Open Vas Final Report

Report generated by Nessus™ Sat, 09 Nov 2019 21:52:12 CST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.1.101

0	1	13	3	110
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Sat Nov 9 21:47:51 2019
End time: Sat Nov 9 21:52:12 2019

Host Information

Netbios Name: SERVER2016
IP: 192.168.1.101
MAC Address: 00:50:56:9A:9B:EA
OS: Microsoft Windows Server 2012 R2 Datacenter

Vulnerabilities

41028 - SNMP Agent Default Community Name (public)

Synopsis

The community name of the remote SNMP server can be guessed.

Description

It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Solution

Disable the SNMP service on the remote host if you do not use it.

Either filter incoming UDP packets going to this port, or change the default community string.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	2112
CVE	CVE-1999-0517

Plugin Information

Published: 2002/11/25, Modified: 2018/08/22

Plugin Output

udp/161

```
The remote SNMP server replies to the following default community
string :

public
```

90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Synopsis

The remote Windows host is affected by an elevation of privilege vulnerability.

Description

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

See Also

http://www.nessus.org/u?52ade1e9

http://badlock.org/

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

Risk Factor

Medium

CVSS v3.0 Base Score

6.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N)

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

BID	86002
CVE	CVE-2016-0128
MSKB	3148527
MSKB	3149090
MSKB	3147461
MSKB	3147458
XREF	MSFT:MS16-047
XREF	CERT:813296
XREF	IAVA:2016-A-0093

Plugin Information

Published: 2016/04/13, Modified: 2019/07/23

Plugin Output

tcp/49157

18405 - 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?8033da0d

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

3.8 (CVSS2#E:U/RL:OF/RC:C)

References

BID	13818
CVE	CVE-2005-1794

Plugin Information

Published: 2005/06/01, Modified: 2018/08/01

Plugin Output

tcp/3389

57608 - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing

http://technet.microsoft.com/en-us/library/cc731957.aspx

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

https://www.samba.org/samba/docs/current/man-html/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 v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

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

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information

Published: 2012/01/19, Modified: 2018/11/15

Plugin Output

tcp/445

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- 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.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2018/11/15

Plugin Output

tcp/3389

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

|-Subject : CN=Server2016
|-Issuer  : CN=Server2016
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- 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.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2018/11/15

Plugin Output

tcp/49159

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

|-Subject : CN=SSL_Self_Signed_Fallback
|-Issuer  : CN=SSL_Self_Signed_Fallback
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

http://www.nessus.org/u?e120eea1

http://www.nessus.org/u?5d894816

http://www.nessus.org/u?51db68aa

http://www.nessus.org/u?9dc7bfba

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS Base Score

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

CVSS Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2009/01/05, Modified: 2019/03/27

Plugin Output

tcp/3389

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

|-Subject             : CN=Server2016
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Oct 10 16:52:54 2019 GMT
|-Valid To            : Apr 10 16:52:54 2020 GMT
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS Base Score

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

Plugin Information

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/49159

```
The identities known by Nessus are :

  192.168.1.101
  192.168.1.101

The Common Name in the certificate is :

  SSL_Self_Signed_Fallback
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS Base Score

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

References

CVE	CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2019/02/28

Plugin Output

tcp/3389

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

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

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS Base Score

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

References

CVE	CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2019/02/28

Plugin Output

tcp/49159

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

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

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

57582 - 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

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

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=Server2016
```

57582 - 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

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/49159

```
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=SSL_Self_Signed_Fallback
```

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Synopsis

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

Description

The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. 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

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11)

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 v3.0 Base Score

4.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N)

CVSS Base Score

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

Plugin Information

Published: 2012/03/23, Modified: 2019/08/20

Plugin Output

tcp/3389

```
Nessus was able to negotiate non-NLA (Network Level Authentication) security.
```

57690 - 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

Published: 2012/01/25, Modified: 2019/08/20

Plugin Output

tcp/3389

```
The terminal services encryption level is set to :

2. Medium
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

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?ac7327a0

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

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

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

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 v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

CVSS Base Score

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

CVSS Temporal Score

2.2 (CVSS2#E:U/RL:ND/RC:C)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2019/07/23

Plugin Output

tcp/3389

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    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}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

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?ac7327a0

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

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

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

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 v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

CVSS Base Score

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

CVSS Temporal Score

2.2 (CVSS2#E:U/RL:ND/RC:C)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2019/07/23

Plugin Output

tcp/49159

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    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}
```

30218 - 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

Published: 2008/02/11, Modified: 2019/08/20

Plugin Output

tcp/3389

```
The terminal services encryption level is set to :

2. Medium (Client Compatible)
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was 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/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21

Plugin Output

tcp/0

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

  cpe:/o:microsoft:windows_server_2012:r2::datacenter
```

10736 - 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

Published: 2001/08/26, Modified: 2019/05/31

Plugin Output

tcp/135

```
The following DCERPC services are available locally :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, 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-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0B25A0

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 : WMsgKRpc0B25A0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
```

```
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-72a283144ccc20528e

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LSMApi

Object UUID : 3bdb59a0-d736-4d44-9074-c1ee00000003
UUID : b2507c30-b126-494a-92ac-ee32b6eeb039, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-7df78e41691f0f8d5a

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000003
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc01C4F84773

Object UUID : 3bdb59a0-d736-4d44-9074-c1ee00000002
UUID : b2507c30-b126-494a-92ac-ee32b6eeb039, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-07decaa971862b7b41

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000002
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc098502052

Objec [...]
```

