Rogue AP WiFi: los peligros de conectarse a redes WiFi desconocidas

Informe Proyecto

Seguridad en Redes de Computadores TEL-312

Autores : Josue Sandoval
josue.sandoval@sansano.usm.cl
Felipe Marquez
felipe.marquez@sansano.usm.cl
Christopher Silva
christopher.silva@sansano.usm.cl

Profesor : Berioska Contreras

Fecha : 6 de julio de 2023

Índice

Índice de figuras

1. Resumen

En este proyecto, se trabajará con uno de los riesgos más significiativos a la hora de conectarse a una red WiFi externa: los Rogue AP. Se busca verificar su capacidad de ataque, la complejidad de estos, sus puntos débiles y fuertes. El objetivo principal de esta labor es concientizar a los usuarios acerca de la fragilidad de sus credenciales y sobre los peligros de conectarse redes WiFi externas sin verificar la legitimidad de estas.

Como experimento, en un ambiente simulado compuesto por dos máquinas virtuales, se replica un Access Point similar a la red Alumnos-USM de la Universidad Técnica Federico Santa María, a la vez que se implementa una página web falsa a la cual se redireccionara la víctima cuando intente conectarse, donde se llevara a cabo el robo de credenciales. De este experimento se obtienen las credenciales ingresadas en la falsa página web desde la otra máquina virtual por la víctima, consolidando el robo de datos.

2. Introducción

Actualmente, se vive en la época dónde la conectividad global es vital para el desempeño diario en diversas áreas de la vida para las personas. Ya sea para buscar algún dato curioso en tiempos de ocio, alguna receta para cocinar al almuerzo, o buscar investigaciones sobre temas en áreas poco exploradas del conocimiento humano, la conexión a internet es vital para mantener el ritmo de vida actual.

Sin embargo, el mismo avance tan rápido de las redes que proveen conexión a internet también implica un crecimiento en el famoso "hacktivismo". De hecho, en 2017 en la National Vulnerability Database (NVD) se registraron 7744 entradas, mientras que en el 2021 (post-pandemia) se registraon 154370 entradas, es decir, que en 4 años la cantidad de ataques aumento casi 20 veces.

Es claro que existe un aumento en la cantidad de ataques, pero también en la creatividad de estos. No solo se aplica conocimientos ténicos, sino que también se aplica ïngenieria socialz otros métodos que permiten engañar a un indivuo con el fin de extraerle información o provocarle algún daño por el robo de datos.

Es en este contexto que surge el Rogue AP: levantar un falso punto de acceso WiFi con un nombre engañoso (dependiendo del lugar dónde se encuentre la víctima) tal que la víctima se conecte a este y así, engañado por la creencia de que está entrando a una red WiFi .ºficial", ingrese datos que son percibidos y robados por el atacante. En este trabajo se investigará tal método para implementarlo en un ambiente virtual y, concluir sobre su efectividad, peligro y como prevenirlo.

3. Métodos

Para realizar este experimento se utilzaran 2 maquinas virtuales, una atacante donde se levantara el Rogue AP y una victima, la cual realizara un conexión con este e interactuara con la pagina web a la cual sera redireccionada.

Dado que se trata de un ambiente virtual, la conexión se realizará mediante un puente entre ambas máquinas (Lo cual equivale a una conexión cableada en la vida real), sin embargo, en práctica la conexión de las maquinas se realiza en una tarjeta WiFi.

3.1. Atacante

Para levantar un Access Point se utilizo un script de código abierto [2] , el cual mediante distintos comandos en una terminal Linux utiliza una tarjeta de red disponible dentro de la computadora para montar un Access Point falso. Para esto es necesario introducir el canal en el cual se implementa el Access Point y el nombre de este, en este caso se utilizará el nombre de "wiFiAP".

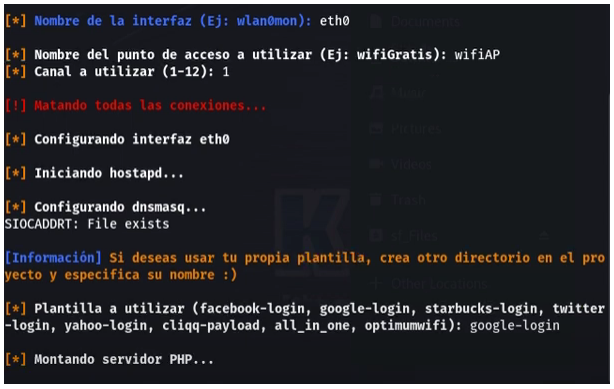


Figura 1: Levantamiento del Rogue AP: Nombre Red y elección de plantilla para servidor PHP falso

En la dirección de este Access Point se levanta un servidor PHP donde se implementa una página web falsa, la cual contiene a su vez sub-servicios que registran los datos ingresados por el usuario en un documento de texto plano. El usuario sera redireccionado a esta página falsa cuando intente conectarse al Rogue AP.

