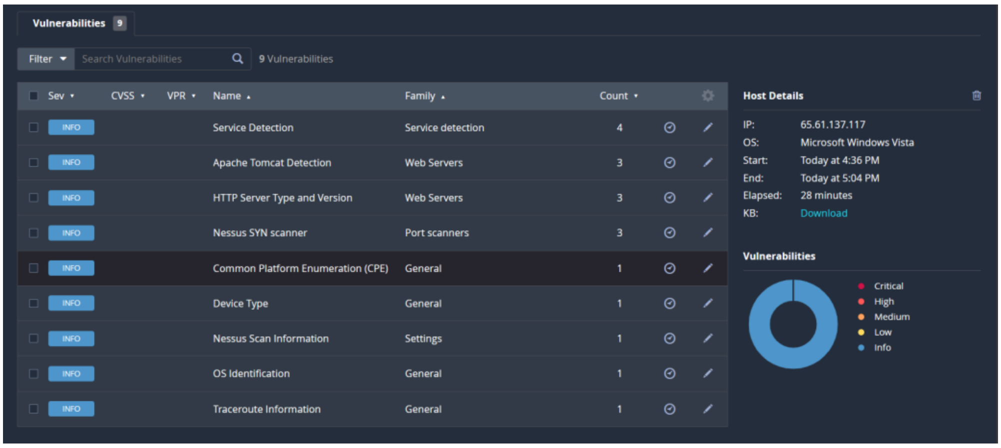
PRACTICE WEBSITE ➔ http://testfire.net

IP: 65.61.137.117

TOOL: NESSUS

(Network scan using nessus)

Vulnerabilities:



Vulnerabilities 9

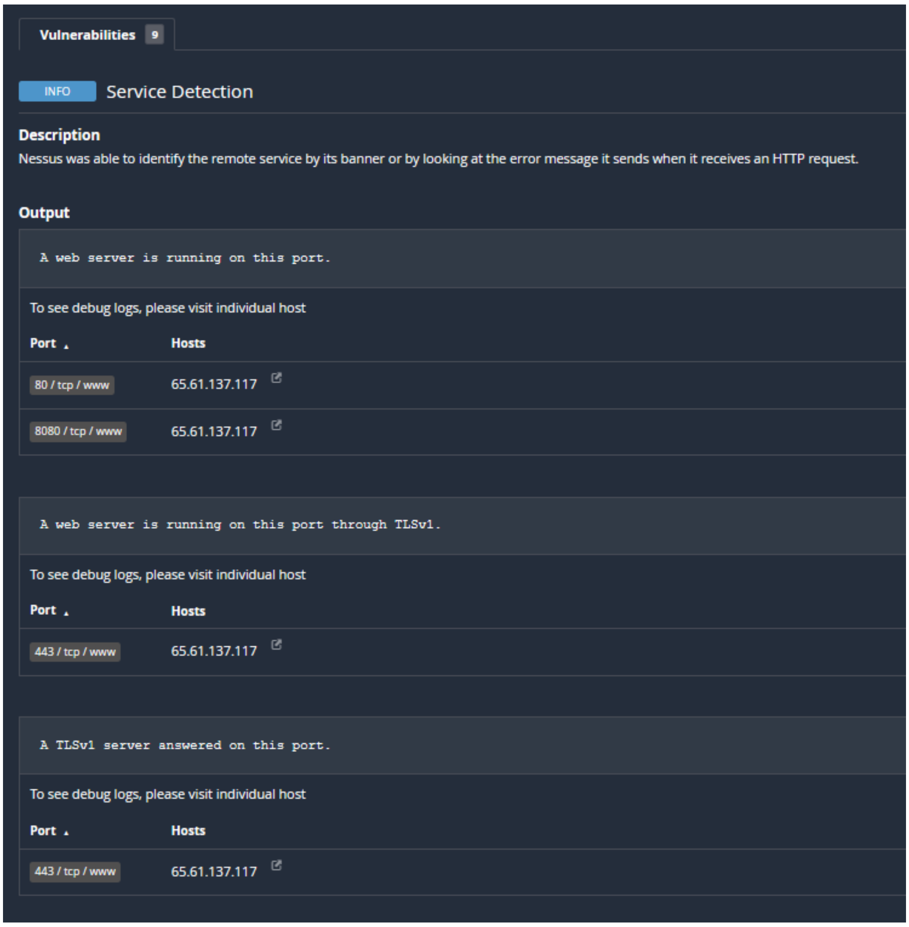
Filter ▾ Search Vulnerabilities 9 Vulnerabilities

☐	Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴	Count ▾		
☐	INFO			Service Detection	Service detection	4		
☐	INFO			Apache Tomcat Detection	Web Servers	3		
☐	INFO			HTTP Server Type and Version	Web Servers	3		
☐	INFO			Nessus SYN scanner	Port scanners	3		
☐	INFO			Common Platform Enumeration (CPE)	General	1		
☐	INFO			Device Type	General	1		
☐	INFO			Nessus Scan Information	Settings	1		
☐	INFO			OS Identification	General	1		
☐	INFO			Traceroute Information	General	1		

Host Details

IP:	65.61.137.117
OS:	Microsoft Windows Vista
Start:	Today at 4:36 PM
End:	Today at 5:04 PM
Elapsed:	28 minutes
KB:	Download

Vulnerabilities



Vulnerabilities 9

INFO Service Detection

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.

Output

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

To see debug logs, please visit individual host

Port ▴	Hosts
80 / tcp / www	65.61.137.117
8080 / tcp / www	65.61.137.117

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

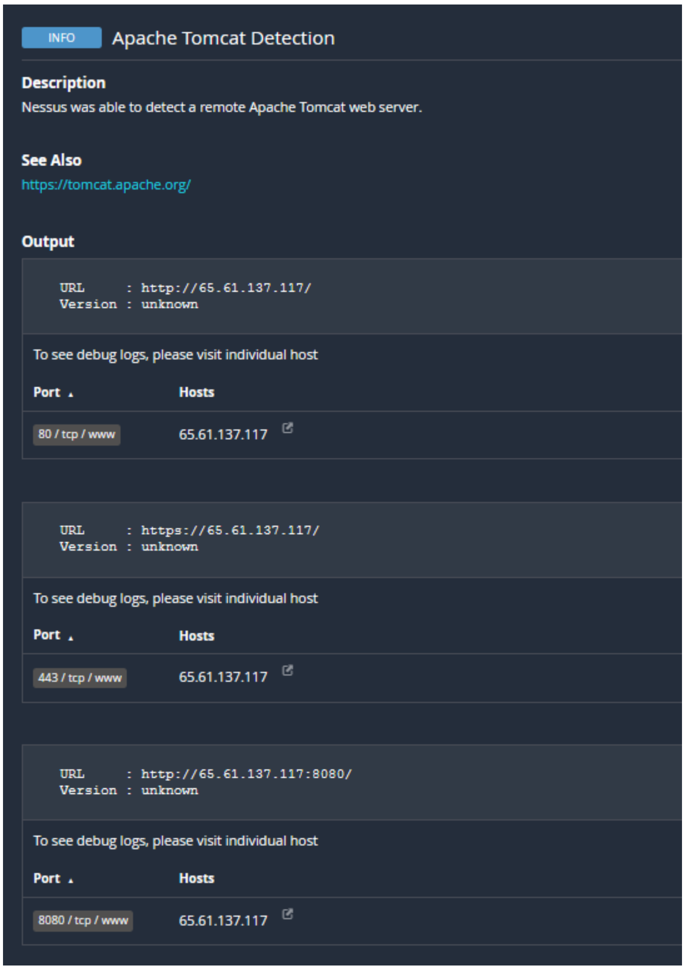
To see debug logs, please visit individual host

Port ▴	Hosts
443 / tcp / www	65.61.137.117

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

To see debug logs, please visit individual host

Port ▴	Hosts
443 / tcp / www	65.61.137.117



INFO Apache Tomcat Detection

Description

Nessus was able to detect a remote Apache Tomcat web server.