10736 - 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

Published: 2001/08/26, Modified: 2019/05/31

Plugin Output

tcp/445

```
The following DCERPC services are available remotely :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\SERVER2016

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 : \\SERVER2016

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \pipe\LSM_API_service
Netbios name : \\SERVER2016

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
```

```
Named pipe : \pipe\lsass
Netbios name : \\SERVER2016

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 : \\SERVER2016

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f1343fe-50a9-4927-a778-0c5859517bac, version 1.0
Description : Unknown RPC service
Annotation : DfsDs service
Type : Remote RPC service
Named pipe : \PIPE\wkssvc
Netbios name : \\SERVER2016

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Remote RPC service
Named pipe : \PIPE\W32TIME_ALT
Netbios name : \\SERVER2016

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 : \\SERVER2016

Object UUID : 00000000-0000-0000-0000 [...]
```

10736 - 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

Published: 2001/08/26, Modified: 2019/05/31

Plugin Output

tcp/2103

```
The following DCERPC services are available on TCP port 2103 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V1
Type : Remote RPC service
TCP Port : 2103
IP : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V2
Type : Remote RPC service
TCP Port : 2103
IP : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QM2QM V1
Type : Remote RPC service
TCP Port : 2103
IP : 192.168.1.101
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0
Description : Unknown RPC service
Annotation : Message Queuing - RemoteRead V1
Type : Remote RPC service
TCP Port : 2103
IP : 192.168.1.101
```

10736 - 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

Published: 2001/08/26, Modified: 2019/05/31

Plugin Output

tcp/2105

```
The following DCERPC services are available on TCP port 2105 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V1
Type : Remote RPC service
TCP Port : 2105
IP : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V2
Type : Remote RPC service
TCP Port : 2105
IP : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QM2QM V1
Type : Remote RPC service
TCP Port : 2105
IP : 192.168.1.101
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0
Description : Unknown RPC service
Annotation : Message Queuing - RemoteRead V1
Type : Remote RPC service
TCP Port : 2105
IP : 192.168.1.101
```

10736 - 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

Published: 2001/08/26, Modified: 2019/05/31

Plugin Output

tcp/2107

```
The following DCERPC services are available on TCP port 2107 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V1
Type : Remote RPC service
TCP Port : 2107
IP : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V2
Type : Remote RPC service
TCP Port : 2107
IP : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QM2QM V1
Type : Remote RPC service
TCP Port : 2107
IP : 192.168.1.101
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0
Description : Unknown RPC service
Annotation : Message Queuing - RemoteRead V1
Type : Remote RPC service
TCP Port : 2107
IP : 192.168.1.101
```

10736 - 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

Published: 2001/08/26, Modified: 2019/05/31

Plugin Output

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 : 192.168.1.101
```

10736 - 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

Published: 2001/08/26, Modified: 2019/05/31

Plugin Output

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 : 192.168.1.101

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 : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1.0
Description : Unknown RPC service
Annotation : Wcm Service
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.1.101

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 : 192.168.1.101

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 : 192.168.1.101
```

10736 - 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

Published: 2001/08/26, Modified: 2019/05/31

Plugin Output

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 : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.1.101

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 : Remote RPC service
TCP Port : 49154
IP : 192.168.1.101

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 : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1.0
Description : Unknown RPC service
Annotation : IdSegSrv service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.1.101

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 : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager provider server endpoint
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager client server endpoint
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version  [...]
```

10736 - 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

Published: 2001/08/26, Modified: 2019/05/31

Plugin Output

tcp/49155

```
The following DCERPC services are available on TCP port 49155 :

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
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
```

```
TCP Port : 49155
IP : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.1.101
```

10736 - 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

Published: 2001/08/26, Modified: 2019/05/31

Plugin Output

tcp/49156

```
The following DCERPC services are available on TCP port 49156 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V1
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V2
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.1.101

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QM2QM V1
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.1.101
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0
Description : Unknown RPC service
Annotation : Message Queuing - RemoteRead V1
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.1.101
```

10736 - 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

Published: 2001/08/26, Modified: 2019/05/31

Plugin Output

tcp/49157

```
The following DCERPC services are available on TCP port 49157 :

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 : 49157
IP : 192.168.1.101
```

10736 - 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

Published: 2001/08/26, Modified: 2019/05/31

Plugin Output

tcp/49217

```
The following DCERPC services are available on TCP port 49217 :

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 : 49217
IP : 192.168.1.101
```

10736 - 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

Published: 2001/08/26, Modified: 2019/05/31

Plugin Output

tcp/49218

```
The following DCERPC services are available on TCP port 49218 :

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 : 49218
IP : 192.168.1.101
```

54615 - 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

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

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

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2018/11/15

Plugin Output

tcp/0

```
The following card manufacturers were identified :

00:50:56:9A:9B:EA : VMware, Inc.
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2018/08/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 00:50:56:9A:9B:EA
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/10/02

