“ATAQUES Y EVALUACIÓN DE VULNERABILIDADES – ATAQUES ACTIVOS”

Trabajo Preparatorio N°1

Laboratorio de Seguridad en Redes

Melanny Dávila
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
melanny.davila@epn.edu.ec

Alejandra Silva
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
alejandra.silva@epn.edu.ec

***Abstract*—En el siguiente documento se tratará temas acerca de ataques y vulnerabilidades a usuarios, específicamente ataques activos los mismos que basan su funcionamiento en el falso aumento en el tráfico de red.**

***Index Terms*—Ataques, máquina virtual, ARP, usuario.**

I. Introducción

En el área de las seguridades se tiene dos tipos de ataques, pasivos y activos en este documento se hablara acerca de los activos que hace referencia a cambiar o modificar el flujo de datos o crear a su vez otro falso haciendo uso de la misma información que se recopilo como nombre de usuarios y contraseña. Este ataques se subdivide en:

- Hombre en Medio: Como su nombre lo dice se encuentra en la mitad entre dos elementos de la red.
- Envenenamiento ARP: Consiste en que la dirección IP que esta asociada a una dirección MAC inventada pertenece a una maquina real.
- Secuestro de sesión: Se hace uso mediante las cookies, lo que le permite robar y controlar la información cuando se encuentra en un sitio web.

II. Objetivos

- Implementar, en un entorno aislado y virtualizado, el ataque de “hombre en el medio” con el fin de evidenciar en la práctica sus consecuencias en una red.
- Analizar técnicamente los resultados de las distintas fases del ataque de “hombre en el medio”.

III. Cuestionario

A. Revisar el marco teórico para la realización de la práctica.

B. Descargar la máquina virtual Kali 2021-2 (Nombre de usuario: kali, contraseña: kali)

En la figura 1 se presenta la máquina virtual Kali 2021-2 ya instalada.

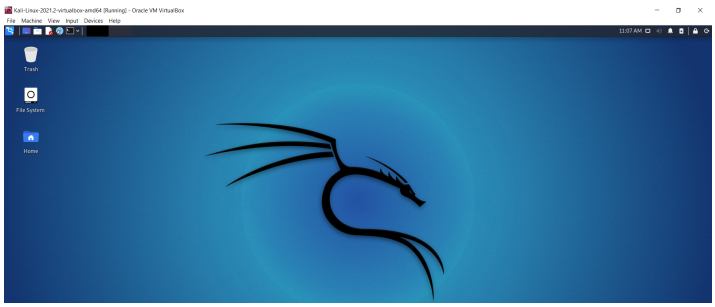

Fig. 1. Kali 2021-2

C. Descargar la máquina virtual Metasploitable2 (Nombre de usuario: msfadmin, contraseña: msfadmin)

En la figura 2 se presenta la máquina virtual máquina virtual Metasploitable2 ya instalada.

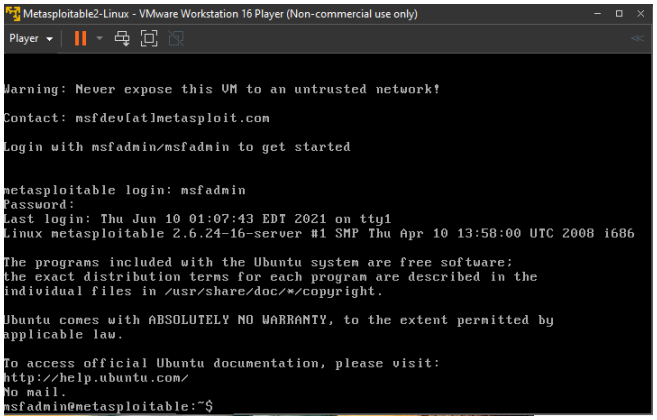

Fig. 2. Metasploitable2

D. Consulte sobre el funcionamiento del Envenenamiento ARP (máximo una carilla)

El envenenamiento ARP, conocido en inglés como ARP Spoofin, es una técnica la infiltración en una red. El principal

objetivo de realizar esto es leer, modificar o detener los paquetes de datos que circulan por una red LAN. Es así como se busca adquirir de los usuarios sus credenciales, contraseñas, mensajes, entre otros. Esto es factible gracias a algunas características que posee el protocolo ARP, las cuales son:

- Una PC presente en la red puede actualizar las cachés ARP de otras PCs presentes en la red, esta técnica es conocida como ARP gratuito.
- El protocolo no autentifica los paquetes que recibe.
- Una caché ARP puede ser modificada siempre y cuando se realice una adecuada petición [1].

