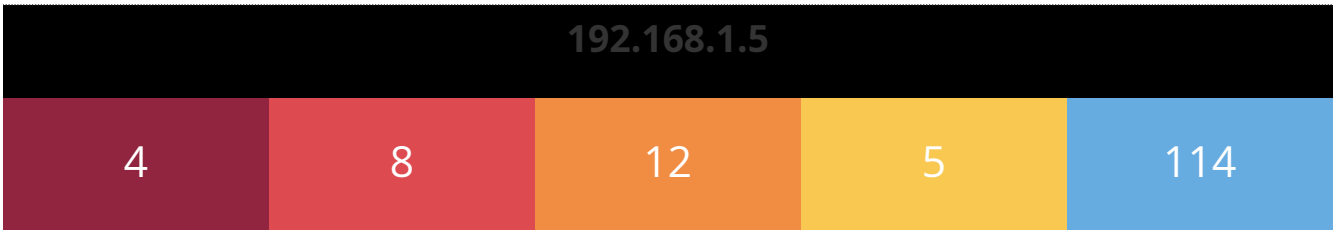
Meta-Adv-scan

Report generated by Nessus™ Fri, 05 Aug 2022 10:20:01 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host



Scan Information

Start time: Fri Aug 5 10:01:01 2022
End time: Fri Aug 5 10:20:00 2022

Host Information

DNS Name: ISLAM-KHALIL.station
Netbios Name: METASPLOITABLE
IP: 192.168.1.5
MAC Address: 08:00:27:39:6D:CD
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis

The remote SSH host keys are weak.

Description

The remote SSH host key 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 set up 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

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: 2008/05/14, Modified: 2018/11/15

Plugin Output

tcp/22/ssh

33850 - Unix Operating System Unsupported Version Detection

Synopsis

The operating system running on the remote host is no longer supported.

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	IAVA:0001-A-0502
XREF	IAVA:0001-A-0648

Plugin Information

Published: 2008/08/08, Modified: 2022/05/18

Plugin Output

tcp/0

```
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).
Upgrade to Ubuntu 21.04 / LTS 20.04 / LTS 18.04.

For more information, see : https://wiki.ubuntu.com/Releases
```

46882 - UnrealIRCd Backdoor Detection

Synopsis

The remote IRC server contains a backdoor.

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

See Also

https://seclists.org/fulldisclosure/2010/Jun/277

https://seclists.org/fulldisclosure/2010/Jun/284

http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

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:C)

References

BID	40820
CVE	CVE-2010-2075

Exploitable With

CANVAS (true) Metasploit (true)

Plugin Information

Published: 2010/06/14, Modified: 2022/04/11

Plugin Output

tcp/6667/irc

```
The remote IRC server is running as :

uid=0(root) gid=0(root)
```

125855 - phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)

Synopsis

The remote web server hosts a PHP application that is affected by SQLi vulnerability.

Description

According to its self-reported version number, the phpMyAdmin application hosted on the remote web server is prior to 4.8.6. It is, therefore, affected by a SQL injection (SQLi) vulnerability that exists in designer feature of phpMyAdmin. An unauthenticated, remote attacker can exploit this to inject or manipulate SQL queries in the back-end database, resulting in the disclosure or manipulation of arbitrary data.

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?c9d7fc8c

Solution

Upgrade to phpMyAdmin version 4.8.6 or later.

Alternatively, apply the patches referenced in the vendor advisories.

Risk Factor

High

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

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

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

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

References

BID	108617
CVE	CVE-2019-11768

Plugin Information

Published: 2019/06/13, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
URL               : http://ISLAM-KHALIL.station/phpMyAdmin
Installed version : 3.1.1
Fixed version     : 4.8.6
```

70728 - Apache PHP-CGI Remote Code Execution

Synopsis

The remote web server contains a version of PHP that allows arbitrary code execution.

Description

The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc.

Solution

Upgrade to PHP 5.3.13 / 5.4.3 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

8.4 (CVSS:3.0/E:H/RL:O/RC:C)

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

6.5 (CVSS2#E:H/RL:OF/RC:C)

References

BID	53388
CVE	CVE-2012-1823
CVE	CVE-2012-2311
CVE	CVE-2012-2335
CVE	CVE-2012-2336
XREF	CERT:520827
XREF	EDB-ID:29290
XREF	EDB-ID:29316
XREF	CISA-KNOWN-EXPLOITED:2022/04/15

Exploitable With

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

Plugin Information

Published: 2013/11/01, Modified: 2022/03/28

Plugin Output

tcp/80/www

```
Nessus was able to verify the issue exists using the following request :

------------------------------ snip ------------------------------
POST /cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+
%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F
%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F
%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E
%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F
%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F
%65%6E%76%3D%30+%2D%6E HTTP/1.1
Host: ISLAM-KHALIL.station
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: 115
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, */*
<?php echo "Content-Type:text/html\r\n\r\n"; echo 'php_cgi_remote_code_execution-1659708831';
 system('id'); die; ?>
------------------------------ snip ------------------------------
```

136808 - ISC BIND Denial of Service

Synopsis

The remote name server is affected by an assertion failure vulnerability.

Description

A denial of service (DoS) vulnerability exists in ISC BIND versions 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 / 9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 and earlier. An unauthenticated, remote attacker can exploit this issue, via a specially-crafted message, to cause the service to stop responding.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://kb.isc.org/docs/cve-2020-8617

Solution

Upgrade to the patched release most closely related to your current version of BIND.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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

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

STIG Severity

I

References

CVE	CVE-2020-8617
XREF	IAVA:2020-A-0217-S

Plugin Information

Published: 2020/05/22, Modified: 2022/05/13

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.11.19
```

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)

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

I

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

```
Installed version : 9.4.2
Fixed version     : 9.11.19
```

59088 - PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution

Synopsis

The remote web server contains a version of PHP that allows arbitrary code execution.

Description

The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc.

See Also

http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/

http://www.php.net/archive/2012.php#id2012-05-08-1

http://www.php.net/ChangeLog-5.php#5.3.13

http://www.php.net/ChangeLog-5.php#5.4.3

http://www.nessus.org/u?80589ce8

https://www-304.ibm.com/support/docview.wss?uid=swg21620314

Solution

If using Lotus Foundations, upgrade the Lotus Foundations operating system to version 1.2.2b or later.

Otherwise, upgrade to PHP 5.3.13 / 5.4.3 or later.

