Práctica de laboratorio: Extraer un ejecutable de un PCAP

Objetivos

Parte 1: Analizar archivos de registros precapturados y capturas de tráfico

Parte 2: Extraer archivos descargados desde archivos PCAP

Aspectos básicos/Situación

Analizar registros es muy importante, pero también lo es comprender de qué manera suceden las transacciones de red al nivel de los paquetes.

En esta práctica de laboratorio analizará el tráfico de un archivo pcap previamente capturado y extraerá un ejecutable del archivo.

Recursos necesarios

- Máquina virtual CyberOps

Instrucciones

Parte 1: Analizar archivos de registros precapturados y capturas de tráfico

En la Parte 2 trabajará con el archivo **nimda.download.pcap**. Capturado en una práctica de laboratorio anterior, **nimda.download.pcap** contiene los paquetes relacionados con la descarga del malware Nimda. Si crearon el archivo en la práctica de laboratorio anterior y no reimportaron sus VM CyberOps Workstation, sus versiones del archivo se almacenarán en el directorio /home/analyst. Sin embargo, también se almacena una copia de ese archivo en la **VM CyberOps** Workstation en el directorio **/home/analyst/lab.support.files/pcaps**, así que podrá realizar esta práctica de laboratorio independientemente de que haya terminado la práctica anterior o no. A fines de preservar la coherencia del resultado, en la práctica de laboratorio se utilizará la versión almacenada en el directorio **pcaps**.

Si bien **tcpdump** se puede utilizar para analizar archivos capturados, la interfaz gráfica de **Wireshark** facilita mucho la tarea. También es importante tener en cuenta que **tcpdump** y **Wireshark** comparten el mismo formato de archivo para las capturas de paquetes; por lo tanto, los archivos PCAP creados con una herramienta se pueden abrir con la otra.

a. Cambie de directorio para ingresar a la carpeta **lab.support.files/pcaps**, y genere un listado de los archivos con el comando **ls –l**.

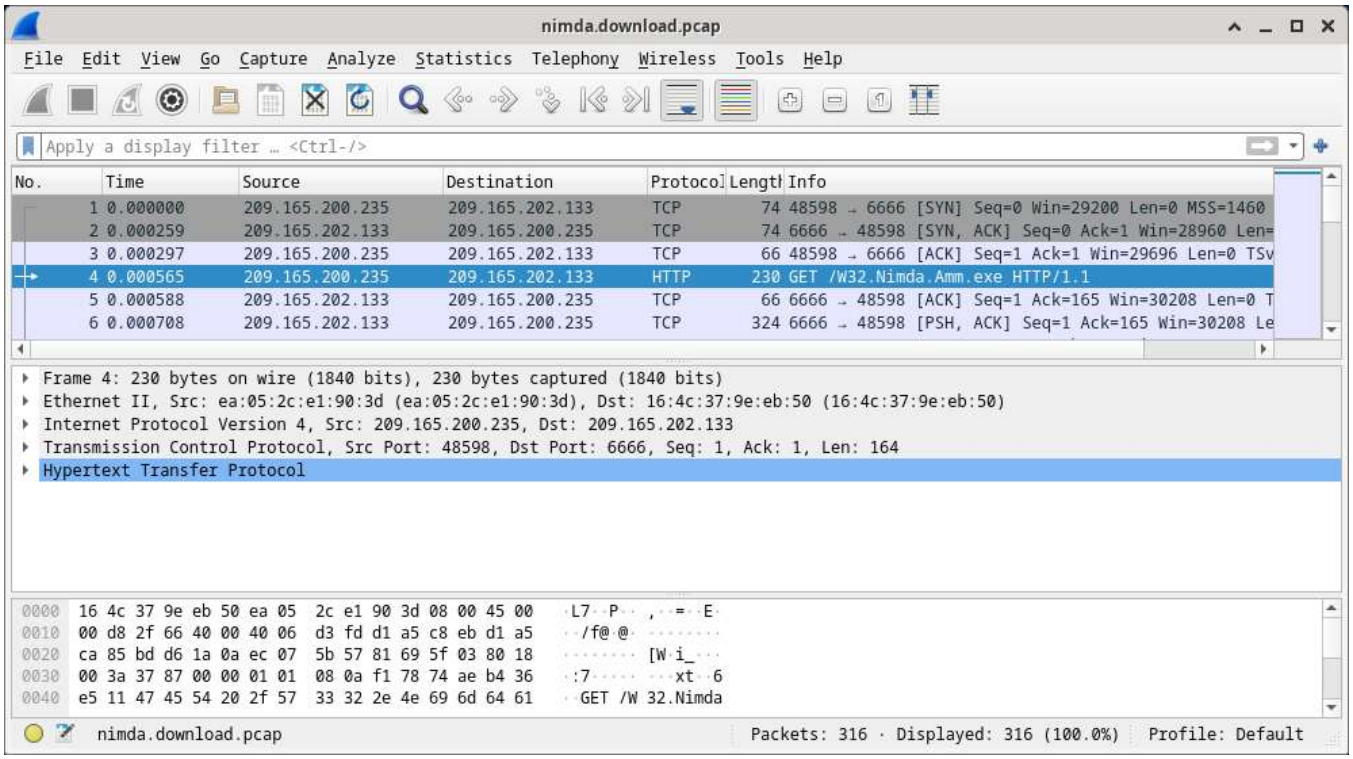
```
[analyst@secOps ~]$ cd lab.support.files/pcaps
[analyst@secOps pcaps]$ ls -l
total 7460
-rw-r--r-- 1 analyst analyst 3510551 Aug 7 15:25 lab_prep.pcap
-rw-r--r-- 1 analyst analyst 371462 Jun 22 10:47 nimda.download.pcap
-rw-r--r-- 1 analyst analyst 3750153 May 25 11:10 wannacry_download_pcap.pcap
[analyst@secOps pcaps]$
```