Plugin Output

tcp/21

```
The remote FTP banner is :

220 Microsoft FTP Service
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/01/04, Modified: 2019/06/07

Plugin Output

tcp/80

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/01/04, Modified: 2019/06/07

Plugin Output

tcp/5985

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/01/04, Modified: 2019/06/07

Plugin Output

tcp/47001

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

24260 - HyperText Transfer Protocol (HTTP) Information

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

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/80

```
Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html; charset=us-ascii
  Server: Microsoft-HTTPAPI/2.0
  Date: Sun, 10 Nov 2019 03:51:11 GMT
  Connection: close
  Content-Length: 315

Response Body :
```

24260 - HyperText Transfer Protocol (HTTP) Information

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

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/5985

```
Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html; charset=us-ascii
  Server: Microsoft-HTTPAPI/2.0
  Date: Sun, 10 Nov 2019 03:51:11 GMT
  Connection: close
  Content-Length: 315

Response Body :
```

24260 - HyperText Transfer Protocol (HTTP) Information

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

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/47001

```
Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html; charset=us-ascii
  Server: Microsoft-HTTPAPI/2.0
  Date: Sun, 10 Nov 2019 03:51:11 GMT
  Connection: close
  Content-Length: 315

Response Body :
```

10114 - 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

CVSS v3.0 Base Score

0.0 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

CVSS Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2019/10/04

Plugin Output

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 -147 seconds.
```

53513 - 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?51eae65d

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

Published: 2011/04/21, Modified: 2019/03/06

Plugin Output

udp/5355

```
According to LLMNR, the name of the remote host is 'Server2016'.
```

117886 - Local Checks Not Enabled (info)

Synopsis

Local checks were not enabled.

Description

Nessus did not enable local checks on the remote host. This does not necessarily indicate a problem with the scan. Credentials may not have been provided, local checks may not be available for the target, the target may not have been identified, or another issue may have occurred that prevented local checks from being enabled. See plugin output for details.

This plugin reports informational findings related to local checks not being enabled. For failure information, see plugin 21745 :

'Authentication Failure - Local Checks Not Run'.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/10/02, Modified: 2018/11/02

Plugin Output

tcp/0

```
The following issues were reported :

  - Plugin      : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : No Credentials Provided
    Message     :
Credentials were not provided for detected SMB service.
```

108761 - MSSQL Host Information in NTLM SSP

Synopsis

Nessus can obtain information about the host by examining the NTLM SSP message.

Description

Nessus can obtain information about the host by examining the NTLM SSP challenge issued during NTLM authentication, over MSSQL.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/03/30, Modified: 2019/10/30

Plugin Output

tcp/49159

```
Nessus was able to obtain the following information about the host, by
parsing the MSSQL server's NTLM SSP message:

Target Name:           SERVER2016
NetBIOS Domain Name:   SERVER2016
NetBIOS Computer Name: SERVER2016
DNS Domain Name:       Server2016
DNS Computer Name:     Server2016
DNS Tree Name:         unknown
Product Version:       6.3.9600
```

69482 - Microsoft SQL Server STARTTLS Support

Synopsis

The remote service supports encrypting traffic.

Description

The remote Microsoft SQL Server service supports the use of encryption initiated during pre-login to switch from a cleartext to an encrypted communications channel.

See Also

https://msdn.microsoft.com/en-us/library/dd304523.aspx

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/07/04, Modified: 2019/07/23

Plugin Output

tcp/49159

```
Here is the Microsoft SQL Server's SSL certificate that Nessus
was able to collect after sending a pre-login packet :

------------------------------ snip ------------------------------
Subject Name:

Common Name: SSL_Self_Signed_Fallback

Issuer Name:

Common Name: SSL_Self_Signed_Fallback

Serial Number: 3A 45 13 D5 18 63 6C 9F 4C 12 41 2F 64 51 0C 39

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Oct 23 06:59:28 2019 GMT
Not Valid After: Oct 23 06:59:28 2049 GMT

Public Key Info:
```

```
Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BE EA 89 03 24 24 F8 76 5B 81 04 8D 56 A4 9C 29 B3 4B BE
            BE 3E F9 26 CF 86 71 17 30 97 9C A5 64 30 F6 5A 17 F4 E3 9A
            F9 63 64 51 92 98 DE 1B 8F 27 68 EE B9 0A 13 5F 86 9F B1 26
            3A EB F4 61 EE 79 27 8F A2 59 3A 61 CA 98 25 F2 E6 EF 2A F2
            5E DF 06 E2 2E BA BE 4B F4 F0 D8 5A 93 80 72 FD B7 69 5B 64
            6A E6 7A 04 06 73 A4 3B 92 7C 1B B5 9A B2 FF 19 6C 35 19 EF
            0E 16 8A A4 6B 3A 48 6E D5 16 08 D3 B7 33 83 42 02 27 85 3E
            41 93 BE 19 7D C5 AD CE 1B E7 93 DC A4 FD C4 44 BF 3D FC 6A
            44 8B 64 D3 3F 2D 22 74 47 44 BA AE FC 58 D8 82 0A 9C 36 F6
            00 33 13 FF 8A 0A B9 B3 56 4A 5F E3 5C BB 95 F6 76 9D D3 26
            73 2E 52 CD 41 80 1A 06 99 16 D8 4A 6D 69 80 0D B5 C8 96 A7
            44 F4 6F 45 80 7A 00 C6 26 67 9F 6F E4 4F BE 6F 68 8E 42 5A
            FB 25 57 91 61 3E 0C 6B 1A BE 10 36 D9 30 08 80 1D
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 8D 69 C0 5F 16 C4 48 BB AA 4F 28 0F 8B 4E B3 BE 85 7A 58
           3B 1C CC EA 65 9D C7 39 16 20 30 CD BB 9F F5 1C 4F A8 72 E2
           FD 79 CF 62 DE AA B3 35 5F A8 AA 21 C2 75 F0 67 A5 AD FD 56
           59 1B E8 BE 4A 98 56 38 22 47 A1 9C 07 A8 3B 96 80 72 7D A5
           99 F2 2D 3A 8D 6A BC 90 CA AB 6C 2B 77 55 05 1D 68 60 79 95
           3B 8F 90 02 E2 16 8F EF C7 00 41 96 36 7A AF 7C 6B 7A 03 19
           D9 23 9C FF 2E 65 06 11 32 CF [...]
```

