Scan Report

February 4, 2025

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "67a114e6390ada1164105bc2-67a1292a390ada1164149a3e-50f76ff2". The scan started at Mon Feb 3 20:38:22 2025 UTC and ended at . 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
194.53.193.163	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.
Only results with a minimum QoD of 70 are shown.

This report contains all 10 results selected by the filtering described above. Before filtering there were 22 results.

2 Results per Host

2.1 194.53.193.163

Host scan start Mon Feb 3 20:39:25 2025 UTC
Host scan end

Service (Port)	Threat Level
53/udp	Log
80/tcp	Log
21/tcp	Log
general/tcp	Log

2.1.1 Log 53/udp

Log (CVSS: 0.0)
NVT: DNS Server Detection (UDP)

Summary
UDP based detection of a DNS server.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The remote DNS server banner is:`
`9.11.36-RedHat-9.11.36-16.el8_10.2`

. . . continues on next page . . .

... continued from previous page ...

Solution:

Log Method
Details: DNS Server Detection (UDP)
OID:1.3.6.1.4.1.25623.1.0.100069
Version used: 2021-11-30T08:05:58Z

[return to 194.53.193.163]

2.1.2 Log 80/tcp

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 (QoD): 80%

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------
↪----------------------------------------------------------------------------
↪-----------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
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
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
```

... continues on next page ...

... continued from previous page ...

```
↪/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-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, 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: 2021-07-14T06:19:43Z

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: HTTP Server type and version

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote HTTP Server banner is:
Server: imunify360-webshield/1.21
```

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
The script consolidates and reports various information for web application (formerly called '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 forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The Hostname/IP "drlovesexshop.com" 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.
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 23.8.5)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
http://drlovesexshop.com/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: Web Application Scanning Consolidation / Info Reporting
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2024-09-19T05:05:57Z

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

[return to 194.53.193.163]

2.1.3 Log 21/tcp

Log (CVSS: 0.0)
NVT: FTP Banner Detection

Summary
This script detects and reports a FTP Server Banner.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Remote FTP server banner:
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 4 of 50 allowed.
220-Local time is now 21:39. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
This is probably (a):
- Pure-FTPd
- Various FTP servers (e.g. Zyxel Access Points)
Server operating system information collected via "SYST" command:
215 UNIX Type: L8
```

Solution:

Log Method
Details: FTP Banner Detection
OID:1.3.6.1.4.1.25623.1.0.10092
Version used: 2024-06-07T15:38:39Z

Log (CVSS: 0.0)
NVT: Pure-FTPd FTP Server Detection

Summary
The script is grabbing the banner of a FTP server and sends a 'HELP' command to identify a Pure-FTPd FTP Server from the reply.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected Pure-FTPd
Version:       unknown
Location:      21/tcp
CPE:           cpe:/a:pureftpd:pure-ftpd
Concluded from version/product identification result:
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 4 of 50 allowed.
220-Local time is now 21:39. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
```

Solution:

Log Method
Details: `Pure-FTPd FTP Server Detection`
OID:1.3.6.1.4.1.25623.1.0.111110
Version used: `2023-07-26T05:05:09Z`

References
`url: https://www.pureftpd.org`

[return to 194.53.193.163]

2.1.4 Log general/tcp

Log (CVSS: 0.0)
NVT: ISC BIND Detection Consolidation

Summary
Consolidation of ISC BIND detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected ISC BIND
```

... continues on next page ...

... continued from previous page ...

```
Version:        9.11.36
Location:       53/udp
CPE:            cpe:/a:isc:bind:9.11.36
Concluded from version/product identification result:
9.11.36-RedHat-9.11.36-16.el8_10.2
```

Solution:

Log Method
Details: ISC BIND Detection Consolidation
OID:1.3.6.1.4.1.25623.1.0.145294
Version used: 2022-03-28T10:48:38Z

References
url: https://www.isc.org/bind/

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 (QoD): 80%

Vulnerability Detection Result

```
Best matching OS:
OS:             Redhat Linux 8
Version:        8
CPE:            cpe:/o:redhat:linux:8
Found by VT:    1.3.6.1.4.1.25623.1.0.108014 (Operating System (OS) Detection (DNS
↪))
Concluded from DNS server banner on port 53/udp: 9.11.36-RedHat-9.11.36-16.el8_1
↪0.2
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS:             Linux/Unix
CPE:            cpe:/o:linux:kernel
Found by VT:    1.3.6.1.4.1.25623.1.0.105355 (Operating System (OS) Detection (FTP
↪))
Concluded from FTP banner on port 21/tcp: 220---------- Welcome to Pure-FTPd [pr
↪ivsep] [TLS] ----------
```

... continues on next page ...

... continued from previous page ...

```
220-You are user number 4 of 50 allowed.
220-Local time is now 21:39. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
```

Solution:

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2025-01-31T15:39:24Z

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

Log (CVSS: 0.0)
NVT: Traceroute

Summary
Collect information about the network route and network distance between the scanner host and the target host.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Network route from scanner (172.18.0.8) to target (194.53.193.163):
172.18.0.8
10.206.7.90
10.206.35.44
10.206.32.2
173.255.239.102
23.203.156.16
62.115.40.44
62.115.137.215
62.115.120.69
62.115.185.93
88.220.206.191
88.220.207.205
88.220.207.206
194.53.193.163
Network distance between scanner and target: 14
```

Solution:

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Insight
For internal networks, the distances are usually small, often less than 4 hosts between scanner and target. For public targets the distance is greater and might be 10 hosts or more.

Log Method
A combination of the protocols ICMP and TCP is used to determine the route. This method is applicable for IPv4 only and it is also known as 'traceroute'.
Details: `Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `2022-10-17T11:13:19Z`

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This VT consolidates and reports the information collected by the following VTs:
- 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 forum.

Quality of Detection (QoD): 80%

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://forum.greenbone.net/c/vulnerabili
↪ty-tests/7:
Banner: Server: imunify360-webshield/1.21
Identified from: HTTP Server banner on port 80/tcp
```

Solution:

Log Method
Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `2023-06-22T10:34:15Z`

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

[return to 194.53.193.163]

This file was automatically generated.