Práctica de laboratorio - Rastreo de redes con Wireshark

Objetivos

En esta práctica de laboratorio, utilizará la utilidad de Linux **tcpdump** para capturar y guardar el tráfico de red. Luego utilizará Wireshark para investigar la captura de tráfico.

- Prepare el host para capturar el tráfico de red.
- Capture y guarde el tráfico de red.
- Ver y analizar la captura de paquetes.

Trasfondo / Escenario

Wireshark es una utilidad de captura de paquetes de red que pueden utilizar los administradores de red para solucionar problemas de red. También se puede utilizar para espiar las comunicaciones de red para recopilar pasivamente información sobre usuarios y servicios. Wireshark se considera una herramienta pasiva porque no crea tráfico en la red.

Recursos necesarios

- Kali VM personalizada para el curso de Ethical Hacker
- Acceso a Internet

Instrucciones

Parte 1: Preparar el host para capturar el tráfico de red.

Paso 1: Iniciar la máquina virtual e iniciar sesión

1. Inicie la máquina virtual de la estación de trabajo Kali. Utilicen las siguientes credenciales de usuario:

   Username: **kali**

   Password: **kali**
2. Inicie una sesión de terminal haciendo clic en el icono de terminal en la barra de menús.

Paso 2: Verificar el entorno.

1. Verifique el directorio de usuarios que se usará para almacenar el tráfico capturado. Para mostrar el directorio actual, use el comando **pwd** para mostrar la ruta completa al directorio de trabajo actual.

```
┌──(kali㉿Kali)-[~]
└─$ pwd
```

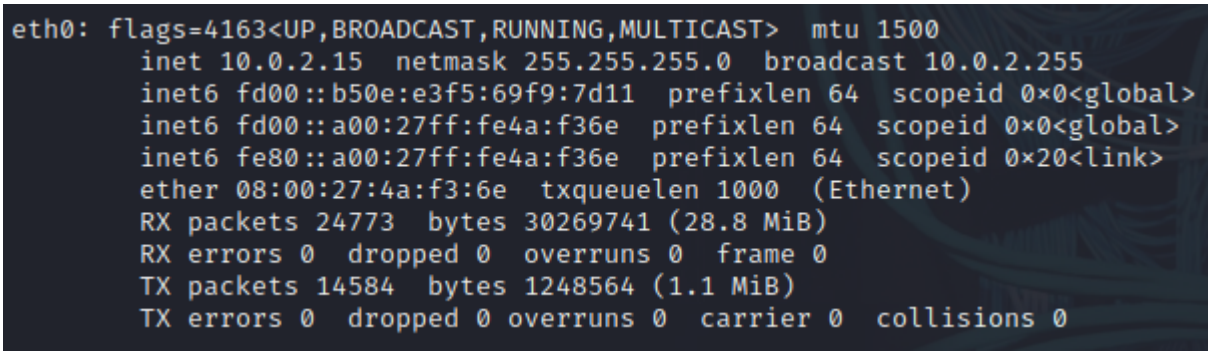
Registre la ubicación del directorio.

```
/home/kali
```

2. Determine la dirección IP de la interfaz Ethernet de Kali con el comando [**ifconfig**. La interfaz ethernet generalmente se denomina **eth0**.

```
┌──(kali㉿Kali)-[~]
└─$ ifconfig
```

Registre la dirección IP y la dirección MAC de la interfaz de red Ethernet. Esta será la dirección de origen de los paquetes que se originan en la máquina Kali.



