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