Check Domain

```
==================================================
[.] Record not found A in domain 'pfe2024-amen.nextstep-it.com'.
[.] Record not found AAAA in domain 'pfe2024-amen.nextstep-it.com'.
[.] Record not found MX in domain 'pfe2024-amen.nextstep-it.com'.
[.] Record not found TXT in domain 'pfe2024-amen.nextstep-it.com'.
[.] DKIM Record : Selector 'pfe2024-amen' 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 pfe2024-amen.nextstep-it.com ----------------------------------------
[-] This domain hasn't SPF config yet
[-] This domain hasn't DMARC register
[!] You can spoof this domain!
[+] Email sended successfully as test@pfe2024-amen.nextstep-it.com
```

WebAuth Bruteforce

```
Failed login for test1:123
Failed login for test1:156
Failed login for test1:admin
Failed login for test2:123
Failed login for test2:156
Failed login for test2:admin
Failed login for admin:123
Failed login for admin:156
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 19:22:39
[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 19:22:41

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 19:22:41
[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 19:22:42

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 19:22:42
[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 19:22:43
```

Imap/pop3 capabilities

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 19:22 CET
Nmap scan report for 10.9.21.200
Host is up (0.019s latency).
```

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

Nmap done: 1 IP address (1 host up) scanned in 8.30 seconds
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-31 19:22 CET
Nmap scan report for 10.9.21.200
Host is up (0.0051s latency).

PORT STATE SERVICE
110/tcp open pop3
|_pop3-capabilities: XOIP SASL(PLAIN) EXPIRE(31 USER) STLS UIDL TOP

Nmap done: 1 IP address (1 host up) scanned in 8.09 seconds

Openvas

Failed to execute: Response Error 400. Target exists already.

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 pfe2024-amen.nextstep-it.com

######## Scan started at Fri May 31 19:23:00 2024 #########
10.9.21.200: admin@pfe2024-amen.nextstep-it.com exists
10.9.21.200: test1@pfe2024-amen.nextstep-it.com
10.9.21.200: test2@pfe2024-amen.nextstep-it.com
######## Scan completed at Fri May 31 19:23:01 2024 #########
1 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 19:23 CET
Nmap scan report for 10.9.21.200
Host is up (0.11s 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 31.63 seconds