

# WiFi Pineapple



PITM: Pineapple in the middle.

# Resumen

En este documento se presentan algunas fallas que da lugar a mecanismos de hacking, una demostración de la forma en que funcionan, probada en un ambiente controlado, junto a recomendaciones para evitar ser víctima de estos procedimientos.

# Introducción

Como usuarios de internet  
estamos expuestos a una  
diversa cantidad de  
amenazas.



Ilustración 1



Ilustración 2

En una red encontraremos usuarios maliciosos, hackers, que intentaran acceder a nuestra información tomando ventaja de alguna vulnerabilidad en la red.

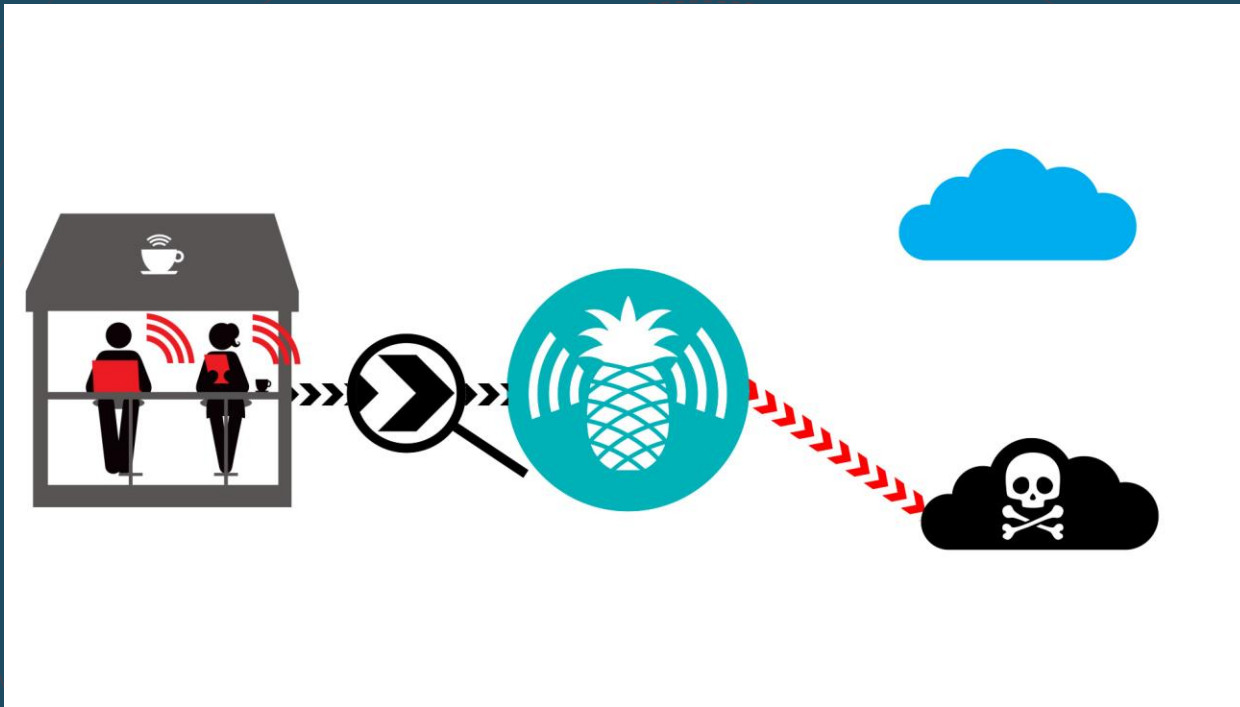


Ilustración 3

Se define PITM como un mecanismo que establece un Rogue AP (Rogue access point) brindando una conexión a usuarios para interceptar la información que estos envían.

Usado junto a un WiFi deauthentication attack presenta una gran oportunidad para engañar usuarios de otro AP.

