Facultad de Ingeniería

Ingeniería en Informática y Sistemas

Redes I

**JULIO ANTHONY ENGELS RUIZ COTO – 1284719**

**EDDIE ALEJANDRO GIRON CARRAZA - 1307419**

# Laboratorio 5 – Redes I

**Parte I – Conceptos**

1. Describa brevemente el funcionamiento de la Capa 2 (OSI y TCP/IP)

R//Es el encargado de la comunicación entre el hardware y software y también del direccionamiento físico por medio de las direcciones MAC, esto codificando los datos en tramas para enviarlos por la capa física.

1. Liste y describa las subcapas en las que se divide la capa de Enlace

* R// Subcapa MAC (Media Access Control): en esta subcapa ocurre la codificación de datos, también la creación de tramas y su envió por la red.
* Subcapa LLC (Logical Link Control): interactúa con el software de la red, en esta subcapa ocurre el dialogo entre el hardware y software a través de los drivers.

1. Nombre que recibe la unidad de datos de protocolo (PDU) de la Capa 2

R// Tramas

1. Liste y describa brevemente protocolos y estándares que funcionan en la capa 2.

R// HDLC (High-Level Dara Link Control): protocolo el cual es orientado a bits que se utiliza para la comunicación a través de enlaces punto a puntos y a su vez multipunto.

1. Liste y describa cada uno de los campos que componen una trama

* R// FCS (Frame Check Sequence): esta nos brinda si dicha trama llega inalterada o no.
* Dirección de origen y destino: dirección MAC propia (origen) y dirección MAC del dispositivo destino.

1. Describa brevemente qué es una MAC Address y cómo está estructurada

R// Se representa como un código hexadecimal que identifica a un controlador de interfaces de red (NIC), son únicas para cada dispositivo de la red a nivel mundial y no puede ser modificada. Esta se compone de 6 pares de caracteres hexadecimales, cada carácter hexadecimal representa 4 bits, 2 caracteres hexadecimales representan 8 bits o 1 byte 6 pares x 8 bits = 42 bits en total. La primera mitad de dígitos se llama OUI (identificador único organizacional) que es asignado por la IEEE a cada empresa fabricante y la segunda mitad corresponde al identificador único que cada fabricante le asigna a un dispositivo.

1. Describa que es un sniffer

R// se describe como una herramienta de software o hardware que permite al usuario monitorear su trafico de red en tiempo real y con ello capturando todo el trafico que sale y entra de su dispositivo, de manera que se puede diagnosticar problemas y evaluar rendimiento.

1. Describa que significa configurar una tarjeta de red (NIC) en modo promiscuo.

R// Es un modo que permite interceptar en su totalidad todos los paquetes que son manejados en la red. Este modo intercepta tanto los paquetes que se encuentren en una red cableada como en una red inalámbrica.

1. Describa brevemente qué es spoffing de MAC Address

R// El spooffing de MAC address o suplantación de dirección MAC consiste en el cambio manual o por medio de programas de la dirección MAC del dispositivo, volviendo así, un dispositivo diferente ante la red.

1. Describa brevemente qué es MAC flooding

R// El MAC flooding es un tipo de ataque el cual consiste en el envío de tramas a gran escala, con el fin de saturar la memoria de la victima y hacer que pierda la asociación de el MAC con los puertos físicos.

1. Investigue y describa brevemente el funcionamiento del Protocolo ARP.

R// Este protocolo realiza un mapeo en el cual traduce los sistemas para que estos puedan reconocerse entre sí y conocer sus direcciones MAC. Esto por medio del envío de un paquete a la dirección de broadcast FF:FF:FF:FF:FF:FF.

1. ¿En cuál capa del modelo OSI funciona ARP?

R// En la capa 2

1. Investigue y describa brevemente para qué se utiliza una puerta de enlace (Gateway).

R// El Gateway o puerta de enlace es un dispositivo que permite conectar redes que cuentan con distintos protocolos o arquitecturas. Sirve como intermediario entre redes, y traduce los datos para la red a la que se dirija.

1. Investigar y explicar brevemente que es un “Ataque de intermediario” (man in the middle).

R// Es un ataque el cual consiste en posicionarse entre la comunicación de un dispositivo y la red, sin que la víctima sea consiente de esto.

**Parte II – ARP Poisoning**

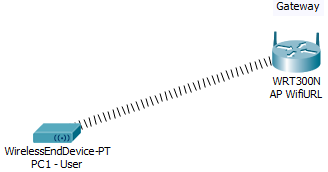
**Objetivo:**

* Explorar y entender el funcionamiento del protocolo ARP durante un proceso de comunicación entre dispositivos a través capa 2 y capa 3.
* Comprender el funcionamiento de la puerta de enlace en un proceso de comunicación.
* Entender las brechas de seguridad que existen en una red, a nivel de capa 2 y 3, y los ataques que pueden explotar dichas vulnerabilidades.

