Win2022_KrishanHimesh

Report generated by Nessus™ Mon, 22 Apr 2024 16:50:02 AEST

TABLE OF CONTENTS

Vulnerabilities by Plugin

Vulnerabilities by Plugin

42873 (1) - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

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

Description

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

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

See Also

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

https://sweet32.info

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

6.1

CVSS v2.0 Base Score

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

References

CVE	CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

192.168.56.50 (tcp/3389/msrdp)

```

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

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

The fields above are :

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

10061 (2) - Echo Service Detection

Synopsis

An echo service is running on the remote host.

Description

The remote host is running the 'echo' service. This service echoes any data which is sent to it.

This service is unused these days, so it is strongly advised that you disable it, as it may be used by attackers to set up denial of services attacks against this host.

Solution

Below are some examples of how to disable the echo service on some common platforms, however many services can exhibit this behavior and the list below is not exhaustive.

Consult vendor documentation for the service exhibiting the echo behavior for more information.

- Under Unix systems, comment out the 'echo' line in /etc/inetd.conf and restart the inetd process.

- Under Ubuntu systems, comment out the 'echo' line in /etc/systemd/system.conf and retart the systemd service.

- Under Windows systems, set the following registry key to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpEcho HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpEcho

Then launch cmd.exe and type :

net stop simptcp net start simptcp

To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

4.4

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0103
CVE	CVE-1999-0635

Plugin Information

Published: 1999/06/22, Modified: 2020/06/12

Plugin Output

```
192.168.56.50 (tcp/7/echo)
192.168.56.50 (udp/7)
```

10198 (2) - Quote of the Day (QOTD) Service Detection

Synopsis

The quote service (qotd) is running on this host.

Description

A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote.

Another quote of the day service is defined as a datagram based application on UDP. A server listens for UDP datagrams on UDP port 17.

When a datagram is received, an answering datagram is sent containing a quote (the data in the received datagram is ignored).

An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Solution

- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd Then launch cmd.exe and type :

net stop simptcp net start simptcp To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

4.4

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0103

Plugin Information

Published: 1999/11/30, Modified: 2019/10/04

Plugin Output

192.168.56.50 (tcp/17/qotd)
192.168.56.50 (udp/17/qotd)

51192 (2) - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

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

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

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

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

See Also

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

192.168.56.50 (tcp/3389/msrdp)

```

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

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

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

10043 (1) - Chargen UDP Service Remote DoS

Synopsis

The remote host is running a 'chargen' service.

Description

When contacted, chargen responds with some random characters (something like all the characters in the alphabet in a row). When contacted via UDP, it will respond with a single UDP packet. When contacted via TCP, it will continue spewing characters until the client closes the connection.

The purpose of this service was to mostly test the TCP/IP protocol by itself, to make sure that all the packets were arriving at their destination unaltered. It is unused these days, so it is suggested you disable it, as an attacker may use it to set up an attack against this host, or against a third-party host using this host as a relay.

An easy attack is 'ping-pong' in which an attacker spoofs a packet between two machines running chargen. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

See Also

http://www.nessus.org/u?f0dbdf05

Solution

- Under Unix systems, comment out the 'chargen' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpChargen HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpChargen

Then launch cmd.exe and type :

net stop simptcp net start simptcp

To restart the service.

Risk Factor

Medium

VPR Score

4.4

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0103

Exploitable With

Metasploit (true)

Plugin Information

Published: 1999/11/29, Modified: 2020/06/12

Plugin Output

192.168.56.50 (udp/19)

57582 (1) - SSL Self-Signed Certificate

Synopsis

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

Description

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

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

Solution

Purchase or generate a proper 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

192.168.56.50 (tcp/3389/msrdp)

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

|-Subject : CN=dc
```

57608 (1) - 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

192.168.56.50 (tcp/445/cifs)

104743 (1) - TLS Version 1.0 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

192.168.56.50 (tcp/3389/msrdp)

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

157288 (1) - TLS Version 1.1 Protocol Deprecated

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

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

See Also

https://datatracker.ietf.org/doc/html/rfc8996

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2023/04/19

Plugin Output

192.168.56.50 (tcp/3389/msrdp)

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

11219 (22) - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

192.168.56.50 (tcp/7/echo)

```
Port 7/tcp was found to be open
```

192.168.56.50 (tcp/9/discard)

```
Port 9/tcp was found to be open
```

192.168.56.50 (tcp/13/daytime)

```
Port 13/tcp was found to be open
```

192.168.56.50 (tcp/17/qotd)

```
Port 17/tcp was found to be open
```

192.168.56.50 (tcp/19/chargen)

```
Port 19/tcp was found to be open
```

192.168.56.50 (tcp/135/epmap)

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

192.168.56.50 (tcp/139/smb)

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

192.168.56.50 (tcp/445/cifs)

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

192.168.56.50 (tcp/3389/msrdp)

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

192.168.56.50 (tcp/5357/www)

```
Port 5357/tcp was found to be open
```

192.168.56.50 (tcp/5985/www)

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

192.168.56.50 (tcp/8834/www)

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

192.168.56.50 (tcp/47001/www)

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

192.168.56.50 (tcp/49664/dce-rpc)

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

192.168.56.50 (tcp/49665/dce-rpc)

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

192.168.56.50 (tcp/49666/dce-rpc)

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

192.168.56.50 (tcp/49667/dce-rpc)

```
Port 49667/tcp was found to be open
```

192.168.56.50 (tcp/49668/dce-rpc)

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

192.168.56.50 (tcp/49669/dce-rpc)

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

192.168.56.50 (tcp/49673/dce-rpc)

```
Port 49673/tcp was found to be open
```

192.168.56.50 (tcp/49681/dce-rpc)

```
Port 49681/tcp was found to be open
```

192.168.56.50 (tcp/49807/dce-rpc)

```
Port 49807/tcp was found to be open
```

10736 (10) - 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

192.168.56.50 (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  [...]
```

192.168.56.50 (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 : \\DC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 29770a8f-829b-4158-90a2-78cd488501f7, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \pipe\SessEnvPublicRpc
Netbios name : \\DC

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 : \\DC

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 : \\DC

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 : \\DC

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 : \\DC

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 : \\DC

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 : \\DC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event 1 [...]
```

192.168.56.50 (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 : 192.168.56.50

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 : 192.168.56.50

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 : 192.168.56.50

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 : 192.168.56.50
```

192.168.56.50 (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 : 192.168.56.50
```

192.168.56.50 (tcp/49666/dce-rpc)

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

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.56.50
```

192.168.56.50 (tcp/49667/dce-rpc)

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

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 : 49667
IP : 192.168.56.50

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 : 49667
IP : 192.168.56.50
```

192.168.56.50 (tcp/49668/dce-rpc)

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

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

```
UUID : 29770a8f-829b-4158-90a2-78cd488501f7, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.56.50
```

192.168.56.50 (tcp/49669/dce-rpc)

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

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49669
IP : 192.168.56.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49669
IP : 192.168.56.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49669
IP : 192.168.56.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49669
IP : 192.168.56.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49669
IP : 192.168.56.50
```

192.168.56.50 (tcp/49673/dce-rpc)

```
The following DCERPC services are available on TCP port 49673 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1.0
Description : Unknown RPC service
Annotation : Remote Fw APIs
Type : Remote RPC service
TCP Port : 49673
IP : 192.168.56.50
```

192.168.56.50 (tcp/49681/dce-rpc)

```
The following DCERPC services are available on TCP port 49681 :

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 : 49681
IP : 192.168.56.50
```

22964 (7) - 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

192.168.56.50 (tcp/7/echo)

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

192.168.56.50 (tcp/19/chargen)

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

192.168.56.50 (tcp/5357/www)

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

192.168.56.50 (tcp/5985/www)

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

192.168.56.50 (tcp/8834/www)

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

192.168.56.50 (tcp/8834/www)

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

192.168.56.50 (tcp/47001/www)

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

10147 (4) - 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

192.168.56.50 (tcp/8834/www)

```
URL          : https://192.168.56.50:8834/
Version      : 10.7.2
NASL Version : 19.8.2
```

10107 (3) - 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

192.168.56.50 (tcp/5985/www)

