Hacking Windows XP

Pablo Andres Balbuena Rios

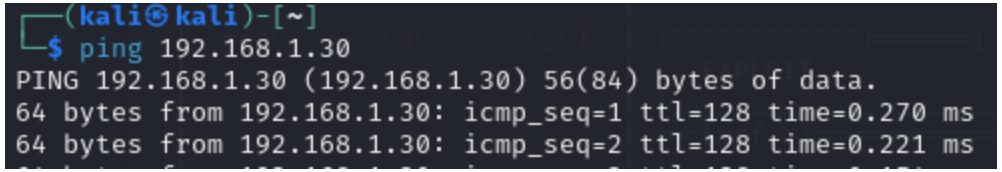
Esercizio 3 Settimana 7

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).

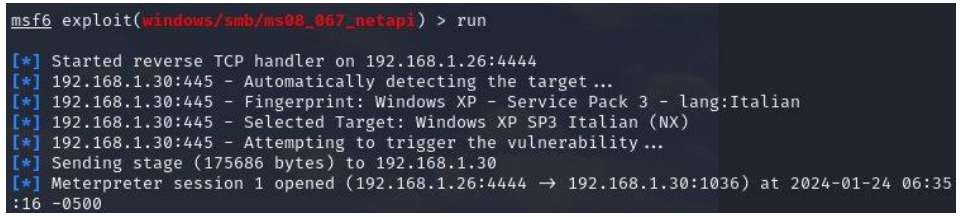
Scansione della Macchina Metasploitable2

- Prima di fare la scansione, si deve fare un Ping per vedere se c'è connessione tre le due macchine
- Poi attraverso Nmap, andiamo a vedere se vi sono vulnerabilità sulle porte aperte.



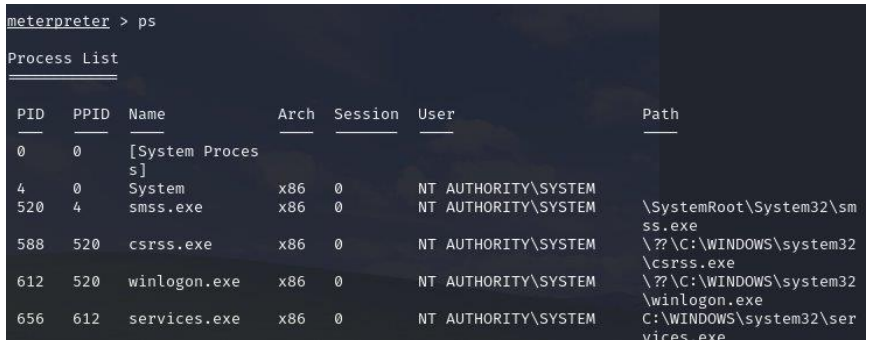
Vulnerability ms08-067

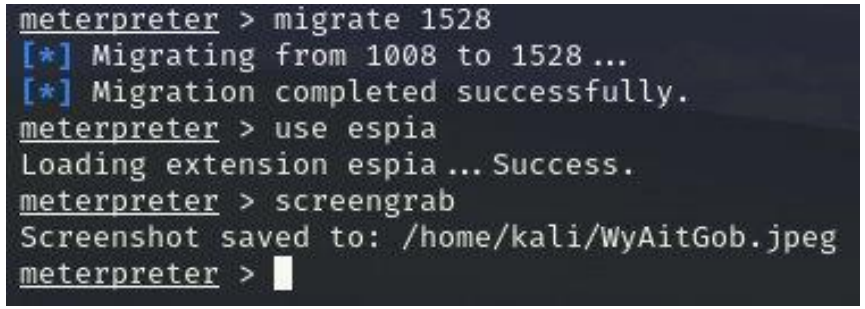
- Attraverso Metasploit proviamo a cercare l' exploit "search ms08-067".
- Dopo averlo trovato, andiamo a settare le impostazioni, cioè rhosts attraverso il comando "set rhosts 192.168.1.30", e facciamo partire metasploit con "run".



Entrare in Windows

- Attraverso Metasploit entriamo a Windows con Meterpreter.
- La prima cosa da fare è il mantenimento, cioè, mantenere l'accesso non autorizzato o a sfruttare ulteriormente la presenza nel sistema senza essere rilevati.
- Fare il mantenimento dobbiamo aprire la lista dei file in esecuzione e traferirci in uno molto più importante.





Screenshot e Webcam

- Prima di eseguire i comandi, dobbiamo eseguire la estensione "spia", attraverso il comando "use spia", che ci permettere di eseguire molti comandi.
- Attraverso il commando "screengrab", possiamo fare uno Screenshot alla finestra Desktop.
- Attraverso il commando "webcam_list", possiamo vedere tutte le webcam che sono disponibile nel pc bersaglio.


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