My Basic Network Scan

Report generated by Tenable Nessus™ Mon, 05 Aug 2024 14:47:10 BST

Vulnerabilities by Host

Vulnerabilities by Host

192.168.0.101

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	3	1	29

Scan Information

Start time: Mon Aug 5 14:37:59 2024
End time: Mon Aug 5 14:47:10 2024

Host Information

IP: 192.168.0.101
MAC Address: 04:03:12:2E:41:22
OS: Linux Kernel 2.6

Vulnerabilities

56983 - SIP Username Enumeration

Synopsis

The SIP server on the remote host allows the enumeration of users.

Description

The SIP server on the remote host appears to respond differently to registration requests for valid and invalid usernames. Using that fact, Nessus was able to enumerate some of the valid usernames.

See Also

https://tools.ietf.org/html/rfc3261

Solution

Configure the SIP server to respond identically to valid and invalid usernames. This can be done in Asterisk, for example, by setting 'alwaysauthreject=yes' in sip.conf.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2011/12/01, Modified: 2022/04/11

Plugin Output

udp/5060/sip

```
The remote SIP server has the following extensions that do not require authentication :

  100
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

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

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

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

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

See Also

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/443/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=CN/ST=ZJ/L=HZ/O=HIKVISION/OU=HZ/CN=hikvision.com
|-Issuer  : C=CN/ST=ZJ/L=HZ/O=HIKVISION/OU=HZ/CN=hikvision.com
```

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/443/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=CN/ST=ZJ/L=HZ/O=HIKVISION/OU=HZ/CN=hikvision.com
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

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

Description

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

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

Solution

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

Risk Factor

Low

VPR Score

4.2

EPSS Score

0.8808

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/05/03

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -3508 seconds.
```

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: 2024/07/31

Plugin Output

tcp/0

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

  cpe:/o:linux:linux_kernel -> Linux Kernel

Following application CPE's matched on the remote system :

  cpe:/a:jquery:jquery -> jQuery
  cpe:/a:jquery:jquery_ui:1.11.0 -> jQuery UI
```

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: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 65
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following card manufacturers were identified :

04:03:12:2E:41:22 : Hangzhou Hikvision Digital Technology Co.,Ltd.
```

86420 - Ethernet MAC Addresses

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 04:03:12:2E:41:22
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/443/www

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

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/443/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 : yes
Options allowed : (Not implemented)
Headers :

  Date: Mon, 05 Aug 2024 14:42:10 GMT
  X-Content-Type-Options: nosniff
  X-Frame-Options: SAMEORIGIN
  X-XSS-Protection: 1; mode=block
  ETag: "9da-a35-6626651f"
  Content-Length: 2613
  Content-Type: text/html
  Connection: keep-alive
  Keep-Alive: timeout=5, max=99
  Last-Modified: Mon, 22 Apr 2024 13:24:47 GMT

Response Body :

<!DOCTYPE html>
<html lang="en" ng-app="webApp">

<head>
```

```
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Cache-Control" content="no-cache, must-revalidate" />
<meta http-equiv="Expires" content="0" />
    <title></title>
    <!-- ##### -->
    <link type='text/css' href='doc/neutral/neutral.css' rel='stylesheet'>
    <!-- <link type='text/css' href='doc/thirdLib/colorPicker/colorpicker.css' rel='stylesheet'> -->
    </link>
</head>

<body>
    <div id="main" ui-view="main" style="height:100%;overflow-y:hidden;"></div>
    <script src="doc/thirdLib/angular/polyfill.min.js"></script>
    <script src="doc/thirdLib/jquery/jquery.min.js"></script>
    <script src="doc/thirdLib/jquery/jquery.qrcode.min.js"></script>
    <script src="doc/thirdLib/jquery/jquery.cookie.js"></script>
    <script src="doc/thirdLib/jquery/jquery-ui.min.js"></script>
    <script src="doc/thirdLib/angular/angular.min.js"></script>
    <script src="doc/thirdLib/timebar/timebar.js"></script>
    <script src="doc/thirdLib/dialog/layer/layer.js"></script>
    <script src="doc/thirdLib/multiVideo/jsVideoPlugin-1.0.0.min.js"></script>
    <script src="doc/thirdLib/layDate/laydate.js"></script>
    <script src="doc/thirdLib/laypage/layui.js"></script>
    <script src="doc/thirdLib/echarts.min.js"></script>
    <script src="doc/thirdLib/nicescroll/jquery.nicescroll.js"></script>
    <script src="doc/thirdLib/webUploader/ [...]
```

106658 - JQuery Detection

Synopsis

The web server on the remote host uses JQuery.

Description

Nessus was able to detect JQuery on the remote host.

See Also

https://jquery.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/07, Modified: 2024/02/08

Plugin Output

tcp/443/www

```
URL     : https://192.168.0.101/doc/thirdLib/jquery/jquery.min.js
Version : unknown
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/80

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/443/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/554

```
Port 554/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/6666

```
Port 6666/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/8000

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

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/07/17

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.1
Nessus build : 20004
Plugin feed version : 202408050932
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : My Basic Network Scan
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.0.104
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 150.467 ms
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 : no
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 : 2024/8/5 14:38 BST
Scan duration : 547 sec
Scan for malware : no
```

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: 2024/06/19

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP

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

SIP:!:YATE/5.5.0
SinFP:
   P1:B10113:F0x12:W64240:O0204ffff:M1460:
   P2:B10113:F0x12:W65160:O0204ffff0402080affffffff4445414401030305:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:191001_7_p=554
SSLcert:!:i/CN:hikvision.comi/O:HIKVISIONi/OU:HZs/CN:hikvision.coms/O:HIKVISIONs/OU:HZ
6ad4f07029591d13d1a804f27f788bd8a7ca0869



The remote host is running Linux Kernel 2.6
```

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: 2023/07/10

Plugin Output

tcp/443/www

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

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
Subject Name:

Country: CN
State/Province: ZJ
Locality: HZ
Organization: HIKVISION
Organization Unit: HZ
Common Name: hikvision.com

Issuer Name:

Country: CN
State/Province: ZJ
Locality: HZ
Organization: HIKVISION
Organization Unit: HZ
Common Name: hikvision.com

Serial Number: 00 8A B4 23 17 C6 2A 20 F1

Version: 1

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Dec 17 12:50:40 2019 GMT
Not Valid After: Dec 31 12:50:40 2037 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 F1 4E 0D 29 36 59 1C 90 D5 90 C0 02 22 EA 2D FA 5F 8C 06
```

```
             C9 64 C1 8C EA BF 84 12 6B A6 EC 1B A5 4C 5D 9C B7 C0 07 C0
             65 64 80 D2 4B 62 30 BB 04 29 36 CF 38 74 6A 39 70 2D AF 9D
             CC CE 5F C1 14 96 89 40 14 50 25 F9 DB 46 86 28 28 27 CF F1
             3C 0B BB 9F 15 C8 D4 4B 53 8F DF BA E7 84 66 20 93 27 60 90
             EB 20 60 3A 7F 6A FB 14 7E 5C C5 B8 C2 57 AA 74 F2 D5 9A A6
             84 98 54 44 4D 99 08 B3 3D 0E 01 91 CF 44 E7 38 91 E8 17 8A
             D7 43 F2 A5 32 A4 D3 61 09 76 12 26 02 1E 42 92 86 25 F5 41
             C1 A2 08 B6 C0 A6 13 13 42 C5 BC 23 9D 2D 69 4B 34 79 AE 11
             85 50 09 F9 CB 15 1D 71 D5 AA 34 3B 9C A1 CA FD 5A 35 D3 23
             61 2C 65 DE B2 2E 01 16 21 42 EF F8 BE A0 D3 A7 B4 88 85 2F
             80 6E 44 EA EB 3C 0E B6 E4 A2 5F 07 3F FC 26 2C 40 81 15 FA
             8D 65 BF BE DE BF 3D 0E 59 6E 14 37 4C D9 D0 BA B7
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 D7 B4 FB 17 00 A1 5F 06 2D D2 29 03 9C 1D 1C 70 40 6F CB
           46 03 11 BD 25 E8 2C 26 F0 E4 A7 0E A6 DE 3F 90 2D F8 13 A6