See Also

https://tomcat.apache.org/

Output

```
  URL     : http://65.61.137.117/
  Version : unknown
```

To see debug logs, please visit individual host

Port ▲	Hosts
80 / tcp / www	65.61.137.117

```
  URL     : https://65.61.137.117/
  Version : unknown
```

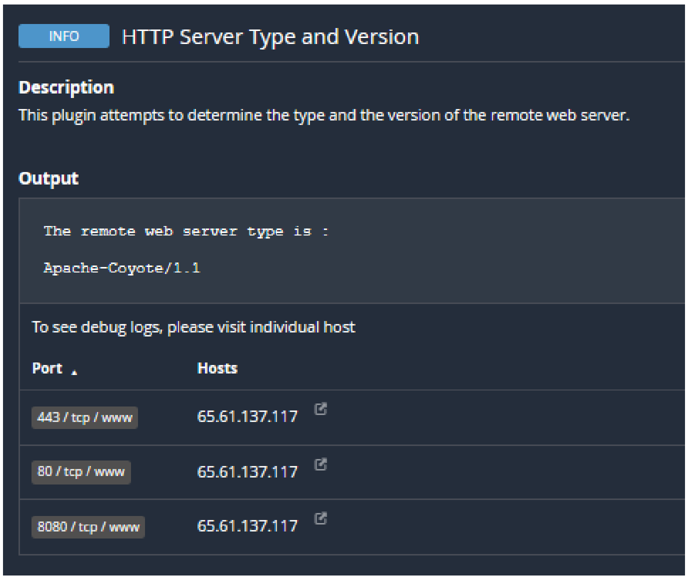
To see debug logs, please visit individual host

Port ▲	Hosts
443 / tcp / www	65.61.137.117

```
  URL     : http://65.61.137.117:8080/
  Version : unknown
```

To see debug logs, please visit individual host

Port ▲	Hosts
8080 / tcp / www	65.61.137.117



INFO HTTP Server Type and Version

Description

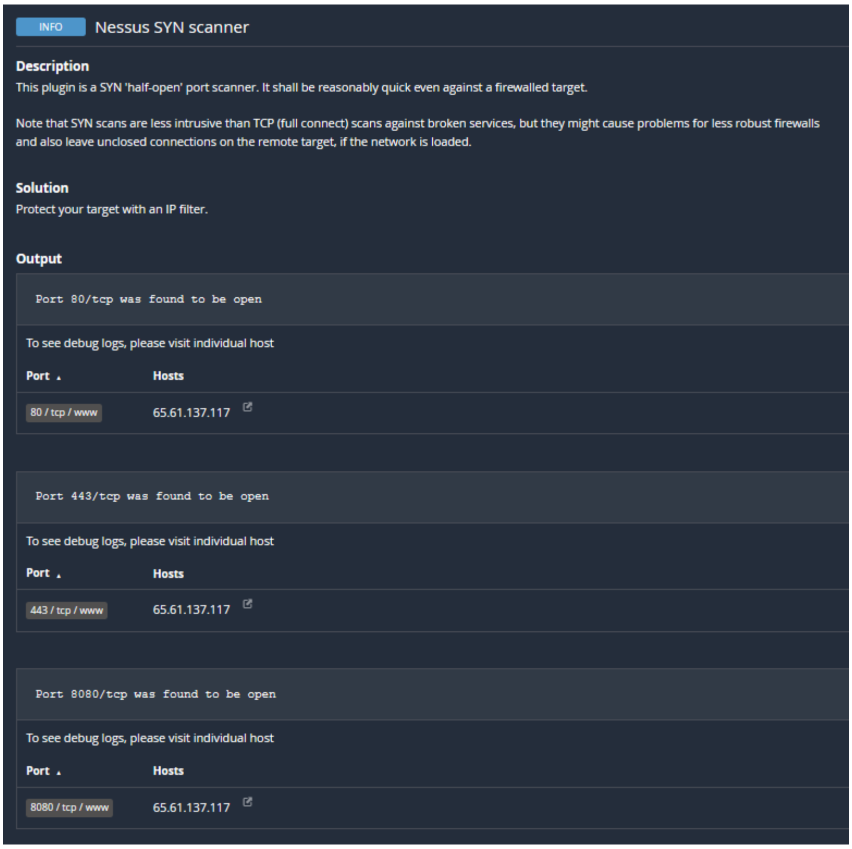
This plugin attempts to determine the type and the version of the remote web server.

Output

```
The remote web server type is :

Apache-Coyote/1.1
```

To see debug logs, please visit individual host

Port ▲	Hosts
443 / tcp / www	65.61.137.117
80 / tcp / www	65.61.137.117
8080 / tcp / www	65.61.137.117



INFO Nessus SYN scanner

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.

Output

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

To see debug logs, please visit individual host

Port ▴	Hosts
80 / tcp / www	65.61.137.117

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

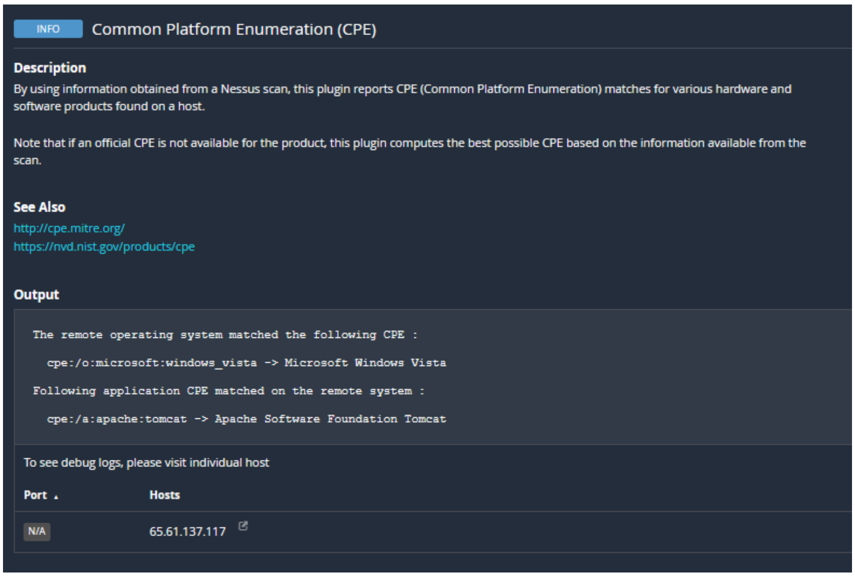
To see debug logs, please visit individual host

Port ▴	Hosts
443 / tcp / www	65.61.137.117

```
Port 8080/tcp was found to be open
```

To see debug logs, please visit individual host

Port ▴	Hosts
8080 / tcp / www	65.61.137.117



INFO Common Platform Enumeration (CPE)