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

192.168.56.50 (tcp/8834/www)

```
The remote web server type is :

NessusWWW
```

192.168.56.50 (tcp/47001/www)

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

24260 (3) - 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

192.168.56.50 (tcp/5985/www)

```

Response Code : HTTP/1.1 404 Not Found

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

  Content-Type: text/html; charset=us-ascii
  Server: Microsoft-HTTPAPI/2.0
  Date: Mon, 22 Apr 2024 06:31:51 GMT
  Connection: close
  Content-Length: 315

Response Body :

```

192.168.56.50 (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: 807b9e0aefe52094d4c4be50fd4230ff
  Connection: close
  X-XSS-Protection: 1; mode=block
  Server: NessusWWW
  Date: Mon, 22 Apr 2024 06:31:51 GMT
  X-Content-Type-Options: nosniff
  Content-Length: 1578
  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
  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=1711560262479" id="theme-link" />
        <link rel="stylesheet" href="tenable_links.css?v=d41d8cd98f00b204e9800998ecf8427e" />
        <link rel="stylesheet" href="wizard_templates.css?v=11939be86ca24a4dbbe8f9b85f95e140" />
        <!--[if lt IE 11]>
            <script>
                window.location = '/unsupported6.html';
            </script>
        <![endif]-->
        <script src="nessus6.js?v=1711560262479"></script>
        <script src="pendo-client.js"></s [...]
```

192.168.56.50 (tcp/47001/www)

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

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

  Content-Type: text/html; charset=us-ascii
  Server: Microsoft-HTTPAPI/2.0
  Date: Mon, 22 Apr 2024 06:31:51 GMT
  Connection: close
  Content-Length: 315
```

```
Response Body :
```

43111 (3) - 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

192.168.56.50 (tcp/5985/www)

```
Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD
    INDEX LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY
    OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /

  - Invalid/unknown HTTP methods are allowed on :

    /
```

192.168.56.50 (tcp/8834/www)

```
Based on tests of each method :

  - HTTP methods DELETE GET HEAD POST PUT are allowed on :

    /session

  - HTTP method GET is allowed on :

    /
```

192.168.56.50 (tcp/47001/www)

```
Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD
    INDEX LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY
    OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /

  - Invalid/unknown HTTP methods are allowed on :

    /
```

10052 (2) - Daytime Service Detection

Synopsis

A daytime service is running on the remote host.

Description

The remote host is running a 'daytime' service. This service is designed to give the local time of the day of this host to whoever connects to this port. The date format issued by this service may sometimes help an attacker to guess the operating system type of this host, or to set up timed authentication attacks against the remote host.

In addition, if the daytime service is running on a UDP port, an attacker may link it to the echo port of a third-party host using spoofing, thus creating a possible denial of service condition between this host and the third party.

Solution

- On Unix systems, comment out the 'daytime' line in /etc/inetd.conf and restart the inetd process.

- On Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDaytime HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpDaytime Next, launch cmd.exe and type :

net stop simptcp net start simptcp This will restart the service.

Risk Factor

None

Plugin Information

Published: 1999/06/22, Modified: 2014/05/09

Plugin Output

192.168.56.50 (tcp/13/daytime)
192.168.56.50 (udp/13/daytime)