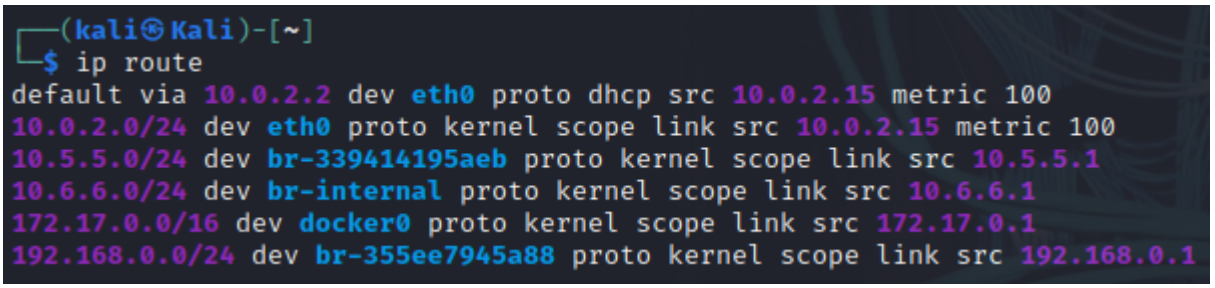

```
IP => 10.0.2.15

MAC => 08:00:27:4a:f3:6e
```

3. Determine la puerta de enlace predeterminada asignada al host Kali mediante el comando **ip route**.

```
┌──(kali㉿Kali)-[~]
└─$ ip route
```

Registre la dirección IP de la puerta de enlace predeterminada. La puerta de enlace predeterminada responde a las solicitudes ARP de direcciones IP de destino ubicadas fuera de la red de origen.



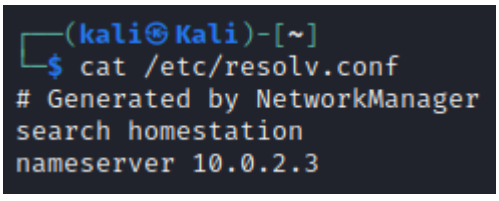

```
Gateway => 10.0.2.2
```

Nota: La dirección IP de la puerta de enlace predeterminada debe estar en la misma subred IP que la dirección de la interfaz Ethernet.

4. Determine la dirección del servidor DNS predeterminado configurado mostrando el contenido del archivo `/etc/resolv.conf`. Puede ver el archivo con el comando `cat` .

```
    cat /etc/resolv.conf
```

Registre la dirección IP del servidor DNS predeterminado configurado. La dirección IP del servidor DNS será la dirección de destino de los paquetes de consulta estándar y la dirección de origen de los paquetes de respuesta DNS.




```
IP Server DNS => 10.0.2.3
```

Parte 2: Capturar y guardar el tráfico de red.

En esta parte utilizarán **tcpdump** para capturar el contenido del tráfico HTTP. Utilizarán opciones de comandos para guardar el tráfico en un archivo de captura de paquetes (pcap). Estos registros se pueden analizar posteriormente con diferentes aplicaciones que leen archivos pcap, incluida Wireshark.

Paso 1: Abrir un terminal e iniciar tcpdump

1. Abra una aplicación del terminal e introduzca el comando **ifconfig**.

   ┌──(kali㉿Kali)-[~]

   └─$ **ifconfig**
2. En la salida **ifconfig**, busque el nombre de la interfaz que corresponde al adaptador Ethernet (generalmente eth0). Haga clic con el botón derecho en el nombre de la

interfaz y seleccione **Copy Selection** (Copiar selección).

3. Ingrese el comando **sudo tcpdump** como se muestra. Reemplace el texto ***<interface>*** con el nombre de la interfaz que copió en el paso anterior. Este comando requiere acceso de usuario root, así que introduzca **kali** como contraseña si se le solicita.

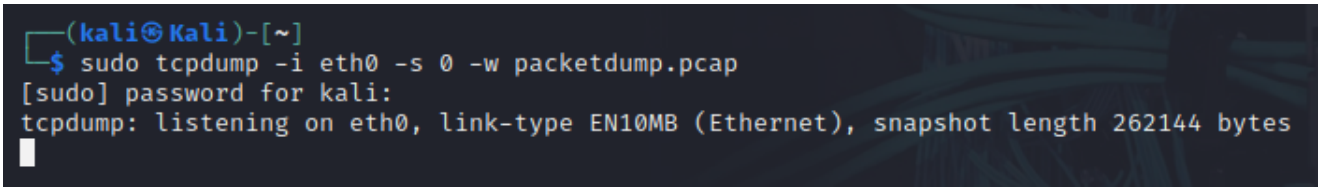
   ┌──(kali㉿Kali)-[~]

   └─$ **sudo tcpdump -i eth0 -s 0 -w packetdump.pcap**

   La opción de comando **-i** le permite especificar la interfaz. Si no se la especifica, tcpdump capturará todo el tráfico en todas las interfaces.