10144 - Microsoft SQL Server TCP/IP Listener Detection

Synopsis

A database server is listening on the remote port.

Description

The remote host is running MSSQL, a database server from Microsoft. It is possible to extract the version number of the remote installation from the server pre-login response.

Solution

Restrict access to the database to allowed IPs only.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/09/12

Plugin Output

tcp/49159

```
The remote MSSQL server accepts cleartext logins.
The remote SQL Server version is 14.0.1000.0.

The remote SQL Server instance name is SQLEXPRESS.
```

10674 - Microsoft SQL Server UDP Query Remote Version Disclosure

Synopsis

It is possible to determine the remote SQL server version.

Description

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

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

Solution

If there is only a single SQL instance installed on the remote host, consider filter incoming traffic to this port.

Risk Factor

None

Plugin Information

Published: 2001/05/25, Modified: 2018/03/13

Plugin Output

udp/1434

```
A 'ping' request returned the following information about the remote
SQL instance :

  ServerName   : SERVER2016
  InstanceName : SQLEXPRESS
  IsClustered  : No
  Version      : 14.0.1000.169
  tcp          : 49159
  np           : \\SERVER2016\pipe\MSSQL$SQLEXPRESS\sql\query
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

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

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2017/11/30

Plugin Output

tcp/445

```
The remote Operating System is : Windows Server 2012 R2 Datacenter 9600
The remote native LAN manager is : Windows Server 2012 R2 Datacenter 6.3
The remote SMB Domain Name is : SERVER2016
```

11011 - 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

Published: 2002/06/05, Modified: 2015/06/02

Plugin Output

tcp/139

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

11011 - 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

Published: 2002/06/05, Modified: 2015/06/02

Plugin Output

tcp/445

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

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2017/06/19

Plugin Output

tcp/445

```
The remote host supports the following versions of SMB :
  SMBv1
  SMBv2
```

106716 - Microsoft Windows SMB2 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2018/09/12

Plugin Output

tcp/445

```
The remote host supports the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
3.0        Windows 8
3.0.2      Windows 8.1

The remote host does NOT support the following SMB dialects :
_version_  _introduced in windows version_
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.1        Windows 10
3.1.1      Windows 10
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/0

```
Nessus SNMP scanner was able to retrieve the open port list
with the community name: p*****
It found 26 open TCP ports and 9 open UDP ports.
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/21

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

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/80

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

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/135

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

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/137

```
Port 137/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/138

```
Port 138/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/139

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

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/161

```
Port 161/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/445

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

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/500

```
Port 500/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/997

```
Port 997/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/1434

```
Port 1434/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/1801

```
Port 1801/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/2103

```
Port 2103/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/2105

```
Port 2105/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/2107

```
Port 2107/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/3389

```
Port 3389/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/3389

```
Port 3389/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/4500

```
Port 4500/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/5355

```
Port 5355/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/5985

```
Port 5985/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/16450

```
Port 16450/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/16451

```
Port 16451/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/16452

```
Port 16452/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/16453

```
Port 16453/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/17001

```
Port 17001/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/47001

```
Port 47001/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/49152

```
Port 49152/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/49153

```
Port 49153/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/49154

```
Port 49154/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/49155

```
Port 49155/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/49156

```
Port 49156/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/49157

```
Port 49157/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/49159

```
Port 49159/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/49217

```
Port 49217/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/49218

```
Port 49218/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin 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

Published: 2005/08/26, Modified: 2019/03/06

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.7.1
Plugin feed version : 201911090320
Scanner edition used : Nessus Home
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.1.205
Port scanner(s) : snmp_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
```

```
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2019/11/9 21:47 CST
Scan duration : 227 sec
```

110723 - No Credentials Provided

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was unable to execute credentialed checks because no credentials were provided.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/06/27, Modified: 2018/10/02