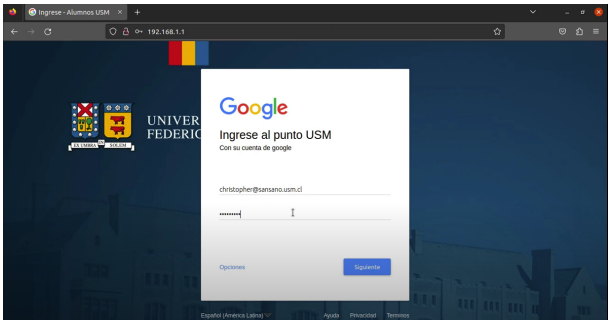
Una vez operativa la pagina web y el AP, el atacante intentara hacer ingreso a la cuenta ingresada por la victima en simultaneo. Es necesario realizar este ataque en simultaneo para poder bypasear el factor de atutenticación de la cuenta si esta la posee.

3.2. Víctima

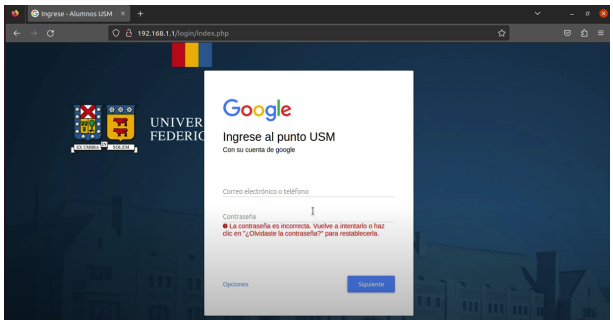
Al momento de realizar la conexión la victima sera redirigida a un sitio web, el cual aparenta ser el un ingreso de sesión de Google habilitado por la UTFSM, el cual solicita al usuario hacer ingreso de sus credenciales universitarias.

Una vez la víctima ingresa sus credenciales, la página web redirecciona a un fallo de ingreso de contraseña, esto se hace por dos razones:

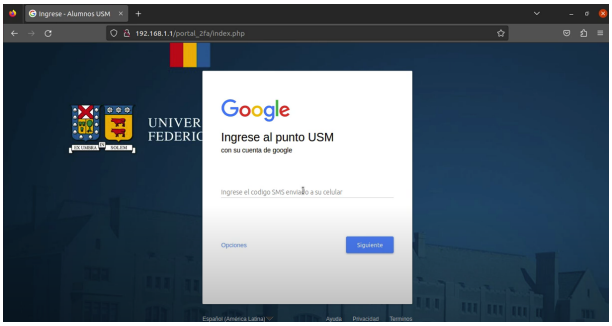
1. Verificar que los datos ingresados por la víctima sean correctos.
2. Dar tiempo al atacante para intentar ingresar con las credenciales de la víctima a su cuenta.



(a) *Inicio de sesión para conectarse a la red*



(b) *Falso intento fallido*



(c) *Ingreso de código de autenticación*

Figura 2: Vistas de la víctima una vez intenta conectarse al punto de acceso WiFi

Luego de tres intentos, la víctima es re-direccionada a una página web donde se le solicita un codigo SMS enviado a su celular. Este código corresponde al intento de inicio de sesión por parte de la atacante.

En caso de que la víctima no vincule su cuenta a un número de celular este paso levantará sospecha, pero dado que la víctima no posee un factor de autenticación secundario, los datos de esta ya estaran disponibles para el atacante.

4. Análisis de Resultados

Como resultado del ataque, el atacante obtiene todas las credenciales necesarias para poder ingresar a la cuenta de la víctima (figura 3). En el caso del experimento se obtienen las credenciales para entrar a la cuenta institucional de un alumno de la Universidad Santa María.

