My Basic Network Scan

Report generated by Tenable Nessus™ Thu, 25 Sep 2025 13:46:05 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Scan Information

Start time: Thu Sep 25 13:29:17 2025
End time: Thu Sep 25 13:46:05 2025

Host Information

DNS Name: Adarsh.lan
Netbios Name: ADARSH
IP:
OS: Windows 11

Vulnerabilities

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: 2022/10/05

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: 2025/06/16

Plugin Output

tcp/8089/www

```
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 : C=US/ST=CA/L=San Francisco/O=Splunk/CN=SplunkCommonCA/E=support@splunk.com
|-Issuer  : C=US/ST=CA/L=San Francisco/O=Splunk/CN=SplunkCommonCA/E=support@splunk.com
```

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: 2025/06/16

Plugin Output

tcp/8191

```
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=SplunkServerDefaultCert/O=SplunkUser
|-Issuer  : C=US/ST=CA/L=San Francisco/O=Splunk/CN=SplunkCommonCA/E=support@splunk.com
```

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: 2025/06/16

Plugin Output

tcp/8834/www

```
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 : O=Nessus Users United/OU=Nessus Server/L=New York/C=US/ST=NY/CN=Adarsh
|-Issuer  : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus
 Certification Authority
```

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/8089/www

```
The identities known by Nessus are :

  adarsh
[redacted]

The Common Name in the certificate is :

  SplunkServerDefaultCert
```

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/8191

```
The identities known by Nessus are :

  adarsh
[redacted]
The Common Name in the certificate is :

  SplunkServerDefaultCert
```

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 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: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/8089/www

```
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 : C=US/ST=CA/L=San Francisco/O=Splunk/CN=SplunkCommonCA/E=support@splunk.com
```

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also

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

Solution

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information

Published: 2010/04/29, Modified: 2022/08/15

Plugin Output

tcp/0

```
The following hostnames point to the remote host :
  - adarsh
```

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: 2025/07/14

Plugin Output

tcp/0

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

  cpe:/o:microsoft:windows -> Microsoft Windows

Following application CPE's matched on the remote system :

  cpe:/a:splunk:splunk:10.0.0 -> Splunk
  cpe:/a:tenable:nessus -> Tenable Nessus
```

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: 2021/10/04

Plugin Output

tcp/135/epmap

```
The following DCERPC services are available locally :

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 : Local RPC service
Named pipe : samss lpc

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 : Local RPC service
Named pipe : SidKey Local End Point

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 : Local RPC service
Named pipe : protected_storage

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 : Local RPC service
```

```
Named pipe : lsasspirpc

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 : Local RPC service
Named pipe : lsapolicylookup

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 : Local RPC service
Named pipe : LSA_EAS_ENDPOINT

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 : Local RPC service
Named pipe : LSA_IDPEXT_ENDPOINT

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 : Local RPC service
Named pipe : lsacap

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc  [...]
```

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: 2021/10/04

Plugin Output

tcp/445/cifs

```
The following DCERPC services are available remotely :

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 : \\ADARSH

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

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

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
```

```
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\ADARSH

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\ADARSH

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\ADARSH

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

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\ADARSH

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0 [...]
```

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: 2021/10/04

Plugin Output

tcp/49664/dce-rpc

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

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 : 49664
IP : [redacted]

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 : 49664
IP : [redacted]

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 : 49664
IP : [redacted]

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 : 49664
IP :
```

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: 2021/10/04

Plugin Output

tcp/49665/dce-rpc

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

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 : 49665
IP : [redacted]
```

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: 2021/10/04

Plugin Output

tcp/49668/dce-rpc

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

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 : 49668
IP [redacted]

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 : 49668
IP : [redacted]
```

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: 2021/10/04

Plugin Output

tcp/49669/dce-rpc

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

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Windows Event Log
Type : Remote RPC service
TCP Port : 49669
IP : [redacted]
```

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: 2021/10/04

Plugin Output

tcp/49670/dce-rpc

```
The following DCERPC services are available on TCP port 49670 :

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 : 49670
IP : [redacted]

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 : 49670
IP : [redacted]

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 : 49670
IP : [redacted]

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 : 49670
IP :

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 : 49670
IP :
```

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: 2021/10/04

Plugin Output

tcp/49680/dce-rpc

```
The following DCERPC services are available on TCP port 49680 :

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 : 49680
IP : [redacted]
```

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: 2025/03/12

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 70
```

19689 - Embedded Web Server Detection

Synopsis

The remote web server is embedded.

