Scan Report

June 19, 2024

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Europe/Paris”, which is abbreviated “CEST”. The task was “Task 192.168.1.202”. The scan started at Wed Jun 19 23:44:24 2024 CEST and ended at Wed Jun 19 23:50:41 2024 CEST. 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.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.1.202 kali.lan	0	0	0	10	0
Total: 1	0	0	0	10	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level “High” are not shown.
Issues with the threat level “Medium” are not shown.
Issues with the threat level “Low” are not shown.
Issues with the threat level “Log” are not shown.
Issues with the threat level “Debug” are not shown.
Issues with the threat level “False Positive” are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains results 1 to 10 of the 23 results selected by the filtering described above. Before filtering there were 23 results.

2 Results per Host

2.1 192.168.1.202

Host scan start	Wed Jun 19 23:45:46 2024 CEST
Host scan end	Wed Jun 19 23:50:34 2024 CEST

Service (Port)	Threat Level
general/tcp	Log
80/tcp	Log
general/CPE-T	Log
9390/tcp	Log

2.1.1 Log general/tcp

Log (CVSS: 0.0)

NVT: Hostname Determination Reporting

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

The script reports information on how the hostname of the target was determined.

Quality of Detection: 80

Vulnerability Detection Result

```
Hostname determination for IP 192.168.1.202:
Hostname|Source
kali.lan|Reverse-DNS
```

Solution:

Log Method

Details: `Hostname Determination Reporting`

OID:1.3.6.1.4.1.25623.1.0.108449

Version used: `2022-07-27T12:11:28+02:00`

Log (CVSS: 0.0)

NVT: OS Detection Consolidation and Reporting

Summary

This script consolidates the OS information detected by several VTs 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 forum.

Quality of Detection: 80

Vulnerability Detection Result

```
Best matching OS:
OS:           Linux/Unix
CPE:          cpe:/o:linux:kernel
Found by VT:  1.3.6.1.4.1.25623.1.0.103825 (OpenVAS / Greenbone Vulnerability Ma
↪nager Detection (OMP/GMP))
Setting key "Host/runs_unixoide" based on this information
```

Solution:

Log Method

Details: `OS Detection Consolidation and Reporting`

OID:1.3.6.1.4.1.25623.1.0.105937

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `2024-06-04T07:05:28+02:00`

References

url: `https://forum.greenbone.net/c/vulnerability-tests/7`

[return to 192.168.1.202]

2.1.2 Log 80/tcp

Log (CVSS: 0.0)

NVT: CGI Scanning Consolidation

Summary

The script consolidates various information for CGI (Web application) 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 forum.

Quality of Detection: 80

Vulnerability Detection Result

```
The Hostname/IP "kali.lan" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 23.0.1)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. 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://kali.lan/
While this is not, in and of itself, a bug, you should manually inspect these di
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method

Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2024-02-08T06:05:59+02:00

References

url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)

NVT: HTTP Security Headers Detection

Summary

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

Quality of Detection: 80

Vulnerability Detection Result

```
Header Name             | Header Value
--------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪---------------------
Content-Security-Policy | default-src 'none'; object-src 'none'; base-uri 'none'
↪; connect-src 'self'; script-src 'self'; frame-ancestors 'none'; form-action '
↪self'; style-src-elem 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'
↪; img-src 'self' blob
X-Frame-Options         | SAMEORIGIN
Missing Headers                   | More Information
--------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪-----------------------------------------------
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-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, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method

Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T08:19:43+02:00

References

url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)

NVT: Response Time / No 404 Error Code Check

Summary
This VT tests if the remote web server does not reply with a 404 error code and checks if it is replying to the scanners requests in a reasonable amount of time.

Quality of Detection: 80

Vulnerability Detection Result

```
The host returns a 30x (e.g. 301) error code when a non-existent file is request
↪ed. Some HTTP-related checks have been disabled.
```

Solution:

Vulnerability Insight
This web server might show the following issues:
- it is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map, search page, authentication page or redirect instead.
The Scanner might enabled some counter measures for that, however they might be insufficient. If a great number of security issues are reported for this port, they might not all be accurate.
- it doesn't response in a reasonable amount of time to various HTTP requests sent by this VT.
In order to keep the scan total time to a reasonable amount, the remote web server might not be tested. If the remote server should be tested it has to be fixed to have it reply to the scanners requests in a reasonable amount of time.
Alternatively the 'Maximum response time (in seconds)' preference could be raised to a higher value if longer scan times are accepted.

Log Method
Details: `Response Time / No 404 Error Code Check`
OID:1.3.6.1.4.1.25623.1.0.10386
Version used: `2023-07-07T07:05:26+02:00`

Log (CVSS: 0.0)

NVT: Services

Summary
This plugin performs service detection.

Quality of Detection: 80

Vulnerability Detection Result

... continues on next page ...

. . . continued from previous page . . .

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

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). 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.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T07:05:19+02:00`

[return to 192.168.1.202]

2.1.3 Log general/CPE-T

Log (CVSS: 0.0)

NVT: CPE Inventory

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.

Quality of Detection: 80

Vulnerability Detection Result

```
192.168.1.202|cpe:/a:greenbone:greenbone_vulnerability_manager:22.5
192.168.1.202|cpe:/o:linux:kernel
```

Solution:

Log Method
Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `2022-07-27T12:11:28+02:00`

. . . continues on next page . . .

. . . continued from previous page . . .

References

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

[return to 192.168.1.202]

2.1.4 Log 9390/tcp

Log (CVSS: 0.0)

NVT: OpenVAS / Greenbone Vulnerability Manager Detection (OMP/GMP)

Summary

OpenVAS Management Protocol (OMP) / Greenbone Management Protocol (GMP) based detection of an OpenVAS Manager (openvasmd) or Greebone Vulnerability Manager (gmvd).

Quality of Detection: 80

Vulnerability Detection Result

```
Detected Greenbone Vulnerability Manager
Version:       22.5
Location:      9390/tcp
CPE:           cpe:/a:greenbone:greenbone_vulnerability_manager:22.5
Concluded from version/product identification result:
 - GMP protocol version request:  <get_version/>
 - GMP protocol version response: <get_version_response status="200" status_text
↪="OK"><version>22.5</version>
```

Solution:

Log Method

Details: OpenVAS / Greenbone Vulnerability Manager Detection (OMP/GMP)

OID:1.3.6.1.4.1.25623.1.0.103825

Version used: 2023-03-24T11:19:42+02:00

Log (CVSS: 0.0)

NVT: Service Detection with '<xml/>' Request

Summary

This plugin performs service detection.

Quality of Detection: 80

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
A OpenVAS / Greenbone Vulnerability Manager supporting the OMP/GMP protocol seem
↪s to be running on this port.
```

Solution:

Vulnerability Insight

This plugin is a complement of the plugin 'Services' (OID: 1.3.6.1.4.1.25623.1.0.10330). It sends a '<xml/>' request to the remaining unknown services and tries to identify them.

Log Method

Details: `Service Detection with '<xml/>' Request`
OID:1.3.6.1.4.1.25623.1.0.108198
Version used: `2023-06-14T07:05:19+02:00`

Log (CVSS: 0.0)

NVT: Services

Summary

This plugin performs service detection.

Quality of Detection: 80

Vulnerability Detection Result

```
A TLScustom server answered on this port
```

Solution:

Vulnerability Insight

This plugin attempts to guess which service is running on the remote port(s). 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.

Log Method

Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T07:05:19+02:00`

[return to 192.168.1.202]