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

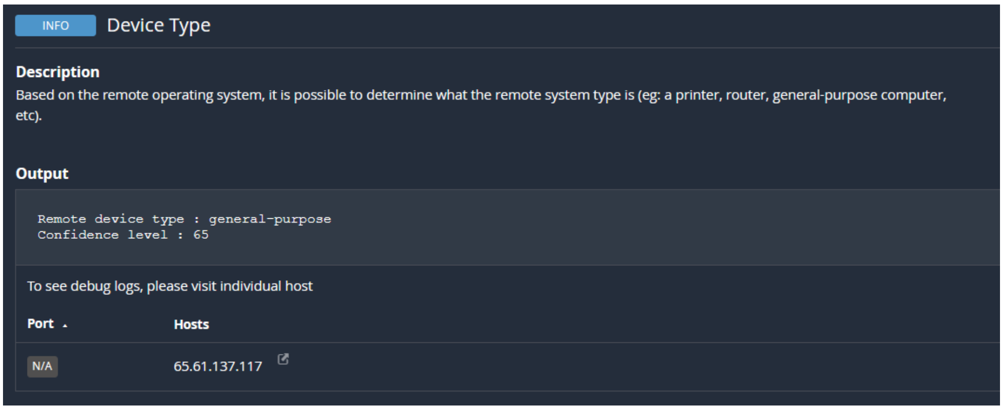
http://cpe.mitre.org/
https://nvd.nist.gov/products/cpe

Output

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

  cpe:/o:microsoft:windows_vista -> Microsoft Windows Vista

Following application CPE matched on the remote system :

  cpe:/a:apache:tomcat -> Apache Software Foundation Tomcat
```

To see debug logs, please visit individual host

Port ▴	Hosts
N/A	65.61.137.117



INFO Device Type

Description

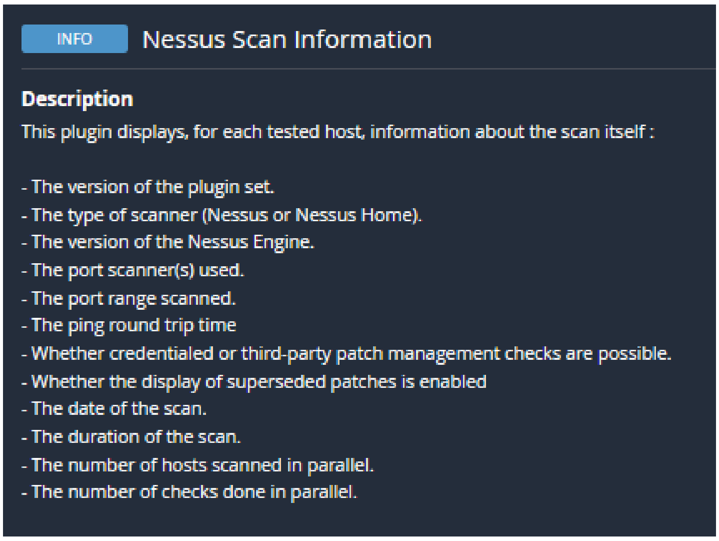
Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Output

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

To see debug logs, please visit individual host

Port ▴	Hosts
N/A	65.61.137.117

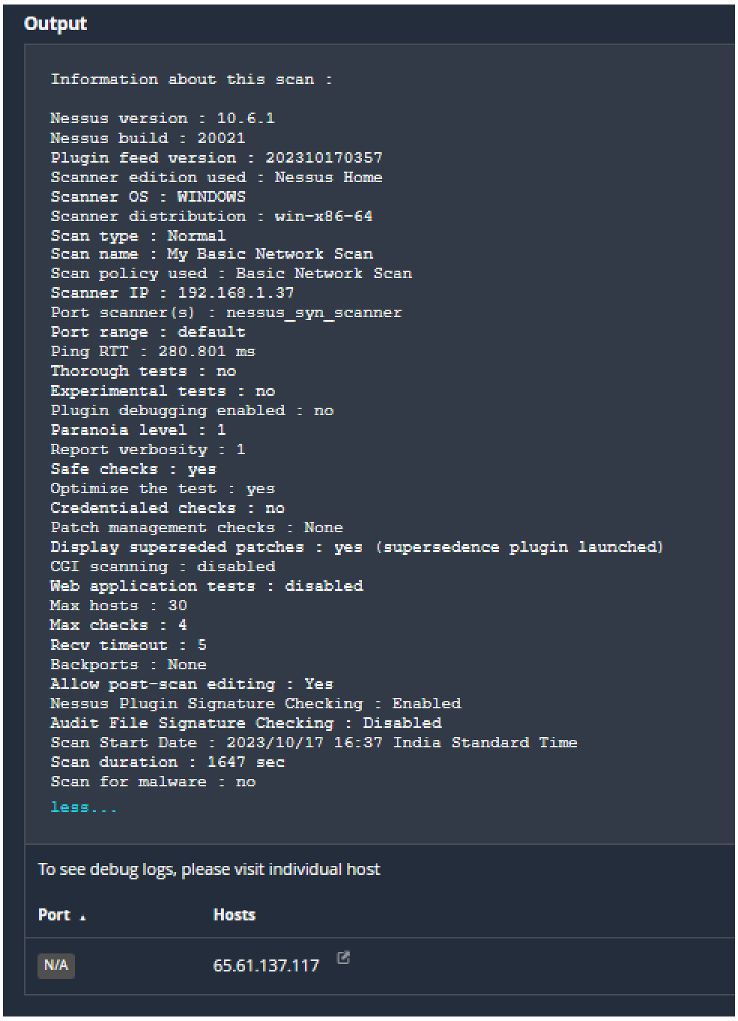


INFO Nessus Scan Information

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.

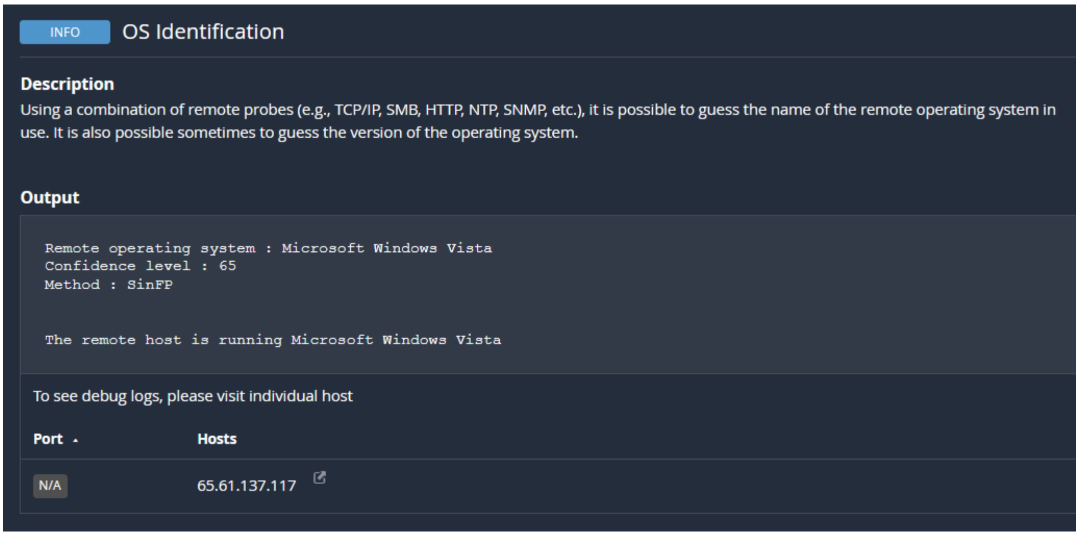


Output