Risk Factor

High

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

6.5 (CVSS2#E:H/RL:OF/RC:C)

References

BID	53388
CVE	CVE-2012-1823
CVE	CVE-2012-2311
XREF	CERT:520827
XREF	EDB-ID:18834
XREF	CISA-KNOWN-EXPLOITED:2022/04/15

Exploitable With

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

Plugin Information

Published: 2012/05/14, Modified: 2022/03/28

Plugin Output

tcp/80/www

```
Nessus was able to verify the issue exists using the following request :

------------------------------ snip ------------------------------
POST /mutillidae/documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php?-d
+allow_url_include%3don+-d+safe_mode%3doff+-d+suhosin.simulation%3don+-d+open_basedir%3doff+-d
+auto_prepend_file%3dphp%3a//input+-n HTTP/1.1
Host: ISLAM-KHALIL.station
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: 82
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, */*
<?php echo 'php_cgi_query_string_code_execution-1659708831'; system('id'); die; ?>
------------------------------ snip ------------------------------
```

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)

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

```
Nessus detected that the Samba Badlock patch has not been applied.
```

19704 - TWiki 'rev' Parameter Arbitrary Command Execution

Synopsis

The remote web server hosts a CGI application that is affected by an arbitrary command execution vulnerability.

Description

The version of TWiki running on the remote host allows an attacker to manipulate input to the 'rev' parameter in order to execute arbitrary shell commands on the remote host subject to the privileges of the web server user id.

See Also

http://www.nessus.org/u?c70904f3

Solution

Apply the appropriate hotfix referenced in the vendor advisory.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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	14834
CVE	CVE-2005-2877

Exploitable With

Metasploit (true)

Plugin Information

Published: 2005/09/15, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Nessus was able to execute the command "id" using the
following request :

http://ISLAM-KHALIL.station/twiki/bin/view/Main/TWikiUsers?rev=2%20%7cid%7c%7cecho%20


This produced the following truncated output (limited to 2 lines) :
------------------------------ snip ------------------------------
uid=33(www-data) gid=33(www-data) groups=33(www-data)

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

10205 - rlogin Service Detection

Synopsis

The rlogin service is running on the remote host.

Description

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.

Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution

Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Risk Factor

High

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0651

Exploitable With

Metasploit (true)

Plugin Information

Published: 1999/08/30, Modified: 2022/04/11

Plugin Output

tcp/513/rlogin

10245 - rsh Service Detection

Synopsis

The rsh service is running on the remote host.

Description

The rsh service is running on the remote host. This service is vulnerable since data is passed between the rsh client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.

Finally, rsh is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution

Comment out the 'rsh' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Risk Factor

High

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0651

Exploitable With

Metasploit (true)

Plugin Information

Published: 1999/08/22, Modified: 2022/04/11

Plugin Output

tcp/514/rsh

11411 - Backup Files Disclosure

Synopsis

It is possible to retrieve file backups from the remote web server.

Description

By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information.

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

Solution

Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2003/03/17, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
It is possible to read the following backup files :

  - File : /twiki/bin/search/Main/SearchResult~
    URL  : http://ISLAM-KHALIL.station/twiki/bin/search/Main/SearchResult~

  - File : /twiki/bin/view/Main/WebHome~
    URL  : http://ISLAM-KHALIL.station/twiki/bin/view/Main/WebHome~
```

40984 - Browsable Web Directories

Synopsis

Some directories on the remote web server are browsable.

Description

Multiple Nessus plugins identified directories on the web server that are browsable.

See Also

http://www.nessus.org/u?0a35179e

Solution

Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

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 v2.0 Base Score

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

Plugin Information

Published: 2009/09/15, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The following directories are browsable :

http://ISLAM-KHALIL.station/dav/
http://ISLAM-KHALIL.station/mutillidae/documentation/
http://ISLAM-KHALIL.station/mutillidae/styles/
http://ISLAM-KHALIL.station/mutillidae/styles/ddsmoothmenu/
http://ISLAM-KHALIL.station/test/
http://ISLAM-KHALIL.station/test/testoutput/
```

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

https://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these HTTP methods. Refer to the plugin output for more information.

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	9506
BID	9561
BID	11604
BID	33374

BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information

Published: 2003/01/23, Modified: 2020/06/12

Plugin Output

tcp/80/www

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus1665516353.html HTTP/1.1
Connection: Close
Host: ISLAM-KHALIL.station
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Fri, 05 Aug 2022 14:05:51 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus1665516353.html HTTP/1.1
Connection: Keep-Alive
Host: ISLAM-KHALIL.station
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

```
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

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

139915 - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

Synopsis

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

Description

According to its self-reported version number, the installation of ISC BIND running on the remote name server is version 9.x prior to 9.11.22, 9.12.x prior to 9.16.6 or 9.17.x prior to 9.17.4. It is, therefore, affected by a denial of service (DoS) vulnerability due to an assertion failure when attempting to verify a truncated response to a TSIG-signed request. An authenticated, remote attacker can exploit this issue by sending a truncated response to a TSIG-signed request to trigger an assertion failure, causing the server to exit.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://kb.isc.org/docs/cve-2020-8622

Solution

Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-8622
XREF	IAVA:2020-A-0385-S

Plugin Information

Published: 2020/08/27, Modified: 2021/06/03

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.11.22, 9.16.6, 9.17.4 or later
```

46803 - PHP expose_php Information Disclosure

Synopsis

The configuration of PHP on the remote host allows disclosure of sensitive information.

Description

The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself.

Other such Easter eggs likely exist, but Nessus has not checked for them.

See Also

https://www.0php.com/php_easter_egg.php

https://seclists.org/webappsec/2004/q4/324

Solution

In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/06/03, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Nessus was able to verify the issue using the following URL :

  http://ISLAM-KHALIL.station/mutillidae/documentation/how-to-access-Mutillidae-over-Virtual-Box-
network.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
```

57608 - 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: 2021/03/15

Plugin Output

tcp/445/cifs

90317 - 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

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
```

42263 - Unencrypted Telnet Server

Synopsis

The remote Telnet server transmits traffic in cleartext.

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution

Disable the Telnet service and use SSH instead.

Risk Factor

Medium

CVSS 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

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

Plugin Information

Published: 2009/10/27, Modified: 2020/06/12

Plugin Output

tcp/23/telnet

```
Nessus collected the following banner from the remote Telnet server :

------------------------------ snip ------------------------------
                _                   _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|
Warning: Never expose this VM to an untrusted network!
```

```
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login:
------------------------------ snip ------------------------------
```

85582 - Web Application Potentially Vulnerable to Clickjacking

Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

See Also

http://www.nessus.org/u?399b1f56

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

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

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.

