Task Potato Advanced

Report generated by Nessus™ Mon, 01 Jul 2024 17:02:58 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

10.0.2.11

0	1	2	3	41
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Mon Jul 1 16:55:50 2024
End time: Mon Jul 1 17:02:58 2024

Host Information

IP: 10.0.2.11
MAC Address: 08:00:27:98:34:29
OS: Linux Kernel 2.6

Vulnerabilities

42424 - CGI Generic SQL Injection (blind)

Synopsis

A CGI application hosted on the remote web server is potentially prone to SQL injection attack.

Description

By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a very different response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database.

An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

See Also

http://www.securiteam.com/securityreviews/5DP0N1P76E.html

http://www.nessus.org/u?ed792cf5

http://www.nessus.org/u?11ab1866

Solution

Modify the affected CGI scripts so that they properly escape arguments.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:20
XREF	CWE:77
XREF	CWE:89
XREF	CWE:91
XREF	CWE:203
XREF	CWE:643
XREF	CWE:713
XREF	CWE:722
XREF	CWE:727
XREF	CWE:751
XREF	CWE:801
XREF	CWE:810
XREF	CWE:928
XREF	CWE:929

Plugin Information

Published: 2009/11/06, Modified: 2024/06/14

Plugin Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to blind SQL injection :

+ The 'login' parameter of the /admin/index.php CGI :

/admin/index.php?username=&password=&login=1zz&password=&login=1yy

-------- output --------
<body>

<p>Bad user/password! </br> Return to the <a href="index.php">login page
</a> <p>
```

```
-------- vs --------
<body>


  <form action="index.php?login=1" method="POST">
------------------------
```

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

Synopsis

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

Description

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

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

See Also

https://terrapin-attack.com/

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-48795

Plugin Information

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

Plugin Output

tcp/22/ssh

```
Supports following ChaCha20-Poly1305 Client to Server algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha1-etm@openssh.com
Supports following ChaCha20-Poly1305 Server to Client algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : hmac-sha1-etm@openssh.com
```

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://10.0.2.11/admin/
  - http://10.0.2.11/admin/index.php
```

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

Low

VPR Score

4.2

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/05/03

Plugin Output

icmp/0

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

42057 - Web Server Allows Password Auto-Completion

Synopsis

The 'autocomplete' attribute is not disabled on password fields.

Description

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

Low

Plugin Information

Published: 2009/10/07, Modified: 2023/07/17

Plugin Output

tcp/80/www

```
Page : /admin/
Destination Page: /admin/index.php?login=1

Page : /admin/index.php
Destination Page: /admin/index.php?login=1
```

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 : /admin/
Destination Page: /admin/index.php?login=1

Page : /admin/index.php
Destination Page: /admin/index.php?login=1
```

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-0030
XREF	IAVT:0001-T-0530

Plugin Information

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

Plugin Output

tcp/80/www

```
URL        : http://10.0.2.11/
Version    : 2.4.99
Source     : Server: Apache/2.4.41 (Ubuntu)
backported : 1
os         : ConvertedUbuntu
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/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.
```

33817 - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/26, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

arbitrary command execution (time based) : S=18         SP=18        AP=42        SC=0         AC=48

format string                            : S=6          SP=6         AP=14        SC=0         AC=16

cross-site scripting (comprehensive test): S=51         SP=51        AP=119       SC=0
 AC=136
injectable parameter                     : S=6          SP=6         AP=14        SC=0         AC=16

arbitrary command execution              : S=66         SP=66        AP=154       SC=0
 AC=176
local file inclusion                     : S=12         SP=12        AP=28        SC=0         AC=32

directory traversal                      : S=87         SP=87        AP=203       SC=0
 AC=232
web code injection                       : S=3          SP=3         AP=7         SC=0         AC=8

blind SQL injection (4 requests)         : S=12         SP=12        AP=28        SC=0         AC=32
```

```
persistent XSS                          : S=12        SP=12        AP=28        SC=0         AC=32

directory traversal (write access)      : S=6         SP=6         AP=14        SC=0         AC=16

XML injection                           : S=3         SP=3         AP=7         SC=0         AC=8

blind SQL injection                     : S=36        SP=36        AP=84        SC=0         AC=96

SQL injection                           : S=84        SP=84        AP=196       SC=0
 AC=224
directory traversal (extended test)     : S=153       SP=153       AP=357       SC=0
 AC=408
SSI injection                           : S=9         SP=9         AP=21        SC=0         AC=24

unseen parameters                       : S=105       SP=105       AP=245       SC=0
 AC=280
SQL injection (2nd order)              [...]
```

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: 2024/06/24

Plugin Output

tcp/0

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

  cpe:/o:linux:linux_kernel -> Linux Kernel

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.4.41 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:openbsd:openssh:8.2 -> OpenBSD OpenSSH
  cpe:/a:openbsd:openssh:8.2p1 -> OpenBSD OpenSSH
```

132634 - Deprecated SSLv2 Connection Attempts

Synopsis

Secure Connections, using a deprecated protocol were attempted as part of the scan

Description

This plugin enumerates and reports any SSLv2 connections which were attempted as part of a scan. This protocol has been deemed prohibited since 2011 because of security vulnerabilities and most major ssl libraries such as openssl, nss, mbed and wolfssl do not provide this functionality in their latest versions. This protocol has been deprecated in Nessus 8.9 and later.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/01/06, Modified: 2020/01/06

Plugin Output

tcp/0

