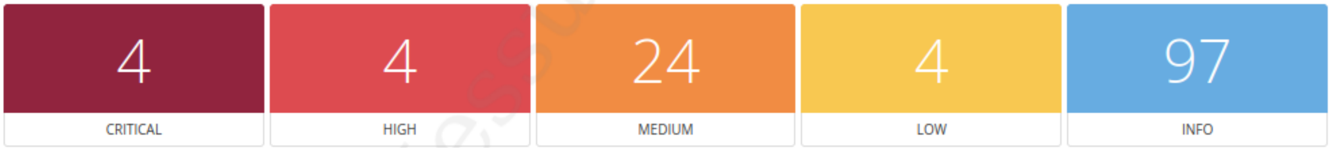
REPORT

Metasploitable Final Scan

Report effettuato da: Anatoliy Prysyazhnyuk

Vulnerabilities by Host

192.168.50.101



4	4	24	4	97
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Jun 2 06:21:02 2023

End time: Fri Jun 2 07:03:54 2023

Host Information

Netbios Name: METASPLOITABLE

IP: 192.168.50.101

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) -

Synopsis

The remote SSL certificate uses a weak key.

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID 29179
CVE CVE-2008-0166
XREF CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/15, Modified: 2020/11/16

Plugin Output

tcp/25/smtp

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) -

Synopsis

The remote SSL certificate uses a weak key.

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID 29179
CVE CVE-2008-0166
XREF CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/15, Modified: 2020/11/16

Plugin Output

tcp/5432/postgresql

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?b06c7e95

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 1.2 (with approved cipher suites) or higher instead.

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 v2.0 Base Score

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

Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

Plugin Output

tcp/25/smtp

```
 - SSLv2 is enabled and the server supports at least one cipher.

  Low Strength Ciphers (<= 64-bit key)

  Name Code KEX Auth Encryption MAC  ---------------------- ---------- --- ---- ---------------------
---  EXP-RC2-CBC-MD5 RSA(512) RSA RC2-CBC(40) MD5  export
 EXP-RC4-MD5 RSA(512) RSA RC4(40) MD5  export

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

  Name Code KEX Auth Encryption MAC  ---------------------- ---------- --- ---- ---------------------
---  DES-CBC3-MD5 RSA RSA 3DES-CBC(168) MD5

  High Strength Ciphers (>= 112-bit key)

  Name Code KEX Auth Encryption MAC  ---------------------- ---------- --- ---- ---------------------
---  RC4-MD5 RSA RSA RC4(128) MD5

The fields above are :

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

 - SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  Low Strength Ciphers (<= 64-bit key)

  Name Code KEX Auth Encryption MAC  ---------------------- ---------- --- ---- ---------------------
---  EXP-EDH-RSA-DES-CBC-SHA DH(512) RSA DES-CBC(40)   SHA1 export
 EDH-RSA-DES-CBC-SHA DH RSA DES-CBC(56) SHA  [...]
```

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?b06c7e95

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 1.2 (with approved cipher suites) or higher instead.

