202

Report generated by Nessus™

Mon, 18 Mar 2019 21:57:38 GMT+0800

TABLE OF CONTENTS

Vulnerabilities by Host

Remediations

Vulnerabilities by Host

202.197.66.62

0	0	1	0	55
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Mon Mar 18 21:57:45 2019
End time:	Mon Mar 18 22:06:50 2019

Host Information

IP:	202.197.66.62
OS:	Linux Kernel 4.4 on Ubuntu 16.04 (xenial), Linux Kernel 2.6 on Ubuntu 16.10 (yakkety)

Vulnerabilities

12049 - Novonyx Web Server Multiple Sample Application Files Present

Synopsis

Default files are installed on this system.

Description

Novell NetWare default Novonyx web server files.

A default installation of Novell 5.x will install the Novonyx web server. Numerous web server files included with this installation could reveal system information.

Solution

If not required, remove all default Novonyx web server files.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.8 (CVSS2#E:F/RL:U/RC:ND)

References

BID	4874
CVE	CVE-2002-1634
XREF	OSVDB:17461
XREF	OSVDB:17462
XREF	OSVDB:17463
XREF	OSVDB:17464
XREF	OSVDB:17465
XREF	OSVDB:17466
XREF	OSVDB:17467
XREF	OSVDB:17468

Plugin Information:

Published: 2004/02/07, Modified: 2011/03/17

Plugin Output

tcp/50013

```

The following Novonyx web server files were found on the server:
/netbasic/websinfo.bas
/lcgi/sewse.nlm?sys:/novonyx/suitespot/docs/sewse/misc/allfield.jse
/lcgi/sewse.nlm?sys:/novonyx/suitespot/docs/sewse/misc/test.jse
/perl/samples/lancgi.pl
/perl/samples/ndslogin.pl
/perl/samples/volscgi.pl
/perl/samples/env.pl
/nsn/env.bas
/nsn/fdir.bas
```

18261 - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

n/a

Risk Factor

None

Plugin Information:

Published: 2005/05/15, Modified: 2017/03/13

Plugin Output

tcp/0

```

The Linux distribution detected was :
 - Ubuntu 16.04 (xenial)
 - Ubuntu 16.10 (yakkety)
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/50013

```
  URL        : http://202.197.66.62:50013/
  Version    : 2.4.99
  backported : 1
  os         : ConvertedUbuntu
```

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/20001

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

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/22000

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

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/33270

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

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/45000

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

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/47000

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

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/50000

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

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP 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/50013

```
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: 2017/06/06

Plugin Output

tcp/0

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

  cpe:/o:canonical:ubuntu_linux:16.04
  cpe:/o:canonical:ubuntu_linux:16.10

Following application CPE's matched on the remote system :

  cpe:/a:openbsd:openssh:7.2
  cpe:/a:apache:http_server:2.4.18
  cpe:/a:igor_sysoev:nginx:1.10.3
```

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: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 85
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/80

```
The remote web server type is :

nginx/1.10.3 (Ubuntu)
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/50013

```
The remote web server type is :

Apache/2.4.18 (Ubuntu)
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/80

```

Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Server: nginx/1.10.3 (Ubuntu)
  Date: Mon, 18 Mar 2019 14:05:33 GMT
  Content-Type: text/html
  Content-Length: 580
  Connection: keep-alive

Response Body :

```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/50013

```
Response Code : HTTP/1.1 302 Found

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Mon, 18 Mar 2019 14:05:33 GMT
  Server: Apache/2.4.18 (Ubuntu)
  Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Cache-Control: no-cache,must-revalidate
  Pragma: no-cache
  Location: /cpcsys.html
  Content-Length: 0
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=utf-8

Response Body :
```

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: 2017/05/22

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: 2017/05/22

Plugin Output

tcp/20001

```
Port 20001/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: 2017/05/22

Plugin Output

tcp/22000

```
Port 22000/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: 2017/05/22

Plugin Output

tcp/33270

```
Port 33270/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: 2017/05/22

Plugin Output

tcp/45000

```
Port 45000/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: 2017/05/22

Plugin Output

tcp/47000

```
Port 47000/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: 2017/05/22

Plugin Output

tcp/50000

```
Port 50000/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: 2017/05/22

Plugin Output

tcp/50013

```
Port 50013/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.
- Whether credentialed or third-party patch management checks are possible.
- 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: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 7.0.3
Plugin feed version : 201803271415
Scanner edition used : Nessus

ERROR: Your plugins have not been updated since 2018/3/27
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
newest vulnerability checks from Nessus.org.

Scan type : Normal
Scan policy used : Basic Network Scan
```

```
Scanner IP : 192.168.1.189
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2019/3/18 21:57
Scan duration : 537 sec
```

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: 2018/01/19

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
Linux Kernel 2.6 on Ubuntu 16.10 (yakkety)
Confidence level : 85
Method : HTTP


The remote host is running one of these operating systems :
Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
Linux Kernel 2.6 on Ubuntu 16.10 (yakkety)
```

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: 2017/08/28

Plugin Output

tcp/20001

```

Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha1
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

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

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 encryption_algorithms_server_to_client :
  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_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 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 compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

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: 2017/08/28

Plugin Output

tcp/22000

```

Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha1
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

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

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 encryption_algorithms_server_to_client :
  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_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 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 compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

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: 2017/08/28

Plugin Output

tcp/33270

```

Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha1
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

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

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 encryption_algorithms_server_to_client :
  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_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 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 compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

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: 2017/08/28

Plugin Output

tcp/45000

```

Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha1
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

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

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 encryption_algorithms_server_to_client :
  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_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 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 compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

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: 2017/08/28

Plugin Output

tcp/47000

```

Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha1
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

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

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 encryption_algorithms_server_to_client :
  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_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 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 compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

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: 2017/08/28

Plugin Output

tcp/50000

```

Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha1
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

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

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 encryption_algorithms_server_to_client :
  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_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 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 compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@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: 2017/05/30

Plugin Output

tcp/20001

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

  - 1.99
  - 2.0
```

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: 2017/05/30

Plugin Output

tcp/22000

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

  - 1.99
  - 2.0
```

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: 2017/05/30

Plugin Output

tcp/33270

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

  - 1.99
  - 2.0
```

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: 2017/05/30

Plugin Output

tcp/45000

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

  - 1.99
  - 2.0
```

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: 2017/05/30

Plugin Output

tcp/47000

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

  - 1.99
  - 2.0
```

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: 2017/05/30

Plugin Output

tcp/50000

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

  - 1.99
  - 2.0
```

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

Plugin Information:

Published: 1999/10/12, Modified: 2017/12/19

Plugin Output

tcp/20001

```
SSH version : SSH-2.0-OpenSSH_7.2p2 Ubuntu-4
SSH supported authentication : publickey,password
```

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

Plugin Information:

Published: 1999/10/12, Modified: 2017/12/19

Plugin Output

tcp/22000

```
SSH version : SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.4
SSH supported authentication : publickey,password
```

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

Plugin Information:

Published: 1999/10/12, Modified: 2017/12/19

Plugin Output

tcp/33270

```
SSH version : SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.6
SSH supported authentication : publickey,password
```

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

Plugin Information:

Published: 1999/10/12, Modified: 2017/12/19

Plugin Output

tcp/45000

```
SSH version : SSH-2.0-OpenSSH_7.2p2 Ubuntu-4
SSH supported authentication : publickey,password
```

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

Plugin Information:

Published: 1999/10/12, Modified: 2017/12/19

Plugin Output

tcp/47000

```
SSH version : SSH-2.0-OpenSSH_7.2p2 Ubuntu-4
SSH supported authentication : publickey,password
```

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

Plugin Information:

Published: 1999/10/12, Modified: 2017/12/19

Plugin Output

tcp/50000

```
SSH version : SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.4
SSH supported authentication : publickey,password
```

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: 2018/03/26

Plugin Output

tcp/80

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/20001

```
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: 2018/03/26

Plugin Output

tcp/22000

```
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: 2018/03/26

Plugin Output

tcp/33270

```
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: 2018/03/26

Plugin Output

tcp/45000

```
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: 2018/03/26

Plugin Output

tcp/47000

```
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: 2018/03/26

Plugin Output

tcp/50000

```
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: 2018/03/26

Plugin Output

tcp/50013

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

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: 2011/03/20

Plugin Output

tcp/0

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: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.189 to 202.197.66.62 :
192.168.1.189
192.168.1.1
202.197.66.62

Hop Count: 2
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/wc/exclusion.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

References

XREF	OSVDB:238

Plugin Information:

Published: 1999/10/12, Modified: 2014/05/09

Plugin Output

tcp/50013

```
Contents of robots.txt :

User-agent: *
Disallow:
```

106375 - nginx HTTP Server Detection

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

https://nginx.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/01/26, Modified: 2018/01/26

Plugin Output

tcp/80

```

  URL     : http://202.197.66.62/
  Version : 1.10.3
  os      : Ubuntu
  source  : Server: nginx/1.10.3 (Ubuntu)
```

202.197.66.72

0	0	0	0	17
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Mon Mar 18 21:57:45 2019
End time:	Mon Mar 18 22:01:47 2019

Host Information

IP:	202.197.66.72
OS:	Linux Kernel 4.4 on Ubuntu 16.04 (xenial), Linux Kernel 2.6 on Ubuntu 16.10 (yakkety)

Vulnerabilities

18261 - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

n/a

Risk Factor

None

Plugin Information:

Published: 2005/05/15, Modified: 2017/03/13

Plugin Output

tcp/0

```

The Linux distribution detected was :
 - Ubuntu 16.04 (xenial)
 - Ubuntu 16.10 (yakkety)
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/80

```
URL        : http://202.197.66.72/
Version    : 2.4.99
backported : 1
os         : ConvertedUbuntu
```

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP 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/80

```
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: 2017/06/06

Plugin Output

tcp/0

```

The remote operating system matched the following CPE's :

  cpe:/o:canonical:ubuntu_linux:16.04
  cpe:/o:canonical:ubuntu_linux:16.10

Following application CPE matched on the remote system :

  cpe:/a:apache:http_server:2.4.18
```

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: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 85
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/80

```
The remote web server type is :

Apache/2.4.18 (Ubuntu)
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/80

```

Response Code : HTTP/1.1 301 Moved Permanently

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Mon, 18 Mar 2019 14:01:23 GMT
  Server: Apache/2.4.18 (Ubuntu)
  location: forum.php
  Content-Length: 0
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=UTF-8

Response Body :

```

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

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Published: 1999/08/01, Modified: 2012/06/18

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -2 seconds.
```

11387 - L2TP Network Server Detection

Synopsis

A VPN service is listening on this port.

Description

The report host understands the L2TP tunneling protocol and appears to be a VPN endpoint, or more specifically, an L2TP Network Server.

See Also

https://en.wikipedia.org/wiki/L2TP

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2003/03/14, Modified: 2017/05/16

Plugin Output

udp/1701

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: 2017/05/22

Plugin Output

tcp/80

```
Port 80/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.
- Whether credentialed or third-party patch management checks are possible.
- 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: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 7.0.3
Plugin feed version : 201803271415
Scanner edition used : Nessus

ERROR: Your plugins have not been updated since 2018/3/27
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
newest vulnerability checks from Nessus.org.

Scan type : Normal
Scan policy used : Basic Network Scan
```

```
Scanner IP : 192.168.1.189
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2019/3/18 21:57
Scan duration : 237 sec
```

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: 2018/01/19

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
Linux Kernel 2.6 on Ubuntu 16.10 (yakkety)
Confidence level : 85
Method : HTTP


The remote host is running one of these operating systems :
Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
Linux Kernel 2.6 on Ubuntu 16.10 (yakkety)
```

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: 2018/03/26

Plugin Output

tcp/80

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

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: 2011/03/20

Plugin Output

tcp/0

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: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.189 to 202.197.66.72 :
192.168.1.189
192.168.1.1
202.197.66.72

Hop Count: 2
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/wc/exclusion.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

References

XREF	OSVDB:238

Plugin Information:

Published: 1999/10/12, Modified: 2014/05/09

Plugin Output

tcp/80

```
Contents of robots.txt :

#
# robots.txt for Discuz! X3
#

User-agent: *
Disallow: /api/
Disallow: /data/
Disallow: /source/
Disallow: /install/
Disallow: /template/
Disallow: /config/
Disallow: /uc_client/
```

```
Disallow: /uc_server/
Disallow: /static/
Disallow: /admin.php
Disallow: /search.php
Disallow: /member.php
Disallow: /api.php
Disallow: /misc.php
Disallow: /connect.php
Disallow: /forum.php?mod=redirect*
Disallow: /forum.php?mod=post*
Disallow: /home.php?mod=spacecp*
Disallow: /userapp.php?mod=app&*
Disallow: /*?mod=misc*
Disallow: /*?mod=attachment*
Disallow: /*mobile=yes*
```

32318 - Web Site Cross-Domain Policy File Detection

Synopsis

The remote web server contains a 'crossdomain.xml' file.

Description

The remote web server contains a cross-domain policy file. This is a simple XML file used by Adobe's Flash Player to allow access to data that resides outside the exact web domain from which a Flash movie file originated.

See Also

http://www.nessus.org/u?577e066f

http://kb2.adobe.com/cps/142/tn_14213.html

http://www.nessus.org/u?74a6a9a5

http://www.nessus.org/u?50ee6db2

Solution

Review the contents of the policy file carefully. Improper policies, especially an unrestricted one with just '*', could allow for cross- site request forgery and cross-site scripting attacks against the web server.

Risk Factor

None

Plugin Information:

Published: 2008/05/15, Modified: 2017/05/16

Plugin Output

tcp/80

```
Nessus was able to obtain a cross-domain policy file from the remote
host using the following URL :

  http://202.197.66.72/crossdomain.xml
```

202.197.66.76

0	0	4	0	41
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Mon Mar 18 21:57:45 2019
End time:	Mon Mar 18 22:35:26 2019

Host Information

IP:	202.197.66.76

Vulnerabilities

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

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

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

Solution

Purchase or generate a proper 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 Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/5001

```
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=TW/ST=Taipei/L=Taipei/O=QNAP Systems, Inc./OU=QTS/CN=QNAP NAS/E=support@qnap.com
|-Issuer  : C=TW/ST=Taipei/L=Taipei/O=QNAP Systems, Inc./OU=QTS/CN=QNAP NAS/E=support@qnap.com
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

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

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

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

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

See Also

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

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

Solution

Purchase or generate a proper 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 Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/8081

```
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=TW/ST=Taipei/L=Taipei/O=QNAP Systems, Inc./OU=QTS/CN=QNAP NAS/E=support@qnap.com
|-Issuer  : C=TW/ST=Taipei/L=Taipei/O=QNAP Systems, Inc./OU=QTS/CN=QNAP NAS/E=support@qnap.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 certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/5001

```
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=TW/ST=Taipei/L=Taipei/O=QNAP Systems, Inc./OU=QTS/CN=QNAP NAS/E=support@qnap.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 certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/8081

```
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=TW/ST=Taipei/L=Taipei/O=QNAP Systems, Inc./OU=QTS/CN=QNAP NAS/E=support@qnap.com
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/80

```
URL        : http://202.197.66.76/
Version    : unknown
backported : 0
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/8081

```
URL        : https://202.197.66.76:8081/
Version    : unknown
backported : 0
```

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). 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: 2015/07/02

Plugin Output

tcp/8081

```

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

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/80

```
The remote web server type is :

Apache
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/8081

```
The remote web server type is :

Apache
```

85805 - HTTP/2 Cleartext Detection

Synopsis

An HTTP/2 server is listening on the remote host.

Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

See Also

https://http2.github.io/

https://tools.ietf.org/html/rfc7540

https://github.com/http2/http2-spec

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information:

Published: 2015/09/04, Modified: 2016/01/07

Plugin Output

tcp/80

```
The server supports direct HTTP/2 connections
without encryption.
```

85805 - HTTP/2 Cleartext Detection

Synopsis

An HTTP/2 server is listening on the remote host.

Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

See Also

https://http2.github.io/

https://tools.ietf.org/html/rfc7540

https://github.com/http2/http2-spec

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information:

Published: 2015/09/04, Modified: 2016/01/07

Plugin Output

tcp/5000

```

The server supports direct HTTP/2 connections
without encryption.
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/80

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Mon, 18 Mar 2019 14:09:29 GMT
  Server: Apache
  X-Frame-Options: SAMEORIGIN
  Upgrade: h2
  Connection: Upgrade, Keep-Alive
  Keep-Alive: timeout=15, max=100
  Transfer-Encoding: chunked
  Content-Type: text/html; charset=UTF-8

Response Body :

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
 <head>
<meta http-equiv="expires" content="0">
<script type='text/javascript'>
 location.href = 'http://202.197.66.76:5000/';
</script>
```

```
  </head>
</html>
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/8081

```

Response Code : HTTP/1.0 200 OK

Protocol version : HTTP/1.0
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Date: Mon, 18 Mar 2019 14:09:30 GMT
  Server: Apache
  X-Frame-Options: SAMEORIGIN
  Upgrade: h2
  Connection: Upgrade, close
  Content-Type: text/html; charset=UTF-8

Response Body :

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
 <head>
<meta http-equiv="expires" content="0">
<script type='text/javascript'>
 location.href = 'https://202.197.66.76:5001/';
</script>
 </head>
```

```
</html>
```

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

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Published: 1999/08/01, Modified: 2012/06/18

Plugin Output

icmp/0

```
This host returns invalid timestamps (bigger than 24 hours).
```

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: 2017/05/22

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: 2017/05/22

Plugin Output

tcp/5000

```
Port 5000/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: 2017/05/22

Plugin Output

tcp/5001

```
Port 5001/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: 2017/05/22

Plugin Output

tcp/8081

```
Port 8081/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.
- Whether credentialed or third-party patch management checks are possible.
- 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: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 7.0.3
Plugin feed version : 201803271415
Scanner edition used : Nessus

ERROR: Your plugins have not been updated since 2018/3/27
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
newest vulnerability checks from Nessus.org.

Scan type : Normal
Scan policy used : Basic Network Scan
```

```
Scanner IP : 192.168.1.189
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2019/3/18 21:57
Scan duration : 2253 sec
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

http://www.openssl.org

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/11/30, Modified: 2013/10/18

Plugin Output

tcp/5001

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

http://www.openssl.org

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/11/30, Modified: 2013/10/18

Plugin Output

tcp/8081

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: 2018/02/15

Plugin Output

tcp/5001

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

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/12/01, Modified: 2018/02/15

Plugin Output

tcp/8081

```
This port supports TLSv1.0/TLSv1.1/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: 2015/12/30

Plugin Output

tcp/5001

```
Subject Name:

Country: TW
State/Province: Taipei
Locality: Taipei
Organization: QNAP Systems, Inc.
Organization Unit: QTS
Common Name: QNAP NAS
Email Address: support@qnap.com

Issuer Name:

Country: TW
State/Province: Taipei
Locality: Taipei
Organization: QNAP Systems, Inc.
Organization Unit: QTS
Common Name: QNAP NAS
Email Address: support@qnap.com

Serial Number: 00 E3 42 57 15 C5 DE F2 AF

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 09 00:59:27 2018 GMT
Not Valid After: Nov 06 00:59:27 2028 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 2048 bits
Public Key: 00 AF BA B1 A1 7F A1 AC F0 BE AF A2 76 56 0E 79 A2 0D 00 A9
            DD 16 17 82 40 C2 30 F6 F6 53 5F 4D EF D1 BD E5 B4 D9 ED 5A
            00 EB 31 9F FD 56 0D 5F 5D D8 70 FA B6 AE 33 73 EA D3 41 37
            5F 66 9D E4 FA 78 10 DA 30 87 4B B2 1A D1 E6 01 85 39 25 94
            37 11 8A 3C 69 FF E8 C0 80 3F 76 05 7E AC CA 7F B5 3B 19 C5
            C7 DB B7 E8 01 AF 78 4C 17 05 0D 2C FE B6 98 17 CD FB 31 E4
            FC 6A 1A D3 B8 01 0A 6A 94 6F DE E9 2E 9F 74 BB AA 9C AF 4B
            77 1D 05 AA D2 64 A8 84 A1 5A BC 6D 65 E7 5D 45 DE 60 D5 1C
            E2 BF CE A1 DA AA 66 49 68 A1 8F 08 45 AD EB 9D CB D5 D7 73
            B2 3B BF CE 9F 0D 96 60 63 4E 51 BD C7 CC D4 10 63 73 68 4A
            90 09 2A A0 63 54 42 BA 22 BA 58 EE FA 2F 7A FE 34 78 6D FB
            B1 CB E0 94 A0 77 6D B1 45 40 94 D6 96 FD 3F 32 1F CF 47 27
            2D D4 71 40 59 54 54 82 25 0D 27 DC EA B7 87 77 8F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 A1 80 0A 4B 76 D1 0D FB 8A B4 F7 0A 2C 6C 1C 1F C1 C5 42
           98 F9 FE 25 4E 4A 51 E1 F4 4C 37 C4 82 7E 93 EB 0A D6 FC 1F
           7E 42 F0 30 62 70 16 40 E2 71 B5 D5 B9 B2 6E BD CB 3C 2D 9E
           18 D9 1C C9 A1 5F B8 21 BB 6D D0 C2 7F 8A 42 BB 0D 42 61 10
           CC C7 3D 2D 30 E1 5E 23 76 29 4A 05 3D 0D C0 F3 1F 58 A2 14
           E0 C4 F6 BB 2D B7 ED 97 F9 80 13 14 A1 1C 8B 1B 04 E1 D6 AF
 [...]
```

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: 2015/12/30

Plugin Output

tcp/8081

