Check Domain

```
====================================================
[.] Record not found A in domain 'project24.next-step.tn'.
[.] Record not found AAAA in domain 'project24.next-step.tn'.
[+] MX Record : 5 webmail.project24.next-step.tn.
[+] SPF Records:
1) v=spf1
2) mx
3) ipv4 -> ['102.128.60.5']
4) ~all -> 'The SPF record has designated the host as NOT being allowed to
send but is in transition.'
[.] DKIM Record : Selector 'project24' or 'selector1' is not found in the
DNS records. Check DKIM configuration or choose the manual selector option.
[.] DMARC : Record not found in DNS record. Check DKIM configuration.
[.] BIMI Record : Policy not is found in DNS record using selector
'default'. Check BIMI configuration or choose the manual selector option.
```

Spoof

```
---------------------------------- Analyzing project24.next-step.tn ----------------------------------------
[+] SPF is present
[-] This domain hasn't DMARC register
```

WebAuth Bruteforce

```
Failed login for test:123
Failed login for test:5699
Failed login for test:admin
Failed login for test55:123
Failed login for test55:5699
Failed login for test55:admin
Failed login for admin:123
Failed login for admin:5699
Failed login for admin:admin
```

Bruteforce

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-31 20:13:15
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:3/p:3), ~1 try per task
[DATA] attacking smtp://10.9.21.200:25/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-31 20:13:16

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-31 20:13:16
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:3/p:3), ~1 try per task
[DATA] attacking imap://10.9.21.200:143/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-31 20:13:17

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-31 20:13:17
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:3/p:3), ~1 try per task
[DATA] attacking pop3://10.9.21.200:110/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-31 20:13:18
```

Imap/pop3 capabilities

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 20:13 CET
Nmap scan report for 10.9.21.200
Host is up (0.0048s latency).

PORT STATE SERVICE
143/tcp open imap
|_imap-capabilities: OK THREAD=ORDEREDSUBJECT CATENATE BINARY SASL-IR SEARCHRES ACL I18NLEVEL=1
IDLE ID MULTIAPPEND LOGINDISABLEDA0001 STARTTLS QUOTA ENABLE ESORT XLIST WITHIN UNSELECT
UIDPLUS completed LIST-STATUS SORT LIST-EXTENDED QRESYNC NAMESPACE CONDSTORE ESEARCH
RIGHTS=ektx IMAP4rev1 LITERAL+ CHILDREN

Nmap done: 1 IP address (1 host up) scanned in 8.12 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 20:13 CET
Nmap scan report for 10.9.21.200
Host is up (0.00039s latency).

PORT STATE SERVICE
110/tcp filtered pop3

Nmap done: 1 IP address (1 host up) scanned in 8.05 seconds
```

Smtp Enumeration

```
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

----------------------------------------------------------
| Scan Information |
----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... /home/kali/Desktop/web/uploads/users.txt
Target count ............. 1
Username count ........... 3
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............ project24.next-step.tn

######## Scan started at Fri May 31 20:24:35 2024 #########
10.9.21.200: admin@project24.next-step.tn
10.9.21.200: test@project24.next-step.tn
10.9.21.200: test55@project24.next-step.tn
######## Scan completed at Fri May 31 20:24:35 2024 #########
0 results.

3 queries in 1 seconds (3.0 queries / sec)
```

Internal Spoof

```
==================================================
email-spoofer-py v0.0.3 (CLI wizard)
Python 3.x based email spoofer
https://github.com/mikechabot/email-spoofer-py
==================================================

Connecting to SMTP socket (10.9.21.200:587)...
Starting TLS session...
Authentication successful
Sending spoofed message...
Message sent!
```

Open Relay

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 20:24 CET
Nmap scan report for 10.9.21.200
Host is up (0.24s latency).

