OpenVas Vulnerability Report

HackerTarget.com

HackerTarget.com hosts the worlds most **trusted open source** vulnerability scanners. Allowing easy access to the process of testing and securing Internet facing systems.

Table of Contents

Summary

This document reports on the results of an automatic security scan. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

It only lists hosts that produced issues.

All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

Scan started:	**Thu Jan 17 23:04:39 2019 UTC**
Scan ended:	Fri Jan 18 07:20:04 2019 UTC
Task:	notary.ir

Vulnerability Summary

HIGH	MEDIUM	LOW
0	0	0

Any **HIGH** and **MEDIUM** risk vulnerabilities should be investigated and confirmed so that remediation can take place. **LOW** risk items should not be ignored as they can be stepping stones to High risk attacks.

Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
104.27.165.241 (notary.ir)	Jan 17, 23:04:47	Jan 18, 07:20:04	0	0	0	36	0
Total: 1			0	0	0	36	0

Results per Host

Host 104.27.165.241

Scanning of this host started at:	Thu Jan 17 23:04:47 2019 UTC
Number of results:	36

Port Summary for Host 104.27.165.241

Service (Port)	Threat Level
8080/tcp	Log
2087/tcp	Log
general/CPE-T	Log
8880/tcp	Log
2086/tcp	Log
general/tcp	Log
8443/tcp	Log
2096/tcp	Log
2052/tcp	Log
2095/tcp	Log
443/tcp	Log
2053/tcp	Log
2083/tcp	Log

Security Issues for Host 104.27.165.241

Log (CVSS: 0.0) general/tcp
NVT: OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

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 informations 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 openvas-plugins@wald.intevation.org.

Vulnerability Detection Result

Best matching OS:
OS: Linux Kernel
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.102002 (ICMP based OS Fingerprinting)
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information

Log Method

Details: OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

Version used: $Revision: 8968 $

Log (CVSS: 0.0) general/tcp
NVT: Traceroute (OID: 1.3.6.1.4.1.25623.1.0.51662)

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.

Vulnerability Detection Result

Here is the route from 45.33.6.98 to 104.27.165.241:
45.33.6.98
45.79.12.4
45.79.12.8
206.53.202.2
104.27.165.241

Solution

Block unwanted packets from escaping your network.

Log Method

Details: Traceroute (OID: 1.3.6.1.4.1.25623.1.0.51662)

Version used: $Revision: 8528 $

Log (CVSS: 0.0) general/CPE-T
NVT: CPE Inventory (OID: 1.3.6.1.4.1.25623.1.0.810002)

Summary

This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.

Vulnerability Detection Result

104.27.165.241|cpe:/o:linux:kernel

Log Method

Details: CPE Inventory (OID: 1.3.6.1.4.1.25623.1.0.810002)

Version used: $Revision: 8140 $

Log (CVSS: 0.0) 443/tcp
NVT: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

Summary

This detects the HTTP Server's type and version.

Vulnerability Detection Result

The remote web server type is :
cloudflare

Solution

Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display' Be sure to remove common logos like apache_pb.gif. With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Log Method

Details: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

Version used: $Revision: 8370 $

Log (CVSS: 0.0) 443/tcp
NVT: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

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 these are wrong please report to openvas-plugins@wald.intevation.org

Vulnerability Detection Result

The Hostname/IP "notary.ir" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable generic web app↵
lication 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 NOT 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 8.0.8)" 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://notary.ir/
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

Log Method

Details: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

Version used: $Revision: 8852 $

Log (CVSS: 0.0) 443/tcp
NVT: Detect Apache HTTPS (OID: 1.3.6.1.4.1.25623.1.0.15588)

Summary

An SSL detection issue might impede the OpenVAS Scan.

Description :

OpenVAS has discovered that it is talking in plain HTTP on a SSL port.

OpenVAS has corrected this issue by enabled HTTPS on this port only. However if other SSL ports are used on the remote host, they might be skipped.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

Enable SSL tests in the 'Services' preference setting, or increase the timeouts if this option is already set and the plugin missed this port.

Log Method

Details: Detect Apache HTTPS (OID: 1.3.6.1.4.1.25623.1.0.15588)

Version used: $Revision: 6065 $

Log (CVSS: 0.0) 2052/tcp
NVT: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

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 these are wrong please report to openvas-plugins@wald.intevation.org

Vulnerability Detection Result

The Hostname/IP "notary.ir" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable generic web app↵
lication scanning" option within the "Global variable settings" of the scan config in use.
This service seems to be NOT 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 8.0.8)" 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://notary.ir:2052/
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

Log Method

Details: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

Version used: $Revision: 8852 $

Log (CVSS: 0.0) 2052/tcp
NVT: Hidden WWW server name (OID: 1.3.6.1.4.1.25623.1.0.11239)

Summary

It seems that your web server tries to hide its version or name, which is a good thing. However, using a special crafted request, OpenVAS was able to discover it.