10863 (2) - 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

192.168.56.50 (tcp/3389/msrdp)

```
Subject Name:

Common Name: dc

Issuer Name:

Common Name: dc

Serial Number: 72 7F CF 91 CE 10 3F 9F 41 5D C1 B0 4A B3 86 FC

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 02:54:16 2024 GMT
Not Valid After: Jul 29 02:54:16 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C6 69 DD 2F 07 47 B3 2F F8 80 DB 02 16 A7 D8 EF 76 DF BD
            B7 1A 0A CD 75 DA BC D1 E5 A3 E8 D2 62 64 F7 23 7C C7 EB 80
            2E 0A E7 69 29 FE B3 CE 37 69 54 A0 60 DD 99 1F 9E A0 15 87
            0A 25 34 41 AA EE 40 00 B8 A5 73 C6 EA 58 BF 9C 27 19 28 88
            8A 1C 32 B9 E0 A0 3B 52 E6 2A 5D A6 60 6B E9 48 ED B9 35 ED
            06 32 99 6F 27 66 71 25 1A FC 19 7C E4 5B 24 B4 91 A9 E6 09
            39 93 8F 07 4B F2 5A 38 64 7F DD E1 EC 94 1B BD FB 3D 88 6A
            83 A0 A8 E0 82 87 9B E7 90 A2 86 28 13 B0 04 28 42 67 97 D9
            A0 96 9C 83 02 04 8C C2 08 6F C5 6B 1B 8C 58 44 1F 52 43 FF
            2A D2 3D E8 34 DB DE C2 0F AE FB 6A 5A E0 D8 3D 54 5F F2 C1
            3D 47 8A 4F 2D 72 FF 2A E0 DC 75 25 8C 54 92 C8 BA F0 84 A0
            38 F3 28 08 60 28 53 66 A9 4C 71 9F F3 A1 A5 E3 13 A0 E3 C2
            D5 88 B9 4A 70 D2 D5 A8 F5 5D 54 37 1F 9A 23 35 01
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 B7 4A 33 5D B5 8A 92 B2 97 BA 57 06 81 19 C4 C0 E0 5D 2F
           5F 3B C3 39 2C 33 D0 61 FA 28 F0 4D 30 FE A1 43 38 7E A5 19
           9F 93 A6 17 EF 55 5C 0E CE 52 14 57 7D A3 BB 6A 45 17 56 F0
           C9 C9 A4 3C CE E5 FF 30 08 E4 01 E9 62 5B 80 86 9A E4 6F 36
           43 0F F5 44 27 F4 4C A8 89 D8 83 34 3A C5 D3 5A 95 81 FC F0
           F8 0F 30 C1 52 36 11 31 3F F6 42 B9 3A 0B 1B 52 BA B4 22 01
           A0 AD F8 F7 17 27 DC DF 15 25 12 C5 E9 CA 03 3B 82 1F 95 07
           D8 45 7F B0 B1 0E FE 4C EF AD 3E CC A5 1D B3 57 74 3B 66 2E
           53 D2 A7 1D 00 4E B0 3C D1 A1 B0 93 69 23 B8 EE 52 51 E0 39
           B3 5E 8D 48 B6 56 7D 87 73 0F CB C9 35 8D 3E [...]
```

192.168.56.50 (tcp/8834/www)

```
Subject Name:

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

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: 3C F7

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Apr 16 09:55:06 2024 GMT
Not Valid After: Apr 15 09:55:06 2028 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C8 C2 8D 6F C1 1B 24 02 CA 11 0D F5 3D 4F 16 8B 17 70 EA
            1E A9 2E 58 31 94 55 FD 1E D5 DD B4 86 1D C4 E0 29 93 3F 6A
            72 B3 50 95 5C B9 9F 65 13 13 09 AC 63 63 77 F7 E8 41 51 DE
            66 7C AA 96 A2 11 ED 3A 54 14 D8 D5 65 B7 74 A1 E9 AA 72 5E
            EA 71 7F 34 B5 8E 50 AF 0C 27 14 AB C9 47 9C F7 C4 52 FC D9
            A5 47 C9 BD 44 14 F3 04 1C 1A 90 9B 16 3C 93 5C D7 EB AF 95
            E6 24 D6 53 DE 0F 80 B5 E4 8A C1 5C B5 D3 ED 0D 7B C3 75 50
            42 D7 87 E9 CD 29 F9 87 46 60 A5 DB 96 FC E3 E3 3A CB 8A DD
            51 3A EB 8B 03 DE E5 9E 88 2B 83 D1 5C 26 37 16 D6 06 36 AB
            EC 4B F9 73 90 D4 DC 11 33 A1 83 88 D0 90 21 3F B4 45 74 B0
            BD 99 A3 25 B3 0C 6D 11 1D 98 D2 60 62 F9 F3 18 92 6A 40 40
            3C 96 A2 66 1E C3 B2 67 1A 7C AC 3A E2 09 08 ED D5 B5 C1 8C
            E9 67 CE FD CD 92 B1 AE 86 4B 5E E4 75 86 E4 63 D1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 87 57 26 09 74 50 CE 94 1E 19 54 7C 40 0C DB 19 1D 16 9A
           D2 0D 90 90 5E BC 05 B8 90 06 F2 7F 5C CA 00 D5 EF 7F 8A 76
```

```
             BD BF 46 05 95 A8 C3 74 37 35 A9 AA 1E E3 D1 7D 67 D3 A8 E5
             2D E2 D8 53 8A F7 89 DB CD 25 50 5B 31 50 60 82 0F E4 A3 69
             0E 64 CF A3 D8 AD 3A F0 95 7C 62 9B B0 D1 25 D6 02 1D 2B 34
             3B 42 7B A2 FF F6 F1 EF FF 50 20 4B 8C 34 97 A9 0B BD 2A 19
             03 65 F5 ED 98 CF 13 E9 [...]
```

