



Ubuntu_Simple_Vul_Scan

Report generated by Nessus™

Sat, 06 Apr 2024 10:26:28 EDT

TABLE OF CONTENTS

Vulnerabilities by Plugin

• 84215 (1) - ProFTPD mod_copy Information Disclosure.....	6
• 92626 (1) - Drupal Coder Module Deserialization RCE.....	8
• 42873 (1) - SSL Medium Strength Cipher Suites Supported (SWEET32).....	10
• 78515 (1) - Drupal Database Abstraction API SQLi.....	12
• 10704 (1) - Apache Multiviews Arbitrary Directory Listing.....	14
• 51192 (1) - SSL Certificate Cannot Be Trusted.....	16
• 57582 (1) - SSL Self-Signed Certificate.....	18
• 57608 (1) - SMB Signing not required.....	19
• 90317 (1) - SSH Weak Algorithms Supported.....	21
• 104743 (1) - TLS Version 1.0 Protocol Detection.....	22
• 157288 (1) - TLS Version 1.1 Protocol Deprecated.....	24
• 187315 (1) - SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795).....	26
• 70658 (1) - SSH Server CBC Mode Ciphers Enabled.....	28
• 71049 (1) - SSH Weak MAC Algorithms Enabled.....	30
• 153953 (1) - SSH Weak Key Exchange Algorithms Enabled.....	32
• 10335 (8) - Nessus TCP scanner.....	34
• 22964 (8) - Service Detection.....	36
• 10107 (3) - HTTP Server Type and Version.....	38
• 24260 (2) - HyperText Transfer Protocol (HTTP) Information.....	39
• 43111 (2) - HTTP Methods Allowed (per directory).....	41
• 10092 (1) - FTP Server Detection.....	43
• 10114 (1) - ICMP Timestamp Request Remote Date Disclosure.....	44
• 10150 (1) - Windows NetBIOS / SMB Remote Host Information Disclosure.....	45
• 10180 (1) - Ping the remote host.....	46
• 10267 (1) - SSH Server Type and Version Information.....	47
• 10287 (1) - Traceroute Information.....	48
• 10395 (1) - Microsoft Windows SMB Shares Enumeration.....	49

• 10719 (1) - MySQL Server Detection.....	50
• 10785 (1) - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure.....	51
• 10859 (1) - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration.....	52
• 10860 (1) - SMB Use Host SID to Enumerate Local Users.....	53
• 10863 (1) - SSL Certificate Information.....	54
• 10881 (1) - SSH Protocol Versions Supported.....	56
• 11011 (1) - Microsoft Windows SMB Service Detection.....	57
• 11936 (1) - OS Identification.....	58
• 17651 (1) - Microsoft Windows SMB : Obtains the Password Policy.....	59
• 18261 (1) - Apache Banner Linux Distribution Disclosure.....	60
• 18638 (1) - Drupal Software Detection.....	61
• 19506 (1) - Nessus Scan Information.....	62
• 19689 (1) - Embedded Web Server Detection.....	64
• 20108 (1) - Web Server / Application favicon.ico Vendor Fingerprinting.....	65
• 21643 (1) - SSL Cipher Suites Supported.....	66
• 25220 (1) - TCP/IP Timestamps Supported.....	68
• 25240 (1) - Samba Server Detection.....	69
• 35716 (1) - Ethernet Card Manufacturer Detection.....	70
• 39519 (1) - Backported Security Patch Detection (FTP).....	71
• 39520 (1) - Backported Security Patch Detection (SSH).....	72
• 39521 (1) - Backported Security Patch Detection (WWW).....	73
• 42410 (1) - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure.....	74
• 45410 (1) - SSL Certificate 'commonName' Mismatch.....	75
• 45590 (1) - Common Platform Enumeration (CPE).....	76
• 48204 (1) - Apache HTTP Server Version.....	77
• 54615 (1) - Device Type.....	78
• 56984 (1) - SSL / TLS Versions Supported.....	79
• 60119 (1) - Microsoft Windows SMB Share Permissions Enumeration.....	80
• 66293 (1) - Unix Operating System on Extended Support.....	82

• 66334 (1) - Patch Report.....	83
• 70544 (1) - SSL Cipher Block Chaining Cipher Suites Supported.....	84
• 70657 (1) - SSH Algorithms and Languages Supported.....	86
• 86420 (1) - Ethernet MAC Addresses.....	88
• 96982 (1) - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check).....	89
• 100871 (1) - Microsoft Windows SMB Versions Supported (remote check).....	91
• 104887 (1) - Samba Version.....	92
• 106716 (1) - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check).....	93
• 110723 (1) - Target Credential Status by Authentication Protocol - No Credentials Provided.....	94
• 117886 (1) - OS Security Patch Assessment Not Available.....	96
• 121010 (1) - TLS Version 1.1 Protocol Detection.....	97
• 135860 (1) - WMI Not Available.....	98
• 149334 (1) - SSH Password Authentication Accepted.....	99
• 153588 (1) - SSH SHA-1 HMAC Algorithms Enabled.....	100
• 156899 (1) - SSL/TLS Recommended Cipher Suites.....	101
• 181418 (1) - OpenSSH Detection.....	103

Vulnerabilities by Plugin

84215 (1) - ProFTPD mod_copy Information Disclosure

Synopsis

The remote host is running a ProFTPD module that is affected by an information disclosure vulnerability.

