ROGUE AP WIFI

LOS RIESGOS DE CONEECTARSE A REDES WIFI DESCONOCIDAS

PRESENTADO POR

Felipe Marquez

Josué Sandoval

Christopher Silva

CONTEXTO DEL PROBLEMA

- *WiFI A.P levantados en lugares concurridos.*
- *Métodos débiles de autenticación (o incluso nulos).*
- *Poco conocimiento sobre protocolos de seguridad.*

IMPLEMENTACIÓN ROGUE AP

¿QUE SUCEDE EN TIEMPO REAL?

#1
Victima se conecta al WiFi falso

#2
Redireccionamiento a falso inicio de sesion

#3
Vista falsa de un inicio de sesión

#4
Víctima escribe sus credenciales

POV DE LA VICTIMA

CUIDADO CON
LOS SMS

Llega SMS con factor a victima

Víctima escribe el SMS en la página falsa

Atacante obtiene acceso total a la cuenta

RESULTADOS

Conexión establecida

Se espera que la víctima caiga en el truco del falso AP, además de que esta conexión debe ser percibida por el atacante.

1

Continuidad de sesión

Se espera que la víctima navege de manera natural a través del flujo establecido dentro de la página.

2

Robo de credenciales

Se espera obtener las credenciales y acceso total al correo USM de la victima.

3

CONCLUSIONES

- *Como grupo queremos concientizar a los usuarios de los peligros que conlleva conectarse a un AP desconocido. Demostrando como información personal importante puede ser robada, sin siquiera saber que fueron vulnerados.*
- *Es relativamente sencillo levantar un WiFI AP falso. Su fuerte está en la capacidad del atacante para adaptarse al entorno elegido para el ataque .*
- *El ataque puede tener consecuencias graves para la confidencialidad de las victimas.*