```
Information about this scan :

Nessus version : 10.6.1
Nessus build : 20021
Plugin feed version : 202310170357
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : My Basic Network Scan
Scan policy used : Basic Network Scan
Scanner IP : 192.168.1.37
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 280.801 ms
Thorough tests : no
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 launched)
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 : 2023/10/17 16:37 India Standard Time
Scan duration : 1647 sec
Scan for malware : no
less...
```

To see debug logs, please visit individual host

Port ▲	Hosts
N/A	65.61.137.117



INFO OS Identification

Description

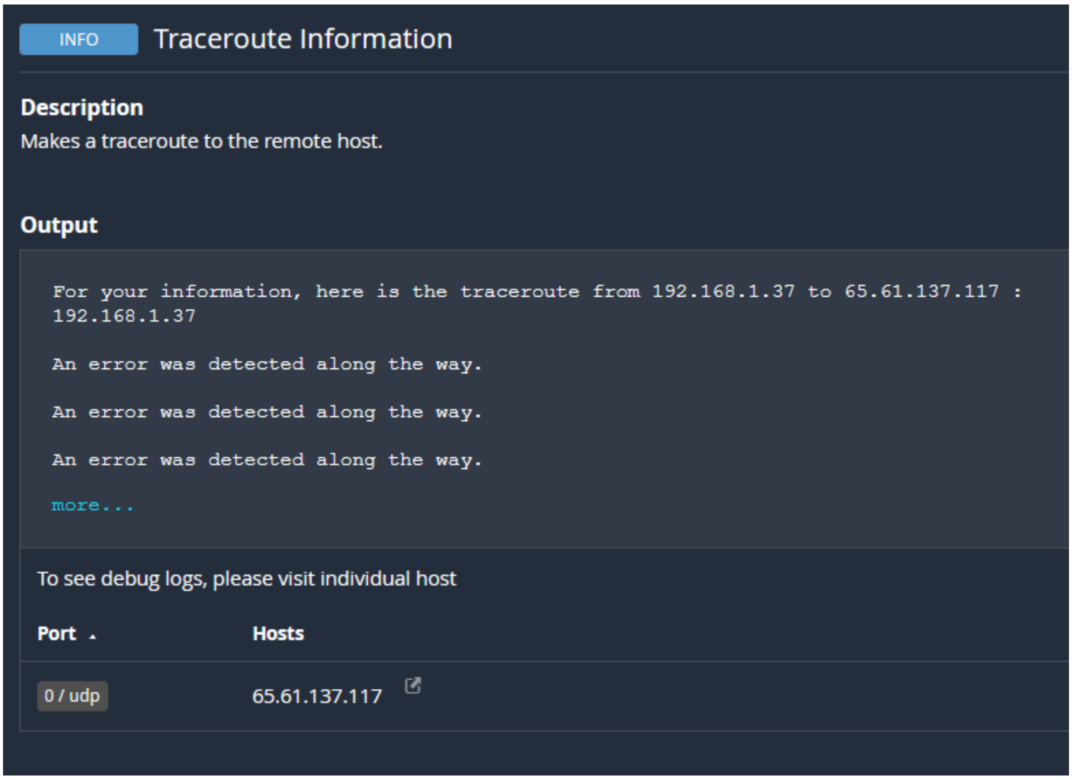
Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Output

```
Remote operating system : Microsoft Windows Vista
Confidence level : 65
Method : SinFP


The remote host is running Microsoft Windows Vista
```

To see debug logs, please visit individual host

Port	Hosts
N/A	65.61.137.117



INFO Traceroute Information

Description

Makes a traceroute to the remote host.

Output

```
For your information, here is the traceroute from 192.168.1.37 to 65.61.137.117 :
192.168.1.37

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

more...
```

To see debug logs, please visit individual host

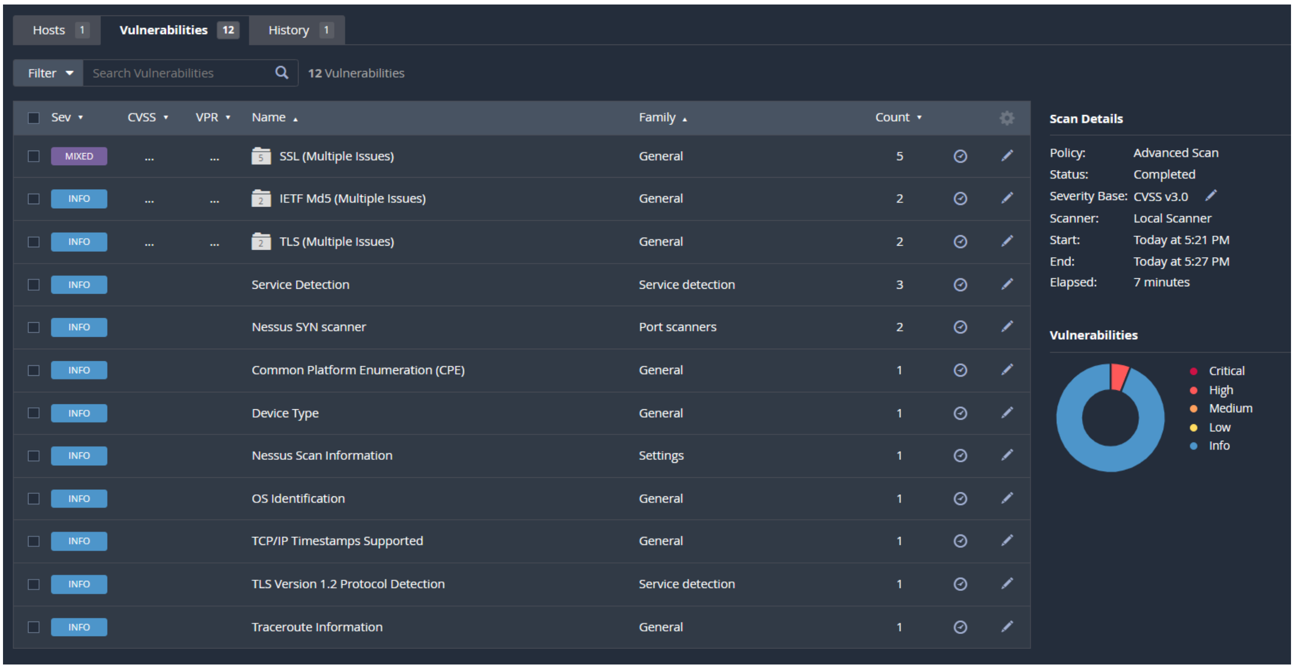
Port	Hosts
0 / udp	65.61.137.117

TEST WEBSITE ➔ https://vtop.vit.ac.in/

IP: 136.233.9.22

TOOL: NESSUS

(Advanced Network scan using Nessus)

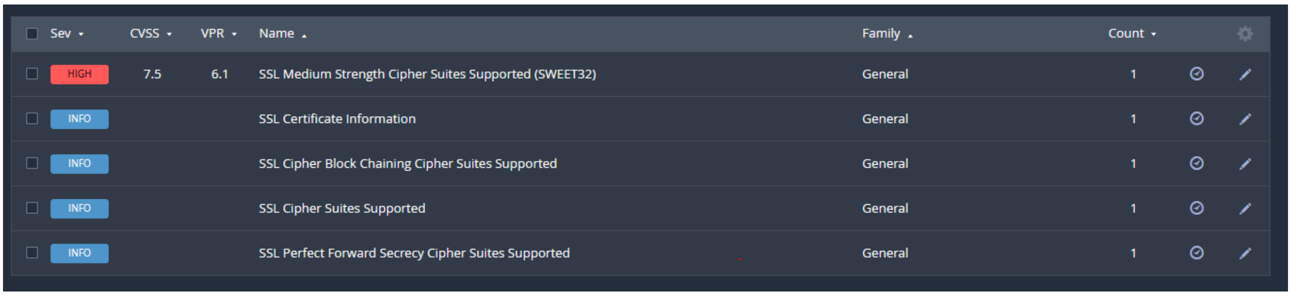


Sev	CVSS	VPR	Name	Family	Count
MIXED	...	...	SSL (Multiple Issues)	General	5
INFO	...	...	IETF Md5 (Multiple Issues)	General	2
INFO	...	...	TLS (Multiple Issues)	General	2
INFO			Service Detection	Service detection	3
INFO			Nessus SYN scanner	Port scanners	2
INFO			Common Platform Enumeration (CPE)	General	1
INFO			Device Type	General	1
INFO			Nessus Scan Information	Settings	1
INFO			OS Identification	General	1
INFO			TCP/IP Timestamps Supported	General	1
INFO			TLS Version 1.2 Protocol Detection	Service detection	1
INFO			Traceroute Information	General	1

Scan Details

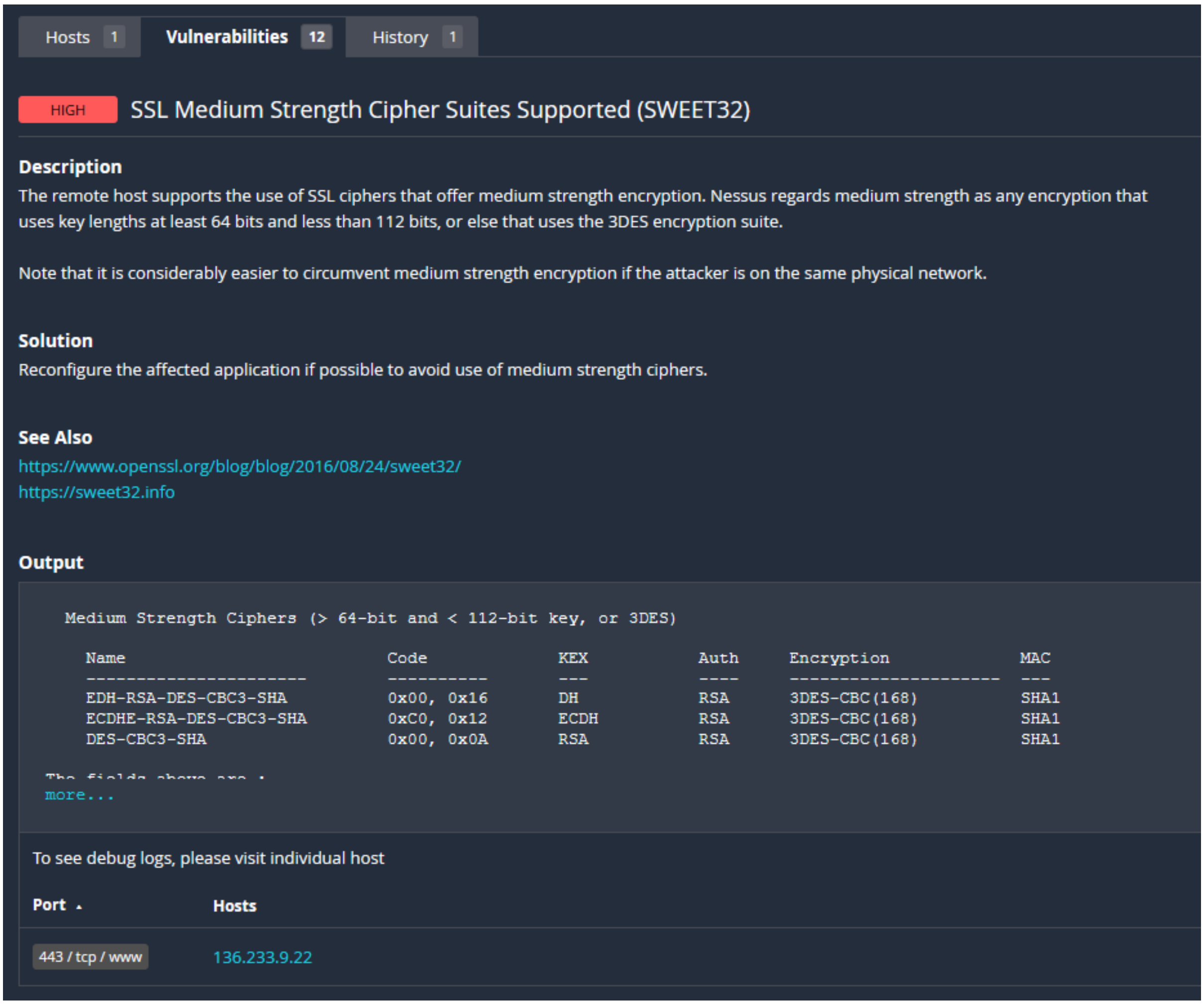
Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:21 PM
End: Today at 5:27 PM
Elapsed: 7 minutes

Vulnerabilities



Sev	CVSS	VPR	Name	Family	Count
HIGH	7.5	6.1	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	1
INFO			SSL Certificate Information	General	1
INFO			SSL Cipher Block Chaining Cipher Suites Supported	General	1
INFO			SSL Cipher Suites Supported	General	1
INFO			SSL Perfect Forward Secrecy Cipher Suites Supported	General	1

VULNERABILITIES



HIGH SSL Medium Strength Cipher Suites Supported (SWEET32)

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.

Solution

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

See Also

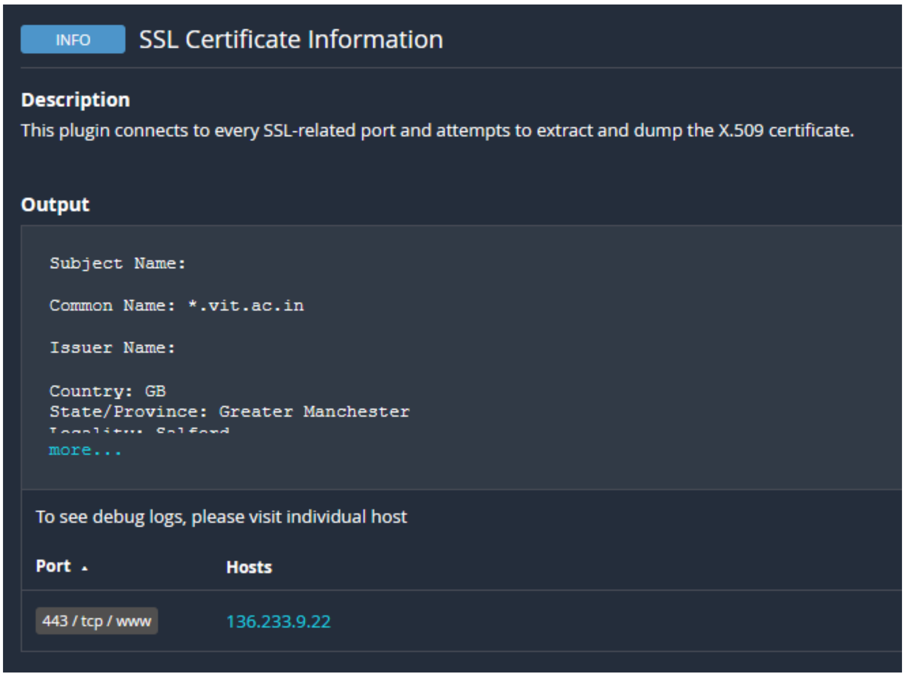
https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Output

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

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)          SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)          SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)          SHA1

  The fields above are :
  more...
```

To see debug logs, please visit individual host

Port ▴	Hosts
443 / tcp / www	136.233.9.22



INFO SSL Certificate Information

Description

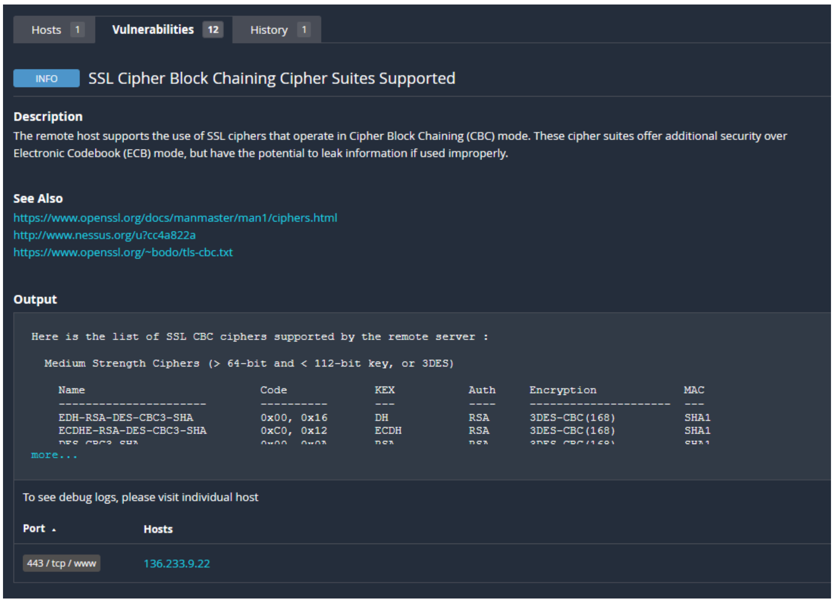
This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Output

```
  Subject Name:

  Common Name: *.vit.ac.in

  Issuer Name:

  Country: GB
  State/Province: Greater Manchester
  Locality: Salford
  more...
```

To see debug logs, please visit individual host

Port ▴	Hosts
443 / tcp / www	136.233.9.22



INFO SSL Cipher Block Chaining Cipher Suites Supported

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

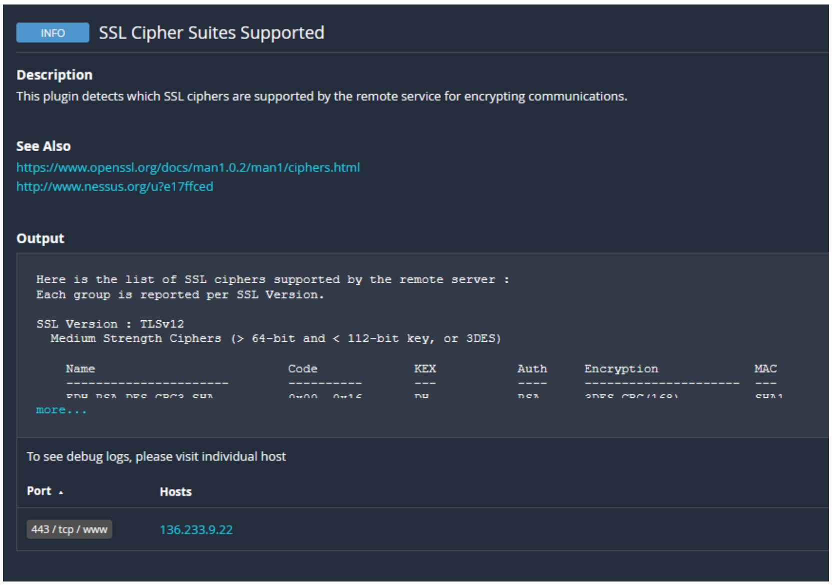
https://www.openssl.org/docs/manmaster/man1/ciphers.html
http://www.nessus.org/u?cc4a822a
https://www.openssl.org/~bodo/tls-cbc.txt

Output

```
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
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)          SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)          SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)          SHA1
more...
```

To see debug logs, please visit individual host

Port ▴	Hosts
443 / tcp / www	136.233.9.22



INFO SSL Cipher Suites Supported

Description

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

See Also

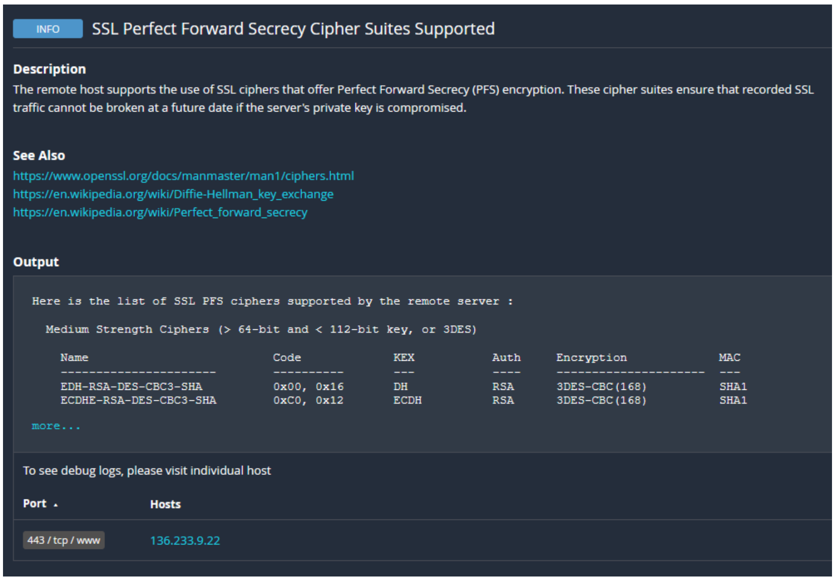
https://www.openssl.org/docs/man1.0.2/man1/ciphers.html
http://www.nessus.org/u?e17ffced

Output

```
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
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)          SHA1
more...
```

