Universidad Rafael Landívar
Tradición Jesuita en Guatemala

Facultad de Ingeniería
Ingeniería en Informática y Sistemas
Redes I

Laboratorio 04 – Redes I

Alexander Villatoro
1182118

Parte I – Conceptos

a. Describa brevemente el funcionamiento de la Capa 2 (OSI y TCP/IP)
   - La capa 2 de TCP/IP en ella se manejan todos los aspectos que un paquete IP requiere para efectuar un enlace físico real con los medios de la red. Y en la capa 2 del modelo OSI llamada capa de enlace se ocupa del direccionamiento físico dentro de cualquier topología de red, esta capa nos permite activar, mantener y deshabilitar la conexión, así como la notificación de errores.

b. Liste y describa las subcapas en las que se divide la capa de Enlace
   - Control de enlace lógico (LLC): coloca en la trama información que identifica qué protocolo de cada de red se utiliza para la trama.
   - Control de acceso al medio (MAC): proporciona direccionamiento de la capa de enlace de datos y acceso a tecnologías de capa física.

c. Nombre que recibe la unidad de datos de protocolo (PDU) de la Capa 2
   - Trama

d. Liste y describa brevemente protocolos y estándares que funcionan en la capa 2.
   - Ethernet: establecer un nivel de protocolo para configurar, acceder y controlar dispositivos.
   - 802.11 inalámbrico: tecnología Wi-Fi.
   - Protocolo punto a punto (PPP): conecta un sistema informativo a otro.
   - HDLC: es un grupo de protocolos de comunicación de la capa de enlace de datos para transmitir datos entre puntos o nodos de la red.
   - Frame Relay: define cómo se enrutan las tramas a través de una red de paquetes rápidos según el campo de dirección de la trama.

e. Liste y describa cada uno de los campos que componen una trama
   - **Indicadores de arranque y detención de trama**: identifica el limite del comienzo y del final de una trama.
   - **Direccionamiento**: indica los nodos de origen y destino en los medios.
   - **Tipo**: identifica el protocolo de capa 3 en el campo de datos.
   - **Control**: identifica el control de flujo, como QoS.
   - **Datos**: Contenido de la trama.
   - **Detección de errores**: comprobación de errores en la recepción de la trama.

f. Describa brevemente qué es una MAC Address y cómo está estructurada
    - Proporciona direccionamiento de la capa de enlace de datos y acceso a tecnologías de capa física. Los primeros 6 es un identificador único de la organización (OUI) eso quiere decir que identifica quien es el fabricante del hardware, y los 6 restantes son asignador por el proveedor (NIC), en el cual es el número de serie que identifica el dispositivo fabricado.

g. Describa que es un sniffer
    - Es una herramienta de software o hardware que le permite al usuario "olfatear" o monitorear su tráfico de Internet en tiempo real, capturando todos los datos que fluyen hacia y desde su computadora.

h. Describa que significa configurar una tarjeta de red (NIC) en modo promiscuo.
    - El modo promiscuo es aquel que conecta una computadora a una red compartida para poder capturar todo el tráfico que circula por ella.

i. Describa brevemente qué es spoofing de MAC Address
    - Es una técnica en la cual se puede cambiar la MAC Address de un dispositivo de red.

j. Describa brevemente qué es MAC flooding
    - Es una técnica para comprometer la seguridad de los switches de red.

k. Investigue y describa brevemente el funcionamiento del Protocolo ARP.
    - Tiene la función de encontrar la dirección MAC (Ethernet MAC) que tiene una determinada dirección IP.

l. ¿En cuál capa del modelo OSI funciona ARP?
    - Capa de enlace de datos.

m. Investigue y describa brevemente para qué se utiliza una puerta de enlace (Gateway).
    - Actúa como interfaz de conexiones entre los dispositivos, y de igual forma da acceso a compartir recursos entre dos o más ordenadores. Enruta toda la información

n. Investigar y explicar brevemente que es un “Ataque de intermediario” (man in the middle).
    - El ataque consiste en visualizar e interceptar los datos o paquetes de la víctima y procurar que no se conozca la violación del enlace entre ellos.

Parte II – ARP Poisoning

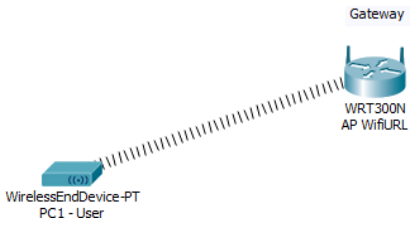
Objetivo:

- 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.