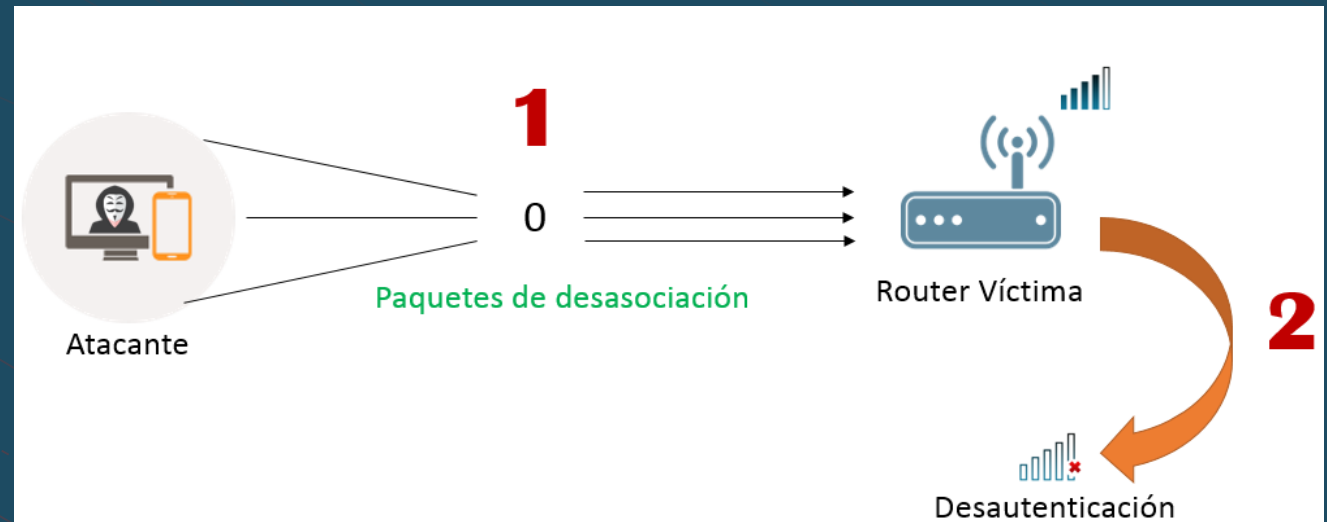


Ilustración 4

Por ejemplo, desconectar a los usuarios de una oficina para hacer que se conecten automáticamente a nuestro Rogue AP.