Description

The remote web server cannot host user-supplied CGIs. CGI scanning will be disabled on this server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/09/14, Modified: 2019/11/22

Plugin Output

tcp/8000/www

19689 - Embedded Web Server Detection

Synopsis

The remote web server is embedded.

Description

The remote web server cannot host user-supplied CGIs. CGI scanning will be disabled on this server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/09/14, Modified: 2019/11/22

Plugin Output

tcp/8089/www

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/8089/www

```
Based on the response to an OPTIONS request :

  - HTTP methods GET HEAD OPTIONS are allowed on :

    /
```

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/8000/www

```
The remote web server type is :

Splunkd
```

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/8089/www

```
The remote web server type is :

Splunkd
```

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/8834/www

```
The remote web server type is :

NessusWWW
```

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: 2025/03/13

Plugin Output

tcp/0

```
[redacted] resolves as Adarsh.lan.
```

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 is 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: 2024/02/26

Plugin Output

tcp/8834/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Cache-Control: must-revalidate
  X-Frame-Options: DENY
  Content-Type: text/html
  ETag: da1036a12aeb2433d28c5f447cb6123b
  Connection: close
  X-XSS-Protection: 1; mode=block
  Server: NessusWWW
  Date: Thu, 25 Sep 2025 08:01:03 GMT
  X-Content-Type-Options: nosniff
  Content-Length: 1217
  Content-Security-Policy: upgrade-insecure-requests; block-all-mixed-content; form-action 'self';
 frame-ancestors 'none'; frame-src https://store.tenable.com; default-src 'self'; connect-src
 'self' www.tenable.com; script-src 'self' www.tenable.com; img-src 'self' data:; style-src 'self'
 www.tenable.com; object-src 'none'; base-uri 'self';
  Strict-Transport-Security: max-age=31536000; includeSubDomains
  Expect-CT: max-age=0
```

```
Response Body :

<!doctype html>
<html lang="en">
    <head>
        <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
        <meta http-equiv="Content-Security-Policy" content="upgrade-insecure-requests; block-all-
mixed-content; form-action 'self'; frame-src https://store.tenable.com; default-src 'self'; connect-
src 'self' www.tenable.com; script-src 'self' www.tenable.com; img-src 'self' data:; style-src
 'self' www.tenable.com; object-src 'none'; base-uri 'self';" />
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <meta charset="utf-8" />
        <title>Nessus</title>
        <link rel="stylesheet" href="nessus6.css?v=1758317946667" id="theme-link" />
        <link rel="stylesheet" href="tenable_links.css?v=ac05d80f1e3731b79d12103cdf9367fc" />
        <link rel="stylesheet" href="wizard_templates.css?v=0e2ae10949ed6782467b3810ccce69c5" />
        <!--[if lt IE 11]>
            <script>
                window.location = '/unsupported6.html';
            </script>
        <![endif]-->
        <script src="nessus6.js?v=1758317946667"></script>
        <script src="p [...]
```

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 :

 ADARSH          = Computer name
 ADARSH          = 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 SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

```
Nessus was able to obtain the following information about the host, by
parsing the SMB2 Protocol's NTLM SSP message:

Target Name: ADARSH
NetBIOS Domain Name: ADARSH
NetBIOS Computer Name: ADARSH
DNS Domain Name: Adarsh
DNS Computer Name: Adarsh
DNS Tree Name: unknown
Product Version: 10.0.26100
```

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 :
  SMBv2
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

Plugin Output

tcp/445/cifs

```
The remote host supports the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
3.0        Windows 8
3.0.2      Windows 8.1
3.1.1      Windows 10

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

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: 2025/06/25

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.9.4
Nessus build : 20037
Plugin feed version : 202509250001
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : My Basic Network Scan
```

```
Scan policy used : Basic Network Scan
Scanner IP [redacted]
Ping RTT : Unavailable
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : 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 did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/9/25 13:29 India Standard Time (UTC +05:30)
Scan duration : 1005 sec
Scan for malware : no
```

10147 - Nessus Server Detection

Synopsis

A Nessus daemon is listening on the remote port.

Description

A Nessus daemon is listening on the remote port.

See Also

https://www.tenable.com/products/nessus/nessus-professional

Solution

Ensure that the remote Nessus installation has been authorized.

Risk Factor

None

References

XREF IAVT:0001-T-0673

Plugin Information

Published: 1999/10/12, Modified: 2023/02/08

Plugin Output

tcp/8834/www