Vulnerability Detection Result

It seems that your web server tries to hide its version
or name, which is a good thing.
However, using a special crafted request, OpenVAS was able
to determine that is is running :
cloudflare
Solution: Fix your configuration.

Solution

Fix your configuration.

Log Method

Details: Hidden WWW server name (OID: 1.3.6.1.4.1.25623.1.0.11239)

Version used: $Revision: 8023 $

Log (CVSS: 0.0) 2052/tcp
NVT: Service Detection with 'GET' Request (OID: 1.3.6.1.4.1.25623.1.0.17975)

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.

Vulnerability Detection Result

A web server is running on this port

Log Method

Details: Service Detection with 'GET' Request (OID: 1.3.6.1.4.1.25623.1.0.17975)

Version used: $Revision: 8977 $

Log (CVSS: 0.0) 2053/tcp
NVT: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

Summary

This detects the HTTP Server's type and version.

Vulnerability Detection Result

The remote web server type is :
cloudflare

Solution

Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display' Be sure to remove common logos like apache_pb.gif. With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Log Method

Details: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

Version used: $Revision: 8370 $

Log (CVSS: 0.0) 2053/tcp
NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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.

Vulnerability Detection Result

A web server is running on this port

Log Method

Details: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

Version used: $Revision: 8188 $

Log (CVSS: 0.0) 2053/tcp
NVT: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

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 these are wrong please report to openvas-plugins@wald.intevation.org

Vulnerability Detection Result

The Hostname/IP "notary.ir" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable generic web app↵
lication 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 NOT 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 8.0.8)" 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://notary.ir:2053/
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

Log Method

Details: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

Version used: $Revision: 8852 $

Log (CVSS: 0.0) 2053/tcp
NVT: Detect Apache HTTPS (OID: 1.3.6.1.4.1.25623.1.0.15588)

Summary

An SSL detection issue might impede the OpenVAS Scan.

Description :

OpenVAS has discovered that it is talking in plain HTTP on a SSL port.

OpenVAS has corrected this issue by enabled HTTPS on this port only. However if other SSL ports are used on the remote host, they might be skipped.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

Enable SSL tests in the 'Services' preference setting, or increase the timeouts if this option is already set and the plugin missed this port.

Log Method

Details: Detect Apache HTTPS (OID: 1.3.6.1.4.1.25623.1.0.15588)

Version used: $Revision: 6065 $

Log (CVSS: 0.0) 2083/tcp
NVT: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

Summary

This detects the HTTP Server's type and version.

Vulnerability Detection Result

The remote web server type is :
cloudflare

Solution

Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display' Be sure to remove common logos like apache_pb.gif. With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Log Method

Details: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

Version used: $Revision: 8370 $

Log (CVSS: 0.0) 2083/tcp
NVT: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

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 these are wrong please report to openvas-plugins@wald.intevation.org

Vulnerability Detection Result

The Hostname/IP "notary.ir" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable generic web app↵
lication 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 NOT 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 8.0.8)" 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://notary.ir:2083/
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

Log Method

Details: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

Version used: $Revision: 8852 $

Log (CVSS: 0.0) 2083/tcp
NVT: Detect Apache HTTPS (OID: 1.3.6.1.4.1.25623.1.0.15588)

Summary

An SSL detection issue might impede the OpenVAS Scan.

Description :

OpenVAS has discovered that it is talking in plain HTTP on a SSL port.

OpenVAS has corrected this issue by enabled HTTPS on this port only. However if other SSL ports are used on the remote host, they might be skipped.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

Enable SSL tests in the 'Services' preference setting, or increase the timeouts if this option is already set and the plugin missed this port.

Log Method

Details: Detect Apache HTTPS (OID: 1.3.6.1.4.1.25623.1.0.15588)

Version used: $Revision: 6065 $

Log (CVSS: 0.0) 2086/tcp
NVT: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

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 these are wrong please report to openvas-plugins@wald.intevation.org

Vulnerability Detection Result

The Hostname/IP "notary.ir" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable generic web app↵
lication scanning" option within the "Global variable settings" of the scan config in use.
This service seems to be NOT 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 8.0.8)" 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://notary.ir:2086/
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

Log Method

Details: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

Version used: $Revision: 8852 $

Log (CVSS: 0.0) 2086/tcp
NVT: Hidden WWW server name (OID: 1.3.6.1.4.1.25623.1.0.11239)

Summary

It seems that your web server tries to hide its version or name, which is a good thing. However, using a special crafted request, OpenVAS was able to discover it.