Description

The remote host is running a version of ProFTPD that is affected by an information disclosure vulnerability in the mod_copy module due to the SITE CPFR and SITE CPTO commands being available to unauthenticated clients. An unauthenticated, remote attacker can exploit this flaw to read and write to arbitrary files on any web accessible path on the host.

See Also

http://bugs.proftpd.org/show_bug.cgi?id=4169

Solution

Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later.

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

9.1 (CVSS:3.0/E:F/RL:O/RC:C)

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 74238

CVE	CVE-2015-3306
XREF	EDB-ID:36742
XREF	EDB-ID:36803

Exploitable With

CANVAS (true) Metasploit (true)

Plugin Information

Published: 2015/06/16, Modified: 2024/01/16

Plugin Output

10.0.2.4 (tcp/21/ftp)

```
Nessus received a 350 response from sending the following unauthenticated request :
```

```
SITE CPFR /etc/passwd
```

92626 (1) - Drupal Coder Module Deserialization RCE

Synopsis

A PHP application running on the remote web server is affected by a remote code execution vulnerability.

Description

The version of Drupal running on the remote web server is affected by a remote code execution vulnerability in the Coder module, specifically in file `coder_upgrade.run.php`, due to improper validation of user-supplied input to the `unserialize()` function. An unauthenticated, remote attacker can exploit this, via a specially crafted request, to execute arbitrary PHP code.

See Also

<https://www.drupal.org/node/2765575>

<https://www.drupal.org/project/coder>

Solution

Upgrade the Coder module to version 7.x-1.3 / 7.x-2.6 or later.

Alternatively, remove the entire Coder module directory from any publicly accessible website.

Risk Factor

Critical

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:ND)

References

XREF EDB-ID:40149

Plugin Information

Published: 2016/07/29, Modified: 2022/04/11

Plugin Output

10.0.2.4 (tcp/80/www)

Nessus was able to exploit the issue using the following request :

`http://10.0.2.4/drupal/sites/all/modules/coder/coder_upgrade/scripts/coder_upgrade.run.php`

This produced the following truncated output (limited to 10 lines) :

```
----- snip -----  
file parameter is not setNo path to parameter file  
----- snip -----
```

42873 (1) - 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

10.0.2.4 (tcp/631/www)

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

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	---	-----	---
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC (168)	
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}

78515 (1) - Drupal Database Abstraction API SQLi

Synopsis

The remote web server is running a PHP application that is affected by a SQL injection vulnerability.

Description

The remote web server is running a version of Drupal that is affected by a SQL injection vulnerability due to a flaw in the Drupal database abstraction API, which allows a remote attacker to use specially crafted requests that can result in arbitrary SQL execution. This may lead to privilege escalation, arbitrary PHP execution, or remote code execution.

See Also

<https://www.drupal.org/SA-CORE-2014-005>

<https://www.drupal.org/project/drupal/releases/7.32>

Solution

Upgrade to version 7.32 or later.

Risk Factor

High

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	70595
CVE	CVE-2014-3704
XREF	EDB-ID:34984
XREF	EDB-ID:34992
XREF	EDB-ID:34993
XREF	EDB-ID:35150

Exploitable With

CANVAS (true) Core Impact (true) (true) Metasploit (true)

Plugin Information

Published: 2014/10/16, Modified: 2022/04/11

Plugin Output

10.0.2.4 (tcp/80/www)

Nessus was able to exploit the issue using the following request :

```
POST /drupal/?q=node&destination=node HTTP/1.1
Host: 10.0.2.4
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Content-Length: 117
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
name[0;SELECT
+@@version;#]=0;&name[0]=nessus&pass=nessus&test2=test&form_build_id=&form_id=user_login_block&op=Log
+in
```

This produced the following truncated output (limited to 5 lines) :

```
----- snip -----
>Warning</em>: mb_strlen() expects parameter 1 to be string, array given in <em
  class="placeholder">drupal_strlen()</em> (line <em class="placeholder">441</em> of <em
  class="placeholder">/var/www/html/drupal/includes/unicode.inc</em>).</li>
<li><em class="placeholder">Warning</em>: addcslashes() expects parameter 1 to be string,
  array given in <em class="placeholder">DatabaseConnection->escapeLike()</em> (line <em
  class="placeholder">965</em> of <em class="placeholder">/var/www/html/drupal/includes/database/
  database.inc</em>).</li>
<li>Sorry, unrecognized username or password. <a href="/drupal/?q=user/password">Have you forgotten
  your password?</a></li>
</ul>
</div>
[...]
```

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

10704 (1) - Apache Multiviews Arbitrary Directory Listing

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

The Apache web server running on the remote host is affected by an information disclosure vulnerability. An unauthenticated, remote attacker can exploit this, by sending a crafted request, to display a listing of a remote directory, even if a valid index file exists in the directory.

