Máster Universitario en Ciberseguridad e Inteligencia de Datos

Asignatura: Seguridad de las Comunicaciones Inalámbricas

Práctica 1: Entorno de trabajo auditoría de redes inalámbricas

1. Objetivo

El objetivo principal de esta práctica es familiarizarnos con el entorno de trabajo utilizado para la auditoría de redes Wi-Fi así como la configuración de los adaptadores de red y del propio sistema para futuras prácticas.

En la asignatura se recomienda utilizar KALI Linux para realizar las prácticas, aunque podría utilizarse cualquier otro sistema Linux siempre y cuando el alumno instale los paquetes necesarios.

2. Introducción teórica

2.1 Kali Linux y entornos de virtualización

La distribución Kali Linux se puede descargar desde la dirección:

https://www.kali.org/get-kali/#kali-platforms

Podemos optar por descargar la imagen ISO para instalar directamente sobre un ordenador, sobre un entorno de virtualización e incluso sobre entorno móvil sobre Android.

La opción más sencilla es utilizar una máquina virtual ya configurada para funcionar sobre VMWare, VirtualBox, Hyper-V o QEMU. Se pueden descargar desde aquí:

https://www.kali.org/get-kali/#kali-virtual-machines

En nuestro caso utilizaremos la máquina preparada para Virtual Box en versión 64 bits.

2.1.1 Instalación de VirtualBox

- Descargar la versión de VirtualBox adecuada a nuestro equipo:

  https://www.virtualbox.org/wiki/Downloads

  e instalamos con las opciones por defecto.

- Descargamos la imagen KALI Linux de la página indicada en el apartado anterior

- Desde VirtualBox cargamos la imagen de KALI a través del Menú Archivo->Importar servicio virtualizado, seleccionando el archivo .OVA de Kali

- A continuación, nos aparecerán las preferencias de la máquina, dejamos sus valores por defecto y pulsamos importar.
- El siguiente paso es seleccionar la máquina virtual y pulsar iniciar. Tras unos segundos

nos pedirá el nombre de usuario y contraseña, que son kali y kali respectivamente.

2.1.2 Alternativa para MacOS con chip Apple Silicon (M1/M2/M3/M4/M5)

En este caso, además de las soluciones comerciales como Parallels, una de las opciones es utilizar la máquina KALI sobre entorno CLOUD como AWS o AZURE.

Concretamente, en AZURE está disponible en:

https://azuremarketplace.microsoft.com/en/marketplace/apps/kali-linux.kali

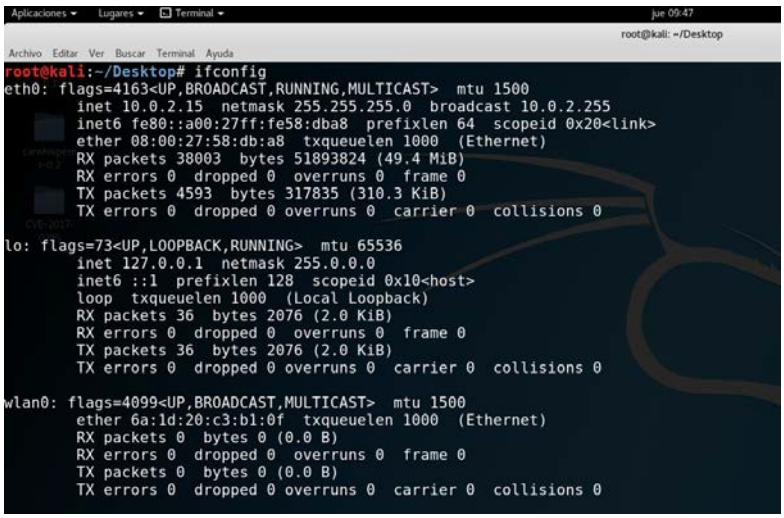
Nota: en el caso de usar Parallels, es necesario usar la imagen ISO de KALI para Apple Silicon(Arm64) desde: Get Kali | Kali Linux.

2.2 Configuración de adaptadores de red y comandos básicos

El objetivo de las primeras prácticas es familiarizarse con comandos útiles en ciberseguridad:

a. De descubrimiento y reconocimiento de redes (para información adicional consultar el documento anexo “Resumen Comandos útiles”):
   - `ipconfig/ifconfig/ip`
   - `ping`
   - `tracert/traceroute`
   - `arp / ip neigh`
   - `netstat /ss`
   - `whois`
   - `nmap`

ifconfig -> Este comando nos permite configurar y conocer diferentes parámetros de las interfaces de red. Para más información acerca del comando siempre podemos ver su manual: **man ifconfig**. **Si bien ya se encuentra en deshuso y se usará posteriormente el comando actual, sus salidas son bastante ilustrativas.**
Si queremos ver las interfaces de red que tenemos disponibles bastaría con poner **ifconfig** sin pasarle ninguna opción ni parámetro en la terminal.



Con esto nos aparecerían las interfaces de red disponibles en nuestra máquina. Podemos observar como aparecen 3. Los prefijos **eth**, **lo** y **wlan** hacen referencia a una interfaz eth, loopback y Wi-Fi respectivamente. Por otro lado, el número 0 en cada una de ellas simplemente enumera la interfaz, ya que podrían haber más de una interfaz del mismo tipo. La concatenación de los prefijos más los números definen el identificador de la interfaz

- Ahora vamos a cambiarle la dirección IP a nuestra interfaz de red Wi-Fi. Para ello ejecutamos el siguiente comando:

  ```
  ifconfig wlan0 10.0.0.32 netmask 255.255.255.0 up
  ```

- Para comprobar que se ha cambiado correctamente hacemos uso del comando de la siguiente forma:

  ```
  ifconfig wlan0
  ```

ping –> Este comando nos permite conocer si tenemos conectividad con otra máquina a través de su dirección IP o nombre de dominio. Este comando se suele utilizar para saber si una máquina es accesible o no.

```
root@kali:~# ping google.es
PING google.es (216.58.211.195) 56(84) bytes of data.

^C
--- google.es ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8172ms
```

traceroute -> Este comando nos permite conocer el camino que recorre un paquete a través de la red. Concretamente nos permite saber por qué máquinas (ordenadores, switches y routers) pasa nuestro paquete, permitiéndonos conocer el correcto funcionamiento de nuestra red.

```
traceroute 193.110.128.109
```

arp -> Este comando nos permite ver y modificar la tabla arp en nuestro dispositivo. Asocia direcciones IP y direcciones MAC. Sirve para ver que máquinas están conectadas con nosotros.

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali:~#
root@kali:~# arp -a
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on eth0
_gateway (192.168.0.1) at 94:4a:0c:3e:bb:a3 [ether] on wlan0
```

netstat -> Este comando nos permite ver todas las conexiones TCP y UDP abiertas en una máquina.

whois -> Este comando nos permite conocer datos sobre dominios. Entre ellos destacan el dueño del mismo, la fecha de expiración y los datos de contacto.

```
whois www.google.com
```

nmap -> Este comando nos permite escanear la red. Sirve para detectar los hosts de la red entre otros muchos usos.

2.3 Captura y análisis de paquetes

- tcpdump
- wireshark

tcpdump -> Este comando nos permite inspeccionar el tráfico de las diferentes interfaces de red para obtener los paquetes intercambiados. Se puede volcar a un fichero la salida para luego analizarla con otros sniffers más potentes y con interfaces gráficos como Wireshark.

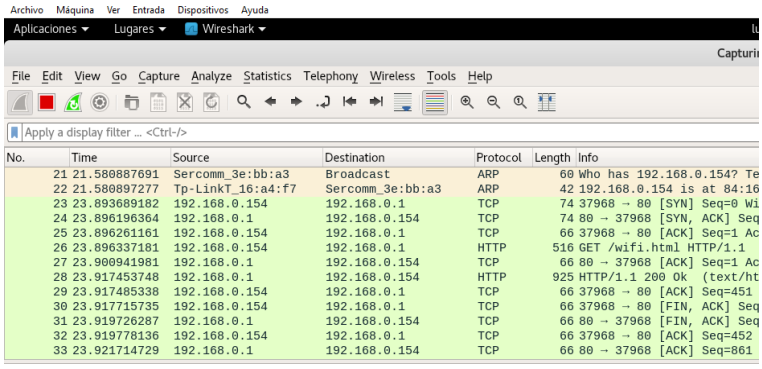
Wireshark es un software que nos permite capturar paquetes en redes. El objetivo es familiarizarnos con su uso para posteriores prácticas.

Para abrir Wireshark, en la terminal ejecutamos el siguiente comando:

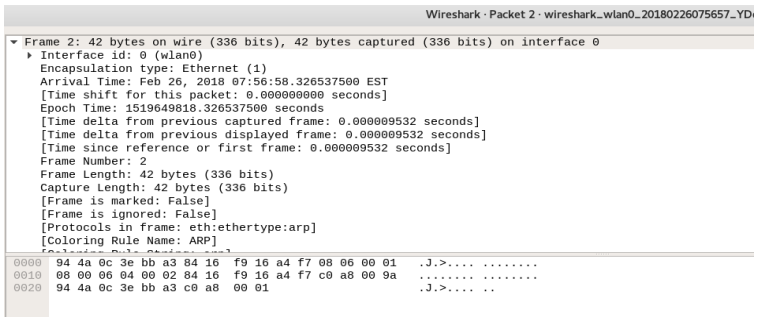
wireshark &

Una vez dentro de Wireshark seleccionamos la tarjeta de red en la que queremos capturar tráfico haciendo doble click sobre ella, en este caso wlan0. En este momento, automáticamente se comenzarán a capturar paquetes. Podemos abrir alguna página o ejecutar el comando ping a alguna página para generar más tráfico y verlo en Wireshark.

Como podemos ver en la siguiente imagen, Wireshark nos muestra el origen y destino de todos los paquetes capturados, el protocolo que utilizan, el tamaño y otros datos relativos a los paquetes capturados.



Además de esto, cuando hacemos doble click en un paquete podemos obtener información más detallada acerca del paquete capturado.



3. Desarrollo de la práctica en línea de comando

Deberá elaborarse un informe indicando la respuesta a cada uno de los siguientes apartados. En cada uno de ellos se debe copiar el enunciado de la pregunta y a continuación la respuesta a cada una de ellas.

a. *Análisis y Configuración de Interfaces de Red*

Arranque la máquina virtual de Kali Linux (por defecto usa usuario:kali/contraseña:kali). Inicie una terminal. Ejecute el comando correspondiente y observe las opciones disponibles.

- Consulte de Manual: Aunque el comando ifconfig es una herramienta heredada (legacy) de net-tools, su reemplazo moderno es ip. Investigue las opciones del comando principal:
  `$ man ip`
- Enumeración de Interfaces: Ejecute el siguiente comando para listar todas las interfaces de red y su configuración.
  `$ ip addr show`
  (Alternativamente, puede usar la forma abreviada $ ip a).

- Análisis de Atributos**:** Realice una enumeración de las interfaces de red activas (p.ej., eth0, lo). Para cada una, documente en su informe los siguientes atributos:
  - **Dirección de Control de Acceso al Medio (MAC):** El valor link/ether.
  - **Direcciones IP (Capa 3):** Las direcciones inet (IPv4) e inet6 (IPv6), observando la notación CIDR (p.ej., /24).
  - **Dirección de Difusión (Broadcast):** El valor brd.
  - **Estado de la Interfaz:** Si se encuentra operativa (STATE UP) o inactiva (STATE DOWN).
  - **Unidad Máxima de Transmisión (MTU):** El valor numérico mtu.

b. Gestión del Estado de la Interfaz y Escalado de Privilegios

La modificación del estado de una interfaz de red requiere privilegios elevados.

- Intento de Desactivación (Sin privilegios): Intente deshabilitar la interfaz de red principal.
  `$ ip link set eth0 down`
- Ejecución Privilegiada: Observe el error de "Permiso denegado". A continuación, utilice sudo (Substitute User DO) para ejecutar la operación con privilegios de superusuario (root).
  `$ sudo ip link set eth0 down`
- **Verificación de Conectividad:** Confirme que la interfaz está inactiva (usando $ ip a) y verifique la pérdida total de conectividad de red (p.ej., intentando acceder a un sitio web). Documente los resultados.
- Reactivación de la Interfaz: Restaure la interfaz a su estado operativo.
  `$ sudo ip link set eth0 up`

- Valide la restauración del servicio ($ ip a) y la conectividad a Internet

- Indique los comandos necesarios para realizar las siguientes acciones:

    a. Cambiar la IP a la eth0
    b. Asignar una nueva máscara de red a la eth0

c. Configuración de Direcciones IP Estáticas (Temporal vs. Persistente)

- **Asignación Temporal**: El comando ip permite la asignación volátil de direcciones, útil para pruebas. (Nota: esto requiere privilegios sudo).
  `$ sudo ip addr add 192.168.1.200/24 dev eth0`
  Esta configuración se perderá al reiniciar el sistema o la interfaz.

- **Configuración Persistente:** En sistemas basados en Debian como Kali, la configuración estática persistente se define en el fichero /etc/network/interfaces. Aunque la configuración automática por DHCP es estándar, es crucial entender cómo definir una IP estática, una máscara y una puerta de enlace (gateway) en este fichero para escenarios de servidores. **NOTA: Este apartado no requiere su inclusión en el informe ya que es únicamente informativo.**

d. Verificación de la Pila TCP/IP y Conectividad Externa

- Prueba de Loopback: Valide la correcta inicialización de la pila TCP/IP local mediante un ping a la interfaz de loopback (127.0.0.1).
  `$ ping -c 4 127.0.0.1`
  (El flag -c 4 limita el envío a 4 paquetes, similar al comportamiento por defecto en Windows).
- Prueba de Conectividad Externa: Verifique la resolución de nombres (DNS) y la conectividad a la WAN (Internet).
  `$ ping -c 4 www.ull.es`
  Analice la salida y documente:
  a. **Estadísticas de Paquetes:** Transmitidos, Recibidos, Pérdida (%).
  b. **Estadísticas de RTT (Round-Trip Time):** Mínimo, Promedio (Avg), Máximo.

e. Análisis de la Caché del Protocolo de Resolución de Direcciones (ARP)

El protocolo ARP traduce direcciones de Capa 3 (IP) a direcciones de Capa 2 (MAC) en la LAN.

- Inspección de la Caché: Inspeccione la tabla de vecinos (caché ARP) del sistema. Use el comando

  `$ arp -a`

  Dado que ya está obsoleto; ¿Qué alternativa hay usando el comando “ip” para obtener una salida equivalente a “arp”?
  Anote las entradas, observando el mapeo IP-MAC de dispositivos en su red, como la puerta de enlace (router).

f. Inspección de la Tabla de Enrutamiento

- Análisis de Rutas: Analice la tabla de enrutamiento del kernel para entender cómo el sistema decide dónde enviar el tráfico. El comando route -n está obsoleto; utilice:
  `$ ip route show`
  (Alternativamente, `$ ip r)`. Identifique la ruta por defecto (default via ...), que indica la dirección IP de su puerta de enlace.

g. Trazado de Ruta de Red (Traceroute)

- Trazado de Saltos: Realice un trazado de la ruta de Capa 3 para determinar los "saltos" (routers) intermedios entre su máquina y un destino.
  `$ traceroute www.ull.es`
  `$ traceroute www.net.berkeley.edu`
  Documente el número total de saltos para cada destino y observe la latencia en cada nodo.

h. Escaneo de Puertos Locales con Nmap

- Auto-descubrimiento: Ejecute un escaneo de Nmap contra la propia dirección IP de la máquina virtual (o localhost) para identificar los puertos que están escuchando (LISTENING) y los servicios asociados.
  `$ nmap -sV localhost`
  (El flag -sV intenta determinar la versión del servicio). Esto simula un reconocimiento inicial desde la perspectiva de un atacante en la misma red.

i. Análisis de Sockets y Conexiones de Red

- Enumeración de Sockets: Use inicialmente el comando `netstat`. No obstante, dado que está obsoleto, utilice también la herramienta moderna ss (socket statistics) para enumerar las conexiones activas.
  `$ ss -tulpn`
  Analice la salida en busca de puertos abiertos inesperados o conexiones remotas (ESTABLISHED) sospechosas.

j. Resolución de Nombres DNS (NSLookup)

- Consulta DNS: Utilice nslookup (o la herramienta más avanzada dig) para realizar consultas DNS.
  `$ nslookup www.ull.es`
  `$ nslookup www.w3c.org`
  Identifique y documente:
  - El **servidor DNS** que está resolviendo su consulta (indicado como Server:).
  - Los **registros "A"** (IPv4) resueltos para cada dominio.

k. Interacción de Red con Netcat (nc)

- Netcat es fundamental para la depuración y explotación de redes.

Revisión de Opciones: Investigue las opciones básicas:

```
$ nc -h
```

Sintaxis Clave: Documente la sintaxis para dos operaciones fundamentales:

- **Modo Escucha (Listener):** Iniciar un servicio que escuche en un puerto TCP específico (p.ej., `$ nc -l -p 1234`).
- **Modo Cliente:** Conectarse a un puerto TCP remoto.

l. Reconocimiento DNS Avanzado con dnsenum

- Enumeración de Dominio: Ejecute dnsenum para recopilar inteligencia de fuentes abiertas (OSINT) sobre un dominio.

  ```
  $ dnsenum tecnomobile.com
  ```

  Analice la salida para extraer información clave:

  i. Registros de Host (A/AAAA)
  ii. Servidores de Nombres (NS)
  iii. Servidores de Correo (MX)
  iv. Cualquier otra sub-enumeración que la herramienta complete con éxito.

m. Análisis de Tráfico en Terminal con tcpdump

- tcpdump es el analizador de paquetes de línea de comandos por excelencia.

Captura Básica: Inicie una captura de tráfico. Requiere privilegios sudo.

```
$ sudo tcpdump -i eth0 -n -c 20
```

- Explicación **:** -i eth0 (escucha en la interfaz eth0), -n (no resuelve nombres DNS/IPs), -c 20 (captura 20 paquetes y se detiene).
- Observe el flujo de tráfico en tiempo real.