WiFi Pineapple – Pineapple in the middle.

Alejandro Muñoz Bravo, alejandrobravo0329@gmail.com
Miguel Ángel Torres Sánchez, mgltorsa@gmail.com
Santiago Gutierrez

Abstract.

There are several kinds of fails on a network, these fails can be used by malicous third parties in order to access network's client information. Clearly also exists forms of security that help us to avoid some types of network attacks, since simple security methods until complex methods.
This paper try to show some security methods for counteract that we defined like PITM, a mechanism that uses WiFi deauthentication attack and Rogue AP attack and explain how these works.

I. Introducción.

Como usuarios de internet, estamos expuestos a una gran cantidad de situaciones desfavorables, que amenazan la seguridad de nuestra información. Al conectarnos a una red, en esta podremos encontrar usuarios mal intencionados que intentaran acceder a nuestros datos, tomando ventaja de las muchas fallas que presenta una infraestructura de comuncación, principalmente las infraestructuras de tecnologia WiFI.
Uno de los fallos presentes en infraestructuras de red, que presentan una tecnologia WiFi, se presencia al ejecutar dos mecanismos, el primero, un WiFi deauthentication attack que da paso al segundo, un Rogue AP.
En este escrito, se hará un acercamiento a el fallo presenciado gracias a estos mecanismos, ejecutados con ayuda de un dispositivo de hardware llamado WiFi Pineapple y las contramedidas necesarias para evitar ser una victima de este ataque que denominamos PITM: "Pineapple in the middle".

II. WiFi Pineapple.

WiFi Pineapple nace como un dispositivo de hardware para realizar auditoria de WiFi, con esto, sus versiones NANO y TETRA presentan una plataforma de software, una suite con diversos modulos funcionales para realizar diversas actividades en la auditoria wireless.
[1]En el nucleo de WiFi Pineapple, se encuentra PineAP, un conjunto avanzado de herramientas de prueba de penetración inalámbricas para el reconocimiento, el control de usuario, el registro y la generación de informes.
Los modulos de WiFi Pineapple son desarrollados por diversos miembros de la comunidad. [2]Cabe destacar que aunque esta suite fue creada para fines de auditoria de red muchos atacantes aprovechan sus capacidades para capturar información y afectar diversas estructuras organizacionales o de seguridad.

III. Man in the middle attacks.

[3]Un ataque man in the middle es, comunmente, en seguridad de computadoras, un ataque en el cual un atacante secretamente intercepta y altera o escucha el trafico entre un par de dispositivos conectados.
Existen diversos tipo de ataque Mitm (*Man in the middle)* de manera que es posible clasificarlos teniendo en cuenta el medio por el cual son realizados, en: ataques contra la capa de enlace y contra la capa de aplicación.

1. ARP Poisoning.

La capa de enlace provee mecanismos de transferencia entre nodos de una red, esta usa ARP para conectar a la capa de red. De igual manera, en las redes wireless (*wlan)* el protocolo 802.11 de la IEEE es reponsable de manejar las direcciones MAC y conexión entre hosts. A si, la capa de aplicación, la de mas alto nivel en el modelo OSI, [4]se encarga de reagrupar estos prtoocolos de comuncacion entre hosts con una asbtraccion de la red que brinda soporte a la comuncación.
ARP poisoning es una forma de ataque en la cual el atacante cambia la dirección MAC y ataca una Ethernet LAN cambiando la caché de ARP de la computadora de destino con un paquete de solicitud y respuesta de ARP falsificado.
[4]Se puede usar para responder a las solicitudes de arp [5 y suplantar la puerta de enlace falsificando su dirección mac. este exploit funciona debido a la resolución automatizada de las direcciones mac a través de arp.

2. De ARP Poisoning a redes Wireless.

En las redes wireless existe un mecanismo similar, donde un cliente posee access points (*AP)* registrados, en su OS transmita un broadcast paquetes *802.11 Probe Request* a cada AP que tengra registrado y el access point que reciba el paquete responde a este con la información necesaria para la conexión.

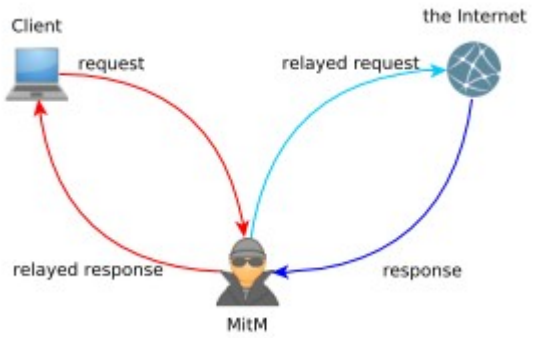

Figure 1: Man in the middle

III. WiFi deauthentication Attack.

Este ataque consiste en atacar un router con paquetes deauth, los cuales solicitan la desconexión de un host falso, esta petición se hace usando spooifng de una dirección de host. El objetivo es generar una desconexion del router que se desea atacar,, cabe aclarar que muchas organizaciones pequeñas, posibles objetivos de ataque, no suelen tener redes demasiado estructuradas y optan por usar tecnologias WiFi, ahora bien, [2]el ataque deauth es utilizado para denegar el servicio en un router con un número considerable de peticiones logrando generar un ataque *DoS* al servicio WLAN, de esta forma cuando las máquinas o hosts conectados al router intenten una nueva conexión, lo harán hacia un posible Rogue AP.

