156)

The following DCERPC services are available on TCP port 49156 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.134.131

192.168.134.131 (tcp/49157)

The following DCERPC services are available on TCP port 49157 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1.0
Description : Unknown RPC service
Annotation : Remote Fw APIs
Type : Remote RPC service
TCP Port : 49157
IP : 192.168.134.131

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 : 49157
IP : 192.168.134.131

11219 (4) - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2014/01/23

Hosts

192.168.134.131 (tcp/135)

Port 135/tcp was found to be open

192.168.134.131 (tcp/554)

Port 554/tcp was found to be open

192.168.134.131 (tcp/2869)

Port 2869/tcp was found to be open

192.168.134.131 (tcp/3389)

Port 3389/tcp was found to be open

11011 (2) - Microsoft Windows SMB Service Detection

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2012/01/31

Hosts

192.168.134.131 (tcp/139)

An SMB server is running on this port.

192.168.134.131 (tcp/445)

A CIFS server is running on this port.

10114 (1) - ICMP Timestamp Request Remote Date Disclosure**Synopsis**

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

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

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

Risk Factor

None

References

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

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Hosts**192.168.134.131 (icmp/0)**

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 -695 seconds.

10150 (1) - Windows NetBIOS / SMB Remote Host Information Disclosure**Synopsis**

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

Description

The remote host listens on UDP port 137 or TCP port 445 and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2013/01/16

Hosts**192.168.134.131 (udp/137)**

The following 6 NetBIOS names have been gathered :

```
WIN-F36N0716668 = File Server Service
WIN-F36N0716668 = Computer name
WORKGROUP = Workgroup / Domain name
WORKGROUP = Browser Service Elections
WORKGROUP = Master Browser
__MSBROWSE__ = Master Browser
```

The remote host has the following MAC address on its adapter :

00:0c:29:50:b1:67

10287 (1) - Traceroute Information**Synopsis**

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Hosts**192.168.134.131 (udp/0)**

```
For your information, here is the traceroute from
192.168.134.129 to 192.168.134.131 :
192.168.134.129
192.168.134.131
```

10394 (1) - Microsoft Windows SMB Log In Possible**Synopsis**

It is possible to log into the remote host.

Description

The remote host is running Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :

- NULL session
- Guest account
- Given Credentials

See Also

<http://support.microsoft.com/kb/143474>

<http://support.microsoft.com/kb/246261>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2014/04/07

Hosts**192.168.134.131 (tcp/445)**

- NULL sessions are enabled on the remote host

10397 (1) - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure**Synopsis**

It is possible to obtain network information.

Description

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

Solution

n/a

Risk Factor

None

References**XREF**[OSVDB:300](#)**Plugin Information:**

Publication date: 2000/05/09, Modification date: 2011/09/14

Hosts**192.168.134.131 (tcp/445)**

Here is the browse list of the remote host :

COMAT-UPVXLC8CB (os : 5.1)
WIN-F36N0716668 (os : 6.1)

10785 (1) - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure**Synopsis**

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/10/17, Modification date: 2014/04/09

Hosts

192.168.134.131 (tcp/445)

The remote Operating System is : Windows 7 Ultimate 7601 Service Pack 1
The remote native lan manager is : Windows 7 Ultimate 6.1
The remote SMB Domain Name is : WIN-F36N0716668

10863 (1) - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2012/04/02

Hosts

192.168.134.131 (tcp/3389)

Subject Name:

Common Name: WIN-F36N0716668

Issuer Name:

Common Name: WIN-F36N0716668

Serial Number: 1E EE BE A2 84 07 A1 B6 46 58 27 4E C2 36 7F 85

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Nov 30 08:21:54 2016 GMT

Not Valid After: Jun 01 08:21:54 2017 GMT

Public Key Info:

Algorithm: RSA Encryption

Key Length: 2048 bits

Public Key: 00 F0 AE 96 0D 73 29 5D 82 D2 3E 1F 21 3C C0 D1 32
A6 88 95

48 32 E5 1A A4 7C 23 F5 F1 A4 05 22 2F B1 B5 4B 15 B4 BB 00
ED BC 35 D0 AB 39 44 23 A7 58 3F 47 05 A5 F2 26 A7 FD 38 6A
95 F5 52 26 48 82 CC CE CC 20 40 76 FF FB 66 94 1C 2F 70 3B
3E FD C5 D7 43 E2 E5 95 6C 7B E8 05 00 E6 1B 88 A8 2F 8B 83
65 BF AB 88 0B 54 8F EB 53 14 E0 13 A7 E9 D3 F9 60 DD 77 42
1F 48 D9 BA C9 F9 F1 02 EE E5 61 C9 83 62 DF F8 81 C6 26 CA
F6 3F D9 68 AC 18 54 B7 C9 DE C4 61 44 53 D6 1E AD 57 A1 71
44 C8 95 B1 6E 60 E8 09 D1 4A 1E 8B B4 BE 2E 5E EC CB F9 0C
10 87 A7 24 01 DB 06 D5 C9 10 3B 7E 7B DC FA 5B 18 6A 6B 67
4B DB 21 5F F4 B0 B2 B2 72 5A 92 D3 3E 1E 95 69 AD 0B C3 D5
12 64 0C FA 46 15 87 E3 AA 2C 83 0F 3B 33 6C 8B AE E0 20 03
74 72 25 25 F7 82 D2 62 B9 D7 83 00 A3 96 2C 46 41

Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 4B 7D 1C DB CC 12 A2 1E 91 44 96 9A 16 48 9B EA 48 F4 CF
70 8C 45 4E F6 B0 FD D6 8C AC 79 9E 35 1E 19 CE BF DB E2 3F
E6 8E A3 B0 03 47 7F FD F9 5F A7 4C 19 C2 F0 D7 60 68 57 8E
08 63 C1 46 E7 26 FA 35 51 81 29 E5 56 79 1D 34 73 08 2F D2
39 6D D0 F9 19 F7 08 E2 51 5B 71 4F 80 85 5A A3 E9 02 1C 40
B5 B3 9F 98 BB E0 F1 44 90 C5 2E 97 EE 34 39 F7 21 44 0F CC
67 D6 BE 0E 14 51 2A C1 34 8E 56 41 87 1C 22 25 F3 BE DA AF
73 D7 30 06 BA A5 68 8B BE 7D F9 C5 DD 82 8E E8 7D 90 7F 7F
13 5C F4 76 DE 19 DA 90 10 7F 5E D3 63 2C 57 D9 9F 5E 7D 49
94 63 22 A1 E0 25 95 F2 7D A8 F7 28 4C 05 5D BA A6 CC F3 6B
A9 27 E5 34 DA AF 6B 2F A4 18 FB 51 FD 05 8F 85 35 40 CF 56
C7 74 D5 A5 C8 7E 44 A5 35 D1 C2 49 CB 97 1B 5C 61 FA FA 3E
40 EF 0D 0E 79 35 59 38 D1 AF B7 CF 9F 57 F8 45 FD

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)

Extension: Key Usage (2.5.29.15)
Critical: 0
Key Usage: Key Encipherment, Data Encipherment

11153 (1) - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

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.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/11/18, Modification date: 2014/04/10

Hosts

192.168.134.131 (tcp/2869)

A web server seems to be running on this port.

11936 (1) - OS Identification

Synopsis

It is possible to guess the remote operating system.

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. It is also sometimes possible to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2014/02/19

Hosts

192.168.134.131 (tcp/0)

Remote operating system : Microsoft Windows 7 Ultimate
Confidence Level : 99
Method : MSRPC

The remote host is running Microsoft Windows 7 Ultimate

12053 (1) - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the FQDN of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/02/11, Modification date: 2012/09/28

Hosts

192.168.134.131 (tcp/0)

192.168.134.131 resolves as WIN-F36N0716668.