This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

XREF	CWE:693

Plugin Information

Published: 2015/08/22, Modified: 2017/05/16

Plugin Output

tcp/80/www

```
The following pages do not use a clickjacking mitigation response header and contain a clickable
 event :

  - http://ISLAM-KHALIL.station/mutillidae/
  - http://ISLAM-KHALIL.station/mutillidae/index.php
  - http://ISLAM-KHALIL.station/phpMyAdmin/
  - http://ISLAM-KHALIL.station/phpMyAdmin/index.php
  - http://ISLAM-KHALIL.station/twiki/bin/search
  - http://ISLAM-KHALIL.station/twiki/bin/search/Main
  - http://ISLAM-KHALIL.station/twiki/bin/search/Main/SearchResult
  - http://ISLAM-KHALIL.station/twiki/bin/view
  - http://ISLAM-KHALIL.station/twiki/bin/view/Main
  - http://ISLAM-KHALIL.station/twiki/bin/view/Main/WebHome
```

11229 - Web Server info.php / phpinfo.php Detection

Synopsis

The remote web server contains a PHP script that is prone to an information disclosure attack.

Description

Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo()' for debugging purposes. Various PHP applications may also include such a file. By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including :

- The username of the user who installed PHP and if they are a SUDO user.

- The IP address of the host.

- The version of the operating system.

- The web server version.

- The root directory of the web server.

- Configuration information about the remote PHP installation.

Solution

Remove the affected file(s).

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 v2.0 Base Score

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

Plugin Information

Published: 2003/02/12, Modified: 2022/06/01

Plugin Output

tcp/80/www

```
Nessus discovered the following URLs that call phpinfo() :

  - http://ISLAM-KHALIL.station/phpinfo.php
```

```
  - http://ISLAM-KHALIL.station/mutillidae/phpinfo.php
```

51425 - phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)

Synopsis

The remote web server hosts a PHP script that is prone to a cross- site scripting attack.

Description

The version of phpMyAdmin fails to validate BBcode tags in user input to the 'error' parameter of the 'error.php' script before using it to generate dynamic HTML.

An attacker may be able to leverage this issue to inject arbitrary HTML or script code into a user's browser to be executed within the security context of the affected site. For example, this could be used to cause a page with arbitrary text and a link to an external site to be displayed.

See Also

https://www.phpmyadmin.net/security/PMASA-2010-9/

Solution

Upgrade to phpMyAdmin 3.4.0-beta1 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	45633
CVE	CVE-2010-4480
XREF	EDB-ID:15699
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712

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

Plugin Information

Published: 2011/01/06, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Nessus was able to exploit the issue using the following URL :

  http://ISLAM-KHALIL.station/phpMyAdmin/error.php?type=phpmyadmin_pmasa_2010_9.nasl&error=%5ba
%40https%3a%2f%2fwww.phpmyadmin.net%2fsecurity%2fPMASA-2010-9%2f%40_self]Click%20here%5b%2fa]
```

36083 - phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)

Synopsis

The remote web server contains a PHP script that is affected by multiple issues.

Description

The version of phpMyAdmin installed on the remote host fails to sanitize user-supplied input to the 'file_path' parameter of the 'bs_disp_as_mime_type.php' script before using it to read a file and reporting it in dynamically-generated HTML. An unauthenticated, remote attacker may be able to leverage this issue to read arbitrary files, possibly from third-party hosts, or to inject arbitrary HTTP headers in responses sent to third-party users.

Note that the application is also reportedly affected by several other issues, although Nessus has not actually checked for them.

See Also

https://www.phpmyadmin.net/security/PMASA-2009-1/

Solution

Upgrade to phpMyAdmin 3.1.3.1 or apply the patch referenced in the project's advisory.

Risk Factor

Medium

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

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

References

BID	34253
XREF	SECUNIA:34468

Plugin Information

Published: 2009/04/03, Modified: 2022/04/11

Plugin Output

tcp/80/www

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

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

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

Solution

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

Risk Factor

Low

CVSS 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

Published: 2013/10/28, Modified: 2018/07/30

Plugin Output

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
```

153953 - 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) draft-ietf-curdle-ssh-kex-sha2-20. 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

http://www.nessus.org/u?b02d91cd

https://datatracker.ietf.org/doc/html/rfc8732

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

Published: 2021/10/13, Modified: 2021/10/13

Plugin Output

tcp/22/ssh

```
The following weak key exchange algorithms are enabled :

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

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

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

Description

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

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

Solution

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

Risk Factor

Low

CVSS 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

tcp/22/ssh

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

  hmac-md5
  hmac-md5-96
  hmac-sha1-96

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

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

26194 - Web Server Transmits Cleartext Credentials

Synopsis

The remote web server might transmit credentials in cleartext.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS v2.0 Base Score

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

References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information

Published: 2007/09/28, Modified: 2016/11/29

Plugin Output

tcp/80/www

```
Page : /phpMyAdmin/
Destination Page: /phpMyAdmin/index.php

Page : /phpMyAdmin/index.php
Destination Page: /phpMyAdmin/index.php
```

10407 - X Server Detection

Synopsis

An X11 server is listening on the remote host

Description

The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client.

Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

Solution

Restrict access to this port. If the X11 client/server facility is not used, disable TCP support in X11 entirely (-nolisten tcp).

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: 2000/05/12, Modified: 2019/03/05

Plugin Output

tcp/6000/x11

```
X11 Version : 11.0
```

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

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

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

See Also

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

Solution

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

www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information

Published: 2010/04/29, Modified: 2020/06/12

Plugin Output

tcp/0

```
The following hostnames point to the remote host :
  - metasploitable
  - metasploitable.station
```

18261 - Apache Banner Linux Distribution Disclosure

Synopsis

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

Description

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The Linux distribution detected was :
 - Ubuntu 8.04 (gutsy)
```

48204 - Apache HTTP Server Version

Synopsis

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

Description

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

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2020/09/22

Plugin Output

tcp/80/www

```
URL        : http://ISLAM-KHALIL.station/
Version    : 2.2.99
backported : 1
modules    : DAV/2
os         : ConvertedUbuntu
```

39519 - 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

tcp/2121/ftp

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

84574 - Backported Security Patch Detection (PHP)

Synopsis

Security patches have been backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/07, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

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

45590 - Common Platform Enumeration (CPE)