```
URL     : https:/[redacted]:8834/
Version : unknown
```

64582 - Netstat Connection Information

Synopsis

Nessus was able to parse the results of the 'netstat' command on the remote host.

Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/13, Modified: 2023/05/23

Plugin Output

tcp/0

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/123

```
Port 123/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/135/epmap

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

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/137

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

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/138

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

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/139/smb

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

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/445/cifs

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

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/1900

```
Port 1900/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/5040

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

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/5050

```
Port 5050/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/5353

```
Port 5353/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/5355

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

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/8000/www

```
Port 8000/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/8089/www

```
Port 8089/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/8191

```
Port 8191/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/8834/www

```
Port 8834/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/49664/dce-rpc

```
Port 49664/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/49665/dce-rpc

```
Port 49665/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/49668/dce-rpc

```
Port 49668/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/49669/dce-rpc

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

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/49670/dce-rpc

```
Port 49670/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/49680/dce-rpc

```
Port 49680/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/50073

```
Port 50073/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/50393

```
Port 50393/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/50395

```
Port 50395/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/52672

```
Port 52672/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/60463

```
Port 60463/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/61795

```
Port 61795/udp was found to be open
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, “OS Identification”, the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

```
Following OS Fingerprints were found

Remote operating system : Windows 11
Confidence level : 70
Method : Misc
Type : general-purpose
Fingerprint : unknown

Following fingerprints could not be used to determine OS :
 HTTP:!:Server: Splunkd

SSLcert:!:i/CN:SplunkCommonCAi/O:Splunks/CN:SplunkServerDefaultCerts/O:SplunkUser
67065829440490db48444a1af09176e8eef80b83
i/CN:Nessus Certification Authorityi/O:Nessus Users Unitedi/OU:Nessus Certification Authoritys/
CN:Adarshs/O:Nessus Users Uniteds/OU:Nessus Server
15d857b6025cf404457356d6a711103ee3bfef40
```

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: 2025/06/03

Plugin Output

tcp/0

```
Remote operating system : Windows 11
Confidence level : 70
Method : Misc


The remote host is running Windows 11
```

97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)

Synopsis

Information about the remote host can be disclosed via an authenticated session.

Description

Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/05/30, Modified: 2025/02/11

Plugin Output

tcp/0

```
Nessus can run commands on localhost to check if patches are applied.

Credentialed checks of Windows are not supported using SSH.

The remote host is not currently supported by this plugin.

Runtime : 1.27623 seconds
```

117886 - OS Security Patch Assessment Not Available

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
The following issues were reported :

  - Plugin      : ssh_get_info2.nasl
    Plugin ID   : 97993
    Plugin Name : OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH
 Library)
    Protocol    : LOCALHOST
    Message     :
Credentialed checks of Windows are not supported using SSH.

  - 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.
```

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: 2025/06/16

Plugin Output

tcp/8089/www

```
This port supports 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: 2025/06/16

Plugin Output

tcp/8191

```
This port supports 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: 2025/06/16

Plugin Output

tcp/8834/www

```
This port supports TLSv1.3/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/8089/www

```
The host name known by Nessus is :

  adarsh

The Common Name in the certificate is :

  splunkserverdefaultcert
```

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/8191

```
The host name known by Nessus is :

  adarsh

The Common Name in the certificate is :

  splunkserverdefaultcert
```