For Apache web server later than 1.3.22, review listing directory configuration to avoid disclosing sensitive information

See Also

<http://www.nessus.org/u?f39e976b>

<http://www.nessus.org/u?a96611bc>

<http://www.nessus.org/u?c1c382bc>

Solution

Upgrade to Apache version 1.3.22 or later. Alternatively, as a workaround, disable Multiviews.

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 v3.0 Temporal Score

4.8 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

2.2

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	3009
CVE	CVE-2001-0731
XREF	OWASP:OWASP-CM-004
XREF	EDB-ID:21002

Plugin Information

Published: 2016/02/16, Modified: 2020/10/21

Plugin Output

10.0.2.4 (tcp/80/www)

Nessus was able to exploit the issue using the following request :

`http://10.0.2.4/?M=A`

This produced the following truncated output (limited to 10 lines) :

```
----- snip -----
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /</title>
</head>
<body>
<h1>Index of /</h1>
<table>
<tr><th valign="top"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr>
[...]
```

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

51192 (1) - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

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

See Also

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/631/www)

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

```
| -Subject : CN=ubuntu  
| -Issuer  : CN=ubuntu
```

57582 (1) - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

10.0.2.4 (tcp/631/www)

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

| -Subject : CN=ubuntu

57608 (1) - SMB Signing not required

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

<http://www.nessus.org/u?df39b8b3>

<http://technet.microsoft.com/en-us/library/cc731957.aspx>

<http://www.nessus.org/u?74b80723>

<https://www.samba.org/samba/docs/current/man-html/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 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 v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

Plugin Information

Published: 2012/01/19, Modified: 2022/10/05

Plugin Output

10.0.2.4 (tcp/445/cifs)

90317 (1) - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

<https://tools.ietf.org/html/rfc4253#section-6.3>

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

Plugin Output

10.0.2.4 (tcp/22/ssh)

The following weak server-to-client encryption algorithms are supported :

```
arcfour
arcfour128
arcfour256
```

The following weak client-to-server encryption algorithms are supported :

```
arcfour
arcfour128
arcfour256
```

104743 (1) - 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 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

10.0.2.4 (tcp/631/www)

TLsv1 is enabled and the server supports at least one cipher.

157288 (1) - TLS Version 1.1 Protocol Deprecated

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

<https://datatracker.ietf.org/doc/html/rfc8996>

<http://www.nessus.org/u?c8ae820d>

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2023/04/19

Plugin Output

10.0.2.4 (tcp/631/www)

TLSv1.1 is enabled and the server supports at least one cipher.

187315 (1) - SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)

Synopsis

The remote SSH server is vulnerable to a mitm prefix truncation attack.

Description

The remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security.

Note that this plugin only checks for remote SSH servers that support either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC and do not support the strict key exchange countermeasures. It does not check for vulnerable software versions.

See Also

<https://terrapin-attack.com/>

Solution

Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.2 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE CVE-2023-48795

Plugin Information

Published: 2023/12/27, Modified: 2024/01/29

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Supports following CBC Client to Server algorithm : cast128-cbc
Supports following CBC Client to Server algorithm : aes192-cbc
Supports following CBC Client to Server algorithm : aes256-cbc
Supports following CBC Client to Server algorithm : rijndael-cbc@lysator.liu.se
Supports following CBC Client to Server algorithm : blowfish-cbc
Supports following CBC Client to Server algorithm : 3des-cbc
Supports following CBC Client to Server algorithm : aes128-cbc
Supports following ChaCha20-Poly1305 Client to Server algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-md5-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha1-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-md5-96-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha1-96-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-ripemd160-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : umac-64-etm@openssh.com
Supports following CBC Server to Client algorithm : cast128-cbc
Supports following CBC Server to Client algorithm : aes192-cbc
Supports following CBC Server to Client algorithm : aes256-cbc
Supports following CBC Server to Client algorithm : rijndael-cbc@lysator.liu.se
Supports following CBC Server to Client algorithm : blowfish-cbc
Supports following CBC Server to Client algorithm : 3des-cbc
Supports following CBC Server to Client algorithm : aes128-c [...]
```

70658 (1) - 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 v3.0 Base Score

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

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

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

Plugin Information

Plugin Output

10.0.2.4 (tcp/22/ssh)

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
```

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
```

71049 (1) - 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 v2.0 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

10.0.2.4 (tcp/22/ssh)

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

```
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
```

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

```
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
```

hmac-sha1-96-etm@openssh.com

153953 (1) - SSH Weak Key Exchange Algorithms Enabled

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) RFC9142. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

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

See Also

<https://datatracker.ietf.org/doc/html/rfc9142>

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Plugin Output

10.0.2.4 (tcp/22/ssh)

The following weak key exchange algorithms are enabled :

```
diffie-hellman-group-exchange-sha1  
diffie-hellman-group1-sha1
```

10335 (8) - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

10.0.2.4 (tcp/21/ftp)