b. Emita el siguiente comando para abrir el archivo **nimda.download.pcap** en Wireshark.

```
[analyst@secOps pcaps]$ wireshark nimda.download.pcap &
```

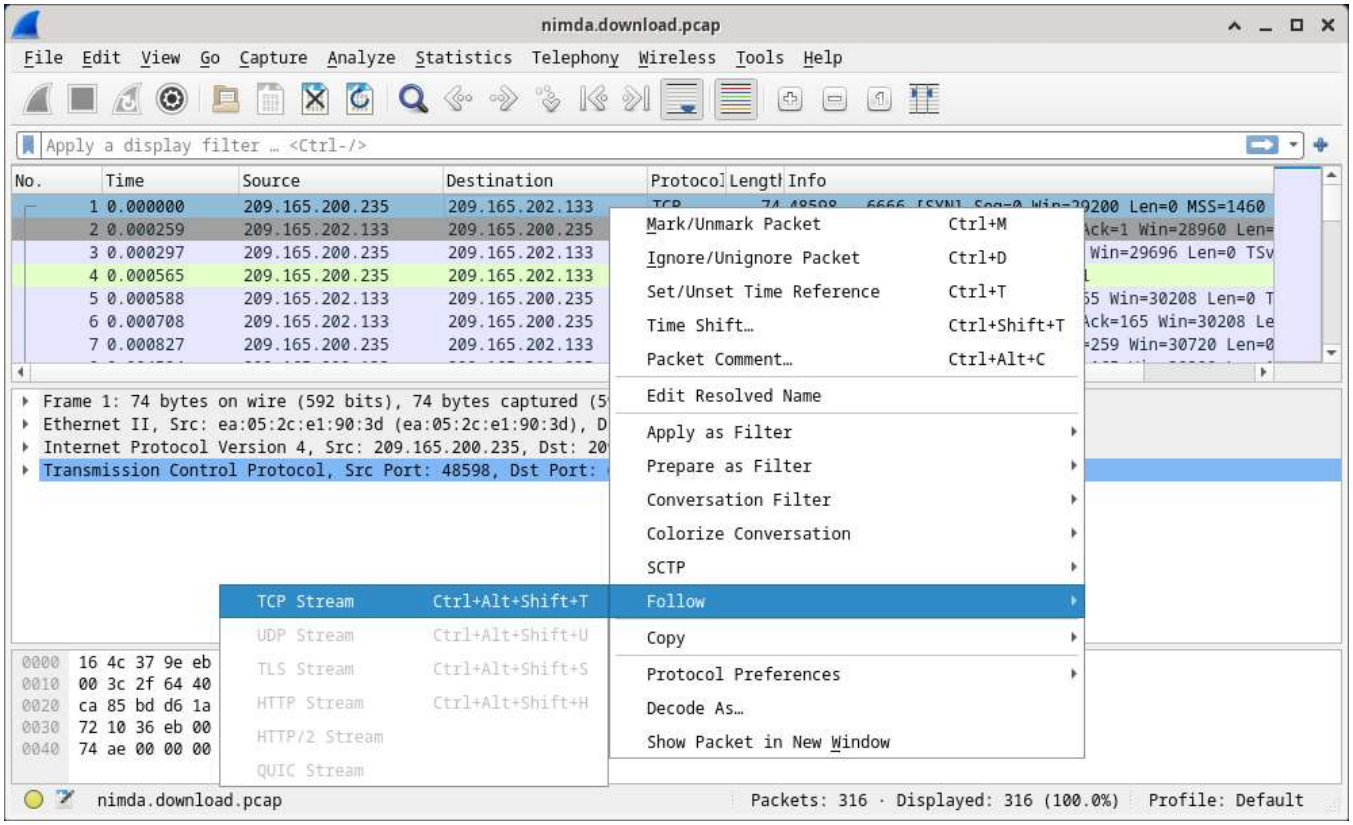
c. El archivo **nimda.download.pcap** contiene la captura de paquetes relacionadas con la descarga de malware que se realizó en la práctica de laboratorio anterior. El **pcap** contiene todos los paquetes enviados y recibidos mientras se estaba ejecutando **tcpdump**. Seleccione el cuarto paquete de la