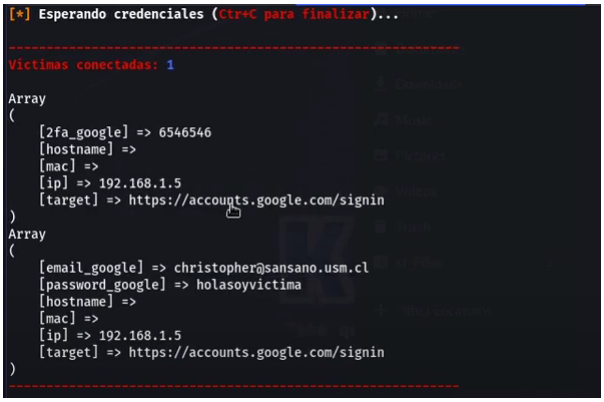


Figura 3: Visualización de datos ingresados por la víctima

4.1. Common Vulnerability Scoring System (CVS)

Para obtener un mejor análisis se hizo uso del CVS [3], que permite cuantificar la gravedad de una vulnerabilidad. En este caso, la vulnerabilidad está en conectarse a una red WiFi falsa, tal como se realizó en el experimento.

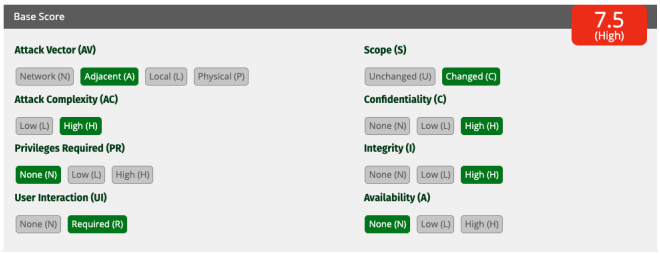


Figura 4: Cálculo del valor CVS para el experimento realizado

En la figura 4 se puede apreciar el valor obtenido para este contexto, el cual es de 7.5 y es definido como "High", es decir, es de un alto riesgo. A continuación, un pequeño análisis de los parámetros del vector:

- **AV**: Su valor es A porque el ataque se limita a la red WiFi generada por el punto de acceso falso.

- **AC**: Su valor es H porque el éxito del ataque está más allá del control del atacante: víctima se conecta voluntariamente al Rogue AP.
- **PR**: Su valor es N porque no se requieren privilegios extras para concretar el ataque.
- **UI**: Su valor es R porque requiere que la víctima se conecte al Rogue AP y escriba sus credenciales.
- **S**: Su valor es C porque las consecuencias van más del componente WiFi atacado.
- **C**: Su valor es H porque con las credenciales robadas se puede acceder a datos restringidos de la víctima.
- **I**: Su valor es H porque el atacante puede alterar configuraciones de aplicaciones asociadas a las credenciales robadas.
- **A**: Su valor es N porque el atacante no puede negar recursos del componente atacado (hasta es posible que la víctima no se de cuenta de que sufrió un robo de datos).

5. Conclusiones y discusiones a futuro

Es concluyente del experimento y sus resultados que esta vulnerabilidad es grave para el usuario. Junto con esto, para un atacante comprometido es relativamente sencillo levantar un punto Rogue WiFi falso y poder engañar a personas que no estén familiarizadas con prácticas de ciberseguridad. Sin embargo, el mayor trabajo que se debe llevar un hacker para poder tener éxito en este tipo de ataques consiste en estudiar previamente al tipo de víctimas al cual estará dirigdo el ataque, en que lugar se realizará, cual es el nivel de ciberseguridad que rodea al lugar dónde se levantará el WiFi AP, etc. Todos estos aspectos, sumados a la habilidad para replicar lo más fielmente posible (sin que levante sospechas) un inicio de sesión y levantar el punto de acceso WiFi, son claves para realizar este tipo de ataques.

Por el momento este es un "punto muerto.[en] la ciberseguridad; queda a responsabilidad de cada uno tener los cuidados mínimos para no caer en este tipo de ataques. Si bien existen métodos para detectar puntos de acceso no autorizados en redes locales, la diversidad de redes junto con la masificación de este tipo de tecnología hacen complicado el panorama para levantar protocolos o métodos técnicos del área de ciberseguridad que sirvan como barrera para este tipos de ataques. Es importante a futuro poder concretar un conjunto de técnicas y protocolos que permitan detectar este tipo de ataques, tal que sea obligatorio para cada lugar dónde se levante una red WiFi el tener protección contra esta vulnerabilidad.

6. Referencias

[1] Github del proyecto
[2] EvilTrust
[3] CVS 3.0 Calculator