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 v2.0 Base Score

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

Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

Plugin Output

tcp/5432/postgresql

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

```
 Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


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

  Name Code KEX Auth Encryption MAC  ---------------------- ---------- --- ---- ---------------------
 ---  EDH-RSA-DES-CBC3-SHA DH RSA 3DES-CBC(168)   SHA1
  DES-CBC3-SHA RSA RSA 3DES-CBC(168)   SHA1

  High Strength Ciphers (>= 112-bit key)

  Name Code KEX Auth Encryption MAC  ---------------------- ---------- --- ---- ---------------------
 ---  DHE-RSA-AES128-SHA DH RSA AES-CBC(128)   SHA1
  DHE-RSA-AES256-SHA DH RSA AES-CBC(256)   SHA1
  AES128-SHA RSA RSA AES-CBC(128)   SHA1
  AES256-SHA RSA RSA AES-CBC(256)   SHA1
  RC4-SHA RSA RSA RC4(128)   SHA1

 The fields above are :

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

136769 - ISC BIND Service Downgrade / Reflected DoS +

Synopsis

The remote name server is affected by Service Downgrade / Reflected DoS vulnerabilities.

Description

According to its self-reported version, the instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities. This is due to BIND DNS not sufficiently limiting the number fetches which may be performed while processing a referral response.

An unauthenticated, remote attacker can exploit this to cause degrade the service of the recursive server or to use the affected server as a reflector in a reflection attack.

See Also

https://kb.isc.org/docs/cve-2020-8616

Solution

Upgrade to the ISC BIND version referenced in the vendor advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.2

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

References

CVE CVE-2020-8616
XREF IAVA:2020-A-0217-S

Plugin Information

Published: 2020/05/22, Modified: 2020/06/26

Plugin Output

udp/53/dns

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

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

Description

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

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

See Also

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

https://sweet32.info

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

6.1

CVSS v2.0 Base Score

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

References

CVE CVE-2016-2183

Plugin Information

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

tcp/25/smtp

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

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

Description

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

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

See Also

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

https://sweet32.info

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

6.1

CVSS v2.0 Base Score

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

References

CVE CVE-2016-2183

Plugin Information

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

tcp/5432/postgresql

90509 - Samba Badlock Vulnerability +

Synopsis

An SMB server running on the remote host is affected by the Badlock vulnerability.

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists 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 who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

See Also

http://badlock.org

https://www.samba.org/samba/security/CVE-2016-2118.html

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID 86002
CVE CVE-2016-2118
XREF CERT:813296

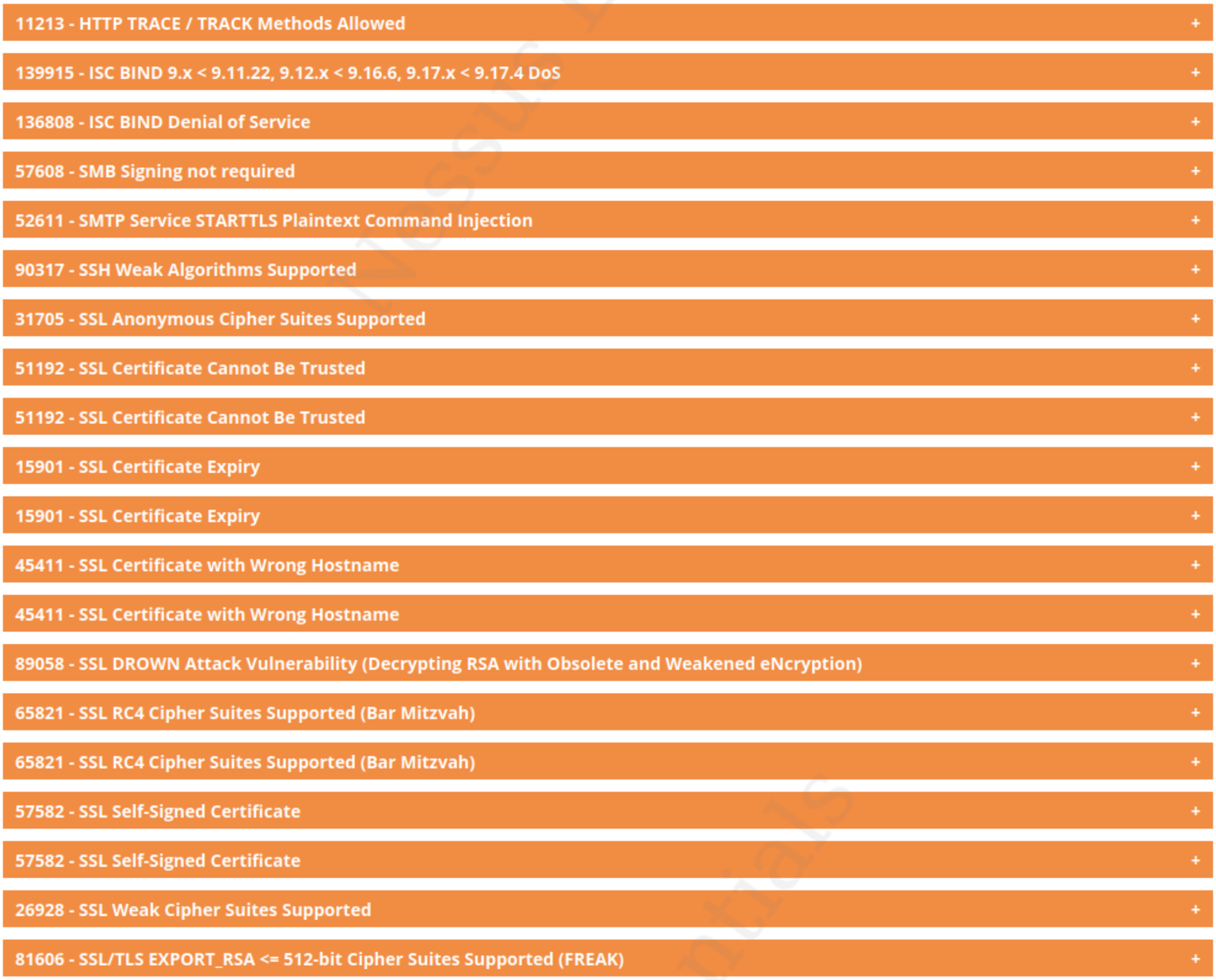
Plugin Information

Published: 2016/04/13, Modified: 2019/11/20

Plugin Output

tcp/445/cifs

Altre criticità:



11213 - HTTP TRACE / TRACK Methods Allowed +
139915 - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS +
136808 - ISC BIND Denial of Service +
57608 - SMB Signing not required +
52611 - SMTP Service STARTTLS Plaintext Command Injection +
90317 - SSH Weak Algorithms Supported +
31705 - SSL Anonymous Cipher Suites Supported +
51192 - SSL Certificate Cannot Be Trusted +
51192 - SSL Certificate Cannot Be Trusted +
15901 - SSL Certificate Expiry +
15901 - SSL Certificate Expiry +
45411 - SSL Certificate with Wrong Hostname +
45411 - SSL Certificate with Wrong Hostname +
89058 - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) +
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) +
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) +