```
Port 21/tcp was found to be open
```

10.0.2.4 (tcp/22/ssh)

```
Port 22/tcp was found to be open
```

10.0.2.4 (tcp/80/www)

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

10.0.2.4 (tcp/445/cifs)

```
Port 445/tcp was found to be open
```

10.0.2.4 (tcp/631/www)

Port 631/tcp was found to be open

10.0.2.4 (tcp/3306/mysql)

Port 3306/tcp was found to be open

10.0.2.4 (tcp/6697/irc)

Port 6697/tcp was found to be open

10.0.2.4 (tcp/8080/www)

Port 8080/tcp was found to be open

22964 (8) - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/21/ftp)

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

10.0.2.4 (tcp/22/ssh)

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

10.0.2.4 (tcp/80/www)

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

10.0.2.4 (tcp/631/www)

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

10.0.2.4 (tcp/631/www)

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

10.0.2.4 (tcp/3306/mysql)

A MySQL server is running on this port.

10.0.2.4 (tcp/6697/irc)

An IRC server is running on this port.

10.0.2.4 (tcp/8080/www)

A web server is running on this port.

10107 (3) - 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

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

10.0.2.4 (tcp/80/www)

The remote web server type is :

Apache/2.4.7 (Ubuntu)

10.0.2.4 (tcp/631/www)

The remote web server type is :

CUPS/1.7 IPP/2.1

10.0.2.4 (tcp/8080/www)

The remote web server type is :

Jetty(8.1.7.v20120910)

24260 (2) - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

10.0.2.4 (tcp/80/www)

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : no

Keep-Alive : yes

Options allowed : (Not implemented)

Headers :

Date: Sat, 06 Apr 2024 14:07:22 GMT

Server: Apache/2.4.7 (Ubuntu)

Vary: Accept-Encoding

Content-Length: 1346

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html; charset=UTF-8

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">

<html>

<head>

<title>Index of /</title>

</head>

<body>

```

<h1>Index of /</h1>
<table>
  <tr><th valign="top"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
  <tr><th colspan="5"><hr></th></tr>
  <tr><td valign="top"></td><td><a href="chat/">chat</a></td><td align="right">2020-10-29 19:37 </td><td align="right"> - </td><td>&nbsp;</td></tr>
  <tr><td valign="top"></td><td><a href="drupal/">drupal</a></td><td align="right">2011-07-27 20:17 </td><td align="right"> - </td><td>&nbsp;</td></tr>
  <tr><td valign="top"></td><td><a href="payroll_app.php">payroll_app.php</a></td><td align="right">2020-10-29 19:37 </td><td align="right">1.7K</td><td>&nbsp;</td></tr>
  <tr><td valign="top"></td><td><a href="phpmyadmin/">phpmyadmin</a></td><td align="right">2013-04-08 12:06 </td><td align="right"> - </td><td>&nbsp;</td></tr>
  <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.7 (Ubuntu) Server at 10.0.2.4 Port 80</address>
</body></html>

```

10.0.2.4 (tcp/8080/www)

Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Date: Sat, 06 Apr 2024 14:07:22 GMT

Content-Type: text/html

Content-Length: 795

Connection: close

Server: Jetty(8.1.7.v20120910)

Response Body :

43111 (2) - 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.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

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.

See Also

<http://www.nessus.org/u?d9c03a9a>

<http://www.nessus.org/u?b019cbdb>

[https://www.owasp.org/index.php/Test_HTTP_Methods_\(OTG-CONFIG-006\)](https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006))

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

10.0.2.4 (tcp/80/www)

Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST are allowed on :
/

10.0.2.4 (tcp/631/www)

Based on the response to an OPTIONS request :

- HTTP methods HEAD OPTIONS POST PUT GET are allowed on :
/

10092 (1) - 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

References

XREF IAVT:0001-T-0030

XREF IAVT:0001-T-0943

Plugin Information

Published: 1999/10/12, Modified: 2023/08/17

Plugin Output

10.0.2.4 (tcp/21/ftp)

The remote FTP banner is :

```
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.2.4]
```

10114 (1) - 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

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0524

XREF CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2023/04/27

Plugin Output

10.0.2.4 (icmp/0)

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

10150 (1) - 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: 2021/02/10

Plugin Output

10.0.2.4 (tcp/445/cifs)

The following 2 NetBIOS names have been gathered :

```
METASPLOITABLE3-UB1404 = Computer name
METASPLOITABLE3-UB1404 = Workgroup / Domain name
```

10180 (1) - Ping the remote host

Synopsis

It was possible to identify the status of the remote host (alive or dead).

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.
- An ICMP ping.
- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.
- A UDP ping (e.g., DNS, RPC, and NTP).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/06/24, Modified: 2024/03/25

Plugin Output

10.0.2.4 (tcp/0)

```
The remote host is up
The host replied to an ARP who-is query.
Hardware address : 08:00:27:c2:98:66
```

10267 (1) - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
SSH version : SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.13
SSH supported authentication : publickey,password
```

10287 (1) - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

10.0.2.4 (udp/0)

For your information, here is the traceroute from 10.0.2.15 to 10.0.2.4 :

10.0.2.15

10.0.2.4

Hop Count: 1

10395 (1) - Microsoft Windows SMB Shares Enumeration

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2022/02/01

Plugin Output

10.0.2.4 (tcp/445/cifs)

Here are the SMB shares available on the remote host :

- print\$
- public
- IPC\$

10719 (1) - 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

References

XREF IAVT:0001-T-0802

Plugin Information

Published: 2001/08/13, Modified: 2022/10/12

Plugin Output

10.0.2.4 (tcp/3306/mysql)

The remote database access is restricted and configured to reject access from unauthorized IPs. Therefore it was not possible to extract its version number.

