Scan Report

March 22, 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 “Immediate scan of IP 10.0.0.112”. The scan started at Fri Mar 21 20:46:05 2025 UTC and ended at Fri Mar 21 20:59:22 2025 UTC. 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
10.0.0.112	0	1	2	24	0
Total: 1	0	1	2	24	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 all 27 results selected by the filtering described above. Before filtering there were 39 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
10.0.0.112	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 10.0.0.112

Host scan start	Fri Mar 21 20:46:47 2025 UTC
Host scan end	Fri Mar 21 20:59:18 2025 UTC

Service (Port)	Threat Level
21/tcp	Medium
general/icmp	Low
general/tcp	Low
80/tcp	Log
53/tcp	Log
21/tcp	Log
139/tcp	Log

. . . (continues) . . .

. . . (continued) . . .

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

2.1.1 Medium 21/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

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

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Please specify the password.
Anonymous sessions:     331 Please specify the password.
```

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

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

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.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2023-12-20T05:05:58Z`

[return to 10.0.0.112]

2.1.2 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
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.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2025-01-21T05:37:33Z`

References
`cve: CVE-1999-0524`
`url: https://datatracker.ietf.org/doc/html/rfc792`
`url: https://datatracker.ietf.org/doc/html/rfc2780`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 10.0.0.112]

2.1.3 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 2560935009
Packet 2: 2560936100
```

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

Solution:
Solution type: Mitigation
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.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

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.
Details: `TCP Timestamps Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

References

```
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[return to 10.0.0.112]

2.1.4 Log 80/tcp

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: Apache/2.4.52 (Ubuntu)
```

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: HTTP Server Banner Enumeration

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).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
It was possible to enumerate the following HTTP server banner(s):
Server banner                 | Enumeration technique
--------------------------------------------------------------------------
↪-----------------
Server: Apache/2.4.52 (Ubuntu) | Invalid HTTP 00.5 GET request (non-existent HTT
↪P version) to '/'
```

Solution:

Log Method

. . . continues on next page . . .

... continued from previous page ...

Details: HTTP Server Banner Enumeration
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: 2025-01-31T15:39:24Z

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
↪/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
```

... continues on next page ...

. . . continued from previous page . . .

```
↪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: 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 "10.0.0.112" 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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪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; Greenbone OS 22.04.27)" was used to ac
↪cess 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://10.0.0.112/
http://10.0.0.112/dvwa
http://10.0.0.112/mutillidae
http://10.0.0.112/mutillidae/src
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
The following directories were excluded from web application scanning because th
↪e "Regex pattern to exclude directories from CGI scanning" setting of the VT "
↪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|graph
↪ic|grafik|picture|bilder|thumbnail|media/|skins?/)"
http://10.0.0.112/icons
http://10.0.0.112/javascript
Directory index found at:
http://10.0.0.112/mutillidae/
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://10.0.0.112/mutillidae/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
```

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

Log (CVSS: 0.0)

NVT: Check open ports

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This plugin checks if the port scanners did not kill a service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by a plugin
```

Solution:

Log Method

Details: `Check open ports`
OID:1.3.6.1.4.1.25623.1.0.10919
Version used: `2023-08-03T05:05:16Z`

Log (CVSS: 0.0)
NVT: Services

Summary

This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
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: `2023-06-14T05:05:19Z`

[return to 10.0.0.112]

2.1.5 Log 53/tcp

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

Summary
TCP based detection of a DNS server.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote DNS server banner is:
9.18.30-0ubuntu0.22.04.2-Ubuntu
```

Solution:

Log Method
Details: `DNS Server Detection (TCP)`
OID:1.3.6.1.4.1.25623.1.0.108018
Version used: `2021-11-30T08:05:58Z`

Log (CVSS: 0.0)
NVT: Check open ports

Summary
This plugin checks if the port scanners did not kill a service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by a plugin
```

Solution:

Log Method
Details: `Check open ports`
OID:1.3.6.1.4.1.25623.1.0.10919
Version used: `2023-08-03T05:05:16Z`

[return to 10.0.0.112]

2.1.6 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 (vsFTPd 3.0.5)
This is probably (a):
- vsFTPd
```

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: vsFTPd FTP Server Detection

Summary
The script is grabbing the banner of a FTP server and attempts to identify a vsFTPd FTP Server and its version from the reply.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected vsFTPd
Version:       3.0.5
Location:      21/tcp
CPE:           cpe:/a:beasts:vsftpd:3.0.5
Concluded from version/product identification result:
220 (vsFTPd 3.0.5)
```

Solution:

Log Method
Details: `vsFTPd FTP Server Detection`
OID:1.3.6.1.4.1.25623.1.0.111050
Version used: `2023-07-26T05:05:09Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: FTP Missing Support For AUTH TLS

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

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

Solution:

Log Method
Details: `SSL/TLS: FTP Missing Support For AUTH TLS`
OID:1.3.6.1.4.1.25623.1.0.108553
Version used: `2021-03-19T08:13:38Z`

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
An FTP server is running on this port.
Here is its banner :
220 (vsFTPd 3.0.5)
```