Synopsis

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

Description

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

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

See Also

http://cpe.mitre.org/

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2022/08/02

Plugin Output

tcp/0

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

  cpe:/o:canonical:ubuntu_linux:8.04 -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.2.8 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apache:http_server:2.2.99 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:isc:bind:9.4. -> ISC BIND
  cpe:/a:isc:bind:9.4.2 -> ISC BIND
  cpe:/a:openbsd:openssh:4.7 -> OpenBSD OpenSSH
  cpe:/a:php:php:5.2.4 -> PHP PHP
  cpe:/a:php:php:5.2.4-2ubuntu5.10 -> PHP PHP
  cpe:/a:phpmyadmin:phpmyadmin:3.1.1 -> phpMYAdmin
  cpe:/a:samba:samba:3.0.20 -> Samba Samba
  cpe:/a:twiki:twiki:01_feb_2003 -> TWiki
```

10028 - DNS Server BIND version Directive Remote Version Detection

Synopsis

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

Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

Risk Factor

None

References

XREF	IAVT:0001-T-0583

Plugin Information

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

Plugin Output

udp/53/dns

```
Version : 9.4.2
```

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

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

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

tcp/53/dns

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

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

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

udp/53/dns

72779 - DNS Server Version Detection

Synopsis

Nessus was able to obtain version information on the remote DNS server.

Description

Nessus was able to obtain version information by sending a special TXT record query to the remote host.

Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0937

Plugin Information

Published: 2014/03/03, Modified: 2020/09/22

Plugin Output

tcp/53/dns

```
DNS server answer for "version.bind" (over TCP) :

  9.4.2
```

35371 - DNS Server hostname.bind Map Hostname Disclosure

Synopsis

The DNS server discloses the remote host name.

Description

It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

Solution

It may be possible to disable this feature. Consult the vendor's documentation for more information.

Risk Factor

None

Plugin Information

Published: 2009/01/15, Modified: 2011/09/14

Plugin Output

udp/53/dns

```
The remote host name is :

metasploitable
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

tcp/0

```
The following card manufacturers were identified :

08:00:27:39:6D:CD : PCS Systemtechnik GmbH
```

86420 - 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

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:39:6D:CD
```

49704 - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

Plugin Output

tcp/80/www

```
104 external URLs were gathered on this web server :
URL...                                  - Seen on...


http://TWiki.org/                       - /twiki/bin/view/Main/WebHome
http://TWiki.org/cgi-bin/view/Main/TWikiAdminGroup - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/Main/TWikiUsers - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/AlWilliams - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/AndreaSterbini - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/BookView - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ChangePassword - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ChristopheVermeulen - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ColasNahaboo - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/CrisBailiff - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/DavidWarman - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/DontNotify - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/FileAttachment - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/FormattedSearch - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/HaroldGottschalk - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/InterwikiPlugin - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/JohnAltstadt - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/JohnTalintyre - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/KevinKinnell - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/KlausWriessnegger - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ManagingTopics - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ManagingWebs - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ManpreetSingh - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/NewUserTemplate - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/NicholasLee - /twiki/TWikiHistory.html
http://TWiki.org/cgi- [...]
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220 (vsFTPd 2.3.4)
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

Plugin Output

tcp/2121/ftp

```
The remote FTP banner is :

220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.1.5]
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

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)

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

```
Based on the response to an OPTIONS request :

  - HTTP methods COPY DELETE GET HEAD LOCK MOVE OPTIONS POST PROPFIND
    PROPPATCH TRACE UNLOCK are allowed on :

    /dav

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

    /doc
    /icons
    /mutillidae/documentation
    /mutillidae/styles
    /mutillidae/styles/ddsmoothmenu
    /test
    /test/testoutput
    /twiki
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/80/www

```
The remote web server type is :

Apache/2.2.8 (Ubuntu) DAV/2
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
192.168.1.5 resolves as ISLAM-KHALIL.station.
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

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

  Date: Fri, 05 Aug 2022 14:11:48 GMT
  Server: Apache/2.2.8 (Ubuntu) DAV/2
  X-Powered-By: PHP/5.2.4-2ubuntu5.10
  Content-Length: 891
  Keep-Alive: timeout=15, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>


 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|
```

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

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: 2019/10/04

Plugin Output

icmp/0

```
The remote clock is synchronized with the local clock.
```

11156 - IRC Daemon Version Detection

Synopsis

The remote host is an IRC server.

Description

This plugin determines the version of the IRC daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/19, Modified: 2016/01/08

Plugin Output

tcp/6667/irc

```
The IRC server version is : Unreal3.2.8.1. FhiXOoE [*=2309]
```

10397 - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

Synopsis

It is possible to obtain network information.

Description

It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/445/cifs

```
Here is the browse list of the remote host :

METASPLOITABLE ( os : 0.0 )
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires 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

tcp/445/cifs

```
The remote Operating System is : Unix
The remote native LAN manager is : Samba 3.0.20-Debian
The remote SMB Domain Name is : METASPLOITABLE
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/139/smb

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

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/445/cifs

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

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

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

106716 - 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

tcp/445/cifs

```
The remote host does NOT support the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.0        Windows 8
3.0.2      Windows 8.1
3.1        Windows 10
3.1.1      Windows 10
```

50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - http://ISLAM-KHALIL.station/
  - http://ISLAM-KHALIL.station/dav/
  - http://ISLAM-KHALIL.station/dvwa/
  - http://ISLAM-KHALIL.station/mutillidae/
  - http://ISLAM-KHALIL.station/mutillidae/documentation/
  - http://ISLAM-KHALIL.station/mutillidae/documentation/how-to-access-Mutillidae-over-Virtual-Box-
network.php
  - http://ISLAM-KHALIL.station/mutillidae/documentation/vulnerabilities.php
  - http://ISLAM-KHALIL.station/mutillidae/framer.html
  - http://ISLAM-KHALIL.station/mutillidae/index.php
  - http://ISLAM-KHALIL.station/mutillidae/set-up-database.php
```