10785 (1) - 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 SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

10.0.2.4 (tcp/445/cifs)

```
The remote Operating System is : Windows 6.1
The remote native LAN manager is : Samba 4.3.11-Ubuntu
The remote SMB Domain Name is : METASPLOITABLE3-UB1404
```

10859 (1) - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).

The host SID can then be used to get the list of local users.

See Also

<http://technet.microsoft.com/en-us/library/bb418944.aspx>

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.

Refer to the 'See also' section for guidance.

Risk Factor

None

Plugin Information

Published: 2002/02/13, Modified: 2024/01/31

Plugin Output

10.0.2.4 (tcp/445/cifs)

The remote host SID value is : S-1-5-21-2892692244-97591703-1708969968

The value of 'RestrictAnonymous' setting is : unknown

10860 (1) - SMB Use Host SID to Enumerate Local Users

Synopsis

Nessus was able to enumerate local users.

Description

Using the host security identifier (SID), Nessus was able to enumerate local users on the remote Windows system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/02/13, Modified: 2023/02/28

Plugin Output

10.0.2.4 (tcp/445/cifs)

```
- nobody (id 501, Guest account)
- chewbacca (id 1000)
```

Note that, in addition to the Administrator, Guest, and Kerberos accounts, Nessus has enumerated local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Enumerate Local Users: Start UID' and/or 'End UID' preferences under 'Assessment->Windows' and re-run the scan. Only UIDs between 1 and 2147483647 are allowed for this range.

10863 (1) - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/631/www)

```
Subject Name:

Common Name: ubuntu

Issuer Name:

Common Name: ubuntu

Serial Number: 00 B4 19 55 57 D4 D9 40 BF

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Oct 29 19:28:07 2020 GMT
Not Valid After: Oct 27 19:28:07 2030 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C4 71 FD 30 C2 2D A6 63 74 4B 39 CE 9B 39 E2 AD 75 F0 BC
            EA 44 C7 55 7C 0C 5D 95 5D 4C 94 25 50 C3 40 88 EC 19 2C 23
            89 40 39 C2 0E D9 C9 48 1F DE 56 1A 75 C5 5F 25 A8 EF 46 B6
            52 14 B8 0A 14 69 D9 CD 86 A5 71 45 45 6E C5 78 95 7C 55 16
            55 B5 41 B3 B3 42 FA F9 58 C2 EA 4F C2 2D 38 41 7B 9A F7 51
            8C 07 24 AF DD 96 02 A1 E3 63 2F FC 7B 65 22 05 F2 4A 19 AE
            72 7F 78 AB EF 21 CF 13 CE 6C 67 9B CA 01 65 47 9B 33 E0 A3
            A2 7E F4 79 DA 43 7F 4B B2 34 F6 B5 5B C5 1E 6E 38 A3 C4 88
            7B 60 EF 25 F4 71 AF FA 75 18 23 02 18 28 1B BE 3F 3F B2 5E
            53 CE 1E F2 88 37 13 D4 60 44 A2 C4 77 7F 40 2E A0 2A EF 0B
```

```
E6 B1 A6 F8 EC E9 73 E1 64 6B 40 FE 92 05 35 FB 2E 74 22 AF
9B 0E B0 53 A4 10 07 84 4B 8C 62 17 7E CE 2E 8F AD 00 61 27
E8 7D 44 0D F0 7F 48 3E 78 D4 EA 9A 10 C8 2E 76 15
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 BA 04 3F 75 9E 17 21 D8 86 A3 C8 E6 78 E7 C3 9E 0D EE 8F
C9 FF 91 80 26 30 3F D3 DA C4 74 9D 3B 2B 40 69 FD 08 4A F1
5C 1A 62 F2 40 9D BA A5 7C FE 34 62 3B C9 33 6D FA 47 18 31
38 03 0C CD A9 5A 26 88 D9 7F D0 57 0D 36 F1 C1 D1 36 0C 71
74 58 54 4A A6 27 1C F8 51 E5 6D 46 6B 2B 44 FA D0 EC D2 DB
1F 74 49 CA 80 7D 30 3A 14 90 BE A3 1B FE 7F 5C DE 66 B9 21
2C 3E F9 B8 96 63 4D 93 3B 21 7F 40 60 0C EE B4 1D E1 F9 33
B1 CF E0 2D 2F 91 58 23 CD FA 0B F1 D7 25 E6 96 41 CC 1A BE
19 54 4A ED 70 1E 5E E5 E5 24 8C B4 1F 99 A0 8F B8 F6 57 32
E3 E6 20 3A 85 0D 9B C4 68 E4 D0 14 E3 0F E5 BF 44 0A 2F [...]
```