```
Subject Name:

Country: TW
State/Province: Taipei
Locality: Taipei
Organization: QNAP Systems, Inc.
Organization Unit: QTS
Common Name: QNAP NAS
Email Address: support@qnap.com

Issuer Name:

Country: TW
State/Province: Taipei
Locality: Taipei
Organization: QNAP Systems, Inc.
Organization Unit: QTS
Common Name: QNAP NAS
Email Address: support@qnap.com

Serial Number: 00 E3 42 57 15 C5 DE F2 AF

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 09 00:59:27 2018 GMT
Not Valid After: Nov 06 00:59:27 2028 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 2048 bits
Public Key: 00 AF BA B1 A1 7F A1 AC F0 BE AF A2 76 56 0E 79 A2 0D 00 A9
            DD 16 17 82 40 C2 30 F6 F6 53 5F 4D EF D1 BD E5 B4 D9 ED 5A
            00 EB 31 9F FD 56 0D 5F 5D D8 70 FA B6 AE 33 73 EA D3 41 37
            5F 66 9D E4 FA 78 10 DA 30 87 4B B2 1A D1 E6 01 85 39 25 94
            37 11 8A 3C 69 FF E8 C0 80 3F 76 05 7E AC CA 7F B5 3B 19 C5
            C7 DB B7 E8 01 AF 78 4C 17 05 0D 2C FE B6 98 17 CD FB 31 E4
            FC 6A 1A D3 B8 01 0A 6A 94 6F DE E9 2E 9F 74 BB AA 9C AF 4B
            77 1D 05 AA D2 64 A8 84 A1 5A BC 6D 65 E7 5D 45 DE 60 D5 1C
            E2 BF CE A1 DA AA 66 49 68 A1 8F 08 45 AD EB 9D CB D5 D7 73
            B2 3B BF CE 9F 0D 96 60 63 4E 51 BD C7 CC D4 10 63 73 68 4A
            90 09 2A A0 63 54 42 BA 22 BA 58 EE FA 2F 7A FE 34 78 6D FB
            B1 CB E0 94 A0 77 6D B1 45 40 94 D6 96 FD 3F 32 1F CF 47 27
            2D D4 71 40 59 54 54 82 25 0D 27 DC EA B7 87 77 8F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 A1 80 0A 4B 76 D1 0D FB 8A B4 F7 0A 2C 6C 1C 1F C1 C5 42
           98 F9 FE 25 4E 4A 51 E1 F4 4C 37 C4 82 7E 93 EB 0A D6 FC 1F
           7E 42 F0 30 62 70 16 40 E2 71 B5 D5 B9 B2 6E BD CB 3C 2D 9E
           18 D9 1C C9 A1 5F B8 21 BB 6D D0 C2 7F 8A 42 BB 0D 42 61 10
           CC C7 3D 2D 30 E1 5E 23 76 29 4A 05 3D 0D C0 F3 1F 58 A2 14
           E0 C4 F6 BB 2D B7 ED 97 F9 80 13 14 A1 1C 8B 1B 04 E1 D6 AF
 [...]
```

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

http://www.openssl.org/docs/apps/ciphers.html

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/5001

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

  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA256

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
```

```
    Au={authentication}
    Enc={symmetric encryption method}
    Mac={message authentication code}
    {export flag}
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

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

Description

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

See Also

http://www.openssl.org/docs/apps/ciphers.html

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/8081

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

  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA256

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
```

```
    Au={authentication}
    Enc={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/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/02/15

Plugin Output

tcp/5001

```

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

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

    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    RSA-AES256-SHA384            Kx=RSA         Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA256


SSL Version : TLSv11
  High Strength Ciphers (>= 112-bit key)
```

```
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1


SSL Version : TLSv1
  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1 [...]
```

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/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/02/15

Plugin Output

tcp/8081

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

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

    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    RSA-AES256-SHA384            Kx=RSA         Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA256


SSL Version : TLSv11
  High Strength Ciphers (>= 112-bit key)
```

```
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1


SSL Version : TLSv1
  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1 [...]
```

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

http://www.openssl.org/docs/apps/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: 2017/06/12

Plugin Output

tcp/5001

```

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

  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
```

```
    Mac={message authentication code}
    {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

http://www.openssl.org/docs/apps/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: 2017/06/12

Plugin Output

tcp/8081

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

  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={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://technet.microsoft.com/en-us/library/cc778623

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: 2016/11/14

Plugin Output

tcp/5001

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

|-Subject             : C=TW/ST=Taipei/L=Taipei/O=QNAP Systems, Inc./OU=QTS/CN=QNAP NAS/
E=support@qnap.com
|-Issuer              : C=TW/ST=Taipei/L=Taipei/O=QNAP Systems, Inc./OU=QTS/CN=QNAP NAS/
E=support@qnap.com
|-Valid From          : Nov 09 00:59:27 2018 GMT
|-Valid To            : Nov 06 00:59:27 2028 GMT
|-Signature Algorithm : SHA-256 With RSA Encryption
```

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://technet.microsoft.com/en-us/library/cc778623

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: 2016/11/14

Plugin Output

tcp/8081

```

The following root Certification Authority certificate was found :

|-Subject             : C=TW/ST=Taipei/L=Taipei/O=QNAP Systems, Inc./OU=QTS/CN=QNAP NAS/
E=support@qnap.com
|-Issuer              : C=TW/ST=Taipei/L=Taipei/O=QNAP Systems, Inc./OU=QTS/CN=QNAP NAS/
E=support@qnap.com
|-Valid From          : Nov 09 00:59:27 2018 GMT
|-Valid To            : Nov 06 00:59:27 2028 GMT
|-Signature Algorithm : SHA-256 With RSA Encryption
```

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: 2018/03/26

Plugin Output

tcp/80

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/5000

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/5001

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

tcp/5001

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

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: 2018/03/26

Plugin Output

tcp/8081

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

tcp/8081

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

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: 2011/03/20

Plugin Output

tcp/0

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: 2016/02/15

Plugin Output

tcp/5001

```
ALPN Supported Protocols:

  http/1.1
  h2
```

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: 2016/02/15

Plugin Output

tcp/8081

```
ALPN Supported Protocols:

  http/1.1
  h2
```

104743 - 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 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.1 requires that TLS 1.0 be disabled entirely by June 2018, except for point-of-sale terminals and their termination points.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information:

Published: 2017/11/22, Modified: 2017/11/22

Plugin Output

tcp/5001

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

104743 - 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 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.1 requires that TLS 1.0 be disabled entirely by June 2018, except for point-of-sale terminals and their termination points.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information:

Published: 2017/11/22, Modified: 2017/11/22

Plugin Output

tcp/8081

```
TLSv1 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: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.189 to 202.197.66.76 :
192.168.1.189
192.168.1.1
202.197.66.76

Hop Count: 2
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/04/28, Modified: 2015/10/13

Plugin Output

tcp/5000

```

The remote web server is very slow - it took 66
seconds to execute the plugin no404.nasl (it usually only takes a few
seconds).

In order to keep the scan total time to a reasonable amount, the
remote web server has not been tested.

If you want to test the remote server, either fix it to have it reply
to Nessus' requests in a reasonable amount of time, or enable the
'Perform thorough tests' setting.
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/04/28, Modified: 2015/10/13

Plugin Output

tcp/5001

```

The remote web server is very slow - it took 66
seconds to execute the plugin no404.nasl (it usually only takes a few
seconds).

In order to keep the scan total time to a reasonable amount, the
remote web server has not been tested.

If you want to test the remote server, either fix it to have it reply
to Nessus' requests in a reasonable amount of time, or enable the
'Perform thorough tests' setting.
```

202.197.66.95

0	0	24	5	52
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Mon Mar 18 22:01:52 2019
End time:	Mon Mar 18 22:39:08 2019

Host Information

IP:	202.197.66.95

Vulnerabilities

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

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

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

Solution

Purchase or generate a proper 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 Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/21

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

|-Subject : C=US/ST=WI/L=Helenville/O=Rhino Software, Inc./OU=Software Development/CN=ftp.Serv-U.com
|-Issuer  : C=US/ST=WI/L=Helenville/O=Rhino Software, Inc./OU=Software Development/CN=ftp.Serv-U.com
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

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

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

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

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

See Also

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

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

Solution

Purchase or generate a proper 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 Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/443

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

|-Subject : C=US/ST=WI/L=Helenville/O=Rhino Software, Inc./OU=Software Development/CN=ftp.Serv-U.com
|-Issuer  : C=US/ST=WI/L=Helenville/O=Rhino Software, Inc./OU=Software Development/CN=ftp.Serv-U.com
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

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

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

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

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

See Also

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

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

Solution

Purchase or generate a proper 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 Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/990

```

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

|-Subject : C=US/ST=WI/L=Helenville/O=Rhino Software, Inc./OU=Software Development/CN=ftp.Serv-U.com
|-Issuer  : C=US/ST=WI/L=Helenville/O=Rhino Software, Inc./OU=Software Development/CN=ftp.Serv-U.com
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an 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. An attacker can exploit this to generate another certificate with the same digital signature, allowing an 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 certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?e120eea1

http://technet.microsoft.com/en-us/security/advisory/961509

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	OSVDB:45106
XREF	OSVDB:45108

XREF	OSVDB:45127
XREF	CERT:836068
XREF	CWE:310

Plugin Information:

Published: 2009/01/05, Modified: 2018/02/20

Plugin Output

tcp/21

```

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

|-Subject             : C=US/ST=WI/L=Helenville/O=Rhino Software, Inc./OU=Software Development/
CN=ftp.Serv-U.com
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Apr 29 15:53:05 2009 GMT
|-Valid To            : Apr 27 15:53:05 2019 GMT
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an 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. An attacker can exploit this to generate another certificate with the same digital signature, allowing an 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 certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?e120eea1

http://technet.microsoft.com/en-us/security/advisory/961509

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	OSVDB:45106
XREF	OSVDB:45108

XREF	OSVDB:45127
XREF	CERT:836068
XREF	CWE:310

Plugin Information:

Published: 2009/01/05, Modified: 2018/02/20

Plugin Output

tcp/443

```

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

|-Subject             : C=US/ST=WI/L=Helenville/O=Rhino Software, Inc./OU=Software Development/
CN=ftp.Serv-U.com
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Apr 29 15:53:05 2009 GMT
|-Valid To            : Apr 27 15:53:05 2019 GMT
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an 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. An attacker can exploit this to generate another certificate with the same digital signature, allowing an 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 certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?e120eea1

http://technet.microsoft.com/en-us/security/advisory/961509

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	OSVDB:45106
XREF	OSVDB:45108

XREF	OSVDB:45127
XREF	CERT:836068
XREF	CWE:310

Plugin Information:

Published: 2009/01/05, Modified: 2018/02/20

Plugin Output

tcp/990

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

|-Subject             : C=US/ST=WI/L=Helenville/O=Rhino Software, Inc./OU=Software Development/
CN=ftp.Serv-U.com
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Apr 29 15:53:05 2009 GMT
|-Valid To            : Apr 27 15:53:05 2019 GMT
```

42873 - SSL Medium Strength Cipher Suites Supported

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/

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2009/11/23, Modified: 2017/09/01

Plugin Output

tcp/21

```

Here is the list of medium strength SSL ciphers supported by the remote server :

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

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :
```

```
{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported

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/

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2009/11/23, Modified: 2017/09/01

Plugin Output

tcp/443

```

Here is the list of medium strength SSL ciphers supported by the remote server :

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

    DES-CBC3-SHA                 Kx=RSA         Au=RSA       Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :
```

```
{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported

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/

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2009/11/23, Modified: 2017/09/01

Plugin Output

tcp/990

```

Here is the list of medium strength SSL ciphers supported by the remote server :

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

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)       Mac=SHA1

The fields above are :
```

```
{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

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 certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/21

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

|-Subject : C=US/ST=WI/L=Helenville/O=Rhino Software, Inc./OU=Software Development/CN=ftp.Serv-U.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 certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/443

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

|-Subject : C=US/ST=WI/L=Helenville/O=Rhino Software, Inc./OU=Software Development/CN=ftp.Serv-U.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 certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/990

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

|-Subject : C=US/ST=WI/L=Helenville/O=Rhino Software, Inc./OU=Software Development/CN=ftp.Serv-U.com
```

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?0bb7b67d

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.1 (with approved cipher suites) or higher instead.

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)

CVSS Base Score

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

Plugin Information:

Published: 2005/10/12, Modified: 2017/07/11

Plugin Output

tcp/21

```
- SSLv3 is enabled and the server supports at least one cipher.
```

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?0bb7b67d

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.1 (with approved cipher suites) or higher instead.

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)

CVSS Base Score

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

Plugin Information:

Published: 2005/10/12, Modified: 2017/07/11

Plugin Output

tcp/443

```
- SSLv3 is enabled and the server supports at least one cipher.
```

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?0bb7b67d

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.1 (with approved cipher suites) or higher instead.

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)

CVSS Base Score

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

Plugin Information:

Published: 2005/10/12, Modified: 2017/07/11

Plugin Output

tcp/990

```

- SSLv3 is enabled and the server supports at least one cipher.
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	70574
CVE	CVE-2014-3566
XREF	OSVDB:113251
XREF	CERT:577193

Plugin Information:

Published: 2014/10/15, Modified: 2016/11/30

Plugin Output

tcp/21

```

Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	70574
CVE	CVE-2014-3566
XREF	OSVDB:113251
XREF	CERT:577193

Plugin Information:

Published: 2014/10/15, Modified: 2016/11/30

Plugin Output

tcp/443

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	70574
CVE	CVE-2014-3566
XREF	OSVDB:113251
XREF	CERT:577193

Plugin Information:

Published: 2014/10/15, Modified: 2016/11/30

Plugin Output

tcp/990

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

71863 - Serv-U FTP Server < 15.0.0.0 Multiple Security Vulnerabilities

Synopsis

The remote FTP server is affected by multiple vulnerabilities.

Description

According to its banner, the installed version of Serv-U is a version prior to version 15.0.0.0. It is, therefore, potentially affected by multiple vulnerabilities :

- An unspecified error exists related to SSL that can be exploited to cause a denial of service.

- An unspecified error exists when using the 'Require Fully Qualified Membership' LDAP login settings.

See Also

http://www.serv-u.com/releasenotes/

Solution

Upgrade to Serv-U version 15.0.0.0 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	61903
XREF	OSVDB:96463
XREF	OSVDB:96464

Plugin Information:

Published: 2014/01/08, Modified: 2014/01/09

Plugin Output

tcp/21

```
 Version source    : 200 Name=Serv-U; Version=14.0.2.0; OS=Windows 7; OSVer=6.1.7601;
CaseSensitive=0;
 Installed version : 14.0.2.0
 Fixed version     : 15.0.0.0
```

71863 - Serv-U FTP Server < 15.0.0.0 Multiple Security Vulnerabilities

Synopsis

The remote FTP server is affected by multiple vulnerabilities.

Description

According to its banner, the installed version of Serv-U is a version prior to version 15.0.0.0. It is, therefore, potentially affected by multiple vulnerabilities :

- An unspecified error exists related to SSL that can be exploited to cause a denial of service.

- An unspecified error exists when using the 'Require Fully Qualified Membership' LDAP login settings.

See Also

http://www.serv-u.com/releasenotes/

Solution

Upgrade to Serv-U version 15.0.0.0 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	61903
XREF	OSVDB:96463
XREF	OSVDB:96464

Plugin Information:

Published: 2014/01/08, Modified: 2014/01/09

Plugin Output

tcp/990

```
 Version source    : 200 Name=Serv-U; Version=14.0.2.0; OS=Windows 7; OSVer=6.1.7601;
CaseSensitive=0;
 Installed version : 14.0.2.0
 Fixed version     : 15.0.0.0
```

72658 - Serv-U FTP Server < 15.0.1.20 DoS

Synopsis

The remote FTP server is affected by a denial of service vulnerability.

Description

According to its banner, the installed version of Serv-U is a version prior to version 15.0.1.20. It is, therefore, affected by an unspecified denial of service vulnerability.

See Also

http://www.serv-u.com/releasenotes/

Solution

Upgrade to Serv-U version 15.0.1.20 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	65698
XREF	OSVDB:103602

Plugin Information:

Published: 2014/02/24, Modified: 2014/02/24

Plugin Output

tcp/21

```
  Version source    : 200 Name=Serv-U; Version=14.0.2.0; OS=Windows 7; OSVer=6.1.7601;
 CaseSensitive=0;
  Installed version : 14.0.2.0
  Fixed version     : 15.0.1.20
```

72658 - Serv-U FTP Server < 15.0.1.20 DoS

Synopsis

The remote FTP server is affected by a denial of service vulnerability.

Description

According to its banner, the installed version of Serv-U is a version prior to version 15.0.1.20. It is, therefore, affected by an unspecified denial of service vulnerability.

See Also

http://www.serv-u.com/releasenotes/

Solution

Upgrade to Serv-U version 15.0.1.20 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	65698
XREF	OSVDB:103602

Plugin Information:

Published: 2014/02/24, Modified: 2014/02/24

Plugin Output

tcp/990

```
  Version source    : 200 Name=Serv-U; Version=14.0.2.0; OS=Windows 7; OSVer=6.1.7601;
 CaseSensitive=0;
  Installed version : 14.0.2.0
  Fixed version     : 15.0.1.20
```

76369 - Serv-U FTP Server < 15.1.0.458 Multiple Vulnerabilities

Synopsis

The remote FTP server is affected by multiple vulnerabilities.

Description

According to its banner, the installed version of Serv-U is a version prior to 15.1.0.458. It is, therefore, affected by a cross-site scripting vulnerability, an information-disclosure vulnerability, and multiple unspecified security vulnerabilities.

See Also

http://www.serv-u.com/releasenotes/

Solution

Upgrade to Serv-U 15.1.0.458 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

5.6 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	67826
XREF	OSVDB:107733
XREF	OSVDB:107734
XREF	OSVDB:107735
XREF	OSVDB:107736
XREF	OSVDB:107737
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712

XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information:

Published: 2014/07/04, Modified: 2015/02/13

Plugin Output

tcp/21

```
 Version source    : 200 Name=Serv-U; Version=14.0.2.0; OS=Windows 7; OSVer=6.1.7601;
CaseSensitive=0;
 Installed version : 14.0.2.0
 Fixed version     : 15.1.0.458
```

76369 - Serv-U FTP Server < 15.1.0.458 Multiple Vulnerabilities

Synopsis

The remote FTP server is affected by multiple vulnerabilities.

Description

According to its banner, the installed version of Serv-U is a version prior to 15.1.0.458. It is, therefore, affected by a cross-site scripting vulnerability, an information-disclosure vulnerability, and multiple unspecified security vulnerabilities.

See Also

http://www.serv-u.com/releasenotes/

Solution

Upgrade to Serv-U 15.1.0.458 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

5.6 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	67826
XREF	OSVDB:107733
XREF	OSVDB:107734
XREF	OSVDB:107735
XREF	OSVDB:107736
XREF	OSVDB:107737
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712

XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information:

Published: 2014/07/04, Modified: 2015/02/13

Plugin Output

tcp/990

```
 Version source    : 200 Name=Serv-U; Version=14.0.2.0; OS=Windows 7; OSVer=6.1.7601;
CaseSensitive=0;
 Installed version : 14.0.2.0
 Fixed version     : 15.1.0.458
```

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.6 (CVSS2#E:ND/RL:ND/RC:ND)

References

BID	32319
CVE	CVE-2008-5161
XREF	OSVDB:50035
XREF	OSVDB:50036
XREF	CERT:958563
XREF	CWE:200

Plugin Information:

Published: 2013/10/28, Modified: 2016/05/12

Plugin Output

tcp/22

```

The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
  rijndael128-cbc
  rijndael192-cbc
  rijndael256-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
  rijndael128-cbc
  rijndael192-cbc
  rijndael256-cbc
```

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS Base Score

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

Plugin Information:

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-sha1-96
  hmac-sha2-256-96
  hmac-sha2-512-96

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-sha1-96
  hmac-sha2-256-96
  hmac-sha2-512-96
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.2 (CVSS2#E:F/RL:TF/RC:ND)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808
XREF	OSVDB:91162
XREF	OSVDB:117855

Plugin Information:

Published: 2013/04/05, Modified: 2018/01/29

Plugin Output

tcp/21

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.2 (CVSS2#E:F/RL:TF/RC:ND)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808
XREF	OSVDB:91162
XREF	OSVDB:117855

Plugin Information:

Published: 2013/04/05, Modified: 2018/01/29

Plugin Output

tcp/443

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.2 (CVSS2#E:F/RL:TF/RC:ND)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808
XREF	OSVDB:91162
XREF	OSVDB:117855

Plugin Information:

Published: 2013/04/05, Modified: 2018/01/29

Plugin Output

tcp/990

```

List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/10/12, Modified: 2018/02/12

Plugin Output

tcp/21

```
The remote FTP banner is :

220 Serv-U FTP Server v14.0 ready...
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/10/12, Modified: 2018/02/12

Plugin Output

tcp/990

```

The remote FTP banner is :

220 Serv-U FTP Server v14.0 ready...
```

42149 - FTP Service AUTH TLS Command Support

Synopsis

The remote directory service supports encrypting traffic.