   La opción de comando **-s** especifica la longitud de la instantánea correspondiente a cada paquete. Al establecer esta opción en 0, se establece el valor predeterminado de 262144.

   La opción de comando **-w** se utiliza para escribir el resultado del comando **tcpdump** en un archivo. Si se agrega la extensión **.pcap**, se garantiza que los sistemas operativos y las aplicaciones podrán leer el archivo. Todo el tráfico registrado se imprimirá al archivo **httpsdump.pcap**, en el directorio de inicio del usuario.



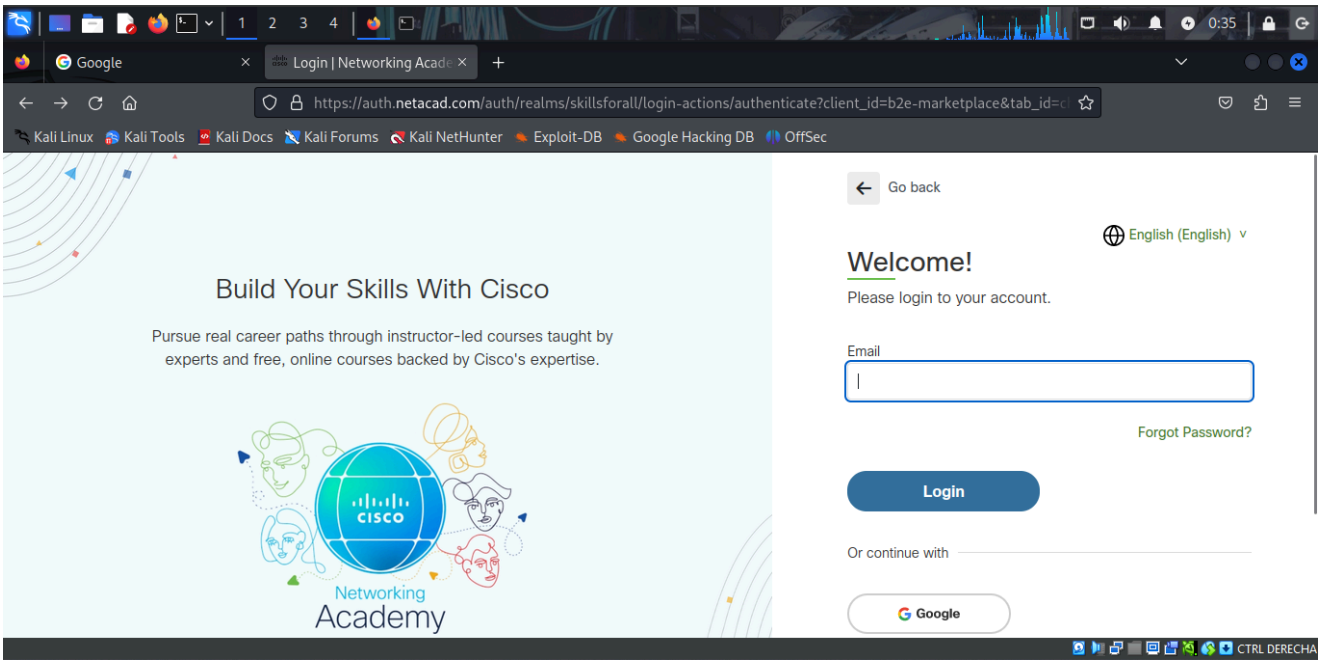
Paso 2: Generar tráfico de red mediante un navegador web.

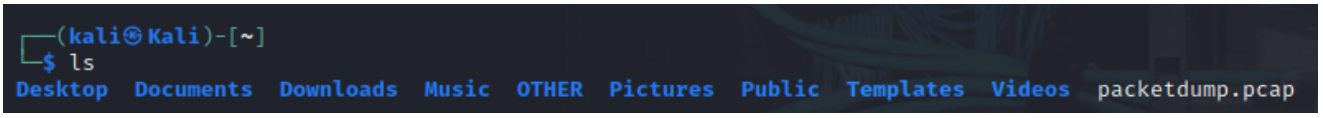
1. Para capturar una solicitud y una respuesta HTTP, abra un navegador web en el escritorio de Kali. Vaya a **Google.com**. No inicie sesión ni busque.
2. Abra una segunda pestaña en el navegador, ingrese **skillsforall.com** en la barra de inicio. Una vez que aparezca la página, haga clic en el icono de usuario en la parte superior derecha de la página. Inicie sesión con su información de inicio de sesión de skillsforall.
3. Regrese a la ventana de terminal que ejecuta la utilidad **tcpdump** e ingrese **CTRL-C** para completar la captura de paquetes.
4. La utilidad tcpdump guardó la salida en un archivo denominado **packetdump.pcap**. Este archivo debe guardarse en el directorio de inicio predeterminado. Verifique que el archivo exista en el directorio mediante el comando **ls**.

   ┌──(kali㉿Kali)-[~]

   └─$ **ls packetdump.pcap**

```
packetdump.pcap
```





Parte 3: Ver y analizar la captura de paquetes.

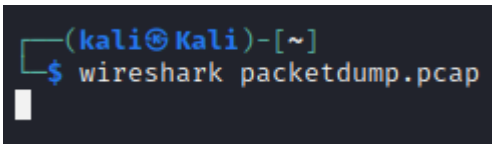
En esta parte, usará Wireshark para analizar el archivo de captura de paquetes que creó en la parte 2 de esta práctica de laboratorio.

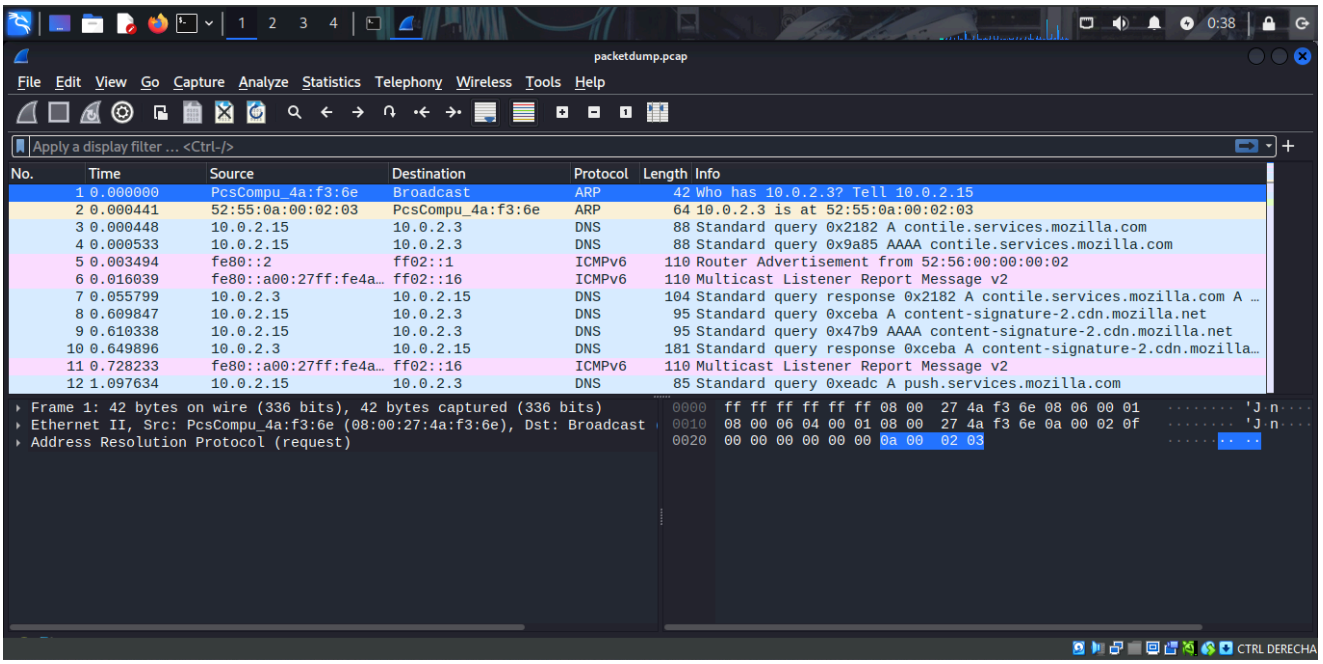
Paso 1: Abra la aplicación Wireshark para ver la captura de paquetes.