10881 (1) - 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: 2021/01/19

Plugin Output

10.0.2.4 (tcp/22/ssh)

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

- 1.99
- 2.0

11011 (1) - 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: 2021/02/11

Plugin Output

10.0.2.4 (tcp/445/cifs)

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

11936 (1) - 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: 2023/11/08

Plugin Output

10.0.2.4 (tcp/0)

```
Remote operating system : Linux Kernel 3.13 on Ubuntu 14.04 (trusty)
Confidence level : 95
Method : HTTP
```

```
The remote host is running Linux Kernel 3.13 on Ubuntu 14.04 (trusty)
```

17651 (1) - Microsoft Windows SMB : Obtains the Password Policy

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/03/30, Modified: 2015/01/12

Plugin Output

10.0.2.4 (tcp/445/cifs)

The following password policy is defined on the remote host:

```
Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0
```

18261 (1) - 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.

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2022/03/21

Plugin Output

10.0.2.4 (tcp/0)

```
The Linux distribution detected was :  
- Ubuntu 14.04 (trusty)
```

18638 (1) - Drupal Software Detection

Synopsis

A content management system is running on the remote web server.

Description

Drupal, an open source content management system written in PHP, is running on the remote web server.

See Also

<https://www.drupal.org/>

Solution

Ensure that the use of this software aligns with your organization's security and acceptable use policies.

Risk Factor

None

References

XREF IAVT:0001-T-0586

Plugin Information

Published: 2005/07/07, Modified: 2023/05/24

Plugin Output

10.0.2.4 (tcp/80/www)

```
URL      : http://10.0.2.4/drupal
Version  : 7.5
```

19506 (1) - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/03/13

Plugin Output

10.0.2.4 (tcp/0)

Information about this scan :

```
Nessus version : 10.7.2
Nessus build : 20029
Plugin feed version : 202404060903
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
```

```
Scan name : Ubuntu_Simple_Vul_Scan
Scan policy used : Basic Network Scan
Scanner IP : 10.0.2.15
Port scanner(s) : nessus_tcp_scanner
Port range : 21,22,80,445,631,3000,3306,3500,6697,8080,8181
Ping RTT : 192.990 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/4/6 9:57 EDT
Scan duration : 1751 sec
Scan for malware : no
```

19689 (1) - Embedded Web Server Detection

Synopsis

The remote web server is embedded.

Description

The remote web server cannot host user-supplied CGIs. CGI scanning will be disabled on this server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/09/14, Modified: 2019/11/22

Plugin Output

10.0.2.4 (tcp/631/www)

20108 (1) - 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

Plugin Information

Published: 2005/10/28, Modified: 2020/06/12

Plugin Output

10.0.2.4 (tcp/8080/www)

```
MD5 fingerprint : ed7d5c39c69262f4ba95418d4f909b10
Web server      : jetty 5.1.14
```

21643 (1) - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

10.0.2.4 (tcp/631/www)

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

SSL Version : TLSv12

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

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC (168)	

SHA1

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
AES128-SHA	0x00, 0x2F	RSA	RSA	AES-CBC (128)	
AES256-SHA	0x00, 0x35	RSA	RSA	AES-CBC (256)	
CAMELLIA128-SHA	0x00, 0x41	RSA	RSA	Camellia-CBC (128)	

SHA1

CAMELLIA256-SHA	0x00, 0x84	RSA	RSA	Camellia-CBC(256)
SHA1				
RSA-AES128-SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)
SHA256				
RSA-AES256-SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)
SHA256				

SSL Version : TLSv11

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

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC(168)	
SHA1					

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
AES128-SHA	0x00, 0x2F	RSA [...]			

25220 (1) - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/0)

25240 (1) - Samba Server Detection

Synopsis

An SMB server is running on the remote host.

Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

See Also

<https://www.samba.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2022/10/12

Plugin Output

10.0.2.4 (tcp/445/cifs)

The remote host tries to hide its SMB server type by changing the MAC address and the LAN manager name.

However by sending several valid and invalid RPC requests it was possible to fingerprint the remote SMB server as Samba.

35716 (1) - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/0)

The following card manufacturers were identified :

08:00:27:C2:98:66 : PCS Systemtechnik GmbH

39519 (1) - Backported Security Patch Detection (FTP)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote FTP 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

10.0.2.4 (tcp/21/ftp)

Give Nessus credentials to perform local checks.

39520 (1) - 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

10.0.2.4 (tcp/22/ssh)

Give Nessus credentials to perform local checks.

39521 (1) - 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

10.0.2.4 (tcp/80/www)

Give Nessus credentials to perform local checks.

42410 (1) - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

Synopsis

It is possible to obtain the network name of the remote host.

