HackDome Advanced Scan

Report generated by Tenable Nessus™ Mon, 21 Apr 2025 17:46:38 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

3.148.28.190

0	0	0	0	31
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

DNS Name: ec2-3-148-28-190.us-east-2.compute.amazonaws.com

IP: 3.148.28.190

Vulnerabilities

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

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

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

See Also

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

Solution

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

www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following hostnames point to the remote host :
  - hackerdom.xyz
  - www.hackerdom.xyz
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

```
Give Nessus credentials to perform local checks.
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/04/15

Plugin Output

tcp/0

```
Following application CPE's matched on the remote system :

  cpe:/a:openbsd:openssh:9.2 -> OpenBSD OpenSSH
  cpe:/a:openbsd:openssh:9.2p1 -> OpenBSD OpenSSH
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2025/03/13

Plugin Output

tcp/0

```
3.148.28.190 resolves as ec2-3-148-28-190.us-east-2.compute.amazonaws.com.
```

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: 2025/02/12

Plugin Output

tcp/22/ssh

```
Port 22/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: 2025/02/12

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: 2025/02/12

Plugin Output

tcp/443/www

```
Port 443/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: 2024/12/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202504210921
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : HackDome Advanced Scan
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.122.129
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 47.392 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 : 256
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/4/21 17:39 EDT (UTC -04:00)
Scan duration : 430 sec
Scan for malware : no
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Following OS Fingerprints were found

Following fingerprints could not be used to determine OS :
 SSH:!:SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u5
HTTP:!:Server: Apache

SSLcert:!:i/CN:E5i/O:Let's Encrypts/CN:hackerdom.xyz
f044bdae205386c12da476740fbca20341cdd370

SinFP:!:
   P1:B11013:F0x12:W64240:O0204ffff:M1460:
   P2:B11013:F0x12:W64240:O0204ffff:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:191003_7_p=22R
```

50350 - OS Identification Failed

Synopsis

It was not possible to determine the remote operating system.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. Unfortunately, though, Nessus does not currently know how to use them to identify the overall system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2024/09/30

Plugin Output

tcp/0

```
If you think that these signatures would help us improve OS fingerprinting,
please submit them by visiting https://www.tenable.com/research/submitsignatures.

SSH:!:SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u5

SSLcert:!:i/CN:E5i/O:Let's Encrypts/CN:hackerdom.xyz
f044bdae205386c12da476740fbca20341cdd370

SinFP:!:
   P1:B11013:F0x12:W64240:O0204ffff:M1460:
   P2:B11013:F0x12:W64240:O0204ffff:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:191003_7_p=22R
```

181418 - OpenSSH Detection

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

https://www.openssh.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2025/04/18

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 9.2p1
Banner  : SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u5
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2025/01/20

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm(s) with the server :

  Client to Server: aes256-ctr
  Server to Client: aes256-ctr

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  rsa-sha2-256
  rsa-sha2-512
  ssh-ed25519
```

```
The server supports the following options for encryption_algorithms_client_to_server :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for kex_algorithms :

  curve25519-sha256
  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha256
  diffie-hellman-group16-sha512
  diffie-hellman-group18-sha512
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521
  kex-strict-s-v00@openssh.com
  sntrup761x25519-sha512
  sntrup761x25519-sha512@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com
```

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u5
SSH supported authentication : publickey
```

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.
```

83298 - SSL Certificate Chain Contains Certificates Expiring Soon

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Solution

Renew any soon to expire SSL certificates.

Risk Factor

None

Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

Plugin Output

tcp/443/www

```
The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject   : CN=hackerdom.xyz
|-Not After : May 23 03:38:22 2025 GMT
```

42981 - SSL Certificate Expiry - Future Expiry

Synopsis

The SSL certificate associated with the remote service will expire soon.

Description

The SSL certificate associated with the remote service will expire soon.

Solution

Purchase or generate a new SSL certificate in the near future to replace the existing one.

Risk Factor

None

Plugin Information

Published: 2009/12/02, Modified: 2020/09/04

Plugin Output

tcp/443/www

```
The SSL certificate will expire within 60 days, at
May 23 03:38:22 2025 GMT :

  Subject          : CN=hackerdom.xyz
  Issuer           : C=US, O=Let's Encrypt, CN=E5
  Not valid before : Feb 22 03:38:23 2025 GMT
  Not valid after  : May 23 03:38:22 2025 GMT
```

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:

Common Name: hackerdom.xyz

Issuer Name:

Country: US
Organization: Let's Encrypt
Common Name: E5

Serial Number: 04 0E EF AB 68 48 46 DE 6F 4A 27 2F C6 1F 23 06 E2 B0

Version: 3

Signature Algorithm: ECDSA With SHA-384

Not Valid Before: Feb 22 03:38:23 2025 GMT
Not Valid After: May 23 03:38:22 2025 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 02 1D 80 5A 0E D4 31 BC 34 86 45 E2 BD FD 8A 71 40 32 2B 6F
              95 B4 E1 69 FF 02 4E 23 87 00 2E AF
Public Key Y: 9E FC 87 84 F4 11 6D BF 5E AD 78 6B E2 EB B5 3E E3 DF 69 59
              2F 00 70 1B 21 18 07 23 C6 88 73 FE

Signature Length: 103 bytes / 824 bits
Signature: 00 30 65 02 31 00 FF F2 FD D9 EC AB 8C BB E2 CA 74 44 5F 8D
           C2 DD 60 B3 D7 0D C6 C5 FC 6A F5 54 7F 4A 9A 1D DD 35 AE 96
```

```
            BA 0C 59 8E 70 49 CD 6D 31 DB 2E 66 47 59 02 30 0E D9 06 5A
            F6 F1 EA DA 85 65 90 A5 23 E2 78 5E 27 4C CE 48 63 7F B7 DD
            41 D7 21 5A 76 83 E8 C6 60 BA 98 98 04 10 C3 84 FF 63 64 8B
            CB F9 46 EE

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature


Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)


Extension: Basic Constraints (2.5.29.19)
Critical: 1


Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 93 84 8B EC 87 0F 16 01 D0 59 7B EC 3C EF F3 5E 4C BD C2 93


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 9F 2B 5F CF 3C 21 4F 9D 04 B7 ED 2B 2C C4 C6 70 8B D2 D7 0D


Extension: Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical: 0
Method#1: Online Certificate Status Protocol
URI: http://e5.o.lencr.org
Method#2: Certificate Authority Issuers
URI: http://e5.i.lencr.org/


Extension: Subject Alternative Name (2.5.29.17)
Critical: 0
DNS: hackerdom.xyz
DNS: www.hackerdom.xyz


Extension: Policies (2.5.29.32)
Critical: 0
Policy ID #1: [...]
```

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-ECDSA-CAMELLIA-CBC-128  0xC0, 0x72        ECDH          ECDSA    Camellia-CBC(128)
 SHA256
    ECDHE-ECDSA-CAMELLIA-CBC-256  0xC0, 0x73        ECDH          ECDSA    Camellia-CBC(256)
 SHA384
    ECDHE-ECDSA-AES128-SHA        0xC0, 0x09        ECDH          ECDSA    AES-CBC(128)
 SHA1
    ECDHE-ECDSA-AES256-SHA        0xC0, 0x0A        ECDH          ECDSA    AES-CBC(256)
 SHA1
    ECDHE-ECDSA-AES128-SHA256     0xC0, 0x23        ECDH          ECDSA    AES-CBC(128)
 SHA256
```

```
    ECDHE-ECDSA-AES256-SHA384     0xC0, 0x24       ECDH          ECDSA    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}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/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
    ----------------------        ----------        ---           ----     ---------------------   ---
    ECDHE-ECDSA-AES-128-CCM-AEAD  0xC0, 0xAC        ECDH          ECDSA    AES-CCM(128)
 AEAD
```

```
   ECDHE-ECDSA-AES-128-CCM8-AEAD 0xC0, 0xAE       ECDH           ECDSA    AES-CCM8(128)
AEAD
   ECDHE-ECDSA-AES128-SHA256     0xC0, 0x2B       ECDH           ECDSA    AES-GCM(128)
SHA256
   ECDHE-ECDSA-AES-256-CCM-AEAD  0xC0, 0xAD       ECDH           ECDSA    AES-CCM(256)
AEAD
   ECDHE-ECDSA-AES-256-CCM8-AEAD 0xC0, 0xAF       ECDH           ECDSA    AES-CCM8(256)
AEAD
   ECDHE-ECDSA-AES256-SHA384     0xC0, 0x2C       ECDH           ECDSA    AES-GCM(256)
SHA384
   ECDHE-ECDSA-CAMELLIA-CBC-128  0xC0, 0x72       ECDH           ECDSA    Camellia-CBC(128)
SHA256
   ECDHE-ECDSA-CAMELLIA-CBC-256  0xC0, 0x73       ECDH           ECDSA    Camellia-CBC(256)
SHA384
   ECDHE-ECDSA-CHACHA20-POLY1305 0xCC, 0xA9       ECDH           ECDSA    ChaCha20-Poly1305(256)
SHA256
   ECDHE-ECDSA-AES128-SHA        0xC0, 0x09       ECDH           ECDSA    AES-CBC(128)
SHA1
   ECDHE-ECDSA-AES256-SHA        0xC0, 0x0A       ECDH           ECDSA     [...]
```