PORT STATE SERVICE
25/tcp open smtp
|_smtp-open-relay: Server doesn't seem to be an open relay, all tests failed
```

```
465/tcp open smtps
|_smtp-open-relay: Server doesn't seem to be an open relay, all tests failed
587/tcp open submission
|_smtp-open-relay: Server doesn't seem to be an open relay, all tests failed

Nmap done: 1 IP address (1 host up) scanned in 38.90 seconds
```

Scan Report

May 31, 2024

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 “project24.next-step.tn”. The scan started at Fri May 31 19:14:05 2024 UTC and ended at Fri May 31 19:24:30 2024 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
10.9.21.200	1	1	0	8	0
Total: 1	1	1	0	8	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 20 results selected by the filtering described above. Before filtering there were 22 results.

2 Results per Host

2.1 10.9.21.200

Host scan start	Fri May 31 19:14:41 2024 UTC
Host scan end	Fri May 31 19:24:25 2024 UTC

Service (Port)	Threat Level
general/tcp	High
25/tcp	Medium
general/CPE-T	Log
general/tcp	Log
25/tcp	Log

2.1.1 High general/tcp

High (CVSS: 10.0)

NVT: Report outdated / end-of-life Scan Engine / Environment (local)

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

This script checks and reports an outdated or end-of-life scan engine for the following environments:
- Greenbone Community Edition
- Greenbone Enterprise TRIAL (formerly Greenbone Security Manager TRIAL / Greenbone Community Edition VM)

used for this scan.

NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the target due to e.g.:
- missing functionalities
- missing bugfixes
- incompatibilities within the feed

Quality of Detection: 97

Vulnerability Detection Result

```
Version of installed component:          22.7.9 (Installed component: openvas-l
↪ibraries on OpenVAS <= 9, openvas-scanner on Greenbone Community Edition >= 10
↪)
Latest available openvas-scanner version: 23.0.1
Reference URL(s) for the latest available version: https://forum.greenbone.net/t
↪/greenbone-community-edition-22-4-stable-initial-release-2022-07-25/12638
```

Solution:

Solution type: VendorFix

Update to the latest available stable release for your scan environment. Please check the references for more information. If you're using packages provided by your Linux distribution please contact the maintainer of the used distribution / repository and request updated packages.

If you want to accept the risk of a possible decreased scan coverage or missing detection of vulnerabilities on the target you can set a global override for this script as described in the linked GSM manual.

Vulnerability Detection Method

Details: `Report outdated / end-of-life Scan Engine / Environment (local)`

OID:1.3.6.1.4.1.25623.1.0.108560

Version used: `2024-05-17T15:38:33Z`

References

```
url: https://www.greenbone.net/en/testnow/
url: https://forum.greenbone.net/t/greenbone-community-edition-22-4-stable-initi
↪al-release-2022-07-25/12638
url: https://forum.greenbone.net/t/greenbone-community-edition-21-04-end-of-life
↪/13837
url: https://forum.greenbone.net/t/gvm-21-04-end-of-life-initial-release-2021-04
↪-16/8942
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://forum.greenbone.net/t/gvm-20-08-end-of-life-initial-release-2020-08
↪-12/6312
url: https://forum.greenbone.net/t/gvm-11-end-of-life-initial-release-2019-10-14
↪/3674
url: https://forum.greenbone.net/t/gvm-10-end-of-life-initial-release-2019-04-05
↪/208
url: https://forum.greenbone.net/t/gvm-9-end-of-life-initial-release-2017-03-07/
↪211
url: https://docs.greenbone.net/GSM-Manual/gos-22.04/en/reports.html#creating-an
↪-override
```

[return to 10.9.21.200]

2.1.2 Medium 25/tcp

Medium (CVSS: 4.8)

NVT: SMTP Unencrypted Cleartext Login

Summary
The remote host is running a SMTP server that allows cleartext logins over unencrypted connections.

Quality of Detection: 70

Vulnerability Detection Result

```
The remote SMTP server accepts logins via the following cleartext authentication
↪ mechanisms over unencrypted connections:
LOGIN
PLAIN
The remote SMTP server supports the 'STARTTLS' command but isn't enforcing the u
↪se of it for the cleartext authentication mechanisms.
```

Impact
An attacker can uncover login names and passwords by sniffing traffic to the SMTP server.

Solution:
Solution type: Mitigation
Enable SMTPS or enforce the connection via the 'STARTTLS' command. Please see the manual of the SMTP server for more information.

Vulnerability Detection Method
Evaluates from previously collected info if a non SMTPS enabled SMTP server is providing the 'PLAIN' or 'LOGIN' authentication methods without sending the 'STARTTLS' command first.

. . . continues on next page . . .

... continued from previous page ...

Details: `SMTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108530
Version used: `2023-10-13T05:06:09Z`

[return to 10.9.21.200]

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