Description

The remote FTP service supports the use of the 'AUTH TLS' command to switch from a cleartext to an encrypted communications channel.

See Also

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

https://tools.ietf.org/html/rfc4217

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/10/15, Modified: 2017/06/15

Plugin Output

tcp/21

```

Here is the FTP server's SSL certificate that Nessus was able to
collect after sending a 'AUTH TLS' command :

------------------------------ snip ------------------------------
Subject Name:

Country: US
State/Province: WI
Locality: Helenville
Organization: Rhino Software, Inc.
Organization Unit: Software Development
Common Name: ftp.Serv-U.com

Issuer Name:

Country: US
State/Province: WI
Locality: Helenville
Organization: Rhino Software, Inc.
Organization Unit: Software Development
Common Name: ftp.Serv-U.com
```

```
Serial Number: 00

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Apr 29 15:53:05 2009 GMT
Not Valid After: Apr 27 15:53:05 2019 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 C2 87 DA 9D 72 FD 62 F5 8E A7 0F 0A 6C A4 B6 96 D4 EA 2C
            76 BA ED 3A 5D 2D EE E8 A8 7F 6F D0 62 CD 11 4E 64 F5 0D 54
            73 D0 3D 12 37 07 8D 8E D0 7F E7 4E BD A4 56 8D 32 D8 44 87
            9F 75 80 DA E7 8A 9C 72 D8 50 36 67 3E F1 E5 FB F4 BF F0 1B
            4E 39 93 BA 32 B5 E0 66 03 06 F3 10 4C 0E 7C 8C 67 F5 35 64
            67 D3 E0 A4 26 F8 42 A9 8E 1E CA 59 18 81 77 67 E1 8E 50 80
            64 18 A0 4B CD F4 FE B3 75
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 2A 1D 4E 32 3D 96 9A DD 3D 59 81 24 5E 4E 64 CB 2F C5 70
           E2 4A EF 8C 97 A8 76 60 94 7D 0C 09 39 A0 9D 19 DA 60 EE 6E
           71 27 A5 46 DF 16 94 36 A2 A1 DD 34 39 3F 65 69 0B A2 59 74
           9A 77 64 E7 BD 27 04 3D 8E 6E 59 29 BE 51 73 D9 36 13 E3 FA
           E2 44 27 8D A0 0D 20 5C 25 7D B8 A5 F3 95 DE DA 45 83 83 80
           AF BF 06 7E 9E 83 82 DC 44 E5 7E C0 D7 ED 0F 54 24 7D E1 ED
           0C 30 58 1D 36 2F 91 67 98

------------------------------ snip ------------------------------
```

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). 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: 2015/07/02

Plugin Output

tcp/443

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

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/80

```
The remote web server type is :

Serv-U/14.0.2.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/443

```
The remote web server type is :

Serv-U/14.0.2.0
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/80

```

Response Code : HTTP/1.0 200 OK

Protocol version : HTTP/1.0
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Server: Serv-U/14.0.2.0
  Date: Mon, 18 Mar 2019 14:08:01 GMT
  Accept-Encoding: deflate
  Connection: close
  X-Frame-Options: sameorigin
  Content-Type: text/html
  Pragma: no-cache
  Cache-Control: no-cache,max-age=0,must-revalidate
  Set-Cookie: Session=; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/
  Content-Length: 37900

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/
loose.dtd"><html><head><title></title><meta http-equiv="Content-Type" content="text/html;
 charset=UTF-8"/><meta http-equiv="X-UA-Compatible" content="IE=9" /><meta name="ROBOTS"
 content="NOINDEX,NOFOLLOW"/><meta name="viewport" content="width=320; initial-scale=1.0; maximum-
scale=1.0; user-scalable=0;"/><meta name="mobileoptimized" content="0"/><meta name="format-
detection" content="telephone=no"/><script type="text/javascript" language="JavaScript">var
```

```
 dtw=false;var qhdb="font-family:Arial,sans-serif !important;font-size:11px;";var hxw=false;var
 mdqb=true;if(parseInt(1)!=1){mdqb=false;}if(0){hxw=true;}var qmv=false;var pdq=false;if(0)
{qmv=true;}if(0){pdq=true;}</script><script type="text/javascript" language="JavaScript" src="/
Common/Scripts/BrowserCheckAW.js"></script><link type="text/css" href="/Common/Style/Dialog.css"
 rel="stylesheet" /><link type="text/css" href="/Web Client/Style/LoginForm.css" rel="stylesheet" /
><link type="text/css" href="/%25CUSTOM_HTML_LOGIN_CSS%25/Web Client/Style/Login.css"
 rel="stylesheet" /><style type="text/css">#UserPlacementRadio .aw-list-item {height: 20px;}.aw-
item-template{height:18px;}</style><script type="text/javascript" language="JavaScript" src="/
Common/Scripts/LayerMenu.js"></script><script type="text/javascript" language="JavaScript">var
 jgwb=navigator.userAgent.toLowerCase();var scp="";if(scp=="")document.title="Serv-U from
 RhinoSoft";var fmdb=false,pxbb=false,kcwb=false,jgpb=false,nfm=false,vjdb=false [...]
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/443

```

Response Code : HTTP/1.0 200 OK

Protocol version : HTTP/1.0
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Server: Serv-U/14.0.2.0
  Date: Mon, 18 Mar 2019 14:08:02 GMT
  Accept-Encoding: deflate
  Connection: close
  X-Frame-Options: sameorigin
  Content-Type: text/html
  Pragma: no-cache
  Cache-Control: no-cache,max-age=0,must-revalidate
  Set-Cookie: Session=; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/
  Content-Length: 37900

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/
loose.dtd"><html><head><title></title><meta http-equiv="Content-Type" content="text/html;
 charset=UTF-8"/><meta http-equiv="X-UA-Compatible" content="IE=9" /><meta name="ROBOTS"
 content="NOINDEX,NOFOLLOW"/><meta name="viewport" content="width=320; initial-scale=1.0; maximum-
scale=1.0; user-scalable=0;"/><meta name="mobileoptimized" content="0"/><meta name="format-
detection" content="telephone=no"/><script type="text/javascript" language="JavaScript">var
```

```
 dtw=false;var qhdb="font-family:Arial,sans-serif !important;font-size:11px;";var hxw=false;var
 mdqb=true;if(parseInt(1)!=1){mdqb=false;}if(0){hxw=true;}var qmv=false;var pdq=false;if(0)
{qmv=true;}if(0){pdq=true;}</script><script type="text/javascript" language="JavaScript" src="/
Common/Scripts/BrowserCheckAW.js"></script><link type="text/css" href="/Common/Style/Dialog.css"
 rel="stylesheet" /><link type="text/css" href="/Web Client/Style/LoginForm.css" rel="stylesheet" /
><link type="text/css" href="/%25CUSTOM_HTML_LOGIN_CSS%25/Web Client/Style/Login.css"
 rel="stylesheet" /><style type="text/css">#UserPlacementRadio .aw-list-item {height: 20px;}.aw-
item-template{height:18px;}</style><script type="text/javascript" language="JavaScript" src="/
Common/Scripts/LayerMenu.js"></script><script type="text/javascript" language="JavaScript">var
 jgwb=navigator.userAgent.toLowerCase();var scp="";if(scp=="")document.title="Serv-U from
 RhinoSoft";var fmdb=false,pxbb=false,kcwb=false,jgpb=false,nfm=false,vjdb=fals [...]
```

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

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Published: 1999/08/01, Modified: 2012/06/18

Plugin Output

icmp/0

```
This host returns invalid timestamps (bigger than 24 hours).
```

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: 2017/05/22

Plugin Output

tcp/21

```
Port 21/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: 2017/05/22

Plugin Output

tcp/22

```
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: 2017/05/22

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: 2017/05/22

Plugin Output

tcp/443

```
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: 2017/05/22

Plugin Output

tcp/990

```
Port 990/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: 2017/05/22

Plugin Output

tcp/45000

```
Port 45000/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.
- Whether credentialed or third-party patch management checks are possible.
- 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: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 7.0.3
Plugin feed version : 201803271415
Scanner edition used : Nessus

ERROR: Your plugins have not been updated since 2018/3/27
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
newest vulnerability checks from Nessus.org.

Scan type : Normal
Scan policy used : Basic Network Scan
```

```
Scanner IP : 192.168.1.189
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2019/3/18 22:02
Scan duration : 2228 sec
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

http://www.openssl.org

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/11/30, Modified: 2013/10/18

Plugin Output

tcp/21

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

http://www.openssl.org

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/11/30, Modified: 2013/10/18

Plugin Output

tcp/990

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information:

Published: 2013/07/08, Modified: 2018/03/13

Plugin Output

tcp/0

```
. You need to take the following action :

[ Serv-U FTP Server < 15.1.0.458 Multiple Vulnerabilities (76369) ]

+ Action to take : Upgrade to Serv-U 15.1.0.458 or later.
```

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: 2017/08/28

Plugin Output

tcp/22

```

Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  diffie-hellman-group1-sha1
  diffie-hellman-group14-sha1

The server supports the following options for server_host_key_algorithms :

  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
  rijndael-cbc@lysator.liu.se
  rijndael128-cbc
  rijndael192-cbc
  rijndael256-cbc

The server supports the following options for encryption_algorithms_server_to_client :
  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
  rijndael-cbc@lysator.liu.se
  rijndael128-cbc
  rijndael192-cbc
  rijndael256-cbc

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-sha1
  hmac-sha1-96
  hmac-sha2-256
  hmac-sha2-256-96
  hmac-sha2-512
  hmac-sha2-512-96

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-sha1
  hmac-sha1-96
  hmac-sha2-256
  hmac-sha2-256-96
  hmac-sha2-512
  hmac-sha2-512-96

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib
```

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

Plugin Information:

Published: 1999/10/12, Modified: 2017/12/19

Plugin Output

tcp/22

```
SSH version : SSH-2.0-Serv-U_14.0.2.0
SSH supported authentication : password,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: 2018/02/15

Plugin Output

tcp/21

```
This port supports SSLv3/TLSv1.0.
```

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: 2018/02/15

Plugin Output

tcp/443

```
This port supports SSLv3/TLSv1.0.
```

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: 2018/02/15

Plugin Output

tcp/990

```
This port supports SSLv3/TLSv1.0.
```

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/21

```

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

|-Subject   : C=US/ST=WI/L=Helenville/O=Rhino Software, Inc./OU=Software Development/CN=ftp.Serv-
U.com
|-Not After : Apr 27 15:53:05 2019 GMT
```

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

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

|-Subject   : C=US/ST=WI/L=Helenville/O=Rhino Software, Inc./OU=Software Development/CN=ftp.Serv-
U.com
|-Not After : Apr 27 15:53:05 2019 GMT
```

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/990

```

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

|-Subject   : C=US/ST=WI/L=Helenville/O=Rhino Software, Inc./OU=Software Development/CN=ftp.Serv-
U.com
|-Not After : Apr 27 15:53:05 2019 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: 2012/04/02

Plugin Output

tcp/21

```

The SSL certificate will expire within 60 days, at
Apr 27 15:53:05 2019 GMT :

  Subject          : C=US, ST=WI, L=Helenville, O=Rhino Software, Inc., OU=Software Development,
 CN=ftp.Serv-U.com
  Issuer           : C=US, ST=WI, L=Helenville, O=Rhino Software, Inc., OU=Software Development,
 CN=ftp.Serv-U.com
  Not valid before : Apr 29 15:53:05 2009 GMT
  Not valid after  : Apr 27 15:53:05 2019 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: 2012/04/02

Plugin Output

tcp/443

```
The SSL certificate will expire within 60 days, at
Apr 27 15:53:05 2019 GMT :

  Subject          : C=US, ST=WI, L=Helenville, O=Rhino Software, Inc., OU=Software Development,
 CN=ftp.Serv-U.com
  Issuer           : C=US, ST=WI, L=Helenville, O=Rhino Software, Inc., OU=Software Development,
 CN=ftp.Serv-U.com
  Not valid before : Apr 29 15:53:05 2009 GMT
  Not valid after  : Apr 27 15:53:05 2019 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: 2012/04/02

Plugin Output

tcp/990

```

The SSL certificate will expire within 60 days, at
Apr 27 15:53:05 2019 GMT :

  Subject          : C=US, ST=WI, L=Helenville, O=Rhino Software, Inc., OU=Software Development,
 CN=ftp.Serv-U.com
  Issuer           : C=US, ST=WI, L=Helenville, O=Rhino Software, Inc., OU=Software Development,
 CN=ftp.Serv-U.com
  Not valid before : Apr 29 15:53:05 2009 GMT
  Not valid after  : Apr 27 15:53:05 2019 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: 2015/12/30

Plugin Output

tcp/21

```
Subject Name:

Country: US
State/Province: WI
Locality: Helenville
Organization: Rhino Software, Inc.
Organization Unit: Software Development
Common Name: ftp.Serv-U.com

Issuer Name:

Country: US
State/Province: WI
Locality: Helenville
Organization: Rhino Software, Inc.
Organization Unit: Software Development
Common Name: ftp.Serv-U.com

Serial Number: 00

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Apr 29 15:53:05 2009 GMT
Not Valid After: Apr 27 15:53:05 2019 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 C2 87 DA 9D 72 FD 62 F5 8E A7 0F 0A 6C A4 B6 96 D4 EA 2C
```

```
            76 BA ED 3A 5D 2D EE E8 A8 7F 6F D0 62 CD 11 4E 64 F5 0D 54
            73 D0 3D 12 37 07 8D 8E D0 7F E7 4E BD A4 56 8D 32 D8 44 87
            9F 75 80 DA E7 8A 9C 72 D8 50 36 67 3E F1 E5 FB F4 BF F0 1B
            4E 39 93 BA 32 B5 E0 66 03 06 F3 10 4C 0E 7C 8C 67 F5 35 64
            67 D3 E0 A4 26 F8 42 A9 8E 1E CA 59 18 81 77 67 E1 8E 50 80
            64 18 A0 4B CD F4 FE B3 75
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 2A 1D 4E 32 3D 96 9A DD 3D 59 81 24 5E 4E 64 CB 2F C5 70
           E2 4A EF 8C 97 A8 76 60 94 7D 0C 09 39 A0 9D 19 DA 60 EE 6E
           71 27 A5 46 DF 16 94 36 A2 A1 DD 34 39 3F 65 69 0B A2 59 74
           9A 77 64 E7 BD 27 04 3D 8E 6E 59 29 BE 51 73 D9 36 13 E3 FA
           E2 44 27 8D A0 0D 20 5C 25 7D B8 A5 F3 95 DE DA 45 83 83 80
           AF BF 06 7E 9E 83 82 DC 44 E5 7E C0 D7 ED 0F 54 24 7D E1 ED
           0C 30 58 1D 36 2F 91 67 98

Fingerprints :

SHA-256 Fingerprint: 23 A1 A4 86 A6 45 41 43 B3 1F D1 DE 0F A4 8F 13 6A 3D C5 4B
                     E1 21 DC 4E B5 0B F2 60 D7 C2 37 9D
SHA-1 Fingerprint: 1E 91 90 86 47 16 96 7D 12 C4 AC 3F 0F 04 98 C2 3C 78 A5 0C
MD5 Fingerprint: ED 84 90 2B D7 B7 00 1A 37 A2 F9 B8 DE 68 B3 45
```

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: 2015/12/30

Plugin Output

tcp/443

```
Subject Name:

Country: US
State/Province: WI
Locality: Helenville
Organization: Rhino Software, Inc.
Organization Unit: Software Development
Common Name: ftp.Serv-U.com

Issuer Name:

Country: US
State/Province: WI
Locality: Helenville
Organization: Rhino Software, Inc.
Organization Unit: Software Development
Common Name: ftp.Serv-U.com

Serial Number: 00

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Apr 29 15:53:05 2009 GMT
Not Valid After: Apr 27 15:53:05 2019 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 C2 87 DA 9D 72 FD 62 F5 8E A7 0F 0A 6C A4 B6 96 D4 EA 2C
```

```
            76 BA ED 3A 5D 2D EE E8 A8 7F 6F D0 62 CD 11 4E 64 F5 0D 54
            73 D0 3D 12 37 07 8D 8E D0 7F E7 4E BD A4 56 8D 32 D8 44 87
            9F 75 80 DA E7 8A 9C 72 D8 50 36 67 3E F1 E5 FB F4 BF F0 1B
            4E 39 93 BA 32 B5 E0 66 03 06 F3 10 4C 0E 7C 8C 67 F5 35 64
            67 D3 E0 A4 26 F8 42 A9 8E 1E CA 59 18 81 77 67 E1 8E 50 80
            64 18 A0 4B CD F4 FE B3 75
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 2A 1D 4E 32 3D 96 9A DD 3D 59 81 24 5E 4E 64 CB 2F C5 70
           E2 4A EF 8C 97 A8 76 60 94 7D 0C 09 39 A0 9D 19 DA 60 EE 6E
           71 27 A5 46 DF 16 94 36 A2 A1 DD 34 39 3F 65 69 0B A2 59 74
           9A 77 64 E7 BD 27 04 3D 8E 6E 59 29 BE 51 73 D9 36 13 E3 FA
           E2 44 27 8D A0 0D 20 5C 25 7D B8 A5 F3 95 DE DA 45 83 83 80
           AF BF 06 7E 9E 83 82 DC 44 E5 7E C0 D7 ED 0F 54 24 7D E1 ED
           0C 30 58 1D 36 2F 91 67 98

Fingerprints :

SHA-256 Fingerprint: 23 A1 A4 86 A6 45 41 43 B3 1F D1 DE 0F A4 8F 13 6A 3D C5 4B
                     E1 21 DC 4E B5 0B F2 60 D7 C2 37 9D
SHA-1 Fingerprint: 1E 91 90 86 47 16 96 7D 12 C4 AC 3F 0F 04 98 C2 3C 78 A5 0C
MD5 Fingerprint: ED 84 90 2B D7 B7 00 1A 37 A2 F9 B8 DE 68 B3 45
```

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: 2015/12/30

Plugin Output

tcp/990

```
Subject Name:

Country: US
State/Province: WI
Locality: Helenville
Organization: Rhino Software, Inc.
Organization Unit: Software Development
Common Name: ftp.Serv-U.com

Issuer Name:

Country: US
State/Province: WI
Locality: Helenville
Organization: Rhino Software, Inc.
Organization Unit: Software Development
Common Name: ftp.Serv-U.com

Serial Number: 00

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Apr 29 15:53:05 2009 GMT
Not Valid After: Apr 27 15:53:05 2019 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 C2 87 DA 9D 72 FD 62 F5 8E A7 0F 0A 6C A4 B6 96 D4 EA 2C
```

```
            76 BA ED 3A 5D 2D EE E8 A8 7F 6F D0 62 CD 11 4E 64 F5 0D 54
            73 D0 3D 12 37 07 8D 8E D0 7F E7 4E BD A4 56 8D 32 D8 44 87
            9F 75 80 DA E7 8A 9C 72 D8 50 36 67 3E F1 E5 FB F4 BF F0 1B
            4E 39 93 BA 32 B5 E0 66 03 06 F3 10 4C 0E 7C 8C 67 F5 35 64
            67 D3 E0 A4 26 F8 42 A9 8E 1E CA 59 18 81 77 67 E1 8E 50 80
            64 18 A0 4B CD F4 FE B3 75
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 2A 1D 4E 32 3D 96 9A DD 3D 59 81 24 5E 4E 64 CB 2F C5 70
           E2 4A EF 8C 97 A8 76 60 94 7D 0C 09 39 A0 9D 19 DA 60 EE 6E
           71 27 A5 46 DF 16 94 36 A2 A1 DD 34 39 3F 65 69 0B A2 59 74
           9A 77 64 E7 BD 27 04 3D 8E 6E 59 29 BE 51 73 D9 36 13 E3 FA
           E2 44 27 8D A0 0D 20 5C 25 7D B8 A5 F3 95 DE DA 45 83 83 80
           AF BF 06 7E 9E 83 82 DC 44 E5 7E C0 D7 ED 0F 54 24 7D E1 ED
           0C 30 58 1D 36 2F 91 67 98

Fingerprints :

SHA-256 Fingerprint: 23 A1 A4 86 A6 45 41 43 B3 1F D1 DE 0F A4 8F 13 6A 3D C5 4B
                     E1 21 DC 4E B5 0B F2 60 D7 C2 37 9D
SHA-1 Fingerprint: 1E 91 90 86 47 16 96 7D 12 C4 AC 3F 0F 04 98 C2 3C 78 A5 0C
MD5 Fingerprint: ED 84 90 2B D7 B7 00 1A 37 A2 F9 B8 DE 68 B3 45
```

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

http://www.openssl.org/docs/apps/ciphers.html

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/21

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

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

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    IDEA-CBC-SHA                 Kx=RSA         Au=RSA      Enc=IDEA-CBC(128)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
```

```
    Enc={symmetric encryption method}
    Mac={message authentication code}
    {export flag}
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

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

Description

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

See Also

http://www.openssl.org/docs/apps/ciphers.html

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/443

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

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

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    IDEA-CBC-SHA                 Kx=RSA         Au=RSA      Enc=IDEA-CBC(128)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
```

```
    Enc={symmetric encryption method}
    Mac={message authentication code}
    {export flag}
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

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

Description

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

See Also

http://www.openssl.org/docs/apps/ciphers.html

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/990

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

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

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    IDEA-CBC-SHA                 Kx=RSA         Au=RSA      Enc=IDEA-CBC(128)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
```

```
    Enc={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/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/02/15

Plugin Output

tcp/21

```

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

SSL Version : TLSv1
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    IDEA-CBC-SHA                 Kx=RSA         Au=RSA      Enc=IDEA-CBC(128)        Mac=SHA1
    RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1


SSL Version : SSLv3
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)
```

```
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    IDEA-CBC-SHA                 Kx=RSA         Au=RSA      Enc=IDEA-CBC(128)        Mac=SHA1
    RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={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/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/02/15

Plugin Output

tcp/443

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

SSL Version : TLSv1
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    IDEA-CBC-SHA                 Kx=RSA         Au=RSA      Enc=IDEA-CBC(128)        Mac=SHA1
    RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1


SSL Version : SSLv3
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)
```

```
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    IDEA-CBC-SHA                 Kx=RSA         Au=RSA      Enc=IDEA-CBC(128)        Mac=SHA1
    RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={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/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/02/15

Plugin Output

tcp/990

```

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

SSL Version : TLSv1
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    IDEA-CBC-SHA                 Kx=RSA         Au=RSA      Enc=IDEA-CBC(128)        Mac=SHA1
    RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1


SSL Version : SSLv3
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)
```

```
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    IDEA-CBC-SHA                 Kx=RSA         Au=RSA      Enc=IDEA-CBC(128)        Mac=SHA1
    RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={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: 2018/03/26

Plugin Output

tcp/21

```
An FTP 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: 2018/03/26

Plugin Output

tcp/22

```
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: 2018/03/26

Plugin Output

tcp/80

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/443

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

tcp/443

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

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: 2018/03/26

Plugin Output

tcp/990

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

tcp/990

```
An FTP server is running on this port through TLSv1.
```

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: 2018/03/26

Plugin Output

tcp/45000

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

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: 2011/03/20

Plugin Output

tcp/0

104743 - 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 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.1 requires that TLS 1.0 be disabled entirely by June 2018, except for point-of-sale terminals and their termination points.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information:

Published: 2017/11/22, Modified: 2017/11/22

Plugin Output

tcp/21

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

104743 - 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 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.1 requires that TLS 1.0 be disabled entirely by June 2018, except for point-of-sale terminals and their termination points.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information:

Published: 2017/11/22, Modified: 2017/11/22

Plugin Output

tcp/443

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

104743 - 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 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.1 requires that TLS 1.0 be disabled entirely by June 2018, except for point-of-sale terminals and their termination points.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information:

Published: 2017/11/22, Modified: 2017/11/22

Plugin Output

tcp/990

```
TLSv1 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: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.189 to 202.197.66.95 :
192.168.1.189
192.168.1.1
202.197.66.95

Hop Count: 2
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/04/28, Modified: 2015/10/13

Plugin Output

tcp/80

```
The following title tag will be used :
Serv-U - Error Occurred
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/04/28, Modified: 2015/10/13

Plugin Output

tcp/443

```
The following title tag will be used :
Serv-U - Error Occurred
```

202.197.66.98

0	0	4	1	31
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Mon Mar 18 22:02:34 2019
End time:	Mon Mar 18 22:13:19 2019

Host Information

IP:	202.197.66.98
OS:	Microsoft Windows Server 2003, Microsoft Windows Vista, Microsoft Windows Server 2008, Microsoft Windows 7, Microsoft Windows Server 2008 R2

Vulnerabilities

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

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

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

Solution

Purchase or generate a proper 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 Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/3389

```

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=Automation2
|-Issuer  : CN=Automation2
```

42873 - SSL Medium Strength Cipher Suites Supported

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/

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2009/11/23, Modified: 2017/09/01

Plugin Output

tcp/3389

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

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

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :
```

```
{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

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 certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/3389

```
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=Automation2
```

42263 - Unencrypted Telnet Server

Synopsis

The remote Telnet server transmits traffic in cleartext.

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution

Disable the Telnet service and use SSH instead.

Risk Factor

Medium

CVSS Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information:

Published: 2009/10/27, Modified: 2015/10/21

Plugin Output

tcp/23

```

Nessus collected the following banner from the remote Telnet server :

------------------------------ snip ------------------------------
............ ...
IP ....: 202.197.66.217
MAC ....:
..........: 2019-03-18 22:07:45
........: .........
------------------------------ snip ------------------------------
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.2 (CVSS2#E:F/RL:TF/RC:ND)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808
XREF	OSVDB:91162
XREF	OSVDB:117855

Plugin Information:

Published: 2013/04/05, Modified: 2018/01/29

Plugin Output

tcp/3389

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=MD5
    RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

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: 2017/06/06

Plugin Output

tcp/0

```

The remote operating system matched the following CPE's :

  cpe:/o:microsoft:windows_2003_server
  cpe:/o:microsoft:windows_vista
  cpe:/o:microsoft:windows_server_2008
  cpe:/o:microsoft:windows_7
  cpe:/o:microsoft:windows_server_2008:r2 -> Microsoft Windows Server 2008 R2
```

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: 2011/05/23

Plugin Output

tcp/0

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

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/80

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/80

```

Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html; charset=us-ascii
  Server: Microsoft-HTTPAPI/2.0
  Date: Mon, 18 Mar 2019 14:10:35 GMT
  Connection: close
  Content-Length: 315

Response Body :

```

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: 2017/05/22

Plugin Output

tcp/23

```
Port 23/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: 2017/05/22

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: 2017/05/22

Plugin Output

tcp/119

```
Port 119/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: 2017/05/22

Plugin Output

tcp/808

```
Port 808/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: 2017/05/22

Plugin Output

tcp/1080

```
Port 1080/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: 2017/05/22

Plugin Output

tcp/2121

```
Port 2121/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: 2017/05/22

Plugin Output

tcp/3389

```
Port 3389/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.
- Whether credentialed or third-party patch management checks are possible.
- 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: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 7.0.3
Plugin feed version : 201803271415
Scanner edition used : Nessus

ERROR: Your plugins have not been updated since 2018/3/27
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
newest vulnerability checks from Nessus.org.

Scan type : Normal
Scan policy used : Basic Network Scan
```

```
Scanner IP : 192.168.1.189
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2019/3/18 22:02
Scan duration : 637 sec
```

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: 2018/01/19

Plugin Output

tcp/0

```

Remote operating system : Microsoft Windows Server 2003
Microsoft Windows Vista
Microsoft Windows Server 2008
Microsoft Windows 7
Microsoft Windows Server 2008 R2
Confidence level : 70
Method : HTTP


The remote host is running one of these operating systems :
Microsoft Windows Server 2003
Microsoft Windows Vista
Microsoft Windows Server 2008
Microsoft Windows 7
Microsoft Windows Server 2008 R2
```

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: 2018/02/15

Plugin Output

tcp/3389

```
This port supports TLSv1.0/TLSv1.1/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/3389

```

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

|-Subject   : CN=Automation2
|-Not After : Apr 20 11:48:11 2019 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: 2012/04/02

Plugin Output

tcp/3389

```
The SSL certificate will expire within 60 days, at
Apr 20 11:48:11 2019 GMT :

  Subject          : CN=Automation2
  Issuer           : CN=Automation2
  Not valid before : Oct 19 11:48:11 2018 GMT
  Not valid after  : Apr 20 11:48:11 2019 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: 2015/12/30

Plugin Output

tcp/3389

```
Subject Name:

Common Name: Automation2

Issuer Name:

Common Name: Automation2

Serial Number: 13 54 5E 01 49 11 FE 84 4C E2 31 F9 26 8C B0 B8

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Oct 19 11:48:11 2018 GMT
Not Valid After: Apr 20 11:48:11 2019 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B0 3E D7 8D 6E 00 E2 A3 29 23 7F 85 15 E1 D5 EE E7 4D 63
            AE CB 0A 90 6E A9 47 CC 56 24 3B CE FF 16 D7 CE 70 21 0A 84
            F6 C4 52 34 B1 E9 5A 4E CE A6 EF E4 EE 68 60 AB 73 90 BF 82
            72 FF E2 54 68 96 6F 23 23 8B 3B 73 59 5B 80 F4 C1 31 6C E3
            27 38 C5 20 19 39 EC 7A D0 FD E5 B8 C7 E5 70 66 45 B0 E6 04
            CD 91 1E E1 91 2B F7 30 ED 94 A1 B7 E7 BE A1 D6 C5 9B 8B 53
            04 41 C1 1A D4 57 C7 16 11 10 7E 76 10 B9 88 A9 F1 10 44 EB
            9E 4F 56 EF 63 F3 E7 3F 32 46 9D 69 40 84 CD 46 84 A6 DE DC
            01 71 08 D2 72 7B FC 9A F2 D3 DE 98 5E 87 55 45 4D 21 45 1C
            1A 1A 57 8B 3C F1 42 DA B5 4F 01 23 39 99 0E D0 A2 C0 99 7E
            0E D0 47 4B DA 06 ED 6F 5C 3A D5 7E A5 1C 27 5D 25 07 C4 A5
            68 48 D7 6B 1C 75 96 50 5D AD B1 DB 12 91 94 FC 3C E9 3E 46
            58 E9 BA 30 73 79 23 F6 29 7D 3E FE 7D BE AB 45 1D
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 3E 37 E2 59 05 37 EB 0C D4 BD DC 74 99 F6 C9 BE 33 CD 3B
           19 85 AB ED C3 78 E6 7C 41 66 FF 7F 9B 3B 4F 67 AA 46 9D 6A
           C3 99 93 50 B9 68 69 F7 11 5A 53 6C 5C 2D 06 C8 9C 9D C3 24
           E9 A0 91 02 1F 1E F8 A6 2B 56 5B 6B 16 BF 37 A3 72 C6 99 BC
           CE 2E D7 2F 45 9E 6B E8 1A FC 24 1D 3E 2D DB B6 0A F4 30 38
           52 3D 06 32 B5 00 D0 88 82 45 F1 ED 90 C6 4F 96 98 07 97 4D
           9C 48 30 79 EE 64 72 5A 10 94 FC 5C DF D4 F0 25 59 13 44 9E
           AA B6 F4 1C 1B E6 B8 AF 01 A9 39 A1 42 45 26 2C D7 A2 1A 1D
           E4 96 B8 28 0E EF C4 66 07 F3 1A 86 97 67 8C E1 88 E9 D2 7A
           63 21 89 E5 58 2C 24 E1 B3 [...]
```

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

http://www.openssl.org/docs/apps/ciphers.html

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/3389

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

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

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA256

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={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/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/02/15

Plugin Output

tcp/3389

```

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)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    DHE-RSA-AES256-SHA384        Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    RSA-AES256-SHA384            Kx=RSA         Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
```

```
      RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1
      ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
      ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
      RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
      RSA-AES256-SHA256            Kx=RSA         Au=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

http://www.openssl.org/docs/apps/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: 2017/06/12

Plugin Output

tcp/3389

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

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    DHE-RSA-AES256-SHA384        Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384

The fields above are :
  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

51891 - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/02/07, Modified: 2013/10/18

Plugin Output

tcp/3389

```
This port supports resuming TLSv1 sessions.
```

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: 2018/03/26

Plugin Output

tcp/80

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

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: 2011/03/20

Plugin Output

tcp/0

104743 - 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 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.1 requires that TLS 1.0 be disabled entirely by June 2018, except for point-of-sale terminals and their termination points.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information:

Published: 2017/11/22, Modified: 2017/11/22

Plugin Output

tcp/3389

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

10281 - Telnet Server Detection

Synopsis

A Telnet server is listening on the remote port.

Description

The remote host is running a Telnet server, a remote terminal server.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information:

Published: 1999/10/12, Modified: 2018/02/12

Plugin Output

tcp/23

```
Here is the banner from the remote Telnet server :

------------------------------ snip ------------------------------
............ ...
IP ....: 202.197.66.217
MAC ....:
..........: 2019-03-18 22:07:45
........: .........
------------------------------ snip ------------------------------
```

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: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.189 to 202.197.66.98 :
192.168.1.189
192.168.1.1
202.197.66.98

Hop Count: 2
```

11154 - Unknown Service Detection: Banner Retrieval

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/11/18, Modified: 2016/03/24

Plugin Output

tcp/119

```
If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

  Port   : 119
  Type   : spontaneous
  Banner :
0x00:  D5 CA BA C5 C8 CF D6 A4 CA A7 B0 DC 20 2E 2E 2E    ............ ...
           0x10:  0D 0A 49 50 20 B5 D8 D6 B7 3A 20 32 30 32 2E 31    ..IP ....: 202.1
           0x20:  39 37 2E 36 36 2E 32 31 37 0D 0A 4D 41 43 20 B5    97.66.217..MAC .
           0x30:  D8 D6 B7 3A 20 0D 0A B7 FE CE F1 B6 CB CA B1 BC    ...: ...........
           0x40:  E4 3A 20 32 30 31 39 2D 30 33 2D 31 38 20 32 32    .: 2019-03-18 22
           0x50:  3A 30 37 3A 32 34 0D 0A D1 E9 D6 A4 BD E1 B9 FB    :07:24..........
           0x60:  3A 20 CE DE D0 A7 D3 C3 BB A7 2E                   : .........
```

11154 - Unknown Service Detection: Banner Retrieval

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/11/18, Modified: 2016/03/24

Plugin Output

tcp/808

```

If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

  Port   : 808
  Type   : spontaneous
  Banner :
0x00:  3C 68 31 3E D5 CA BA C5 C8 CF D6 A4 CA A7 B0 DC    <h1>............
           0x10:  20 2E 2E 2E 3C 2F 68 31 3E 0D 0A 3C 68 32 3E 49     ...</h1>..<h2>I
           0x20:  50 20 B5 D8 D6 B7 3A 20 32 30 32 2E 31 39 37 2E    P ....: 202.197.
           0x30:  36 36 2E 32 31 37 3C 62 72 3E 0D 0A 4D 41 43 20    66.217<br>..MAC
           0x40:  B5 D8 D6 B7 3A 20 3C 62 72 3E 0D 0A B7 FE CE F1    ....: <br>......
           0x50:  B6 CB CA B1 BC E4 3A 20 32 30 31 39 2D 30 33 2D    ......: 2019-03-
           0x60:  31 38 20 32 32 3A 30 37 3A 32 32 3C 62 72 3E 0D    18 22:07:22<br>.
           0x70:  0A D1 E9 D6 A4 BD E1 B9 FB 3A 20 CE DE D0 A7 D3    .........: .....
           0x80:  C3 BB A7 2E 3C 2F 68 32 3E                         ....</h2>

```

11154 - Unknown Service Detection: Banner Retrieval

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/11/18, Modified: 2016/03/24

Plugin Output

tcp/1080

```

If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

  Port   : 1080
  Type   : spontaneous
  Banner :
0x00:  D5 CA BA C5 C8 CF D6 A4 CA A7 B0 DC 20 2E 2E 2E    ............ ...
           0x10:  0D 0A 49 50 20 B5 D8 D6 B7 3A 20 32 30 32 2E 31    ..IP ....: 202.1
           0x20:  39 37 2E 36 36 2E 32 31 37 0D 0A 4D 41 43 20 B5    97.66.217..MAC .
           0x30:  D8 D6 B7 3A 20 0D 0A B7 FE CE F1 B6 CB CA B1 BC    ...: ...........
           0x40:  E4 3A 20 32 30 31 39 2D 30 33 2D 31 38 20 32 32    .: 2019-03-18 22
           0x50:  3A 30 37 3A 32 32 0D 0A D1 E9 D6 A4 BD E1 B9 FB    :07:22..........
           0x60:  3A 20 CE DE D0 A7 D3 C3 BB A7 2E                   : .........

```

11154 - Unknown Service Detection: Banner Retrieval

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/11/18, Modified: 2016/03/24

Plugin Output

tcp/2121

```

If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

  Port   : 2121
  Type   : spontaneous
  Banner :
0x00:  D5 CA BA C5 C8 CF D6 A4 CA A7 B0 DC 20 2E 2E 2E    ............ ...
           0x10:  0D 0A 49 50 20 B5 D8 D6 B7 3A 20 32 30 32 2E 31    ..IP ....: 202.1
           0x20:  39 37 2E 36 36 2E 32 31 37 0D 0A 4D 41 43 20 B5    97.66.217..MAC .
           0x30:  D8 D6 B7 3A 20 0D 0A B7 FE CE F1 B6 CB CA B1 BC    ...: ...........
           0x40:  E4 3A 20 32 30 31 39 2D 30 33 2D 31 38 20 32 32    .: 2019-03-18 22
           0x50:  3A 30 37 3A 32 32 0D 0A D1 E9 D6 A4 BD E1 B9 FB    :07:22..........
           0x60:  3A 20 CE DE D0 A7 D3 C3 BB A7 2E                   : .........

```

10940 - Windows Terminal Services Enabled

Synopsis

The remote Windows host has Terminal Services enabled.

Description

Terminal Services allows a Windows 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 Terminal Services 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: 2017/08/07

Plugin Output

tcp/3389

202.197.66.155

1	0	3	0	26
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Mon Mar 18 22:06:50 2019
End time:	Mon Mar 18 22:10:52 2019

Host Information

Netbios Name:	CSU-I5MB90AEIFG
IP:	202.197.66.155
MAC Address:	00:16:76:05:cf:1c
OS:	Microsoft Windows Server 2003 Service Pack 2

Vulnerabilities

84729 - Microsoft Windows Server 2003 Unsupported Installation Detection

Synopsis

The remote operating system is no longer supported.

Description

The remote host is running Microsoft Windows Server 2003. Support for this operating system by Microsoft ended July 14th, 2015.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.

See Also

http://www.nessus.org/u?c0dbe792

http://www.nessus.org/u?321523eb

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

http://www.nessus.org/u?8dcab5e4

Solution

Upgrade to a version of Windows that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

9.2 (CVSS:3.0/E:F/RL:O/RC:X)

CVSS Base Score

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

CVSS Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:ND)

References

XREF	OSVDB:155633
XREF	EDB-ID:41929

Plugin Information:

Published: 2015/07/14, Modified: 2017/11/21

Plugin Output

tcp/0

90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Synopsis

The remote Windows host is affected by an elevation of privilege vulnerability.

Description

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

See Also

https://technet.microsoft.com/library/security/MS16-047

http://badlock.org/

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.6 (CVSS2#E:F/RL:OF/RC:ND)

STIG Severity

I

References

BID	86002
CVE	CVE-2016-0128
MSKB	3148527
MSKB	3149090

MSKB	3147461
MSKB	3147458
XREF	OSVDB:136339
XREF	MSFT:MS16-047
XREF	CERT:813296
XREF	IAVA:2016-A-0093

Plugin Information:

Published: 2016/04/13, Modified: 2017/08/30

Plugin Output

tcp/1025

26920 - Microsoft Windows SMB NULL Session Authentication

Synopsis

It is possible to log into the remote Windows host with a NULL session.

Description

The remote host is running Microsoft Windows. It is possible to log into it using a NULL session (i.e., with no login or password).

Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.

See Also

http://support.microsoft.com/kb/q143474/

http://support.microsoft.com/kb/q246261/

http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx

Solution

Apply the following registry changes per the referenced Technet advisories :

Set :

- HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1

Remove BROWSER from :

- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes

Reboot once the registry changes are complete.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:U/RL:U/RC:ND)

References

BID	494

CVE	CVE-1999-0519
CVE	CVE-1999-0520
CVE	CVE-2002-1117
XREF	OSVDB:299
XREF	OSVDB:8230

Plugin Information:

Published: 2007/10/04, Modified: 2012/02/29

Plugin Output

tcp/445

```
It was possible to bind to the \browser pipe
```

57608 - SMB Signing Disabled

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

https://support.microsoft.com/en-us/kb/887429

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

http://www.samba.org/samba/docs/man/manpages-3/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 Base Score

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

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information:

Published: 2012/01/19, Modified: 2016/12/09

Plugin Output

tcp/445

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: 2017/06/06

Plugin Output

tcp/0

```

The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_2003_server::sp2 -> Microsoft Windows 2003 Server Service Pack 2
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/08/26, Modified: 2014/05/12

Plugin Output

tcp/135

```

The following DCERPC services are available locally :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Description : Unknown RPC service
Annotation : ICF+ FW API
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Description : Unknown RPC service
Annotation : ICF+ FW API
Type : Local RPC service
Named pipe : keysvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Description : Unknown RPC service
Annotation : ICF+ FW API
```

```
Type : Local RPC service
Named pipe : AudioSrv

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Description : Unknown RPC service
Annotation : ICF+ FW API
Type : Local RPC service
Named pipe : OLE8C0F5DDE7A244CED9D0555E3FD4E

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ac109027-2eb9-4d3e-ab82-d2f8da000d5d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : {533D49E0-1325-4f6a-B887-F038F5DE78BC}

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ac109027-2eb9-4d3e-ab82-d2f8da000d5d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : {8925C90C-6F3F-45AF-98C0-E81886914AA8}

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ac109027-2eb9-4d3e-ab82-d2f8da000d5d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : Dbguard

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0
Description : Telephony service
Windows process : svchost.exe
Annotation : Unimodem LRPC Endpoint
Type : Local RPC se [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/08/26, Modified: 2014/05/12

Plugin Output

tcp/445

```

The following DCERPC services are available remotely :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Description : Unknown RPC service
Annotation : ICF+ FW API
Type : Remote RPC service
Named pipe : \PIPE\ROUTER
Netbios name : \\CSU-I5MB90AEIFG

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Description : Unknown RPC service
Annotation : ICF+ FW API
Type : Remote RPC service
Named pipe : \PIPE\srvsvc
Netbios name : \\CSU-I5MB90AEIFG

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Description : Unknown RPC service
Annotation : ICF+ FW API
Type : Remote RPC service
Named pipe : \pipe\keysvc
Netbios name : \\CSU-I5MB90AEIFG

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
```

```
Description : Unknown RPC service
Annotation : ICF+ FW API
Type : Remote RPC service
Named pipe : \PIPE\wkssvc
Netbios name : \\CSU-I5MB90AEIFG

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Description : Unknown RPC service
Annotation : ICF+ FW API
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\CSU-I5MB90AEIFG

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0
Description : Telephony service
Windows process : svchost.exe
Annotation : Unimodem LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\tapsrv
Netbios name : \\CSU-I5MB90AEIFG

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
Named pipe : \PIPE\lsass
Netbios name : \\CSU-I5MB90AEIFG

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
T [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/08/26, Modified: 2014/05/12

Plugin Output

tcp/1025

```
The following DCERPC services are available on TCP port 1025 :

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 : 1025
IP : 202.197.66.155
```

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: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 99
```

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

http://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: 2017/11/17

Plugin Output

tcp/0

```

The following card manufacturers were identified :

00:16:76:05:cf:1c : Intel Corporate
```

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

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Published: 1999/08/01, Modified: 2012/06/18

Plugin Output

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 -3 seconds.
```

10397 - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

Synopsis

It is possible to obtain network information.

Description

It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

Solution

n/a

Risk Factor

None

References

XREF	OSVDB:300

Plugin Information:

Published: 2000/05/09, Modified: 2015/01/12

Plugin Output

tcp/445

```
Here is the browse list of the remote host :

CSU-I5MB90AEIFG ( os : 5.2 )
LAPTOP-5GELS3JU ( os : 10.0 )
```

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :

- NULL session
- Guest account
- Supplied credentials

See Also

https://support.microsoft.com/kb/143474

https://support.microsoft.com/kb/246261

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/05/09, Modified: 2017/11/06

Plugin Output

tcp/445

```
- NULL sessions are enabled on the remote host.
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/10/17, Modified: 2017/11/30

Plugin Output

tcp/445

```
The remote Operating System is : Windows Server 2003 3790 Service Pack 2
The remote native LAN manager is : Windows Server 2003 5.2
The remote SMB Domain Name is : CSU-I5MB90AEIFG
```

26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\winreg on the remote host.

If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access'

service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/10/04, Modified: 2011/03/27

Plugin Output

tcp/445

```
Could not connect to the registry because:
Could not connect to \winreg
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/06/05, Modified: 2015/06/02

Plugin Output

tcp/139

```

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

11011 - Microsoft Windows SMB Service Detection

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/06/05, Modified: 2015/06/02

Plugin Output

tcp/445

```

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

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2017/06/19, Modified: 2017/06/19

Plugin Output

tcp/445

```

The remote host supports the following versions of SMB :
  SMBv1
```

106716 - Microsoft Windows SMB2 Dialects Supported (remote check)

Synopsis

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

Description

Nessus was able to obtain the set of SMB2 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: 2018/02/09

Plugin Output

tcp/445

```

The remote host does NOT support the following SMB dialects :
 _version_  _introduced in windows version_
 2.0.2      Windows 2008
 2.1        Windows 7
 2.2.2      Windows 8 Beta
 2.2.4      Windows 8 Beta
 3.0        Windows 8
 3.0.2      Windows 8.1
 3.1        Windows 10
 3.1.1      Windows 10
```

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: 2017/05/22

Plugin Output

tcp/135

```
Port 135/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: 2017/05/22

Plugin Output

tcp/139

```
Port 139/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: 2017/05/22

Plugin Output

tcp/445

```
Port 445/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: 2017/05/22

Plugin Output

tcp/1025

```
Port 1025/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.
- Whether credentialed or third-party patch management checks are possible.
- 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: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 7.0.3
Plugin feed version : 201803271415
Scanner edition used : Nessus

ERROR: Your plugins have not been updated since 2018/3/27
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
newest vulnerability checks from Nessus.org.

Scan type : Normal
Scan policy used : Basic Network Scan
```

```
Scanner IP : 192.168.1.189
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2019/3/18 22:06
Scan duration : 237 sec
```

24786 - Nessus Windows Scan Not Performed with Admin Privileges

Synopsis

The Nessus scan of this host may be incomplete due to insufficient privileges provided.

Description

The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.

Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.

If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

Plugin Information:

Published: 2007/03/12, Modified: 2013/01/07

Plugin Output

tcp/0

```
It was not possible to connect to '\\CSU-I5MB90AEIFG\ADMIN$' with the supplied credentials.
```

43815 - 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

udp/137

```

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

  - 202.197.66.155
  - 192.168.0.1
```

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: 2018/01/19

Plugin Output

tcp/0

```

Remote operating system : Microsoft Windows Server 2003 Service Pack 2
Confidence level : 99
Method : MSRPC


The remote host is running Microsoft Windows Server 2003 Service Pack 2
```

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/kb/2696547

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?36fd3072

http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF	OSVDB:151058

Plugin Information:

Published: 2017/02/03, Modified: 2017/02/16

Plugin Output

tcp/445

```
The remote host supports SMBv1.
```

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: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.189 to 202.197.66.155 :
192.168.1.189
192.168.1.1
202.197.66.155

Hop Count: 2
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/10/12, Modified: 2017/09/27

Plugin Output

udp/137

```
The following 6 NetBIOS names have been gathered :

 CSU-I5MB90AEIFG  = Computer name
 WORKGROUP        = Workgroup / Domain name
 CSU-I5MB90AEIFG  = File Server Service
 WORKGROUP        = Browser Service Elections
 WORKGROUP        = Master Browser
 __MSBROWSE__     = Master Browser

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

   00:16:76:05:cf:1c
```

202.197.66.166

0	1	3	0	97
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Mon Mar 18 22:10:52 2019
End time:	Mon Mar 18 22:18:01 2019

Host Information

IP:	202.197.66.166
OS:	Linux Kernel 3.16 on Debian 8.0 (jessie)

Vulnerabilities

10483 - PostgreSQL Default Unpassworded Account

Synopsis

The remote database server can be accessed without a password.

Description

It is possible to connect to the remote PostgreSQL database server using an unpassworded account. This may allow an attacker to launch further attacks against the database.

Solution

Log into this host and set a password for any affected accounts using the 'ALTER USER' command.

In addition, configure the service by editing the file 'pg_hba.conf'

to require a password (or Kerberos) authentication for all remote hosts that have legitimate access to this service and to require a password locally using the line 'local all password'.

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-1999-0508
XREF	OSVDB:382

Exploitable With

Metasploit (true)

Plugin Information:

Published: 2000/07/27, Modified: 2015/09/24

Plugin Output

tcp/5432

```

Nessus was able to log in as the user 'postgres'.

Here is the list of the databases on the remote host :

. ctype
```

12085 - Apache Tomcat Default Files

Synopsis

The remote web server contains default files.

Description

The default error page, default index page, example JSPs, and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

See Also

https://wiki.apache.org/tomcat/FAQ/Miscellaneous#Q6

https://www.owasp.org/index.php/Securing_tomcat

Solution

Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751

XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information:

Published: 2004/03/02, Modified: 2018/01/30

Plugin Output

tcp/85

```
The following default files were found :

/docs/
/examples/servlets/index.html
/examples/jsp/index.html
/examples/websocket/index.xhtml
/nessus-check/default-404-error-page.html
```

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

http://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these methods. Refer to the plugin output for more information.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:H/RL:OF/RC:C)

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:5648

XREF	OSVDB:11408
XREF	OSVDB:50485
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information:

Published: 2003/01/23, Modified: 2016/11/23

Plugin Output

tcp/8090

```

To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus776306427.html HTTP/1.1
Connection: Close
Host: 202.197.66.166
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Mon, 18 Mar 2019 14:17:44 GMT
Server: Apache/2.4.10 (Debian) PHP/5.6.13
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus776306427.html HTTP/1.1
Connection: Keep-Alive
Host: 202.197.66.166
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

```
  ------------------------------ snip ------------------------------
```

12218 - mDNS Detection (Remote Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts that are not on the network segment on which Nessus resides.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2004/04/28, Modified: 2013/05/31

Plugin Output

udp/5353

```
Nessus was able to extract the following information :

  - mDNS hostname       : labserver.local.

  - Advertised services :
    o Service name      : web's remote desktop on labserver._rfb._tcp.local.
      Port number       : 5900
```

18261 - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

n/a

Risk Factor

None

Plugin Information:

Published: 2005/05/15, Modified: 2017/03/13

Plugin Output

tcp/0

```

The Linux distribution detected was :
 - Debian 8.0 (jessie)
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/80

```
URL        : http://202.197.66.166/
Version    : 2.4.99
backported : 1
os         : ConvertedUbuntu
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/81

```
URL        : http://202.197.66.166:81/
Version    : 2.4.99
backported : 1
os         : ConvertedUbuntu
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/82

```
URL        : http://202.197.66.166:82/
Version    : 2.4.99
backported : 1
os         : ConvertedUbuntu
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/83

```
  URL        : http://202.197.66.166:83/
  Version    : 2.4.99
  backported : 1
  os         : ConvertedUbuntu
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/84

```
  URL        : http://202.197.66.166:84/
  Version    : 2.4.99
  backported : 1
  os         : ConvertedUbuntu
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/88

```
URL        : http://202.197.66.166:88/
Version    : 2.4.99
backported : 1
os         : ConvertedUbuntu
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/1664

```
URL        : http://202.197.66.166:1664/
Version    : 2.4.99
backported : 1
os         : ConvertedUbuntu
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/8090

```
URL        : http://202.197.66.166:8090/
Version    : 2.4.99
backported : 1
modules    : PHP/5.6.13
os         : ConvertedDebian
```

39446 - Apache Tomcat Detection

Synopsis

The remote web server is an Apache Tomcat server.

Description

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

See Also

https://tomcat.apache.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/06/18, Modified: 2018/01/24

Plugin Output

tcp/85

```
  URL        : http://202.197.66.166:85/
  Version    : 8.0.37
  backported : 0
  source     : <title>Apache Tomcat/8.0.37
```

84574 - Backported Security Patch Detection (PHP)

Synopsis

Security patches have been backported.

Description

Security patches may have been 'backported' to the remote PHP install 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: 2015/07/07, Modified: 2015/07/07

Plugin Output

tcp/82

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

84574 - Backported Security Patch Detection (PHP)

Synopsis

Security patches have been backported.

Description

Security patches may have been 'backported' to the remote PHP install 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: 2015/07/07, Modified: 2015/07/07

Plugin Output

tcp/84

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

84574 - Backported Security Patch Detection (PHP)

Synopsis

Security patches have been backported.

Description

Security patches may have been 'backported' to the remote PHP install 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: 2015/07/07, Modified: 2015/07/07

Plugin Output

tcp/1664

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

84574 - Backported Security Patch Detection (PHP)

Synopsis

Security patches have been backported.

Description

Security patches may have been 'backported' to the remote PHP install 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: 2015/07/07, Modified: 2015/07/07

Plugin Output

tcp/8090

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

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

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

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP 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/80

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

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP 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/81

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

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP 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/82

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

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP 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/83

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

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP 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/84

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

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP 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/88

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

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP 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/1664

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

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP 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/8090

```
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: 2017/06/06

Plugin Output

tcp/0

```

The remote operating system matched the following CPE :

  cpe:/o:canonical:ubuntu_linux:16.04

Following application CPE's matched on the remote system :

  cpe:/a:openbsd:openssh:7.2
  cpe:/a:apache:http_server:2.4.7 -> Apache Software Foundation Apache HTTP Server 2.4.7
  cpe:/a:apache:http_server:2.4.10 -> Apache Software Foundation Apache HTTP Server 2.4.10
  cpe:/a:php:php:5.6.13 -> PHP PHP 5.6.13
  cpe:/a:php:php:5.5.9 -> PHP 5.5.9
```

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: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 95
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

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.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/12/10, Modified: 2013/05/09

Plugin Output

tcp/80

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

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

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.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/12/10, Modified: 2013/05/09

Plugin Output

tcp/83

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

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

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.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/12/10, Modified: 2013/05/09

Plugin Output

tcp/88

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

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

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.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/12/10, Modified: 2013/05/09

Plugin Output

tcp/3000

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

  - HTTP methods GET HEAD are allowed on :

    /
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

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.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/12/10, Modified: 2013/05/09

Plugin Output

tcp/8081

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

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

    /
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/80

```
The remote web server type is :

Apache/2.4.7 (Ubuntu)
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/81

```
The remote web server type is :

Apache/2.4.7 (Ubuntu)
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/82

```
The remote web server type is :

Apache/2.4.7 (Ubuntu)
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/83

```
The remote web server type is :

Apache/2.4.7 (Ubuntu)
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/84

```
The remote web server type is :

Apache/2.4.7 (Ubuntu)
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/85

```
The remote web server type is :

Apache-Coyote/1.1
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/88

```
The remote web server type is :

Apache/2.4.7 (Ubuntu)
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/1664

```
The remote web server type is :

Apache/2.4.7 (Ubuntu)
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/8090

```
The remote web server type is :

Apache/2.4.10 (Debian) PHP/5.6.13
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/80

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Mon, 18 Mar 2019 14:17:48 GMT
  Server: Apache/2.4.7 (Ubuntu)
  Last-Modified: Fri, 16 Nov 2018 07:44:29 GMT
  ETag: "1223-57ac356525140"
  Accept-Ranges: bytes
  Content-Length: 4643
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :



<!DOCTYPE html>

<html lang="zh">
```

```
<head>

<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<link rel="icon" href="favicon.jpg" type="image/x-icon">
<title>vulstudy</title>
<link rel="stylesheet" type="text/css" href="index.css">
<link rel="stylesheet" href="bootstrap.min.css">
</head>

<body style="background-color: #2e3030;">

<div style="width:240px;height:50px;margin: 0 auto;border: 0px solid #000000;">
<a href="http://github.com/c0ny1/vulstudy" style="text-decoration:none;" target="view_window"><h1
 style="color: #fbcc04;font-size: 60px;">vulstudy</h1></a>
</div>

<div id="Wrapper">

<div id="Box">



<table class="table table-hover" style="width: 90%;margin: 0 auto;font-size: 18px;">
      <thead>
        <tr>
          <th style="text-align: center;color: #7f160e;font-weight: border;font-size:
 22px;">......</th>
          <th style="text-align: center;color: #7f160e;font-weight: border;font-size:
 22px;">............</th>
          <th style="text-align: center;color: #7f160e;font-weight: border;font-size:
 22px;">............</th>
          <th style="text-align: center;color: #7f160e;font-weight: border;font-size:
 22px;">......</th>
          <th style="text-align: center;color: #7f160e;font-weight: border;font-size:
 22px;">......</th>
        </tr>
      </thead>
      <tbody>
        <tr onClick="openURL(':81/')">
          <th scope="row" style="text-align: center;">1</th>
          <td>DVWA</td>
          <td>......</td>
          <td>.. [...]
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/81

```

Response Code : HTTP/1.1 302 Found

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Mon, 18 Mar 2019 14:17:48 GMT
  Server: Apache/2.4.7 (Ubuntu)
  Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
  Pragma: no-cache
  Location: login.php
  Content-Length: 0
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=UTF-8

Response Body :

```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/82

```

Response Code : HTTP/1.1 302 Found

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Mon, 18 Mar 2019 14:17:48 GMT
  Server: Apache/2.4.7 (Ubuntu)
  X-Powered-By: PHP/5.5.9-1ubuntu4.14
  Location: portal.php
  Content-Length: 0
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/83

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Mon, 18 Mar 2019 14:17:48 GMT
  Server: Apache/2.4.7 (Ubuntu)
  Last-Modified: Tue, 15 May 2018 12:01:03 GMT
  ETag: "1efd-56c3d5b3bbdc0"
  Accept-Ranges: bytes
  Content-Length: 7933
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://
www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"><meta http-equiv="Content-Type" content="text/html;
 charset=UTF-8"/><!--This file has been created with freemind2html.xsl--><head><title>SQL
 Injections</title><link rel="stylesheet" href="index.html_files/freemind2html.css" type="text/css"/
```

```
><meta name="generator" content="FreeMind-XSL Stylesheet (see: http://freemind-xsl.dev.slash-me.net/
 for details)"/><script type="text/javascript" src="index.html_files/freemind2html.js">..
 </script><script type="text/javascript"><!--

               function toggle(id)
               {
                   div_el = document.getElementById(id);
                   img_el = document.getElementById('img'+id);
                   if (div_el.style.display != 'none')
                   {


                      div_el.style.display='none';
                      img_el.src = 'index.html_files/show.png';

                   }
                   else
                   {

                      div_el.style.display='block';
                      img_el.src = 'index.html_files/hide.png';

                   };
               };

          -->
</script>
</head>
<body>
<h1><a id="fm_main" href="#fm_imagemap"><font color="#FF0040">SQLi-LABS  Page-1<i>(Basic
 Challenges)</i></font></a></h1>
<a href="sql-connections/setup-db.php"><font color="#E4287C">Setup/reset Database for labs</font></
a></br></br>
<a href= [...]
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/84

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Mon, 18 Mar 2019 14:17:49 GMT
  Server: Apache/2.4.7 (Ubuntu)
  X-Powered-By: PHP/5.5.9-1ubuntu4.24
  Logged-In-User:
  X-XSS-Protection: 0
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Transfer-Encoding: chunked
  Content-Type: text/html

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/1999/REC-
html401-19991224/loose.dtd">
<html>
<head>
 <link rel="shortcut icon" href="./images/favicon.ico" type="image/x-icon" />
 <link rel="stylesheet" type="text/css" href="./styles/global-styles.css" />
```

```
<link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu.css" />
<link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu-v.css" />

<script type="text/javascript" src="./javascript/bookmark-site.js"></script>
<script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmoothmenu.js"></script>
<script type="text/javascript" src="./javascript/ddsmoothmenu/jquery.min.js">
 /***********************************************
 * Smooth Navigational Menu- (c) Dynamic Drive DHTML code library (www.dynamicdrive.com)
 * This notice MUST stay intact for legal use
 * Visit Dynamic Drive at http://www.dynamicdrive.com/ for full source code
 ***********************************************/
</script>
<script type="text/javascript">
 ddsmoothmenu.init({
  mainmenuid: "smoothmenu1", //menu DIV id
  orientation: 'v', //Horizontal or vertical menu: Set to "h" or "v"
  classname: 'ddsmoothmenu', //class added to menu's outer DIV
  //customtheme: ["#cccc44", "#cccccc"],
  contentsource: "markup" //"markup" or ["container_id", "path_to_menu_file"]
 });
</script>
<script type="text/javascript">
 $(function() {
  $('[ReflectedXSSExecutionPoint]').attr("title", "");
  $('[ReflectedXSSExecutionPoint]').balloon();
  $ [...]
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/85

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : GET, HEAD, POST, PUT, DELETE, OPTIONS
Headers :

  Server: Apache-Coyote/1.1
  Content-Type: text/html;charset=UTF-8
  Transfer-Encoding: chunked
  Date: Mon, 18 Mar 2019 14:17:48 GMT
  Connection: close

Response Body :




<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="UTF-8" />
        <title>Apache Tomcat/8.0.37</title>
        <link href="favicon.ico" rel="icon" type="image/x-icon" />
        <link href="favicon.ico" rel="shortcut icon" type="image/x-icon" />
        <link href="tomcat.css" rel="stylesheet" type="text/css" />
    </head>

    <body>
        <div id="wrapper">
            <div id="navigation" class="curved container">
                <span id="nav-home"><a href="http://tomcat.apache.org/">Home</a></span>
                <span id="nav-hosts"><a href="/docs/">Documentation</a></span>
                <span id="nav-config"><a href="/docs/config/">Configuration</a></span>
                <span id="nav-examples"><a href="/examples/">Examples</a></span>
                <span id="nav-wiki"><a href="http://wiki.apache.org/tomcat/FrontPage">Wiki</a></
span>
                <span id="nav-lists"><a href="http://tomcat.apache.org/lists.html">Mailing Lists</
a></span>
                <span id="nav-help"><a href="http://tomcat.apache.org/findhelp.html">Find Help</a></
span>
                <br class="separator" />
            </div>
            <div id="asf-box">
                <h1>Apache Tomcat/8.0.37</h1>
            </div>
            <div id="upper" class="curved container">
                <div id="congrats" class="curved container">
                    <h2>If you're seeing this, you've successfully installed Tomcat.
 Congratulations!</h2>
                </div>
                <div id="notice">
                    <img src="tomcat.png" alt="[tomcat logo]" />
                    <div id="tasks">
                        <h3>Recommended Reading:</h3>
                        <h4><a h [...]
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/88

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Mon, 18 Mar 2019 14:17:49 GMT
  Server: Apache/2.4.7 (Ubuntu)
  Last-Modified: Thu, 29 Nov 2018 08:14:58 GMT
  ETag: "760-57bc947486cd5"
  Accept-Ranges: bytes
  Content-Length: 1888
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<!DOCTYPE html>
<html>
  <head>
    <link rel="stylesheet" href="global.css" type="text/css" />
  </head>
  <body>
```

```
    <div id="main">
      <pre>
##\   ##\  ######\   ######\                  &$\                               &$\     &$\
## |  ## |##  __##\ ##  __##\                 $$ | Version 0.3.1 - by AJ00200  $$ |    \__| GNU GPL
 v3
\##\ ##  |## /  \__|## /  \__| &$$$$$\   &$$$$$$ |&$\   &$\  &$$$$$$\ &$$$$$\ &$$$$$\   &$\  &$$$$$\
  &$$$$$$\
 \####  / \######\  \######\  $$  __$$\ $$  __$$ |$$ |  $$ |$$  _____|\____$$\\_$$  _|  $$ |$$  __$$
\ $$  __$$\
 ##  ##<   \____##\  \____##\ $$$$$$$$ |$$ /  $$ |$$ |  $$ |$$ /      &$$$$$$ | $$ |    $$ |$$ /  $$
 |$$ |  $$ |
##  /\##\ ##\   ## |##\   ## |$$   ____|$$ |  $$ |$$ |  $$ |$$ |     $$  __$$ | $$ |&$\ $$ |$$ |  $$
 |$$ |  $$ |
## /  ## |\######  |\######  |\$$$$$$$\ \$$$$$$$ |\$$$$$$  |\$$$$$$$\\$$$$$$$ | \$$$$  |$$ |\$$$$$$
 |$$ |  $$ |
\__|  \__| \______/  \______/  \_______| \_______| \______/  \_______|\_______|  \____/ \__|
 \______/ \__|  \__|
    </pre>
      <p>XSSeducation is a set of XSS vulnerable PHP pages for testing (and fun, don't forget the
 fun).</p>
      <h3>Level 1</h3>
      <ul>
 <li><a href="basicxss/">Basic XSS</a> - execute code in the page</li>
 <li><a href="javascriptxss/">JavaScript XSS</a> - execute code in the page</li>
      </ul>
      <h3>Level 2</h3>
      <ul>
 <li><a href="filteredxss/">Filtered XSS</a> - alert() the credit card number</li>
      </ul>
      <h3>Level 3</h3>
      <ul>
 <li><a href="chainedxss/">Chained XSS</a> - change the password to 1234, the user must NOT notic
 [...]
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/1664