11011 (2) - Microsoft Windows SMB Service Detection

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

192.168.56.50 (tcp/139/smb)

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

192.168.56.50 (tcp/445/cifs)

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

21643 (2) - 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: 2023/07/10

Plugin Output

192.168.56.50 (tcp/3389/msrdp)

```

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

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

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

  High Strength Ciphers (>= 112-bit key)

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

192.168.56.50 (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}
```

56984 (2) - 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: 2023/07/10

Plugin Output

192.168.56.50 (tcp/3389/msrdp)

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

192.168.56.50 (tcp/8834/www)

```
This port supports TLSv1.3/TLSv1.2.
```

57041 (2) - 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

192.168.56.50 (tcp/3389/msrdp)

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

  High Strength Ciphers (>= 112-bit key)

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

192.168.56.50 (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}
```

136318 (2) - 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

192.168.56.50 (tcp/3389/msrdp)

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

192.168.56.50 (tcp/8834/www)

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

10114 (1) - ICMP Timestamp Request Remote Date Disclosure

Synopsis

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

Description

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

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

Solution

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

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2023/04/27

Plugin Output

192.168.56.50 (icmp/0)

```
The ICMP timestamps seem to be in little endian format (not in network format)
The difference between the local and remote clocks is -1 seconds.
```

10150 (1) - 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

192.168.56.50 (udp/137/netbios-ns)

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

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

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

   08:00:27:d5:e2:40
```

10287 (1) - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

192.168.56.50 (udp/0)

```
For your information, here is the traceroute from 192.168.56.34 to 192.168.56.50 :
192.168.56.34
192.168.56.50

Hop Count: 1
```

10785 (1) - 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

192.168.56.50 (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: DC
NetBIOS Domain Name: DC
NetBIOS Computer Name: DC
DNS Domain Name: dc
DNS Computer Name: dc
DNS Tree Name: unknown
Product Version: 10.0.20348
```

10940 (1) - Remote Desktop Protocol Service Detection

Synopsis

The remote host has an remote desktop protocol service enabled.

Description

The Remote Desktop Protocol allows a user to remotely obtain a graphical login (and therefore act as a local user on the remote host).

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

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

Solution

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

Risk Factor

None

Plugin Information

Published: 2002/04/20, Modified: 2023/08/21

Plugin Output

192.168.56.50 (tcp/3389/msrdp)

11032 (1) - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

Solution

n/a

Risk Factor

None

References

XREF	OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2021/08/17

Plugin Output

192.168.56.50 (tcp/8834/www)

```
The following directories were discovered:
/session

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

11153 (1) - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'

request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2018/11/26

Plugin Output

192.168.56.50 (tcp/13/daytime)

```
Daytime is running on this port.
```

11367 (1) - Discard Service Detection

Synopsis

A discard service is running on the remote host.

Description

The remote host is running a 'discard' service. This service typically sets up a listening socket and will ignore all the data which it receives.

This service is unused these days, so it is advised that you disable it.

Solution

- Under Unix systems, comment out the 'discard' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry key to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDiscard Then launch cmd.exe and type :

net stop simptcp net start simptcp To restart the service.