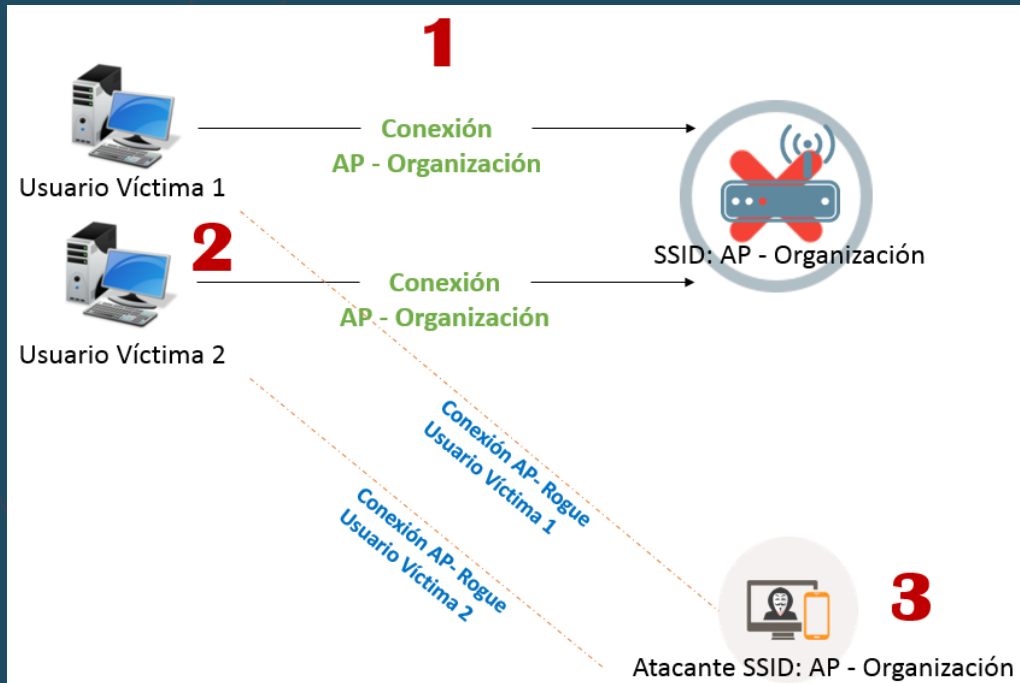


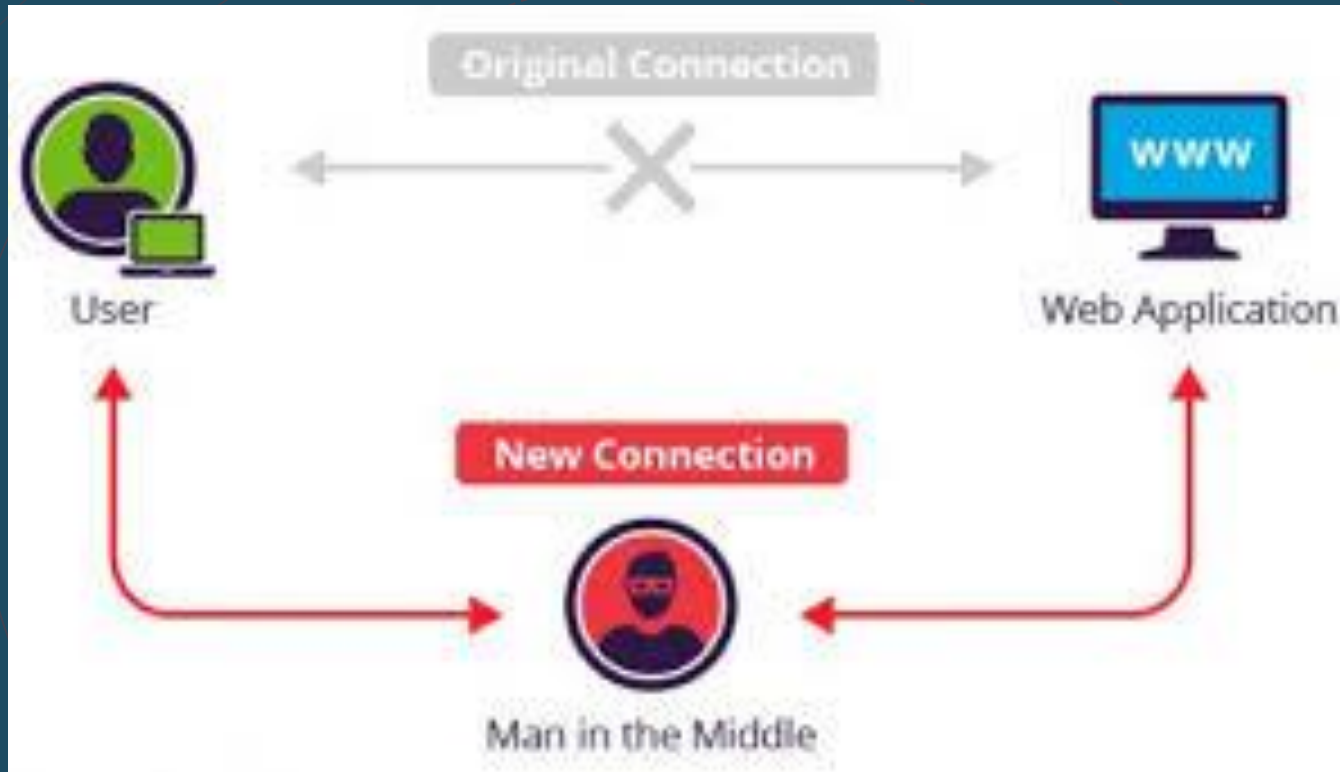
Ilustración 5



Una red WiFi, generalmente desplegada en contextos personales y profesionales, presenta fallos que pueden afectar la integridad y confidencialidad de la información.