```
    - http://ISLAM-KHALIL.station/mutillidae/styles/
    - http://ISLAM-KHALIL.station/mutillidae/styles/ddsmoothmenu/
    - http://ISLAM-KHALIL.station/phpMyAdmin/
    - http://ISLAM-KHALIL.station/phpMyAdmin/index.php
    - http://ISLAM-KHALIL.station/test/
    - http://ISLAM-KHALIL.station/test/testoutput/
    - http://ISLAM-KHALIL.station/twiki/
    - http://ISLAM-KHALIL.station/twiki/TWikiHistory.html
    - http://ISLAM-KHALIL.station/twiki/bin/oops
    - http://ISLAM-KHALIL.station/twiki/bin/oops/Main
    - http://ISLAM-KHALIL.station/twiki/bin/oops/Main/WebHomemailto%3Awebmasteryour
    - http://ISLAM-KHALIL.station/twiki/bin/oops/Main/WebHomemailto%3Awebmasteryour/company
    - http://ISLAM-KHALIL.station/twiki/bin/search
    - http://ISLAM-KHALIL.station/twiki/bin/search/Main
    - http://ISLAM-KHALIL.station/twiki/bin/search/Main/SearchResult
    - http://ISLAM-KHALIL.station/twiki/bin/view
    - http://ISLAM-KHALIL.station/twiki/bin/view/Main
    - http://ISLAM-KHALIL.station/twiki/bin/view/Main/WebHome
```

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

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

http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://ISLAM-KHALIL.station/
  - http://ISLAM-KHALIL.station/dav/
  - http://ISLAM-KHALIL.station/dvwa/
  - http://ISLAM-KHALIL.station/mutillidae/
  - http://ISLAM-KHALIL.station/mutillidae/documentation/
  - http://ISLAM-KHALIL.station/mutillidae/documentation/how-to-access-Mutillidae-over-Virtual-Box-
network.php
  - http://ISLAM-KHALIL.station/mutillidae/documentation/vulnerabilities.php
  - http://ISLAM-KHALIL.station/mutillidae/framer.html
  - http://ISLAM-KHALIL.station/mutillidae/index.php
  - http://ISLAM-KHALIL.station/mutillidae/set-up-database.php
  - http://ISLAM-KHALIL.station/mutillidae/styles/
  - http://ISLAM-KHALIL.station/mutillidae/styles/ddsmoothmenu/
  - http://ISLAM-KHALIL.station/phpMyAdmin/
  - http://ISLAM-KHALIL.station/phpMyAdmin/index.php
  - http://ISLAM-KHALIL.station/test/
```

```
    - http://ISLAM-KHALIL.station/test/testoutput/
    - http://ISLAM-KHALIL.station/twiki/
    - http://ISLAM-KHALIL.station/twiki/TWikiHistory.html
    - http://ISLAM-KHALIL.station/twiki/bin/oops
    - http://ISLAM-KHALIL.station/twiki/bin/oops/Main
    - http://ISLAM-KHALIL.station/twiki/bin/oops/Main/WebHomemailto%3Awebmasteryour
    - http://ISLAM-KHALIL.station/twiki/bin/oops/Main/WebHomemailto%3Awebmasteryour/company
    - http://ISLAM-KHALIL.station/twiki/bin/search
    - http://ISLAM-KHALIL.station/twiki/bin/search/Main
    - http://ISLAM-KHALIL.station/twiki/bin/search/Main/SearchResult
    - http://ISLAM-KHALIL.station/twiki/bin/view
    - http://ISLAM-KHALIL.station/twiki/bin/view/Main
    - http://ISLAM-KHALIL.station/twiki/bin/view/Main/WebHome
```

10437 - NFS Share Export List

Synopsis

The remote NFS server exports a list of shares.

Description

This plugin retrieves the list of NFS exported shares.

See Also

http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

Solution

Ensure each share is intended to be exported.

Risk Factor

None

Plugin Information

Published: 2000/06/07, Modified: 2019/10/04

Plugin Output

tcp/2049/rpc-nfs

```
Here is the export list of ISLAM-KHALIL.station :
  /mnt/newdisk 192.168.1.5
```

112154 - Nessus Launched Plugin List

Synopsis

This plugin displays information about the launched plugins.

Description

This plugin displays the list of launched plugins in a semicolon delimited list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/08/28, Modified: 2018/09/24

Plugin Output

tcp/0

```
56009;20869;11761;35308;45405;11663;82710;35610;107222;11655;17597;15982;81512;31345;57766;27803;19309;11017;87314
 [...]
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/21/ftp

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/22/ssh

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/23/telnet

```
Port 23/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/25

```
Port 25/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/53/dns

```
Port 53/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/80/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/111/rpc-portmapper

```
Port 111/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/139/smb

```
Port 139/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/445/cifs

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/512

```
Port 512/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/513/rlogin

```
Port 513/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/514/rsh

```
Port 514/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/1099/rmi_registry

```
Port 1099/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/2049/rpc-nfs

```
Port 2049/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/2121/ftp

```
Port 2121/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/3632

```
Port 3632/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/5900/vnc

```
Port 5900/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/6000/x11

```
Port 6000/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/6667/irc

```
Port 6667/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/8180

```
Port 8180/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/8787

```
Port 8787/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2022/06/09

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.3.0
Nessus build : 20080
Plugin feed version : 202208050547
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian9-x86-64
Scan type : Normal
Scan name : Meta-Adv-scan
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.1.15
Port scanner(s) : nessus_syn_scanner
Port range : Default
Ping RTT : 148.671 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : enabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Scan Start Date : 2022/8/5 10:01 EDT
Scan duration : 1134 sec
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2022/03/09

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
Confidence level : 95
Method : HTTP


The remote host is running Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
```

117886 - 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

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.
```

48243 - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0936

Plugin Information

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

Plugin Output

tcp/80/www

```
Nessus was able to identify the following PHP version information :

  Version : 5.2.4-2ubuntu5.10
  Source  : X-Powered-By: PHP/5.2.4-2ubuntu5.10
  Source  : http://ISLAM-KHALIL.station/phpinfo.php
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

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

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: 2022/08/04

Plugin Output

tcp/0

```
. You need to take the following 5 actions :

[ ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS (139915) ]

+ Action to take : Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).


[ Samba Badlock Vulnerability (90509) ]

+ Action to take : Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.


[ TWiki 'rev' Parameter Arbitrary Command Execution (19704) ]

+ Action to take : Apply the appropriate hotfix referenced in the vendor advisory.


[ UnrealIRCd Backdoor Detection (46882) ]

+ Action to take : Re-download the software, verify it using the published MD5 / SHA1 checksums, and
 re-install it.
```

```
[ phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3) (125855) ]

+ Action to take : Upgrade to phpMyAdmin version 4.8.6 or later.
Alternatively, apply the patches referenced in the vendor advisories.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

22227 - RMI Registry Detection

Synopsis

An RMI registry is listening on the remote host.

