RK3 Loc

Vulnerabilities by Host

Vulnerabilities by Host

30.90.90.99

0	3	8	1	94
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Jul 2 02:10:04 2021
End time: Fri Jul 2 03:21:52 2021

Host Information

DNS Name: rk3adcsrv.rubberkingtyres.net
Netbios Name: RK3ADCSRV
IP: 30.90.90.99
OS: Microsoft Windows Server 2012 R2 Standard

Vulnerabilities

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 SSL 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 v2.0 Base Score

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

CVSS v2.0 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: 2020/04/27

Plugin Output

tcp/21112

```
  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=ofcsslagent
```

```
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Apr 08 02:48:37 2021 GMT
|-Valid To            : Dec 31 23:59:59 2039 GMT
```

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 v2.0 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: 2021/02/03

Plugin Output

tcp/21112

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

    Name                        Code        KEX     Auth    Encryption            MAC
    ----------------------      ----------  ---     ----    --------------------  ---
    DES-CBC3-SHA                0x00, 0x0A  RSA     RSA     3DES-CBC(168)
  SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

Risk Factor

High

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 v2.0 Base Score

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

Plugin Information

Published: 2005/10/12, Modified: 2020/05/06

Plugin Output

tcp/21112

```
 - SSLv3 is enabled and the server supports at least one cipher.
 Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3

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

     Name                       Code          KEX       Auth    Encryption            MAC
     ---------------------      ----------    ---       ----    --------------------  ---
     DES-CBC3-SHA                             RSA       RSA     3DES-CBC(168)
 SHA1

   High Strength Ciphers (>= 112-bit key)

     Name                       Code          KEX       Auth    Encryption            MAC
     ---------------------      ----------    ---       ----    --------------------  ---
     DHE-RSA-AES128-SHA                       DH        RSA     AES-CBC(128)
 SHA1
     DHE-RSA-AES256-SHA                       DH        RSA     AES-CBC(256)
 SHA1
     ECDHE-RSA-AES128-SHA                     ECDH      RSA     AES-CBC(128)
 SHA1
     ECDHE-RSA-AES256-SHA                     ECDH      RSA     AES-CBC(256)
 SHA1
     AES128-SHA                               RSA       RSA     AES-CBC(128)
 SHA1
     AES256-SHA                               RSA       RSA     AES-CBC(256)
 SHA1
     RC4-MD5                                  RSA       RSA     RC4(128)              MD5
     RC4-SHA                                  RSA       RSA     RC4(128)
 SHA1
     ECDHE-RSA-AES128-SHA256                  ECDH      RSA     AES-CBC(128)
 SHA256
     ECDHE-RSA-AES256-SHA384                  ECDH      RSA     AES-CBC(256)
 SHA384
     RSA-AES128-SHA256                        RSA       RSA     AES-CBC(128)
 SHA256
     RSA-AES256-SHA256                        RSA       RSA     AES-CBC(256)
 SHA256

 The fields above are :

   {Tenable ciphername}
   {Cipher ID code} [...]
```

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.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 v2.0 Base Score

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

CVSS v2.0 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: 2021/03/30

Plugin Output

tcp/3389/msrdp

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 SSL 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 v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/21112

```
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=ofcsslagent
|-Issuer  : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=Fortinet Untrusted
 CA/E=support@fortinet.com
```

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 SSL 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 v2.0 Base Score

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

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/21112

```
The identities known by Nessus are :

  169.254.130.101
  30.90.90.99
  rk3adcsrv.rubberkingtyres.net

The Common Name in the certificate is :

  ofcsslagent
```

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

https://www.rc4nomore.com/

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

Medium

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 v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (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: 2021/02/03

Plugin Output

tcp/21112

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

  High Strength Ciphers (>= 112-bit key)

    Name                       Code          KEX       Auth    Encryption              MAC
    ---------------------      ----------    ---       ----    --------------------    ---
    RC4-MD5                    0x00, 0x04    RSA       RSA     RC4(128)                MD5
    RC4-SHA                    0x00, 0x05    RSA       RSA     RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID   70574
CVE   CVE-2014-3566
XREF   CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2020/06/12

Plugin Output

tcp/21112

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

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 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

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.

See Also

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

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/21112

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

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 v2.0 Base Score

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

Plugin Information

Published: 2012/03/23, Modified: 2021/04/20

Plugin Output

tcp/3389/msrdp

```
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 v2.0 Base Score

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

Plugin Information

Published: 2012/01/25, Modified: 2021/04/20

Plugin Output

tcp/3389/msrdp

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

2. Medium
```

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 v2.0 Base Score

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

Plugin Information

Published: 2008/02/11, Modified: 2021/04/20

Plugin Output

tcp/3389/msrdp

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

2. Medium (Client Compatible)
```

10761 - COM+ Internet Services (CIS) Server Detection

Synopsis

A COM+ Internet Services (CIS) server is listening on this port.

Description

COM+ Internet Services are RPC over HTTP tunneling and require IIS to operate. CIS ports shouldn't be visible on internet but only behind a firewall.

See Also

http://www.nessus.org/u?d02f7e6e

https://support.microsoft.com/en-us/support/kb/articles/q282/2/61.asp

Solution

If you do not use this service, disable it with DCOMCNFG.

Otherwise, limit access to this port.

Risk Factor

None

Plugin Information

Published: 2001/09/14, Modified: 2019/11/22

Plugin Output

tcp/49158/ncacn_http

```
Server banner :

ncacn_http/1.0
```

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, Modified: 2021/06/03

Plugin Output

tcp/0

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

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

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: 2020/08/20

Plugin Output

tcp/135/epmap

```
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 : WMsgKRpc0736D0

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 : WMsgKRpc0736D0

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-8dd241be6fa5ece207

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-5cb30099057515259c

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 : WMsgKRpc013A64D3

Object UUID : 95b1a011-40c6-4422-996f-110868a22740
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-7bd67d2f01701cc7e1

Object UUID : b5b130e7-d1bb-4d66-bf00-e974fb93b331
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Wind [...]
```

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: 2020/08/20

Plugin Output

tcp/445/cifs

```
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 : \\RK3ADCSRV

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 : \\RK3ADCSRV

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 : \\RK3ADCSRV

Object UUID : 7364746e-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
```

```
Named pipe : \pipe\lsass
Netbios name : \\RK3ADCSRV

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 : \\RK3ADCSRV

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0
Description : Active Directory Replication Interface
Windows process : unknown
Annotation : MS NT Directory DRS Interface
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\RK3ADCSRV

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0
Description : Active Directory Replication Interface
Windows process : unknown
Annotation : MS NT Directory DRS Interface
Type : Remote RPC service
Named pipe : \pipe\d0b114e9350042ce
Netbios name : \\RK3ADCSRV

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0
Description : Local Security Authority
Windows process : lsas [...]
```

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: 2020/08/20

Plugin Output

tcp/6160/dce-rpc

```
The following DCERPC services are available on TCP port 6160 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d107c6e0-fc35-49ba-ba03-3e192de6797d, version 1.0
Description : Unknown RPC service
Annotation : Veeam Deployer
Type : Remote RPC service
TCP Port : 6160
IP : 30.90.90.99

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1.0
Description : Unknown RPC service
Annotation : Veeam RPC Invoker
Type : Remote RPC service
TCP Port : 6160
IP : 30.90.90.99
```

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: 2020/08/20

Plugin Output

tcp/6161/dce-rpc

```
The following DCERPC services are available on TCP port 6161 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1.0
Description : Unknown RPC service
Annotation : Veeam Invoker
Type : Remote RPC service
TCP Port : 6161
IP : 30.90.90.99
```

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: 2020/08/20

Plugin Output

tcp/6162/dce-rpc

```
The following DCERPC services are available on TCP port 6162 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1.0
Description : Unknown RPC service
Annotation : Veeam Invoker
Type : Remote RPC service
TCP Port : 6162
IP : 30.90.90.99
```

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: 2020/08/20

Plugin Output

tcp/6190/dce-rpc

```
The following DCERPC services are available on TCP port 6190 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1.0
Description : Unknown RPC service
Annotation : Veeam Invoker
Type : Remote RPC service
TCP Port : 6190
IP : 30.90.90.99
```

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: 2020/08/20

Plugin Output

tcp/6210/dce-rpc

```
The following DCERPC services are available on TCP port 6210 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 844d6366-6a97-4eb5-8345-b88e8276c20d, version 1.0
Description : Unknown RPC service
Annotation : Veeam HV Integration
Type : Remote RPC service
TCP Port : 6210
IP : 30.90.90.99

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1.0
Description : Unknown RPC service
Annotation : Veeam Invoker
Type : Remote RPC service
TCP Port : 6210
IP : 30.90.90.99
```

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: 2020/08/20

Plugin Output

tcp/11731/dce-rpc

```
The following DCERPC services are available on TCP port 11731 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d107c6e0-fc35-49ba-ba03-3e192de6797d, version 1.0
Description : Unknown RPC service
Annotation : Veeam Deployer
Type : Remote RPC service
TCP Port : 11731
IP : 30.90.90.99

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1.0
Description : Unknown RPC service
Annotation : Veeam RPC Invoker
Type : Remote RPC service
TCP Port : 11731
IP : 30.90.90.99
```

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: 2020/08/20

Plugin Output

tcp/49152/dce-rpc

```
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 : 30.90.90.99
```

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: 2020/08/20

Plugin Output

tcp/49153/dce-rpc

```
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 : 30.90.90.99

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 : 30.90.90.99

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 : 30.90.90.99

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 : 30.90.90.99

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 : 30.90.90.99
```

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: 2020/08/20

Plugin Output

tcp/49154/dce-rpc

```
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 : 30.90.90.99

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 : 30.90.90.99

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 : 30.90.90.99

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 : 30.90.90.99

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 : 30.90.90.99

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 : 30.90.90.99

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 : 30.90.90.99

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 : 30.90.90.99

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description  [...]
```

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: 2020/08/20

Plugin Output

tcp/49155/dce-rpc

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

Object UUID : 7364746e-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49155
IP : 30.90.90.99

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49155
IP : 30.90.90.99

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0
Description : Active Directory Replication Interface
Windows process : unknown
Annotation : MS NT Directory DRS Interface
Type : Remote RPC service
TCP Port : 49155
IP : 30.90.90.99

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

```
UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0
Description : Local Security Authority
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49155
IP : 30.90.90.99


Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49155
IP : 30.90.90.99


Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49155
IP : 30.90.90.99


Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0
Description : Network Logon Service
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49155
IP : 30.90.90.99


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
TCP Port : 49155
IP : 30.90.90.99
```

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: 2020/08/20

Plugin Output

tcp/49157/dce-rpc

```
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 : 30.90.90.99

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0
Description : Active Directory Replication Interface
Windows process : unknown
Annotation : MS NT Directory DRS Interface
Type : Remote RPC service
TCP Port : 49157
IP : 30.90.90.99

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0
Description : Local Security Authority
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49157
IP : 30.90.90.99

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
```

```
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49157
IP : 30.90.90.99

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49157
IP : 30.90.90.99

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0
Description : Network Logon Service
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49157
IP : 30.90.90.99

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
TCP Port : 49157
IP : 30.90.90.99
```

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: 2020/08/20

Plugin Output

tcp/49175/dce-rpc

```
The following DCERPC services are available on TCP port 49175 :

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 : 49175
IP : 30.90.90.99

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 : 49175
IP : 30.90.90.99

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 : 49175
IP : 30.90.90.99

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 : 49175
IP : 30.90.90.99

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 : 49175
IP : 30.90.90.99
```

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: 2020/08/20

Plugin Output

tcp/52877/dce-rpc

