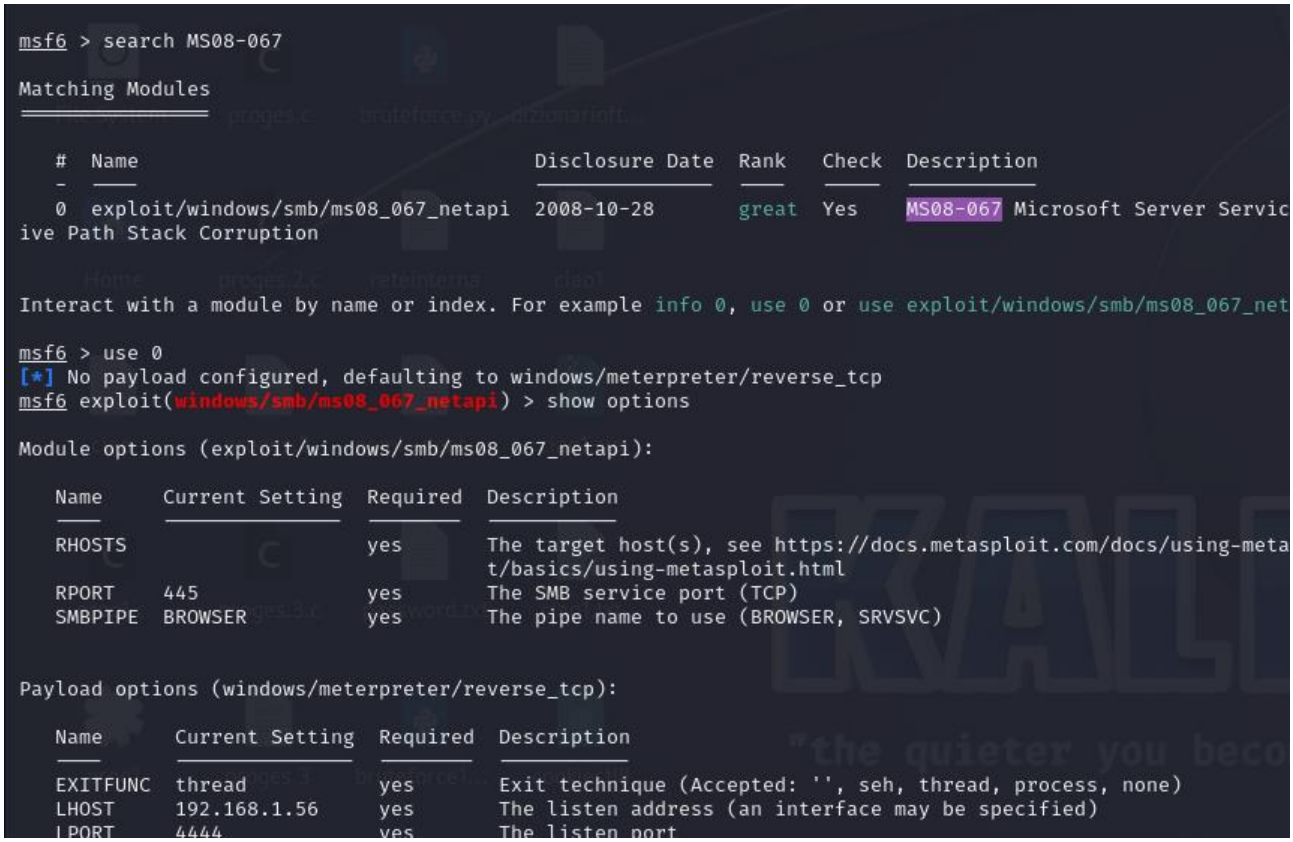
Oggi mi viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, si dovrà recuperare uno screenshot tramite la sessione Meterpreter.

Prima di fare tutto, ho verificato che la mia macchina e Windows XP pingassero.

Per prima cosa avvio metasploit sul terminale root di Kali con il comando “msfconsole”. Successivamente cercherò la vulnerabilita richiesta, con il comando “search” + nome vulnerabilità. Seleziono l’exploit che mi interessa (numero 0). Verrà usato il payload di default. Digito show option per vedere se ci sono settaggi da configurare. Noto che viene richiesto di inserire l’ip del dispositivo vittima.

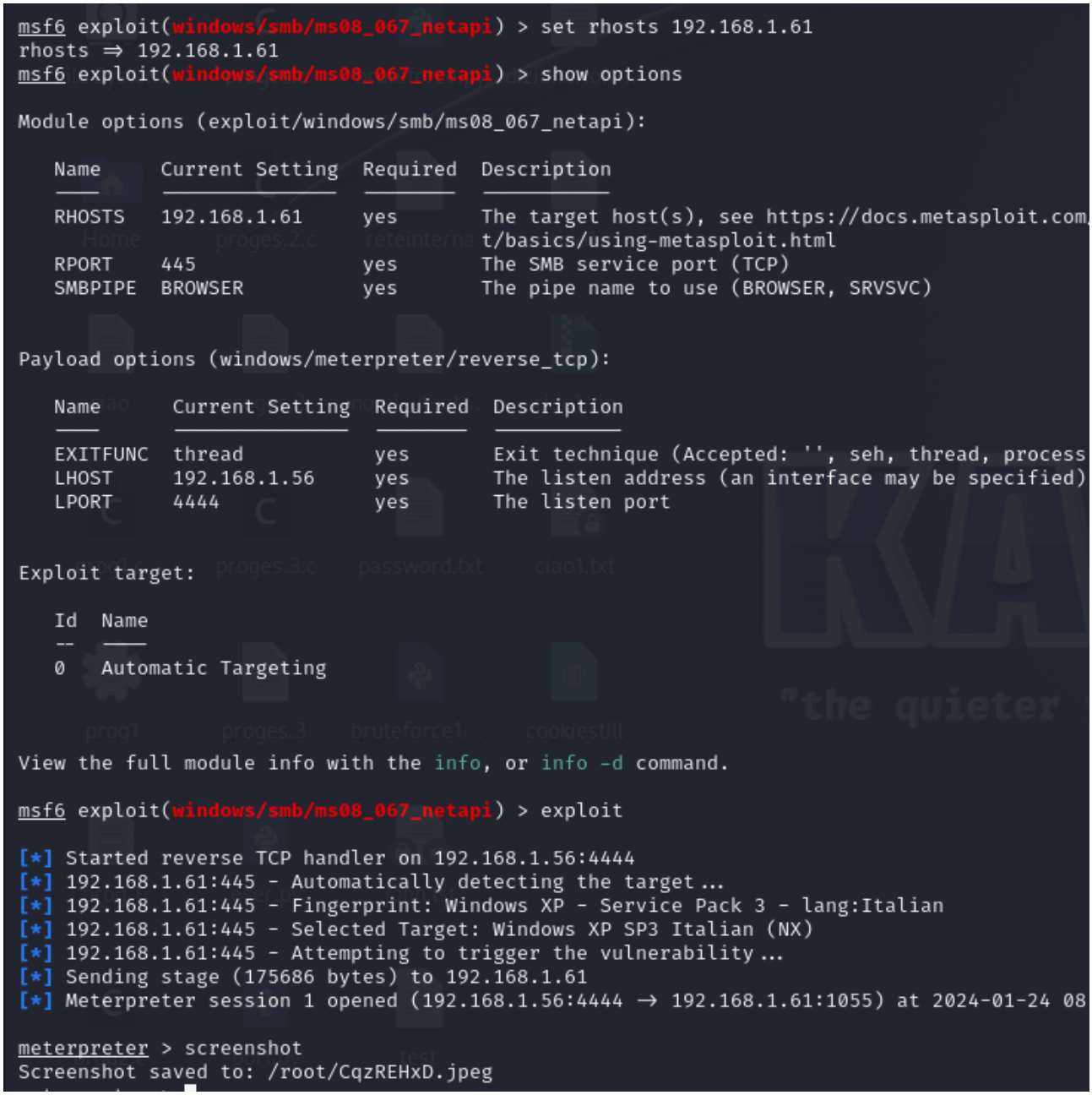


Inserisco l'ip del dispositivo vittima, e ricontrollo le opzioni per vedere che l'abbia preso correttamente.

Dopodichè posso lanciare l'attacco con il comando exploit.

La shell è stata creata, ora sono dentro il dispositivo vittima.

Con la sessione Meterpreter appena aperta, acquisisco uno screenshot del display della macchina vittima, con il comando "screenshot". Lo screenshot è stato salvato nella directory "/root".