captura y expanda el Protocolo de transferencia de hipertexto (HTTP) para que aparezca como se indica a continuación.

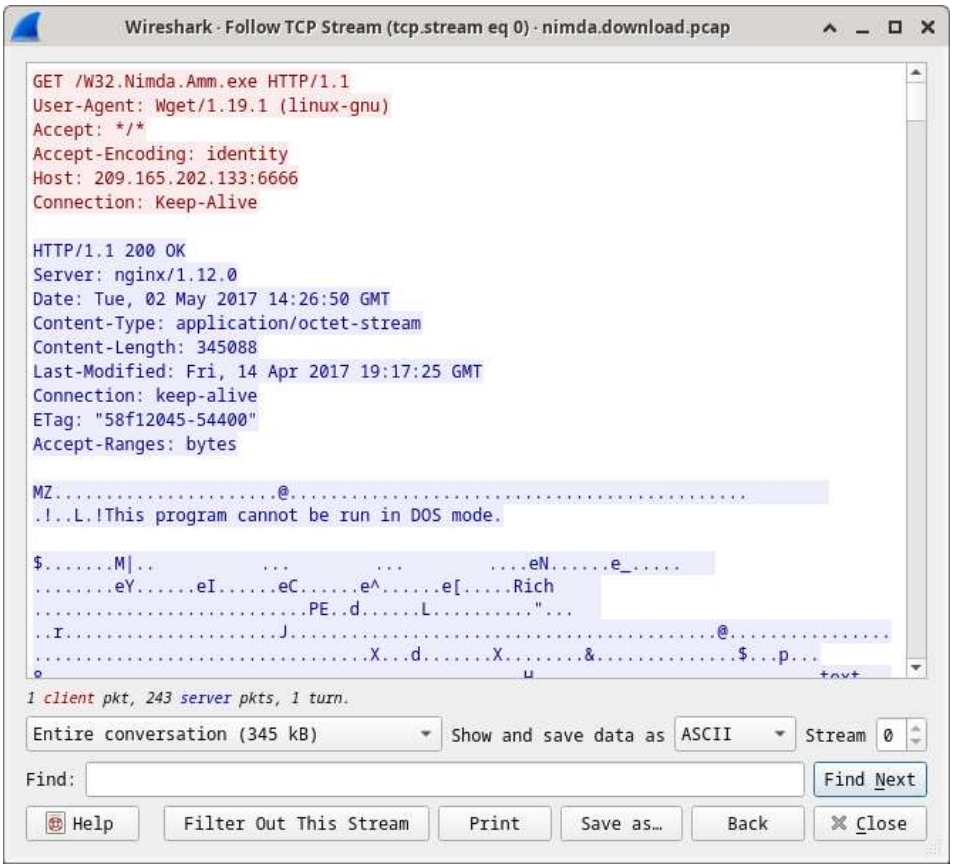


d. Los paquetes del uno al tres son la el protocolo de enlace TCP. En el cuarto paquete se muestra la solicitud correspondiente al archivo de malware. A modo de confirmación de lo que ya se sabía, la solicitud se realizó por HTTP, y se envió como solicitud GET.

e. Como HTTP se ejecuta por TCP, se puede utilizar la característica **Follow TCP Stream (Seguir flujo de TCP)** de **Wireshark** para reconstruir la transacción TCP. Seleccione el primer paquete TCP de la captura; es un paquete SYN. Haga clic derecho y elijan **Follow** >**TCP Stream**.



f. En Wireshark se abre otra ventana con los detalles correspondientes a todo el flujo de TCP seleccionado.