1. Utilice Wireshark para ver los paquetes capturados. Inicie la aplicación gráfica Wireshark escribiendo **wireshark** en el indicador de la CLI.

   ```
   ┌──(kali㉿Kali)-[~]
   └─$ wireshark
   ```

   La aplicación Wireshark debería abrirse en una ventana diferente. Expanda la ventana de Wireshark a pantalla completa.
2. Utilice la opción de menú **File -> Open** e introduzca **packetdump.pcap** en el campo Nombre de archivo. Haga clic en **Open** (Abrir). Debe abrirse una pantalla que muestre el contenido del archivo **packetdump.pcap**.



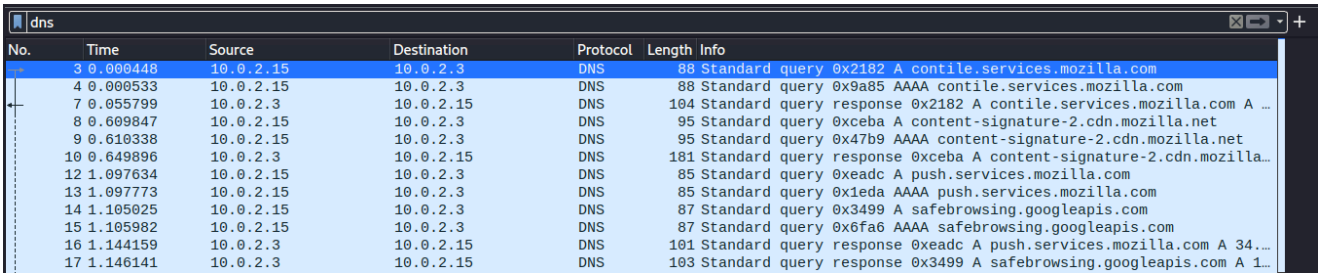


Paso 2: Analizar el tráfico DNS.

Cuando se escribe la URL de un sitio web en el navegador, la PC realiza una consulta de DNS a la dirección IP del servidor DNS. La observación de las consultas y respuestas del DNS proporciona los nombres (URL) y las direcciones IP de los sitios que visita un usuario. Conocer los sitios web que los usuarios visitan comúnmente puede ser valioso al formular ataques de ingeniería social.

1. Filtre el tráfico capturado para mostrar solo las consultas y respuestas de DNS. Introduzca **dns** en el campo Filtro de la pantalla principal de Wireshark. Observará que, además del sitio web **skillsforall** que solicitó, se muestran otras búsquedas de DNS. Corresponden a enlaces contenidos en las páginas de inicio de skillsforall y Google.