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/8089/www

```
Subject Name:

Common Name: SplunkServerDefaultCert
Organization: SplunkUser

Issuer Name:

Country: US
State/Province: CA
Locality: San Francisco
Organization: Splunk
Common Name: SplunkCommonCA
Email Address: support@splunk.com

Serial Number: 44 97 BF D4 DF 7B 73 DE A5 00 D2 8D 82 F0 92 75 AD E5 58 E2

Version: 1

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jul 30 06:02:43 2025 GMT
Not Valid After: Jul 29 06:02:43 2028 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C6 03 5A F1 E9 E3 C6 63 A9 DA 2D 1C CF A3 19 61 72 66 BB
            C3 DD 6C 0D 35 0B 9F 2D 09 8D C4 DF 15 49 9B 59 5E F9 05 51
            2C 3C 57 85 EE 7E 65 F7 13 48 38 B0 04 DB F2 84 3F 22 97 51
            69 1E 21 A4 77 4B 28 99 83 0A DE 98 B8 B4 1B D0 72 0B 2F FD
            92 13 F9 7F EC F9 64 41 98 C4 85 54 F9 5B 6D 05 1C 60 0B BC
```

```
             8F 93 48 FB 90 8F 67 03 77 76 5E AA 95 67 99 1E FE 82 32 7B
             64 7B 2B 7E 0D 85 DF A2 C1 9B 1D A2 32 6E 1C B7 98 6E F0 C4
             06 AD 1C B0 3B 0B 2A DC D0 D9 AD FE 71 1D 0A 35 C7 21 16 8D
             8D 30 0B 93 E9 56 C9 4A 8B CE 7C 6D EA F1 69 D2 91 6E 21 A6
             F6 F9 31 C2 E2 46 77 00 E2 16 7D BA 14 1A 4F 24 EE 2D B1 5C
             62 41 6E BC D4 22 5C E7 08 10 22 5A A2 42 65 17 12 71 32 EB
             96 3F 95 39 3F 43 AB F7 1D 84 62 3E AF EA 07 9C B7 BC 34 CF
             9E 8B 59 C5 5A A3 3C 90 D9 D1 28 96 BA B0 F8 C2 2F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 B2 06 3D F7 34 2E D2 04 49 4F FD 0E BC 2A 5E B8 C2 BD 70
           A2 47 0B 54 AE 39 06 97 79 1B 37 90 A0 DD 4D 0C F1 80 19 39
           00 E9 F6 57 D3 5A A6 F2 37 1A BF 49 9E BD DA 19 9C D3 08 68
           F7 23 DC F1 97 5C 4F 66 30 56 C4 44 4A E9 AF E7 17 70 39 AA
           DB D9 1E 92 FA A5 6B EC 56 C7 BF FD 12 8D 5B 62 BB C4 3D 70
           0D EA D2 C6 5A F6 C3 D5 FC C1 0D 00 32 F3 49 C9 75 2E 1B 38
           1E AA 57 07 2A EC 5E 21 50 ED 60 2D 40 50 8B 39 74 76 7A BD
           43 4B 49 [...]
```

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/8191

```
Subject Name:

Common Name: SplunkServerDefaultCert
Organization: SplunkUser

Issuer Name:

Country: US
State/Province: CA
Locality: San Francisco
Organization: Splunk
Common Name: SplunkCommonCA
Email Address: support@splunk.com

Serial Number: 36 DB B1 DC 00 78 1A 96 54 07 4C 63 CB BF F1 F7 B4 E8 FE 27

Version: 1

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jul 29 03:43:20 2025 GMT
Not Valid After: Jul 28 03:43:20 2028 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 D9 A0 6D 6B 6E D8 DE FD E6 F7 7A E6 5B 32 F4 35 4C 21 CD
            76 54 D8 48 14 31 AA 6E 53 0D 06 D1 7F 6F 71 8F 9D 72 2C 28
            9C E7 03 9A 22 D3 3B F6 D4 B3 7D 02 A4 F5 D3 9B FA F3 60 34
            5E E6 7C D1 82 D1 C8 1D 24 68 02 2C 5F 7A E6 30 24 8F 6C CE
            69 19 CA D4 E1 B0 DD C7 07 83 9A FA 40 2E A1 69 C1 B9 DE F0
```

```
             3B C8 C5 E0 FC 47 5F EF E3 94 64 23 4F F5 8A 45 DA A5 15 9F
             27 DC 73 58 47 1E BB 44 21 07 CC 99 D8 4F D4 E6 05 9A 58 A2
             26 6B 4B 6D 26 0A 5F 35 C8 D8 18 52 A1 BC 73 4C 4B 0E 1F 76
             4B 4C 5F 4E E2 EC 09 A0 06 FA 1E 47 99 E1 CF 99 33 58 C3 17
             B0 BD EE 17 3A 67 F6 AA C7 8A 6D 97 31 CA 6A EA 10 EA 74 52
             4B 20 D9 E0 A7 AB 1A 97 88 00 E1 A4 AF 5F CE A5 CF B0 F4 AE
             39 40 09 68 F6 60 46 36 33 F1 75 0D 61 F2 5F F3 5D 90 A0 BC
             76 4A FB 4E 59 33 44 6D 77 43 BE CE E4 5E 99 A8 69
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 A3 DD 08 AC BB 85 96 83 59 73 08 0C 00 EB 25 B7 D7 7A B8
           CD 75 5A F3 D4 42 58 F3 CB 58 85 A7 DF 48 7B 39 ED B3 3F 89
           3B E2 85 D7 5D 45 3B CE FD 6C E5 6A 9D AD 9C 3B 1D 3E FE E1
           92 3C B4 BA 15 EE 32 BB 7E 7C C8 D7 E2 2E 43 65 6A 16 4B 99
           46 AB D9 53 94 89 30 5C 9D 15 A4 E7 CD C5 25 CF 58 84 A1 5E
           E1 80 D4 CC 8D CA 10 78 40 AD B5 FD 0D 4B A5 45 1C B2 DD B2
           A6 0A A8 E5 A9 93 DF 51 23 5C 02 85 33 93 70 36 0B 2F 70 B2
           EC 12 A7 [...]
```