Description

The remote host listens on tcp port 445 and replies to SMB requests.

By sending an NTLMSSP authentication request it is possible to obtain the name of the remote system and the name of its domain.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/11/06, Modified: 2019/11/22

Plugin Output

10.0.2.4 (tcp/445/cifs)

```
The following 2 NetBIOS names have been gathered :
```

```
METASPLOITABLE3-UB1404 = Computer name  
METASPLOITABLE3-UB1404 = Workgroup / Domain name
```

45410 (1) - 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: 2021/03/09

Plugin Output

10.0.2.4 (tcp/631/www)

The host name known by Nessus is :

metasploitable3-ub1404

The Common Name in the certificate is :

ubuntu

45590 (1) - Common Platform Enumeration (CPE)

Synopsis

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

Description

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

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

See Also

<http://cpe.mitre.org/>

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2024/04/03

Plugin Output

10.0.2.4 (tcp/0)

The remote operating system matched the following CPE :

cpe:/o:canonical:ubuntu_linux:14.04 -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.4.7 -> Apache Software Foundation Apache HTTP Server
cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server
cpe:/a:drupal:drupal:7.5 -> Drupal
cpe:/a:mysql:mysql -> MySQL MySQL
cpe:/a:openbsd:openssh:6.6 -> OpenBSD OpenSSH
cpe:/a:openbsd:openssh:6.6.1p1 -> OpenBSD OpenSSH
cpe:/a:samba:samba -> Samba Samba
cpe:/a:samba:samba:4.3.11 -> Samba Samba

48204 (1) - 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.

See Also

<https://httpd.apache.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0030

XREF IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

10.0.2.4 (tcp/80/www)

```
URL      : http://10.0.2.4/
Version  : 2.4.99
Source   : Server: Apache/2.4.7 (Ubuntu)
backported : 1
os       : ConvertedUbuntu
```

54615 (1) - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

10.0.2.4 (tcp/0)

```
Remote device type : general-purpose  
Confidence level : 95
```

56984 (1) - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

Plugin Output

10.0.2.4 (tcp/631/www)

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

60119 (1) - Microsoft Windows SMB Share Permissions Enumeration

Synopsis

It was possible to enumerate the permissions of remote network shares.

Description

By using the supplied credentials, Nessus was able to enumerate the permissions of network shares. User permissions are enumerated for each network share that has a list of access control entries (ACEs).

See Also

<https://technet.microsoft.com/en-us/library/bb456988.aspx>

<https://technet.microsoft.com/en-us/library/cc783530.aspx>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/07/25, Modified: 2022/08/11

Plugin Output

10.0.2.4 (tcp/445/cifs)

```
Share path : \\METASPLOITABLE3-UB1404\print$
Local path : C:\var\lib\samba\printers
Comment : Printer Drivers
[*] Allow ACE for Everyone (S-1-1-0): 0x001f01ff
    FILE_GENERIC_READ:      YES
    FILE_GENERIC_WRITE:     YES
    FILE_GENERIC_EXECUTE:   YES

Share path : \\METASPLOITABLE3-UB1404\public
Local path : C:\var\www\html\
Comment : WWW
[*] Allow ACE for Everyone (S-1-1-0): 0x001f01ff
    FILE_GENERIC_READ:      YES
    FILE_GENERIC_WRITE:     YES
    FILE_GENERIC_EXECUTE:   YES

Share path : \\METASPLOITABLE3-UB1404\IPC$
Local path : C:\tmp
Comment : IPC Service (metasploitable3-ub1404 server (Samba, Ubuntu))
[*] Allow ACE for Everyone (S-1-1-0): 0x001f01ff
```


FILE_GENERIC_READ:	YES
FILE_GENERIC_WRITE:	YES
FILE_GENERIC_EXECUTE:	YES

66293 (1) - Unix Operating System on Extended Support

Synopsis

The remote host is running an operating system that is on extended support.

Description

According to its version, the remote host uses a Unix or Unix-like operating system that has transitioned to an extended portion in its support life cycle. Continued access to new security updates requires payment of an additional fee and / or configuration changes to the package management tool. Without that, the host likely will be missing security updates.

Solution

Ensure that the host subscribes to the vendor's extended support plan and continues to receive security updates.

Risk Factor

None

References

XREF IAVA:0001-A-0648

Plugin Information

Published: 2013/05/02, Modified: 2023/05/10

Plugin Output

10.0.2.4 (tcp/0)

```
Ubuntu 14.04 support ends on 2019-04-30 (end of maintenance) / 2024-04-30 (end of extended security maintenance).
```

66334 (1) - 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.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2024/03/19

Plugin Output

10.0.2.4 (tcp/0)

. You need to take the following 2 actions :

[ProFTPD mod_copy Information Disclosure (84215)]

+ Action to take : Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later.

[SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) (187315)]

+ Action to take : Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

70544 (1) - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/631/www)

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

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

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC (168)	
SHA1					

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
AES128-SHA	0x00, 0x2F	RSA	RSA	AES-CBC (128)	
SHA1					

AES256-SHA	0x00, 0x35	RSA	RSA	AES-CBC(256)
SHA1				
CAMELLIA128-SHA	0x00, 0x41	RSA	RSA	Camellia-CBC(128)
SHA1				
CAMELLIA256-SHA	0x00, 0x84	RSA	RSA	Camellia-CBC(256)
SHA1				
RSA-AES128-SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)
SHA256				
RSA-AES256-SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)
SHA256				

The fields above are :

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

70657 (1) - 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

10.0.2.4 (tcp/22/ssh)

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-sha1
diffie-hellman-group-exchange-sha256
diffie-hellman-group1-sha1
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
ssh-dss
ssh-ed25519
ssh-rsa
```

The server supports the following options for `encryption_algorithms_client_to_server` :

```
3des-cbc
aes128-cbc
aes128-ctr
aes128-gcm@openssh.com
aes192-cbc
aes192-ctr
```

```
aes256-cbc
aes256-ctr
aes256-gcm@openssh.com
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
chacha20-poly1305@openssh.com
rijndael-cbc@lysator.liu.se
```

The server supports the following options for `encryption_algorithms_server_to_client` :

```
3des-cbc
aes128-cbc
aes128-ctr
aes128-gcm@openssh.com
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
aes256-gcm@openssh.com
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
chacha20-poly1305@openssh.com
rijndael-cbc@lysator.liu.se
```

The server supports the following options for `mac_algorithms_client_to_server` :

```
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-ripemd160
hmac-ripemd160-etm@openssh.com
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
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-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-ripemd160
hmac-ripemd160-etm@openssh.com
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
hmac-sh [...]
```

86420 (1) - Ethernet MAC Addresses

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/0)

```
The following is a consolidated list of detected MAC addresses:  
- 08:00:27:C2:98:66
```


96982 (1) - 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/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and>

<http://www.nessus.org/u?8dcab5e4>

<http://www.nessus.org/u?234f8ef8>

<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 IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2020/09/22

Plugin Output

10.0.2.4 (tcp/445/cifs)

The remote host supports SMBv1.

100871 (1) - 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: 2019/11/22

Plugin Output

10.0.2.4 (tcp/445/cifs)

```
The remote host supports the following versions of SMB :  
SMBv1  
SMBv2
```

104887 (1) - Samba Version

Synopsis

It was possible to obtain the samba version from the remote operating system.

Description

Nessus was able to obtain the samba version from the remote operating 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: 2017/11/30, Modified: 2019/11/22

Plugin Output

10.0.2.4 (tcp/445/cifs)

```
The remote Samba Version is : Samba 4.3.11-Ubuntu
```

106716 (1) - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 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: 2020/03/11

Plugin Output

10.0.2.4 (tcp/445/cifs)

```
The remote host supports 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
```

110723 (1) - Target Credential Status by Authentication Protocol - No Credentials Provided

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.
- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2023/02/13

Plugin Output

10.0.2.4 (tcp/0)

```
SSH was detected on port 22 but no credentials were provided.
```

SSH local checks were not enabled.

117886 (1) - OS Security Patch Assessment Not Available

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

10.0.2.4 (tcp/0)

The following issues were reported :

```
- Plugin      : no_local_checks_credentials.nasl
  Plugin ID   : 110723
  Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
  Message     :
  Credentials were not provided for detected SSH service.
```


121010 (1) - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>

<http://www.nessus.org/u?c8ae820d>

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

References

XREF CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

10.0.2.4 (tcp/631/www)

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

135860 (1) - WMI Not Available

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vulnerabilities that exist on the remote host.

See Also

<https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2024/03/26

Plugin Output

10.0.2.4 (tcp/445/cifs)

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

149334 (1) - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

<https://tools.ietf.org/html/rfc4252#section-8>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

10.0.2.4 (tcp/22/ssh)

153588 (1) - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

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

Description

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/22/ssh)

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

```
hmac-sha1
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
hmac-sha1-etm@openssh.com
```

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

```
hmac-sha1
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
hmac-sha1-etm@openssh.com
```

156899 (1) - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

<https://ssl-config.mozilla.org/>

Solution

Only enable support for recommended cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

10.0.2.4 (tcp/631/www)

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:

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

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
DES-CBC3-SHA SHA1	0x00, 0x0A	RSA	RSA	3DES-CBC(168)	

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
AES128-SHA SHA1	0x00, 0x2F	RSA	RSA	AES-CBC(128)	
AES256-SHA SHA1	0x00, 0x35	RSA	RSA	AES-CBC(256)	
CAMELLIA128-SHA SHA1	0x00, 0x41	RSA	RSA	Camellia-CBC(128)	
CAMELLIA256-SHA SHA1	0x00, 0x84	RSA	RSA	Camellia-CBC(256)	
RSA-AES128-SHA256 SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)	
RSA-AES256-SHA256 SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)	

The fields above are :

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

181418 (1) - OpenSSH Detection

Synopsis

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

Description

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

See Also

<https://www.openssh.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2024/03/27

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Service : ssh
Version : 6.6.1p1
Banner  : SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.13
```