```

Response Code : HTTP/1.1 302 Found

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Mon, 18 Mar 2019 14:17:49 GMT
  Server: Apache/2.4.7 (Ubuntu)
  X-Powered-By: PHP/5.5.9-1ubuntu4.14
  Location: ./installation/install.php
  Content-Length: 0
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/3000

```

Response Code : HTTP/1.1 302 Found

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  X-Powered-By: Express
  Location: /login?returnurl=/
  Vary: Accept
  Content-Type: text/plain; charset=utf-8
  Content-Length: 40
  Date: Mon, 18 Mar 2019 14:17:49 GMT
  Connection: close

Response Body :

Found. Redirecting to /login?returnurl=/
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/8080

```

Response Code : HTTP/1.1 404

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : GET, HEAD, POST, PUT, DELETE, OPTIONS
Headers :

  Content-Length: 0
  Date: Mon, 18 Mar 2019 14:17:48 GMT
  Connection: close

Response Body :

```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/8081

```

Response Code : HTTP/1.1 404

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : GET, HEAD, POST, PUT, DELETE, OPTIONS
Headers :

  X-Content-Type-Options: nosniff
  X-XSS-Protection: 1; mode=block
  Cache-Control: no-cache, no-store, max-age=0, must-revalidate
  Pragma: no-cache
  Expires: 0
  X-Frame-Options: DENY
  X-Application-Context: application:8081
  Content-Type: text/html;charset=UTF-8
  Content-Language: en
  Content-Length: 306
  Date: Mon, 18 Mar 2019 14:17:48 GMT
  Connection: close

Response Body :
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/8090

```

Response Code : HTTP/1.1 302 Found

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Mon, 18 Mar 2019 14:17:49 GMT
  Server: Apache/2.4.10 (Debian) PHP/5.6.13
  X-Powered-By: PHP/5.6.13
  Location: splash/index.php
  Content-Length: 0
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=UTF-8

Response Body :
```

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

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Published: 1999/08/01, Modified: 2012/06/18

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -95 seconds.
```

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: 2017/05/22

Plugin Output

tcp/22

```
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: 2017/05/22

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: 2017/05/22

Plugin Output

tcp/81

```
Port 81/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: 2017/05/22

Plugin Output

tcp/82

```
Port 82/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: 2017/05/22

Plugin Output

tcp/83

```
Port 83/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: 2017/05/22

Plugin Output

tcp/84

```
Port 84/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: 2017/05/22

Plugin Output

tcp/85

```
Port 85/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: 2017/05/22

Plugin Output

tcp/88

```
Port 88/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: 2017/05/22

Plugin Output

tcp/1664

```
Port 1664/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: 2017/05/22

Plugin Output

tcp/3000

```
Port 3000/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: 2017/05/22

Plugin Output

tcp/5432

```
Port 5432/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: 2017/05/22

Plugin Output

tcp/5900

```
Port 5900/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: 2017/05/22

Plugin Output

tcp/8080

```
Port 8080/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: 2017/05/22

Plugin Output

tcp/8081

```
Port 8081/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: 2017/05/22

Plugin Output

tcp/8090

```
Port 8090/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.
- Whether credentialed or third-party patch management checks are possible.
- 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: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 7.0.3
Plugin feed version : 201803271415
Scanner edition used : Nessus

ERROR: Your plugins have not been updated since 2018/3/27
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
newest vulnerability checks from Nessus.org.

Scan type : Normal
Scan policy used : Basic Network Scan
```

```
Scanner IP : 192.168.1.189
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2019/3/18 22:10
Scan duration : 423 sec
```

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: 2018/01/19

Plugin Output

tcp/0

```

Remote operating system : Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
Confidence level : 95
Method : SSH


The remote host is running Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
```

48243 - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/08/04, Modified: 2017/07/07

Plugin Output

tcp/82

```

Nessus was able to identify the following PHP version information :

  Version : 5.5.9-1ubuntu4.14
  Source  : X-Powered-By: PHP/5.5.9-1ubuntu4.14
```

48243 - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/08/04, Modified: 2017/07/07

Plugin Output

tcp/84

```

Nessus was able to identify the following PHP version information :

  Version : 5.5.9-1ubuntu4.24
  Source  : X-Powered-By: PHP/5.5.9-1ubuntu4.24
```

48243 - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/08/04, Modified: 2017/07/07

Plugin Output

tcp/1664

```
Nessus was able to identify the following PHP version information :

  Version : 5.5.9-1ubuntu4.14
  Source  : X-Powered-By: PHP/5.5.9-1ubuntu4.14
```

48243 - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/08/04, Modified: 2017/07/07

Plugin Output

tcp/8090

```

Nessus was able to identify the following PHP version information :

  Version : 5.6.13
  Source  : Server: Apache/2.4.10 (Debian) PHP/5.6.13
```

26024 - PostgreSQL Server Detection

Synopsis

A database service is listening on the remote host.

Description

The remote service is a PostgreSQL database server, or a derivative such as EnterpriseDB.

See Also

http://www.postgresql.org/

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information:

Published: 2007/09/14, Modified: 2013/02/14

Plugin Output

tcp/5432

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: 2017/08/28

Plugin Output

tcp/22

```

Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha1
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

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

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 encryption_algorithms_server_to_client :
  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_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 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 compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@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: 2017/05/30

Plugin Output

tcp/22

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

  - 1.99
  - 2.0
```

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

Plugin Information:

Published: 1999/10/12, Modified: 2017/12/19

Plugin Output

tcp/22

```
SSH version : SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.6
SSH supported authentication : publickey,password
```

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: 2018/03/26

Plugin Output

tcp/22

```
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: 2018/03/26

Plugin Output

tcp/80

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/81

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/82

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/83

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/84

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/85

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/88

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/1664

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/3000

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/8080

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/8081

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/8090

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

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: 2011/03/20

Plugin Output

tcp/0

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: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.189 to 202.197.66.166 :
192.168.1.189
192.168.1.1
202.197.66.166

Hop Count: 2
```

20108 - Web Server / Application favicon.ico Vendor Fingerprinting

Synopsis

The remote web server contains a graphic image that is prone to information disclosure.

Description

The 'favicon.ico' file found on the remote web server belongs to a popular web server. This may be used to fingerprint the web server.

Solution

Remove the 'favicon.ico' file or create a custom one for your site.

Risk Factor

None

References

XREF	OSVDB:39272

Plugin Information:

Published: 2005/10/28, Modified: 2014/10/14

Plugin Output

tcp/85

```
MD5 fingerprint : 4644f2d45601037b8423d45e13194c93
Web server      : Apache Tomcat or Alfresco Community
```

11422 - Web Server Unconfigured - Default Install Page Present

Synopsis

The remote web server is not configured or is improperly configured.

Description

The remote web server uses its default welcome page. Therefore, it's probable that this server is not used at all or is serving content that is meant to be hidden.

Solution

Disable this service if you do not use it.

Risk Factor

None

References

XREF	OSVDB:3233

Plugin Information:

Published: 2003/03/20, Modified: 2016/03/09

Plugin Output

tcp/85

```
The default welcome page is from Tomcat.
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/wc/exclusion.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

References

XREF	OSVDB:238

Plugin Information:

Published: 1999/10/12, Modified: 2014/05/09

Plugin Output

tcp/81

```
Contents of robots.txt :

User-agent: *
Disallow: /
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/wc/exclusion.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

References

XREF	OSVDB:238

Plugin Information:

Published: 1999/10/12, Modified: 2014/05/09

Plugin Output

tcp/82

```
Contents of robots.txt :

User-agent: GoodBot
Disallow:

User-agent: BadBot
Disallow: /

User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /passwords/
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/wc/exclusion.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

References

XREF	OSVDB:238

Plugin Information:

Published: 1999/10/12, Modified: 2014/05/09

Plugin Output

tcp/84

```
Contents of robots.txt :

User-agent: *
Disallow: passwords/
Disallow: config.inc
Disallow: classes/
Disallow: javascript/
Disallow: owasp-esapi-php/
Disallow: documentation/
Disallow: phpmyadmin/
Disallow: includes/
```

202.197.66.200

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	9	0	28

Scan Information

Start time:	Mon Mar 18 22:13:24 2019
End time:	Mon Mar 18 22:19:55 2019

Host Information

IP:	202.197.66.200
OS:	Mac OS X 10.4, Microsoft Windows 2000, Microsoft Windows XP

Vulnerabilities

12217 - DNS Server Cache Snooping Remote Information Disclosure

Synopsis

The remote DNS server is vulnerable to cache snooping attacks.

Description

The remote DNS server responds to queries for third-party domains that do not have the recursion bit set.

This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.

For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.

Note: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported.

See Also

http://cs.unc.edu/~fabian/course_papers/cache_snooping.pdf

Solution

Contact the vendor of the DNS software for a fix.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2004/04/27, Modified: 2016/12/06

Plugin Output

udp/53

```
Nessus sent a non-recursive query for example.edu
and received 1 answer :

93.184.216.34
```

10539 - DNS Server Recursive Query Cache Poisoning Weakness

Synopsis

The remote name server allows recursive queries to be performed by the host running nessusd.

Description

It is possible to query the remote name server for third-party names.

If this is your internal nameserver, then the attack vector may be limited to employees or guest access if allowed.

If you are probing a remote nameserver, then it allows anyone to use it to resolve third party names (such as www.nessus.org).

This allows attackers to perform cache poisoning attacks against this nameserver.

If the host allows these recursive queries via UDP, then the host can be used to 'bounce' Denial of Service attacks against another network or system.

See Also

http://www.nessus.org/u?c4dcf24a

Solution

Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it).

If you are using bind 8, you can do this by using the instruction 'allow-recursion' in the 'options' section of your named.conf.

If you are using bind 9, you can define a grouping of internal addresses using the 'acl' command.

Then, within the options block, you can explicitly state:

'allow-recursion { hosts_defined_in_acl }'

If you are using another name server, consult its documentation.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:U/RL:U/RC:C)

References

BID	136
BID	678
CVE	CVE-1999-0024
XREF	OSVDB:438
XREF	CERT-CC:CA-1997-22

Plugin Information:

Published: 2000/10/27, Modified: 2016/11/11

Plugin Output

udp/53

35450 - DNS Server Spoofed Request Amplification DDoS

Synopsis

The remote DNS server could be used in a distributed denial of service attack.

Description

The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone ('.') and get an answer that is bigger than the original request. By spoofing the source IP address, a remote attacker can leverage this 'amplification' to launch a denial of service attack against a third-party host using the remote DNS server.

See Also

https://isc.sans.edu/diary/DNS+queries+for+/5713

Solution

Restrict access to your DNS server from public network or reconfigure it to reject such queries.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.1 (CVSS2#E:F/RL:OF/RC:ND)

References

CVE	CVE-2006-0987
XREF	OSVDB:25895

Plugin Information:

Published: 2009/01/22, Modified: 2016/04/28

Plugin Output

udp/53

```
The DNS query was 17 bytes long, the answer is 228 bytes long.
```

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

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

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

Solution

Purchase or generate a proper 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 Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/7000

```
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=YTH
|-Issuer  : CN=YTH
```

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

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

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

Solution

Purchase or generate a proper 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 Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/8989

```
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=DESKTOP-2G4UUG9
|-Issuer  : CN=DESKTOP-2G4UUG9
```

42873 - SSL Medium Strength Cipher Suites Supported

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/

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2009/11/23, Modified: 2017/09/01

Plugin Output

tcp/7000

```

Here is the list of medium strength SSL ciphers supported by the remote server :

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

    DES-CBC3-SHA                 Kx=RSA        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :
```

```
{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported

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/

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2009/11/23, Modified: 2017/09/01

Plugin Output

tcp/8989

```

Here is the list of medium strength SSL ciphers supported by the remote server :

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

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :
```

```
{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

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 certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/7000

```
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=YTH
```

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 certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/8989

```
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=DESKTOP-2G4UUG9
```

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: 2017/06/06

Plugin Output

tcp/0

```

The remote operating system matched the following CPE's :

  cpe:/o:apple:mac_os_x:10.4 -> Apple Mac OS X 10.4
  cpe:/o:microsoft:windows_2000
  cpe:/o:microsoft:windows_xp
```

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

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

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information:

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

tcp/53

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

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

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information:

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

udp/53

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: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 54
```

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

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Published: 1999/08/01, Modified: 2012/06/18

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -2 seconds.
```

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: 2017/05/22

Plugin Output

tcp/53

```
Port 53/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: 2017/05/22

Plugin Output

tcp/7000

```
Port 7000/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: 2017/05/22

Plugin Output

tcp/8989

```
Port 8989/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.
- Whether credentialed or third-party patch management checks are possible.
- 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: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 7.0.3
Plugin feed version : 201803271415
Scanner edition used : Nessus

ERROR: Your plugins have not been updated since 2018/3/27
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
newest vulnerability checks from Nessus.org.

Scan type : Normal
Scan policy used : Basic Network Scan
```

```
Scanner IP : 192.168.1.189
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2019/3/18 22:13
Scan duration : 384 sec
```

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: 2018/01/19

Plugin Output

tcp/0

```

Remote operating system : Mac OS X 10.4
Microsoft Windows 2000
Microsoft Windows XP
Confidence level : 54
Method : SinFP


The remote host is running one of these operating systems :
Mac OS X 10.4
Microsoft Windows 2000
Microsoft Windows XP
```

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: 2018/02/15

Plugin Output

tcp/7000

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

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/12/01, Modified: 2018/02/15

Plugin Output

tcp/8989

```
This port supports TLSv1.0/TLSv1.1/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: 2015/12/30

Plugin Output

tcp/7000

```
Subject Name:

Common Name: YTH

Issuer Name:

Common Name: YTH

Serial Number: 15 30 33 A1 D3 E7 9E 8F 4F 3F D8 05 B2 FB C9 45

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Dec 27 01:12:16 2018 GMT
Not Valid After: Jun 28 01:12:16 2019 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C6 B8 A2 23 22 A3 3B 96 3B 8D B0 34 EB FA 46 96 12 1B 77
            D1 AA 12 E2 47 C5 E2 6A 9E 4F D6 2C B5 3F DD EC FC 3D 80 8E
            9A 6A B4 68 6F 34 A6 B3 58 8F 5B 32 E2 19 D4 D9 3F 4A F9 16
            80 7B CA 47 A7 6A 01 85 C6 2D 90 4B 89 48 AF C9 B5 03 77 9C
            17 1A 49 1D 37 83 99 B9 68 B2 C8 9D 25 01 17 D2 2B 5E D6 24
            0F D0 B4 03 DF 8F C0 FC 50 27 81 7C 1F 4F 55 1E 75 9A 4D 4B
            52 DD 14 46 2A E3 48 09 B8 97 84 02 C3 CF C2 43 9C E1 EA B8
            32 53 2D DF A2 0C 8D 05 48 53 DD 04 89 F5 DB 05 14 D3 DE 70
            6A 7B 70 44 2F D5 0B 0C 18 A1 56 91 36 66 D3 6B 33 04 5C 64
            AC F3 A0 05 22 7B 33 EF 03 61 AE E9 3D B9 9F A4 89 EE E1 97
            91 6F 30 72 F8 BA E6 A5 63 39 A6 3D A6 F2 53 F3 F8 13 A9 F3
            6C D4 B4 4C C5 AE F3 85 2E 96 48 CE ED 25 86 84 00 E5 5A C9
            C0 02 A4 3E 50 4C 52 A6 A4 7A 86 16 73 76 45 54 59
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 13 CC BE 06 84 0C C4 3C 90 7D 0D 75 51 BC 49 9D A9 09 25
           6C 6E B7 B7 C6 3E 5D 43 6F 66 E9 58 7D B7 44 B0 8E 0B 94 B5
           6A 38 41 F2 E9 41 80 17 8D 54 D8 97 70 0D 27 ED 59 02 79 8E
           E2 23 CF F7 A0 AF D0 85 3B C3 06 F9 7F 72 8A 36 CA AA CB EE
           AA 60 17 4C 93 01 DB C3 60 A1 1A F9 ED 2F 52 91 A4 A3 91 45
           03 2B DA 10 D9 C9 9A 5D 72 50 97 66 A1 08 53 EF 12 F2 10 1A
           AE 96 D6 C6 47 7F 32 F5 5B 05 9C A5 CE 1F 97 6D 86 20 CA 3E
           6E 1A 61 4F A7 4C 7B F7 DF AC 9C F7 1A A5 4D 7C 52 BD 10 B7
           A8 26 6C AF E1 EE 50 4F CF 52 7C 22 1F 8C 72 01 40 77 85 F6
           8E 43 24 36 64 B7 63 B5 0D 0E 99 E3 1F F4  [...]
```

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: 2015/12/30

Plugin Output

tcp/8989

```
Subject Name:

Common Name: DESKTOP-2G4UUG9

Issuer Name:

Common Name: DESKTOP-2G4UUG9

Serial Number: 37 86 78 4D C2 21 46 90 46 DB 9A C5 8E 45 AF A4

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 26 12:21:47 2018 GMT
Not Valid After: May 28 12:21:47 2019 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C7 D3 6F 3B A1 88 23 E1 6C 7C 5A E9 81 0A 8B B9 C8 A0 54
            F7 63 67 7B 08 C0 05 1C 49 D7 AD 4E 5A A5 8C 16 1E 1E 2F 6A
            84 6A 25 04 3F DE 23 64 14 0C 1B 8B 30 77 5E 09 24 2F 7D A5
            68 2F 53 39 88 CF F6 4D 21 59 54 DE 4E F6 2E E5 FA 8D 55 D8
            B3 95 B6 10 72 C1 03 EF 19 30 78 8B 87 6A 47 9B F8 AD A4 7F
            9B DA 81 10 52 2C 8B 39 B2 CB 12 66 7E FC E7 FB 2D EA 93 8C
            97 AE CD C7 E3 FC FA 39 C5 DC D0 6D E9 4D 90 DD 00 A2 BC 28
            F4 B0 21 4F 98 F1 BF 12 BD 28 D5 31 C8 EB 03 60 65 48 EC 85
            C1 8A E8 26 8A 70 98 74 4C F3 BB 2F BE CF 74 6E E8 B3 6A F0
            F9 D9 94 53 3D D6 68 64 E1 25 C6 37 E1 AF 49 D1 80 D4 9B 8B
            54 4F 9B 7E 20 2C 5A D9 E4 2C F3 BB 2D 8A 01 6E 8D F1 B6 99
            D5 53 AF 91 07 1E A4 5B 79 07 CD 7B F1 C1 9C 83 64 8D 20 CB
            E3 7A 08 0B C5 88 C3 F0 23 BC DF 1C 13 32 35 62 61
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 C1 CB 97 FD 8E C3 D0 72 50 25 53 30 CA 4E C0 09 E0 F3 34
           0C 35 9C 41 C0 5A DD A5 87 7A 94 B8 1E BF 7F 1F 8C E8 87 8F
           3D 5E EE F7 81 49 B3 AC 94 55 96 9B 7D F5 D6 92 5E B4 00 A1
           C8 92 BB 60 FE 2D DE F2 77 55 AB 50 2B 98 1D 4B 09 26 F4 85
           46 68 0B 63 83 AC 04 E8 11 7E C2 5F EC 23 9E CC AA 03 0E 67
           15 8A 71 CF A1 4F 21 95 60 82 4D 38 AB 49 FF 57 5F BF D2 93
           D4 46 78 A0 FF AF 3C 60 77 75 77 59 E5 81 69 6F 30 4A 90 8C
           8F A2 13 EF 1F 32 2D 27 88 57 50 F1 2A 57 F2 F6 33 B2 AB 2E
           FA 99 D5 B5 FB CE A1 DE 11 A9 1B 34 B1 30 68 15 E0 AF 1C CA
           51 57 E9 E0 7B 6B  [...]
```