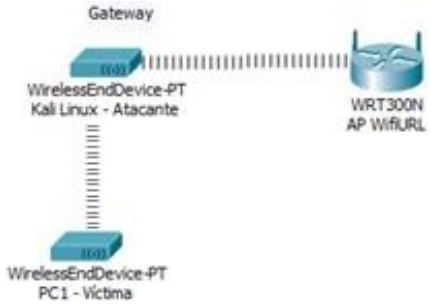
Práctica:

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:



Preparar el ambiente

Opción 1.

a. 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/

Opción 2.

b. Ejecute Kali Linux desde una máquina virtual.
   b.1. Asegúrese de configurar la tarjeta de red de la VM en modo Puente / Bridge Adapter.

Nota:

- **Debe deshabilitar el firewall de Windows y el antivirus para realizar esta práctica.**

Turn off Defender antivirus protection in Windows Security

1. Select Start > Settings > Update & Security > Windows Security > **Virus & threat protection** > Manage settings (or Virus & threat protection settings in previous versions of Windows 10).
2. Switch Real-time protection to Off.

Turn off Defender antivirus protection in Windows Security

1. Select Start > Settings > Update & Security > Windows Security > **Firewall & Network protection** > Domain Network
2. Switch Microsoft defender Firewall protection to Off.

Realizar el Ataque

a. Identifique sus datos de Red de la maquina real / victima.
    a. Dirección IP
    b. Mac address
    c. Gateway / Puerta de Enlace.

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

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

    Para ver el tráfico desde Ettercap seleccionar : menú > View > Connections

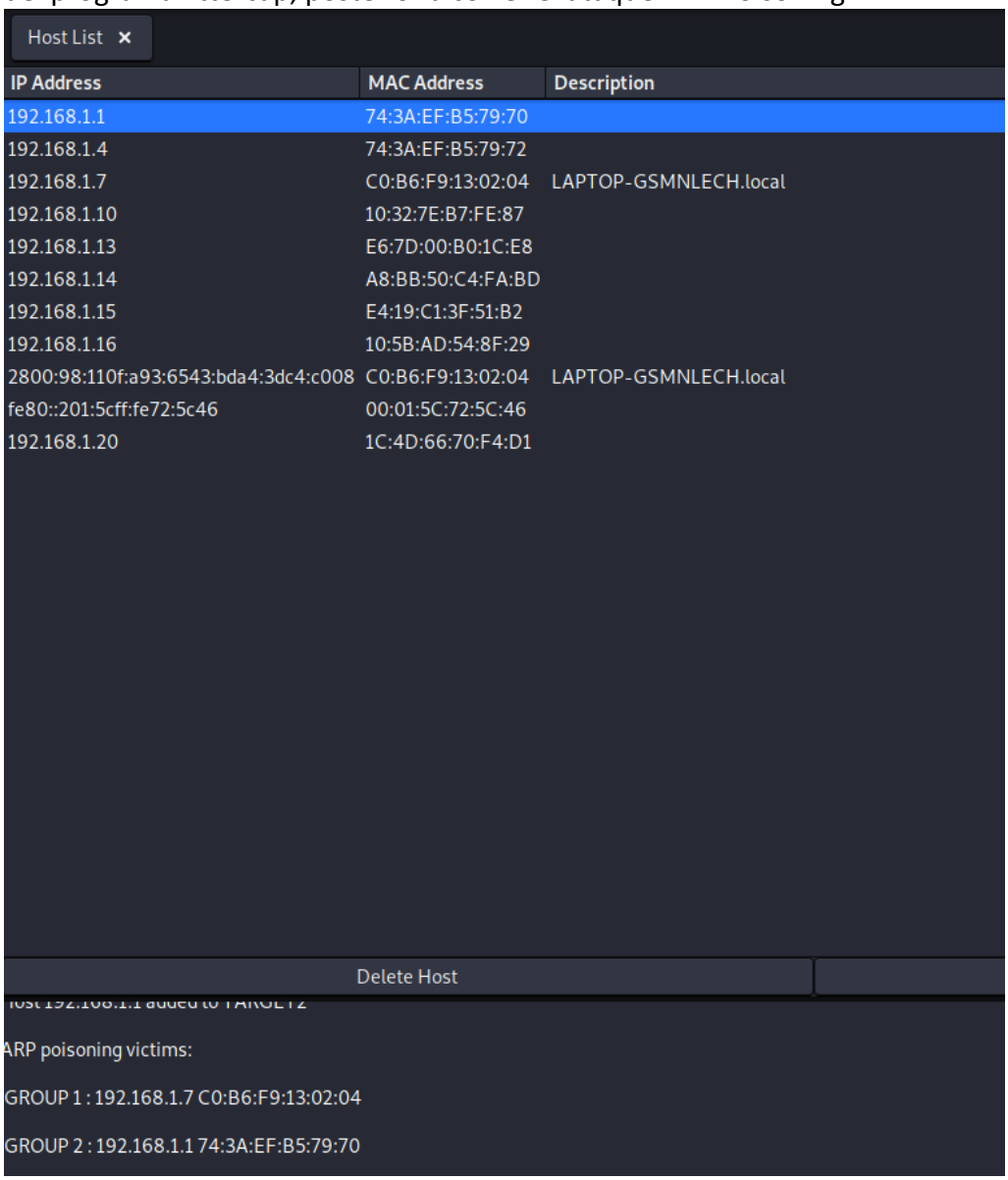
    https://null-byte.wonderhowto.com/how-to/use-ettercap-intercept-passwords-with-arp-spoofing-0191191/