To see debug logs, please visit individual host

Port ▴	Hosts
443 / tcp / www	136.233.9.22



INFO SSL Perfect Forward Secrecy Cipher Suites Supported

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

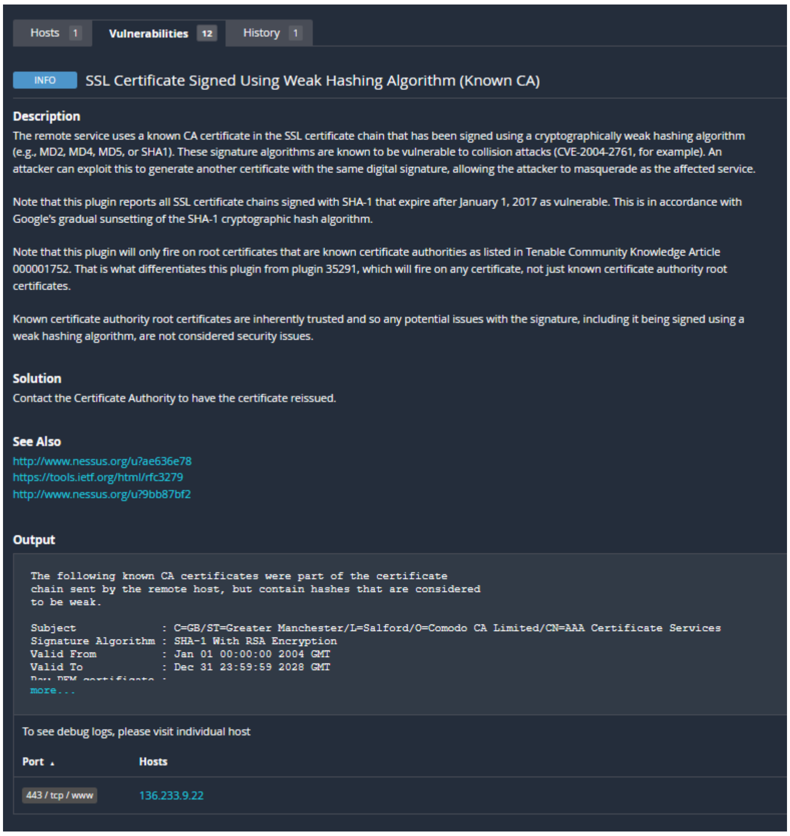
https://www.openssl.org/docs/manmaster/man1/ciphers.html
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Output

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

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

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)          SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)          SHA1
more...
```

To see debug logs, please visit individual host

Port ▴	Hosts
443 / tcp / www	136.233.9.22



SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

Solution

Contact the Certificate Authority to have the certificate reissued.

See Also

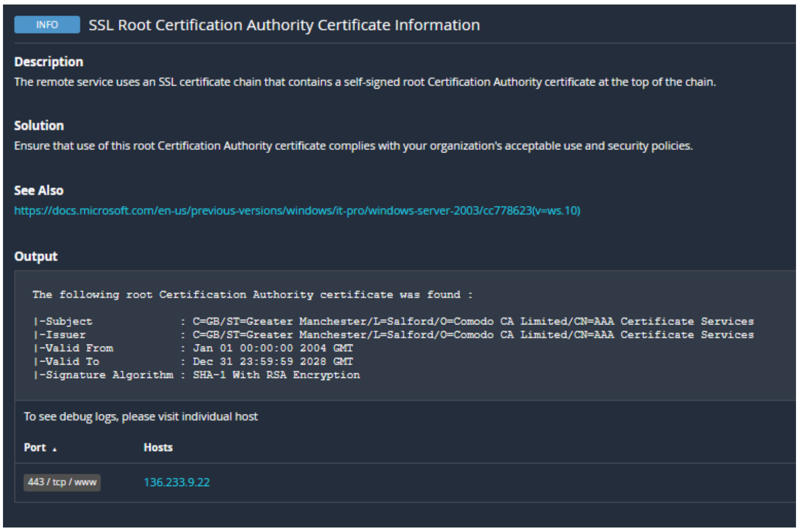
http://www.nessus.org/u?ae636e78
https://tools.ietf.org/html/rfc3279
http://www.nessus.org/u?9bb87bf2

Output

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
more...
```

To see debug logs, please visit individual host

Port ▴	Hosts
443 / tcp / www	136.233.9.22



SSL Root Certification Authority Certificate Information

Description

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

Solution

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

See Also

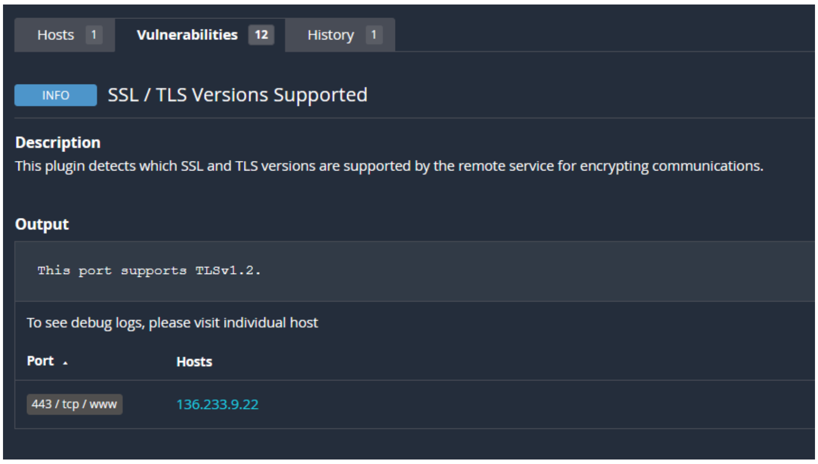
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Output

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

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

To see debug logs, please visit individual host

Port ▴	Hosts
443 / tcp / www	136.233.9.22



SSL / TLS Versions Supported

Description

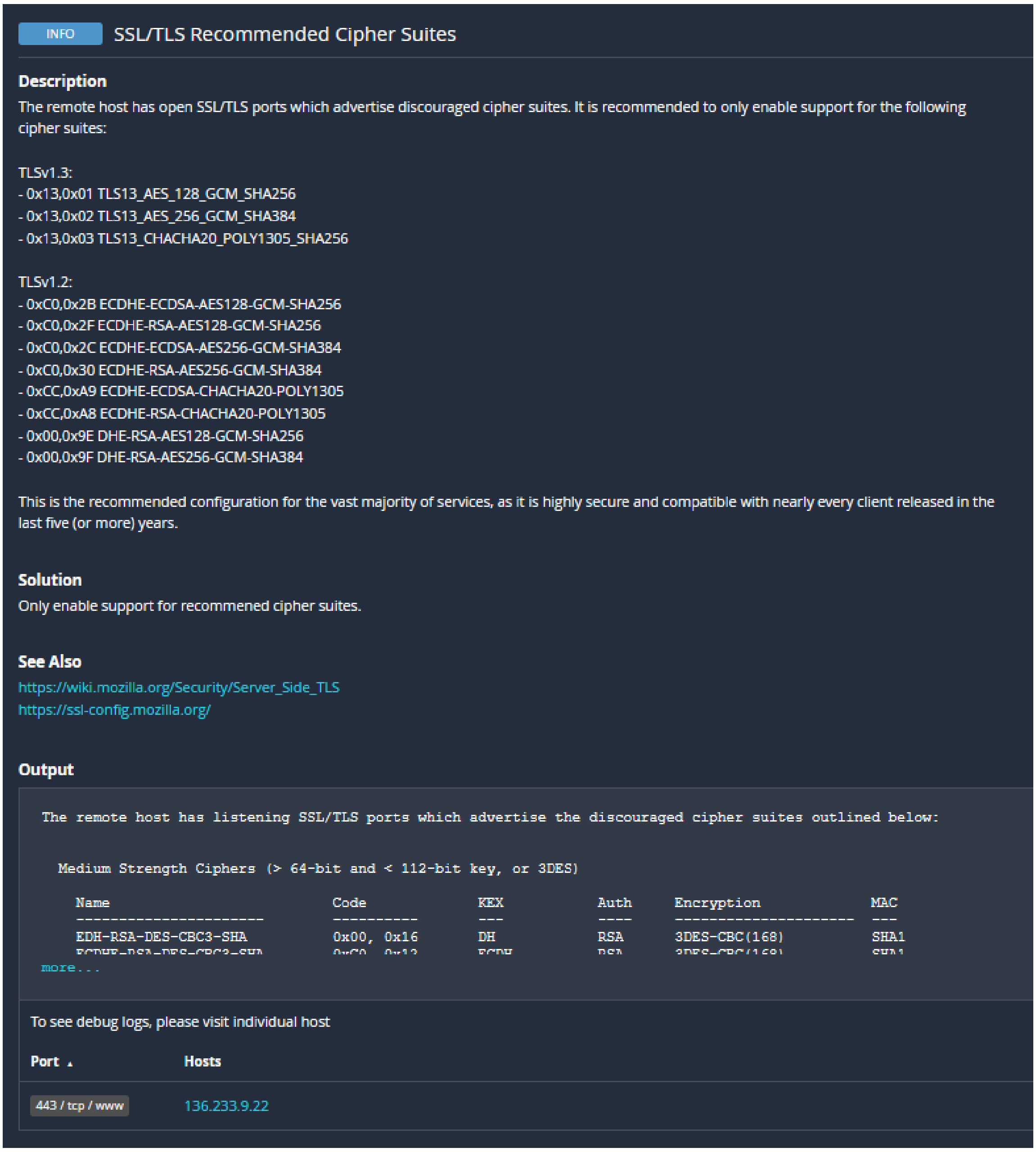
This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Output

```
This port supports TLSv1.2.
```