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

http://www.openssl.org/docs/apps/ciphers.html

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/7000

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

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

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA256
```

```
The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

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

Description

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

See Also

http://www.openssl.org/docs/apps/ciphers.html

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/8989

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

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

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)         Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)          Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)          Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)          Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)          Mac=SHA1
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)          Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)          Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(128)          Mac=SHA256
    RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(256)          Mac=SHA256
```

```
The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={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/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/02/15

Plugin Output

tcp/7000

```
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)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    DHE-RSA-AES256-SHA384        Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    RSA-AES256-SHA384            Kx=RSA         Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA256


SSL Version : TLSv11
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SH [...]
```

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/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/02/15

Plugin Output

tcp/8989

```

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)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)       Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    DHE-RSA-AES256-SHA384        Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    RSA-AES256-SHA384            Kx=RSA         Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA256


SSL Version : TLSv11
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SH [...]
```

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

http://www.openssl.org/docs/apps/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: 2017/06/12

Plugin Output

tcp/7000

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

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    DHE-RSA-AES256-SHA384        Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
```

```
    Au={authentication}
    Enc={symmetric encryption method}
    Mac={message authentication code}
    {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

http://www.openssl.org/docs/apps/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: 2017/06/12

Plugin Output

tcp/8989

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

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    DHE-RSA-AES256-SHA384        Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
```

```
    Au={authentication}
    Enc={symmetric encryption method}
    Mac={message authentication code}
    {export flag}
```

51891 - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/02/07, Modified: 2013/10/18

Plugin Output

tcp/7000

```
This port supports resuming TLSv1 sessions.
```

51891 - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/02/07, Modified: 2013/10/18

Plugin Output

tcp/8989

```
This port supports resuming TLSv1 sessions.
```

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: 2018/03/26

Plugin Output

tcp/7000

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/8989

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

104743 - 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 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.1 requires that TLS 1.0 be disabled entirely by June 2018, except for point-of-sale terminals and their termination points.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information:

Published: 2017/11/22, Modified: 2017/11/22

Plugin Output

tcp/7000

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

104743 - 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 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.1 requires that TLS 1.0 be disabled entirely by June 2018, except for point-of-sale terminals and their termination points.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information:

Published: 2017/11/22, Modified: 2017/11/22

Plugin Output

tcp/8989

```
TLSv1 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: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.189 to 202.197.66.200 :
192.168.1.189
192.168.1.1
202.197.66.200

Hop Count: 2
```

10940 - Windows Terminal Services Enabled

Synopsis

The remote Windows host has Terminal Services enabled.

Description

Terminal Services allows a Windows 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 Terminal Services 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: 2017/08/07

Plugin Output

tcp/8989

202.197.66.204

1	1	16	3	95
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Mon Mar 18 22:18:01 2019
End time:	Mon Mar 18 22:25:50 2019

Host Information

Netbios Name:	WIN-OSH9IHLQHH8
IP:	202.197.66.204
MAC Address:	00:1b:78:9a:5c:99
OS:	Microsoft Windows Server 2008 R2 Enterprise

Vulnerabilities

97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

See Also

https://technet.microsoft.com/library/security/MS17-010

http://www.nessus.org/u?321523eb

http://www.nessus.org/u?7bec1941

http://www.nessus.org/u?d9f569cf

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/kb/2696547

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?36fd3072

http://www.nessus.org/u?4c7e0cf3

https://github.com/stamparm/EternalRocks/

http://www.nessus.org/u?59db5b5b

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

9.5 (CVSS:3.0/E:F/RL:U/RC:X)

CVSS Base Score

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

CVSS Temporal Score

9.5 (CVSS2#E:F/RL:U/RC:ND)

STIG Severity

l

References

BID	96703
BID	96704
BID	96705
BID	96706
BID	96707
BID	96709
CVE	CVE-2017-0143
CVE	CVE-2017-0144
CVE	CVE-2017-0145
CVE	CVE-2017-0146
CVE	CVE-2017-0147
CVE	CVE-2017-0148
MSKB	4012212
MSKB	4012213
MSKB	4012214
MSKB	4012215
MSKB	4012216
MSKB	4012217
MSKB	4012606
MSKB	4013198
MSKB	4013429
MSKB	4012598
XREF	OSVDB:153673
XREF	OSVDB:153674
XREF	OSVDB:153675
XREF	OSVDB:153676
XREF	OSVDB:153677
XREF	OSVDB:153678
XREF	OSVDB:155620
XREF	OSVDB:155634
XREF	OSVDB:155635
XREF	EDB-ID:41891
XREF	EDB-ID:41987
XREF	MSFT:MS17-010
XREF	IAVA:2017-A-0065

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information:

Published: 2017/03/20, Modified: 2018/03/01

Plugin Output

tcp/445

58435 - MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)

Synopsis

The remote Windows host could allow arbitrary code execution.

Description

An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted.

If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it.

This plugin also checks for a denial of service vulnerability in Microsoft Terminal Server.

Note that this script does not detect the vulnerability if the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting is enabled or the security layer is set to 'SSL (TLS 1.0)' on the remote host.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Note that an extended support contract with Microsoft is required to obtain the patch for this vulnerability for Windows 2000.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

BID	52353
BID	52354
CVE	CVE-2012-0002
CVE	CVE-2012-0152
MSKB	2621440
MSKB	2667402
XREF	OSVDB:80000
XREF	OSVDB:80004
XREF	EDB-ID:18606
XREF	MSFT:MS12-020
XREF	IAVA:2012-A-0039

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information:

Published: 2012/03/22, Modified: 2018/01/29

Plugin Output

tcp/3389

90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Synopsis

The remote Windows host is affected by an elevation of privilege vulnerability.

Description

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

See Also

https://technet.microsoft.com/library/security/MS16-047

http://badlock.org/

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.6 (CVSS2#E:F/RL:OF/RC:ND)

STIG Severity

I

References

BID	86002
CVE	CVE-2016-0128
MSKB	3148527
MSKB	3149090

MSKB	3147461
MSKB	3147458
XREF	OSVDB:136339
XREF	MSFT:MS16-047
XREF	CERT:813296
XREF	IAVA:2016-A-0093

Plugin Information:

Published: 2016/04/13, Modified: 2017/08/30

Plugin Output

tcp/49155

18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

Synopsis

It may be possible to get access to the remote host.

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

See Also

http://www.oxid.it/downloads/rdp-gbu.pdf

http://www.nessus.org/u?e2628096

http://technet.microsoft.com/en-us/library/cc782610.aspx

Solution

- Force the use of SSL as a transport layer for this service if supported, or/and

- Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.6 (CVSS2#E:F/RL:W/RC:ND)

References

BID	13818
CVE	CVE-2005-1794
XREF	OSVDB:17131

Plugin Information:

Published: 2005/06/01, Modified: 2016/11/23

Plugin Output

tcp/3389

57608 - SMB Signing Disabled

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

https://support.microsoft.com/en-us/kb/887429

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

http://www.samba.org/samba/docs/man/manpages-3/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 Base Score

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

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information:

Published: 2012/01/19, Modified: 2016/12/09

Plugin Output

tcp/445

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

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

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

Solution

Purchase or generate a proper 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 Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/443

```
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=WIN-OSH9IHLQHH8
|-Issuer  : CN=WIN-OSH9IHLQHH8
```

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

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

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

Solution

Purchase or generate a proper 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 Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/1433

```
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=SSL_Self_Signed_Fallback
|-Issuer  : CN=SSL_Self_Signed_Fallback
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an 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. An attacker can exploit this to generate another certificate with the same digital signature, allowing an 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 certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?e120eea1

http://technet.microsoft.com/en-us/security/advisory/961509

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	OSVDB:45106
XREF	OSVDB:45108

XREF	OSVDB:45127
XREF	CERT:836068
XREF	CWE:310

Plugin Information:

Published: 2009/01/05, Modified: 2018/02/20

Plugin Output

tcp/1433

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

|-Subject             : CN=SSL_Self_Signed_Fallback
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Feb 27 10:44:10 2019 GMT
|-Valid To            : Feb 27 10:44:10 2049 GMT
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/1433

```

The identities known by Nessus are :

  192.168.137.204
  202.197.66.204
  202.197.66.204

The Common Name in the certificate is :

  SSL_Self_Signed_Fallback
```

42873 - SSL Medium Strength Cipher Suites Supported

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/

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2009/11/23, Modified: 2017/09/01

Plugin Output

tcp/443

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

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

    ECDHE-RSA-DES-CBC3-SHA       Kx=ECDH        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
```

```
The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported

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/

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2009/11/23, Modified: 2017/09/01

Plugin Output

tcp/1433

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

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

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :
```

```
{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

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 certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/443

```
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=WIN-OSH9IHLQHH8
```

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 certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/1433

```
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=SSL_Self_Signed_Fallback
```

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?0bb7b67d

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.1 (with approved cipher suites) or higher instead.

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)

CVSS Base Score

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

Plugin Information:

Published: 2005/10/12, Modified: 2017/07/11

Plugin Output

tcp/1433

```

- SSLv3 is enabled and the server supports at least one cipher.
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	70574
CVE	CVE-2014-3566
XREF	OSVDB:113251
XREF	CERT:577193

Plugin Information:

Published: 2014/10/15, Modified: 2016/11/30

Plugin Output

tcp/1433

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

80035 - TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)

Synopsis

It was possible to obtain sensitive information from the remote host with TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the TLS server not verifying block cipher padding when using a cipher suite that employs a block cipher such as AES and DES. The lack of padding checking can allow encrypted TLS traffic to be decrypted. This vulnerability could allow for the decryption of HTTPS traffic by an unauthorized third party.

See Also

https://www.imperialviolet.org/2014/12/08/poodleagain.html

https://support.f5.com/csp/#/article/K15882

http://www.nessus.org/u?3bcd20bf

Solution

Contact the vendor for an update.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.6 (CVSS2#E:F/RL:OF/RC:C)

References

BID	71549
CVE	CVE-2014-8730
XREF	OSVDB:115590
XREF	OSVDB:115591

Plugin Information:

Published: 2014/12/15

Plugin Output

tcp/1433

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Synopsis

The remote Terminal Services doesn't use Network Level Authentication only.

Description

The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

See Also

http://technet.microsoft.com/en-us/library/cc732713.aspx

http://www.nessus.org/u?e2628096

Solution

Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information:

Published: 2012/03/23, Modified: 2018/01/29

Plugin Output

tcp/3389

```
Nessus was able to negotiate non-NLA (Network Level Authentication) security.
```

57690 - Terminal Services Encryption Level is Medium or Low

Synopsis

The remote host is using weak cryptography.

Description

The remote Terminal Services service is not configured to use strong cryptography.

Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.

Solution

Change RDP encryption level to one of :

3. High

4. FIPS Compliant

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information:

Published: 2012/01/25, Modified: 2018/01/29

Plugin Output

tcp/3389

```
The terminal services encryption level is set to :

2. Medium
```

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Synopsis

The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Description

At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.

Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.

Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

See Also

https://www.cabforum.org/Baseline_Requirements_V1.pdf

Solution

Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Risk Factor

Low

Plugin Information:

Published: 2013/09/03, Modified: 2014/04/10

Plugin Output

tcp/1433

```
The following certificates were part of the certificate chain
sent by the remote host, but contain RSA keys that are considered
to be weak :

|-Subject        : CN=SSL_Self_Signed_Fallback
|-RSA Key Length : 1024 bits
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.2 (CVSS2#E:F/RL:TF/RC:ND)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808
XREF	OSVDB:91162
XREF	OSVDB:117855

Plugin Information:

Published: 2013/04/05, Modified: 2018/01/29

Plugin Output

tcp/1433

```

List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

30218 - Terminal Services Encryption Level is not FIPS-140 Compliant

Synopsis

The remote host is not FIPS-140 compliant.

Description

The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.

Solution

Change RDP encryption level to :

4. FIPS Compliant

Risk Factor

Low

CVSS Base Score

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

Plugin Information:

Published: 2008/02/11, Modified: 2018/01/29

Plugin Output

tcp/3389

```
The terminal services encryption level is set to :

2. Medium (Client Compatible)
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/443

```
URL        : https://202.197.66.204/
Version    : unknown
backported : 0
```

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: 2017/06/06

Plugin Output

tcp/0

```

The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_server_2008:r2::enterprise
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/08/26, Modified: 2014/05/12

Plugin Output

tcp/135

```

The following DCERPC services are available locally :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0186F40

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0186F40

Object UUID : 6d726574-7273-0076-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
```

```
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-008b31a17acf3af402

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000001
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0188E51

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc

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
Annotation : IPSec Policy agent endpoint
Type : Local RPC service
Named pipe : LRPC-29304ddf487d947937

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0
Description : Telephony service
Windows process : svchost.exe
Annotation : Unimodem LRPC Endpoint
Type : Local RPC  [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/08/26, Modified: 2014/05/12

Plugin Output

tcp/445

```
The following DCERPC services are available remotely :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\WIN-OSH9IHLQHH8

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\WIN-OSH9IHLQHH8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0
Description : Telephony service
Windows process : svchost.exe
Annotation : Unimodem LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\tapsrv
Netbios name : \\WIN-OSH9IHLQHH8

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
Named pipe : \pipe\lsass
Netbios name : \\WIN-OSH9IHLQHH8

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
Named pipe : \PIPE\protected_storage
Netbios name : \\WIN-OSH9IHLQHH8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Remote RPC service
Named pipe : \PIPE\W32TIME_ALT
Netbios name : \\WIN-OSH9IHLQHH8

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 : \\WIN-OSH9IHLQHH8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Ty [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/08/26, Modified: 2014/05/12

Plugin Output

tcp/49152

```

The following DCERPC services are available on TCP port 49152 :

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 : 49152
IP : 202.197.66.204

```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/08/26, Modified: 2014/05/12

Plugin Output

tcp/49153

```

The following DCERPC services are available on TCP port 49153 :

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 : 49153
IP : 202.197.66.204

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 202.197.66.204

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 202.197.66.204

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
```

```
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 202.197.66.204
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/08/26, Modified: 2014/05/12

Plugin Output

tcp/49154

```

The following DCERPC services are available on TCP port 49154 :

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 : 49154
IP : 202.197.66.204

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
TCP Port : 49154
IP : 202.197.66.204

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49154
IP : 202.197.66.204

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
```

```
Annotation : XactSrv service
Type : Remote RPC service
TCP Port : 49154
IP : 202.197.66.204

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 202.197.66.204

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49154
IP : 202.197.66.204
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/08/26, Modified: 2014/05/12

Plugin Output

tcp/49155

```
The following DCERPC services are available on TCP port 49155 :

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 : 49155
IP : 202.197.66.204
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/08/26, Modified: 2014/05/12

Plugin Output

tcp/49162

```
The following DCERPC services are available on TCP port 49162 :

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 : 49162
IP : 202.197.66.204
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/08/26, Modified: 2014/05/12

Plugin Output

tcp/49163

```

The following DCERPC services are available on TCP port 49163 :

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 : 49163
IP : 202.197.66.204

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
Annotation : IPSec Policy agent endpoint
Type : Remote RPC service
TCP Port : 49163
IP : 202.197.66.204
```

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: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 99
```

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

http://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: 2017/11/17

Plugin Output

tcp/0

```

The following card manufacturers were identified :

00:1b:78:9a:5c:99 : Hewlett Packard
```

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). 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: 2015/07/02

Plugin Output

tcp/443

```

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

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/80

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/443

```
The remote web server type is :

Apache
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/6666

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/8030

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/8033

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/8080

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/8888

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/8999

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/80

```

Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html; charset=us-ascii
  Server: Microsoft-HTTPAPI/2.0
  Date: Mon, 18 Mar 2019 14:22:22 GMT
  Connection: close
  Content-Length: 315

Response Body :
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/443

```

Response Code : HTTP/1.1 401 Authorization Required

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Mon, 18 Mar 2019 14:22:22 GMT
  Server: Apache
  WWW-Authenticate: Basic realm="VisualSVN Server"
  Content-Length: 401
  Keep-Alive: timeout=5
  Connection: Keep-Alive
  Content-Type: text/html; charset=iso-8859-1

Response Body :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Authorization Required</title>
</head><body>
<h1>Authorization Required</h1>
<p>This server could not verify that you
are authorized to access the document
requested.  Either you supplied the wrong
credentials (e.g., bad password), or your
```

```
browser doesn't understand how to supply
the credentials required.</p>
</body></html>
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/6666

```

Response Code : HTTP/1.1 400 Bad Request

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html; charset=us-ascii
  Server: Microsoft-HTTPAPI/2.0
  Date: Mon, 18 Mar 2019 14:22:22 GMT
  Connection: close
  Content-Length: 334

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Bad Request</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Bad Request - Invalid Hostname</h2>
<hr><p>HTTP Error 400. The request hostname is invalid.</p>
</BODY></HTML>
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/8030

```

Response Code : HTTP/1.1 400 Bad Request

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html; charset=us-ascii
  Server: Microsoft-HTTPAPI/2.0
  Date: Mon, 18 Mar 2019 14:22:22 GMT
  Connection: close
  Content-Length: 334

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Bad Request</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Bad Request - Invalid Hostname</h2>
<hr><p>HTTP Error 400. The request hostname is invalid.</p>
</BODY></HTML>
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/8033

```

Response Code : HTTP/1.1 400 Bad Request

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html; charset=us-ascii
  Server: Microsoft-HTTPAPI/2.0
  Date: Mon, 18 Mar 2019 14:22:22 GMT
  Connection: close
  Content-Length: 334

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Bad Request</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Bad Request - Invalid Hostname</h2>
<hr><p>HTTP Error 400. The request hostname is invalid.</p>
</BODY></HTML>
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/8080

```

Response Code : HTTP/1.1 400 Bad Request

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html; charset=us-ascii
  Server: Microsoft-HTTPAPI/2.0
  Date: Mon, 18 Mar 2019 14:22:22 GMT
  Connection: close
  Content-Length: 334

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Bad Request</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Bad Request - Invalid Hostname</h2>
<hr><p>HTTP Error 400. The request hostname is invalid.</p>
</BODY></HTML>
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/8099

```

Response Code : HTTP/1.1 400 Bad Request

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Headers :

  Content-Type: text/html; charset=us-ascii
  Server: Microsoft-HTTPAPI/2.0
  Date: Mon, 18 Mar 2019 14:22:27 GMT
  Connection: close
  Content-Length: 334

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Bad Request</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Bad Request - Invalid Hostname</h2>
<hr><p>HTTP Error 400. The request hostname is invalid.</p>
</BODY></HTML>
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/8888

```

Response Code : HTTP/1.1 400 Bad Request

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html; charset=us-ascii
  Server: Microsoft-HTTPAPI/2.0
  Date: Mon, 18 Mar 2019 14:22:22 GMT
  Connection: close
  Content-Length: 334

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Bad Request</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Bad Request - Invalid Hostname</h2>
<hr><p>HTTP Error 400. The request hostname is invalid.</p>
</BODY></HTML>
```

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 and HTTP pipelining are 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: 2017/11/13

Plugin Output

tcp/8999

```

Response Code : HTTP/1.1 400 Bad Request

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html; charset=us-ascii
  Server: Microsoft-HTTPAPI/2.0
  Date: Mon, 18 Mar 2019 14:22:22 GMT
  Connection: close
  Content-Length: 334

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Bad Request</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Bad Request - Invalid Hostname</h2>
<hr><p>HTTP Error 400. The request hostname is invalid.</p>
</BODY></HTML>
```

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

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Published: 1999/08/01, Modified: 2012/06/18

Plugin Output

icmp/0

```
This host returns non-standard timestamps (high bit is set)
The ICMP timestamps might be in little endian format (not in network format)
The difference between the local and remote clocks is -371 seconds.
```

69482 - Microsoft SQL Server STARTTLS Support

Synopsis

The remote service supports encrypting traffic.

Description

The remote Microsoft SQL Server service supports the use of encryption initiated during pre-login to switch from a cleartext to an encrypted communications channel.

See Also

http://msdn.microsoft.com/en-us/library/dd304523.aspx

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/07/04, Modified: 2018/03/13

Plugin Output

tcp/1433