```
The following DCERPC services are available on TCP port 52877 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5.0
Description : DNS Server
Windows process : dns.exe
Type : Remote RPC service
TCP Port : 52877
IP : 30.90.90.99
```

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: 2020/08/20

Plugin Output

tcp/58434/dce-rpc

```
The following DCERPC services are available on TCP port 58434 :

Object UUID : 5bc1ed07-f5f5-485f-9dfd-6fd0acf9a23c
UUID : 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1.0
Description : Unknown RPC service
Annotation : Frs2 Service
Type : Remote RPC service
TCP Port : 58434
IP : 30.90.90.99
```

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: 2020/08/20

Plugin Output

tcp/61977/dce-rpc

```
The following DCERPC services are available on TCP port 61977 :

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 : 61977
IP : 30.90.90.99
```

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: 2020/08/20

Plugin Output

tcp/61980/dce-rpc

```
The following DCERPC services are available on TCP port 61980 :

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 : 61980
IP : 30.90.90.99
```

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

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

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

udp/53/dns

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
```

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

References

XREF   IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/5985/www

```
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

References

XREF   IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/47001/www

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

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

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
30.90.90.99 resolves as rk3adcsrv.rubberkingtyres.net.
```

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: 2019/11/22

Plugin Output

tcp/5985/www

```
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: Fri, 02 Jul 2021 13:43:43 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: 2019/11/22

Plugin Output

tcp/47001/www

```
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: Fri, 02 Jul 2021 13:43:43 GMT
  Connection: close
  Content-Length: 315

Response Body :
```

43829 - Kerberos Information Disclosure

Synopsis

The remote Kerberos server is leaking information.

Description

Nessus was able to retrieve the realm name and/or server time of the remote Kerberos server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/01/08, Modified: 2015/09/24

Plugin Output

tcp/88

```
 Nessus gathered the following information :

   Server time  : 2021-07-02 13:38:55 UTC
   Realm        : RUBBERKINGTYRES.NET
```

25701 - LDAP Crafted Search Request Server Information Disclosure

Synopsis

It is possible to discover information about the remote LDAP server.

Description

By sending a search request with a filter set to 'objectClass=*', it is possible to extract information about the remote LDAP server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/07/12, Modified: 2012/02/20

Plugin Output

tcp/389/ldap

```
[+]-namingContexts:
    |   DC=rubberkingtyres,DC=net
    |   CN=Configuration,DC=rubberkingtyres,DC=net
    |   CN=Schema,CN=Configuration,DC=rubberkingtyres,DC=net
    |   DC=ForestDnsZones,DC=rubberkingtyres,DC=net
    |   DC=DomainDnsZones,DC=rubberkingtyres,DC=net
[+]-currentTime:
    |   20210702134508.0Z
[+]-subschemaSubentry:
    |   CN=Aggregate,CN=Schema,CN=Configuration,DC=rubberkingtyres,DC=net
[+]-dsServiceName:
    |   CN=NTDS Settings,CN=RK3ADCSRV,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=rubberkingtyres,DC=net
[+]-namingContexts:
    |   DC=rubberkingtyres,DC=net
    |   CN=Configuration,DC=rubberkingtyres,DC=net
    |   CN=Schema,CN=Configuration,DC=rubberkingtyres,DC=net
    |   DC=ForestDnsZones,DC=rubberkingtyres,DC=net
    |   DC=DomainDnsZones,DC=rubberkingtyres,DC=net
[+]-defaultNamingContext:
    |   DC=rubberkingtyres,DC=net
[+]-schemaNamingContext:
    |   CN=Schema,CN=Configuration,DC=rubberkingtyres,DC=net
[+]-configurationNamingContext:
    |   CN=Configuration,DC=rubberkingtyres,DC=net
[+]-rootDomainNamingContext:
    |   DC=rubberkingtyres,DC=net
[+]-supportedControl:
    |   1.2.840.113556.1.4.319
    |   1.2.840.113556.1.4.801
```

```
|  1.2.840.113556.1.4.473
|  1.2.840.113556.1.4.528
|  1.2.840.113556.1.4.417
|  1.2.840.113556.1.4.619
|  1.2.840.113556.1.4.841
|  1.2.840.113556.1.4.529
|  1.2.840.113556.1.4.805
|  1.2.840.113556.1.4.521
|  1.2.840.113556.1.4.970
|  1.2.840.113556.1.4.1338
|  1.2.840.113556.1.4.474
|  1.2.840.113556.1.4.1339
|  1.2.840.113556.1.4.1340
|  1.2.840.113556.1.4.1413
|  2.16.840.1.113730.3.4.9
|  2.16.840.1.113730.3.4.10
|  1.2.840.113556.1.4.1504
|  1.2.840.113556.1.4.1852
|  1.2.840.113556.1.4.802
|  1.2.840.113556.1.4.1907
|  1.2.840.113556.1.4.1948
|  1.2.840.113556.1.4.1974
|  1.2.840.113556.1.4.1341
|  1.2.840.113556.1.4.2026
|  1.2.840.113556.1.4.2064
|  1.2.840.113556.1.4.2065
|  1.2.840.113556.1.4.2066
|  1.2.840.113556.1.4.2090
|  1.2.840.113556.1.4.2205
|  1.2.840.113556.1.4 [...]
```

20870 - LDAP Server Detection

Synopsis

An LDAP server was detected on the remote host.

Description

The remote host is running a Lightweight Directory Access Protocol (LDAP) server. LDAP is a protocol for providing access to directory services over TCP/IP.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/02/10, Modified: 2019/11/22

Plugin Output

tcp/389/ldap

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

References

XREF   IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2020/09/22

Plugin Output

tcp/0

```
  The following issues were reported :

    - Plugin      : no_local_checks_credentials.nasl
      Plugin ID   : 110723
      Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
      Message     :
  Credentials were not provided for detected SMB service.
```

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

Synopsis

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

Description

The remote host listens on tcp port 445 and replies to SMB requests.

By sending an NTLMSSP authentication request it is possible to obtain the name of the remote system and the name of its domain.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/11/06, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The following 2 NetBIOS names have been gathered :

 RK3ADCSRV       = Computer name
 RUBBERKINGTYRES = Workgroup / Domain name
```

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: 2020/01/22

Plugin Output

tcp/445/cifs

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

26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

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

If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access'

service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

References

XREF   IAVB:0001-B-0506

Plugin Information

Published: 2007/10/04, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
Could not connect to the registry because:
Could not connect to IPC$
```

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: 2021/02/11

Plugin Output

tcp/139/smb

```
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: 2021/02/11

Plugin Output

tcp/445/cifs

```
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: 2019/11/22

Plugin Output

tcp/445/cifs

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/21

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/25

```
Port 25/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/53

```
Port 53/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/80

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/88

```
Port 88/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/110

```
Port 110/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/111

```
Port 111/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/135/epmap

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/139/smb

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/143

```
Port 143/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/389/ldap

```
Port 389/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/443

```
Port 443/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/445/cifs

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/464

```
Port 464/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/636

```
Port 636/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/3389/msrdp

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/5985/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/6160/dce-rpc

```
Port 6160/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/6162/dce-rpc

```
Port 6162/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8015

```
Port 8015/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/9380

```
Port 9380/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/9381

```
Port 9381/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/11731/dce-rpc

```
Port 11731/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/21112

```
Port 21112/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/47001/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/49152/dce-rpc

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/49155/dce-rpc

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/49158/ncacn_http

```
Port 49158/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.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- 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: 2021/01/27

Plugin Output

tcp/0

```
 Information about this scan :

 Nessus version : 8.14.0
 Plugin feed version : 202106121427
 Scanner edition used : Nessus
 Scan type : Normal
 Scan policy used : rubber kin
 Scanner IP : 192.168.58.131
 Port scanner(s) : nessus_syn_scanner
 Port range : 0-65535
```

```
Ping RTT : Unavailable
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
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/7/2 2:10 EDT
Scan duration : 4308 sec
```

43815 - NetBIOS Multiple IP Address Enumeration

Synopsis

The remote host is configured with multiple IP addresses.

Description

By sending a special NetBIOS query, Nessus was able to detect the use of multiple IP addresses on the remote host. This indicates the host may be running virtualization software, a VPN client, or has multiple network interfaces.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/01/06, Modified: 2011/09/02

Plugin Output

udp/137

```
The remote host appears to be using the following IP addresses :

  - 30.90.90.99
  - 169.254.130.101
```

10884 - Network Time Protocol (NTP) Server Detection

Synopsis

An NTP server is listening on the remote host.

Description

An NTP server is listening on port 123. If not securely configured, it may provide information about its version, current date, current time, and possibly system information.

See Also

http://www.ntp.org

Solution

n/a

Risk Factor

None

References

XREF   IAVT:0001-T-0934

Plugin Information

Published: 2015/03/20, Modified: 2021/02/24

Plugin Output

udp/123/ntp

```
An NTP service has been discovered, listening on port 123.

No sensitive information has been disclosed.

Version : unknown
```

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: 2021/05/12

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows Server 2012 R2 Standard
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.

NTP:!:unknown
HTTP:Server: Microsoft-HTTPAPI/2.0

SinFP:
   P1:B11013:F0x12:W64240:O0204ffff:M1460:
   P2:B11013:F0x12:W64240:O0204ffff:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:181310_7_p=49155R
SSLcert:!:i/CN:Fortinet Untrusted CAi/O:Fortineti/OU:Certificate Authoritys/CN:ofcsslagent
dce394e5fca93475bce84f84ea4f81a6b63c3549



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

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: 2021/04/20

Plugin Output

tcp/3389/msrdp

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

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: 2021/02/03

Plugin Output

tcp/21112

```
This port supports SSLv3/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: 2021/03/09

Plugin Output

tcp/21112

```
The host names known by Nessus are :

  rk3adcsrv
  rk3adcsrv.rubberkingtyres.net

The Common Name in the certificate is :

  ofcsslagent
```

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: 2021/02/03

Plugin Output

tcp/21112

```
Subject Name:

Common Name: ofcsslagent

Issuer Name:

Country: US
State/Province: California
Locality: Sunnyvale
Organization: Fortinet
Organization Unit: Certificate Authority
Common Name: Fortinet Untrusted CA
Email Address: support@fortinet.com

Serial Number: 0A 8D 2F 46 9A C6 F6 69

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Apr 08 02:48:37 2021 GMT
Not Valid After: Dec 31 23:59:59 2039 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A0 33 C6 14 23 4B D0 A6 E1 26 24 E2 FC 41 12 0A C5 92 81
            BB 61 D7 A5 79 4E C6 C1 2C 73 B5 84 42 6A D3 F4 2C D6 57 DC
            B7 7C 8D 86 4C 45 73 A8 B6 DE AB 94 8E 61 7E 4A 87 28 29 A6
            91 D4 B7 B1 C5 51 9F CB 15 02 A6 BF 52 7F 36 81 2F BF FA 44
            72 3E 68 32 27 84 3A F7 41 F2 CC 22 8E 01 EB 7A EB 09 B1 90
```

```
            23 4B A8 06 F5 8F 8A 1A 4A 46 4D 61 A9 23 9D 13 2C 3E C7 83
            3C 97 3B 5D 9D 1D 7D 01 7E F8 31 0A E8 66 FF AF F9 2F F2 20
            E9 B1 01 29 94 19 0F 71 CA CC 66 27 90 32 83 FF 47 23 95 25
            D0 97 09 69 65 14 90 C7 BB EC 7D D8 05 2B EB 10 85 EB 44 5A
            F2 24 4B 50 4F 4E CF B8 03 66 2D A2 8B 90 69 65 DA 94 12 DE
            F6 4D BB 3A 2B 1E 64 7D A2 2C 64 AD 46 A3 30 5E 64 08 79 17
            96 9B 55 CB B7 73 63 7E 20 71 CE B0 39 FA 7A 57 F7 73 6C EE
            54 DA 5C 12 4C 33 E5 67 53 70 E9 8B 7E CC 70 4B 03
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 67 CF C4 FE 00 E1 34 DD E6 EF 1B 03 39 85 06 70 EA 82 A3
           61 25 30 66 48 6A 39 9A C7 37 B2 BA A4 CC 89 22 C3 E6 BD A5
           A3 26 61 28 7F 03 F1 49 A5 3F E2 85 51 84 23 5B 1B F5 B5 67
           0F 2E 41 C6 E3 35 93 5A CD ED DB 45 CF 2C FB 8E 39 D0 D2 4B
           7F E4 15 1D 4F 64 B5 74 08 10 04 46 78 59 71 26 29 11 30 ED
           E2 E9 67 4B D6 C8 27 86 B6 E2 6D D6 5B 1E E7 83 3B 21 37 C4
           64 1E D1 28 BD DB 2C 62 58 D6 74 13 07 86 59 16 AE CB 3F 48
           BC 2E FF 04 F9 CD F5 4F AD  [...]
```