Description

The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

See Also

https://docs.oracle.com/javase/1.5.0/docs/guide/rmi/spec/rmiTOC.html

http://www.nessus.org/u?b6fd7659

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/08/16, Modified: 2022/06/01

Plugin Output

tcp/1099/rmi_registry
tcp/1099/rmi_registry

```
Valid response recieved for port 1099:
0x00:  51 AC ED 00 05 77 0F 01 E2 5C 7B 0E 00 00 01 82    Q....w...\{.....
0x10:  6E 52 E7 97 80 02 75 72 00 13 5B 4C 6A 61 76 61    nR....ur..[Ljava
0x20:  2E 6C 61 6E 67 2E 53 74 72 69 6E 67 3B AD D2 56    .lang.String;..V
0x30:  E7 E9 1D 7B 47 02 00 00 70 78 70 00 00 00 00       ...{G...pxp....
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/111/rpc-portmapper

```
The following RPC services are available on TCP port 111 :

 - program: 100000 (portmapper), version: 2
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/111/rpc-portmapper

```
The following RPC services are available on UDP port 111 :

 - program: 100000 (portmapper), version: 2
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/2049/rpc-nfs

```
The following RPC services are available on TCP port 2049 :

 - program: 100003 (nfs), version: 2
 - program: 100003 (nfs), version: 3
 - program: 100003 (nfs), version: 4
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/2049/rpc-nfs

```
The following RPC services are available on UDP port 2049 :

 - program: 100003 (nfs), version: 2
 - program: 100003 (nfs), version: 3
 - program: 100003 (nfs), version: 4
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/40003/rpc-nlockmgr

```
The following RPC services are available on UDP port 40003 :

 - program: 100021 (nlockmgr), version: 1
 - program: 100021 (nlockmgr), version: 3
 - program: 100021 (nlockmgr), version: 4
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/46789/rpc-status

```
The following RPC services are available on TCP port 46789 :

 - program: 100024 (status), version: 1
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/47560/rpc-status

```
The following RPC services are available on UDP port 47560 :

 - program: 100024 (status), version: 1
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/53844/rpc-nlockmgr

```
The following RPC services are available on TCP port 53844 :

 - program: 100021 (nlockmgr), version: 1
 - program: 100021 (nlockmgr), version: 3
 - program: 100021 (nlockmgr), version: 4
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/57261/rpc-mountd

```
The following RPC services are available on UDP port 57261 :

 - program: 100005 (mountd), version: 1
 - program: 100005 (mountd), version: 2
 - program: 100005 (mountd), version: 3
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/57371/rpc-mountd

```
The following RPC services are available on TCP port 57371 :

 - program: 100005 (mountd), version: 1
 - program: 100005 (mountd), version: 2
 - program: 100005 (mountd), version: 3
```

53335 - RPC portmapper (TCP)

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/04/08, Modified: 2011/08/29

Plugin Output

tcp/111/rpc-portmapper

10223 - RPC portmapper Service Detection

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

Solution

n/a

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0632

Plugin Information

Published: 1999/08/19, Modified: 2019/10/04

Plugin Output

udp/111/rpc-portmapper

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-sha1

The server supports the following options for server_host_key_algorithms :

  ssh-dss
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

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

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

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

149334 - 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

tcp/22/ssh

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2021/01/19

Plugin Output

tcp/22/ssh

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

  - 1.99
  - 2.0
```

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

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

Description

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

  hmac-sha1
  hmac-sha1-96

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

  hmac-sha1
  hmac-sha1-96
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0933

Plugin Information

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

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
SSH supported authentication : publickey,password
```

25240 - 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: 2019/11/22

Plugin Output

tcp/445/cifs

104887 - 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

tcp/445/cifs

```
The remote Samba Version is : Samba 3.0.20-Debian
```

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

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/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

tcp/445/cifs

```
The remote host supports SMBv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2022/07/26

Plugin Output

tcp/21/ftp

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2022/07/26

Plugin Output

tcp/22/ssh

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2022/07/26

Plugin Output

tcp/23/telnet

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2022/07/26

Plugin Output

tcp/80/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2022/07/26

Plugin Output

tcp/2121/ftp

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2022/07/26

Plugin Output

tcp/5900/vnc

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

17975 - Service Detection (GET request)

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0935

Plugin Information

Published: 2005/04/06, Modified: 2021/10/27

Plugin Output

tcp/6667/irc

```
An IRC daemon is listening on this port.
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

tcp/0

11819 - TFTP Daemon Detection

Synopsis

A TFTP server is listening on the remote port.

Description

The remote host is running a TFTP (Trivial File Transfer Protocol) daemon. TFTP is often used by routers and diskless hosts to retrieve their configuration. It can also be used by worms to propagate.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 2003/08/13, Modified: 2019/11/22

Plugin Output

udp/69/tftp

19941 - TWiki Detection

Synopsis

The remote web server hosts a Wiki system written in Perl.

Description

The remote host is running TWiki, an open source wiki system written in Perl.

See Also

http://twiki.org

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/10/06, Modified: 2022/06/01

Plugin Output

tcp/80/www

```
URL     : http://ISLAM-KHALIL.station/twiki/bin/view/Main
Version : 01 Feb 2003
```

110723 - 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: 2021/11/19

Plugin Output

tcp/0

```
SSH was detected on port 22 but no credentials were provided.
SSH local checks were not enabled.
```

10281 - Telnet Server Detection

Synopsis

A Telnet server is listening on the remote port.

Description

The remote host is running a Telnet server, a remote terminal server.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2020/06/12

Plugin Output

tcp/23/telnet

```
Here is the banner from the remote Telnet server :

------------------------------ snip ------------------------------
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login:
------------------------------ snip ------------------------------
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.15 to 192.168.1.5 :
192.168.1.15
192.168.1.5

Hop Count: 1
```