Vulnerability Detection Result

It seems that your web server tries to hide its version
or name, which is a good thing.
However, using a special crafted request, OpenVAS was able
to determine that is is running :
cloudflare
Solution: Fix your configuration.

Solution

Fix your configuration.

Log Method

Details: Hidden WWW server name (OID: 1.3.6.1.4.1.25623.1.0.11239)

Version used: $Revision: 8023 $

Log (CVSS: 0.0) 2086/tcp
NVT: Service Detection with 'GET' Request (OID: 1.3.6.1.4.1.25623.1.0.17975)

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.

Vulnerability Detection Result

A web server is running on this port

Log Method

Details: Service Detection with 'GET' Request (OID: 1.3.6.1.4.1.25623.1.0.17975)

Version used: $Revision: 8977 $

Log (CVSS: 0.0) 2087/tcp
NVT: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

Summary

This detects the HTTP Server's type and version.

Vulnerability Detection Result

The remote web server type is :
cloudflare

Solution

Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display' Be sure to remove common logos like apache_pb.gif. With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Log Method

Details: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

Version used: $Revision: 8370 $

Log (CVSS: 0.0) 2087/tcp
NVT: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

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 these are wrong please report to openvas-plugins@wald.intevation.org

Vulnerability Detection Result

The Hostname/IP "notary.ir" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable generic web app↵
lication 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 NOT 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 8.0.8)" 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://notary.ir:2087/
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

Log Method

Details: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

Version used: $Revision: 8852 $

Log (CVSS: 0.0) 2087/tcp
NVT: Detect Apache HTTPS (OID: 1.3.6.1.4.1.25623.1.0.15588)

Summary

An SSL detection issue might impede the OpenVAS Scan.

Description :

OpenVAS has discovered that it is talking in plain HTTP on a SSL port.

OpenVAS has corrected this issue by enabled HTTPS on this port only. However if other SSL ports are used on the remote host, they might be skipped.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

Enable SSL tests in the 'Services' preference setting, or increase the timeouts if this option is already set and the plugin missed this port.

Log Method

Details: Detect Apache HTTPS (OID: 1.3.6.1.4.1.25623.1.0.15588)

Version used: $Revision: 6065 $

Log (CVSS: 0.0) 2095/tcp
NVT: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

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 these are wrong please report to openvas-plugins@wald.intevation.org

Vulnerability Detection Result

The Hostname/IP "notary.ir" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable generic web app↵
lication scanning" option within the "Global variable settings" of the scan config in use.
This service seems to be NOT 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 8.0.8)" 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://notary.ir:2095/
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

Log Method

Details: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

Version used: $Revision: 8852 $

Log (CVSS: 0.0) 2095/tcp
NVT: Hidden WWW server name (OID: 1.3.6.1.4.1.25623.1.0.11239)

Summary

It seems that your web server tries to hide its version or name, which is a good thing. However, using a special crafted request, OpenVAS was able to discover it.

Vulnerability Detection Result

It seems that your web server tries to hide its version
or name, which is a good thing.
However, using a special crafted request, OpenVAS was able
to determine that is is running :
cloudflare
Solution: Fix your configuration.

Solution

Fix your configuration.

Log Method

Details: Hidden WWW server name (OID: 1.3.6.1.4.1.25623.1.0.11239)

Version used: $Revision: 8023 $

Log (CVSS: 0.0) 2095/tcp
NVT: Service Detection with 'GET' Request (OID: 1.3.6.1.4.1.25623.1.0.17975)

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.

Vulnerability Detection Result

A web server is running on this port

Log Method

Details: Service Detection with 'GET' Request (OID: 1.3.6.1.4.1.25623.1.0.17975)

Version used: $Revision: 8977 $

Log (CVSS: 0.0) 2096/tcp
NVT: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

Summary

This detects the HTTP Server's type and version.

Vulnerability Detection Result

The remote web server type is :
cloudflare

Solution

Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display' Be sure to remove common logos like apache_pb.gif. With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Log Method

Details: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

Version used: $Revision: 8370 $

Log (CVSS: 0.0) 2096/tcp
NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

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.