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: `2023-06-14T05:05:19Z`

[return to 10.0.0.112]

2.1.7 Log 139/tcp

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

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

Solution:

Log Method
Details: `SMB/CIFS Server Detection`
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: `2023-08-01T13:29:10Z`

[return to 10.0.0.112]

2.1.8 Log 445/tcp

Log (CVSS: 0.0)
NVT: SMB log in

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

Quality of Detection (QoD): 97%

Vulnerability Detection Result

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

Solution:

Log Method
Details: `SMB log in`
OID:1.3.6.1.4.1.25623.1.0.10394
Version used: `2023-11-28T05:05:32Z`

Log (CVSS: 0.0)
NVT: SMB Remote Version Detection

Summary
Detection of Server Message Block(SMB).
This script sends SMB Negotiation request and try to get the version from the response.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
SMBv2 and SMBv3 are enabled on remote target
```

Solution:

Log Method
Details: `SMB Remote Version Detection`
OID:1.3.6.1.4.1.25623.1.0.807830
Version used: `2023-07-26T05:05:09Z`

Log (CVSS: 0.0)
NVT: SMB Login Successful For Authenticated Checks

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution:

Log Method
Details: `SMB Login Successful For Authenticated Checks`
OID:1.3.6.1.4.1.25623.1.0.108539
Version used: `2023-07-28T16:09:07Z`

Log (CVSS: 0.0)
NVT: Microsoft Windows SMB Accessible Shares

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

. . . continues on next page . . .

. . . continued from previous page . . .

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following shares were found
IPC$
```

Solution:

Log Method

Details: `Microsoft Windows SMB Accessible Shares`
OID:1.3.6.1.4.1.25623.1.0.902425
Version used: `2023-01-31T10:08:41Z`

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

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

Solution:

Log Method

Details: `SMB/CIFS Server Detection`
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: `2023-08-01T13:29:10Z`

[return to 10.0.0.112]

2.1.9 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:

. . . continues on next page . . .

. . . continued from previous page . . .

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 (QoD): 80%

Vulnerability Detection Result

```
10.0.0.112|cpe:/a:apache:http_server:2.4.52
10.0.0.112|cpe:/a:beasts:vsftpd:3.0.5
10.0.0.112|cpe:/a:isc:bind:9.18.30
10.0.0.112|cpe:/o:canonical:ubuntu_linux
```

Solution:

Log Method

Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `2022-07-27T10:11:28Z`

References

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

[return to 10.0.0.112]

2.1.10 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
Version:       9.18.30
Location:      53/tcp
CPE:           cpe:/a:isc:bind:9.18.30
Concluded from version/product identification result:
9.18.30-0ubuntu0.22.04.2-Ubuntu
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

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: Apache HTTP Server Detection Consolidation

Summary

Consolidation of Apache HTTP Server detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected Apache HTTP Server
Version:       2.4.52
Location:      80/tcp
CPE:           cpe:/a:apache:http_server:2.4.52
Concluded from version/product identification result:
Server: Apache/2.4.52 (Ubuntu)
```

Solution:

Log Method

Details: `Apache HTTP Server Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.117232
Version used: `2024-03-08T15:37:10Z`

References

`url: https://httpd.apache.org`

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.

. . . continues on next page . . .

... continued from previous page ...

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:           Ubuntu
CPE:          cpe:/o:canonical:ubuntu_linux
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/tcp: 9.18.30-0ubuntu0.22.04.2-Ubuntu
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 (vsFTPd 3.0.5)
OS:           Ubuntu 22.04
Version:      22.04
CPE:          cpe:/o:canonical:ubuntu_linux:22.04
Found by VT:  1.3.6.1.4.1.25623.1.0.111067 (Operating System (OS) Detection (HTT
↪P))
Concluded from HTTP Server banner on port 80/tcp: Server: Apache/2.4.52 (Ubuntu)
OS:           Ubuntu
CPE:          cpe:/o:canonical:ubuntu_linux
Found by VT:  1.3.6.1.4.1.25623.1.0.111067 (Operating System (OS) Detection (HTT
↪P))
Concluded from HTTP Server default page on port 80/tcp: <title>Apache2 Ubuntu De
↪fault Page
```

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

... continues on next page ...

. . . continued from previous page . . .

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 (10.0.0.116) to target (10.0.0.112):
10.0.0.116
10.0.0.112
Network distance between scanner and target: 2
```

Solution:

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: Hostname Determination Reporting

Summary

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Hostname determination for IP 10.0.0.112:
Hostname|Source
10.0.0.112|IP-address
```

Solution:

Log Method

Details: `Hostname Determination Reporting`
OID:1.3.6.1.4.1.25623.1.0.108449
Version used: `2022-07-27T10:11:28Z`

[return to 10.0.0.112]

This file was automatically generated.