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/8834/www

```
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: Adarsh

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 EB 04

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Sep 25 07:03:50 2025 GMT
Not Valid After: Sep 24 07:03:50 2029 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E4 0A FF 8E 94 F8 56 6F 59 D9 B4 FC 82 C5 65 F7 A0 5C 3D
```

```
             E2 BF F0 F3 60 62 BA 7F 43 9F 9C 23 CF D2 14 A7 8A 99 91 40
             B5 60 EF 31 51 A3 3F BB 93 85 23 04 30 04 84 08 2F 2A 14 AD
             E5 3E 8A 36 68 BD 3D 7C E9 4A 2B F0 02 2F 53 DE 73 B0 4C 2C
             89 23 D0 98 41 21 16 6C 8E 51 2B 3D C2 AE 2B A0 EA 24 3E 16
             FC 57 C5 DE 3F 14 3D D6 25 04 62 C8 01 0B 0F 09 18 F3 9D 45
             76 5B 6B 12 43 F1 C6 F1 40 D6 AC EB 3E B2 63 66 4E 96 1E 49
             04 6F 32 9A 26 13 D8 C0 E4 51 84 76 06 DD 8D E9 86 91 2B FB
             31 5F 4A 68 55 A4 AE 7F D7 D5 69 C4 46 09 4D B3 A0 DA 1B DD
             82 76 DB 9E 8F 4E 86 3C 2D 22 85 1C 4F 17 CA 84 B6 35 E2 DE
             AB EA E0 B3 B3 92 6E 24 36 D9 52 86 71 16 F5 07 38 42 37 10
             B9 23 99 36 E8 0B 4B F8 C1 34 BE C8 2F 62 27 1B E3 9A 8B 1E
             80 9A 48 90 39 A5 D1 DE AA F7 61 90 2A D6 4D 45 97
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 0E 13 53 81 93 FE DB 27 78 FD 7F 5B 5C D6 1A 61 C5 57 89
           A2 E3 41 FF B7 5E 1D 5E 96 31 93 A9 E5 2B 84 57 77 DD CB C1
           5E F4 62 2E 45 9A 9E 6C 67 85 AE A1 A3 E7 0F 20 75 1A 36 D2
           63 98 0E 8E D9 C1 F8 BA 11 21 DA CB 06 5E 2A 00 0E 71 9D 71
           39 E4 0A 72 D3 C5 B1 85 58 AE 91 FB 2D 0D CA A7 3E 44 93 46
           3F E9 98 39 A6 D7 7B 1F 64 74 7B DB BC F2 83 52 FC 24 80 A6
           AF 2B BC CB DC C [...]
```

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/8089/www

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth      Encryption             MAC
    ----------------------        ----------        ---           ----      ---------------------  ---
    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

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/8191

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ----------------------  ---
    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/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/8089/www

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

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                         Code              KEX           Auth     Encryption             MAC
    ----------------------       ----------        ---           ----     --------------------   ---
    ECDHE-RSA-AES128-SHA256      0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384      0xC0, 0x30        ECDH          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
    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
```

```
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/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/8191

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

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                         Code              KEX           Auth     Encryption             MAC
    ----------------------       ----------        ---           ----     --------------------   ---
    ECDHE-RSA-AES128-SHA256      0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384      0xC0, 0x30        ECDH          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
    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/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/8834/www

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

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    TLS_AES_128_GCM_SHA256        0x13, 0x01        -             -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02        -             -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03        -             -        ChaCha20-Poly1305(256)
 AEAD


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
```

```
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(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}
```

62563 - SSL Compression Methods Supported

Synopsis

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

Description

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

See Also

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

https://tools.ietf.org/html/rfc3749

https://tools.ietf.org/html/rfc3943

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/10/16, Modified: 2022/04/11

Plugin Output

tcp/8089/www

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

  DEFLATE (0x01)
```

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/8089/www

```
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
    ----------------------        ----------        ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA      AES-GCM(256)
 SHA384
    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/8191

```
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
    ----------------------        ----------        ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA      AES-GCM(256)
 SHA384
    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/8834/www

```
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
    ----------------------        ----------        ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA      AES-GCM(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}
```

35297 - SSL Service Requests Client Certificate

Synopsis

The remote service requests an SSL client certificate.