Principio de funcionamiento:

- Cuando el dispositivo que atacará a la red conoce las direcciones IP de los dos nodos que desea intervenir; podrá obtener las direcciones MAC mediante ARP.
- Con el uso de ARP gratuito se modifica el contenido del caché de los dispositivos que son afectados; dando como resultado que la dirección IP de uno de los nodos se designe a la dirección MAC del atacante.
- Dando lugar a que cada vez que se envíen paquetes de datos dentro de la red, se obtendrá la dirección MAC y como es obvio se enviará a la dirección del atacante.
- Así, el dispositivo de conmutación enviará las tramas de datos directamente hacia el dispositivo que se inflitró en la red y éste las enviará a la aplicación.
- De igual manera, el dispositivo inflitrado enviará dichas tramas al correcto destino y la principal diferencia sería la dirección del destinatario, aunque los datos también pueden ser modificados.
- Es así como mediante la técnica conocida como hombre en el medio el dispositivo infiltrado a recibido todo el tráfico que era destinado a un dispositivo en específico [1].

Tipos de ataque

- ARP DoS: Básicamente es confundir al dispositivo, dado a que una dirección IP es asociada con una dirección MAC no existente, por lo que cada que vez que se busque entablar comunicación con dicha dirección, el dispositivo de conmutación enviará los datos hacia un sistema que no existe y no llegarán a su destino. En el caso de que la dirección IP manipulada sea una dirección de acceso, se perderá la comunicación con el exterior [2].
- ARP hijacking o proxying: Un ataque no esta completo si la información robada no es reenviada para provecho de quien se la está robando. Los dispositivos a los que se les reenvía la información suelen ser computadoras personales o puertas de enlace. Como principio, estos dispositivos responden de manera normal para no alertar al usuario del dispositivo que es atacado. Además, el uso de estos dispositivos optimiza el ataque ya que puede permitir que más información se almacene y sea capturada a la vez.
- ARP Sniffing: En este caso el tráfico de la red es redirigido por el dispositivo víctima hacia él mismo, esto se consigue debido a que el atacante hace creer que una dirección IP esta asociada a una MAC. Es por esto que la tarjeta de red ignora los datos y de esta manera el atacante puede obtener información que el dispositivo víctima cree que está enviando.

En conclusión, un ataque ARP se resume en: convencer al sistema víctima de que la dirección MAC del atacante es la de la puerta de enlace mientras que la auténtica es la atacante. Luego, hacer creer al sistema auténtico que la dirección MAC del atacante es la dirección MAC de la víctima y, finalmente, "enrutar" la información que ya es revisada de manera que el ataque sea transparente y ninguna de las partes sospeche [2].

E. Consulte para que sirve la herramienta MITMf y sus principales características (máximo una carilla)

La herramienta MITMf por sus siglas en ingles "MAN IN THE MIDDLE framework" que se basa en tener una estructura de trabajo que realiza un ataque, cuyo objetivo es dar una ventana única para realizar este tipo de taque (Man- In- The-Middle) con ataques de red en tiempos iguales, fue creado para eliminar y ayudar a otras herramientas que poseían muchos problemas. Este ataque permite leer, modificar e insertar por voluntad propia mensajes entre dos partes sin que se revele que interacción ha sido violada, este ataque se da principalmente en el protocolo de intercambio de claves de Diffie-Hellman cuando no se tiene autenticación. [4]

Características:

- Captura FTP, IRC, POP, Telnet, SMTP ,SNMP, IMAP y credenciales de Kerberos con la ayuda de Net-Creds.
- Contiene servidor SMB, DNS y HTTP
- Posee una versión mucho mejor del proxy SSLStrip que ayuda a cambiar HTTP y un bypass parcial de HSTS. [4]
- Desde la versión 0.98 admite filtrado y manipulación de paquetes lo que le da al usuario el permiso de manipular cualquier tipo de protocolo o trafico.
- Manipula, observa y filtra paquetes de red lo que ayuda a implementar un plugin para ataques.
- Soporta servidores WPAD. [3]

REFERENCES

[1] "Envenenamiento de las tablas ARP (ARP spoofing)", Tecno y Soft. https://tecnoysoft.com (accedido jun. 09, 2021).

[2] "Envenenamiento ARP". http://blackspiral.org/docs/arp_spoofing.html (accedido jun. 09, 2021).

[3] "Man in the middle framework (MITMf)". https://www.lesand.cl/foro/man-middle-framework-mitmf (accedido jun.09,2021).

[4] "HACER ATAQUES Man-in-the-middle con (MITMF) EN KALI LINUX". https://www.creadpag.com/2018/05/hacer-ataques-man-in-middle-con-mitmf.html (accedido jun.09,2021).

[5] "MITMf: Ataques modernos en redes de datos IPv4 " . //https://www.elladodelmal.com/2017/02/mitmf-ataques-modernos-en-redes-de.html (accedido jun.09,2021).