Debido a la gran importancia de la información en la actualidad, es necesario tener contramedidas para defenderse de usuarios malintencionados, hackers.

# Hipótesis



Existen metodos para evitar un ataque PITM.

Ilustración 6



# Objetivos

## Alcanzables

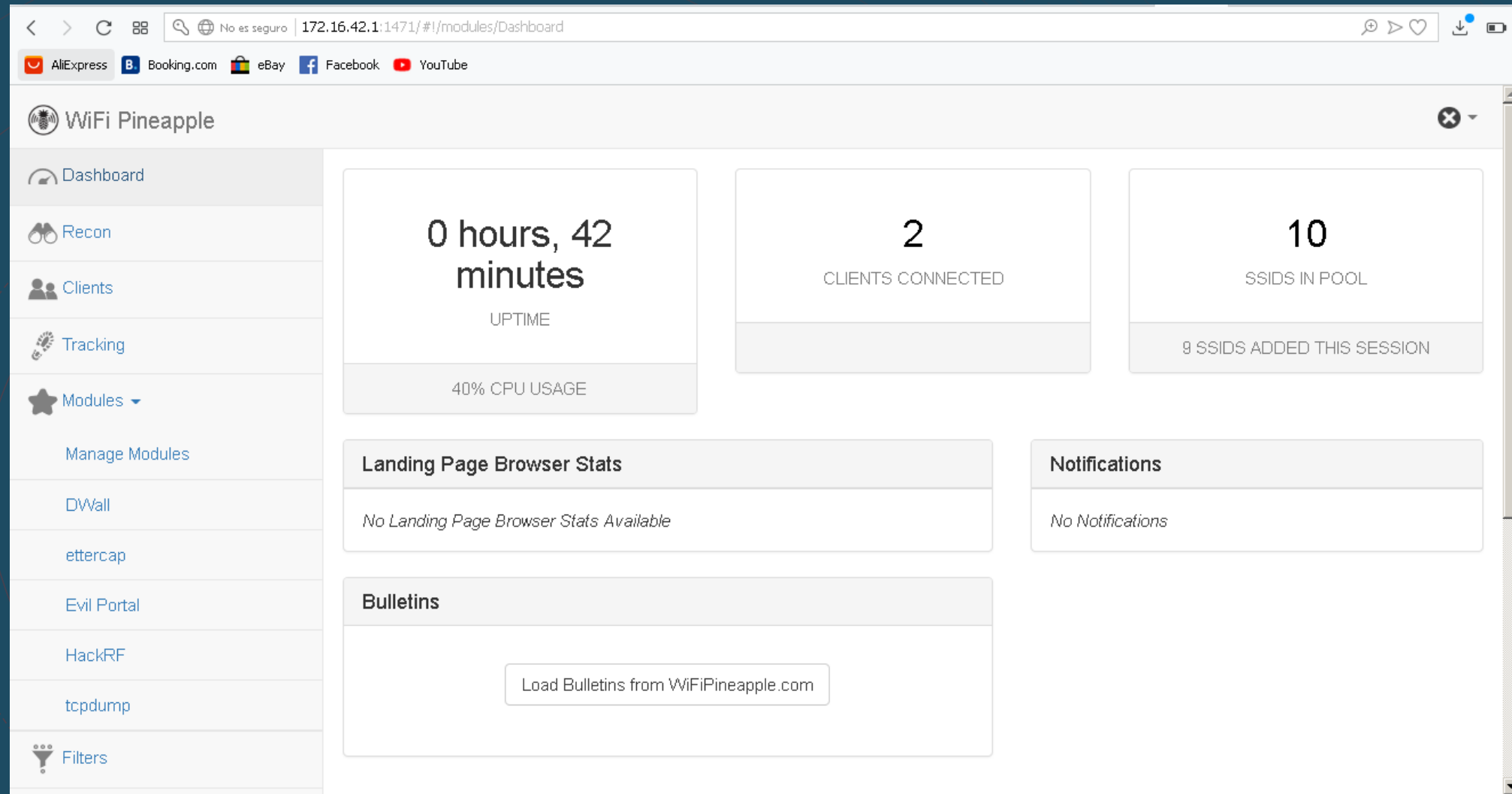
Establecer un AP-Rogue en un ambiente controlado.