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
    ----------------------        ----------        ---           ----     ----------------------  ---
    ECDHE-ECDSA-AES-128-CCM-AEAD  0xC0, 0xAC        ECDH          ECDSA    AES-CCM(128)
 AEAD
    ECDHE-ECDSA-AES-128-CCM8-AEAD 0xC0, 0xAE        ECDH          ECDSA    AES-CCM8(128)
 AEAD
    ECDHE-ECDSA-AES128-SHA256     0xC0, 0x2B        ECDH          ECDSA    AES-GCM(128)
 SHA256
    ECDHE-ECDSA-AES-256-CCM-AEAD  0xC0, 0xAD        ECDH          ECDSA    AES-CCM(256)
 AEAD
    ECDHE-ECDSA-AES-256-CCM8-AEAD 0xC0, 0xAF        ECDH          ECDSA    AES-CCM8(256)
 AEAD
```

```
    ECDHE-ECDSA-AES256-SHA384     0xC0, 0x2C       ECDH           ECDSA    AES-GCM(256)
  SHA384
    ECDHE-ECDSA-CAMELLIA-CBC-128  0xC0, 0x72       ECDH           ECDSA    Camellia-CBC(128)
  SHA256
    ECDHE-ECDSA-CAMELLIA-CBC-256  0xC0, 0x73       ECDH           ECDSA    Camellia-CBC(256)
  SHA384
    ECDHE-ECDSA-CHACHA20-POLY1305 0xCC, 0xA9       ECDH           ECDSA    ChaCha20-Poly1305(256)
  SHA256
    ECDHE-ECDSA-AES128-SHA        0xC0, 0x09       ECDH           ECDSA    AES-CBC(128)
  SHA1
    ECDHE-ECDSA-AES256-SHA        0xC0, 0x0A       ECDH           ECDSA    AES-CBC(256)
  SHA1
    ECDHE-ECDSA-AES128-SHA256     0xC0, 0x23       ECDH           ECDSA    AES-CBC(128)
  SHA256
    ECDHE-ECDSA-AES256-SHA384     0xC0, 0x24       ECDH           ECDSA    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}
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/443/www

```
The following root Certification Authority certificate was found :

|-Subject             : C=US/O=Internet Security Research Group/CN=ISRG Root X1
|-Issuer              : C=US/O=Internet Security Research Group/CN=ISRG Root X1
|-Valid From          : Jun 04 11:04:38 2015 GMT
|-Valid To            : Jun 04 11:04:38 2035 GMT
|-Signature Algorithm : SHA-256 With RSA Encryption
```

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
    ----------------------        ----------        ---           ----     --------------------    ---
    ECDHE-ECDSA-AES-128-CCM-AEAD  0xC0, 0xAC       ECDH          ECDSA    AES-CCM(128)
 AEAD
    ECDHE-ECDSA-AES-128-CCM8-AEAD 0xC0, 0xAE       ECDH          ECDSA    AES-CCM8(128)
 AEAD
    ECDHE-ECDSA-AES-256-CCM-AEAD  0xC0, 0xAD       ECDH          ECDSA    AES-CCM(256)
 AEAD
    ECDHE-ECDSA-AES-256-CCM8-AEAD 0xC0, 0xAF       ECDH          ECDSA    AES-CCM8(256)
 AEAD
    ECDHE-ECDSA-CAMELLIA-CBC-128  0xC0, 0x72       ECDH          ECDSA    Camellia-CBC(128)
 SHA256
    ECDHE-ECDSA-CAMELLIA-CBC-256  0xC0, 0x73       ECDH          ECDSA    Camellia-CBC(256)
 SHA384
    ECDHE-ECDSA-AES128-SHA        0xC0, 0x09       ECDH          ECDSA    AES-CBC(128)
 SHA1
    ECDHE-ECDSA-AES256-SHA        0xC0, 0x0A       ECDH          ECDSA    AES-CBC(256)
 SHA1
    ECDHE-ECDSA-AES128-SHA256     0xC0, 0x23       ECDH          ECDSA    AES-CBC(128)
 SHA256
    ECDHE-ECDSA-AES256-SHA384     0xC0, 0x24       ECDH          ECDSA    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}
```

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/22/ssh

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

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

tcp/443/www

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

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/html/rfc7301

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/17, Modified: 2024/09/11

Plugin Output

tcp/443/www

```
http/1.1
```

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 192.168.122.129 to 3.148.28.190 :
192.168.122.129
192.168.122.2
3.148.28.190

Hop Count: 2
```