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: 2021/02/03

Plugin Output

tcp/21112

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

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

     Name                     Code         KEX        Auth     Encryption           MAC
     ----------------------   ----------   ---        ----     --------------------  ---
     DES-CBC3-SHA             0x00, 0x0A   RSA        RSA      3DES-CBC(168)
   SHA1

   High Strength Ciphers (>= 112-bit key)

     Name                     Code         KEX        Auth     Encryption           MAC
     ----------------------   ----------   ---        ----     --------------------  ---
     DHE-RSA-AES128-SHA       0x00, 0x33   DH         RSA      AES-CBC(128)
   SHA1
     DHE-RSA-AES256-SHA       0x00, 0x39   DH         RSA      AES-CBC(256)
   SHA1
```

```
    ECDHE-RSA-AES128-SHA          0xC0, 0x13      ECDH         RSA        AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14      ECDH         RSA        AES-CBC(256)
SHA1
    AES128-SHA                    0x00, 0x2F      RSA          RSA        AES-CBC(128)
SHA1
    AES256-SHA                    0x00, 0x35      RSA          RSA        AES-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27      ECDH         RSA        AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28      ECDH         RSA        AES-CBC(256)
SHA384
    RSA-AES128-SHA256             0x00, 0x3C      RSA          RSA        AES-CBC(128)
SHA256
    RSA-AES256-SHA256             0x00, 0x3D      RSA          RSA        AES-CBC(256)
SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={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: 2021/03/09

Plugin Output

tcp/21112

```
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)

    Name                     Code        KEX     Auth    Encryption           MAC
    ---------------------    ----------  ---     ----    --------------------  ---
    DES-CBC3-SHA             0x00, 0x0A  RSA     RSA     3DES-CBC(168)
  SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                     Code        KEX     Auth    Encryption           MAC
    ---------------------    ----------  ---     ----    --------------------  ---
    DHE-RSA-AES128-SHA256    0x00, 0x9E  DH      RSA     AES-GCM(128)
  SHA256
    DHE-RSA-AES256-SHA384    0x00, 0x9F  DH      RSA     AES-GCM(256)
  SHA384
    RSA-AES128-SHA256        0x00, 0x9C  RSA     RSA     AES-GCM(128)
  SHA256
    RSA-AES256-SHA384        0x00, 0x9D  RSA     RSA     AES-GCM(256)
  SHA384
```

```
    DHE-RSA-AES128-SHA           0x00, 0x33     DH       RSA      AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA           0x00, 0x39     DH       RSA      AES-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA         0xC0, 0x13     ECDH     RSA      AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA         0xC0, 0x14     ECDH     RSA      AES-CBC(256)
SHA1
    AES128-SHA                   0x00, 0x2F     RSA      RSA      AES-CBC(128)
SHA1
    AES256-SHA                   0x00, 0x35     RSA      RSA      AES-CBC(256)
SHA1
    RC4-MD5                      0x00, 0x04     RSA      RSA      RC4(128)          MD5
    RC4-SHA                      0x00, 0x05     RSA      RSA      RC4(128)
SHA1
    ECDHE-RSA-AES128-SHA256      0xC0, 0x27     ECDH     RSA      AE [...]
```

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: 2021/03/09

Plugin Output

tcp/21112

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

   High Strength Ciphers (>= 112-bit key)

     Name                      Code          KEX       Auth    Encryption            MAC
     --------------------      ----------    ---       ----    --------------------  ---
     DHE-RSA-AES128-SHA256     0x00, 0x9E    DH        RSA     AES-GCM(128)
  SHA256
     DHE-RSA-AES256-SHA384     0x00, 0x9F    DH        RSA     AES-GCM(256)
  SHA384
     DHE-RSA-AES128-SHA        0x00, 0x33    DH        RSA     AES-CBC(128)
  SHA1
     DHE-RSA-AES256-SHA        0x00, 0x39    DH        RSA     AES-CBC(256)
  SHA1
     ECDHE-RSA-AES128-SHA      0xC0, 0x13    ECDH      RSA     AES-CBC(128)
  SHA1
```

```
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH        RSA       AES-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH        RSA       AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH        RSA       AES-CBC(256)
SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

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

References

XREF   IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
  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: 2021/04/14

Plugin Output

tcp/21

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

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: 2021/04/14

Plugin Output

tcp/25

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

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: 2021/04/14

Plugin Output

tcp/143

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

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: 2021/04/14

Plugin Output

tcp/443

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

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: 2021/04/14

Plugin Output

tcp/636

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

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: 2021/04/14

Plugin Output

tcp/5985/www

```
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: 2021/04/14

Plugin Output

tcp/21112

```
A TLSv1.2 server answered 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: 2021/04/14

Plugin Output

tcp/47001/www

```
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: 2021/04/14

Plugin Output

tcp/49158/ncacn_http

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

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

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

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: 2020/08/07

Plugin Output

tcp/21112

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/21112

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

110723 - Target Credential Status by Authentication Protocol - 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 not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF   IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2021/01/25

Plugin Output

tcp/0

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

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: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.58.131 to 30.90.90.99 :
192.168.58.131
192.168.58.2
30.90.90.99

Hop Count: 2
```

135860 - WMI Not Available

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2021/06/09

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

33139 - WS-Management Server Detection

Synopsis

The remote web server is used for remote management.

Description

The remote web server supports the Web Services for Management (WS-Management) specification, a general web services protocol based on SOAP for managing systems, applications, and other such entities.

See Also

https://www.dmtf.org/standards/ws-man

https://en.wikipedia.org/wiki/WS-Management

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2008/06/11, Modified: 2021/05/19

Plugin Output

tcp/5985/www

```
Here is some information about the WS-Management Server :

  Product Vendor  : Microsoft Corporation
  Product Version : OS: 0.0.0 SP: 0.0 Stack: 3.0
```

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: 2021/02/10

Plugin Output

tcp/445/cifs

```
The following 2 NetBIOS names have been gathered :

 RK3ADCSRV        = Computer name
 RUBBERKINGTYRES  = Workgroup / Domain name
```

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.
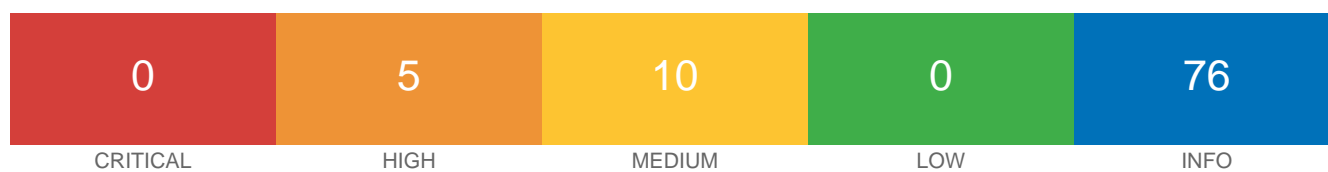
Risk Factor

None

Plugin Information

Published: 2002/04/20, Modified: 2020/07/08

Plugin Output

tcp/3389/msrdp

30.90.90.100

0	5	10	0	76
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Jul 2 02:10:04 2021
End time: Fri Jul 2 03:18:16 2021

Host Information

DNS Name: rk3rdpsrv.rubberkingtyres.net
Netbios Name: RK3RDPSRV
IP: 30.90.90.100
OS: Microsoft Windows Server 2012 R2 Standard

Vulnerabilities

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 SSL 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 v2.0 Base Score

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

CVSS v2.0 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: 2020/04/27

Plugin Output

tcp/443

```
  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=RK3RDPSRV.rubberkingtyres.net
```

```
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Mar 09 05:47:16 2021 GMT
|-Valid To            : Sep 08 05:47:16 2021 GMT
```

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 SSL 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 v2.0 Base Score

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

CVSS v2.0 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: 2020/04/27

Plugin Output

tcp/3389/msrdp

```
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=RK3RDPSRV.rubberkingtyres.net
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From         : Mar 09 05:11:40 2021 GMT
|-Valid To           : Sep 08 05:11:40 2021 GMT
```

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 v2.0 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: 2021/02/03

Plugin Output

tcp/443

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

      Name                       Code           KEX        Auth      Encryption              MAC
      ---------------------      ----------     ---        ----      --------------------    ---
      DES-CBC3-SHA               0x00, 0x0A     RSA        RSA       3DES-CBC(168)
   SHA1

The fields above are :

   {Tenable ciphername}
   {Cipher ID code}
   Kex={key exchange}
   Auth={authentication}
   Encrypt={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 v2.0 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: 2021/02/03

Plugin Output

tcp/3389/msrdp

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

     Name                          Code         KEX       Auth     Encryption             MAC
     ----------------------        ----------   ---       ----     --------------------   ---
     DES-CBC3-SHA                  0x00, 0x0A   RSA       RSA      3DES-CBC(168)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

Risk Factor

High

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 v2.0 Base Score

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

Plugin Information

Published: 2005/10/12, Modified: 2020/05/06

Plugin Output

tcp/443

```
- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3

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

    Name                      Code         KEX       Auth    Encryption            MAC
    ---------------------     ----------   ---       ----    --------------------  ---
    DES-CBC3-SHA                           RSA       RSA     3DES-CBC(168)
SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                      Code         KEX       Auth    Encryption            MAC
    ---------------------     ----------   ---       ----    --------------------  ---
    DHE-RSA-AES128-SHA                     DH        RSA     AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA                     DH        RSA     AES-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA                   ECDH      RSA     AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA                   ECDH      RSA     AES-CBC(256)
SHA1
    AES128-SHA                             RSA       RSA     AES-CBC(128)
SHA1
    AES256-SHA                             RSA       RSA     AES-CBC(256)
SHA1
    RC4-MD5                                RSA       RSA     RC4(128)              MD5
    RC4-SHA                                RSA       RSA     RC4(128)
SHA1
    ECDHE-RSA-AES128-SHA256                ECDH      RSA     AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384                ECDH      RSA     AES-CBC(256)
SHA384
    RSA-AES128-SHA256                      RSA       RSA     AES-CBC(128)
SHA256
    RSA-AES256-SHA256                      RSA       RSA     AES-CBC(256)
SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code} [...]
```