Determinar medidas contra ataques PITM.

## No alcanzables

Establecer un ataque PITM en un ambiente comun, no controlado.

# Resultados



# Resultados

No es seguro

172.16.42.1:1471/#!/modules/Clients

AliExpress

Booking.com

eBay

Facebook

YouTube

WiFi Pineapple

Dashboard

Recon

Clients

Tracking

Modules

Clients

Refresh

MAC Address	IP Address	SSID	Hostname	Kick Client
<div></div> <div></div>	172.16.42.146	<div></div> Open Network	D021E18	<div>Kick</div>
<div></div> <div></div>	172.16.42.133	<div></div> emcali	mglrorsa-K401UQ	<div>Kick</div>

Clientes conectados en  
escenario preparado

# Resultados

WiFi Pineapple

Dashboard Recon Clients Tracking Modules Manage Modules DWall ettercap Evil Portal HackRF tcpdump Filters

DWall Settings


DWall is currently running.

Disable Stop Listening

URLs

Client	URL
172.16.42.148	http://pubmatic-cm.p.veruta.com/adserver/cookie...
172.16.42.148	http://ads.stickyadstv.com/user-registering?dataProvi...
172.16.42.148	http://ads.stickyadstv.com/user-registering?dataProvi...
172.16.42.148	http://ads.stickyadstv.com/user-registering?dataProvi...
172.16.42.148	http://pixel.tapad.com/idsync/ex/receive?partner_id=20...
172.16.42.148	http://d5p.de17a.com/getuid/stickyads?
172.16.42.148	http://odr.mookie1.com/tv2/sync?tagid=V2_2739&src...

Images



Trafico  
capturado en  
pagina no  
segura

# Resultados






View History - November 23 2018 21:36:36

```
Rq _t
4!<@
GET /cgi-olib?infile=user.glu&auth_this=y&style=user HTTP/1.1
Host: biblioteca2.
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://biblioteca2./cgi-olib?infile=reset.glue&style=reset
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: _ga=GA1.3.1590737981.1539386901; ezproxy=xAnwX4r7ouNBMDY; cX_S=jor9dpwvg8oauc5i; cX_P=jor9dpwxwzwnpxep; cX_G
40m@
extension-updates.opera.com
http/1.1
```

Close

Detalles del  
trafico  
de pagina no  
segura

# Resultados

 Dashboard	<div>Clients <span>Refresh</span></div>				
 Recon					
 Clients					
 Tracking					
 Modules ▾					
Manage Modules					
DWall					
ettercap					

MAC Address	IP Address	SSID	Hostname	Kick Client
<input type="checkbox"/> [REDACTED]	172.16.42.148	<input type="checkbox"/> emcali	android-5e0a3ad3a1d793fa	<input type="button" value="Kick"/>
<input type="checkbox"/> [REDACTED]	172.16.42.133	<input type="checkbox"/> publica	mglrorsa-K401UQ	<input type="button" value="Kick"/>
<input type="checkbox"/> [REDACTED]	172.16.42.113	<input type="checkbox"/> PUBLICA	iPhonedancamilo	<input type="button" value="Kick"/>
<input type="checkbox"/> [REDACTED]	No IP	No SSID	No Hostname	<input type="button" value="Kick"/>
<input type="checkbox"/> [REDACTED]	No IP	No SSID	No Hostname	<input type="button" value="Kick"/>