19506 (1) - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :

- The version of the plugin set
- The type of scanner (Nessus or Nessus Home)
- 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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2014/04/07

Hosts**192.168.134.131 (tcp/0)**

Information about this scan :

Nessus version : 5.2.5 (Nessus 5.2.6 is available - consider upgrading)

Plugin feed version : 201405201615

Scanner edition used : Nessus Home

ERROR: Your plugins have not been updated since 2014/5/20
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run `nessus-update-plugins` to
get the
newest vulnerability checks from Nessus.org.

Scan policy used : Day2_1
Scanner IP : 192.168.134.129
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 : 5
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2016/12/2 11:26
Scan duration : 1877 sec

20094 (1) - VMware Virtual Machine Detection**Synopsis**

The remote host seems to be a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2011/03/27

Hosts**192.168.134.131 (tcp/0)****21643 (1) - SSL Cipher Suites Supported**

Synopsis

The remote service encrypts communications using SSL.

Description

This script detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

<http://www.openssl.org/docs/apps/ciphers.html>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2014/01/15

Hosts

192.168.134.131 (tcp/3389)

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

TLSt1

ECDHE-RSA-AES128-SHA Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA1

ECDHE-RSA-AES256-SHA Kx=ECDH Au=RSA Enc=AES-CBC(256) Mac=SHA1

DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1

AES128-SHA Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA1

AES256-SHA Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA1

RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5

RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}

Kx={key exchange}

Au={authentication}

Enc={symmetric encryption method}

Mac={message authentication code}

{export flag}

24786 (1) - Nessus Windows Scan Not Performed with Admin Privileges**Synopsis**

The Nessus scan of this host may be incomplete due to insufficient privileges provided.

Description

The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.

Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.

If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

Plugin Information:

Publication date: 2007/03/12, Modification date: 2013/01/07

Hosts

192.168.134.131 (tcp/0)

It was not possible to connect to '\\WIN-F36N0716668\\ADMIN\$' with the supplied credentials.

25220 (1) - TCP/IP Timestamps Supported**Synopsis**

The remote service implements TCP timestamps.

Description

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

See Also

<http://www.ietf.org/rfc/rfc1323.txt>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Hosts

192.168.134.131 (tcp/0)

26917 (1) - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry**Synopsis**

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\\winreg on the remote host.

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/10/04, Modification date: 2011/03/27

Hosts

192.168.134.131 (tcp/445)

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

35716 (1) - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be deduced from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2011/03/27

Hosts

192.168.134.131 (tcp/0)

The following card manufacturers were identified :

00:0c:29:50:b1:67 : VMware, Inc.

45590 (1) - Common Platform Enumeration (CPE)

Synopsis

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

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

<http://cpe.mitre.org/>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2014/05/15

Hosts

192.168.134.131 (tcp/0)

The remote operating system matched the following CPE :

cpe:/o:microsoft:windows_7:::ultimate

46215 (1) - Inconsistent Hostname and IP Address

Synopsis

The remote host's hostname is not consistent with DNS information.

Description

The name of this machine either does not resolve or resolves to a different IP address.

This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host.

As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.

Solution

Fix the reverse DNS or host file.

Risk Factor

None

Plugin Information:

Publication date: 2010/05/03, Modification date: 2011/10/06

Hosts

192.168.134.131 (tcp/0)

The host name 'WIN-F36N0716668' resolves to 192.168.134.129, not to 192.168.134.131

51891 (1) - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/02/07, Modification date: 2013/10/18

Hosts

192.168.134.131 (tcp/3389)

This port supports resuming TLSv1 sessions.

53513 (1) - Link-Local Multicast Name Resolution (LLMNR) Detection

Synopsis

The remote device supports LLMNR.

Description

The remote device answered to a Link-local Multicast Name Resolution (LLMNR) request. This protocol provides a name lookup service similar to NetBIOS or DNS. It is enabled by default on modern Windows versions.