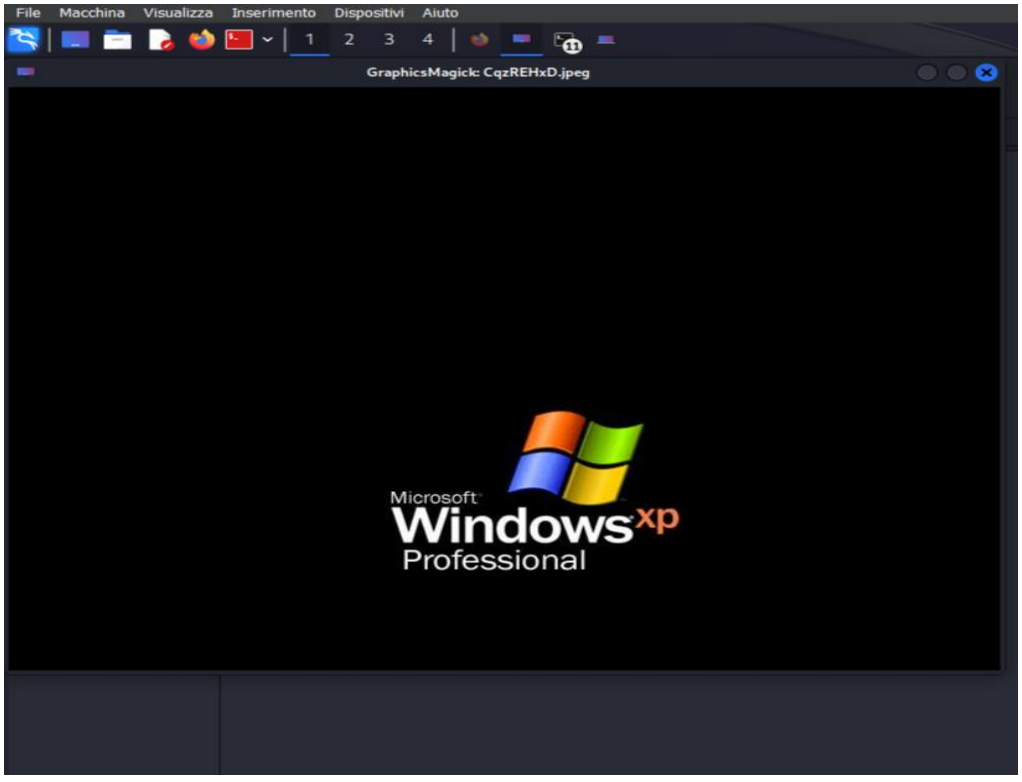
Per visualizzare lo screenshot appena acquisito, apro un nuovo terminale root. Digitanto “ls” mi viene mostrata l’immagine appena salvata. Digitanto “diplay” + nome dell’immagine, il terminale mi fa capire che il comando display non è stato ancora installato, allora lo installo con “apt install graphicsmagick-imagemagick-compat”.

```
┌──(root㉿kali)-[~]
└─# ls
CqzREHxD.jpeg

┌──(root㉿kali)-[~]
└─# display  CqzREHxD.jpeg
Command 'display' not found, but can be installed with:
apt install graphicsmagick-imagemagick-compat
Do you want to install it? (N/y)y
apt install graphicsmagick-imagemagick-compat
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  graphicsmagick libgraphicsmagick-q16-3 libsharpyuv0 libwebp7 libw
Suggested packages:
  graphicsmagick-dbg
The following NEW packages will be installed:
  graphicsmagick graphicsmagick-imagemagick-compat libgraphicsmagic
The following packages will be upgraded:
  libwebp7 libwebpdemux2 libwebpmux3
3 upgraded, 4 newly installed, 0 to remove and 1471 not upgraded.
Need to get 2,937 kB of archives.
```

Successivamente, digitando nuovamente il comando “display” + nome dell’immagine, notiamo come ora ci prenderà il comando, e ci renderà visibile lo screeshot effettuato precedentemente.

```
┌──(root㉿kali)-[~]
└─# display  CqzREHxD.jpeg
```



Per vedere se è presente o meno la Webcam sulla macchina vittima, basta cercare di acquisire un'immagine istantanea della webcam con il comando "webcam_snap". Nel mio caso mi è stato risposto che la vittima non ha nessuna webcam.