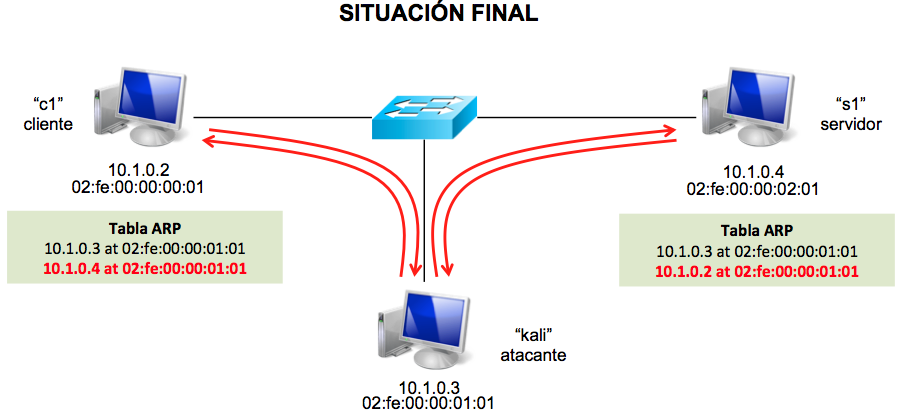
Practica 4 – “Dispositivos En Conmutación De Paquetes



**Conmutación:**

* Paquetes
* Circuitos
* Mensajes

**ARP Spoofing:**

El principio del ARP Spoofing es enviar mensajes ARP falsos (falsificados, o spoofed) a la Ethernet. Normalmente la finalidad es asociar la dirección MAC del atacante con la dirección IP de otro nodo (el nodo atacado), como por ejemplo la puerta de enlace predeterminada (gateway). Cualquier tráfico dirigido a la dirección IP de ese nodo, será erróneamente enviado al atacante, en lugar de a su destino real. El atacante, puede entonces elegir, entre reenviar el tráfico a la puerta de enlace predeterminada real (ataque pasivo o escucha), o modificar los datos antes de reenviarlos (ataque activo). El atacante puede incluso lanzar un ataque de tipo DoS (Denegación de Servicio) contra una víctima, asociando una dirección MAC inexistente con la dirección IP de la puerta de enlace predeterminada de la víctima.

**#Comandos:**

***Ifconfig*: muestra las configuraciones de internet**

***Arp – a*: devuelve las direcciones Mac con sus respectivas direcciones IP**

**Herramientas:**

Mac changer: Altera las direcciones Mac

* Las puede asignar de forma automática
* Las puede asignar de forma manual

MAC: las direcciones Mac están constituidas los primeros 6 dígitos por el fabricante

**Mac Changer comandos:**

***# -r eth0***

Primero se tiene que detener las interfaces para que se pueda permitir modificar las direcciones MAC, con el siguiente comando

**# *if config eth0 down***

Después de cambiar el estado insertar los siguientes comandos:

***# macchanger -r eth0***

***# if config eth0 up***

***# arp -a***

***#macchanger -m 00:A1:B1:C1:D1:G1 eth0***

Las dos últimas líneas de comandos son para levantar la interfaz nuevamente y verificar que la dirección Mac ha cambiado

Estas vulnerabilidades se encuentran en el cache y en el Buffer

**Conclusiones:**

El ARP, Flooding, Spooning nos ayuda a penetrar las redes por medio de puertos vulnerables que se encuentran en el sistema, como lo es el cache y el Buffer, estas vulnerabilidades las usa el ARP para poder sobrecargar el tráfico de datos y de esta manera modificar la tabla de direcciones Mac y así permitirnos hacernos pasar por otro usuario que tenga esta dirección Mac, esta práctica fue realmente interesante ya que ayudo a conocer y aprender sobre los posibles ataques a los que nos encontramos vulnerables