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

http://www.nessus.org/u?df39b8b3

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 v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

Plugin Information

Published: 2012/01/19, Modified: 2021/03/15

Plugin Output

tcp/445/cifs

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 SSL 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 v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/443

```
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=RK3RDPSRV.rubberkingtyres.net
|-Issuer  : CN=RK3RDPSRV.rubberkingtyres.net
```

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 SSL 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 v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/3389/msrdp

```
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=RK3RDPSRV.rubberkingtyres.net
|-Issuer  : CN=RK3RDPSRV.rubberkingtyres.net
```

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

https://www.rc4nomore.com/

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

Medium

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 v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (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: 2021/02/03

Plugin Output

tcp/443

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

  High Strength Ciphers (>= 112-bit key)

    Name                       Code          KEX        Auth    Encryption            MAC
    ---------------------      ----------    ---        ----    --------------------  ---
    RC4-MD5                    0x00, 0x04    RSA        RSA     RC4(128)              MD5
    RC4-SHA                    0x00, 0x05    RSA        RSA     RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={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

https://www.rc4nomore.com/

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

Medium

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 v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (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: 2021/02/03

Plugin Output

tcp/3389/msrdp

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

  High Strength Ciphers (>= 112-bit key)

    Name                       Code          KEX        Auth     Encryption              MAC
    ---------------------      ----------    ---        ----     --------------------    ---
    RC4-MD5                    0x00, 0x04    RSA        RSA      RC4(128)                MD5
    RC4-SHA                    0x00, 0x05    RSA        RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={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 SSL certificate for this service.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

tcp/443

```
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=RK3RDPSRV.rubberkingtyres.net
```

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 SSL certificate for this service.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

tcp/3389/msrdp

```
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=RK3RDPSRV.rubberkingtyres.net
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID   70574
CVE   CVE-2014-3566
XREF   CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2020/06/12

Plugin Output

tcp/443

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

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 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

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.

See Also

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

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/443

```
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 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

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.

See Also

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

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/3389/msrdp

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

10761 - COM+ Internet Services (CIS) Server Detection

Synopsis

A COM+ Internet Services (CIS) server is listening on this port.

Description

COM+ Internet Services are RPC over HTTP tunneling and require IIS to operate. CIS ports shouldn't be visible on internet but only behind a firewall.

See Also

http://www.nessus.org/u?d02f7e6e

https://support.microsoft.com/en-us/support/kb/articles/q282/2/61.asp

Solution

If you do not use this service, disable it with DCOMCNFG.

Otherwise, limit access to this port.

Risk Factor

None

Plugin Information

Published: 2001/09/14, Modified: 2019/11/22

Plugin Output

tcp/3388/ncacn_http

```
Server banner :

ncacn_http/1.0
```

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, Modified: 2021/06/03

Plugin Output

tcp/0

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

  cpe:/o:microsoft:windows_server_2012:r2

Following application CPE matched on the remote system :

  cpe:/a:microsoft:iis:8.5
```

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: 2020/08/20

Plugin Output

tcp/135/epmap

```
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 : WMsgKRpc062350

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 : WMsgKRpc062350

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 : dabrpc

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-fd8b75018e948de555

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000014
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc015128DD614

Object UUID : 52ef130c-08fd-4388-86b3-6edf00000014
UUID : 12e65dd8-887f-41ef-91bf-8d816c42c2e7, version 1.0
Description : Unknown RPC service
Annotation : Secure Desktop LRPC interface
Type : Local RPC service
Named pipe : WMsgKRpc015128DD614

Object UUID : 3bdb59a0-d736-4d44-9074-c1ee00000011
UUID : b2507c30-b126-494a-92ac-ee32b6eeb039, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-acf38c84280d56a468

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000011
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC servi [...]
```

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: 2020/08/20

Plugin Output

tcp/445/cifs

```
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 : \\RK3RDPSRV

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 : \\RK3RDPSRV

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 : \\RK3RDPSRV

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3d267954-eeb7-11d1-b94e-00c04fa3080d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \pipe\HydraLsPipe
```

```
Netbios name : \\RK3RDPSRV

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12d4b7c8-77d5-11d1-8c24-00c04fa3080d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \pipe\HydraLsPipe
Netbios name : \\RK3RDPSRV

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \pipe\trkwks
Netbios name : \\RK3RDPSRV

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\RK3RDPSRV

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\RK3RDPSRV

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Sec [...]
```

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: 2020/08/20

Plugin Output

tcp/5504/dce-rpc

```
The following DCERPC services are available on TCP port 5504 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ed96b012-c8ce-4f60-a682-35535b12ff75, version 2.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 5504
IP : 30.90.90.100
```

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: 2020/08/20

Plugin Output

tcp/6160/dce-rpc

```
The following DCERPC services are available on TCP port 6160 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d107c6e0-fc35-49ba-ba03-3e192de6797d, version 1.0
Description : Unknown RPC service
Annotation : Veeam Deployer
Type : Remote RPC service
TCP Port : 6160
IP : 30.90.90.100

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1.0
Description : Unknown RPC service
Annotation : Veeam RPC Invoker
Type : Remote RPC service
TCP Port : 6160
IP : 30.90.90.100
```

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: 2020/08/20

Plugin Output

tcp/6183/dce-rpc

```
The following DCERPC services are available on TCP port 6183 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1.0
Description : Unknown RPC service
Annotation : Veeam Invoker
Type : Remote RPC service
TCP Port : 6183
IP : 30.90.90.100

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d107c6e0-fc35-49ba-ba03-3e192de6797d, version 1.0
Description : Unknown RPC service
Annotation : Veeam Deployer
Type : Remote RPC service
TCP Port : 6183
IP : 30.90.90.100
```

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: 2020/08/20

Plugin Output

tcp/11731/dce-rpc

```
The following DCERPC services are available on TCP port 11731 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d107c6e0-fc35-49ba-ba03-3e192de6797d, version 1.0
Description : Unknown RPC service
Annotation : Veeam Deployer
Type : Remote RPC service
TCP Port : 11731
IP : 30.90.90.100

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1.0
Description : Unknown RPC service
Annotation : Veeam RPC Invoker
Type : Remote RPC service
TCP Port : 11731
IP : 30.90.90.100
```

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: 2020/08/20

Plugin Output

tcp/49152/dce-rpc

```
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 : 30.90.90.100
```

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: 2020/08/20

Plugin Output

tcp/49153/dce-rpc

```
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 : 30.90.90.100

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 : 30.90.90.100

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 : 30.90.90.100

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 : 30.90.90.100

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 : 30.90.90.100
```

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: 2020/08/20

Plugin Output

tcp/49154/dce-rpc

```
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 : 30.90.90.100

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 : 30.90.90.100

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 : 30.90.90.100

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 : 30.90.90.100

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 : 30.90.90.100

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 : 30.90.90.100

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Remote RPC service
TCP Port : 49154
IP : 30.90.90.100

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 : 30.90.90.100

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1.0
Description  [...]
```

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: 2020/08/20

Plugin Output

tcp/49155/dce-rpc

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

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49155
IP : 30.90.90.100

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49155
IP : 30.90.90.100

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49155
IP : 30.90.90.100

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
TCP Port : 49155
IP : 30.90.90.100
```

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: 2020/08/20

Plugin Output

tcp/49173/dce-rpc

```
The following DCERPC services are available on TCP port 49173 :

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 : 49173
IP : 30.90.90.100

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
TCP Port : 49173
IP : 30.90.90.100
```

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: 2020/08/20

Plugin Output

tcp/49177/dce-rpc

```
The following DCERPC services are available on TCP port 49177 :

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 : 49177
IP : 30.90.90.100

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 : 49177
IP : 30.90.90.100

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 : 49177
IP : 30.90.90.100

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 : 49177
IP : 30.90.90.100

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 : 49177
IP : 30.90.90.100
```

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: 2020/08/20

Plugin Output

tcp/56943/dce-rpc

```
The following DCERPC services are available on TCP port 56943 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3357951c-a1d1-47db-a278-ab945d063d03, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 56943
IP : 30.90.90.100
```

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: 2020/08/20

Plugin Output

tcp/57608/dce-rpc

```
The following DCERPC services are available on TCP port 57608 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3d267954-eeb7-11d1-b94e-00c04fa3080d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 57608
IP : 30.90.90.100

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12d4b7c8-77d5-11d1-8c24-00c04fa3080d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 57608
IP : 30.90.90.100
```

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: 2020/08/20

Plugin Output

tcp/57640/dce-rpc

```
The following DCERPC services are available on TCP port 57640 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : aa177641-fc9b-41bd-80ff-f964a701596f, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 57640
IP : 30.90.90.100

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 32e36e84-4ba2-496c-ba85-fb450f325107, version 2.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 57640
IP : 30.90.90.100
```

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: 2020/08/20

Plugin Output

tcp/57648/dce-rpc

```
The following DCERPC services are available on TCP port 57648 :

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 : 57648
IP : 30.90.90.100
```

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: 2020/08/20

Plugin Output

tcp/57651/dce-rpc

```
The following DCERPC services are available on TCP port 57651 :

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 : 57651
IP : 30.90.90.100
```

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: 2020/08/20

Plugin Output

tcp/57660/dce-rpc

```
The following DCERPC services are available on TCP port 57660 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b3195fe-d603-43d1-a0d5-9072d7cde122, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 57660
IP : 30.90.90.100

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 89759fce-5a25-4086-8967-de12f39a60b5, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 57660
IP : 30.90.90.100
```

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
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

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

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
30.90.90.100 resolves as rk3rdpsrv.rubberkingtyres.net.
```

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

References

XREF   IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2020/09/22

Plugin Output

tcp/0

```
  The following issues were reported :

    - Plugin      : no_local_checks_credentials.nasl
      Plugin ID   : 110723
      Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
      Message     :
  Credentials were not provided for detected SMB service.
```

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

Synopsis

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

Description

The remote host listens on tcp port 445 and replies to SMB requests.

By sending an NTLMSSP authentication request it is possible to obtain the name of the remote system and the name of its domain.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/11/06, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The following 2 NetBIOS names have been gathered :

 RK3RDPSRV       = Computer name
 RUBBERKINGTYRES = Workgroup / Domain name
```

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: 2020/01/22

Plugin Output

tcp/445/cifs

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

26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

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

If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access'

service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

References

XREF   IAVB:0001-B-0506

Plugin Information

Published: 2007/10/04, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

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

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: 2021/02/11

Plugin Output

tcp/139/smb

```
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: 2021/02/11

Plugin Output

tcp/445/cifs

```
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: 2019/11/22

Plugin Output

tcp/445/cifs

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/21

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/25

```
Port 25/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/80

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/110

```
Port 110/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/135/epmap

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/139/smb

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/143

```
Port 143/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/443

```
Port 443/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/445/cifs

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/3388/ncacn_http

```
Port 3388/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/3389/msrdp

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/5985

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/6184

```
Port 6184/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8008

```
Port 8008/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/49152/dce-rpc

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/49155/dce-rpc

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/56943/dce-rpc

```
Port 56943/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/57660/dce-rpc

```
Port 57660/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.

- The ping round trip time

- Whether credentialed or third-party patch management checks are possible.

- Whether the display of superseded patches is enabled

- 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: 2021/01/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.14.0
Plugin feed version : 202106121427
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : rubber kin
Scanner IP : 192.168.58.131
Port scanner(s) : nessus_syn_scanner
Port range : 0-65535
```

```
Ping RTT : Unavailable
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
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/7/2 2:10 EDT
Scan duration : 4091 sec
```