Plugin Output

tcp/0

```
SMB was detected on port 445 but no credentials were provided.
SMB local checks were not enabled.
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2019/09/04

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows Server 2012 R2 Datacenter
Confidence level : 99
Method : MSRPC

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

SNMP:!:Hardware: Intel64 Family 6 Model 63 Stepping 2 AT/AT COMPATIBLE - Software: Windows Version
 6.3 (Build 9600 Multiprocessor Free)
HTTP:Server: Microsoft-HTTPAPI/2.0

SSLcert:!:i/CN:Server2016s/CN:Server2016
aecd2a995dc10495cd5340d735d8ccdac9765fac
i/CN:SSL_Self_Signed_Fallbacks/CN:SSL_Self_Signed_Fallback
7096254afbbd903c434cec731fa70b0c8f2d15ad



The remote host is running Microsoft Windows Server 2012 R2 Datacenter
```

66173 - 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

Published: 2013/04/22, Modified: 2019/08/20

Plugin Output

tcp/3389

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

35296 - SNMP Protocol Version Detection

Synopsis

This plugin reports the protocol version negotiated with the remote SNMP agent.

Description

By sending an SNMP 'get-next-request', it is possible to determine the protocol version of the remote SNMP agent.

See Also

https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2009/01/06, Modified: 2019/06/05

Plugin Output

udp/161

```
Nessus has negotiated SNMP communications at SNMPv2c.
```

34022 - SNMP Query Routing Information Disclosure

Synopsis

The list of IP routes on the remote host can be obtained via SNMP.

Description

It is possible to obtain the routing information on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.4.21

An attacker may use this information to gain more knowledge about the network topology.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2008/08/21, Modified: 2011/05/24

Plugin Output

udp/161

```
127.0.0.0/255.0.0.0
127.0.0.1/255.255.255.255
127.255.255.255/255.255.255.255
192.168.1.0/255.255.255.0
192.168.1.101/255.255.255.255
192.168.1.255/255.255.255.255
224.0.0.0/240.0.0.0
255.255.255.255/255.255.255.255
```

10550 - SNMP Query Running Process List Disclosure

Synopsis

The list of processes running on the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of running processes on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.25.4.2.1.2

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2000/11/13, Modified: 2011/05/24

Plugin Output

udp/161

```
  PID   CPU   MEM COMMAND           ARGS
    1 2954558     4 System Idle Process
    4  3555   148 System
  112     0  5760 csrss.exe
  260     0   548 smss.exe
  272     0  4816 winlogon.exe
  324    14  1440 csrss.exe
  392     0   156 csrss.exe
  400     9  1276 wininit.exe
  428     0    40 winlogon.exe
  492     2  3464 services.exe
  500   326  9692 lsass.exe
  560    32  4816 svchost.exe     -k DcomLaunch
  572     0  3432 spoolsv.exe
  592    14  3316 svchost.exe     -k RPCSS
  680     0   172 dwm.exe
  696     0    36 vmacthlp.exe
  728     0   284 fdhost.exe       "MSSQL14.SQLEXPRESSHe3c2277ffd37ef482efa381f1f9cc415a0b62jcc"
"MSSQL14.SQLEXPRESS" "MSSQL14.SQLEXPRESS" "4" "" "4096" "M" "0" "
  732     0   780 svchost.exe     -k apphost
  752   737  8404 svchost.exe     -k LocalServiceNetworkRestricted
  780   747 20624 svchost.exe     -k netsvcs
  804     1  6552 svchost.exe     -k LocalService
  880   334  8644 svchost.exe     -k ftpsvc
  892    35  6444 svchost.exe     -k NetworkService
 1004     1  3756 svchost.exe     -k LocalServiceNoNetwork
```

```
 1016     0   836 inetinfo.exe
 1056     2  2592 mqsvc.exe
 1088     0   376 dllhost.exe     /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
 1280  8256 305744 sqlservr.exe     -sSQLEXPRESS
 1316     0  1136 SMSvcHost.exe
 1328     0    40 fdlauncher.exe   -s MSSQL14.SQLEXPRESS
 1412     0  1532 svchost.exe     -k PeerDist
 1452    64  7652 snmp.exe
 1488     0   760 sqlbrowser.exe
 1508     0  1588 svchost.exe     -k NetworkServiceNetworkRestricted
 1568     0  4828 winlogon.exe
 1612    31 26160 sqlceip.exe      -Service SQLEXPRESS
 1672     0   872 SMSvcHost.exe    -NetMsmqActivator
 1684     0    20 sqlwriter.exe
 1700     1  7960 svchost.exe     -k LocalSystemNetworkRestricted
 1740     0    28 VGAuthService.exe
 1852   670  6176 vmtoolsd.exe
 1896     0  2476 svchost.exe     -k iissvcs
 1976 14288  2448 Launchpad.exe
 1996    47  3708 M [...]
```

10800 - SNMP Query System Information Disclosure

Synopsis

The System Information of the remote host can be obtained via SNMP.

Description

It is possible to obtain the system information about the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.1.1.