Vulnerability Detection Result

A web server is running on this port

Log Method

Details: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

Version used: $Revision: 8188 $

Log (CVSS: 0.0) 2096/tcp
NVT: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

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 these are wrong please report to openvas-plugins@wald.intevation.org

Vulnerability Detection Result

The Hostname/IP "notary.ir" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable generic web app↵
lication 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 NOT 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 8.0.8)" 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://notary.ir:2096/
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

Log Method

Details: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

Version used: $Revision: 8852 $

Log (CVSS: 0.0) 2096/tcp
NVT: Detect Apache HTTPS (OID: 1.3.6.1.4.1.25623.1.0.15588)

Summary

An SSL detection issue might impede the OpenVAS Scan.

Description :

OpenVAS has discovered that it is talking in plain HTTP on a SSL port.

OpenVAS has corrected this issue by enabled HTTPS on this port only. However if other SSL ports are used on the remote host, they might be skipped.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

Enable SSL tests in the 'Services' preference setting, or increase the timeouts if this option is already set and the plugin missed this port.

Log Method

Details: Detect Apache HTTPS (OID: 1.3.6.1.4.1.25623.1.0.15588)

Version used: $Revision: 6065 $

Log (CVSS: 0.0) 8080/tcp
NVT: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

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 these are wrong please report to openvas-plugins@wald.intevation.org

Vulnerability Detection Result

The Hostname/IP "notary.ir" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable generic web app↵
lication scanning" option within the "Global variable settings" of the scan config in use.
This service seems to be NOT 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 8.0.8)" 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://notary.ir: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

Log Method

Details: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

Version used: $Revision: 8852 $

Log (CVSS: 0.0) 8080/tcp
NVT: Hidden WWW server name (OID: 1.3.6.1.4.1.25623.1.0.11239)

Summary

It seems that your web server tries to hide its version or name, which is a good thing. However, using a special crafted request, OpenVAS was able to discover it.

Vulnerability Detection Result

It seems that your web server tries to hide its version
or name, which is a good thing.
However, using a special crafted request, OpenVAS was able
to determine that is is running :
cloudflare
Solution: Fix your configuration.

Solution

Fix your configuration.

Log Method

Details: Hidden WWW server name (OID: 1.3.6.1.4.1.25623.1.0.11239)

Version used: $Revision: 8023 $

Log (CVSS: 0.0) 8080/tcp
NVT: Service Detection with 'GET' Request (OID: 1.3.6.1.4.1.25623.1.0.17975)

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.

Vulnerability Detection Result

A web server is running on this port

Log Method

Details: Service Detection with 'GET' Request (OID: 1.3.6.1.4.1.25623.1.0.17975)

Version used: $Revision: 8977 $

Log (CVSS: 0.0) 8443/tcp
NVT: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

Summary

This detects the HTTP Server's type and version.

Vulnerability Detection Result

The remote web server type is :
cloudflare

Solution

Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display' Be sure to remove common logos like apache_pb.gif. With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Log Method

Details: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

Version used: $Revision: 8370 $

Log (CVSS: 0.0) 8443/tcp
NVT: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

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 these are wrong please report to openvas-plugins@wald.intevation.org

Vulnerability Detection Result

The Hostname/IP "notary.ir" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable generic web app↵
lication 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 NOT 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 8.0.8)" 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://notary.ir:8443/
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

Log Method

Details: CGI Scanning Consolidation (OID: 1.3.6.1.4.1.25623.1.0.111038)

Version used: $Revision: 8852 $

Log (CVSS: 0.0) 8443/tcp
NVT: Detect Apache HTTPS (OID: 1.3.6.1.4.1.25623.1.0.15588)

Summary

An SSL detection issue might impede the OpenVAS Scan.

Description :

OpenVAS has discovered that it is talking in plain HTTP on a SSL port.

OpenVAS has corrected this issue by enabled HTTPS on this port only. However if other SSL ports are used on the remote host, they might be skipped.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

Enable SSL tests in the 'Services' preference setting, or increase the timeouts if this option is already set and the plugin missed this port.

Log Method

Details: Detect Apache HTTPS (OID: 1.3.6.1.4.1.25623.1.0.15588)

Version used: $Revision: 6065 $

Log (CVSS: 0.0) 8880/tcp
NVT: Service Detection with 'GET' Request (OID: 1.3.6.1.4.1.25623.1.0.17975)

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.

Vulnerability Detection Result

A web server is running on this port

Log Method

Details: Service Detection with 'GET' Request (OID: 1.3.6.1.4.1.25623.1.0.17975)

Version used: $Revision: 8977 $

This file was automatically generated.