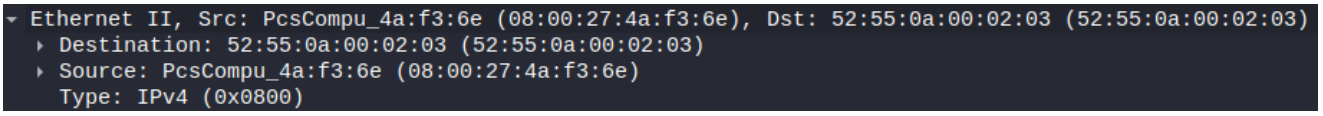
¿Cuáles son algunos de los sitios web que se enumeran en las consultas estándar de DNS?



2. Haga clic en el icono de búsqueda y busque el nombre de host **skillsforall**.com. Seleccione **String** en el cuadro desplegable e ingrese **skillsforall** en el cuadro de búsqueda.
3. Seleccione la primera consulta estándar para el sitio web **skillsforall.com**. Expanda el panel de detalles de la consulta debajo de la lista de paquetes para ver el contenido del paquete de consulta.

4. Expanda la información de **Ethernet II** para mostrar los datos del encabezado de capa 2 contenidos en el paquete. La dirección MAC de origen es la MAC de la interfaz del dispositivo de envío, en este caso la VM Kali, y la dirección MAC de destino es la MAC de la puerta de enlace predeterminada, ya que el servidor DNS no está en la misma red de capa 2.

¿La dirección MAC de origen coincide con la dirección que registró en la parte 1?



5. Expanda la sección **Domain Name System (query)** para ver los detalles de lo que se envía al servidor DNS. También indica la línea que contiene el paquete de respuesta que se recibió en respuesta a la consulta. Haga doble clic en el enlace a la respuesta. Se muestran los detalles del paquete de respuesta a la consulta estándar.

¿Qué direcciones IP están asociadas con la URL skillsforall.com?

```
3.160.90.39
3.160.90.31
3.160.90.104
3.160.90.56
```

6. Cierre Wireshark para volver al indicador de la CLI.

Paso 3: Analizar una sesión HTTP

En este paso, capturará y analizará una solicitud y una respuesta web. Utilizará Wireshark para capturar el tráfico y analizar los mensajes intercambiados entre el servidor web y el cliente. El servidor del sitio web es un servidor de VM que se ejecuta en un contenedor de Docker en el host de Kali Linux.

1. Utilice **ifconfig** para determinar qué interfaz de la VM Kali Linux está configurada en la red 10.6.6.0/24.

   ┌──(kali㉿Kali)-[~]

   └─$ **ifconfig**

¿Cuál es el nombre de la interfaz conectada a la red 10.6.6.0/24?

```
br-internal: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.6.6.1  netmask 255.255.255.0  broadcast 10.6.6.255
        inet6 fe80::42:13ff:feb8:c649  prefixlen 64  scopeid 0x20<link>
        ether 02:42:13:b8:c6:49  txqueuelen 0  (Ethernet)
        RX packets 11301  bytes 1214086 (1.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12240  bytes 1362129 (1.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

¿Cuál es la dirección IP asignada a esa interfaz?

```
10.6.6.1
```

2. Abra Wireshark escribiendo **wireshark** en la línea de comandos. Wireshark se abrirá en una nueva ventana, expandirá la ventana a pantalla completa. En el centro de la pantalla principal de Wireshark habrá una lista de nombres de interfaz para capturar el tráfico. Haga doble clic en el nombre de la interfaz que coincida con el nombre de la interfaz que descubrió en el paso 2a.
3. Abra una ventana del navegador e ingrese la dirección IP 10.6.6.13 en la barra de inicio. Aparece una pantalla de inicio de sesión para el servidor web DVWA.
   Escriba **admin** tanto como nombre de usuario y la **contraseña**.

   Username: **admin**

   Password: **password**
4. Cuando aparezca la página principal de DVWA, haga clic en el botón **Instructions** en la parte superior del menú en el lado izquierdo de la pantalla. Cuando aparezca la página de instrucciones, cierre la ventana del navegador.
5. Regrese a la ventana de Wireshark. Detenga la captura con el **icono cuadrado rojo** en la barra de menús. El servidor web DVWA utiliza HTTP, no HTTPs. Utilice el **icono de búsqueda** para encontrar la cadena **POST** en los paquetes capturados. Los mensajes POST transfieren datos del formulario del cliente al servidor, en este caso la información de inicio de sesión.
6. Haga doble clic en el primer paquete POST para ver los detalles en una ventana separada. Expanda la sección titulada **HTML Form URL Encoded**:

¿Qué información contiene esta sección?

- Nombre de usuario
- Contraseña
- User_token