11154 - Unknown Service Detection: Banner Retrieval

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2022/07/26

Plugin Output

tcp/8787

```
If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

  Port   : 8787
  Type   : get_http
  Banner :
0x0000:  00 00 00 03 04 08 46 00 00 03 A1 04 08 6F 3A 16    ......F......o:.
           0x0010:  44 52 62 3A 3A 44 52 62 43 6F 6E 6E 45 72 72 6F    DRb::DRbConnErro
           0x0020:  72 07 3A 07 62 74 5B 17 22 2F 2F 75 73 72 2F 6C    r.:.bt[."//usr/l
           0x0030:  69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F    ib/ruby/1.8/drb/
           0x0040:  64 72 62 2E 72 62 3A 35 37 33 3A 69 6E 20 60 6C    drb.rb:573:in `l
           0x0050:  6F 61 64 27 22 37 2F 75 73 72 2F 6C 69 62 2F 72    oad'"7/usr/lib/r
           0x0060:  75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62 2E    uby/1.8/drb/drb.
           0x0070:  72 62 3A 36 31 32 3A 69 6E 20 60 72 65 63 76 5F    rb:612:in `recv_
           0x0080:  72 65 71 75 65 73 74 27 22 37 2F 75 73 72 2F 6C    request'"7/usr/l
           0x0090:  69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F    ib/ruby/1.8/drb/
           0x00A0:  64 72 62 2E 72 62 3A 39 31 31 3A 69 6E 20 60 72    drb.rb:911:in `r
           0x00B0:  65 63 76 5F 72 65 71 75 65 73 74 27 22 3C 2F 75    ecv_request'"</u
           0x00C0:  73 72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F    sr/lib/ruby/1.8/
           0x00D0:  64 72 62 2F 64 72 62 2E 72 62 3A 31 35 33 30 3A    drb/drb.rb:1530:
           0x00E0:  69 6E 20 60 69 6E 69 74 5F 77 69 74 68 5F 63 6C    in `init_with_cl
           0x00F0:  69 65 6E 74 27 22 39 2F 75 73 72 2F 6C 69 62 2F    ient'"9/usr/lib/
           0x0100:  72 75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62    ruby/1.8/drb/drb
           0x0110:  2E 72 62 3A 31 35 34 32 3A 69 6E 20 60 73 65 74    .rb:1542:in `set
           0x0120:  75 70 5F 6D 65 73 73 61 67 65 27 22 33 2F 75 73    up_message'"3/us
           0x0130:  72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F 64    r/lib/ruby/1.8/d
           0x0140:  72 62 2F 64 72 62 2E 72 62 3A 31 34 39 34  [...]
```

19288 - VNC Server Security Type Detection

Synopsis

A VNC server is running on the remote host.

Description

This script checks the remote VNC server protocol version and the available 'security types'.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/07/22, Modified: 2021/07/13

Plugin Output

tcp/5900/vnc

```
\nThe remote VNC server chose security type #2 (VNC authentication)
```

65792 - VNC Server Unencrypted Communication Detection

Synopsis

A VNC server with one or more unencrypted 'security-types' is running on the remote host.

Description

This script checks the remote VNC server protocol version and the available 'security types' to determine if any unencrypted 'security-types' are in use or available.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/04/03, Modified: 2014/03/12

Plugin Output

tcp/5900/vnc

```
The remote VNC server supports the following security type
which does not perform full data communication encryption :

  2 (VNC authentication)
```

10342 - VNC Software Detection

Synopsis

The remote host is running a remote display software (VNC).

Description

The remote host is running VNC (Virtual Network Computing), which uses the RFB (Remote Framebuffer) protocol to provide remote access to graphical user interfaces and thus permits a console on the remote host to be displayed on another.

See Also

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

Solution

Make sure use of this software is done in accordance with your organization's security policy and filter incoming traffic to this port.

Risk Factor

None

Plugin Information

Published: 2000/03/07, Modified: 2017/06/12

Plugin Output

tcp/5900/vnc

```
The highest RFB protocol version supported by the server is :

  3.3
```

135860 - 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 vunerabilities 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: 2022/07/19

Plugin Output

tcp/445/cifs

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

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/80/www

```
The following cookies are expired :

Name : pma_collation_connection
Path : /phpMyAdmin/
Value : deleted
Domain :
Version : 1
Expires : Thu, 05-Aug-2021 14:13:37 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_theme
Path : /phpMyAdmin/
Value : deleted
```

```
Domain :
Version : 1
Expires : Thu, 05-Aug-2021 14:12:55 GMT
Comment :
Secure : 0
Httponly : 0
Port :
```

85601 - Web Application Cookies Not Marked HttpOnly

Synopsis

HTTP session cookies might be vulnerable to cross-site scripting attacks.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

See Also

https://www.owasp.org/index.php/HttpOnly

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801

XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/80/www

```
The following cookies do not set the HttpOnly cookie flag :

Name : security
Path : /
Value : high
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : 9db53fd980d70bacc273a3a2daf39aaf
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure'

cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

See Also

https://www.owasp.org/index.php/SecureFlag

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:522
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/80/www

```
The following cookies do not set the secure cookie flag :

Name : pma_lang
Path : /phpMyAdmin/
Value : en-utf-8
Domain :
Version : 1
Expires : Sun, 04-Sep-2022 14:05:33 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : security
Path : /
Value : high
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : phpMyAdmin
Path : /phpMyAdmin/
Value : 939627539bcdd6aec7f95bc2f0bc9e05fe67cf46
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_charset
Path : /phpMyAdmin/
Value : utf-8
Domain :
Version : 1
Expires : Sun, 04-Sep-2022 14:05:33 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_theme
Path : /phpMyAdmin/
Value : original
Domain :
Version : 1
Expires : Sun, 04-Sep-2022 14:05:33 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PHPSESSID
Path : /
Value : 9db53fd980d70bacc273a3a2daf39aaf
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 0
Port :
```

91815 - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

tcp/80/www

```
The following sitemap was created from crawling linkable content on the target host :

  - http://ISLAM-KHALIL.station/
  - http://ISLAM-KHALIL.station/dav/
  - http://ISLAM-KHALIL.station/dvwa/
  - http://ISLAM-KHALIL.station/mutillidae/
  - http://ISLAM-KHALIL.station/mutillidae/documentation/
  - http://ISLAM-KHALIL.station/mutillidae/documentation/Mutillidae-Test-Scripts.txt
  - http://ISLAM-KHALIL.station/mutillidae/documentation/how-to-access-Mutillidae-over-Virtual-Box-
network.php
  - http://ISLAM-KHALIL.station/mutillidae/documentation/mutillidae-installation-on-xampp-win7.pdf
  - http://ISLAM-KHALIL.station/mutillidae/documentation/sqlmap-help.txt
  - http://ISLAM-KHALIL.station/mutillidae/documentation/vulnerabilities.php
  - http://ISLAM-KHALIL.station/mutillidae/favicon.ico
  - http://ISLAM-KHALIL.station/mutillidae/framer.html
  - http://ISLAM-KHALIL.station/mutillidae/index.php
  - http://ISLAM-KHALIL.station/mutillidae/set-up-database.php
  - http://ISLAM-KHALIL.station/mutillidae/styles/
  - http://ISLAM-KHALIL.station/mutillidae/styles/ddsmoothmenu/
  - http://ISLAM-KHALIL.station/mutillidae/styles/ddsmoothmenu/ddsmoothmenu-v.css
  - http://ISLAM-KHALIL.station/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
  - http://ISLAM-KHALIL.station/mutillidae/styles/ddsmoothmenu/readme.txt
  - http://ISLAM-KHALIL.station/mutillidae/styles/global-styles.css
  - http://ISLAM-KHALIL.station/phpMyAdmin/
```