Risk Factor

None

Plugin Information

Published: 2003/03/12, Modified: 2011/03/11

Plugin Output

192.168.56.50 (tcp/9/discard)

11936 (1) - 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: 2023/11/08

Plugin Output

192.168.56.50 (tcp/0)

```

Remote operating system : Microsoft Windows
Confidence level : 70
Method : HTTP


The remote host is running Microsoft Windows
```

14788 (1) - IP Protocols Scan

Synopsis

This plugin detects the protocols understood by the remote IP stack.

Description

This plugin detects the protocols understood by the remote IP stack.

See Also

http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/09/22, Modified: 2022/08/15

Plugin Output

192.168.56.50 (tcp/0)

```
The following IP protocols are accepted on this host:
1ICMP
2IGMP
6TCP
17UDP
50ESP
51AH
```

17975 (1) - Service Detection (GET request)

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0935

Plugin Information

Published: 2005/04/06, Modified: 2021/10/27

Plugin Output

192.168.56.50 (tcp/17/qotd)

```
qotd seems to be running on this port.
```

19506 (1) - 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: 2024/03/13

Plugin Output

192.168.56.50 (tcp/0)

```
Information about this scan :

Nessus version : 10.7.2
Nessus build : 20029
Plugin feed version : 202404212146
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : Win2022_KrishanHimesh
Scan policy used : Basic Network Scan
Scanner IP : 192.168.56.34
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Ping RTT : 132.649 ms
Thorough tests : yes
Experimental tests : 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 : enabled
Web application tests : enabled
Web app tests -  Test mode : all_pairs
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 10 minutes.
Web app tests -  Stop at first flaw : param
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 : 2024/4/22 16:24 AEST
Scan duration : 1493 sec
Scan for malware : no
```

22319 (1) - MSRPC Service Detection

Synopsis

A DCE/RPC server is listening on the remote host.

Description

The remote host is running a Windows RPC service. This service replies to the RPC Bind Request with a Bind Ack response.

However it is not possible to determine the uuid of this service.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/09/11, Modified: 2019/09/25

Plugin Output

192.168.56.50 (tcp/49807/dce-rpc)

25220 (1) - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

192.168.56.50 (tcp/0)

33139 (1) - WS-Management Server Detection

Synopsis

The remote web server is used for remote management.

Description

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

See Also

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

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

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

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

Plugin Output

192.168.56.50 (tcp/5985/www)

```

Here is some information about the WS-Management Server :

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

35716 (1) - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

192.168.56.50 (tcp/0)

```

The following card manufacturers were identified :

08:00:27:D5:E2:40 : PCS Systemtechnik GmbH
```

42822 (1) - 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

192.168.56.50 (tcp/8834/www)

```

The STS header line is :

Strict-Transport-Security: max-age=31536000

```

43815 (1) - NetBIOS Multiple IP Address Enumeration

Synopsis

The remote host is configured with multiple IP addresses.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

192.168.56.50 (udp/137/netbios-ns)

```

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

  - 192.168.56.50
  - 10.0.2.15
```

45590 (1) - 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: 2024/04/15

Plugin Output

192.168.56.50 (tcp/0)

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

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

Following application CPE matched on the remote system :

  cpe:/a:tenable:nessus:10.7.2 -> Tenable Nessus
```

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

Synopsis

The remote device supports LLMNR.

Description

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

See Also

http://www.nessus.org/u?51eae65d

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

Solution

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

Risk Factor

None

Plugin Information

Published: 2011/04/21, Modified: 2023/10/17

Plugin Output

192.168.56.50 (udp/5355/llmnr)

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

54615 (1) - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

192.168.56.50 (tcp/0)

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

64814 (1) - Terminal Services Use SSL/TLS

Synopsis

The remote Terminal Services use SSL/TLS.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/22, Modified: 2023/07/10