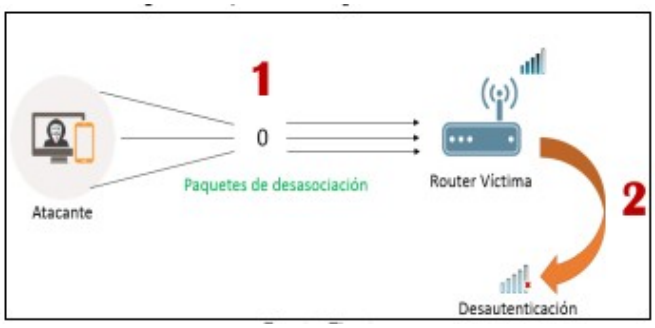

Figure 2: Deauthentication attack

[2]El tiempo que toma un *"Deauth attack"* es proporcional a la calidad de router, un router común no durara demasiado tiempo antes de dar resultados en el ataque.

IV. ROGUE AP.

Traducido al español como punto de acceso falso, es el AP utilizado por el atacante como señuelo para capturar la información de los clientes de red, generar problemas de disponibilidad de algunos servicios y suplantación de sitios web.

Junto al deauthentication attack presentado anteriormente puede ser usado para traer los clientes de una red a el Rogue AP y empezar el ataque, primero se usaria el deauthentication attack para desconectar a los clientes de su AP preferido, sin embargo, como los clientes generalmente tienen registrado su AP preferido y la conexión a este no esta disponible por el ataque, el cliente se conectara a el Rogue AP, que simula el router caido.

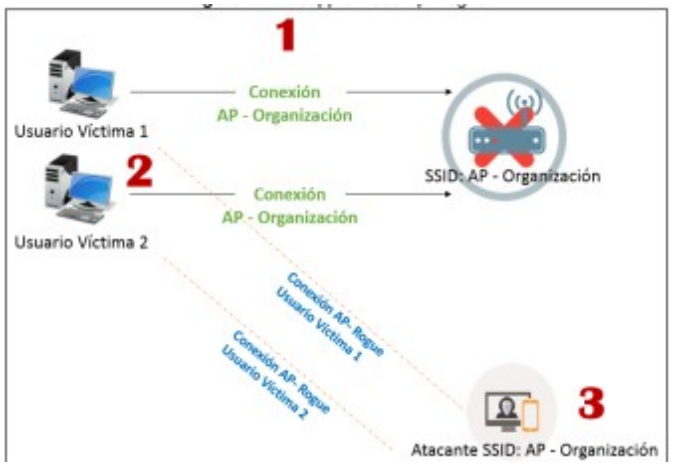

Figure 3: Pineapple modo Rogue AP

V. Conclusiones.

Dado que la situación de access points registrados en dispositivos clientes ,permite el desarrollo de los ataques mencionados, como contramedida se recomienda no guardar redes en dispositivos, a la vez, verificar si la red segura a la cual se desea conectar requiere contraseña. El uso de transferencia con información cifrada tambien es util, ya que esto dificultara la visión de la información, aun si el dispositivo malicioso atrapa el paquete no podra ver su información tan facilmente.

Es necesario, en cualquier lugar, informar a sus clientes de una red, sobre las vulnerabilidades a las que se enfrentaran al conectarse a una red, a su vez, brindarles información y medidas de seguridad como las concluidas con anterioridad.

Referencias.

[1] "WiFi Pineapple - Home", *Wifipineapple.com*, 2018. [Online]. Available: https://www.wifipineapple.com. [Accessed: 28- Nov- 2018].

[2] J. Quintero Tamayo, "Hardware malicioso como herramienta de Pentesting orientado al puesto de trabajo", 2016.

[3]O. Eigner, P. Kreimel and P. Tavolato, "Detection of Man-in-the-Middle Attacks on Industrial Control Networks", *University of Applied Sciences St. Pölten,*, 2018.

[4] C. Claure, X. Martin, J. Fiquet and P. Louis, "Pineapple, Raspberry and WiFi. WiFi Man-in-the-Middle attacks", 2018.

[5] R. Wagner. Address resolution protocol spoofing and F. Callegati, W. Cerroni, and M. Ramilli. man-in-the-middle attacks. The SANS Institute, 2001.

Figuras.

1. JC. Claure, X. Martin, J. Fiquet and P. Louis, "Pineapple, Raspberry and WiFi. WiFi Man-in-the-Middle attacks", *Figura 1 Mitm*, 2018.

2. Quintero Tamayo, "Hardware malicioso como herramienta de Pentesting orientado al puesto de trabajo", *Figura 6: Ataque Deauth dirigido a un Router víctima*, 2016.

3. J. Quintero Tamayo, "Hardware malicioso como herramienta de Pentesting orientado al puesto de trabajo", *Figura 12 Pineapple modo Ap-Rogue*, 2016.