```
10.9.21.200|cpe:/a:postfix:postfix
10.9.21.200|cpe:/h:hp:jetdirect
```

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 10.9.21.200]

2.1.4 Log general/tcp

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: 80

Vulnerability Detection Result

```
Hostname determination for IP 10.9.21.200:
Hostname|Source
10.9.21.200|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`

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:           HP JetDirect
CPE:          cpe:/h:hp:jetdirect
Found by VT:  1.3.6.1.4.1.25623.1.0.102002 (Operating System (OS) Detection (ICM
↪P))
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Log Method
Details: `OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: `2024-05-16T05:05:35Z`

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

Log (CVSS: 0.0)

NVT: SSL/TLS: Hostname discovery from server certificate

Summary
It was possible to discover an additional hostname of this server from its certificate Common or Subject Alt Name.

Quality of Detection: 98

Vulnerability Detection Result

```
The following additional but not resolvable hostnames were detected:
mail.pfe2024-amen.nextstep-it.com
```

Solution:

Log Method
Details: `SSL/TLS: Hostname discovery from server certificate`
OID:1.3.6.1.4.1.25623.1.0.111010
Version used: `2021-11-22T15:32:39Z`

[return to 10.9.21.200]

2.1.5 Log 25/tcp

Log (CVSS: 0.0)

NVT: Postfix SMTP Server Detection (SMTP)

Summary
SMTP based detection of Postfix.

. . . continues on next page . . .

. . . continued from previous page . . .

Quality of Detection: 80

Vulnerability Detection Result

```
Detected Postfix
Version:       unknown
Location:      25/tcp
CPE:           cpe:/a:postfix:postfix
Concluded from version/product identification result:
220 mail.pfe2024-amen.nextstep-it.com ESMTP Postfix
```

Solution:

Log Method

Details: `Postfix SMTP Server Detection (SMTP)`
OID:1.3.6.1.4.1.25623.1.0.111086
Version used: `2024-01-12T05:05:56Z`

References

url: `https://www.postfix.org/`

Log (CVSS: 0.0)

NVT: Services

Summary

This plugin performs service detection.

Quality of Detection: 80

Vulnerability Detection Result

```
An SMTP server is running on this port
Here is its banner :
220 mail.pfe2024-amen.nextstep-it.com ESMTP Postfix
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2023-06-14T05:05:19Z

Log (CVSS: 0.0)

NVT: SMTP Server type and version

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

Quality of Detection: 80

Vulnerability Detection Result

```
Remote SMTP server banner:
220 mail.pfe2024-amen.nextstep-it.com ESMTP Postfix
The remote SMTP server is announcing the following available ESMTP commands (EHL
↪O response) via an unencrypted connection:
8BITMIME, AUTH LOGIN PLAIN, AUTH=LOGIN PLAIN, CHUNKING, DSN, ENHANCEDSTATUSCODES
↪, ETRN, PIPELINING, SIZE 10240000, STARTTLS, VRFY
```

Solution:

Log Method
Details: SMTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10263
Version used: 2024-02-02T14:37:52Z

Log (CVSS: 0.0)

NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Quality of Detection: 98

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)             | 554B7666A30267BFCD568D3DD3309DB0E068F63E
fingerprint (SHA-256)           | CE0C76736376AB44290EA5D72C881A512BA89221016D66
↪EC0C8B0F6B231C4985
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
issued by                       | CN=mail.pfe2024-amen.nextstep-it.com,OU=Zimbra
↪ Collaboration Server,O=CA
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 1709042147
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=mail.pfe2024-amen.nextstep-it.com,OU=Zimbra
↪ Collaboration Server
subject alternative names (SAN) | mail.pfe2024-amen.nextstep-it.com
valid from                      | 2024-02-27 13:55:52 UTC
valid until                     | 2029-02-25 13:55:52 UTC
```

Solution:

Log Method

Details: `SSL/TLS: Collect and Report Certificate Details`
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: `2023-02-17T10:19:33Z`

[return to 10.9.21.200]

This file was automatically generated.