Plugin Output

192.168.56.50 (tcp/3389/msrdp)

```
Subject Name:

Common Name: dc

Issuer Name:

Common Name: dc

Serial Number: 72 7F CF 91 CE 10 3F 9F 41 5D C1 B0 4A B3 86 FC

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 02:54:16 2024 GMT
Not Valid After: Jul 29 02:54:16 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C6 69 DD 2F 07 47 B3 2F F8 80 DB 02 16 A7 D8 EF 76 DF BD
            B7 1A 0A CD 75 DA BC D1 E5 A3 E8 D2 62 64 F7 23 7C C7 EB 80
            2E 0A E7 69 29 FE B3 CE 37 69 54 A0 60 DD 99 1F 9E A0 15 87
            0A 25 34 41 AA EE 40 00 B8 A5 73 C6 EA 58 BF 9C 27 19 28 88
            8A 1C 32 B9 E0 A0 3B 52 E6 2A 5D A6 60 6B E9 48 ED B9 35 ED
            06 32 99 6F 27 66 71 25 1A FC 19 7C E4 5B 24 B4 91 A9 E6 09
            39 93 8F 07 4B F2 5A 38 64 7F DD E1 EC 94 1B BD FB 3D 88 6A
            83 A0 A8 E0 82 87 9B E7 90 A2 86 28 13 B0 04 28 42 67 97 D9
            A0 96 9C 83 02 04 8C C2 08 6F C5 6B 1B 8C 58 44 1F 52 43 FF
            2A D2 3D E8 34 DB DE C2 0F AE FB 6A 5A E0 D8 3D 54 5F F2 C1
            3D 47 8A 4F 2D 72 FF 2A E0 DC 75 25 8C 54 92 C8 BA F0 84 A0
            38 F3 28 08 60 28 53 66 A9 4C 71 9F F3 A1 A5 E3 13 A0 E3 C2
            D5 88 B9 4A 70 D2 D5 A8 F5 5D 54 37 1F 9A 23 35 01
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 B7 4A 33 5D B5 8A 92 B2 97 BA 57 06 81 19 C4 C0 E0 5D 2F
           5F 3B C3 39 2C 33 D0 61 FA 28 F0 4D 30 FE A1 43 38 7E A5 19
           9F 93 A6 17 EF 55 5C 0E CE 52 14 57 7D A3 BB 6A 45 17 56 F0
           C9 C9 A4 3C CE E5 FF 30 08 E4 01 E9 62 5B 80 86 9A E4 6F 36
           43 0F F5 44 27 F4 4C A8 89 D8 83 34 3A C5 D3 5A 95 81 FC F0
           F8 0F 30 C1 52 36 11 31 3F F6 42 B9 3A 0B 1B 52 BA B4 22 01
           A0 AD F8 F7 17 27 DC DF 15 25 12 C5 E9 CA 03 3B 82 1F 95 07
           D8 45 7F B0 B1 0E FE 4C EF AD 3E CC A5 1D B3 57 74 3B 66 2E
           53 D2 A7 1D 00 4E B0 3C D1 A1 B0 93 69 23 B8 EE 52 51 E0 39
           B3 5E 8D 48 B6 56 7D 87 73 0F CB C9 35 8D 3E [...]
```

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

Synopsis

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

Description

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

See Also

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

192.168.56.50 (tcp/3389/msrdp)

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

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

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    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}
```

86420 (1) - Ethernet MAC Addresses

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

192.168.56.50 (tcp/0)

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:D5:E2:40
```

91815 (1) - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

192.168.56.50 (tcp/8834/www)

```

The following sitemap was created from crawling linkable content on the target host :

  - https://192.168.56.50:8834/
  - https://192.168.56.50:8834/nessus6.css
  - https://192.168.56.50:8834/tenable_links.css
  - https://192.168.56.50:8834/wizard_templates.css

Attached is a copy of the sitemap file.
```

100871 (1) - 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

192.168.56.50 (tcp/445/cifs)

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

106716 (1) - 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

192.168.56.50 (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
```

110723 (1) - 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

192.168.56.50 (tcp/0)

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

117886 (1) - 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

192.168.56.50 (tcp/0)

```

The following issues were reported :

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

121010 (1) - TLS Version 1.1 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

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

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

See Also

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

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

Solution

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

Risk Factor

None

References

XREF	CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

192.168.56.50 (tcp/3389/msrdp)

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

135860 (1) - 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: 2024/04/15

Plugin Output

192.168.56.50 (tcp/445/cifs)

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

138330 (1) - 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

192.168.56.50 (tcp/8834/www)

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

156899 (1) - 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

192.168.56.50 (tcp/3389/msrdp)

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


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

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

  High Strength Ciphers (>= 112-bit key)

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