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 ttt:123
Failed login for ttt:fafani123
Failed login for admin:123
Login successful!!
Valid Credentials:
admin : fafani123

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 2024-05-27 00:23:01
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:2/p:2), ~1 try per task
[DATA] attacking smtp://10.9.21.200:25/
[25][smtp] host: 10.9.21.200 login: admin password: fafani123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-27 00:23:02

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 2024-05-27 00:23:02
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:2/p:2), ~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 2024-05-27 00:23:03

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 2024-05-27 00:23:03
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:2/p:2), ~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 2024-05-27 00:23:04

Imap/pop3 capabilities

Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-27 00:23 CET
Nmap scan report for 10.9.21.200
Host is up (0.00042s latency).

PORT STATE SERVICE

143/tcp filtered imap

Nmap done: 1 IP address (1 host up) scanned in 8.21 seconds
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-27 00:23 CET
Nmap scan report for 10.9.21.200
Host is up (0.0054s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 7.94 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 2
Target TCP port 25
Query timeout ..... 5 secs
Target domain 10.9.21.200

######## Scan started at Mon May 27 00:32:10 2024 #########
pfe2024-amen.nextstep-it.com: admin@10.9.21.200
pfe2024-amen.nextstep-it.com: ttt@10.9.21.200
######## Scan completed at Mon May 27 00:32:10 2024 #########
0 results.

2 queries in 1 seconds (2.0 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 2024-05-27 00:32 CET
Nmap scan report for 10.9.21.200
Host is up (0.012s 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 29.74 seconds