Facultad de Ingeniería

Ingeniería en Informática y Sistemas

Redes I

# Laboratorio 5 – Redes I

**Parte I – Conceptos**

1. Describa brevemente el funcionamiento de la Capa 2 (OSI y TCP/IP)
2. Liste y describa las subcapas en las que se divide la capa de Enlace
3. Nombre que recibe la unidad de datos de protocolo (PDU) de la Capa 2
4. Liste y describa brevemente protocolos y estándares que funcionan en la capa 2.
5. Liste y describa cada uno de los campos que componen una trama
6. Describa brevemente qué es una MAC Address y cómo esta estructurada
7. Describa que es un sniffer
8. Describa que significa configurar una tarjeta de red (NIC) en modo promiscuo.
9. Describa brevemente qué es spoffing de MAC Address
10. Describa brevemente qué es MAC flooding
11. Investigue y describa brevemente el funcionamiento del Protocolo ARP.
12. ¿En cuál capa del modelo OSI funciona ARP?
13. Investigue y describa brevemente para qué se utiliza una puerta de enlace (Gateway).
14. Investigar y explicar brevemente que es un “Ataque de intermediario” (man in the middle).

**Parte II – ARP Poisoning**

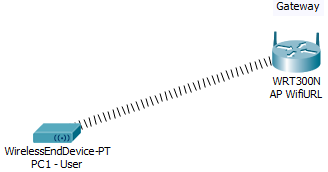
**Objetivo:**

* 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.

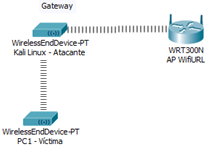
**Práctica:**

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.
* Computadora atacante (Kali Linux), mostrando la tabla de Hosts y la consola de Output del programa Ettercap, posterior a correr el ataque ARP Poisoning.
* 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?
2. ¿Cómo logra el software Ettercap, que corrió en Kali Linux, colocar su MAC Address en la tabla ARP del equipo víctima?
3. ¿Qué maneras o mecanismos existen para mitigar un ataque ARP Poisoning en una red real?