See Also

<http://www.nessus.org/u?85beb421>

<http://technet.microsoft.com/en-us/library/bb878128.aspx>

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2011/04/21, Modification date: 2012/03/05

Hosts

192.168.134.131 (udp/5355)

According to LLMNR, the name of the remote host is 'WIN-F36N0716668'.

54615 (1) - Device Type

Synopsis

It is possible to guess the remote 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).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Hosts

192.168.134.131 (tcp/0)

Remote device type : general-purpose
Confidence level : 99

56984 (1) - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2014/04/14

Hosts**192.168.134.131 (tcp/3389)**

This port supports TLSv1.0.

57041 (1) - SSL Perfect Forward Secrecy Cipher Suites Supported**Synopsis**

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

<http://www.openssl.org/docs/apps/ciphers.html>

http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

http://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2012/04/02

Hosts**192.168.134.131 (tcp/3389)**

Here is the list of SSL PFS ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

TLSv1

ECDHE-RSA-AES128-SHA Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA1

ECDHE-RSA-AES256-SHA Kx=ECDH Au=RSA Enc=AES-CBC(256) Mac=SHA1

The fields above are :

{OpenSSL ciphername}

Kx={key exchange}

Au={authentication}

Enc={symmetric encryption method}

Mac={message authentication code}

{export flag}

62563 (1) - SSL Compression Methods Supported**Synopsis**

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

<http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml>

<http://tools.ietf.org/html/rfc3749>

<http://tools.ietf.org/html/rfc3943>

<http://tools.ietf.org/html/rfc5246>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/10/16, Modification date: 2013/10/18

Hosts

192.168.134.131 (tcp/3389)

Nessus was able to confirm that the following compression method is supported by the target :

NULL (0x00)

64814 (1) - Terminal Services Use SSL/TLS

Synopsis

The remote Terminal Services use SSL/TLS.

Description

The remote Terminal Services is configured to use SSL/TLS.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/02/22, Modification date: 2013/08/28

Hosts

192.168.134.131 (tcp/3389)

Subject Name:

Common Name: WIN-F36N0716668

Issuer Name:

Common Name: WIN-F36N0716668

Serial Number: 1E EE BE A2 84 07 A1 B6 46 58 27 4E C2 36 7F 85

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Nov 30 08:21:54 2016 GMT
Not Valid After: Jun 01 08:21:54 2017 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 F0 AE 96 0D 73 29 5D 82 D2 3E 1F 21 3C C0 D1 32
A6 88 95
48 32 E5 1A A4 7C 23 F5 F1 A4 05 22 2F B1 B5 4B 15 B4 BB 00
ED BC 35 D0 AB 39 44 23 A7 58 3F 47 05 A5 F2 26 A7 FD 38 6A
95 F5 52 26 48 82 CC CE CC 20 40 76 FF FB 66 94 1C 2F 70 3B
3E FD C5 D7 43 E2 E5 95 6C 7B E8 05 00 E6 1B 88 A8 2F 8B 83
65 BF AB 88 0B 54 8F EB 53 14 E0 13 A7 E9 D3 F9 60 DD 77 42
1F 48 D9 BA C9 F9 F1 02 EE E5 61 C9 83 62 DF F8 81 C6 26 CA
F6 3F D9 68 AC 18 54 B7 C9 DE C4 61 44 53 D6 1E AD 57 A1 71
44 C8 95 B1 6E 60 E8 09 D1 4A 1E 8B B4 BE 2E 5E EC CB F9 0C
10 87 A7 24 01 DB 06 D5 C9 10 3B 7E 7B DC FA 5B 18 6A 6B 67
4B DB 21 5F F4 B0 B2 B2 72 5A 92 D3 3E 1E 95 69 AD 0B C3 D5
12 64 0C FA 46 15 87 E3 AA 2C 83 0F 3B 33 6C 8B AE E0 20 03
74 72 25 25 F7 82 D2 62 B9 D7 83 00 A3 96 2C 46 41
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 4B 7D 1C DB CC 12 A2 1E 91 44 96 9A 16 48 9B EA 48
F4 CF
70 8C 45 4E F6 B0 FD D6 8C AC 79 9E 35 1E 19 CE BF DB E2 3F
E6 8E A3 B0 03 47 7F FD F9 5F A7 4C 19 C2 F0 D7 60 68 57 8E
08 63 C1 46 E7 26 FA 35 51 81 29 E5 56 79 1D 34 73 08 2F D2
39 6D D0 F9 19 F7 08 E2 51 5B 71 4F 80 85 5A A3 E9 02 1C 40
B5 B3 9F 98 BB E0 F1 44 90 C5 2E 97 EE 34 39 F7 21 44 0F CC
67 D6 BE 0E 14 51 2A C1 34 8E 56 41 87 1C 22 25 F3 BE DA AF
73 D7 30 06 BA A5 68 8B BE 7D F9 C5 DD 82 8E E8 7D 90 7F 7F
13 5C F4 76 DE 19 DA 90 10 7F 5E D3 63 2C 57 D9 9F 5E 7D 49
94 63 22 A1 E0 25 95 F2 7D A8 F7 28 4C 05 5D BA A6 CC F3 6B
A9 27 E5 34 DA AF 6B 2F A4 18 FB 51 FD 05 8F 85 35 40 CF 56
C7 74 D5 A5 C8 7E 44 A5 35 D1 C2 49 CB 97 1B 5C 61 FA FA 3E
40 EF 0D 0E 79 35 59 38 D1 AF B7 CF 9F 57 F8 45 FD