```

Here is the Microsoft SQL Server's SSL certificate that Nessus
was able to collect after sending a pre-login packet :

------------------------------ snip ------------------------------
Subject Name:

Common Name: SSL_Self_Signed_Fallback

Issuer Name:

Common Name: SSL_Self_Signed_Fallback

Serial Number: 10 9A 8F E9 06 F7 CB B1 43 A9 2F 16 B8 07 50 02

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Feb 27 10:44:10 2019 GMT
Not Valid After: Feb 27 10:44:10 2049 GMT

Public Key Info:
```

```
Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 B8 37 52 82 03 25 1B 3F 1A E8 03 AA DF 7C AE 6A 1A 8A D0
            49 C2 26 16 85 D6 D0 6E 04 F3 C2 05 3C 92 20 5F 91 60 5C EB
            AC 0D 36 C4 85 26 47 F6 89 D9 AD 8A D5 4A BA 5B 51 C0 BC 2C
            62 1D E2 FD C7 0A 8A 84 F6 6A FE D6 BB BD CB 5F F3 C9 F2 65
            50 E0 09 0D 73 FC CE 95 86 A7 B9 63 21 B4 95 4A 03 F2 D2 8E
            7C 13 DA 5C E8 9D B7 71 14 C3 20 A5 D7 E9 93 BB D7 74 A7 A5
            75 21 AA 3C 67 E7 75 DA AB
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 48 E6 52 15 C3 67 8A D5 DC 59 EE C8 D2 C2 01 B7 2F 5E 4B
           24 4B 76 7F 02 50 79 B7 28 28 9D B1 C9 BF 0C 70 99 0D F1 12
           01 EB FD 46 87 E6 9A E2 30 75 50 6C CF 8F 3A 98 A9 23 B3 A8
           B5 51 BA E1 99 19 49 86 92 AE D6 A4 FF 5E 17 79 B5 44 45 90
           D1 DA E1 BA 32 0E 54 26 33 07 DA 45 F0 18 BF E7 79 99 12 D3
           0C BB 26 E0 6D 6B B0 C6 3A 80 29 C2 D0 38 62 28 F4 75 F4 C2
           AC A2 5E ED 68 0B 2D 16 E8


------------------------------ snip ------------------------------


  SQL Server Version   : 10.0.1600.0
```

10144 - Microsoft SQL Server TCP/IP Listener Detection

Synopsis

A database server is listening on the remote port.

Description

The remote host is running MSSQL, a database server from Microsoft. It is possible to extract the version number of the remote installation from the server pre-login response.

Solution

Restrict access to the database to allowed IPs only.

Risk Factor

None

References

XREF	OSVDB:112

Plugin Information:

Published: 1999/10/12, Modified: 2018/03/13

Plugin Output

tcp/1433

```
The remote SQL Server version is 10.0.1600.0.
```

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :

- NULL session
- Guest account
- Supplied credentials

See Also

https://support.microsoft.com/kb/143474

https://support.microsoft.com/kb/246261

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/05/09, Modified: 2017/11/06

Plugin Output

tcp/445

```
- NULL sessions are enabled on the remote host.
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/10/17, Modified: 2017/11/30

Plugin Output

tcp/445

```
The remote Operating System is : Windows Server 2008 R2 Enterprise 7600
The remote native LAN manager is : Windows Server 2008 R2 Enterprise 6.1
The remote SMB Domain Name is : WIN-OSH9IHLQHH8
```

26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\winreg on the remote host.

If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access'

service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/10/04, Modified: 2011/03/27

Plugin Output

tcp/445

```
Could not connect to the registry because:
Could not connect to \winreg
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/06/05, Modified: 2015/06/02

Plugin Output

tcp/139

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

11011 - Microsoft Windows SMB Service Detection

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/06/05, Modified: 2015/06/02

Plugin Output

tcp/445

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

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2017/06/19, Modified: 2017/06/19

Plugin Output

tcp/445

```

The remote host supports the following versions of SMB :
  SMBv1
  SMBv2
```

106716 - Microsoft Windows SMB2 Dialects Supported (remote check)

Synopsis

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

Description

Nessus was able to obtain the set of SMB2 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: 2018/02/09

Plugin Output

tcp/445

```

The remote host supports the following SMB dialects :
 _version_  _introduced in windows version_
 2.0.2      Windows 2008
 2.1        Windows 7

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
 3.0        Windows 8
 3.0.2      Windows 8.1
 3.1        Windows 10
 3.1.1      Windows 10
```

10719 - MySQL Server Detection

Synopsis

A database server is listening on the remote port.

Description

The remote host is running MySQL, an open source database server.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/08/13, Modified: 2013/01/07

Plugin Output

tcp/3306

```
Version  : 5.7.4-m14
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :
  CLIENT_LONG_PASSWORD (new more secure passwords)
  CLIENT_FOUND_ROWS (Found instead of affected rows)
  CLIENT_LONG_FLAG (Get all column flags)
  CLIENT_CONNECT_WITH_DB (One can specify db on connect)
  CLIENT_NO_SCHEMA (Don't allow database.table.column)
  CLIENT_COMPRESS (Can use compression protocol)
  CLIENT_ODBC (ODBC client)
  CLIENT_LOCAL_FILES (Can use LOAD DATA LOCAL)
  CLIENT_IGNORE_SPACE (Ignore spaces before "("
  CLIENT_PROTOCOL_41 (New 4.1 protocol)
  CLIENT_INTERACTIVE (This is an interactive client)
  CLIENT_SIGPIPE (IGNORE sigpipes)
  CLIENT_TRANSACTIONS (Client knows about transactions)
  CLIENT_RESERVED (Old flag for 4.1 protocol)
  CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

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: 2017/05/22

Plugin Output

tcp/21

```
Port 21/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: 2017/05/22

Plugin Output

tcp/22

```
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: 2017/05/22

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: 2017/05/22

Plugin Output

tcp/135

```
Port 135/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: 2017/05/22

Plugin Output

tcp/139

```
Port 139/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: 2017/05/22

Plugin Output

tcp/443

```
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: 2017/05/22

Plugin Output

tcp/445

```
Port 445/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: 2017/05/22

Plugin Output

tcp/1433

```
Port 1433/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: 2017/05/22

Plugin Output

tcp/2383

```
Port 2383/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: 2017/05/22

Plugin Output

tcp/3306

```
Port 3306/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: 2017/05/22

Plugin Output

tcp/3389

```
Port 3389/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: 2017/05/22

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: 2017/05/22

Plugin Output

tcp/8030

```
Port 8030/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: 2017/05/22

Plugin Output

tcp/8033

```
Port 8033/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: 2017/05/22

Plugin Output

tcp/8080

```
Port 8080/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: 2017/05/22

Plugin Output

tcp/8888

```
Port 8888/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: 2017/05/22

Plugin Output

tcp/8999

```
Port 8999/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.
- Whether credentialed or third-party patch management checks are possible.
- 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: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 7.0.3
Plugin feed version : 201803271415
Scanner edition used : Nessus

ERROR: Your plugins have not been updated since 2018/3/27
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
newest vulnerability checks from Nessus.org.

Scan type : Normal
Scan policy used : Basic Network Scan
```

```
Scanner IP : 192.168.1.189
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2019/3/18 22:18
Scan duration : 463 sec
```

24786 - Nessus Windows Scan Not Performed with Admin Privileges

Synopsis

The Nessus scan of this host may be incomplete due to insufficient privileges provided.

Description

The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.

Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.

If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

Plugin Information:

Published: 2007/03/12, Modified: 2013/01/07

Plugin Output

tcp/0

```
It was not possible to connect to '\\WIN-OSH9IHLQHH8\ADMIN$' with the supplied credentials.
```

43815 - 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

udp/137

```

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

  - 192.168.137.204
  - 202.197.66.204
```

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: 2018/01/19

Plugin Output

tcp/0

```

Remote operating system : Microsoft Windows Server 2008 R2 Enterprise
Confidence level : 99
Method : MSRPC


The remote host is running Microsoft Windows Server 2008 R2 Enterprise
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

http://www.openssl.org

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/11/30, Modified: 2013/10/18

Plugin Output

tcp/443

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information:

Published: 2013/07/08, Modified: 2018/03/13

Plugin Output

tcp/0

```
. You need to take the following action :

[ MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)
 (uncredentialed check) (58435) ]

+ Action to take : Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and
 2008 R2.

Note that an extended support contract with Microsoft is required to obtain the patch for this
 vulnerability for Windows 2000.
```

66173 - RDP Screenshot

Synopsis

It is possible to take a screenshot of the remote login screen.

Description

This script attempts to connect to the remote host via RDP (Remote Desktop Protocol) and attempts to take a screenshot of the login screen.

While this is not a vulnerability by itself, some versions of Windows display the names of the users who can connect and which ones are connected already.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/04/22, Modified: 2018/01/29

Plugin Output

tcp/3389

```
It was possible to gather the following screenshot of the remote login screen.
```

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: 2018/02/15

Plugin Output

tcp/443

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

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/12/01, Modified: 2018/02/15

Plugin Output

tcp/1433

```
This port supports SSLv3/TLSv1.0.
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information:

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/1433

```

The host name known by Nessus is :

  win-osh9ihlqhh8

The Common Name in the certificate is :

  ssl_self_signed_fallback
```

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: 2015/12/30

Plugin Output

tcp/443

```
Subject Name:

Common Name: WIN-OSH9IHLQHH8

Issuer Name:

Common Name: WIN-OSH9IHLQHH8

Serial Number: 00 F0 69 4A 54 C3 73 F0 BE

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Dec 30 00:58:05 2016 GMT
Not Valid After: Dec 28 00:58:05 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B3 53 32 34 6D BD 0B D5 10 A1 3B 6B DC 73 02 F3 05 E2 D0
            FB 99 70 07 47 4B EA 47 AC 26 0B A3 73 18 A5 F3 D2 B3 F3 1E
            3B 43 92 76 86 48 61 B7 A0 5D 86 B9 A5 E9 AA AD 38 16 EC 66
            ED 11 EA 26 E3 ED 01 7A 79 ED E6 4C A9 86 8B 95 A2 16 EC F8
            8E 40 D8 96 EF 27 CB 40 56 F0 D0 D2 1E F0 F7 6A 01 38 6F 03
            A0 80 1E 9F 25 5F 56 45 B5 78 43 EC 3E E0 F1 60 2D 4C DF 48
            CC 10 0C B2 29 83 33 BA D3 F4 B7 10 4A DD CA F6 59 3E 42 90
            66 90 05 F2 91 B0 7E 10 1E 05 55 71 85 0C FE AF FD F5 33 65
            CA BB 39 DC 36 D9 87 70 75 AD 4A 55 B0 D6 2B 21 CB 0B 8B C8
            6B 52 18 91 6F 4B 24 5C 8D 82 F5 DD 8C 1B 9D 1C 61 C6 0D D4
            43 A7 C5 6B 5F 9A FD 43 06 7C 10 63 63 09 6B A3 22 B0 BF AF
            14 46 66 A7 35 06 EA BA 01 90 D9 AE 4D 08 3B 9A DF B8 19 5A
            06 39 48 A6 7D 78 10 43 37 D6 F1 9D C7 A8 FA 48 19
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 15 DC EF 46 19 1B 55 0C 63 D8 DD D3 A8 31 CB 5D 9E 37 53
           5C 35 AD 3E 81 37 EA E6 87 4F 8B 2E A1 9C 5B B4 A6 DC E6 CC
           3C 30 FB D0 E5 A7 BC CC 4E 8F 49 22 4C 26 41 57 A5 49 7D 3C
           B4 1B F7 A2 40 5F C8 21 19 53 2B F8 7C A4 4F 52 80 CE C3 B3
           31 8C 27 18 BD A5 B4 27 B6 9E 1D 46 AD 43 1B 6A 01 9E 9A 7E
           5B 5D 8B A2 02 12 33 99 9E C8 AA 01 E8 A0 0C 08 E7 D2 1E 64
           0F 33 93 FA BB 26 C7 AB 26 C5 17 62 D4 7A 47 78 9A D6 AA 02
           A5 27 F4 61 D7 FE 0D D5 90 36 37 18 66 3B 46 25 BE A5 57 0D
           08 AF 2B 09 C2 2D DB 61 64 B0 2B F9 7E 0F 12 AA D3 87 48 1F
           A7 45 28 F3 82 36 9C 4E 8C 0F E6 20 59  [...]
```

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: 2015/12/30

Plugin Output

tcp/1433

```
Subject Name:

Common Name: SSL_Self_Signed_Fallback

Issuer Name:

Common Name: SSL_Self_Signed_Fallback

Serial Number: 10 9A 8F E9 06 F7 CB B1 43 A9 2F 16 B8 07 50 02

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Feb 27 10:44:10 2019 GMT
Not Valid After: Feb 27 10:44:10 2049 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 B8 37 52 82 03 25 1B 3F 1A E8 03 AA DF 7C AE 6A 1A 8A D0
            49 C2 26 16 85 D6 D0 6E 04 F3 C2 05 3C 92 20 5F 91 60 5C EB
            AC 0D 36 C4 85 26 47 F6 89 D9 AD 8A D5 4A BA 5B 51 C0 BC 2C
            62 1D E2 FD C7 0A 8A 84 F6 6A FE D6 BB BD CB 5F F3 C9 F2 65
            50 E0 09 0D 73 FC CE 95 86 A7 B9 63 21 B4 95 4A 03 F2 D2 8E
            7C 13 DA 5C E8 9D B7 71 14 C3 20 A5 D7 E9 93 BB D7 74 A7 A5
            75 21 AA 3C 67 E7 75 DA AB
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 48 E6 52 15 C3 67 8A D5 DC 59 EE C8 D2 C2 01 B7 2F 5E 4B
```

```
           24 4B 76 7F 02 50 79 B7 28 28 9D B1 C9 BF 0C 70 99 0D F1 12
           01 EB FD 46 87 E6 9A E2 30 75 50 6C CF 8F 3A 98 A9 23 B3 A8
           B5 51 BA E1 99 19 49 86 92 AE D6 A4 FF 5E 17 79 B5 44 45 90
           D1 DA E1 BA 32 0E 54 26 33 07 DA 45 F0 18 BF E7 79 99 12 D3
           0C BB 26 E0 6D 6B B0 C6 3A 80 29 C2 D0 38 62 28 F4 75 F4 C2
           AC A2 5E ED 68 0B 2D 16 E8

Fingerprints :

SHA-256 Fingerprint: A8 64 84 82 90 A0 79 6F 33 AA 53 C8 11 FF 2A 8B 1F 68 F6 45
                     76 66 C4 E6 34 C6 EC 54 35 C1 D0 D1
SHA-1 Fingerprint: EF D5 4B 52 3A 95 64 04 CB C1 92 28 23 8D 0B 37 FB D8 3F 53
MD5 Fingerprint: 7E 72 2C 54 94 3C 8D 2F 57 F7 B2 20 E2 7F 3B 70
```

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

http://www.openssl.org/docs/apps/ciphers.html

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/443

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

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

    ECDHE-RSA-DES-CBC3-SHA       Kx=ECDH        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    DHE-RSA-AES256-SHA256        Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA256
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA256

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

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

Description

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

See Also

http://www.openssl.org/docs/apps/ciphers.html

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/1433

```

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

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

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)         Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)          Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)          Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)          Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)          Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
```

```
    Au={authentication}
    Enc={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/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/02/15

Plugin Output

tcp/443

```
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)

    ECDHE-RSA-DES-CBC3-SHA       Kx=ECDH        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    DHE-RSA-AES256-SHA384        Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    RSA-AES256-SHA384            Kx=RSA         Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
```

```
      DHE-RSA-AES128-SHA256          Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
      DHE-RSA-AES256-SHA256          Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA256
      ECDHE-RSA-AES128-SHA256        Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
      ECDHE-RSA-AES256-SHA384        Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
      RSA-AES128-SHA256              Kx=RSA         Au=RSA    [...]
```

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/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/02/15

Plugin Output

tcp/1433

```

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

SSL Version : TLSv1
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1


SSL Version : SSLv3
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
  High Strength Ciphers (>= 112-bit key)

    RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

http://www.openssl.org/docs/apps/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: 2017/06/12

Plugin Output

tcp/443

```

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

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

    ECDHE-RSA-DES-CBC3-SHA       Kx=ECDH        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    DHE-RSA-AES256-SHA384        Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
```

```
      DHE-RSA-AES256-SHA256        Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA256
      ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
      ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384

  The fields above are :

    {OpenSSL ciphername}
    Kx={key exchange}
    Au={authentication}
    Enc={symmetric encryption method}
    Mac={message authentication code}
    {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

http://www.openssl.org/docs/apps/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: 2017/06/12

Plugin Output

tcp/1433

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

  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

51891 - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/02/07, Modified: 2013/10/18

Plugin Output

tcp/1433

```
This port supports resuming TLSv1 / SSLv3 sessions.
```

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/kb/2696547

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?36fd3072

http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF	OSVDB:151058

Plugin Information:

Published: 2017/02/03, Modified: 2017/02/16

Plugin Output

tcp/445

```
The remote host supports SMBv1.
```

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: 2018/03/26

Plugin Output

tcp/21

```
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: 2018/03/26

Plugin Output

tcp/22

```
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: 2018/03/26

Plugin Output

tcp/80

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/443

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

tcp/443

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

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: 2018/03/26

Plugin Output

tcp/6666

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/8030

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/8033

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/8080

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/8888

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/03/26

Plugin Output

tcp/8999

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

11153 - 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: 2017/06/08

Plugin Output

tcp/3306

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

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: 2011/03/20

Plugin Output

tcp/0

104743 - 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 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.1 requires that TLS 1.0 be disabled entirely by June 2018, except for point-of-sale terminals and their termination points.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information:

Published: 2017/11/22, Modified: 2017/11/22

Plugin Output

tcp/443

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

104743 - 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 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.1 requires that TLS 1.0 be disabled entirely by June 2018, except for point-of-sale terminals and their termination points.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information:

Published: 2017/11/22, Modified: 2017/11/22

Plugin Output

tcp/1433

```
TLSv1 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: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.189 to 202.197.66.204 :
192.168.1.189
192.168.1.1
202.197.66.204

Hop Count: 2
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/10/12, Modified: 2017/09/27

Plugin Output

udp/137

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

 WORKGROUP        = Workgroup / Domain name
 WIN-OSH9IHLQHH8  = Computer name
 WIN-OSH9IHLQHH8  = File Server Service

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

   00:1b:78:9a:5c:99
```

10940 - Windows Terminal Services Enabled

Synopsis

The remote Windows host has Terminal Services enabled.

Description

Terminal Services allows a Windows 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 Terminal Services 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: 2017/08/07

Plugin Output

tcp/3389

202.197.66.249

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	9

Scan Information

Start time:	Mon Mar 18 22:19:55 2019
End time:	Mon Mar 18 22:30:31 2019

Host Information

IP:	202.197.66.249

Vulnerabilities

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: 2017/06/06

Plugin Output

tcp/0

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

  cpe:/a:mysql:mysql:5.6.33
```

10719 - MySQL Server Detection

Synopsis

A database server is listening on the remote port.

Description

The remote host is running MySQL, an open source database server.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/08/13, Modified: 2013/01/07

Plugin Output

tcp/3306

```
Version  : 5.6.33
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities : 
  CLIENT_LONG_PASSWORD (new more secure passwords)
  CLIENT_FOUND_ROWS (Found instead of affected rows)
  CLIENT_LONG_FLAG (Get all column flags)
  CLIENT_CONNECT_WITH_DB (One can specify db on connect)
  CLIENT_NO_SCHEMA (Don't allow database.table.column)
  CLIENT_COMPRESS (Can use compression protocol)
  CLIENT_ODBC (ODBC client)
  CLIENT_LOCAL_FILES (Can use LOAD DATA LOCAL)
  CLIENT_IGNORE_SPACE (Ignore spaces before "("
  CLIENT_PROTOCOL_41 (New 4.1 protocol)
  CLIENT_INTERACTIVE (This is an interactive client)
  CLIENT_SIGPIPE (IGNORE sigpipes)
  CLIENT_TRANSACTIONS (Client knows about transactions)
  CLIENT_RESERVED (Old flag for 4.1 protocol)
  CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

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: 2017/05/22

Plugin Output

tcp/3000

```
Port 3000/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: 2017/05/22

Plugin Output

tcp/3306

```
Port 3306/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.
- Whether credentialed or third-party patch management checks are possible.
- 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: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 7.0.3
Plugin feed version : 201803271415
Scanner edition used : Nessus

ERROR: Your plugins have not been updated since 2018/3/27
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
newest vulnerability checks from Nessus.org.

Scan type : Normal
Scan policy used : Basic Network Scan
```

```
Scanner IP : 192.168.1.189
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2019/3/18 22:20
Scan duration : 625 sec
```

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: 2018/03/26

Plugin Output

tcp/3000

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

11153 - 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: 2017/06/08

Plugin Output

tcp/3306

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

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: 2011/03/20

Plugin Output

tcp/0

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: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.189 to 202.197.66.249 :
192.168.1.189
192.168.1.1
202.197.66.249

Hop Count: 2
```

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 0% of the vulnerabilities on the network.

ACTION TO TAKE	VULNS	HOSTS
Serv-U FTP Server < 15.1.0.458 Multiple Vulnerabilities: Upgrade to Serv-U 15.1.0.458 or later.	0	1