Description

The remote service encrypts communications using SSL/TLS, requests a client certificate, and may require a valid certificate in order to establish a connection to the underlying service.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/01/06, Modified: 2022/04/11

Plugin Output

tcp/8191

```
A TLSv12 server is listening on this port that requests a client certificate.
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/8089/www

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  High Strength Ciphers (>= 112-bit key)

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

The fields above are :

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

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/8191

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  High Strength Ciphers (>= 112-bit key)

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

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: 2024/03/26

Plugin Output

tcp/8000/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: 2024/03/26

Plugin Output

tcp/8089/www

```
A TLSv1.2 server answered on this port.
```

tcp/8089/www

```
A web server is running on this port through TLSv1.2.
```

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: 2024/03/26

Plugin Output

tcp/8191

```
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: 2024/03/26

Plugin Output

tcp/8834/www

```
A TLSv1.2 server answered on this port.
```

tcp/8834/www

```
A web server is running on this port through TLSv1.2.
```

49069 - Splunk Management API Detection

Synopsis

An infrastructure monitoring tool is running on the remote host.

Description

The remote web server is an instance of the Splunk management API.
Splunk is a search, monitoring, and reporting tool for system administrators.

See Also

https://www.splunk.com/en_us/software.html
http://dev.splunk.com/restapi
http://www.nessus.org/u?3aa0f4e2
https://www.splunk.com/en_us/download/universal-forwarder.html

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

References

XREF IAVT:0001-T-0722

Plugin Information

Published: 2010/09/01, Modified: 2022/10/12

Plugin Output

tcp/8089/www

```
URL            : https:/[redacted]:8089/
Version        : 10.0.0
Build          : e8eb0c4654f8
Management API : 1
```

47619 - Splunk Web Detection

Synopsis

An infrastructure monitoring tool is running on the remote host.

Description

The web interface for Splunk is running on the remote host. Splunk is a search, monitoring, and reporting tool for system administrators.

Note that HTTP Basic Authentication credentials may be required to retrieve version information for some recent Splunk releases.

See Also

https://www.splunk.com/en_us/software.html

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0723

Plugin Information

Published: 2010/07/07, Modified: 2025/04/02

Plugin Output

tcp/8000/www

```
URL           : http:[redacted]:8000/
Version       : 10.0.0
License       : Enterprise
Web interface : 1
```

42822 - Strict Transport Security (STS) Detection

Synopsis

The remote web server implements Strict Transport Security.

Description

The remote web server implements Strict Transport Security (STS).

The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.

All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

See Also

http://www.nessus.org/u?2fb3aca6

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/11/16, Modified: 2019/11/22

Plugin Output

tcp/8834/www

```
The STS header line is :

Strict-Transport-Security: max-age=31536000; includeSubDomains
```

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/8089/www

```
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/8191

```
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/8834/www

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

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

https://tools.ietf.org/html/rfc8446

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/8834/www

```
TLSv1.3 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: 2024/04/19

Plugin Output

tcp/0

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

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: 2025/07/21

Plugin Output

tcp/445/cifs

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

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/8000/www

```
The following cookie is expired :

Name : session_id_8000
Path : /
Value : f5d91c7b6568e109e44f1315fea9666cefa767ee
Domain :
Version : 1
Expires : Thu, 25 Sep 2025 09:00:38 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/8089/www

```
The following cookie is expired :

Name : session_id_8000
Path : /
Value : f5d91c7b6568e109e44f1315fea9666cefa767ee
Domain :
Version : 1
Expires : Thu, 25 Sep 2025 09:00:38 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/8834/www

```
The following cookie is expired :

Name : session_id_8000
Path : /
Value : f5d91c7b6568e109e44f1315fea9666cefa767ee
Domain :
Version : 1
Expires : Thu, 25 Sep 2025 09:00:38 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

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 :

 ADARSH           = Computer name
 ADARSH           = Workgroup / Domain name
```