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2001/11/06, Modified: 2011/05/24

Plugin Output

udp/161

```
System information :
 sysDescr     : Hardware: Intel64 Family 6 Model 63 Stepping 2 AT/AT COMPATIBLE - Software: Windows
 Version 6.3 (Build 9600 Multiprocessor Free)
 sysObjectID  : 1.3.6.1.4.1.311.1.1.3.1.2
 sysUptime    : 1d 18h 53m 15s
 sysContact   : HASH(0xDEADBEF)
 sysName      : Hacked
 sysLocation  :
 sysServices  : 79
```

10551 - SNMP Request Network Interfaces Enumeration

Synopsis

The list of network interfaces cards of the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of the network interfaces installed on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.2.1.0

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2000/11/13, Modified: 2011/05/24

Plugin Output

udp/161

```
Interface 1 information :
ifIndex       : 1
ifDescr       : Software Loopback Interface 1
```

40448 - SNMP Supported Protocols Detection

Synopsis

This plugin reports all the protocol versions successfully negotiated with the remote SNMP agent.

Description

Extend the SNMP settings data already gathered by testing for\ SNMP versions other than the highest negotiated.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/07/31, Modified: 2013/01/19

Plugin Output

udp/161

```
This host supports SNMP version SNMPv1.
This host supports SNMP version SNMPv2c.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2019/03/01

Plugin Output

tcp/3389

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2019/03/01

Plugin Output

tcp/49159

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2019/06/25

Plugin Output

tcp/49159

```
The host name known by Nessus is :

  server2016

The Common Name in the certificate is :

  ssl_self_signed_fallback
```

10863 - 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

Published: 2008/05/19, Modified: 2019/07/18

Plugin Output

tcp/3389

```
Subject Name:

Common Name: Server2016

Issuer Name:

Common Name: Server2016

Serial Number: 5D 7E 64 2F 8D 23 B4 9A 46 F0 AF 69 47 87 F2 B7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 10 16:52:54 2019 GMT
Not Valid After: Apr 10 16:52:54 2020 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E1 7D F4 37 92 EC 6D 25 85 44 27 3E 5A EE 4E 13 23 94 C6
            86 CE 43 B8 07 93 39 94 92 1F 5B 38 BF 1F 93 24 18 DA A5 4F
            88 7B 92 6C 11 70 FB C7 7B 39 D1 6F A3 E7 25 EF 5C D6 AB 8B
            85 EB A8 81 65 02 A7 2A 12 E4 79 7C 49 4D 66 B5 1D BA 34 7A
            52 1A E3 F7 EB A8 44 7C 9F 0A 8D 5B B8 B1 E8 08 B1 53 03 63
            AF 82 3C CC 4A A1 2E 6F CC CC B1 D9 C2 6E 92 06 45 EE EA A2
            4A 9E 06 76 11 A2 C1 DD 2E EB 97 A7 C9 37 B8 85 4B 7D 5F 3E
            71 E5 AB F3 FF 81 9C E4 21 1E E8 03 9E EA 89 67 99 B4 CF C8
            8F 08 61 72 EF AE 60 56 67 AA 8E 2B F5 17 7C 74 65 0B A8 08
            5B 02 69 E1 FE BA A4 A8 1D 38 15 C0 E6 F7 F6 9C 86 00 88 B7
            5D B3 7B DF 81 3E 6D 52 1D 36 0D C3 85 5F E1 CB C6 58 79 A3
```

```
            19 5B 95 B7 87 40 94 9C 7A A0 B8 32 24 FF AC 29 A6 A2 31 E9
            02 91 1A 45 84 D3 C1 90 C5 E9 B5 E0 49 6F AF F0 8F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 39 C7 0B E4 A1 F2 70 63 0B 04 89 88 5B B9 C2 AE D4 D0 9B
           3B A9 BA EA F3 04 20 72 CA EF 62 43 1C 62 90 16 7F 05 68 1A
           F3 53 D6 47 47 E5 22 72 57 E6 FA FB 38 28 6D 86 66 1E F8 20
           00 61 47 9A E9 0D 0E 8C E6 62 22 10 E3 61 4A A3 84 DE 17 2E
           8E 8C 43 95 D9 46 ED 0B 69 6E 62 DA 3F 03 77 5C AE 0C FA EA
           1B C0 BB 93 DF 7D 9A 6D 97 C4 E6 EC 0E 3A D5 AB 98 5B 90 18
           70 BC 55 31 65 84 62 4B 47 47 90 B6 BD E8 DB 2A 85 74 C9 EC
           97 C7 C4 98 3E 1A 31 4C 9F BF 97 E5 B5 42 94 10 AA 02 C8 71
           06 80 2F D9 2A 38 59 E9 73 DE D1 D7 FC 99 FE 5A BF 64 46 85
           AE 94 38 8B 8A D6 6D E4 15 A8  [...]
```

10863 - 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

Published: 2008/05/19, Modified: 2019/07/18

Plugin Output

tcp/49159

```
Subject Name:

Common Name: SSL_Self_Signed_Fallback

Issuer Name:

Common Name: SSL_Self_Signed_Fallback

Serial Number: 3A 45 13 D5 18 63 6C 9F 4C 12 41 2F 64 51 0C 39

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Oct 23 06:59:28 2019 GMT
Not Valid After: Oct 23 06:59:28 2049 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BE EA 89 03 24 24 F8 76 5B 81 04 8D 56 A4 9C 29 B3 4B BE
            BE 3E F9 26 CF 86 71 17 30 97 9C A5 64 30 F6 5A 17 F4 E3 9A
            F9 63 64 51 92 98 DE 1B 8F 27 68 EE B9 0A 13 5F 86 9F B1 26
            3A EB F4 61 EE 79 27 8F A2 59 3A 61 CA 98 25 F2 E6 EF 2A F2
            5E DF 06 E2 2E BA BE 4B F4 F0 D8 5A 93 80 72 FD B7 69 5B 64
            6A E6 7A 04 06 73 A4 3B 92 7C 1B B5 9A B2 FF 19 6C 35 19 EF
            0E 16 8A A4 6B 3A 48 6E D5 16 08 D3 B7 33 83 42 02 27 85 3E
            41 93 BE 19 7D C5 AD CE 1B E7 93 DC A4 FD C4 44 BF 3D FC 6A
            44 8B 64 D3 3F 2D 22 74 47 44 BA AE FC 58 D8 82 0A 9C 36 F6
            00 33 13 FF 8A 0A B9 B3 56 4A 5F E3 5C BB 95 F6 76 9D D3 26
            73 2E 52 CD 41 80 1A 06 99 16 D8 4A 6D 69 80 0D B5 C8 96 A7
```

```
             44 F4 6F 45 80 7A 00 C6 26 67 9F 6F E4 4F BE 6F 68 8E 42 5A
             FB 25 57 91 61 3E 0C 6B 1A BE 10 36 D9 30 08 80 1D
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 8D 69 C0 5F 16 C4 48 BB AA 4F 28 0F 8B 4E B3 BE 85 7A 58
           3B 1C CC EA 65 9D C7 39 16 20 30 CD BB 9F F5 1C 4F A8 72 E2
           FD 79 CF 62 DE AA B3 35 5F A8 AA 21 C2 75 F0 67 A5 AD FD 56
           59 1B E8 BE 4A 98 56 38 22 47 A1 9C 07 A8 3B 96 80 72 7D A5
           99 F2 2D 3A 8D 6A BC 90 CA AB 6C 2B 77 55 05 1D 68 60 79 95
           3B 8F 90 02 E2 16 8F EF C7 00 41 96 36 7A AF 7C 6B 7A 03 19
           D9 23 9C FF 2E 65 06 11 32 CF 09 D8 6F D6 36 12 44 70 D5 E1
           1B AF 19 C5 36 E3 81 F7 FA 6C 75 C1 EB A8 35 38 A1 84 15 E8
           DC B8 B9 DB 23 6D 05 E0 D0 6F AA 5C F3 CE DF A6 36 DC B5 C0
            [...]
```

70544 - 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

https://www.openssl.org/docs/manmaster/man1/ciphers.html

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

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2018/11/15

Plugin Output

tcp/3389

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

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

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

  High Strength Ciphers (>= 112-bit key)

    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
    AES128-SHA                  Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                  Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256     Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384     Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
    RSA-AES128-SHA256           Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    RSA-AES256-SHA256           Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA256
```

```
The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

70544 - 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

https://www.openssl.org/docs/manmaster/man1/ciphers.html

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

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2018/11/15

Plugin Output

tcp/49159

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

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

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

  High Strength Ciphers (>= 112-bit key)

    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
    AES128-SHA                  Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                  Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256     Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384     Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
    RSA-AES128-SHA256           Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    RSA-AES256-SHA256           Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA256
```

```
The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2019/05/10

Plugin Output

tcp/3389

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

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

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA256       Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    DHE-RSA-AES256-SHA384       Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    RSA-AES128-SHA256           Kx=RSA         Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    RSA-AES256-SHA384           Kx=RSA         Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    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
    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
    ECDHE-RSA-AES128-SHA256     Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384     Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
    RSA-AES128-SHA256           Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
```

```
    RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA256


SSL Version : TLSv11
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

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

  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA  [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2019/05/10

Plugin Output

tcp/49159

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

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

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA256       Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    DHE-RSA-AES256-SHA384       Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    RSA-AES128-SHA256           Kx=RSA         Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    RSA-AES256-SHA384           Kx=RSA         Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    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
    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
    ECDHE-RSA-AES128-SHA256     Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384     Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
    RSA-AES128-SHA256           Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
```

```
    RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA256


SSL Version : TLSv11
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

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

  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA  [...]
```

57041 - 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

https://www.openssl.org/docs/manmaster/man1/ciphers.html

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2018/11/15

Plugin Output

tcp/3389

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

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    DHE-RSA-AES256-SHA384        Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    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
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
```

```
    Mac={message authentication code}
    {export flag}
```

57041 - 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

https://www.openssl.org/docs/manmaster/man1/ciphers.html

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2018/11/15

Plugin Output

tcp/49159

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

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    DHE-RSA-AES256-SHA384        Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    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
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
```

```
    Mac={message authentication code}
    {export flag}
```

51891 - 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

Published: 2011/02/07, Modified: 2013/10/18

Plugin Output

tcp/3389

```
This port supports resuming TLSv1 sessions.
```

51891 - 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

Published: 2011/02/07, Modified: 2013/10/18

Plugin Output

tcp/49159

```
This port supports resuming TLSv1 sessions.
```

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?234f8ef8

http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

Plugin Information

Published: 2017/02/03, Modified: 2018/11/15

Plugin Output

tcp/445

```
The remote host supports SMBv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2019/10/29

Plugin Output

tcp/21

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2019/10/29

Plugin Output

tcp/80

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2019/10/29

Plugin Output

tcp/5985

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2019/10/29

Plugin Output

tcp/47001

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

25220 - 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

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

tcp/0

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information

Published: 2017/11/22, Modified: 2018/07/11

Plugin Output

tcp/3389