24786 - Nessus Windows Scan Not Performed with Admin Privileges

Synopsis

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

Description

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

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

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

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

References

XREF   IAVB:0001-B-0505

Plugin Information

Published: 2007/03/12, Modified: 2020/09/22

Plugin Output

tcp/0

```
It was not possible to connect to '\\RK3RDPSRV\ADMIN$' with the supplied credentials.
```

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: 2021/05/12

Plugin Output

tcp/0

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


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

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: 2021/02/03

Plugin Output

tcp/443

```
This port supports SSLv3/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: 2021/02/03

Plugin Output

tcp/3389/msrdp

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

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: 2021/02/03

Plugin Output

tcp/443

```
Subject Name:

Common Name: RK3RDPSRV.rubberkingtyres.net

Issuer Name:

Common Name: RK3RDPSRV.rubberkingtyres.net

Serial Number: 08 F5 D4 3F E2 39 DE 02

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 09 05:47:16 2021 GMT
Not Valid After: Sep 08 05:47:16 2021 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A0 33 C6 14 23 4B D0 A6 E1 26 24 E2 FC 41 12 0A C5 92 81
            BB 61 D7 A5 79 4E C6 C1 2C 73 B5 84 42 6A D3 F4 2C D6 57 DC
            B7 7C 8D 86 4C 45 73 A8 B6 DE AB 94 8E 61 7E 4A 87 28 29 A6
            91 D4 B7 B1 C5 51 9F CB 15 02 A6 BF 52 7F 36 81 2F BF FA 44
            72 3E 68 32 27 84 3A F7 41 F2 CC 22 8E 01 EB 7A EB 09 B1 90
            23 4B A8 06 F5 8F 8A 1A 4A 46 4D 61 A9 23 9D 13 2C 3E C7 83
            3C 97 3B 5D 9D 1D 7D 01 7E F8 31 0A E8 66 FF AF F9 2F F2 20
            E9 B1 01 29 94 19 0F 71 CA CC 66 27 90 32 83 FF 47 23 95 25
            D0 97 09 69 65 14 90 C7 BB EC 7D D8 05 2B EB 10 85 EB 44 5A
            F2 24 4B 50 4F 4E CF B8 03 66 2D A2 8B 90 69 65 DA 94 12 DE
            F6 4D BB 3A 2B 1E 64 7D A2 2C 64 AD 46 A3 30 5E 64 08 79 17
```

```
                96 9B 55 CB B7 73 63 7E 20 71 CE B0 39 FA 7A 57 F7 73 6C EE
                54 DA 5C 12 4C 33 E5 67 53 70 E9 8B 7E CC 70 4B 03
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 9F 99 CB 68 65 20 32 F8 6B E3 63 00 3A 9E DB 84 54 72 D6
                19 79 F9 92 F7 A4 79 61 97 1E 80 3F E7 CC 39 D5 02 95 DA 66
                23 B6 62 68 C8 DA 29 C8 D8 CB 49 A7 13 B1 8F A6 71 36 85 F1
                84 3D 5A 45 8C FF 6C 95 3F B4 6C 19 DC 22 C1 2E D3 AA C9 15
                39 91 DD 59 DB 67 25 2D 08 C8 40 0F 3B C3 78 BC 23 47 87 37
                F6 A3 38 6E 76 B1 80 68 AC 7E 79 7A 10 B3 DF 56 02 E9 87 9B
                6C 88 1C 93 DE 6C 84 3A BA C9 75 85 8B F2 FE D8 FB 2B D5 06
                46 22 93 AF 1A EA 8B 3F 5E 03 06 8E 39 7B DD CD E7 86 A6 3D
                A0 B5 EB 5A 46 D8 7B F7 82 A8 70 5B C8 B4 82 BD E7 78 5B 00
                7D A9 26 CF 15 8 [...]
```

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: 2021/02/03

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: RK3RDPSRV.rubberkingtyres.net

Issuer Name:

Common Name: RK3RDPSRV.rubberkingtyres.net

Serial Number: 1E FA 7D AB 75 76 32 93 4C 50 02 54 2C A9 17 21

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 09 05:11:40 2021 GMT
Not Valid After: Sep 08 05:11:40 2021 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C1 7B 89 D3 B5 FD 06 60 EB 79 2E C3 8A EE 61 69 BA 85 B0
            90 A4 28 E9 0A 58 E8 29 62 74 FA D5 DA E8 6C DA 2E E7 FE DC
            0C 23 84 7C 62 99 63 2B FB 13 B6 63 EF DC 3F 2A EC E6 FD DB
            97 C6 14 40 A3 76 E5 62 36 15 E2 B9 23 3B 19 B6 5D B1 C6 C2
            22 E2 48 42 08 E3 2A CF 53 49 53 38 97 19 FE 04 96 C6 79 35
            4B 87 92 0B 4E 26 A9 01 23 66 60 B1 7C 5F 76 B9 29 15 41 F6
            DC F9 86 96 AC 25 DA C4 70 7D 39 C2 8D 62 C6 75 9E 2B B4 C8
            7F 72 4B 7E 11 F2 F5 34 1E E0 2B 08 BD 9A AB AF C7 B5 47 55
            C8 F1 B0 67 2B E3 6B C3 A3 A4 0F 54 21 58 69 27 C9 EC 0B 5B
            68 A7 79 41 2E 05 64 BE 02 6E 66 43 42 C5 3F 8D DC 5E CB 50
            43 94 4C 28 D7 0C D9 62 B4 7C 0C 13 A4 80 4D 3D 64 7E 7B 68
```

```
                2D 3D BE CC 25 4B C0 C7 39 0C 63 A6 F7 CE 25 29 01 FF 29 6C
                DE 3A C9 B8 11 D8 CC 44 1E EF A5 4C 37 5E 7F E8 4D
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 88 3F 90 C1 D9 50 7C CF F8 B6 6A 3A 3A FF F8 7A D8 BA 13
                DA 91 4D 9B 8A 86 72 BD CB F7 F4 48 A1 DE 41 95 03 2D BD A4
                AA F0 FC B9 A5 54 10 5A 27 7A 72 32 75 38 BE 3C 71 0C 47 35
                84 0B 4F 37 92 17 DF 1E FE 6E 4A 9C 0A 11 DC 6D 0A F6 17 0D
                B6 14 31 5B 2F AF 89 E3 F2 74 39 8B DE EC 45 C3 08 CF 99 DF
                F0 1E B8 BB BD 27 A1 DD 01 A4 5E 6D FC BC 40 4C F2 B6 D2 4F
                6A A0 73 8E 16 D5 72 98 9B E6 40 1E D7 9D 7D 33 3B 0C B2 DE
                92 9A 7C 34 96 27 E0 DE BA E4 96 A6 78 AC D2 AE FB D9 2A B4
                0A 47 7E 37 D7 F2 87 A1 48 40 71 05 27 BC 84 93 63 2B 1B FA
        [...]
```

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: 2021/02/03

Plugin Output

tcp/443

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

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

    Name                      Code        KEX        Auth      Encryption            MAC
    ----------------------    ----------  ---        ----      --------------------  ---
    DES-CBC3-SHA              0x00, 0x0A  RSA        RSA       3DES-CBC(168)
  SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                      Code        KEX        Auth      Encryption            MAC
    ----------------------    ----------  ---        ----      --------------------  ---
    DHE-RSA-AES128-SHA        0x00, 0x33  DH         RSA       AES-CBC(128)
  SHA1
    DHE-RSA-AES256-SHA        0x00, 0x39  DH         RSA       AES-CBC(256)
  SHA1
```

```
    ECDHE-RSA-AES128-SHA              0xC0, 0x13      ECDH        RSA       AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA              0xC0, 0x14      ECDH        RSA       AES-CBC(256)
SHA1
    AES128-SHA                       0x00, 0x2F      RSA         RSA       AES-CBC(128)
SHA1
    AES256-SHA                       0x00, 0x35      RSA         RSA       AES-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA256          0xC0, 0x27      ECDH        RSA       AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384          0xC0, 0x28      ECDH        RSA       AES-CBC(256)
SHA384
    RSA-AES128-SHA256                0x00, 0x3C      RSA         RSA       AES-CBC(128)
SHA256
    RSA-AES256-SHA256                0x00, 0x3D      RSA         RSA       AES-CBC(256)
SHA256


The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={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: 2021/02/03

Plugin Output

tcp/3389/msrdp

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

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

     Name                      Code         KEX        Auth      Encryption            MAC
     ----------------------    ----------   ---        ----      --------------------  ---
     DES-CBC3-SHA              0x00, 0x0A   RSA        RSA       3DES-CBC(168)
   SHA1

   High Strength Ciphers (>= 112-bit key)

     Name                      Code         KEX        Auth      Encryption            MAC
     ----------------------    ----------   ---        ----      --------------------  ---
     DHE-RSA-AES128-SHA        0x00, 0x33   DH         RSA       AES-CBC(128)
   SHA1
     DHE-RSA-AES256-SHA        0x00, 0x39   DH         RSA       AES-CBC(256)
   SHA1
```

```
    ECDHE-RSA-AES128-SHA          0xC0, 0x13      ECDH        RSA         AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14      ECDH        RSA         AES-CBC(256)
SHA1
    AES128-SHA                    0x00, 0x2F      RSA         RSA         AES-CBC(128)
SHA1
    AES256-SHA                    0x00, 0x35      RSA         RSA         AES-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27      ECDH        RSA         AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28      ECDH        RSA         AES-CBC(256)
SHA384
    RSA-AES128-SHA256             0x00, 0x3C      RSA         RSA         AES-CBC(128)
SHA256
    RSA-AES256-SHA256             0x00, 0x3D      RSA         RSA         AES-CBC(256)
SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={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: 2021/03/09

Plugin Output

tcp/443

```
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)

    Name                    Code         KEX      Auth     Encryption           MAC
    ----------------------  ----------   ---      ----     --------------------  ---
    DES-CBC3-SHA            0x00, 0x0A   RSA      RSA      3DES-CBC(168)
  SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                    Code         KEX      Auth     Encryption           MAC
    ----------------------  ----------   ---      ----     --------------------  ---
    DHE-RSA-AES128-SHA256   0x00, 0x9E   DH       RSA      AES-GCM(128)
  SHA256
    DHE-RSA-AES256-SHA384   0x00, 0x9F   DH       RSA      AES-GCM(256)
  SHA384
    RSA-AES128-SHA256       0x00, 0x9C   RSA      RSA      AES-GCM(128)
  SHA256
    RSA-AES256-SHA384       0x00, 0x9D   RSA      RSA      AES-GCM(256)
  SHA384
```

```
    DHE-RSA-AES128-SHA          0x00, 0x33      DH          RSA         AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA          0x00, 0x39      DH          RSA         AES-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA        0xC0, 0x13      ECDH        RSA         AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA        0xC0, 0x14      ECDH        RSA         AES-CBC(256)
SHA1
    AES128-SHA                  0x00, 0x2F      RSA         RSA         AES-CBC(128)
SHA1
    AES256-SHA                  0x00, 0x35      RSA         RSA         AES-CBC(256)
SHA1
    RC4-MD5                     0x00, 0x04      RSA         RSA         RC4(128)                MD5
    RC4-SHA                     0x00, 0x05      RSA         RSA         RC4(128)
SHA1
    ECDHE-RSA-AES128-SHA256     0xC0, 0x27      ECDH        RSA         AE [...]
```

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: 2021/03/09

Plugin Output

tcp/3389/msrdp

```
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)

    Name                    Code         KEX        Auth    Encryption           MAC
    ----------------------  ----------   ---        ----    --------------------  ---
    DES-CBC3-SHA            0x00, 0x0A   RSA        RSA     3DES-CBC(168)
  SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                    Code         KEX        Auth    Encryption           MAC
    ----------------------  ----------   ---        ----    --------------------  ---
    DHE-RSA-AES128-SHA256   0x00, 0x9E   DH         RSA     AES-GCM(128)
  SHA256
    DHE-RSA-AES256-SHA384   0x00, 0x9F   DH         RSA     AES-GCM(256)
  SHA384
    RSA-AES128-SHA256       0x00, 0x9C   RSA        RSA     AES-GCM(128)
  SHA256
    RSA-AES256-SHA384       0x00, 0x9D   RSA        RSA     AES-GCM(256)
  SHA384
```

DHE-RSA-AES128-SHA	0x00, 0x33	DH	RSA	AES-CBC(128)	SHA1
DHE-RSA-AES256-SHA	0x00, 0x39	DH	RSA	AES-CBC(256)	SHA1
ECDHE-RSA-AES128-SHA	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	SHA1
ECDHE-RSA-AES256-SHA	0xC0, 0x14	ECDH	RSA	AES-CBC(256)	SHA1
AES128-SHA	0x00, 0x2F	RSA	RSA	AES-CBC(128)	SHA1
AES256-SHA	0x00, 0x35	RSA	RSA	AES-CBC(256)	SHA1
RC4-MD5	0x00, 0x04	RSA	RSA	RC4(128)	MD5
RC4-SHA	0x00, 0x05	RSA	RSA	RC4(128)	SHA1
ECDHE-RSA-AES128-SHA256	0xC0, 0x27	ECDH	RSA	AE [...]	

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: 2021/03/09

Plugin Output

tcp/443

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

   High Strength Ciphers (>= 112-bit key)

     Name                     Code           KEX        Auth     Encryption            MAC
     --------------------     ----------     ---        ----     --------------------  ---
     DHE-RSA-AES128-SHA256    0x00, 0x9E     DH         RSA      AES-GCM(128)
   SHA256
     DHE-RSA-AES256-SHA384    0x00, 0x9F     DH         RSA      AES-GCM(256)
   SHA384
     DHE-RSA-AES128-SHA       0x00, 0x33     DH         RSA      AES-CBC(128)
   SHA1
     DHE-RSA-AES256-SHA       0x00, 0x39     DH         RSA      AES-CBC(256)
   SHA1
     ECDHE-RSA-AES128-SHA     0xC0, 0x13     ECDH       RSA      AES-CBC(128)
   SHA1
```

```
    ECDHE-RSA-AES256-SHA           0xC0, 0x14      ECDH        RSA       AES-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA256        0xC0, 0x27      ECDH        RSA       AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384        0xC0, 0x28      ECDH        RSA       AES-CBC(256)
SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={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: 2021/03/09

Plugin Output

tcp/3389/msrdp

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

  High Strength Ciphers (>= 112-bit key)

    Name                     Code         KEX      Auth    Encryption           MAC
    --------------------     ----------   ---      ----    --------------------  ---
    DHE-RSA-AES128-SHA256    0x00, 0x9E   DH       RSA     AES-GCM(128)
SHA256
    DHE-RSA-AES256-SHA384    0x00, 0x9F   DH       RSA     AES-GCM(256)
SHA384
    DHE-RSA-AES128-SHA       0x00, 0x33   DH       RSA     AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA       0x00, 0x39   DH       RSA     AES-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA     0xC0, 0x13   ECDH     RSA     AES-CBC(128)
  SHA1
```

```
     ECDHE-RSA-AES256-SHA            0xC0, 0x14        ECDH          RSA          AES-CBC(256)
  SHA1
     ECDHE-RSA-AES128-SHA256         0xC0, 0x27        ECDH          RSA          AES-CBC(128)
  SHA256
     ECDHE-RSA-AES256-SHA384         0xC0, 0x28        ECDH          RSA          AES-CBC(256)
  SHA384

  The fields above are :

   {Tenable ciphername}
   {Cipher ID code}
   Kex={key exchange}
   Auth={authentication}
   Encrypt={symmetric encryption method}
   MAC={message authentication code}
   {export flag}
```

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

References

XREF   IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
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: 2021/04/14

Plugin Output

tcp/21

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

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: 2021/04/14

Plugin Output

tcp/25

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

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: 2021/04/14

Plugin Output

tcp/443

```
A TLSv1.2 server answered 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: 2021/04/14

Plugin Output

tcp/3388/ncacn_http

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

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

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

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: 2020/08/07

Plugin Output

tcp/443

```
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

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

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: 2020/08/07

Plugin Output

tcp/3389/msrdp

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/443

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/3389/msrdp

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

110723 - Target Credential Status by Authentication Protocol - 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 not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF   IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2021/01/25

Plugin Output

tcp/0

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

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: 2021/02/24

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: RK3RDPSRV.rubberkingtyres.net

Issuer Name:

Common Name: RK3RDPSRV.rubberkingtyres.net

Serial Number: 1E FA 7D AB 75 76 32 93 4C 50 02 54 2C A9 17 21

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 09 05:11:40 2021 GMT
Not Valid After: Sep 08 05:11:40 2021 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C1 7B 89 D3 B5 FD 06 60 EB 79 2E C3 8A EE 61 69 BA 85 B0
            90 A4 28 E9 0A 58 E8 29 62 74 FA D5 DA E8 6C DA 2E E7 FE DC
            0C 23 84 7C 62 99 63 2B FB 13 B6 63 EF DC 3F 2A EC E6 FD DB
            97 C6 14 40 A3 76 E5 62 36 15 E2 B9 23 3B 19 B6 5D B1 C6 C2
            22 E2 48 42 08 E3 2A CF 53 49 53 38 97 19 FE 04 96 C6 79 35
            4B 87 92 0B 4E 26 A9 01 23 66 60 B1 7C 5F 76 B9 29 15 41 F6
            DC F9 86 96 AC 25 DA C4 70 7D 39 C2 8D 62 C6 75 9E 2B B4 C8
            7F 72 4B 7E 11 F2 F5 34 1E E0 2B 08 BD 9A AB AF C7 B5 47 55
            C8 F1 B0 67 2B E3 6B C3 A3 A4 0F 54 21 58 69 27 C9 EC 0B 5B
            68 A7 79 41 2E 05 64 BE 02 6E 66 43 42 C5 3F 8D DC 5E CB 50
            43 94 4C 28 D7 0C D9 62 B4 7C 0C 13 A4 80 4D 3D 64 7E 7B 68
```

```
                 2D 3D BE CC 25 4B C0 C7 39 0C 63 A6 F7 CE 25 29 01 FF 29 6C
                 DE 3A C9 B8 11 D8 CC 44 1E EF A5 4C 37 5E 7F E8 4D
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 88 3F 90 C1 D9 50 7C CF F8 B6 6A 3A 3A FF F8 7A D8 BA 13
           DA 91 4D 9B 8A 86 72 BD CB F7 F4 48 A1 DE 41 95 03 2D BD A4
           AA F0 FC B9 A5 54 10 5A 27 7A 72 32 75 38 BE 3C 71 0C 47 35
           84 0B 4F 37 92 17 DF 1E FE 6E 4A 9C 0A 11 DC 6D 0A F6 17 0D
           B6 14 31 5B 2F AF 89 E3 F2 74 39 8B DE EC 45 C3 08 CF 99 DF
           F0 1E B8 BB BD 27 A1 DD 01 A4 5E 6D FC BC 40 4C F2 B6 D2 4F
           6A A0 73 8E 16 D5 72 98 9B E6 40 1E D7 9D 7D 33 3B 0C B2 DE
           92 9A 7C 34 96 27 E0 DE BA E4 96 A6 78 AC D2 AE FB D9 2A B4
           0A 47 7E 37 D7 F2 87 A1 48 40 71 05 27 BC 84 93 63 2B 1B FA
      [...]
```

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: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.58.131 to 30.90.90.100 :
192.168.58.131
192.168.58.2
30.90.90.100

Hop Count: 2
```

135860 - WMI Not Available

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2021/06/09

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

33139 - WS-Management Server Detection

Synopsis

The remote web server is used for remote management.

Description

The remote web server supports the Web Services for Management (WS-Management) specification, a general web services protocol based on SOAP for managing systems, applications, and other such entities.

See Also

https://www.dmtf.org/standards/ws-man

https://en.wikipedia.org/wiki/WS-Management

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2008/06/11, Modified: 2021/05/19

Plugin Output

tcp/5985

```
Here is some information about the WS-Management Server :

  Product Vendor  : Microsoft Corporation
  Product Version : OS: 0.0.0 SP: 0.0 Stack: 3.0
```

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: 2021/02/10

Plugin Output

tcp/445/cifs

```
The following 2 NetBIOS names have been gathered :

 RK3RDPSRV       = Computer name
 RUBBERKINGTYRES  = Workgroup / Domain name
```

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: 2020/07/08

Plugin Output

tcp/3389/msrdp

30.90.90.108

0	0	0	0	46
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Jul 2 02:10:04 2021
End time: Fri Jul 2 03:18:06 2021

Host Information

DNS Name: rk3up-pc.rubberkingtyres.net
Netbios Name: RK3UP-PC
IP: 30.90.90.108
MAC Address: 00:E4:5C:68:58:7C
OS: Windows

Vulnerabilities

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, Modified: 2021/06/03

Plugin Output

tcp/0

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

  cpe:/o:microsoft:windows
```

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: 2020/08/20

Plugin Output

tcp/135/epmap

```
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 : WMsgKRpc07E0A0

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 : WMsgKRpc07E0A0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
```

```
Description : Unknown RPC service
Type : Local RPC service
Named pipe : dabrpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : csebpub

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-d93776669d2fd0b157

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : LRPC-5c89f61353bbca634d

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : e8d5f0e9-0b5f-4a58-9bee-6ef8652dd818

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d2716e94-25cb-4820-bc15-537866578562, version 1.0
Description :  [...]
```

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: 2020/08/20

Plugin Output

tcp/445/cifs

```
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 : \\RK3UP-PC

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 : \\RK3UP-PC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1.0
Description : Unknown RPC service
Annotation : Vpn APIs
Type : Remote RPC service
Named pipe : \PIPE\ROUTER
Netbios name : \\RK3UP-PC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0
Description : Telephony service
Windows process : svchost.exe
```

```
Annotation : Unimodem LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\tapsrv
Netbios name : \\RK3UP-PC

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\RK3UP-PC

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\RK3UP-PC

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 : \\RK3UP-PC

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 : \\RK3UP-PC

Object UUID : 0 [...]
```

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: 2020/08/20

Plugin Output

tcp/49664/dce-rpc

```
The following DCERPC services are available on TCP port 49664 :

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 : 49664
IP : 30.90.90.108
```

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: 2020/08/20

Plugin Output

tcp/49665/dce-rpc

```
The following DCERPC services are available on TCP port 49665 :

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 : 49665
IP : 30.90.90.108

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 : 49665
IP : 30.90.90.108
```

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: 2020/08/20

Plugin Output

tcp/49666/dce-rpc

```
The following DCERPC services are available on TCP port 49666 :

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 : 49666
IP : 30.90.90.108
```

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: 2020/08/20

Plugin Output

tcp/49667/dce-rpc

```
The following DCERPC services are available on TCP port 49667 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 29770a8f-829b-4158-90a2-78cd488501f7, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49667
IP : 30.90.90.108
```