57582 - SSL Self-Signed Certificate +
57582 - SSL Self-Signed Certificate +
26928 - SSL Weak Cipher Suites Supported +
81606 - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK) +

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

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

104743 - TLS Version 1.0 Protocol Detection +

104743 - TLS Version 1.0 Protocol Detection +

70658 - SSH Server CBC Mode Ciphers Enabled +

153953 - SSH Weak Key Exchange Algorithms Enabled +

71049 - SSH Weak MAC Algorithms Enabled +

83738 - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam) +

18261 - Apache Banner Linux Distribution Disclosure +

48204 - Apache HTTP Server Version +

84574 - Backported Security Patch Detection (PHP) +

39520 - Backported Security Patch Detection (SSH) +

39521 - Backported Security Patch Detection (WWW) +

45590 - Common Platform Enumeration (CPE) +

10028 - DNS Server BIND version Directive Remote Version Detection +

11002 - DNS Server Detection +

11002 - DNS Server Detection +

72779 - DNS Server Version Detection +

35371 - DNS Server hostname.bind Map Hostname Disclosure +

54615 - Device Type +

10092 - FTP Server Detection +

10107 - HTTP Server Type and Version +

24260 - HyperText Transfer Protocol (HTTP) Information +

10114 - ICMP Timestamp Request Remote Date Disclosure +

10397 - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure +

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure +

11011 - Microsoft Windows SMB Service Detection +

11011 - Microsoft Windows SMB Service Detection +

11011 - Microsoft Windows SMB Service Detection +

100871 - Microsoft Windows SMB Versions Supported (remote check) +

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) +

11219 - Nessus SYN scanner +

11219 - Nessus SYN scanner +

11219 - Nessus SYN scanner +

11219 - Nessus SYN scanner +

11219 - Nessus SYN scanner +

11219 - Nessus SYN scanner +

11219 - Nessus SYN scanner +

11219 - Nessus SYN scanner +

11219 - Nessus SYN scanner +

11219 - Nessus SYN scanner +

11219 - Nessus SYN scanner +

11219 - Nessus SYN scanner +

11219 - Nessus SYN scanner +

11219 - Nessus SYN scanner +

11219 - Nessus SYN scanner +

11219 - Nessus SYN scanner +

11219 - Nessus SYN scanner +

11219 - Nessus SYN scanner +

19506 - Nessus Scan Information +

11936 - OS Identification +

117886 - OS Security Patch Assessment Not Available +

50845 - OpenSSL Detection +

50845 - OpenSSL Detection +

48243 - PHP Version Detection +

66334 - Patch Report +

118224 - PostgreSQL STARTTLS Support +

26024 - PostgreSQL Server Detection +

22227 - RMI Registry Detection +

11111 - RPC Services Enumeration +

11111 - RPC Services Enumeration +

11111 - RPC Services Enumeration +

11111 - RPC Services Enumeration +

53335 - RPC portmapper (TCP) +

10223 - RPC portmapper Service Detection +

10263 - SMTP Server Detection +

42088 - SMTP Service STARTTLS Command Support +

70657 - SSH Algorithms and Languages Supported +

149334 - SSH Password Authentication Accepted +

10881 - SSH Protocol Versions Supported +

153588 - SSH SHA-1 HMAC Algorithms Enabled +

10267 - SSH Server Type and Version Information +

56984 - SSL / TLS Versions Supported +

56984 - SSL / TLS Versions Supported +

45410 - SSL Certificate 'commonName' Mismatch +

45410 - SSL Certificate 'commonName' Mismatch +

10863 - SSL Certificate Information +

10863 - SSL Certificate Information +

70544 - SSL Cipher Block Chaining Cipher Suites Supported +

70544 - SSL Cipher Block Chaining Cipher Suites Supported +

21643 - SSL Cipher Suites Supported +

21643 - SSL Cipher Suites Supported +

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported +

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported +

51891 - SSL Session Resume Supported +

156899 - SSL/TLS Recommended Cipher Suites +

156899 - SSL/TLS Recommended Cipher Suites +

104887 - Samba Version +

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) +

22964 - Service Detection +

22964 - Service Detection +

22964 - Service Detection +

22964 - Service Detection +

17975 - Service Detection (GET request) +

25220 - TCP/IP Timestamps Supported +

11819 - TFTP Daemon Detection +

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided +

10287 - Traceroute Information +

11154 - Unknown Service Detection: Banner Retrieval +

11154 - Unknown Service Detection: Banner Retrieval +

135860 - WMI Not Available +

11424 - WebDAV Detection +

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure +