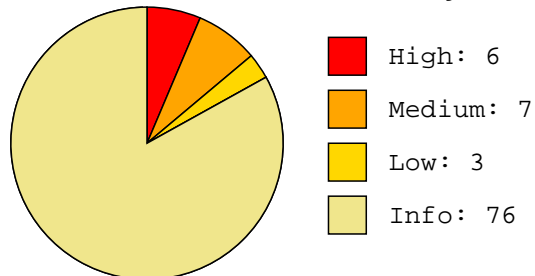




: I.T Security Vulnerability Report

Job Name:	msf before fix	Scan time:	2020-05-13 20:39:31
Profile:	Default - Non destructive Full and Fast scan	Generated:	2020-05-13 20:41:01

Total number of vulnerabilities identified on 1 system(s)



Total number of vulnerabilities identified per system

HostIP	HostName	Critical	High	Med	Low	Info
192.168.2.200	msf	--	6	7	3	76

192.168.2.200

msf

High:

Drupal Coder Remote Code Execution

Risk: High

Application: http

Port: 80

Protocol: tcp

ScriptID: 105818

Vulnerability Detection Result:

Vulnerable url: http://192.168.2.200/drupal/sites/all/modules/coder/coder_upgrade/scripts/coder_upgrade.run.php

Summary:

The remote Drupal installation is prone to a remote code execution vulnerability.

Vulnerability Detection Method:

Check for known error message from affected modules

Solution:

Install the latest version:

Insight:

The Coder module checks your Drupal code against coding standards and other best practices. It can also fix coding standard violations and perform basic upgrades on modules. The module doesn't sufficiently validate user inputs in a script file that has the php extension. A malicious unauthenticated user can make requests directly to this file to execute arbitrary php code.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

References:

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

CVSS Base Score: 10.0

Family name: Web application abuses

Category: attack

Copyright: This script is Copyright (C) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 12313 \$

High:

Drupal Core SQL Injection Vulnerability

Risk: High

Application: http

Port: 80

Protocol: tcp

ScriptID: 105101

Impact:

Exploiting this issue could allow an attacker to execute arbitrary code, to gain elevated privileges and to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

Summary:

Drupal is prone to an SQL-injection vulnerability

Vulnerability Detection Method:

Send a special crafted HTTP POST request and check the response.

Affected Software/OS:

Drupal 7.x versions prior to 7.32 are vulnerable.

Solution:

Updates are available

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Insight:

Drupal fails to sufficiently sanitize user-supplied data before using it in an SQL query.

References:

<http://www.securityfocus.com/bid/70595>

<http://drupal.org/>

CVSS Base Score: 7.5

Family name: Web application abuses

Category: attack

Copyright: This script is Copyright (C) 2014 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 13659 \$

CVEs: CVE-2014-3704

High:

ProFTPD `mod_copy` Unauthenticated Copying Of Files Via SITE CPFR/CPTO

Risk: High

Application: ftp

Port: 21

Protocol: tcp

ScriptID: 105254

Vulnerability Detection Result:

The target was found to be vulnerable

Summary:

ProFTPD is prone to an unauthenticated copying of files vulnerability.

Impact:

Under some circumstances this could result in remote code execution

Vulnerability Detection Method:

Try to copy /etc/passwd to /tmp/passwd.copy with SITE CPFR/CPTO

Solution:

Ask the vendor for an update

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

References:

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

CVSS Base Score: 10.0

Family name: FTP

Category: attack

Copyright: This script is Copyright (C) 2015 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 11831 \$

CVEs: CVE-2015-3306

High:

Check for Backdoor in UnrealIRCd

Risk: High

Application: irc

Port: 6667

Protocol: tcp

ScriptID: 80111

Summary:

Detection of backdoor in UnrealIRCd.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Insight:

Remote attackers can exploit this issue

to execute arbitrary system commands within the context of the affected application.

The issue affects Unreal 3.2.8.1 for Linux. Reportedly package Unreal3.2.8.1.tar.gz downloaded in November 2009 and later is affected. The MD5 sum of the affected file is 752e46f2d873c1679fa99de3f52a274d. Files with MD5 sum of 7b741e94e867c0a7370553fd01506c66 are not affected.

Solution:

Install latest version of unrealircd

and check signatures of software you're installing.

References:

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

<http://seclists.org/fulldisclosure/2010/Jun/277>

<http://www.securityfocus.com/bid/40820>

CVSS Base Score: 7.5

Family name: Gain a shell remotely

Category: unknown

Copyright: This script is Copyright (C) 2010 Vlatko Kosturjak

Version: \$Revision: 13960 \$

CVEs: CVE-2010-2075

High:

SSH Brute Force Logins With Default Credentials Reporting

Risk: High

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 103239

Vulnerability Detection Result:

It was possible to login with the following credentials <User>:<Password>

vagrant:vagrant

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Solution:

Change the password as soon as possible.

Vulnerability Detection Method:

Reports default credentials detected by the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013).

Summary:

It was possible to login into the remote SSH server using default credentials.

As the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

CVSS Base Score: 7.5

Family name: Default Accounts

Category: end

Copyright: Copyright (c) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-26T13:48:10+0000

High:

Test HTTP dangerous methods

Risk: High

Application: http

Port: 80

Protocol: tcp

ScriptID: 10498

Vulnerability Detection Result:

We could upload the following files via the PUT method at this web server:

http://192.168.2.200/uploads/puttest2059152704.html

We could delete the following files via the DELETE method at this web server:

http://192.168.2.200/uploads/puttest2059152704.html

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Solution:

Use access restrictions to these dangerous HTTP methods
or disable them completely.

Impact:

- Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server.
- Enabled DELETE method: This might allow an attacker to delete additional files on this web server.

Summary:

Misconfigured web servers allows remote clients to perform
dangerous HTTP methods such as PUT and DELETE.

This script checks if they are enabled and can be misused to upload or delete files.

References:

OWASP:OWASP-CM-001

CVSS Base Score: 7.5

Family name: Remote file access

Category: unknown

Copyright: This script is Copyright (C) 2000 Michel Arboi

Version: 2019-12-04T13:23:25+0000

Medium:

Drupal Information Disclosure Vulnerability

Risk: Medium

Application: http

Port: 80

Protocol: tcp

ScriptID: 902574

Vulnerability Detection Result:

Vulnerable url: <http://192.168.2.200/drupal/modules/simpletest/tests/upgrade/drupal-6.upload.database.php>

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:N/A:N

Insight:

The flaw is due to insufficient error checking, allows remote attackers to obtain sensitive information via a direct request to a .php file, which reveals the installation path in an error message.

Solution:

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS:

Drupal Version 7.0.

Summary:

The host is running Drupal and is prone to information disclosure vulnerability.

Impact:

Successful exploitation will allow attacker to obtain sensitive information that could aid in further attacks.

References:

http://code.google.com/p/inspathx/source/browse/trunk/paths_vuln/!_README

http://code.google.com/p/inspathx/source/browse/trunk/paths_vuln/drupal-7.0

CVSS Base Score: 5.0

Family name: Web application abuses

Category: attack

Copyright: Copyright (C) 2011 SecPod

Summary: NOSUMMARY

Version: 2019-05-14T12:12:41+0000

CVEs: CVE-2011-3730

Medium:

FTP Unencrypted Cleartext Login

Risk: Medium

Application: ftp

Port: 21

Protocol: tcp

ScriptID: 108528

Vulnerability Detection Result:

The remote FTP service accepts logins without a previous sent 'AUTH TLS' command. Response(s):

Anonymous sessions: 331 Anonymous login ok, send your complete email address as your password

Non-anonymous sessions: 331 Password required for openvas-vt

Impact:

An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Summary:

The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Method:

Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.

Solution:

Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

CVSS Base Vector:

AV:A/AC:L/Au:N/C:P/I:P/A:N

CVSS Base Score: 4.8

Family name: General

Category: unknown

Copyright: Copyright (C) 2019 Greenbone Networks GmbH

Version: 2020-03-24T12:27:11+0000

Medium:

SSL/TLS: Report Weak Cipher Suites

Risk: Medium

Application: ipp

Port: 631

Protocol: tcp

ScriptID: 103440

Vulnerability Detection Result:

Weak ciphers offered by this service:

TLS1_RSA_DES_192_CBC3_SHA

TLS1_RSA_DES_192_CBC3_SHA

TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA

Insight:

These rules are applied for the evaluation of the cryptographic strength:

- Any SSL/TLS using no cipher is considered weak.
- All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol.
- RC4 is considered to be weak.
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak.
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:N/A:N

Solution:

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

Summary:

This routine search for weak SSL ciphers offered by a service.

CVSS Base Score: 4.3

Family name: SSL and TLS

Category: infos

Copyright: This script is Copyright (C) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 11135 \$

CVEs: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000

Medium:

SSH Weak Encryption Algorithms Supported

Risk: Medium

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 105611

Vulnerability Detection Result:

The following weak client-to-server encryption algorithms are supported by the remote service:

3des-cbc

aes128-cbc

aes192-cbc

aes256-cbc

arcfour

arcfour128

arcfour256

blowfish-cbc

cast128-cbc

rijndael-cbc@lysator.liu.se

The following weak server-to-client encryption algorithms are supported by the remote service:

3des-cbc

aes128-cbc

aes192-cbc

aes256-cbc

arcfour

arcfour128

arcfour256

blowfish-cbc

cast128-cbc

rijndael-cbc@lysator.liu.se

Vulnerability Detection Method:

Check if remote ssh service supports Arcfour, none or CBC ciphers.

Summary:

The remote SSH server is configured to allow weak encryption algorithms.

Insight:

The `arcfour` cipher is the Arcfour stream cipher with 128-bit keys.

The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.

The `none` algorithm specifies that no encryption is to be done.

Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.

A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:N/A:N

Solution:

Disable the weak encryption algorithms.

References:

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

<https://www.kb.cert.org/vuls/id/958563>

CVSS Base Score: 4.3

Family name: General

Category: infos

Copyright: This script is Copyright (C) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-26T13:48:10+0000

Medium:

Cleartext Transmission of Sensitive Information via HTTP

Risk: Medium

Application: http

Port: 80

Protocol: tcp

ScriptID: 108440

Vulnerability Detection Result:

The following input fields were identified (URL:input name):

http://192.168.2.200/drupal/:pass

http://192.168.2.200/drupal/?D=A:pass

http://192.168.2.200/payroll_app.php:password

http://192.168.2.200/phpmyadmin/:pma_password

http://192.168.2.200/phpmyadmin/?D=A:pma_password

http://192.168.2.200/phpmyadmin/index.php:pma_password

http://192.168.2.200/phpmyadmin/license.php:pma_password

http://192.168.2.200/phpmyadmin/url.php:pma_password

Summary:

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Impact:

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Affected Software/OS:

Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method:

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.

The script is currently checking the following:

- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'

Solution:

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

CVSS Base Vector:

AV:A/AC:L/Au:N/C:P/I:P/A:N

References:

https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management

https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure

<https://cwe.mitre.org/data/definitions/319.html>

CVSS Base Score: 4.8

Family name: Web application abuses

Category: infos

Copyright: Copyright (C) 2018 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 10726 \$

Medium:

Unprotected Web App Installers (HTTP)

Risk: Medium

Application: http

Port: 80

Protocol: tcp

ScriptID: 107307

Vulnerability Detection Result:

The following Web App installers are unprotected and publicly accessible (URL:Description):

<http://192.168.2.200/phpmyadmin/setup/index.php> - CubeCart / phpMyAdmin installer

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:N/A:N

Solution:

Setup and/or installation pages for Web Apps should not be publicly accessible via a web server. Restrict access to it or remove it completely.

Vulnerability Detection Method:

Enumerate the remote web server and check if unprotected

Web Apps are accessible for installation.

Summary:

The script attempts to identify installation pages of various

Web Apps that are publicly accessible and not protected by account restrictions.

Impact:

It is possible to install or reconfigure the software. In doing so, the attacker could overwrite existing configurations. It could be possible for the attacker to gain access to the base system

CVSS Base Score: 5.0

Family name: Web application abuses

Category: infos

Copyright: Copyright (C) 2018 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-12-17T11:41:26+0000

Medium:

UnrealIRCd Authentication Spoofing Vulnerability

Risk: Medium

Application: irc

Port: 6667

Protocol: tcp

ScriptID: 809883

Vulnerability Detection Result:

Installed version: 3.2.8.1

Fixed version: 3.2.10.7

Affected Software/OS:

UnrealIRCd before 3.2.10.7 and
4.x before 4.0.6.

Vulnerability Detection Method:

Checks if a vulnerable version is present on the target host.

Impact:

Successful exploitation of this vulnerability

will allow remote attackers to spoof certificate fingerprints and consequently
log in as another user.

Summary:

This host is installed with UnrealIRCd

and is prone to authentication spoofing vulnerability.

Insight:

The flaw exists due to an error in

the 'm_authenticate' function in 'modules/m_sasl.c' script.

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

Solution:

Upgrade to UnrealIRCd 3.2.10.7,
or 4.0.6, or later.

References:

<http://seclists.org/oss-sec/2016/q3/420>

<http://www.openwall.com/lists/oss-security/2016/09/05/8>

<https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86bc50ba1a34a766>

https://bugs.unrealircd.org/main_page.php

CVSS Base Score: 6.8

Family name: General

Category: infos

Copyright: Copyright (C) 2017 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 11874 \$

CVEs: CVE-2016-7144

Low:

ICMP Timestamp Detection

Risk: Low

Application: general

Port: 0

Protocol: icmp

ScriptID: 103190

Summary:

The remote host responded to an ICMP timestamp request.

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

CVSS Base Vector:

AV:L/AC:L/Au:N/C:N/I:N/A:N

References:

<http://www.ietf.org/rfc/rfc0792.txt>

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: This script is Copyright (C) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 10411 \$

CVEs: CVE-1999-0524

Low:

SSH Weak MAC Algorithms Supported

Risk: Low

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 105610

Vulnerability Detection Result:

The following weak client-to-server MAC algorithms are supported by the remote service:

hmac-md5

hmac-md5-96

hmac-md5-96-etm@openssh.com

hmac-md5-etm@openssh.com

hmac-sha1-96

hmac-sha1-96-etm@openssh.com

The following weak server-to-client MAC algorithms are supported by the remote service:

hmac-md5

hmac-md5-96

hmac-md5-96-etm@openssh.com

hmac-md5-etm@openssh.com

hmac-sha1-96

hmac-sha1-96-etm@openssh.com

CVSS Base Vector:

AV:N/AC:H/Au:N/C:P/I:N/A:N

Solution:

Disable the weak MAC algorithms.

Summary:

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

CVSS Base Score: 2.6

Family name: General

Category: infos

Copyright: This script is Copyright (C) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-26T13:48:10+0000

Low:

TCP timestamps

Risk: Low

Application: general

Port: 0

Protocol: tcp

ScriptID: 80091

Vulnerability Detection Result:

It was detected that the host implements RFC1323.

The following timestamps were retrieved with a delay of 1 seconds in-between:

Packet 1: 1526145

Packet 2: 1526420

Affected Software/OS:

TCP/IPv4 implementations that implement RFC1323.

Vulnerability Detection Method:

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Summary:

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Impact:

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

CVSS Base Vector:

AV:N/AC:H/Au:N/C:P/I:N/A:N

Insight:

The remote host implements TCP timestamps, as defined by RFC1323.

Solution:

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

References:

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

<http://www.microsoft.com/en-us/download/details.aspx?id=9152>

CVSS Base Score: 2.6

Family name: General

Category: unknown

Copyright: Copyright (C) 2008 Michel Arboi

Version: 2020-03-21T13:23:23+0000

Info:

Apache Web Server Version Detection

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 900498

Vulnerability Detection Result:

Detected Apache HTTP/Web Server

Version: 2.4.7

Location: 80/tcp

CPE: cpe:/a:apache:http_server:2.4.7

Concluded from version/product identification result:

Server: Apache/2.4.7

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Checks whether Apache HTTP/Web Server is present
on the target system.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 SecPod

Summary: NOSUMMARY

Version: 2020-03-04T13:56:06+0000

Info:

CGI Scanning Consolidation

Risk: Info

Application: unknown

Port: 8181

Protocol: tcp

ScriptID: 111038

Vulnerability Detection Result:

The Hostname/IP "192.168.2.200" was used to access the remote host.

Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.

Requests to this service are done via HTTP/1.1.

This service seems to be able to host PHP scripts.

This service seems to be able to host ASP scripts.

The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access the remote host.

Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.

The following directories were used for CGI scanning:

http://192.168.2.200:8181/

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

Summary:

The script consolidates various information for CGI scanning.

This information is based on the following scripts / settings:

- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use

If you think any of this information is wrong please report it to the referenced community portal.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

References:

<https://community.greenbone.net/c/vulnerability-tests>

CVSS Base Score: 0.0

Family name: Web application abuses

Category: infos

Copyright: This script is Copyright (C) 2015 SCHUTZWERK GmbH

Summary: NOSUMMARY

Version: 2019-09-23T09:25:24+0000

Info:

CUPS Version Detection

Risk: Info

Application: ipp

Port: 631

Protocol: tcp

ScriptID: 900348

Vulnerability Detection Result:

Detected CUPS

Version: 1.7.2

Location: /

CPE: cpe:/a:apple:cups:1.7.2

Concluded from version/product identification result:

<TITLE>Home - CUPS 1.7.2</TITLE>

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Detects the installed version of Common Unix Printing System (CUPS)

This script sends an HTTP GET request and tries to get the version from the response.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 SecPod

Summary: NOSUMMARY

Version: 2019-12-17T11:41:26+0000

Info:

Drupal Version Detection

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 100169

Vulnerability Detection Result:

Detected Drupal

Version: 7.5

Location: /drupal

CPE: cpe:/a:drupal:drupal:7.5

Concluded from version/product identification result:

Drupal 7.5, 2011-07-27

Concluded from version/product identification location:

http://192.168.2.200/drupal/CHANGELOG.txt

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Detects the installed version of Drupal.

This script sends an HTTP GET request and tries to get the version from the response.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-12-10T12:07:42+0000

Info:

Fingerprint web server with favicon.ico

Risk: Info

Application: http-proxy

Port: 8080

Protocol: tcp

ScriptID: 20108

Vulnerability Detection Result:

The following apps/services were identified:

"jetty (5.1.14)" fingerprinted by the file: "http://192.168.2.200:8080/favicon.ico"

Impact:

The 'favicon.ico' file found on the remote web server belongs to a popular webserver/application. This may be used to fingerprint the webserver/application.

Summary:

The remote web server contains a graphic image that is prone to information disclosure.

Solution:

Remove the 'favicon.ico' file or create a custom one for your site.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Web application abuses

Category: unknown

Copyright: Copyright (C) 2005 Javier Fernandez-Sanguino

Version: 2020-02-26T12:57:19+0000

Info:

Fingerprint web server with favicon.ico

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 20108

Vulnerability Detection Result:

The following apps/services were identified:

"Drupal CMS (5.10) " fingerprinted by the file: "http://192.168.2.200/drupal/misc/favicon.ico"

"phpmyadmin (2.11.8.1 - 4.2.x)" fingerprinted by the file: "http://192.168.2.200/phpmyadmin/favicon.ico"

Impact:

The 'favicon.ico' file found on the remote web server belongs to a popular webserver/application. This may be used to fingerprint the webserver/application.

Summary:

The remote web server contains a graphic image that is prone to information disclosure.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution:

Remove the 'favicon.ico' file or create a custom one for your site.

CVSS Base Score: 0.0

Family name: Web application abuses

Category: unknown

Copyright: Copyright (C) 2005 Javier Fernandez-Sanguino

Version: 2020-02-26T12:57:19+0000

Info:

FTP Banner Detection

Risk: Info

Application: ftp

Port: 21

Protocol: tcp

ScriptID: 10092

Vulnerability Detection Result:

Remote FTP server banner:

220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.2.200]

This is probably:

- ProFTPD

Server operating system information collected via "SYST" command:

215 UNIX Type: L8

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This Plugin detects and reports a FTP Server Banner.

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2005 SecuriTeam

Version: 2020-03-24T12:27:11+0000

Info:

FTP Missing Support For AUTH TLS

Risk: Info

Application: ftp

Port: 21

Protocol: tcp

ScriptID: 108553

Vulnerability Detection Result:

The remote FTP server does not support the 'AUTH TLS' command.

Summary:

The remote FTP server does not support the 'AUTH TLS' command.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: FTP

Category: unknown

Copyright: Copyright (C) 2019 Greenbone Networks GmbH

Version: \$Revision: 13863 \$

Info:

CGI Scanning Consolidation

Risk: Info

Application: http-proxy

Port: 8080

Protocol: tcp

ScriptID: 111038

Vulnerability Detection Result:

The Hostname/IP "192.168.2.200" was used to access the remote host.

Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.

Requests to this service are done via HTTP/1.1.

This service seems to be able to host PHP scripts.

This service seems to be able to host ASP scripts.

The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access the remote host.

Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.

The following directories were used for CGI scanning:

http://192.168.2.200:8080/

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

Summary:

The script consolidates various information for CGI scanning.

This information is based on the following scripts / settings:

- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use

If you think any of this information is wrong please report it to the referenced community portal.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

References:

<https://community.greenbone.net/c/vulnerability-tests>

CVSS Base Score: 0.0

Family name: Web application abuses

Category: infos

Copyright: This script is Copyright (C) 2015 SCHUTZWERK GmbH

Summary: NOSUMMARY

Version: 2019-09-23T09:25:24+0000

Info:

HTTP Security Headers Detection

Risk: Info

Application: unknown

Port: 8181

Protocol: tcp

ScriptID: 112081

Vulnerability Detection Result:

Header Name	Header Value
-------------	--------------

X-Content-Type-Options	nosniff
------------------------	---------

X-Frame-Options	SAMEORIGIN
-----------------	------------

X-Xss-Protection	1; mode=block
------------------	---------------

Missing Headers	More Information
-----------------	------------------

Content-Security-Policy	https://owasp.org/www-project-secure-headers/#content-security-policy
-------------------------	---

Feature-Policy	https://owasp.org/www-project-secure-headers/#feature-policy
----------------	---

Referrer-Policy	https://owasp.org/www-project-secure-headers/#referrer-policy
-----------------	---

X-Permitted-Cross-Domain-Policies	
-----------------------------------	--

<https://owasp.org/www-project-secure-headers/#x-permitted-cross-domain-policies>

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

All known security headers are being checked on the host. On completion a report

will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

References:

<https://owasp.org/www-project-secure-headers/>

<https://owasp.org/www-project-secure-headers/#div-headers>

<https://securityheaders.io/>

CVSS Base Score: 0.0

Family name: General

Category: infos

Copyright: This script is Copyright (C) 2017 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-18T09:31:42+0000

Info:

HTTP Security Headers Detection

Risk: Info

Application: unknown

Port: 3500

Protocol: tcp

ScriptID: 112081

Vulnerability Detection Result:

Header Name	Header Value
-------------	--------------

X-Content-Type-Options	nosniff
------------------------	---------

X-Frame-Options	SAMEORIGIN
-----------------	------------

X-Xss-Protection	1; mode=block
------------------	---------------

Missing Headers	More Information
-----------------	------------------

Content-Security-Policy	https://owasp.org/www-project-secure-headers/#content-security-policy
-------------------------	---

Feature-Policy	https://owasp.org/www-project-secure-headers/#feature-policy
----------------	---

Referrer-Policy	https://owasp.org/www-project-secure-headers/#referrer-policy
-----------------	---

X-Permitted-Cross-Domain-Policies	
-----------------------------------	--

<https://owasp.org/www-project-secure-headers/#x-permitted-cross-domain-policies>

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

All known security headers are being checked on the host. On completion a report

will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

References:

<https://owasp.org/www-project-secure-headers/>

<https://owasp.org/www-project-secure-headers/#div-headers>

<https://securityheaders.io/>

CVSS Base Score: 0.0

Family name: General

Category: infos

Copyright: This script is Copyright (C) 2017 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-18T09:31:42+0000

Info:

HTTP Security Headers Detection

Risk: Info

Application: ipp

Port: 631

Protocol: tcp

ScriptID: 112081

Vulnerability Detection Result:

Missing Headers | [More Information](#)

Content-Security-Policy | <https://owasp.org/www-project-secure-headers/#content-security-policy>

Expect-CT | <https://owasp.org/www-project-secure-headers/#expect-ct>

Feature-Policy | <https://owasp.org/www-project-secure-headers/#feature-policy>

Public-Key-Pins | Please check the output of the VTs including 'SSL/TLS:' and 'HPKP' in their name for more information and configuration help.

Referrer-Policy | <https://owasp.org/www-project-secure-headers/#referrer-policy>

Strict-Transport-Security | Please check the output of the VTs including 'SSL/TLS:' and 'HSTS' in their name for more information and configuration help.

X-Content-Type-Options | <https://owasp.org/www-project-secure-headers/#x-content-type-options>

X-Frame-Options | <https://owasp.org/www-project-secure-headers/#x-frame-options>

X-Permitted-Cross-Domain-Policies |

<https://owasp.org/www-project-secure-headers/#x-permitted-cross-domain-policies>

X-XSS-Protection | <https://owasp.org/www-project-secure-headers/#x-xss-protection>

Summary:

All known security headers are being checked on the host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

References:

<https://owasp.org/www-project-secure-headers/>

<https://owasp.org/www-project-secure-headers/#div-headers>

<https://securityheaders.io/>

CVSS Base Score: 0.0

Family name: General

Category: infos

Copyright: This script is Copyright (C) 2017 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-18T09:31:42+0000

Info:

HTTP Security Headers Detection

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 112081

Vulnerability Detection Result:

Missing Headers | [More Information](#)

Content-Security-Policy | <https://owasp.org/www-project-secure-headers/#content-security-policy>

Feature-Policy | <https://owasp.org/www-project-secure-headers/#feature-policy>

Referrer-Policy | <https://owasp.org/www-project-secure-headers/#referrer-policy>

X-Content-Type-Options | <https://owasp.org/www-project-secure-headers/#x-content-type-options>

X-Frame-Options | <https://owasp.org/www-project-secure-headers/#x-frame-options>

X-Permitted-Cross-Domain-Policies |

<https://owasp.org/www-project-secure-headers/#x-permitted-cross-domain-policies>

X-XSS-Protection | <https://owasp.org/www-project-secure-headers/#x-xss-protection>

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

All known security headers are being checked on the host. On completion a report

will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

References:

<https://owasp.org/www-project-secure-headers/>

<https://owasp.org/www-project-secure-headers/#div-headers>

<https://securityheaders.io/>

CVSS Base Score: 0.0

Family name: General

Category: infos

Copyright: This script is Copyright (C) 2017 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-18T09:31:42+0000

Info:

HTTP Server Banner Enumeration

Risk: Info

Application: unknown

Port: 8181

Protocol: tcp

ScriptID: 108708

Vulnerability Detection Result:

It was possible to enumerate the following HTTP server banner(s):

Server banner	Enumeration technique
---------------	-----------------------

Server: WEBrick/1.3.1 (Ruby/2.3.7/2018-03-28) Valid HTTP 1.0 GET request to '/index.htm'	

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2020 Greenbone Networks GmbH

Version: 2020-02-25T12:12:27+0000

Info:

HTTP Server Banner Enumeration

Risk: Info

Application: http-proxy

Port: 8080

Protocol: tcp

ScriptID: 108708

Vulnerability Detection Result:

It was possible to enumerate the following HTTP server banner(s):

Server banner	Enumeration technique
---------------	-----------------------

Server: Jetty(8.1.7.v20120910) Valid HTTP 0.9 GET request to '/index.html'	

Summary:

This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2020 Greenbone Networks GmbH

Version: 2020-02-25T12:12:27+0000

Info:

HTTP Server Banner Enumeration

Risk: Info

Application: unknown

Port: 3500

Protocol: tcp

ScriptID: 108708

Vulnerability Detection Result:

It was possible to enumerate the following HTTP server banner(s):

Server banner	Enumeration technique
---------------	-----------------------

Server: WEBrick/1.3.1 (Ruby/2.3.7/2018-03-28) | Valid HTTP 1.0 GET request to '/index.htm'

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2020 Greenbone Networks GmbH

Version: 2020-02-25T12:12:27+0000

Info:

HTTP Server Banner Enumeration

Risk: Info

Application: ipp

Port: 631

Protocol: tcp

ScriptID: 108708

Vulnerability Detection Result:

It was possible to enumerate the following HTTP server banner(s):

Server banner	Enumeration technique
---------------	-----------------------

Server: CUPS/1.7 IPP/2.1 | Valid HTTP 0.9 GET request to '/index.html'

Summary:

This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2020 Greenbone Networks GmbH

Version: 2020-02-25T12:12:27+0000

Info:

HTTP Server Banner Enumeration

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 108708

Vulnerability Detection Result:

It was possible to enumerate the following HTTP server banner(s):

Server banner | Enumeration technique

Server: Apache/2.4.7 (Ubuntu) | Valid HTTP 0.9 GET request to '/index.html'

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2020 Greenbone Networks GmbH

Version: 2020-02-25T12:12:27+0000

Info:

HTTP Server type and version

Risk: Info

Application: unknown

Port: 8181

Protocol: tcp

ScriptID: 10107

Vulnerability Detection Result:

The remote HTTP Server banner is:

Server: WEBrick/1.3.1 (Ruby/2.3.7/2018-03-28)

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script detects and reports the HTTP Server's banner which might provide the type and version of it.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2005 H. Scholz & Contributors

Version: 2020-02-06T14:44:42+0000

Info:

CGI Scanning Consolidation

Risk: Info

Application: unknown

Port: 3500

Protocol: tcp

ScriptID: 111038

Vulnerability Detection Result:

The Hostname/IP "192.168.2.200" was used to access the remote host.

Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.

Requests to this service are done via HTTP/1.1.

This service seems to be able to host PHP scripts.

This service seems to be able to host ASP scripts.

The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access the remote host.

Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.

The following directories were used for CGI scanning:

<http://192.168.2.200:3500/>

<http://192.168.2.200:3500/rails/info>

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

Summary:

The script consolidates various information for CGI scanning.

This information is based on the following scripts / settings:

- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use

If you think any of this information is wrong please report it to the referenced community portal.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

References:

<https://community.greenbone.net/c/vulnerability-tests>

CVSS Base Score: 0.0

Family name: Web application abuses

Category: infos

Copyright: This script is Copyright (C) 2015 SCHUTZWERK GmbH

Summary: NOSUMMARY

Version: 2019-09-23T09:25:24+0000

Info:

HTTP Server type and version

Risk: Info

Application: http-proxy

Port: 8080

Protocol: tcp

ScriptID: 10107

Vulnerability Detection Result:

The remote HTTP Server banner is:

Server: Jetty(8.1.7.v20120910)

Summary:

This script detects and reports the HTTP Server's banner
which might provide the type and version of it.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2005 H. Scholz & Contributors

Version: 2020-02-06T14:44:42+0000

Info:

HTTP Server type and version

Risk: Info

Application: unknown

Port: 3500

Protocol: tcp

ScriptID: 10107

Vulnerability Detection Result:

The remote HTTP Server banner is:

Server: WEBrick/1.3.1 (Ruby/2.3.7/2018-03-28)

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script detects and reports the HTTP Server's banner
which might provide the type and version of it.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2005 H. Scholz & Contributors

Version: 2020-02-06T14:44:42+0000

Info:

HTTP Server type and version

Risk: Info

Application: ipp

Port: 631

Protocol: tcp

ScriptID: 10107

Vulnerability Detection Result:

The remote HTTP Server banner is:

Server: CUPS/1.7 IPP/2.1

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script detects and reports the HTTP Server's banner
which might provide the type and version of it.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2005 H. Scholz & Contributors

Version: 2020-02-06T14:44:42+0000

Info:

HTTP Server type and version

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 10107

Vulnerability Detection Result:

The remote HTTP Server banner is:

Server: Apache/2.4.7 (Ubuntu)

Summary:

This script detects and reports the HTTP Server's banner
which might provide the type and version of it.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2005 H. Scholz & Contributors

Version: 2020-02-06T14:44:42+0000

Info:

IRC Server Banner Detection

Risk: Info

Application: irc

Port: 6667

Protocol: tcp

ScriptID: 11156

Vulnerability Detection Result:

The IRC server banner is:

:irc.TestIRC.net 002 IDFHDDABH :Your host is irc.TestIRC.net, running version Unreal3.2.8.1

Summary:

This script tries to detect the banner of an IRC server.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: This script is Copyright (C) 2002 Michel Arboi

Version: \$Revision: 13541 \$

Info:

Jetty Version Detection

Risk: Info

Application: http-proxy

Port: 8080

Protocol: tcp

ScriptID: 800953

Vulnerability Detection Result:

Detected Jetty Web Server

Version: 8.1.7.20120910

Location: 8080/tcp

CPE: cpe:/a:eclipse:jetty:8.1.7.20120910

Concluded from version/product identification result:

Server: Jetty(8.1.7.v20120910)

Summary:

Detection of Jetty Web Server.

The script sends a connection request to the server and attempts to extract the version number from the reply.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

References:

<https://www.eclipse.org/jetty/>

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-11-20T13:37:34+0000

Info:

Microsoft Windows SMB Accessible Shares

Risk: Info

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 902425

Vulnerability Detection Result:

The following shares were found

IPC\$

Summary:

The script detects the Windows SMB Accessible Shares and sets the result into KB.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Windows

Category: infos

Copyright: Copyright (c) 2012 SecPod

Summary: NOSUMMARY

Version: \$Revision: 11420 \$

Info:

MySQL/MariaDB Detection

Risk: Info

Application: mysql

Port: 3306

Protocol: tcp

ScriptID: 100152

Vulnerability Detection Result:

Detected MySQL

Version: unknown

Location: 3306/tcp

CPE: cpe:/a:oracle:mysql

Extra information:

Scanner received a ER_HOST_NOT_PRIVILEGED error from the remote MySQL server.

Some tests may fail. Allow the scanner to access the remote MySQL server for better results.

Summary:

Detects the installed version of

MySQL/MariaDB.

Detect a running MySQL/MariaDB by getting the banner, extract the version from the banner.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: This script is Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-11-05T16:13:01+0000

Info:

Obtain list of all port mapper registered programs via RPC

Risk: Info

Application: rpcbind

Port: 111

Protocol: tcp

ScriptID: 11111

Vulnerability Detection Result:

These are the registered RPC programs:

RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) on port 111/TCP

RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) on port 111/TCP

RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/TCP

RPC program #100024 version 1 'status' on port 33816/TCP

RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) on port 111/UDP

RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) on port 111/UDP

RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/UDP

RPC program #100024 version 1 'status' on port 44502/UDP

Summary:

This script calls the DUMP RPC on the port mapper, to obtain the
list of all registered programs.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: RPC

Category: unknown

Copyright: This script is Copyright (C) 2002 Michel Arboi

Version: \$Revision: 13541 \$

Info:

CGI Scanning Consolidation

Risk: Info

Application: ipp

Port: 631

Protocol: tcp

ScriptID: 111038

Vulnerability Detection Result:

The Hostname/IP "192.168.2.200" was used to access the remote host.

Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.

Requests to this service are done via HTTP/1.1.

This service seems to be able to host PHP scripts.

This service seems to be able to host ASP scripts.

The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access the remote host.

Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.

A possible recursion was detected during CGI scanning:

The service is using a relative URL in one or more HTML references where e.g. /file1.html contains and a subsequent request for subdir/file2.html is linking to subdir/file2.html. This would resolve to subdir/subdir/file2.html causing a recursion. To work around this counter-measures have been enabled but the service should be fixed as well to not use such problematic links. Below an excerpt of URLs is shown to help identify those issues.

Syntax : URL (HTML link)

[https://192.168.2.200:631/fr \(help/accounting.html\)](https://192.168.2.200:631/fr (help/accounting.html))

[https://192.168.2.200:631/fr \(help/api-cups.html\)](https://192.168.2.200:631/fr (help/api-cups.html))

[https://192.168.2.200:631/fr \(help/api-filter.html\)](https://192.168.2.200:631/fr (help/api-filter.html))

[https://192.168.2.200:631/fr \(help/api-httpipp.html\)](https://192.168.2.200:631/fr (help/api-httpipp.html))

[https://192.168.2.200:631/fr \(help/api-overview.html\)](https://192.168.2.200:631/fr (help/api-overview.html))

The following directories were used for CGI scanning:

<https://192.168.2.200:631/>

<https://192.168.2.200:631/admin>

<https://192.168.2.200:631/admin-bak>

<https://192.168.2.200:631/admin-console>

<https://192.168.2.200:631/admin-old>

<https://192.168.2.200:631/admin.back>

<https://192.168.2.200:631/admin/log>

https://192.168.2.200:631/admin_

<https://192.168.2.200:631/adminer>

<https://192.168.2.200:631/administration>

<https://192.168.2.200:631/administrator>

<https://192.168.2.200:631/adminuser>

<https://192.168.2.200:631/adminweb>

<https://192.168.2.200:631/classes>

<https://192.168.2.200:631/es>

<https://192.168.2.200:631/fr>

<https://192.168.2.200:631/help>

<https://192.168.2.200:631/helpdesk>

<https://192.168.2.200:631/printers>

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

The following directories were excluded from CGI scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the NVT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\.php|image|img|css|js\$|js|/javascript|style|theme|icon|jquery|graphic|grafik|picture|bilder|thumbnail|media|/skins?/)"

<https://192.168.2.200:631/images>

NOTE: The 'Maximum number of items shown for each list' setting has been reached. There are 1 additional entries available for the following truncated list.

The following CGIs were discovered:

Syntax : cginame (arguments [default value])

<https://192.168.2.200:631/admin> (USER_CANCEL_ANY [] SHARE_PRINTERS [] DEBUG_LOGGING [] REMOTE_ANY [] org.cups.sid [e775ba658e5e841b40664df56d5d250d] CHANGESSETTINGS [Change Settings] KERBEROS [] OP [config-server] REMOTE_ADMIN [])

<https://192.168.2.200:631/admin/> (org.cups.sid [e775ba658e5e841b40664df56d5d250d] ADVANCEDSETTINGS [YES] OP [add-printer])

https://192.168.2.200:631/admin/log/access_log ()

https://192.168.2.200:631/admin/log/error_log ()

https://192.168.2.200:631/admin/log/page_log ()

<https://192.168.2.200:631/classes/> (CLEAR [Clear] QUERY [])

<https://192.168.2.200:631/help/> (SEARCH [Search] CLEAR [Clear] TOPIC [Getting+Started] QUERY [])

<https://192.168.2.200:631/help/accounting.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Getting+Started])

<https://192.168.2.200:631/help/api-array.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Programming] QUERY [])

<https://192.168.2.200:631/help/api-cgi.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Programming] QUERY [])

<https://192.168.2.200:631/help/api-cups.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Programming] QUERY [])

<https://192.168.2.200:631/help/api-driver.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Programming] QUERY [])

<https://192.168.2.200:631/help/api-filedir.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Programming] QUERY [])

<https://192.168.2.200:631/help/api-filter.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Programming] QUERY [])

<https://192.168.2.200:631/help/api-htppipp.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Programming] QUERY [])

<https://192.168.2.200:631/help/api-mime.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Programming] QUERY [])

<https://192.168.2.200:631/help/api-overview.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Programming] QUERY [])

<https://192.168.2.200:631/help/api-ppd.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Programming] QUERY [])

<https://192.168.2.200:631/help/api-ppdc.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Programming] QUERY [])

<https://192.168.2.200:631/help/api-raster.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Programming] QUERY [])

<https://192.168.2.200:631/help/cgi.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Getting+Started])

<https://192.168.2.200:631/help/glossary.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Getting+Started])

<https://192.168.2.200:631/help/kerberos.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Getting+Started] QUERY [])

<https://192.168.2.200:631/help/license.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Getting+Started])

<https://192.168.2.200:631/help/man-backend.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])

<https://192.168.2.200:631/help/man-cancel.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])

<https://192.168.2.200:631/help/man-classes.conf.html> (TOPIC [Man+Pages])

<https://192.168.2.200:631/help/man-cups-config.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])

<https://192.168.2.200:631/help/man-cups-deviced.html> (TOPIC [Man+Pages])

<https://192.168.2.200:631/help/man-cups-driverd.html> (TOPIC [Man+Pages])

<https://192.168.2.200:631/help/man-cups-lpd.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Man+Pages])

<https://192.168.2.200:631/help/man-cups-snmp.conf.html> (TOPIC [Man+Pages])

<https://192.168.2.200:631/help/man-cups-snmp.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Man+Pages])

<https://192.168.2.200:631/help/man-cupsaccept.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])

<https://192.168.2.200:631/help/man-cupsaddsmb.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])

<https://192.168.2.200:631/help/man-cupsd.conf.html> (TOPIC [Man+Pages])

<https://192.168.2.200:631/help/man-cupsd.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Man+Pages])

<https://192.168.2.200:631/help/man-cupsenable.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])

<https://192.168.2.200:631/help/man-cupsfilter.html> (TOPIC [Man+Pages])

<https://192.168.2.200:631/help/man-cupstestdsc.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])

<https://192.168.2.200:631/help/man-cupstestppd.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])

<https://192.168.2.200:631/help/man-filter.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Man+Pages])

<https://192.168.2.200:631/help/man-ipptool.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])

<https://192.168.2.200:631/help/man-ipptoolfile.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])

<https://192.168.2.200:631/help/man-lp.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])

<https://192.168.2.200:631/help/man-lpadmin.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Man+Pages])

<https://192.168.2.200:631/help/man-lpc.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])

<https://192.168.2.200:631/help/man-lpinfo.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Man+Pages])

<https://192.168.2.200:631/help/man-lpmove.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])

<https://192.168.2.200:631/help/man-lpoptions.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])

<https://192.168.2.200:631/help/man-lppasswd.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])

<https://192.168.2.200:631/help/man-lpq.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])

<https://192.168.2.200:631/help/man-lpr.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])

<https://192.168.2.200:631/help/man-lprm.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [])

TOPIC [Man+Pages])
https://192.168.2.200:631/help/man-lpstat.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])
https://192.168.2.200:631/help/man-mime.convs.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])
https://192.168.2.200:631/help/man-mime.types.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])
https://192.168.2.200:631/help/man-notifier.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])
https://192.168.2.200:631/help/man-ppdc.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])
https://192.168.2.200:631/help/man-ppdhtml.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])
https://192.168.2.200:631/help/man-ppdi.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])
https://192.168.2.200:631/help/man-ppdmerge.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])
https://192.168.2.200:631/help/man-ppdpo.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])
https://192.168.2.200:631/help/man-printers.conf.html (TOPIC [Man+Pages])
https://192.168.2.200:631/help/network.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Getting+Started])
https://192.168.2.200:631/help/options.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Getting+Started])
https://192.168.2.200:631/help/overview.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Getting Started])
https://192.168.2.200:631/help/perqueue.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Getting+Started])
https://192.168.2.200:631/help/policies.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Getting+Started])
https://192.168.2.200:631/help/postscript-driver.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Programming] QUERY [])
https://192.168.2.200:631/help/ppd-compiler.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Programming] QUERY [])
https://192.168.2.200:631/help/raster-driver.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] TOPIC [Programming] QUERY [])
https://192.168.2.200:631/help/ref-access_log.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [References])
https://192.168.2.200:631/help/ref-classes-conf.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [References])
https://192.168.2.200:631/help/ref-client-conf.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [References])
https://192.168.2.200:631/help/ref-cups-files-conf.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [References])
https://192.168.2.200:631/help/ref-cupsd-conf.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [References])
https://192.168.2.200:631/help/ref-error_log.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [References])
https://192.168.2.200:631/help/ref-mailto-conf.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [References])
https://192.168.2.200:631/help/ref-page_log.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [References])
https://192.168.2.200:631/help/ref-ppdcfile.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY []

TOPIC [References])
<https://192.168.2.200:631/help/ref-printers-conf.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [References])
<https://192.168.2.200:631/help/ref-snmp-conf.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [References])
<https://192.168.2.200:631/help/ref-subscriptions-conf.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [References])
<https://192.168.2.200:631/help/security.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Getting+Started])
<https://192.168.2.200:631/help/sharing.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Getting+Started])
<https://192.168.2.200:631/help/spec-banner.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Specifications])
<https://192.168.2.200:631/help/spec-cmp.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Specifications])
<https://192.168.2.200:631/help/spec-command.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Specifications])
<https://192.168.2.200:631/help/spec-design.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Specifications])
<https://192.168.2.200:631/help/spec-ipp.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Specifications])
<https://192.168.2.200:631/help/spec-pdf.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Specifications])
<https://192.168.2.200:631/help/spec-postscript.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Specifications])
<https://192.168.2.200:631/help/spec-ppd.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Specifications])
<https://192.168.2.200:631/help/spec-raster.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Specifications])
<https://192.168.2.200:631/help/spec-stp.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Specifications])
<https://192.168.2.200:631/help/translation.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Getting+Started])
<https://192.168.2.200:631/help/whatsnew.html> (SEARCH [Search] CLEAR [Clear] PRINTABLE [YES] QUERY [] TOPIC [Getting+Started])
<https://192.168.2.200:631/jobs> (which_jobs [completed])
Summary:
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
<https://community.greenbone.net/c/vulnerability-tests>
CVSS Base Score: 0.0

Family name: Web application abuses

Category: infos

Copyright: This script is Copyright (C) 2015 SCHUTZWERK GmbH

Summary: NOSUMMARY

Version: 2019-09-23T09:25:24+0000

Info:

OpenSSH Detection Consolidation

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 108577

Vulnerability Detection Result:

Detected OpenSSH Server

Version: 6.6.1p1

Location: 22/tcp

CPE: cpe:/a:openbsd:openssh:6.6.1p1

Concluded from version/product identification result:

SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.10

Summary:

The script reports a detected OpenSSH including the version number.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

References:

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

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2019 Greenbone Networks GmbH

Version: 2019-05-23T06:42:35+0000

Info:

OS Detection Consolidation and Reporting

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 105937

Vulnerability Detection Result:

Best matching OS:

OS: Ubuntu

Version: 14.04

CPE: cpe:/o:canonical:ubuntu_linux:14.04

Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (SSH OS Identification)

Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.10

Setting key "Host/runs_unixoid" based on this information

Other OS detections (in order of reliability):

OS: Ubuntu 14.04 or 16.04

CPE: cpe:/o:canonical:ubuntu_linux:16.04

Found by NVT: 1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan)

Concluded from SMB/Samba banner on port 445/tcp:

OS String: Windows 6.1

SMB String: Samba 4.3.11-Ubuntu

Note: The service is running on a Linux/Unix based OS but reporting itself with an Windows related OS string.

OS: Ubuntu

CPE: cpe:/o:canonical:ubuntu_linux

Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)

Concluded from HTTP Server banner on port 80/tcp: Server: Apache/2.4.7 (Ubuntu)

OS: Linux/Unix

CPE: cpe:/o:linux:kernel

Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)

Concluded from HTTP Server banner on port 631/tcp: Server: CUPS/1.7 IPP/2.1

OS: Linux/Unix

CPE: cpe:/o:linux:kernel

Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)

Concluded from HTTP Server default page on port 631/tcp: <TITLE>Home - CUPS 1.7.2</TITLE>

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.

Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information

which might help to improve the OS detection.

If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

References:

<https://community.greenbone.net/c/vulnerability-tests>

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: This script is Copyright (C) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-30T08:21:10+0000

Info:

PHP Version Detection (Remote)

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 800109

Vulnerability Detection Result:

Detected PHP

Version: 5.4.5

Location: 80/tcp

CPE: cpe:/a:php:php:5.4.5

Concluded from version/product identification result:

X-Powered-By: PHP/5.4.5

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Detects the installed version of PHP.

This script sends an HTTP GET request and tries to get the version from the response.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2008 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-12-17T14:07:10+0000

Info:

phpMyAdmin Detection

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 900129

Vulnerability Detection Result:

Detected phpMyAdmin

Version: 3.5.8

Location: /phpmyadmin

CPE: cpe:/a:phpmyadmin:phpmyadmin:3.5.8

Concluded from version/product identification result:

Version 3.5.8

Concluded from version/product identification location:

<http://192.168.2.200/phpmyadmin/README>

Extra information:

- Possible unprotected setup dir identified at <http://192.168.2.200/phpmyadmin/setup/>

Summary:

Detection of phpMyAdmin.

The script sends a connection request to the server and attempts to extract the version number from the reply.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2008 SecPod

Summary: NOSUMMARY

Version: 2019-12-04T13:23:25+0000

Info:

Ping Host

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 100315

Vulnerability Detection Result:

The alive test was not launched because no method was selected.

Summary:

This check tries to determine whether a remote host is up (alive).

Several methods are used for this depending on configuration of this check. Whether a host is up can be detected in 3 different ways:

- A ICMP message is sent to the host and a response is taken as alive sign.
- An ARP request is sent and a response is taken as alive sign.
- A number of typical TCP services (namely the 20 top ports of nmap) are tried and their presence is taken as alive sign.

None of the methods is failsafe. It depends on network and/or host configurations whether they succeed or not. Both, false positives and false negatives can occur.

Therefore the methods are configurable.

If you select to not mark unreachable hosts as dead, no alive detections are executed and the host is assumed to be available for scanning.

In case it is configured that hosts are never marked as dead, this can cause considerable timeouts and therefore a long scan duration in case the hosts are in fact not available.

The available methods might fail for the following reasons:

- ICMP: This might be disabled for a environment and would then cause false negatives as hosts are believed to be dead that actually are alive. In contrast it is also possible that a Firewall between the scanner and the target host is answering to the ICMP message and thus hosts are believed to be alive that actually are dead.
- TCP ping: Similar to the ICMP case a Firewall between the scanner and the target might answer to the sent probes and thus hosts are believed to be alive that actually are dead.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Port scanners

Category: scanner

Copyright: This script is Copyright (C) 2009, 2014, 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-26T16:09:27+0000

Info:

ProFTPD Server Version Detection (Remote)

Risk: Info

Application: ftp

Port: 21

Protocol: tcp

ScriptID: 900815

Vulnerability Detection Result:

Detected ProFTPD

Version: 1.3.5

Location: 21/tcp

CPE: cpe:/a:proftpd:proftpd:1.3.5

Concluded from version/product identification result:

220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.2.200]

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script detects the installed version of ProFTP Server.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 SecPod

Summary: NOSUMMARY

Version: 2020-03-24T12:27:11+0000

Info:

robot(s).txt exists on the Web Server

Risk: Info

Application: unknown

Port: 3500

Protocol: tcp

ScriptID: 10302

Vulnerability Detection Result:

The file 'robots.txt' contains the following:

See <http://www.robotstxt.org/robotstxt.html> for documentation on how to use the robots.txt file

#

To ban all spiders from the entire site uncomment the next two lines:

User-agent: *

Disallow: /

Summary:

Web Servers can use a file called /robot(s).txt to ask search engines

to ignore certain files and directories. By nature this file can not be used to protect private files from public read access.

Solution:

Review the content of the robots file and consider removing the files

from the server or protect them in other ways in case you actually intended non-public availability.

Insight:

Any serious web search engine will honor the /robot(s).txt file

and not scan the files and directories listed there.

Any entries listed in this file are not even hidden anymore.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Web application abuses

Category: unknown

Copyright: This script is Copyright (C) 1999 SecuriTeam

Version: 2019-11-22T13:51:04+0000

Info:

robot(s).txt exists on the Web Server

Risk: Info

Application: ipp

Port: 631

Protocol: tcp

ScriptID: 10302

Vulnerability Detection Result:

The file 'robots.txt' contains the following:

```
#
# "$Id: robots.txt 3494 2003-03-19 15:37:44Z mike $"
#
# This file tells search engines not to index your CUPS server.
#
# Copyright 1993-2003 by Easy Software Products.
#
# These coded instructions, statements, and computer programs are the
# property of Easy Software Products and are protected by Federal
# copyright law. Distribution and use rights are outlined in the file
# "LICENSE.txt" which should have been included with this file. If this
# file is missing or damaged please contact Easy Software Products
# at:
#
#   Attn: CUPS Licensing Information
#   Easy Software Products
#   44141 Airport View Drive, Suite 204
#   Hollywood, Maryland 20636-3111 USA
#
#   Voice: (301) 373-9600
#   EMail: cups-info@cups.org
#   WWW: http://www.cups.org
#
User-agent: *
Disallow: /
#
# End of "$Id: robots.txt 3494 2003-03-19 15:37:44Z mike $".
#
```

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Insight:

Any serious web search engine will honor the /robot(s).txt file
and not scan the files and directories listed there.

Any entries listed in this file are not even hidden anymore.

Solution:

Review the content of the robots file and consider removing the files
from the server or protect them in other ways in case you actually intended non-public availability.

Summary:

Web Servers can use a file called /robot(s).txt to ask search engines
to ignore certain files and directories. By nature this file can not be used to protect private files
from public read access.

CVSS Base Score: 0.0

Family name: Web application abuses

Category: unknown

Copyright: This script is Copyright (C) 1999 SecuriTeam

Version: 2019-11-22T13:51:04+0000

Info:

RPC portmapper (TCP)

Risk: Info

Application: rpcbind

Port: 111

Protocol: tcp

ScriptID: 108090

Vulnerability Detection Result:

RPC portmapper is running on this port.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script performs detection of RPC portmapper on TCP.

CVSS Base Score: 0.0

Family name: RPC

Category: infos

Copyright: Copyright (C) 2009 SecPod

Summary: NOSUMMARY

Version: 2020-03-26T06:41:35+0000

Info:

CGI Scanning Consolidation

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 111038

Vulnerability Detection Result:

The Hostname/IP "192.168.2.200" was used to access the remote host.

Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.

Requests to this service are done via HTTP/1.1.

This service seems to be able to host PHP scripts.

This service seems to be NOT able to host ASP scripts.

The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access the remote host.

Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.

A possible recursion was detected during CGI scanning:

The service is using a relative URL in one or more HTML references where e.g. /file1.html contains and a subsequent request for subdir/file2.html is linking to subdir/file2.html. This would resolve to subdir/subdir/file2.html causing a recursion. To work around this counter-measures have been enabled but the service should be fixed as well to not use such problematic links. Below an excerpt of URLs is shown to help identify those issues.

Syntax : URL (HTML link)

<http://192.168.2.200/drupal/sites/all/modules/coder/?D=A> (images/)

<http://192.168.2.200/drupal/sites/default/files/styles/medium/public/field/> (image/)

<http://192.168.2.200/drupal/sites/default/files/styles/thumbnail/> (public/)

<http://192.168.2.200/phpmyadmin/index.php> (themes/dot.gif)

<http://192.168.2.200/phpmyadmin/license.php> (themes/dot.gif)

The following directories were used for CGI scanning:

<http://192.168.2.200/>

<http://192.168.2.200/cgi-bin>

<http://192.168.2.200/chat>

<http://192.168.2.200/drupal>

<http://192.168.2.200/drupal/misc>

<http://192.168.2.200/drupal/misc/farbtastic>

<http://192.168.2.200/drupal/misc/ui>

<http://192.168.2.200/drupal/sites>

<http://192.168.2.200/drupal/sites/all>

<http://192.168.2.200/drupal/sites/all/modules>

<http://192.168.2.200/drupal/sites/all/modules/coder>

http://192.168.2.200/drupal/sites/all/modules/coder/coder_review

http://192.168.2.200/drupal/sites/all/modules/coder/coder_sniffer

http://192.168.2.200/drupal/sites/all/modules/coder/coder_upgrade

<http://192.168.2.200/drupal/sites/all/modules/coder/scripts>

<http://192.168.2.200/drupal/sites/default>

<http://192.168.2.200/drupal/sites/default/files>

<http://192.168.2.200/drupal/sites/default/files/field>

<http://192.168.2.200/phpmyadmin>

<http://192.168.2.200/phpmyadmin/setup>

<http://192.168.2.200/uploads>

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

The following directories were excluded from CGI scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the NVT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: `"/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|picture|bilder|thumbnail|media/|skins?/)"`

`http://192.168.2.200/drupal/misc/ui/images`
`http://192.168.2.200/drupal/sites/all/themes`
`http://192.168.2.200/drupal/sites/default/files/field/image`
`http://192.168.2.200/drupal/sites/default/files/styles`
`http://192.168.2.200/drupal/sites/default/files/styles/large`
`http://192.168.2.200/drupal/sites/default/files/styles/large/public`
`http://192.168.2.200/drupal/sites/default/files/styles/medium`
`http://192.168.2.200/drupal/sites/default/files/styles/medium/public`
`http://192.168.2.200/drupal/sites/default/files/styles/medium/public/field`
`http://192.168.2.200/drupal/sites/default/files/styles/thumbnail`
`http://192.168.2.200/icons`
`http://192.168.2.200/phpmyadmin/js`
`http://192.168.2.200/phpmyadmin/js/jquery`
`http://192.168.2.200/phpmyadmin/themes`
`http://192.168.2.200/phpmyadmin/themes/original/img`
`http://192.168.2.200/phpmyadmin/themes/original/img/pmd`
`http://192.168.2.200/phpmyadmin/themes/pmahomme/img`
`http://192.168.2.200/phpmyadmin/themes/pmahomme/jquery`

Directory index found at:

`http://192.168.2.200/`
`http://192.168.2.200/drupal/misc/`
`http://192.168.2.200/drupal/misc/ui/`
`http://192.168.2.200/drupal/sites/`
`http://192.168.2.200/drupal/sites/all/`
`http://192.168.2.200/drupal/sites/all/themes/`
`http://192.168.2.200/drupal/sites/default/files/`
`http://192.168.2.200/drupal/sites/default/files/field/`
`http://192.168.2.200/drupal/sites/default/files/field/image/`
`http://192.168.2.200/drupal/sites/default/files/styles/`
`http://192.168.2.200/drupal/sites/default/files/styles/large/`
`http://192.168.2.200/drupal/sites/default/files/styles/medium/`
`http://192.168.2.200/drupal/sites/default/files/styles/medium/public/`
`http://192.168.2.200/drupal/sites/default/files/styles/medium/public/field/`
`http://192.168.2.200/drupal/sites/default/files/styles/thumbnail/`
`http://192.168.2.200/uploads/`

The "Number of pages to mirror" setting (Current: 200) of the NVT "Web mirroring" (OID: 1.3.6.1.4.1.25623.1.0.10662) was reached. Raising this limit allows to mirror this host more thoroughly but might increase the scanning time.

The following CGIs were discovered:

Syntax : `cginame (arguments [default value])`

`http://192.168.2.200/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])`

`http://192.168.2.200/chat/index.php (name [] enter [Enter])`

`http://192.168.2.200/drupal/ (destination [node] form_build_id`

`[form-DJ-isCjU-PELM9E1ZfuHVxK3oWWA8sQW7TWDaa3vifw] pass [] name [] q [rss.xml] op [Log in] form_id [user_login_block])`

`http://192.168.2.200/drupal/misc/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])`

`http://192.168.2.200/drupal/misc/farbtastic/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])`

http://192.168.2.200/drupal/misc/ui/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://192.168.2.200/drupal/sites/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://192.168.2.200/drupal/sites/all/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://192.168.2.200/drupal/sites/all/modules/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://192.168.2.200/drupal/sites/all/modules/coder/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://192.168.2.200/drupal/sites/all/themes/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://192.168.2.200/drupal/sites/default/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://192.168.2.200/drupal/sites/default/files/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://192.168.2.200/drupal/sites/default/files/field/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://192.168.2.200/drupal/sites/default/files/field/image/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://192.168.2.200/drupal/sites/default/files/styles/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://192.168.2.200/drupal/sites/default/files/styles/large/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://192.168.2.200/drupal/sites/default/files/styles/medium/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://192.168.2.200/drupal/sites/default/files/styles/medium/public/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://192.168.2.200/drupal/sites/default/files/styles/medium/public/field/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
)
http://192.168.2.200/drupal/sites/default/files/styles/thumbnail/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://192.168.2.200/payroll_app.php (user [] password [] s [OK])
http://192.168.2.200/phpmyadmin/index.php (token [4a33b4cac6a3adaa153765d5c8fb3f8e] pma_username [] table []
collation_connection [utf8_general_ci] lang [] server [1] db [] pma_password [])
http://192.168.2.200/phpmyadmin/js/get_image.js.php (theme [pmahomme])
http://192.168.2.200/phpmyadmin/js/messages.php (token [4a33b4cac6a3adaa153765d5c8fb3f8e]
collation_connection [utf8_general_ci] lang [en] db [])
http://192.168.2.200/phpmyadmin/phpmyadmin.css.php (token [4a33b4cac6a3adaa153765d5c8fb3f8e]
collation_connection [utf8_general_ci] lang [en] js_frame [right] server [1] nocache [4263716059])
http://192.168.2.200/phpmyadmin/setup/ (D [A] token [e0f64248bcb6e82ae610a53a87079ce8] version_check [1]
formset [Features] collation_connection [utf8_general_ci] lang [] page [form])
http://192.168.2.200/phpmyadmin/setup/config.php (token [e0f64248bcb6e82ae610a53a87079ce8] tab_hash []
submit_clear [Clear] ServerDefault [] submit_download [Download] submit_delete [Delete] submit_load [Load]
collation_connection [utf8_general_ci] submit_save [Save] lang [en] submit_display [Display] eol [] DefaultLang [])
http://192.168.2.200/phpmyadmin/setup/index.php (token [e0f64248bcb6e82ae610a53a87079ce8] submit [New
server] tab_hash [] collation_connection [utf8_general_ci] mode [add] lang [en] page [servers] check_page_refresh [])
http://192.168.2.200/phpmyadmin/url.php (token [4a33b4cac6a3adaa153765d5c8fb3f8e] url
[http%3A%2F%2Fwww.phpmyadmin.net%2F] collation_connection [utf8_general_ci] lang [en])
http://192.168.2.200/uploads/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
The following cgi scripts were excluded from CGI scanning because of the "Regex pattern to exclude cgi scripts"
setting of the NVT "Web mirroring" (OID: 1.3.6.1.4.1.25623.1.0.10662) for this scan was: "\.(js|css)\$"

Syntax : cginame (arguments [default value])

http://192.168.2.200/drupal/misc/drupal.js (or3865 [])

http://192.168.2.200/drupal/misc/jquery.js (v [1.4.4])

http://192.168.2.200/drupal/misc/jquery.once.js (v [1.2])

http://192.168.2.200/phpmyadmin/js/cross_framing_protection.js (ts [1365422810])

http://192.168.2.200/phpmyadmin/js/functions.js (ts [1365422810])

http://192.168.2.200/phpmyadmin/js/jquery/jquery-1.6.2.js (ts [1365422810])

http://192.168.2.200/phpmyadmin/js/jquery/jquery-ui-1.8.16.custom.js (ts [1365422810])

http://192.168.2.200/phpmyadmin/js/jquery/jquery.qtip-1.0.0-rc3.js (ts [1365422810])

http://192.168.2.200/phpmyadmin/js/update-location.js (ts [1365422810])

Summary:

The script consolidates various information for CGI scanning.

This information is based on the following scripts / settings:

- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)

- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use

If you think any of this information is wrong please report it to the referenced community portal.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

References:

<https://community.greenbone.net/c/vulnerability-tests>

CVSS Base Score: 0.0

Family name: Web application abuses

Category: infos

Copyright: This script is Copyright (C) 2015 SCHUTZWERK GmbH

Summary: NOSUMMARY

Version: 2019-09-23T09:25:24+0000

Info:

Ruby on Rails Version Detection

Risk: Info

Application: unknown

Port: 3500

Protocol: tcp

ScriptID: 902089

Vulnerability Detection Result:

Detected Ruby on Rails

Version: 4.2.4

Location: /

CPE: cpe:/a:rubyonrails:ruby_on_rails:4.2.4

Concluded from version/product identification result:
>4.2.4

Extra information:

Version information available at /rails/info/properties/

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script finds the running Ruby on Rails version.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (c) 2010 SecPod

Summary: NOSUMMARY

Version: 2019-11-21T13:29:18+0000

Info:

Ruby on Rails Version Detection

Risk: Info

Application: unknown

Port: 3500

Protocol: tcp

ScriptID: 902089

Vulnerability Detection Result:

Detected Ruby

Version: 2.3.7-p456

Location: /

CPE: cpe:/a:ruby-lang:ruby:2.3.7

Concluded from version/product identification result:

>2.3.7-p456

Extra information:

Version information available at /rails/info/properties/

Summary:

This script finds the running Ruby on Rails version.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (c) 2010 SecPod

Summary: NOSUMMARY

Version: 2019-11-21T13:29:18+0000

Info:

Service Detection with 'GET' Request

Risk: Info

Application: irc

Port: 6667

Protocol: tcp

ScriptID: 17975

Vulnerability Detection Result:

An IRC server seems to be running on this port.

Summary:

This plugin performs service detection.

This plugin is a complement of find_service.nasl. It sends a 'GET' request to the remaining unknown services and tries to identify them.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2005 Michel Arboi

Version: 2020-03-25T13:50:09+0000

Info:

Services

Risk: Info

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

An ssh server is running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>

Version: 2019-07-08T14:12:44+0000

Info:

Services

Risk: Info

Application: mysql

Port: 3306

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

A MySQL server is running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>

Version: 2019-07-08T14:12:44+0000

Info:

Services

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

A web server is running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>

Version: 2019-07-08T14:12:44+0000

Info:

Services

Risk: Info

Application: ipp

Port: 631

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

A TLScustom server answered on this port

Summary:

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>

Version: 2019-07-08T14:12:44+0000

Info:

Services

Risk: Info

Application: ipp

Port: 631

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

A web server is running on this port through SSL

Summary:

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>

Version: 2019-07-08T14:12:44+0000

Info:

Services

Risk: Info

Application: unknown

Port: 3500

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

A web server is running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>

Version: 2019-07-08T14:12:44+0000

Info:

Services

Risk: Info

Application: ftp

Port: 21

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

An FTP server is running on this port.

Here is its banner :

220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.2.200]

Summary:

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>

Version: 2019-07-08T14:12:44+0000

Info:

Services

Risk: Info

Application: http-proxy

Port: 8080

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

A web server is running on this port

Summary:

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>

Version: 2019-07-08T14:12:44+0000

Info:

Services

Risk: Info

Application: unknown

Port: 8181

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

A web server is running on this port

Summary:

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>

Version: 2019-07-08T14:12:44+0000

Info:

SMB log in

Risk: Info

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 10394

Vulnerability Detection Result:

It was possible to log into the remote host using the SMB protocol.

Summary:

This script attempts to logon into the remote host using login/password credentials.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Windows

Category: unknown

Copyright: Copyright (C) 2008 SecPod

Version: 2019-10-16T06:21:07+0000

Info:

SMB Login Successful For Authenticated Checks

Risk: Info

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 108539

Summary:

It was possible to login using the provided SMB credentials. Hence authenticated checks are enabled.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Windows

Category: unknown

Copyright: Copyright (C) 2019 Greenbone Networks GmbH

Version: \$Revision: 13248 \$

Info:

SMB NativeLanMan

Risk: Info

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 102011

Vulnerability Detection Result:

Detected Samba

Version: 4.3.11

Location: 445/tcp

CPE: cpe:/a:samba:samba:4.3.11

Concluded from version/product identification result:

Samba 4.3.11-Ubuntu

Extra information:

Detected SMB workgroup: WORKGROUP

Detected SMB server: Samba 4.3.11-Ubuntu

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: Copyright (C) 2009 LSS

Summary: NOSUMMARY

Version: 2019-12-12T09:38:57+0000

Info:

SMB NativeLanMan

Risk: Info

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 102011

Vulnerability Detection Result:

Detected SMB workgroup: WORKGROUP

Detected SMB server: Samba 4.3.11-Ubuntu

Detected OS: Ubuntu 14.04 or Ubuntu 16.04

Summary:

It is possible to extract OS, domain and SMB server information

from the Session Setup AndX Response packet which is generated during NTLM authentication.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: Copyright (C) 2009 LSS

Summary: NOSUMMARY

Version: 2019-12-12T09:38:57+0000

Info:

SMB Remote Version Detection

Risk: Info

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 807830

Vulnerability Detection Result:

SMBv1 and SMBv2 are enabled on remote target

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Detection of Server Message Block(SMB).

This script sends SMB Negotiation request and try to get the version from the response.

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: Copyright (C) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-05-16T07:13:31+0000

Info:

SMB/CIFS Server Detection

Risk: Info

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 11011

Vulnerability Detection Result:

A CIFS server is running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script detects whether port 445 and 139 are open and
if they are running a CIFS/SMB server.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: This script is Copyright (C) 2002 Renaud Deraison

Version: \$Revision: 13541 \$

Info:

SMB/CIFS Server Detection

Risk: Info

Application: netbios-ssn

Port: 139

Protocol: tcp

ScriptID: 11011

Vulnerability Detection Result:

A SMB server is running on this port

Summary:

This script detects whether port 445 and 139 are open and
if they are running a CIFS/SMB server.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: This script is Copyright (C) 2002 Renaud Deraison

Version: \$Revision: 13541 \$

Info:

SMBv1 enabled (Remote Check)

Risk: Info

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 140151

Vulnerability Detection Result:

SMBv1 is enabled for the SMB Server

Vulnerability Detection Method:

Checks if SMBv1 is enabled for the SMB Server based on the information provided by the following VT:

- SMB Remote Version Detection (OID: 1.3.6.1.4.1.25623.1.0.807830).

Summary:

The host has enabled SMBv1 for the SMB Server.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

References:

<https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices>

<https://support.microsoft.com/en-us/kb/2696547>

<https://support.microsoft.com/en-us/kb/204279>

CVSS Base Score: 0.0

Family name: Windows

Category: infos

Copyright: Copyright (C) 2017 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-05-20T06:24:13+0000

Info:

SSH Protocol Algorithms Supported

Risk: Info

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 105565

Vulnerability Detection Result:

The following options are supported by the remote ssh service:

kex_algorithms:

curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1

server_host_key_algorithms:

ssh-rsa,ssh-dss,ecdsa-sha2-nistp256,ssh-ed25519

encryption_algorithms_client_to_server:

aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chaCha20-poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se

encryption_algorithms_server_to_client:

aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chaCha20-poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se

mac_algorithms_client_to_server:

hmac-md5-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-96-etm@openssh.com,hmac-md5,hmac-sha1,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96

mac_algorithms_server_to_client:

hmac-md5-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-96-etm@openssh.com,hmac-md5,hmac-sha1,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96

compression_algorithms_client_to_server:

none,zlib@openssh.com

compression_algorithms_server_to_client:

none,zlib@openssh.com

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script detects which algorithms are supported by the remote SSH Service.

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: This script is Copyright (C) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-26T13:48:10+0000

Info:

SSH Protocol Versions Supported

Risk: Info

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 100259

Vulnerability Detection Result:

The remote SSH Server supports the following SSH Protocol Versions:

1.99

2.0

SSHv2 Fingerprint(s):

ecdsa-sha2-nistp256: 6f:3a:67:21:7c:1c:cc:71:f3:f2:33:58:ba:ea:17:0f

ssh-dss: b9:07:bc:1e:21:f8:aa:09:7a:f3:66:c9:4c:1e:93:82

ssh-ed25519: 31:0c:79:ba:be:a8:ef:8f:0a:f6:bb:45:70:97:b3:9b

ssh-rsa: 41:1c:56:97:4e:77:d2:3a:c5:fc:e1:e8:bb:52:c7:58

Summary:

Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service.

The following versions are tried: 1.33, 1.5, 1.99 and 2.0

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: This script is Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-26T13:48:10+0000

Info:

SSH Server type and version

Risk: Info

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 10267

Vulnerability Detection Result:

Remote SSH server banner: SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.10

Remote SSH supported authentication: password,publickey

Remote SSH text/login banner: (not available)

This is probably:

- OpenSSH

Concluded from remote connection attempt with credentials:

Login: OpenVAS-VT

Password: OpenVAS-VT

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This detects the SSH Server's type and version by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking.

Versions and Types should be omitted where possible.

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2006 SecuriTeam

Version: 2020-03-26T13:48:10+0000

Info:

SSL/TLS: Certificate - Self-Signed Certificate Detection

Risk: Info

Application: ipp

Port: 631

Protocol: tcp

ScriptID: 103140

Vulnerability Detection Result:

The certificate of the remote service is self signed.

Certificate details:

subject ...: CN=ubuntu

subject alternative names (SAN):

None

issued by .: CN=ubuntu

serial: 00CAF8B28C21AF760A

valid from : 2018-07-29 13:09:31 UTC

valid until: 2028-07-26 13:09:31 UTC

fingerprint (SHA-1): 2E765C0FA2F712952EEAAA57F287394B6C715C1D

fingerprint (SHA-256): 14B55D5019ECA82A814A4107ED1139BCC30EB3B97C717D5A9106C159C98B7F61

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

The SSL/TLS certificate on this port is self-signed.

References:

http://en.wikipedia.org/wiki/Self-signed_certificate

CVSS Base Score: 0.0

Family name: SSL and TLS

Category: infos

Copyright: This script is Copyright (C) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 8981 \$

Info:

SSL/TLS: Collect and Report Certificate Details

Risk: Info

Application: ipp

Port: 631

Protocol: tcp

ScriptID: 103692

Vulnerability Detection Result:

The following certificate details of the remote service were collected.

Certificate details:

subject ...: CN=ubuntu

subject alternative names (SAN):

None

issued by .: CN=ubuntu

serial: 00CAF8B28C21AF760A

valid from : 2018-07-29 13:09:31 UTC

valid until: 2028-07-26 13:09:31 UTC

fingerprint (SHA-1): 2E765C0FA2F712952EEAAA57F287394B6C715C1D

fingerprint (SHA-256): 14B55D5019ECA82A814A4107ED1139BCC30EB3B97C717D5A9106C159C98B7F61

Summary:

This script collects and reports the details of all SSL/TLS certificates.

This data will be used by other tests to verify server certificates.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: SSL and TLS

Category: infos

Copyright: Copyright 2013 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-04-04T13:38:03+0000

Info:

SSL/TLS: Hostname discovery from server certificate

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 111010

Vulnerability Detection Result:

The following additional but not resolvable hostnames were detected:

ubuntu

Summary:

It was possible to discover an additional hostname

of this server from its certificate Common or Subject Alt Name.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: SSL and TLS

Category: infos

Copyright: This script is Copyright (C) 2015 SCHUTZWERK GmbH

Summary: NOSUMMARY

Version: \$Revision: 13774 \$

Info:

SSL/TLS: HTTP Public Key Pinning (HPKP) Missing

Risk: Info

Application: ipp

Port: 631

Protocol: tcp

ScriptID: 108247

Vulnerability Detection Result:

The remote web server is not enforcing HPKP.

HTTP-Banner:

HTTP/1.1 200 OK

Date: ***replaced***

Server: CUPS/1.7 IPP/2.1

Content-Language: en

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

Last-Modified: ***replaced***

Content-Length: ***replaced***

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution:

Enable HPKP or add / configure the required directives correctly following the guides linked in the references.

Summary:

The remote web server is not enforcing HPKP.

References:

<https://owasp.org/www-project-secure-headers/>

<https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-for-http-hpkp>

<https://tools.ietf.org/html/rfc7469>

<https://securityheaders.io/>

CVSS Base Score: 0.0

Family name: SSL and TLS

Category: infos

Copyright: This script is Copyright (C) 2017 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-18T09:31:42+0000

Info:

SSL/TLS: HTTP Strict Transport Security (HSTS) Missing

Risk: Info

Application: ipp

Port: 631

Protocol: tcp

ScriptID: 105879

Vulnerability Detection Result:

The remote web server is not enforcing HSTS.

HTTP-Banner:

HTTP/1.1 200 OK

Date: ***replaced***

Server: CUPS/1.7 IPP/2.1

Content-Language: en

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

Last-Modified: ***replaced***

Content-Length: ***replaced***

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution:

Enable HSTS or add / configure the required directives correctly following the guides linked in the references.

Summary:

The remote web server is not enforcing HSTS.

References:

<https://owasp.org/www-project-secure-headers/>

https://owasp.org/www-project-secure-headers/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

<https://owasp.org/www-project-secure-headers/#http-strict-transport-security-hsts>

<https://tools.ietf.org/html/rfc6797>

<https://securityheaders.io/>

CVSS Base Score: 0.0

Family name: SSL and TLS

Category: infos

Copyright: This script is Copyright (C) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-02-28T07:44:42+0000

Info:

Traceroute

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 51662

Vulnerability Detection Result:

Here is the route from 192.168.2.100 to 192.168.2.200:

192.168.2.100

192.168.2.200

Summary:

A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution:

Block unwanted packets from escaping your network.

CVSS Base Score: 0.0

Family name: General

Category: unknown

Copyright: Copyright (C) 2010 E-Soft Inc. <http://www.securityspace.com>

Version: 2020-03-21T13:23:23+0000

Info:

Unknown OS and Service Banner Reporting

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 108441

Vulnerability Detection Result:

Unknown banners have been collected which might help to identify the OS running on this host. If these banners containing information about the host OS please report the following information to

<https://community.greenbone.net/c/vulnerability-tests>:

Banner: 220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.2.200]

Identified from: FTP banner on port 21/tcp

Summary:

This NVT consolidates and reports the information collected by the following NVTs:

- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

If you know any of the information reported here, please send the full output to the referenced community portal.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

References:

<https://community.greenbone.net/c/vulnerability-tests>

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: Copyright (C) 2018 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 12934 \$

Info:

UnrealIRCd Detection

Risk: Info

Application: irc

Port: 6667

Protocol: tcp

ScriptID: 809884

Vulnerability Detection Result:

Detected UnrealIRCd

Version: 3.2.8.1

Location: 6667/tcp

CPE: cpe:/a:unrealircd:unrealircd:3.2.8.1

Concluded from version/product identification result:

Unreal3.2.8.1

Summary:

Detection of UnrealIRCd Daemon. This script

sends a request to the server and gets the version from the response.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2017 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 10987 \$

Info:

WEBrick Detection (HTTP)

Risk: Info

Application: unknown

Port: 8181

Protocol: tcp

ScriptID: 112709

Vulnerability Detection Result:

Detected WEBrick

Version: 1.3.1

Location: 8181/tcp

CPE: cpe:/a:ruby-lang:webrick:1.3.1

Concluded from version/product identification result:

1.3.1

Summary:

This script detects the installed version of WEBrick.

In addition this script also tries to detect Ruby itself.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

References:

<https://github.com/ruby/webrick>

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2020 Greenbone Networks GmbH

Version: 2020-03-12T10:10:18+0000

Info:

WEBrick Detection (HTTP)

Risk: Info

Application: unknown

Port: 8181

Protocol: tcp

ScriptID: 112709

Vulnerability Detection Result:

Detected Ruby

Version: 2.3.7

Location: 8181/tcp

CPE: cpe:/a:ruby-lang:ruby:2.3.7

Concluded from version/product identification result:
2.3.7

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script detects the installed version of WEBrick.

In addition this script also tries to detect Ruby itself.

References:

<https://github.com/ruby/webrick>

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2020 Greenbone Networks GmbH

Version: 2020-03-12T10:10:18+0000

Info:

CPE Inventory

Risk: Info

Application: general

Port: 0

Protocol: CPE-T

ScriptID: 810002

Vulnerability Detection Result:

192.168.2.200|cpe:/a:apache:http_server:2.4.7

192.168.2.200|cpe:/a:apple:cups:1.7.2

192.168.2.200|cpe:/a:drupal:drupal:7.5

192.168.2.200|cpe:/a:eclipse:jetty:8.1.7.20120910

192.168.2.200|cpe:/a:openbsd:openssh:6.6.1p1

192.168.2.200|cpe:/a:oracle:mysql

192.168.2.200|cpe:/a:php:php:5.4.5

192.168.2.200|cpe:/a:phpmyadmin:phpmyadmin:3.5.8

192.168.2.200|cpe:/a:proftpd:proftpd:1.3.5

192.168.2.200|cpe:/a:ruby-lang:ruby:2.3.7

192.168.2.200|cpe:/a:ruby-lang:webrick:1.3.1

192.168.2.200|cpe:/a:rubyonrails:ruby_on_rails:4.2.4

192.168.2.200|cpe:/a:samba:samba:4.3.11

192.168.2.200|cpe:/a:unrealircd:unrealircd:3.2.8.1

192.168.2.200|cpe:/o:canonical:ubuntu_linux:14.04

Summary:

This routine uses information collected by other routines about

CPE identities of operating systems, services and applications detected during the scan.

Note: Some CPEs for specific products might show up twice or more in the output. Background:

After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

References:

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

CVSS Base Score: 0.0

Family name: Service detection

Category: end

Copyright: Copyright (c) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-10-24T11:29:24+0000

Info:

WEBrick Detection (HTTP)

Risk: Info

Application: unknown

Port: 3500

Protocol: tcp

ScriptID: 112709

Vulnerability Detection Result:

Detected WEBrick

Version: 1.3.1

Location: 3500/tcp

CPE: cpe:/a:ruby-lang:webrick:1.3.1

Concluded from version/product identification result:

1.3.1

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script detects the installed version of WEBrick.

In addition this script also tries to detect Ruby itself.

References:

<https://github.com/ruby/webrick>

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2020 Greenbone Networks GmbH

Version: 2020-03-12T10:10:18+0000

Info:

WEBrick Detection (HTTP)

Risk: Info

Application: unknown

Port: 3500

Protocol: tcp

ScriptID: 112709

Vulnerability Detection Result:

Detected Ruby

Version: 2.3.7

Location: 3500/tcp

CPE: cpe:/a:ruby-lang:ruby:2.3.7

Concluded from version/product identification result:

2.3.7

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script detects the installed version of WEBrick.

In addition this script also tries to detect Ruby itself.

References:

<https://github.com/ruby/webrick>

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2020 Greenbone Networks GmbH

Version: 2020-03-12T10:10:18+0000