```
    - http://ISLAM-KHALIL.station/phpMyAdmin/favicon.ico
    - http://ISLAM-KHALIL.station/phpMyAdmin/index.php
    - http://ISLAM-KHALIL.station/phpMyAdmin/phpmyadmin.css.php
    - http://ISLAM-KHALIL.station/phpMyAdmin/print.css
    - http://ISLAM-KHALIL.station/test/
    - http://ISLAM-KHALIL.station/test/testoutput/
    - http://ISLAM-KHALIL.station/test/testoutput/ESAPI_logging_file_test
    - http://ISLAM-KHALIL.station/twiki/
    - http://ISLAM-KHALIL.station/twiki/TWikiHistory.html
    - http://ISLAM-KHALIL.station/twiki/bin/oops
    - http://ISLAM-KHALIL.station/twiki/bin/oops/Main
    - http://ISLAM-KHALIL.station/twiki/bin [...]
```

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

Solution

n/a

Risk Factor

None

References

XREF OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2021/08/17

Plugin Output

tcp/80/www

```
The following directories were discovered:
/cgi-bin, /doc, /test, /icons, /phpMyAdmin, /twiki/bin

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

49705 - Web Server Harvested Email Addresses

Synopsis

Email addresses were harvested from the web server.

Description

Nessus harvested HREF mailto: links and extracted email addresses by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2018/05/24

Plugin Output

tcp/80/www

```
The following email address has been gathered :

- 'SomeWikiName@somewhere.test', referenced from :
   /twiki/TWikiHistory.html
```

11419 - Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor

None

Plugin Information

Published: 2003/03/19, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
The following office-related files are available on the remote server :

  - Adobe Acrobat files (.pdf) :
    /mutillidae/documentation/mutillidae-installation-on-xampp-win7.pdf
```

10662 - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/05/04, Modified: 2022/07/19

Plugin Output

tcp/80/www

```
Webmirror performed 75 queries in 9s (8.0333 queries per second)

The following CGIs have been discovered :


+ CGI : /phpMyAdmin/phpmyadmin.css.php
  Methods : GET
  Argument : js_frame
   Value: right
  Argument : nocache
   Value: 2457687151
  Argument : token
   Value: 4d1c7633379bb927e73a1e7cd368c7ff


+ CGI : /phpMyAdmin/index.php
  Methods : POST
  Argument : db
  Argument : lang
  Argument : pma_password
  Argument : pma_username
  Argument : server
   Value: 1
  Argument : table
  Argument : token
   Value: 4d1c7633379bb927e73a1e7cd368c7ff
```

```
+ CGI : /mutillidae/index.php
  Methods : GET
  Argument : do
   Value: toggle-security
  Argument : page
   Value: notes.php
  Argument : username
   Value: anonymous


+ CGI : /mutillidae/
  Methods : GET
  Argument : page
   Value: source-viewer.php


+ CGI : /rdiff/TWiki/TWikiHistory
  Methods : GET
  Argument : rev1
   Value: 1.8
  Argument : rev2
   Value: 1.7


+ CGI : /view/TWiki/TWikiHistory
  Methods : GET
  Argument : rev
   Value: 1.7


+ CGI : /oops/TWiki/TWikiHistory
  Methods : GET
  Argument : param1
   Value: 1.10
  Argument : template
   Value: oopsrev


+ CGI : /twiki/bin/view/Main/WebHome
  Methods : GET
  Argument : topic


+ CGI : /twiki/bin/search/Main/SearchResult
  Methods : GET
  Argument : search


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/edit/Main/WebHome
  Methods : GET
  Argument : t
   Value: 1659708337


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/search/Main/SearchResult
  Methods : GET
  Argument : regex
   Value: on
  Argument : scope
   Value: text
  Argument : search
   Value: Web%20*Home%5B%5EA-Za-z%5D


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/view/Main/WebHome
  Methods : GET
  Argument : rev
   Value: 1.18
  Argument : skin
```

```
    Value: print


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/rdiff/Main/WebHome
  Methods : GET
  Argument : rev1
    Value: 1.19
  Argument : rev2
    Value: 1.18


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/oops/Main/WebHome
  Methods : GET
  Argument : param1
    Value: 1.20
  Argumen [...]
```

11424 - WebDAV Detection

Synopsis

The remote server is running with WebDAV enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

Solution

http://support.microsoft.com/default.aspx?kbid=241520

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2011/03/14

Plugin Output

tcp/80/www

24004 - WebDAV Directory Enumeration

Synopsis

Several directories on the remote host are DAV-enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

Solution

Disable DAV support if you do not use it.

Risk Factor

None

Plugin Information

Published: 2007/01/11, Modified: 2011/03/14

Plugin Output

tcp/80/www

```
The following directories are DAV enabled :
 - /dav/
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

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

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

Plugin Output

udp/137/netbios-ns

```
The following 5 NetBIOS names have been gathered :

 METASPLOITABLE   = Computer name
 METASPLOITABLE   = Messenger Service
 METASPLOITABLE   = File Server Service
 WORKGROUP        = Workgroup / Domain name
 WORKGROUP        = Browser Service Elections

This SMB server seems to be a Samba server - its MAC address is NULL.
```

17219 - phpMyAdmin Detection

Synopsis

The remote web server hosts a database management application written in PHP.

Description

The remote host is running phpMyAdmin, a web-based MySQL administration tool written in PHP.

See Also

https://www.phpmyadmin.net/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/02/25, Modified: 2022/06/01

Plugin Output

tcp/80/www

```
The following instance of phpMyAdmin was detected on the remote host :

  Version : 3.1.1
  URL     : http://ISLAM-KHALIL.station/phpMyAdmin/
```

52703 - vsftpd Detection

Synopsis

An FTP server is listening on the remote port.

Description

The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.

See Also

http://vsftpd.beasts.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/03/17, Modified: 2019/11/22

Plugin Output

tcp/21/ftp

```
Source  : 220 (vsFTPd 2.3.4)
Version : 2.3.4
```