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: 2020/08/20

Plugin Output

tcp/49668/dce-rpc

```
The following DCERPC services are available on TCP port 49668 :

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49668
IP : 30.90.90.108

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49668
IP : 30.90.90.108

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 : 49668
IP : 30.90.90.108

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
TCP Port : 49668
IP : 30.90.90.108

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 49668
IP : 30.90.90.108

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 49668
IP : 30.90.90.108
```

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: 2020/08/20

Plugin Output

tcp/49669/dce-rpc

```
The following DCERPC services are available on TCP port 49669 :

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 : 49669
IP : 30.90.90.108

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 : 49669
IP : 30.90.90.108

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 : 49669
IP : 30.90.90.108

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 : 49669
IP : 30.90.90.108

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 : 49669
IP : 30.90.90.108
```

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: 2020/08/20

Plugin Output

tcp/49679/dce-rpc

```
The following DCERPC services are available on TCP port 49679 :

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 : 49679
IP : 30.90.90.108
```

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: 2020/08/20

Plugin Output

tcp/49696/dce-rpc

```
The following DCERPC services are available on TCP port 49696 :

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 : 49696
IP : 30.90.90.108
```

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: 2020/08/20

Plugin Output

tcp/49714/dce-rpc

```
The following DCERPC services are available on TCP port 49714 :

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 : 49714
IP : 30.90.90.108

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
TCP Port : 49714
IP : 30.90.90.108

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 49714
IP : 30.90.90.108

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
```

```
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 49714
IP : 30.90.90.108
```

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 : 50
```

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: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 00:E4:5C:68:58:7C
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

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

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
30.90.90.108 resolves as rk3up-pc.rubberkingtyres.net.
```

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: 2019/11/22

Plugin Output

tcp/8008/www

```
Response Code : HTTP/1.1 302 Found

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

  Location: https://rk3up-pc.rubberkingtyres.net:8010/
  Connection: close
  X-Frame-Options: SAMEORIGIN
  X-XSS-Protection: 1; mode=block
  X-Content-Type-Options: nosniff
  Content-Security-Policy: frame-ancestors 'self'

Response Body :
```

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

References

XREF   IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2020/09/22

Plugin Output

tcp/0

```
  The following issues were reported :

   - Plugin      : no_local_checks_credentials.nasl
     Plugin ID   : 110723
     Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
     Message     :
 Credentials were not provided for detected SMB service.
```

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: 2021/02/11

Plugin Output

tcp/139/smb

```
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: 2021/02/11

Plugin Output

tcp/445/cifs

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/21

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/25

```
Port 25/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/80

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/110

```
Port 110/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/135/epmap

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/139/smb

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/143

```
Port 143/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/443

```
Port 443/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/445/cifs

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/2000

```
Port 2000/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/3389

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/5040

```
Port 5040/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/5060

```
Port 5060/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8008/www

```
Port 8008/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8020

```
Port 8020/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/49666/dce-rpc

```
Port 49666/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/49669/dce-rpc

```
Port 49669/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/49714/dce-rpc

```
Port 49714/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.

- The ping round trip time

- Whether credentialed or third-party patch management checks are possible.

- Whether the display of superseded patches is enabled

- 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: 2021/01/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.14.0
Plugin feed version : 202106121427
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : rubber kin
Scanner IP : 192.168.58.131
Port scanner(s) : nessus_syn_scanner
Port range : 0-65535
```

```
Ping RTT : Unavailable
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
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/7/2 2:10 EDT
Scan duration : 4022 sec
```

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: 2021/05/12

Plugin Output

tcp/0

```
Remote operating system : Windows
Confidence level : 50
Method : Misc

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.

SinFP:!:
    P1:B11013:F0x12:W64240:O0204ffff:M1460:
    P2:B11013:F0x12:W64240:O0204ffff:M1460:
    P3:B00000:F0x00:W0:O0:M0
    P4:181310_7_p=80R


The remote host is running Windows
```

10919 - Open Port Re-check

Synopsis

Previously open ports are now closed.

Description

One of several ports that were previously open are now closed or unresponsive.

There are several possible reasons for this :

- The scan may have caused a service to freeze or stop running.

- An administrator may have stopped a particular service during the scanning process.

This might be an availability problem related to the following :

- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.

- This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.

- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again.

Solution

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF   IAVB:0001-B-0509

Plugin Information

Published: 2002/03/19, Modified: 2020/09/22

Plugin Output

tcp/0

```
 Port 135 was detected as being open but is now unresponsive
```

```
Port 3389 was detected as being open initialy but was found unresponsive later.
 It is now unresponsive
Port 49666 was detected as being open but is now unresponsive
Port 49714 was detected as being open initialy but was found unresponsive later.
 It is now unresponsive
Port 5040 was detected as being open but is now unresponsive
Port 49669 was detected as being open but is now unresponsive
```

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: 2021/04/14

Plugin Output

tcp/8008/www

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

110723 - Target Credential Status by Authentication Protocol - 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 not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF   IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2021/01/25

Plugin Output

tcp/0

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

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: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.58.131 to 30.90.90.108 :
192.168.58.131
192.168.58.2
30.90.90.108

Hop Count: 2
```

135860 - WMI Not Available

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2021/06/09

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2020/06/12

Plugin Output

tcp/8008/www

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 302
rather than 404. The requested URL was :

    http://rk3up-pc.rubberkingtyres.net:8008/riej2LPs67hY.html
```

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: 2021/02/10

Plugin Output

udp/137/netbios-ns

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

 RK3UP-PC        = File Server Service
 RK3UP-PC        = Computer name
 RUBBERKINGTYRES = Workgroup / Domain name

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

   00:e4:5c:68:58:7c
```

30.90.90.111

0	0	0	0	10
CRITICAL	HIGH	MEDIUM	LOW	INFO
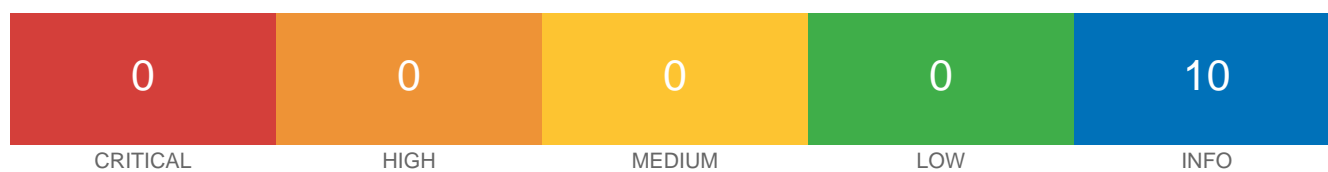
Scan Information

Start time: Fri Jul 2 02:10:04 2021
End time: Fri Jul 2 03:13:49 2021

Host Information

IP: 30.90.90.111
OS: CISCO PIX 7.0

Vulnerabilities

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, Modified: 2021/06/03

Plugin Output

tcp/0

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

  cpe:/o:cisco:pix_firewall:7.0
```

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 : firewall
Confidence level : 70
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/2000

```
Port 2000/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/5900

```
Port 5900/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/6000

```
Port 6000/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8008

```
Port 8008/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8020

```
Port 8020/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.

- The ping round trip time

- Whether credentialed or third-party patch management checks are possible.

- Whether the display of superseded patches is enabled

- 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: 2021/01/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.14.0
Plugin feed version : 202106121427
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : rubber kin
Scanner IP : 192.168.58.131
Port scanner(s) : nessus_syn_scanner
Port range : 0-65535
```

```
Ping RTT : Unavailable
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
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/7/2 2:10 EDT
Scan duration : 3817 sec
```

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: 2021/05/12

Plugin Output

tcp/0

```
Remote operating system : CISCO PIX 7.0
Confidence level : 70
Method : SinFP


The remote host is running CISCO PIX 7.0
```

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
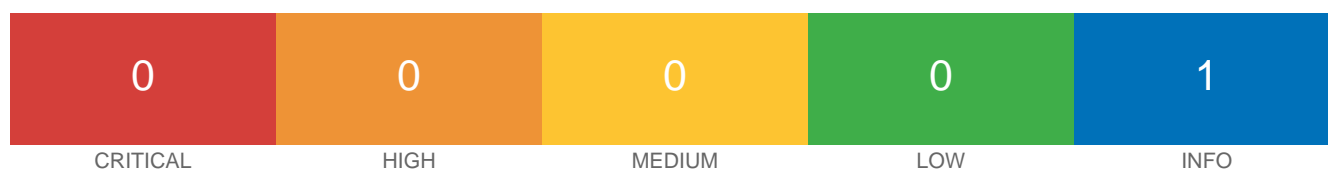
Published: 1999/11/27, Modified: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.58.131 to 30.90.90.111 :
192.168.58.131
192.168.58.2
30.90.90.111

Hop Count: 2
```

30.90.90.112

0	0	0	0	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Jul 2 02:10:04 2021
End time: Fri Jul 2 02:17:53 2021

Host Information

IP: 30.90.90.112

Vulnerabilities

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/0

```
The TCP port scan could not complete: The remote target has been silent for too long.
This could indicate that it has been switched off, or that an IPS is now blocking the scanner probes
```

30.90.90.125

0	0	0	0	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Jul 2 02:10:04 2021
End time: Fri Jul 2 02:28:59 2021

Host Information

IP: 30.90.90.125

Vulnerabilities

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

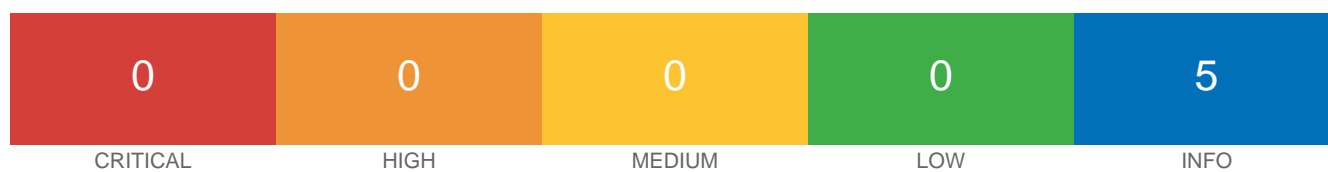**Risk Factor**

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/0

```
The TCP port scan could not complete: The remote target has been silent for too long.
This could indicate that it has been switched off, or that an IPS is now blocking the scanner probes
```

30.90.90.149

0	**0**	**0**	**0**	**5**
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Jul 2 02:10:04 2021
End time: Fri Jul 2 03:13:51 2021

Host Information

IP: 30.90.90.149

Vulnerabilities

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/21

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/143

```
Port 143/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8015

```
Port 8015/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.

- The ping round trip time

- Whether credentialed or third-party patch management checks are possible.

- Whether the display of superseded patches is enabled

- 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: 2021/01/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.14.0
Plugin feed version : 202106121427
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : rubber kin
Scanner IP : 192.168.58.131
Port scanner(s) : nessus_syn_scanner
Port range : 0-65535
```

```
Ping RTT : Unavailable
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
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/7/2 2:10 EDT
Scan duration : 3826 sec
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

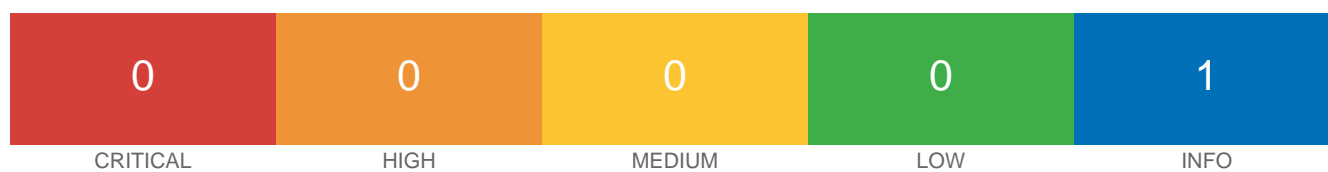n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.58.131 to 30.90.90.149 :
192.168.58.131
192.168.58.2
30.90.90.149

Hop Count: 2
```