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)

Extension: Key Usage (2.5.29.15)
Critical: 0
Key Usage: Key Encipherment, Data Encipherment

66173 (1) - RDP Screenshot

Synopsis

It is possible to take a screenshot of the remote login screen.

Description

This script attempts to connect to the remote host via RDP (Remote Desktop Protocol) and attempts to take a screenshot of the login screen.

While this is not a vulnerability by itself, some versions of Windows display the names of the users who can connect and which ones are connected already.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/04/22, Modification date: 2014/01/07

Hosts

192.168.134.131 (tcp/3389)

It was possible to gather the following screenshot of the remote login screen.

66334 (1) - Patch Report**Synopsis**

The remote host is missing several patches.

Description

The remote host is missing one or several security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information:

Publication date: 2013/05/07, Modification date: 2014/05/13

Hosts

192.168.134.131 (tcp/0)

. You need to take the following 2 actions:

[Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness (18405)]

+ Action to take: - Force the use of SSL as a transport layer for this service if supported, or/and

- Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

[MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435)]

+ Action to take: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Note that an extended support contract with Microsoft is required to obtain the patch for this vulnerability for Windows 2000.

+ Impact: Taking this action will resolve 2 different vulnerabilities (CVEs).

70544 (1) - SSL Cipher Block Chaining Cipher Suites Supported**Synopsis**

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

<http://www.openssl.org/docs/apps/ciphers.html>

<http://www.nessus.org/u?cc4a822a>

<http://www.openssl.org/~bodo/tls-cbc.txt>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/22, Modification date: 2013/10/22

Hosts

192.168.134.131 (tcp/3389)

Here is the list of SSL CBC ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

TLSv1

ECDHE-RSA-AES128-SHA Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA1

ECDHE-RSA-AES256-SHA Kx=ECDH Au=RSA Enc=AES-CBC(256) Mac=SHA1

DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1

AES128-SHA Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA1

AES256-SHA Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA1

The fields above are :

{OpenSSL ciphername}

Kx={key exchange}

Au={authentication}

Enc={symmetric encryption method}

Mac={message authentication code}

{export flag}

This is a report from the Nessus Vulnerability Scanner .

Nessus is published by Tenable Network Security, Inc | 7021 Columbia Gateway Drive Suite 500, Columbia, MD 21046

© 2016 Tenable Network Security, Inc. All rights reserved.