To see debug logs, please visit individual host

Port ▴	Hosts
443 / tcp / www	136.233.9.22



INFO

SSL/TLS Recommended Cipher Suites

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
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

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.

Solution

Only enable support for recommened cipher suites.

See Also

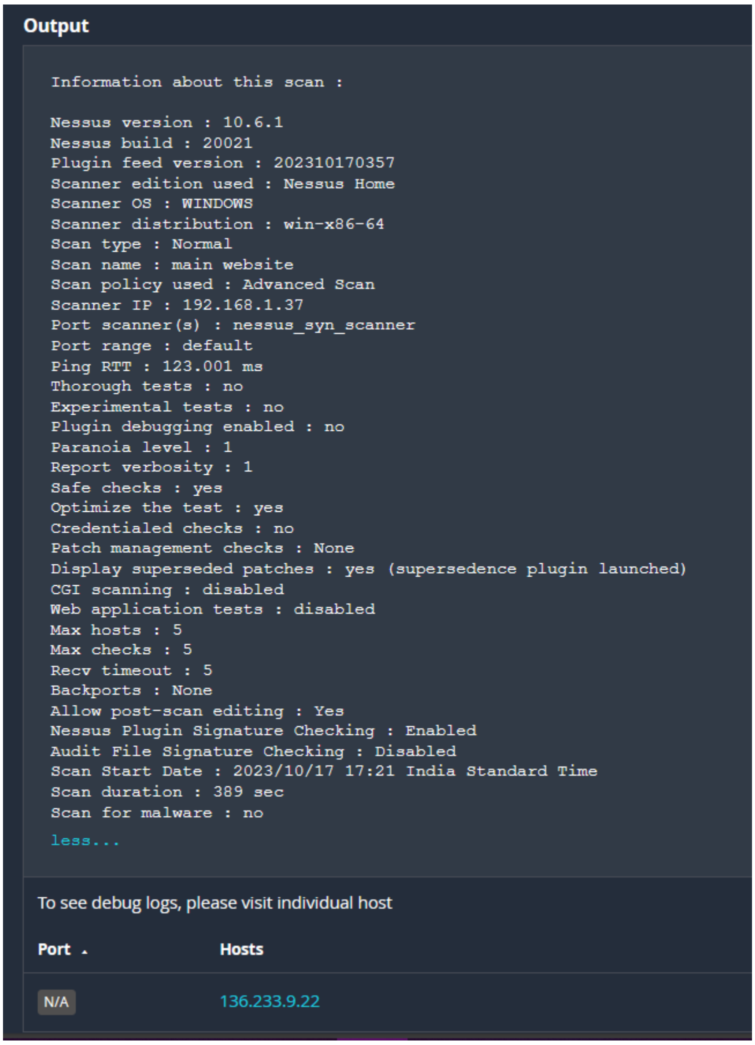
https://wiki.mozilla.org/Security/Server_Side_TLS
https://ssl-config.mozilla.org/

Output

```
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
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)          SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)          SHA1
```
more...

To see debug logs, please visit individual host

Port ▴	Hosts
443 / tcp / www	136.233.9.22

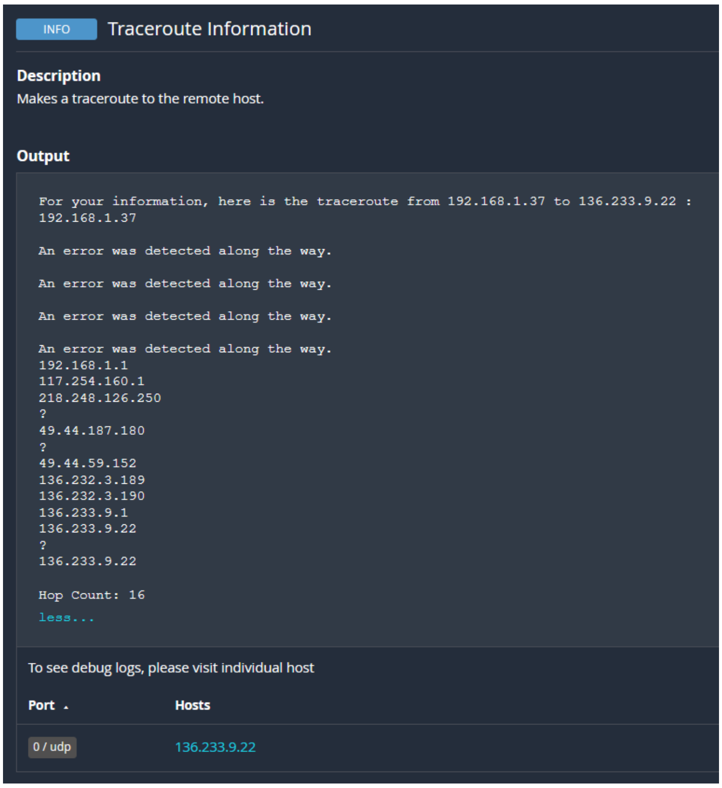


Output

```
Information about this scan :

Nessus version : 10.6.1
Nessus build : 20021
Plugin feed version : 202310170357
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : main website
Scan policy used : Advanced Scan
Scanner IP : 192.168.1.37
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 123.001 ms
Thorough tests : no
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 launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 5
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/10/17 17:21 India Standard Time
Scan duration : 389 sec
Scan for malware : no
less...
```

To see debug logs, please visit individual host

Port ▴	Hosts
N/A	136.233.9.22



INFO Traceroute Information

Description

Makes a traceroute to the remote host.

Output

```
For your information, here is the traceroute from 192.168.1.37 to 136.233.9.22 :
192.168.1.37

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.
192.168.1.1
117.254.160.1
218.248.126.250
?
49.44.187.180
?
49.44.59.152
136.232.3.189
136.232.3.190
136.233.9.1
136.233.9.22
?
136.233.9.22

Hop Count: 16
less...
```

To see debug logs, please visit individual host

Port ▴	Hosts
0 / udp	136.233.9.22