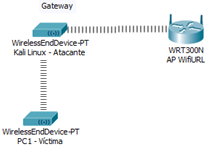
**Práctica:**

En esta práctica, suplantaremos la identidad del equipo Gateway que permite acceder a Internet desde el Laboratorio de Clase por una computadora corriendo Kali Linux. El Gateway para comunicarse a Internet desde el Laboratorio es el Access Point de la red inalámbrica. Este equipo con Kali Linux asociará su MAC Address a la IP del Gateway registrado en la tabla de ARP del equipo atacado, el cuál comenzará a enviar su tráfico de Internet al equipo atacante.

Comunicación Normal:



Man in the middle:



1. En una USB, con capacidad de por lo menos 4 GB, instalar los archivos de Kali Linux para arrancar una laptop desde dicha USB.

* Para descargar Kali Linux: <https://www.kali.org/downloads/>
* Software Rufus para convertir una USB en booteable: <http://rufus.akeo.ie/>

1. En la computadora atacante (computadora corriendo Kali Linux) realizar el ataque de ARP Spoffing siguiendo las instrucciones de este sitio:

<https://www.redeszone.net/2016/11/12/ataque-arp-poisoning-con-kali-linux/>

<https://null-byte.wonderhowto.com/how-to/use-ettercap-intercept-passwords-with-arp-spoofing-0191191/>

1. Realizar pruebas de autenticación desde el siguiente sitio:

<http://testphp.vulnweb.com/login.php>

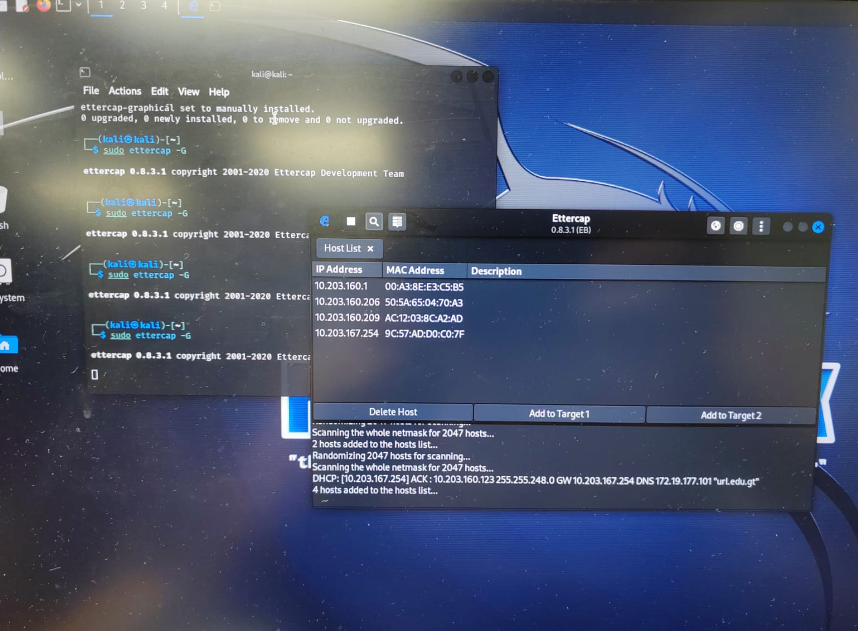
1. Colocar en esta parte fotografías como evidencia de lo siguiente:

* Computadora cliente (víctima), con CMD abierto mostrando su tabla ARP. (Correr comando “arp -a” en un CMD) previo al ataque de envenenamiento.

Interfaz de usuario gráfica

Descripción generada automáticamente

* Computadora atacante (Kali Linux), mostrando la tabla de Hosts y la consola de Output del programa Ettercap, posterior a correr el ataque ARP Poisoning.