```
Nessus attempted the following SSLv2 connection(s) as part of this scan:

Plugin ID: 42476
Timestamp: 2024-07-01 20:56:19
Port: 22
```

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: 2022/09/09

Plugin Output

tcp/0

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

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 :

08:00:27:98:34:29 : 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:
  - 08:00:27:98:34:29
```

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

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0943

Plugin Information

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

Plugin Output

tcp/2112/ftp

```
The remote FTP banner is :

220 ProFTPD Server (Debian) [::ffff:10.0.2.11]
```

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 GET HEAD OPTIONS POST are allowed on :

    /icons


Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /admin
    /icons
```

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/2.4.41 (Ubuntu)
```

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

```
10.0.2.11 resolves as potato.
```

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 is enabled, etc...

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Mon, 01 Jul 2024 20:56:33 GMT
  Server: Apache/2.4.41 (Ubuntu)
  Vary: Accept-Encoding
  Content-Length: 245
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=UTF-8

Response Body :

<html>
<head><title>Potato company</title></head>
<body>
  <h1>Potato company</h1>
  <p>At the moment, there is nothing. This site is under construction. To make you wait, here is a
 photo of a potato:</p>
  <img src="potato.jpg">
```

```
</body>
<html>
```

14788 - IP Protocols Scan

Synopsis

This plugin detects the protocols understood by the remote IP stack.

Description

This plugin detects the protocols understood by the remote IP stack.

See Also

http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/09/22, Modified: 2022/08/15

Plugin Output

tcp/0

```
The following IP protocols are accepted on this host:
1ICMP
2IGMP
6TCP
17UDP
103PIM
136UDPLite
```

46215 - Inconsistent Hostname and IP Address

Synopsis

The remote host's hostname is not consistent with DNS information.

Description

The name of this machine either does not resolve or resolves to a different IP address.

This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host.

As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.

Solution

Fix the reverse DNS or host file.

Risk Factor

None

Plugin Information

Published: 2010/05/03, Modified: 2016/08/05

Plugin Output

tcp/0

```
The host name 'potato' does not resolve to an IP address
```

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://10.0.2.11/
  - http://10.0.2.11/admin/
  - http://10.0.2.11/admin/index.php
```

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://10.0.2.11/
  - http://10.0.2.11/admin/
  - http://10.0.2.11/admin/index.php
```

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: 2024/06/04

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.7.4
Nessus build : 20055
Plugin feed version : 202407011351
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : Task Potato Advanced
```

```
Scan policy used : Advanced Scan
Scanner IP : 10.0.2.15
Port scanner(s) : nessus_tcp_scanner
Port range : 1-65535
Ping RTT : 262.608 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : yes
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : single
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/7/1 16:55 EDT
Scan duration : 423 sec
Scan for malware : no
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/22/ssh

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

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/80/www

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

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/2112/ftp

```
Port 2112/tcp was found to be open
```

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: 2024/06/19

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP


The remote host is running Linux Kernel 2.6
```

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.
```

181418 - OpenSSH Detection

Synopsis

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

Description

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

See Also

https://www.openssh.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2024/06/28

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 8.2p1
Banner  : SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
```

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: 2024/06/27

Plugin Output

tcp/0

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

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

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

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 :

  curve25519-sha256
  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha256
  diffie-hellman-group16-sha512
  diffie-hellman-group18-sha512
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

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

The server supports the following options for encryption_algorithms_client_to_server :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
```

```
  chacha20-poly1305@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

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-etm@openssh.com

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

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

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_8.2p1 Ubuntu-4ubuntu0.1
SSH supported authentication : publickey,password
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

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: 2024/03/26

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: 2024/03/26

Plugin Output

tcp/2112/ftp

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

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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: 2024/04/19

Plugin Output

tcp/0

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

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: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.0.2.15 to 10.0.2.11 :
10.0.2.15
10.0.2.11

Hop Count: 1
```

40773 - Web Application Potentially Sensitive CGI Parameter Detection

Synopsis

An application was found that may use CGI parameters to control sensitive information.

Description

According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. These parameters should be examined to determine what type of data is controlled and if it poses a security risk.

** This plugin only reports information that may be useful for auditors

** or pen-testers, not a real flaw.

Solution

Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.

Risk Factor

None

Plugin Information

Published: 2009/08/25, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
Potentially sensitive parameters for CGI /admin/index.php :

password : Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack
```

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://10.0.2.11/
  - http://10.0.2.11/admin/
  - http://10.0.2.11/admin/index.php

Attached is a copy of the sitemap file.
```

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: 2024/06/07

Plugin Output

tcp/80/www

```
The following directories were discovered:
/admin, /icons

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
```

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: 2024/05/20

Plugin Output

tcp/80/www

```
Webmirror performed 5 queries in 1s (5.000 queries per second)

The following CGIs have been discovered :


+ CGI : /admin/index.php
  Methods : POST
  Argument : login
   Value: 1
  Argument : password
  Argument : username
```