c. Colocar en esta parte fotografías/capturas de pantalla como evidencia de lo siguiente:

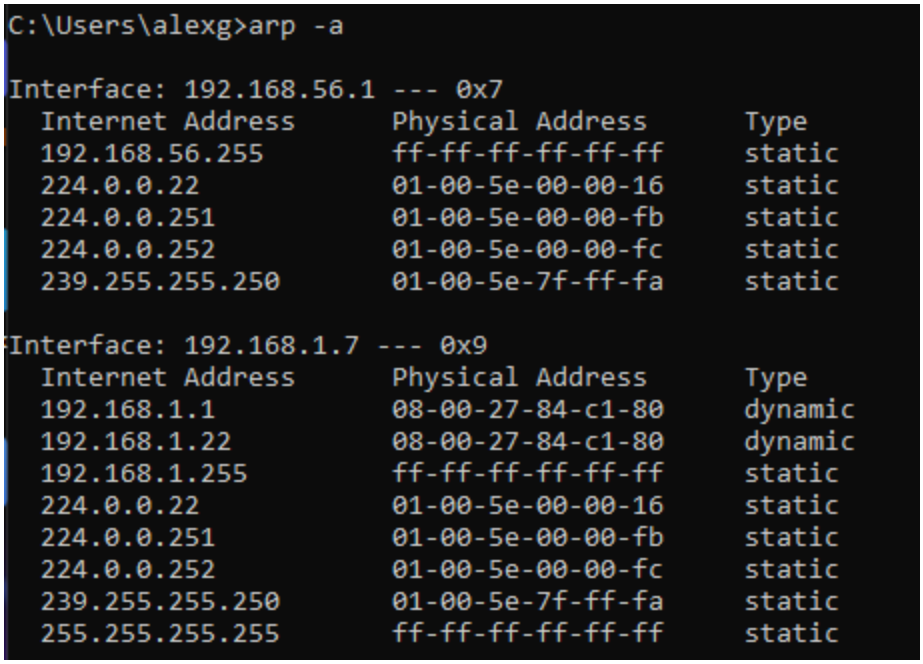
- Computadora cliente (víctima), con CMD abierto mostrando su tabla ARP. (Correr comando “arp -a” en un CMD) previo al ataque de envenenamiento.

```
C:\Users\alexg>arp -a

Interface: 192.168.56.1 --- 0x7
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.1.7 --- 0x9
  Internet Address      Physical Address      Type
  192.168.1.1           74-3a-ef-b5-79-70     dynamic
  192.168.1.3           4c-c9-5e-68-81-93     dynamic
  192.168.1.11          c8-d9-d2-80-b8-d9     dynamic
  192.168.1.18          a8-82-00-65-a1-d4     dynamic
  192.168.1.22          08-00-27-84-c1-80     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\alexg>
```

- 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?
    - Consiste en hacer que alguna computadora sea el Gateway de la red local. Hacer que una maquina finja que es un Router.
2. ¿Cómo logra el software Ettercap, que corrió en Kali Linux, colocar su MAC Address en la tabla ARP del equipo víctima?
    - Ettercap funciona poniendo la interfaz de red en modo promiscuo y con esto poder envenenar las máquinas de destino con el ARP en el cual este modifica la MAC address del router para poder creer que la maquina atacante sea el router y con esto poder recibir los paquetes de la maquina víctima.
3. ¿Qué maneras o mecanismos existen para mitigar un ataque ARP Poisoning en una red real?
    - Entradas estáticas en tabla ARP ya que la IP se asocia a una MAC address y esta no cambiar en un largo tiempo.
    - DHCP snooping es una función en la cual detecta si se hace un cambio en la MAC address.
    - Detectar ARP spoofing: es un programa que monitorea y detectan tipos de ataques en red y como de igual forma notifican al administrador.
    - RARP es una consulta en la cual es a partir de una MAC Address de la IP correspondiente, si esta retorna múltiples IP’s, esto nos da a entender que la MAC ha sido clonada.