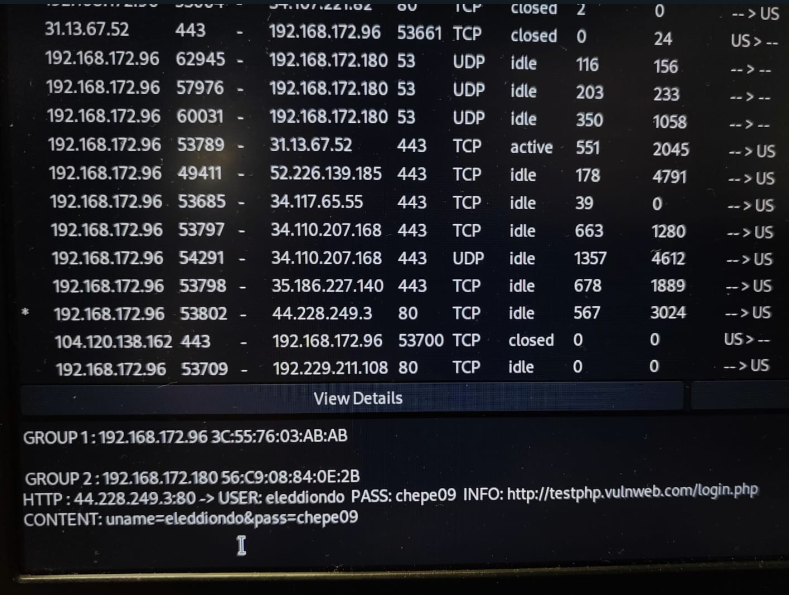


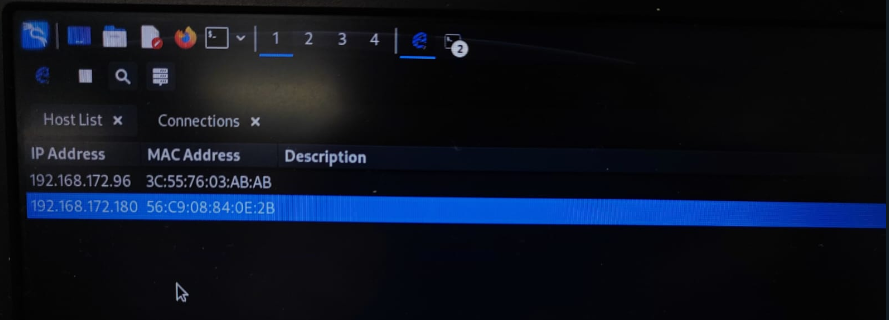
Una captura de pantalla de una computadora

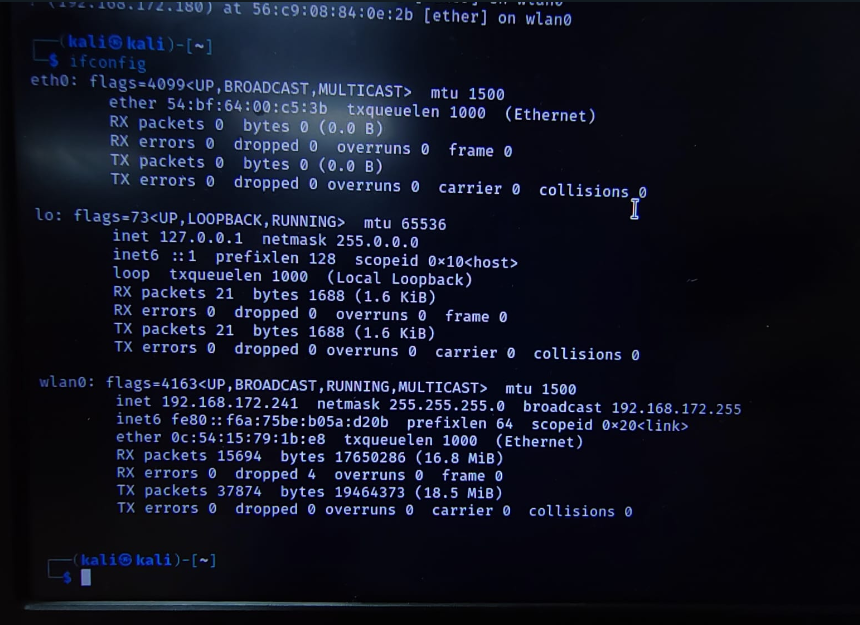
Descripción generada automáticamente con confianza media

Pantalla de computadora con letras

Descripción generada automáticamente con confianza media







Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Pantalla de computadora con letras

Descripción generada automáticamente con confianza media

* Computadora cliente (víctima), con CMD abierto mostrando su tabla ARP. (Correr comando “arp -a” en un CMD) posterior al ataque de envenenamiento.

**Conclusiones**

Posterior a realizar la práctica conteste lo siguiente:

1. ¿Cómo funciona el ataque ARP Poisoning que acaba de ejecutar?

R// Consiste en envenenar a la víctima haciéndole creer que el router es el atacante con el objetivo de que la víctima reenvíe todo su tráfico a este atacante para realizar un sniffing de todas y cada una de las conexiones que realice.

1. ¿Cómo logra el software Ettercap, que corrió en Kali Linux, colocar su MAC Address en la tabla ARP del equipo víctima?

R// Colocando la MAC address del atacante en la MAC address del Gateway de la víctima.

1. ¿Qué maneras o mecanismos existen para mitigar un ataque ARP Poisoning en una red real?

R// Filtrado de paquetes: Estos filtros se encargan de inspeccionar todos los paquetes que se transmiten a través de una determinada red. Pueden filtrar y bloquear paquetes que contengan información de una fuente de conflicto.

Software de detección: En el mercado podemos encontrar muchos programas que nos ayudan a prevenir estos ataques. Su principal tarea es inspeccionar los datos antes de su transmisión y si encuentra algún peligro, lo bloquea.

Uso de protocolos criptográficos: Estos protocolos se encargan de reforzar la seguridad en la prevención de estos ataques. Para ello, usan el cifrado de datos previamente a que sean transmitidos y revisan la autentificación cuando son recibidos. Algunos de ellos con TLS, SSH, HTTPS