```
TLSv1 is enabled and the server supports at least one cipher.
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information

Published: 2017/11/22, Modified: 2018/07/11

Plugin Output

tcp/49159

```
TLSv1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

PCI DSS v3.2 still allows TLS 1.1 as of June 30, 2018, but strongly recommends the use of TLS 1.2. A proposal is currently before the IETF to fully deprecate TLS 1.1 and many vendors have already proactively done this.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2019/01/08

Plugin Output

tcp/3389

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

PCI DSS v3.2 still allows TLS 1.1 as of June 30, 2018, but strongly recommends the use of TLS 1.2. A proposal is currently before the IETF to fully deprecate TLS 1.1 and many vendors have already proactively done this.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2019/01/08

Plugin Output

tcp/49159

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

64814 - 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

Published: 2013/02/22, Modified: 2018/03/29

Plugin Output

tcp/3389

```
Subject Name:

Common Name: Server2016

Issuer Name:

Common Name: Server2016

Serial Number: 5D 7E 64 2F 8D 23 B4 9A 46 F0 AF 69 47 87 F2 B7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 10 16:52:54 2019 GMT
Not Valid After: Apr 10 16:52:54 2020 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E1 7D F4 37 92 EC 6D 25 85 44 27 3E 5A EE 4E 13 23 94 C6
            86 CE 43 B8 07 93 39 94 92 1F 5B 38 BF 1F 93 24 18 DA A5 4F
            88 7B 92 6C 11 70 FB C7 7B 39 D1 6F A3 E7 25 EF 5C D6 AB 8B
            85 EB A8 81 65 02 A7 2A 12 E4 79 7C 49 4D 66 B5 1D BA 34 7A
            52 1A E3 F7 EB A8 44 7C 9F 0A 8D 5B B8 B1 E8 08 B1 53 03 63
            AF 82 3C CC 4A A1 2E 6F CC CC B1 D9 C2 6E 92 06 45 EE EA A2
            4A 9E 06 76 11 A2 C1 DD 2E EB 97 A7 C9 37 B8 85 4B 7D 5F 3E
            71 E5 AB F3 FF 81 9C E4 21 1E E8 03 9E EA 89 67 99 B4 CF C8
            8F 08 61 72 EF AE 60 56 67 AA 8E 2B F5 17 7C 74 65 0B A8 08
            5B 02 69 E1 FE BA A4 A8 1D 38 15 C0 E6 F7 F6 9C 86 00 88 B7
            5D B3 7B DF 81 3E 6D 52 1D 36 0D C3 85 5F E1 CB C6 58 79 A3
```

```
             19 5B 95 B7 87 40 94 9C 7A A0 B8 32 24 FF AC 29 A6 A2 31 E9
             02 91 1A 45 84 D3 C1 90 C5 E9 B5 E0 49 6F AF F0 8F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 39 C7 0B E4 A1 F2 70 63 0B 04 89 88 5B B9 C2 AE D4 D0 9B
           3B A9 BA EA F3 04 20 72 CA EF 62 43 1C 62 90 16 7F 05 68 1A
           F3 53 D6 47 47 E5 22 72 57 E6 FA FB 38 28 6D 86 66 1E F8 20
           00 61 47 9A E9 0D 0E 8C E6 62 22 10 E3 61 4A A3 84 DE 17 2E
           8E 8C 43 95 D9 46 ED 0B 69 6E 62 DA 3F 03 77 5C AE 0C FA EA
           1B C0 BB 93 DF 7D 9A 6D 97 C4 E6 EC 0E 3A D5 AB 98 5B 90 18
           70 BC 55 31 65 84 62 4B 47 47 90 B6 BD E8 DB 2A 85 74 C9 EC
           97 C7 C4 98 3E 1A 31 4C 9F BF 97 E5 B5 42 94 10 AA 02 C8 71
           06 80 2F D9 2A 38 59 E9 73 DE D1 D7 FC 99 FE 5A BF 64 46 85
           AE 94 38 8B 8A D6 6D E4 15 A8  [...]
```

10287 - 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

Published: 1999/11/27, Modified: 2019/03/06

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.205 to 192.168.1.101 :
192.168.1.205
192.168.1.101

Hop Count: 1
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/09/25

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

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

Description

The remote host is listening 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

Published: 1999/10/12, Modified: 2019/05/31

Plugin Output

udp/137

```
The following 3 NetBIOS names have been gathered :

 SERVER2016       = File Server Service
 SERVER2016       = Computer name
 WORKGROUP        = Workgroup / Domain name

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

   00:50:56:9a:9b:ea
```

10940 - Windows Terminal Services Enabled

Synopsis

The remote Windows host has Terminal Services enabled.

Description

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

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

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

Solution

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

Risk Factor

None

Plugin Information

Published: 2002/04/20, Modified: 2017/08/07

Plugin Output

tcp/3389