30.90.90.158

0	0	0	0	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Jul 2 02:10:04 2021
End time: Fri Jul 2 02:22:30 2021

Host Information

IP: 30.90.90.158

Vulnerabilities

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.
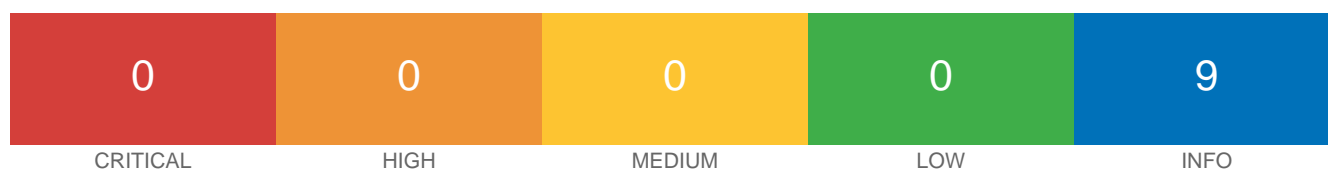
Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/0

The TCP port scan could not complete: The remote target has been silent for too long.
This could indicate that it has been switched off, or that an IPS is now blocking the scanner probes

30.90.90.218

0	0	0	0	9
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Jul 2 02:10:04 2021
End time: Fri Jul 2 03:13:50 2021

Host Information

IP: 30.90.90.218
OS: CISCO PIX 7.0

Vulnerabilities

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, Modified: 2021/06/03

Plugin Output

tcp/0

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

  cpe:/o:cisco:pix_firewall:7.0
```

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 : firewall
Confidence level : 70
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/2000

```
Port 2000/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8000

```
Port 8000/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8008

```
Port 8008/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8020

```
Port 8020/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.

- The ping round trip time

- Whether credentialed or third-party patch management checks are possible.

- Whether the display of superseded patches is enabled

- 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: 2021/01/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.14.0
Plugin feed version : 202106121427
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : rubber kin
Scanner IP : 192.168.58.131
Port scanner(s) : nessus_syn_scanner
Port range : 0-65535
```

```
Ping RTT : Unavailable
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
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/7/2 2:10 EDT
Scan duration : 3825 sec
```

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: 2021/05/12

Plugin Output

tcp/0

```
Remote operating system : CISCO PIX 7.0
Confidence level : 70
Method : SinFP


The remote host is running CISCO PIX 7.0
```

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: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.58.131 to 30.90.90.218 :
192.168.58.131
192.168.58.2
30.90.90.218

Hop Count: 2
```

30.90.90.219

0	0	0	0	8
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Jul 2 02:10:04 2021
End time: Fri Jul 2 03:14:25 2021

Host Information

IP: 30.90.90.219
OS: CISCO PIX 7.0

Vulnerabilities

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, Modified: 2021/06/03

Plugin Output

tcp/0

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

  cpe:/o:cisco:pix_firewall:7.0
```

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 : firewall
Confidence level : 70
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/110

```
Port 110/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8008

```
Port 8008/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8020

```
Port 8020/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.

- The ping round trip time

- Whether credentialed or third-party patch management checks are possible.

- Whether the display of superseded patches is enabled

- 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: 2021/01/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.14.0
Plugin feed version : 202106121427
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : rubber kin
Scanner IP : 192.168.58.131
Port scanner(s) : nessus_syn_scanner
Port range : 0-65535
```

```
Ping RTT : Unavailable
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
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/7/2 2:10 EDT
Scan duration : 3860 sec
```

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: 2021/05/12

Plugin Output

tcp/0

```
Remote operating system : CISCO PIX 7.0
Confidence level : 70
Method : SinFP


The remote host is running CISCO PIX 7.0
```

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: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.58.131 to 30.90.90.219 :
192.168.58.131
192.168.58.2
?
30.90.90.219

Hop Count: 3
```

30.90.90.221

0	1	0	0	19
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Jul 2 02:10:04 2021

End time: Fri Jul 2 02:12:52 2021

Host Information

Netbios Name: NPIC39933

IP: 30.90.90.221

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 v2.0 Base Score

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

CVSS v2.0 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/snmp

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

public
```

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 1 open TCP ports and 13 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

udp/123

```
Port 123/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/137/netbios-ns

```
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

udp/427

```
Port 427/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/1022

```
Port 1022/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/1023

```
Port 1023/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/5353

```
Port 5353/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/8291

```
Port 8291/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/35441

```
Port 35441/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/39445

```
Port 39445/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/43299

```
Port 43299/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/46101

```
Port 46101/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/55183

```
Port 55183/udp 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.

- The ping round trip time

- Whether credentialed or third-party patch management checks are possible.

- Whether the display of superseded patches is enabled

- 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: 2021/01/27

Plugin Output

tcp/0

```
 Information about this scan :

 Nessus version : 8.14.0
 Plugin feed version : 202106121427
 Scanner edition used : Nessus
 Scan type : Normal
 Scan policy used : rubber kin
 Scanner IP : 192.168.58.131
 Port scanner(s) : snmp_scanner
 Port range : 0-65535
```

```
Ping RTT : Unavailable
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
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/7/2 2:10 EDT
Scan duration : 167 sec
```

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/snmp

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

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: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.58.131 to 30.90.90.221 :
192.168.58.131
192.168.58.2
?

Hop Count: 2
```

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: 2021/02/10

Plugin Output

udp/137/netbios-ns

```
The following 2 NetBIOS names have been gathered :

 NPIC39933       = Computer name
 WORKGROUP       = Workgroup / Domain name

This SMB server seems to be a Samba server - its MAC address is NULL.
```

30.90.90.222

0	1	0	0	17
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Jul 2 02:10:04 2021
End time: Fri Jul 2 03:12:52 2021

Host Information

IP: 30.90.90.222
OS: CISCO PIX 7.0

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 v2.0 Base Score

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

CVSS v2.0 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/snmp

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

public
```

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, Modified: 2021/06/03

Plugin Output

tcp/0

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

  cpe:/o:cisco:pix_firewall:7.0
```

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 : firewall
Confidence level : 70
```

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 0 open TCP ports and 6 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

udp/69

```
Port 69/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/123

```
Port 123/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/161/snmp

```
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

udp/3000

```
Port 3000/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/8021

```
Port 8021/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/8022

```
Port 8022/udp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/80

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8008

```
Port 8008/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.

- The ping round trip time

- Whether credentialed or third-party patch management checks are possible.

- Whether the display of superseded patches is enabled

- 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: 2021/01/27

Plugin Output

tcp/0

```
 Information about this scan :

 Nessus version : 8.14.0
 Plugin feed version : 202106121427
 Scanner edition used : Nessus
 Scan type : Normal
 Scan policy used : rubber kin
 Scanner IP : 192.168.58.131
 Port scanner(s) : nessus_syn_scanner
 Port range : 0-65535
```

```
Ping RTT : Unavailable
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
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/7/2 2:10 EDT
Scan duration : 3762 sec
```

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: 2021/05/12

Plugin Output

tcp/0

```
Remote operating system : CISCO PIX 7.0
Confidence level : 70
Method : SinFP


The remote host is running CISCO PIX 7.0
```

10919 - Open Port Re-check

Synopsis

Previously open ports are now closed.

Description

One of several ports that were previously open are now closed or unresponsive.

There are several possible reasons for this :

- The scan may have caused a service to freeze or stop running.

- An administrator may have stopped a particular service during the scanning process.

This might be an availability problem related to the following :

- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.

- This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.

- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again.

Solution

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF   IAVB:0001-B-0509

Plugin Information

Published: 2002/03/19, Modified: 2020/09/22

Plugin Output

tcp/0

```
  Port 80 was detected as being open initialy but was found unresponsive later.
```

```
  It is now closed
Port 8008 was detected as being open but is now closed
```

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: 2019/11/22

Plugin Output

udp/161/snmp

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

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/snmp

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

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: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.58.131 to 30.90.90.222 :
192.168.58.131
192.168.58.2
?
30.90.90.222

Hop Count: 3
```

30.90.90.250

0	0	0	0	8
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Jul 2 02:10:04 2021
End time: Fri Jul 2 03:13:50 2021

Host Information

IP: 30.90.90.250
OS: CISCO PIX 7.0

Vulnerabilities

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, Modified: 2021/06/03

Plugin Output

tcp/0

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

  cpe:/o:cisco:pix_firewall:7.0
```

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 : firewall
Confidence level : 70
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/21

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/80

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/2000

```
Port 2000/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.

- The ping round trip time

- Whether credentialed or third-party patch management checks are possible.

- Whether the display of superseded patches is enabled

- 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: 2021/01/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.14.0
Plugin feed version : 202106121427
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : rubber kin
Scanner IP : 192.168.58.131
Port scanner(s) : nessus_syn_scanner
Port range : 0-65535
```

```
Ping RTT : Unavailable
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
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/7/2 2:10 EDT
Scan duration : 3825 sec
```

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: 2021/05/12

Plugin Output

tcp/0

```
Remote operating system : CISCO PIX 7.0
Confidence level : 70
Method : SinFP


The remote host is running CISCO PIX 7.0
```

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: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.58.131 to 30.90.90.250 :
192.168.58.131
192.168.58.2
30.90.90.250

Hop Count: 2
```

30.90.90.252

0	0	0	0	19
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Jul 2 02:10:04 2021
End time: Fri Jul 2 03:20:59 2021

Host Information

IP: 30.90.90.252

Vulnerabilities

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: 2019/11/22

Plugin Output

tcp/8008/www

```
Response Code : HTTP/1.1 302 Found

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

  Location: https://30.90.90.252:8010/
  Connection: close
  X-Frame-Options: SAMEORIGIN
  X-XSS-Protection: 1; mode=block
  X-Content-Type-Options: nosniff
  Content-Security-Policy: frame-ancestors 'self'

Response Body :
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/21

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/25

```
Port 25/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/80

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/110

```
Port 110/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/143

```
Port 143/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/443

```
Port 443/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/2000

```
Port 2000/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8008/www

```
Port 8008/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8010

```
Port 8010/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8013

```
Port 8013/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8015

```
Port 8015/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/8020

```
Port 8020/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/30197

```
Port 30197/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.

- The ping round trip time

- Whether credentialed or third-party patch management checks are possible.

- Whether the display of superseded patches is enabled

- 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: 2021/01/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.14.0
Plugin feed version : 202106121427
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : rubber kin
Scanner IP : 192.168.58.131
Port scanner(s) : nessus_syn_scanner
Port range : 0-65535
```

```
Ping RTT : Unavailable
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
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/7/2 2:10 EDT
Scan duration : 4253 sec
```

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: 2021/04/14

Plugin Output

tcp/8008/www

```
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: 2021/04/14

Plugin Output

tcp/8013

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

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: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.58.131 to 30.90.90.252 :
192.168.58.131
192.168.58.2
30.90.90.252

Hop Count: 2
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2020/06/12

Plugin Output

tcp/8008/www

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 302
rather than 404. The requested URL was :

    http://30.90.90.252:8008/dVYQQcP5hXqZ.html
```