           04 56 31 69 14 C9 D8 72 0F DE FD B8 EE 57 F4 D3 6D B9 7B 90
           17 9D D2 36 41 48 CD 6E B1 B6 C3 04 FD 99 60 FC A7 28 1E 1D
           C0 61 89 85 9A 8F 04 12 2C 7F E4 63 07 24 EB 8D 12 E0 50 14
           39 F4 D5 5E 73 FD 7A 89 8A E1 78 85 6B BE F7 13 E4 1D 00 F4
           CB 26 7C A9 68 5D E1 D1 A9 95 60 17 40 22 FD EA B8 B3 88 CE
           D2 B3 0 [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/443/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-CAMELLIA-CBC-128    0xC0, 0x76        ECDH          RSA      Camellia-CBC(128)
 SHA256
    ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77        ECDH          RSA      Camellia-CBC(256)
 SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
 SHA1
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45        DH            RSA      Camellia-CBC(128)
 SHA1
```

```
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH           RSA      Camellia-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH         RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH         RSA      AES-CBC(256)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA          RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00, 0x35       RSA          RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA               0x00, 0x41       RSA          RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA               0x00, 0x84       RSA          RSA      Camellia-CBC(256)
SHA1
   DHE-RSA-AES128-SHA256         0x00, 0x67       DH           RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B       DH           RSA      AES-CBC(256)
SHA256
   DHE-RSA-CAMELLIA128-SHA256    0x00, 0xBE       DH           RSA      Camellia-CBC(128)
SHA256
   DHE-RSA-CAMELLIA256-SHA256    0x00, 0xC4       DH           RSA      Camellia-CBC(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH         RSA      AES-CBC(128)     [...]
```

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: 2023/07/10

Plugin Output

tcp/443/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
    ----------------------        ----------        ---           ----     ---------------------   ---
    DHE-RSA-AES-128-CCM-AEAD      0xC0, 0x9E        DH            RSA      AES-CCM(128)
 AEAD
```

```
   DHE-RSA-AES-128-CCM8-AEAD     0xC0, 0xA2       DH            RSA      AES-CCM8(128)
AEAD
   DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
SHA256
   DHE-RSA-AES-256-CCM-AEAD      0xC0, 0x9F       DH            RSA      AES-CCM(256)
AEAD
   DHE-RSA-AES-256-CCM8-AEAD     0xC0, 0xA3       DH            RSA      AES-CCM8(256)
AEAD
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
SHA384
   DHE-RSA-CHACHA20-POLY1305     0xCC, 0xAA       DH            RSA      ChaCha20-Poly1305(256)
SHA256
   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-CAMELLIA-CBC-128    0xC0, 0x76       ECDH          RSA      Camellia-CBC(128)
SHA256
   ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77       ECDH          RSA     [...]
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/443/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
    ----------------------        ----------        ---           ----      ---------------------  ---
    DHE-RSA-AES-128-CCM-AEAD      0xC0, 0x9E        DH            RSA       AES-CCM(128)
 AEAD
    DHE-RSA-AES-128-CCM8-AEAD     0xC0, 0xA2        DH            RSA       AES-CCM8(128)
 AEAD
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA       AES-GCM(128)
 SHA256
    DHE-RSA-AES-256-CCM-AEAD      0xC0, 0x9F        DH            RSA       AES-CCM(256)
 AEAD
    DHE-RSA-AES-256-CCM8-AEAD     0xC0, 0xA3        DH            RSA       AES-CCM8(256)
 AEAD
```