Cierre del escenario  
preparado



# Conclusiones

## Contramedidas recomendadas:

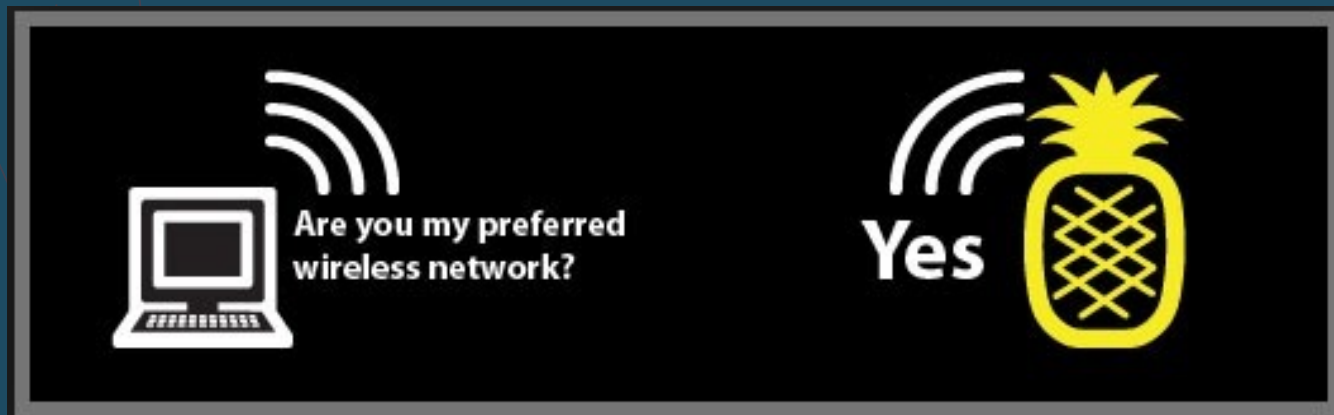
- ☐ Tener en cuenta desde el puesto de trabajo del usuario las redes inalámbricas existentes en la organización.



# Conclusiones

## Contramedidas recomendadas:

- ❑ No recordar las redes inalámbricas y no seleccionar la opción de conectarse automáticamente a dicha red.



SSID Pool

Refresh

Open Network  
PUBLICA  
PUBLICO  
ICESI-ADMIN  
WWWcalix  
emcali  
WiFi\_j2t\_P

SSID

Add

Remove

Pool Location

/etc/pineapple/

Save

# Conclusiones

## Contramedidas recomendadas:

- Tener como norma nunca conectar a una red abierta, Pineapple genera las redes inalámbricas abiertas para que sus víctimas sean engañadas con facilidad.



# Trabajo a futuro.

El trabajo adicional o a futuro comprenderá tres actividades a realizar b, en primer lugar, realizar un WiFi deauthentication attack para desconectar a

# Referencias

1. Quintero Tamayo, J. *Hardware malicioso como herramienta de Pentesting orientado al puesto de trabajo*. España, Enero, 2016.
2. C. Claire, X. Martin, J. F. Jean-David and P. Louis. Pineapple, Raspberry and WiFi. WiFi Man-in-the-Middle attacks.
3. E. Oliver, K. Philipp and T. Paul, Detection of Man-in-the-Middle Attacks on Industrial Control Networks.

# Ilustraciones

1. <https://pixabay.com/en/target-group-advertising-buyer-3460039/>
2. <https://pixabay.com/en/phishing-fraud-cyber-security-3390518/>
3. <https://www.hak5.org/wp-content/uploads/2015/01/pineap.jpg>
- 4,5. Quintero Tamayo, J. *Hardware malicioso como herramienta de Pentesting orientado al puesto de trabajo*. España, Enero, 2016.
6. <https://securityhacklabs.net/sites/default/files/styles/large/public/2018-04/14.png?itok=xmtH1NNO>