Protocolos de Comunicación TCP/IP

Trabajo de Laboratorio N° 1

Temas:

- Instalación de Sistema Operativo
- Configuración y testeo básico de TCP/IP
- Protocolo ARP

Laboratorio 1: Instalando y creando nueva máquina virtual

1. Inicie sesión como administrador.
2. Inicie VirtualBox.
3. Cree una nuevo equipo Virtual.
4. En nombre y ubicación ponga "TCPIP Martes" o "TCPIP Jueves" según corresponda.
5. Elija Windows 2003 como sistema Operativo.
6. Asignele al menos 256 MB y un nuevo disco virtual de espacio dinámico de 20 GB y finalice el wizard.
7. Vaya a configuración y configure la red con 1 placa de red y elija en attached to a Adaptador Puente o Bridge y seleccione abajo la placa de red del equipo host.
8. En Cd/Dvd rom monte la imagen de Windows 2003 que se encuentra en c:\imagenes.

Laboratorio 2: Instalando Sistema Operativo en Máquina Virtual

1. Inicie la máquina virtual y espere para comenzar la instalación.
2. Presione Enter para empezar la Instalación de Windows 2003, Luego Aprete F8 para aceptar la licencia.
3. Cree una partición eligiendo el disco y luego formatee con NTFS (rápido).
4. Espere a que se copie los archivos iniciales y pulse enter para reiniciar el

equipo virtual.

5. Cuando reinicie en la configuración regional pulse siguiente.
6. Complete nombre y siguiente.
7. Ingrese clave del producto provista por el profesor.
8. En licencia presione siguiente.
9. Luego ponga nombre de equipo provista por profesor y sin clave.
10. Verifique fecha y hora y elija -03 en zona horaria.
11. Elija configuración personalizada de red y verifique que opciones hay para configurar (deje todo como viene por defecto).
12. Designe a LABTCPIP como grupo de trabajo.
13. Termine de instalar y reinicie la máquina virtual.

Laboratorio 3: Verificación, Configuración y Testeo de TCP/IP en Windows

- Verificación de la instalación de TCP/IP en Windows.
  1. Inicie sesión como administrador.
  2. Instale los guest additions del virtual box (permite ampliar la pantalla y otras propiedades entre el host y el guest de la máquina virtual).
  3. Reinicie y vuelva a iniciar sesión como administrador.
  4. En el menú de Inicio, elija configuración y luego Panel de Control. Elija “Conexiones de red y de acceso telefónico”.
  5. Abra el ítem “Conexión de área local” y a continuación “Propiedades”.
  6. En la ventana que se muestra podrá verificar todos los parámetros relacionados con la configuración de la red de dicha estación.
  7. Ingrese en las propiedades del “Protocolo internet TCP/IP”.
- Configuración de Dirección IP
  1. Configure los parámetros con los datos proporcionados por el docente a cargo (dirección IP y máscara de subred).
  2. Revise que otros parámetros tiene posibilidad de configurar y anótelos para futuras referencias. Investigue que finalidad tienen.

3. Una vez terminada la configuración cierre la ventana y acepte los cambios.

Laboratorio 4: Instalando un snifer y verficando la comunicación

1. En el menú inicio elija ejecutar y ejecute \\192.168.1.4 Usuario: samba y Password: 12345678.
2. Elija la carpeta Soft.
3. Copie el programa wireshark.exe a su equipo virtual.
4. Instale siguiendo las opciones predeterminada.
5. Ejecute la herramienta “Wireshark” que se encuentra instalada en su equipo.
6. Seleccione la interface de red para capturar e inicie la captura.
7. Minimice la ventana y continúe con el siguiente ejercicio, luego se analizarán los datos capturados.

- Testeo de la configuración.

1. Realice un **ping** a la dirección de “loopback”, (127.0.0.1) ¿Qué respuesta obtiene?
2. Realice un **ping** a su propia dirección IP.
3. Realice un **ping** a una máquina de su propia subred. (la dirección de un compañero).
4. Realice un **ping** a la IP 10.10.0.31 ¿Funciona?
5. Verifique los paquetes capturados e identifique cuales a que comandos pertenecen.

Laboratorio 5: Cache del ARP en Windows

1. En la ventana de comandos ejecute **arp –g.** Documente las entradas que posee la tabla de cache.
2. Borre las entradas de la tabla de cache a través del comando **arp –d *.**
3. Verifique de nuevo la tabla de cache.
4. Realice un **ping** a un host de la red local. Vuelva a ejecutar arp –g, ¿qué entrada fue agregada? ¿Qué tipo de entrada es? Verifique si en el equipo

remoto que hizo ping se agregó la entrada de su máquina.

Laboratorio 6: Identificación de problemas de configuración de IP.

- Problemas con IP duplicado.
  1. Pare y reinicie la captura en wireshark.
  2. En la opción “Show the capture options…” del menú seleccione para “Capture Filter” el valor “Ethernet type 0x0806 (ARP) y acepte.
  3. Acceda a las propiedades del TCP/IP.
  4. En el Dirección IP del “host” ingrese un número IP existente en la red. (la IP de su compañero).
  5. Un mensaje de error le aparecerá cuando acepte la nueva configuración.
  6. Cierre el menú de Configuración de la red.
  7. Restaure la configuración a la dirección original.
- Análisis de la captura de paquetes
  1. En la ventana de captura seleccione “Stop” para detenerla.
  2. Expanda el contenido de los paquetes de request y reply de ARP y documente los campos del paquete
  3. En un paquete de request de ARP y en un paquete de reply: ¿Cuál es el valor de los campos “Destination Address” a nivel Ethernet y “Target MAC Address” a nivel ARP? ¿Son iguales?
  4. Analice grupalmente junto al docente a cargo la información obtenida en la captura.

Laboratorio 7 (OPCIONAL Y debe informar antes de empezar esta parte):

Realizando envenenamiento ARP.

El envenenamiento de **ARP**, es una técnica usada para infiltrarse en una red Ethernet conmutada (basada en switch y no en hubs), que puede permitir al atacante “husmear” paquetes de datos en la LAN (red de área local), modificar el tráfico, o incluso detener el tráfico (conocido como DoS: Denegación de Servicio).

El principio del ARP Spoofing es enviar mensajes ARP falsos 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.

1. Instale la herramienta Ettercap que se encuentra en el equipo servidor **(IP provista anteriormenter**).
2. Ejecute la herramienta “Wireshark” nuevamente siguiendo los pasos de la parte 3 del laboratorio.
3. Ejecute la herramienta Ettercap.
4. En el menú **Sniff** seleccione **Unified Sniffing.**
5. Seleccione la interface de red de ethernet y pulse ok.
6. En el menú **Hosts** seleccione **Scan for Hosts.**
7. Luego seleccionar en el mismo menú **Host list.**
8. Seleccione una IP y luego pulse en **Target 1.**
9. Seleccione la IP de la Puerta de enlace y pulse en **Target 2.**
10. En el menú **Mitm** seleccione **Arp poisoning.**
11. Como parámetro opcional seleccione **Sniff remote connections.**
12. Para comenzar seleccione **Start Sniffing** del menú start.
13. Para verificar que se realizo el envenenamiento ARP, en el menú **Plugins** seleccione **Manage the plugins**. Después haga doble clic en el **chk_poison** plugin . Anote la respuesta que obtuvo.
14. Termine el programa ettercap primero en el menú Mitm seleccione **stop mitm attack** y del menú start seleccione **stop sniffing**.
15. En la ventana de captura de “wireshark” seleccione **“Stop”** para detenerla.
16. Analice los paquetes capturados viendo cómo funciona el ataque de envenenamiento de ARP.

Cuestionario

1. Ud. hace un ping a la dirección de loopback y no obtiene ningún mensaje de error. Sin embargo hace un ping a un host de su misma red y no puede obtener comunicación. Liste todas las razones por las cuales puede ocurrir este escenario.
2. ¿Qué ocurre con entrada estática en el cache ARP cuando se reinicia el computador? ¿Y cuando se reinicia una nueva sesión?
3. Suponga que Ud. envía un paquete ARP Request desde un Host A a un Host B. Se actualizarán los caches ARP de todos los hosts con el par: IP Host A, MAC A. Haga la prueba y realice una discusión sobre el tema.
4. ¿Por qué en lugar de utilizar el protocolo para el mapeo de una dirección IP a una dirección MAC, no se genera directamente un broadcast de capa MAC con el datagrama IP encapsulado? Argumente.
5. Si quisiera comunicarme con un host en otra subred, al intentar obtener la dirección física del mismo, que entrada se agregaría en el cache ARP?
6. Explique para que sería beneficioso el uso de envenenamiento de ARP.