```
   DHE-RSA-AES256-SHA384         0x00, 0x9F      DH          RSA      AES-GCM(256)
SHA384
   DHE-RSA-CHACHA20-POLY1305     0xCC, 0xAA      DH          RSA      ChaCha20-Poly1305(256)
SHA256
   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-CAMELLIA-CBC-128    0xC0, 0x76      ECDH        RSA      Camellia-CBC(128)
SHA256
   ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77      ECDH        RSA      Camellia-CBC(256)
SHA384
   ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8      ECDH        RSA      ChaCha20-Poly1305(256)
SHA256
   DHE-RSA-AES128-SHA            0x00, 0x33      DH          RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39      DH          RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45      DH          RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88      DH          RSA      Camellia-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13      ECDH        RSA      AES-CBC(128) [...]
```

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/443/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
    ----------------------        ----------        ---           ----     --------------------    ---
    DHE-RSA-AES-128-CCM-AEAD      0xC0, 0x9E        DH            RSA      AES-CCM(128)
AEAD
    DHE-RSA-AES-128-CCM8-AEAD     0xC0, 0xA2        DH            RSA      AES-CCM8(128)
AEAD
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA      AES-GCM(128)
SHA256
    DHE-RSA-AES-256-CCM-AEAD      0xC0, 0x9F        DH            RSA      AES-CCM(256)
AEAD
    DHE-RSA-AES-256-CCM8-AEAD     0xC0, 0xA3        DH            RSA      AES-CCM8(256)
AEAD
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA      AES-GCM(256)
SHA384
    ECDHE-RSA-CAMELLIA-CBC-128    0xC0, 0x76        ECDH          RSA      Camellia-CBC(128)
SHA256
    ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77        ECDH          RSA      Camellia-CBC(256)
SHA384
    RSA-AES-128-CCM-AEAD          0xC0, 0x9C        RSA           RSA      AES-CCM(128)
AEAD
    RSA-AES-128-CCM8-AEAD         0xC0, 0xA0        RSA           RSA      AES-CCM8(128)
AEAD
    RSA-AES128-SHA256             0x00, 0x9C        RSA           RSA      AES-GCM(128)
SHA256
    RSA-AES-256-CCM-AEAD          0xC0, 0x9D        RSA           RSA      AES-CCM(256)
AEAD
    RSA-AES-256-CCM8-AEAD         0xC0, 0xA1        RSA           RSA      AES-CCM8(256)
AEAD
    RSA-AES256-SHA384             0x00, 0x9D        RSA           RSA      AES-GCM(256)
SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45        DH [...]
```

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/80

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/443/www

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

tcp/443/www

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

21642 - Session Initiation Protocol Detection

Synopsis

The remote system is a SIP signaling device.

Description

The remote system is running software that speaks the Session Initiation Protocol (SIP).

SIP is a messaging protocol to initiate communication sessions between systems. It is a protocol used mostly in IP Telephony networks / systems to setup, control, and teardown sessions between two or more systems.

See Also

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

Solution

If possible, filter incoming connections to the port so that it is used only by trusted sources.

Risk Factor

None

Plugin Information

Published: 2003/12/29, Modified: 2019/11/22

Plugin Output

udp/5060/sip

```
The remote service was identified as :

  YATE/5.5.0
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/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/443/www

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

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.0.104 to 192.168.0.101 :
192.168.0.104
192.168.0.101

Hop Count: 1
```

156439 - jQuery UI Detection

Synopsis

The web server on the remote host uses jQuery UI.

Description

The web server on the remote host uses jQuery UI.

See Also

https://releases.jquery.com/ui/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/12/31, Modified: 2023/05/24

Plugin Output

tcp/443/www

```
URL     : https://192.168.0.101/doc/thirdLib/jquery/jquery-ui.min.js
Version : 1.11.0
```