```
Al no usar un protocolo cifrado, losd atos de este estilo aparecen en texto plano y son vulnerables al secuestro.
```

7. Las cookies se utilizan para diversos fines. Con mayor frecuencia, se utilizan para guardar información sobre la sesión de un usuario. Las cookies pueden ser secuestradas y utilizadas en ataques de secuestro de sesiones. La cookie inicial para una sesión se envía desde el servidor web al cliente con el valor **Set-Cookie** en una respuesta HTTP. Utilice el icono de búsqueda para encontrar la cadena **302 Found** en el panel de paquetes. Haga doble clic en el primer paquete encontrado y expanda la sección **Hypertext Transport Protocol**.

¿Qué valor se establece en la cookie que se envía desde el servidor web al cliente Kali?

```
PHPSESSID => El uso de `PHPSESSID` revela que el backend es PHP y que se manejan sesiones nativas. Esto indica probable almacenamiento en disco (como `/var/lib/php/sessions`) y cookies sin cifrado si no están bien configuradas. Se puede investigar session fixation, hijacking o incluso si el ID es predecible. Si no se renueva tras login, hay riesgo de fijación. Desde Burp se podrá analizar flags de seguridad y comportamiento del token.
```

8. Examine el siguiente paquete **GET** que se envía desde el navegador del cliente Kali después de recibir la información de la cookie. Expanda la sección **Hypertext Transport Protocol**. Busque los valores de cookie que se envían en el paquete.

¿El PHPSESSID que se envía de vuelta al servidor en la solicitud GET es el mismo que el enviado desde el servidor en la respuesta anterior?

```
RTA => Sí
```

9. Cierre Wireshark. Tendrá la opción de guardar el archivo `.pcap` que contiene la captura o salir sin guardar. El archivo `.pcap` se guardará en el directorio de trabajo actual a menos que se especifique lo contrario.

Preguntas de reflexión

1.En esta práctica de laboratorio, tuvo la oportunidad de familiarizarse con la captura de paquetes tanto en la utilidad `tcpdump` como en la aplicación Wireshark. ¿Cuáles son los beneficios de utilizar las utilidades de captura de paquetes al realizar un reconocimiento pasivo en un objetivo potencial?

```
Las herramientas como tcpdump y Wireshark permiten observar el tráfico sin interactuar directamente con el objetivo, lo que resulta importante en un
```

reconocimiento pasivo. Ayudan a detectar si el tráfico está cifrado o si se transmite en texto plano, lo que revela posibles vulnerabilidades.
Permiten identificar comportamientos anómalos que podrían indicar ataques tipo MITM o fugas de información.
Verifican si los paquetes realmente llegan a destino y cómo responden los servicios del objetivo.
También muestran protocolos en uso, ayudando a perfilar la infraestructura y posibles vectores de ataque.

2.¿Qué información se puede recopilar mediante la captura de paquetes?

Mediante la captura de paquetes se puede obtener información valiosa como direcciones IP, protocolos usados y dominios accedidos.
También se pueden detectar credenciales si el tráfico no está cifrado, como en formularios HTTP o peticiones básicas de autenticación.
Observar patrones de navegación permite preparar ataques personalizados como spear phishing o watering hole (bebedero).
Se identifican dispositivos y sistemas operativos por su comportamiento en red, ayudando al fingerprinting (identificar detalles técnicos de un sistema o aplicación, sin necesidad de acceder directamente a ellos).
Incluso pueden revelarse datos sensibles como correos, chats o tokens si no hay medidas de protección adecuadas.