¿Qué son todos esos símbolos que se ven en la ventana de **Follow TCP Stream**? ¿Son interferencias de conexión? ¿Son datos? Explique.

Se pueden distinguir algunas palabras dispersas entre los símbolos. ¿Por qué están allí?

Pregunta de desafío: Pese al nombre **W32.Nimda.Amm.exe**, este ejecutable no es el famoso gusano. Por motivos de seguridad, se trata de otro archivo ejecutable al que se le cambió el nombre a **W32.Nimda.Amm.exe. Si utilizan los fragmentos de las palabras que se muestran en la ventana de Follow TCP Stream** de Wireshark, ¿puede decir de qué ejecutable se trata en realidad?

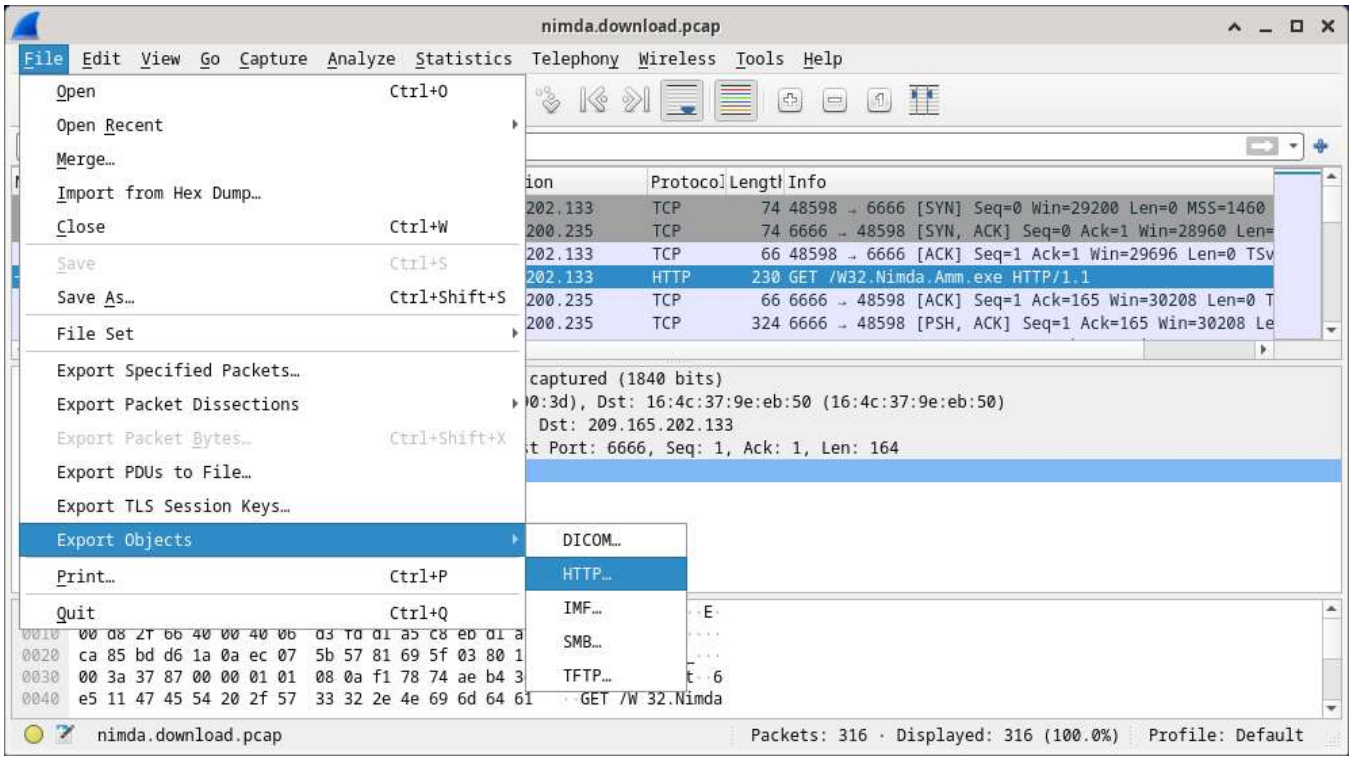
g. En la ventana de Follow TCP Stream, haga clic en **Close** (Cerrar) para regresar al archivo nimda.download.pcap de Wireshark.

Parte 2: Extraer archivos descargados desde archivos PCAP

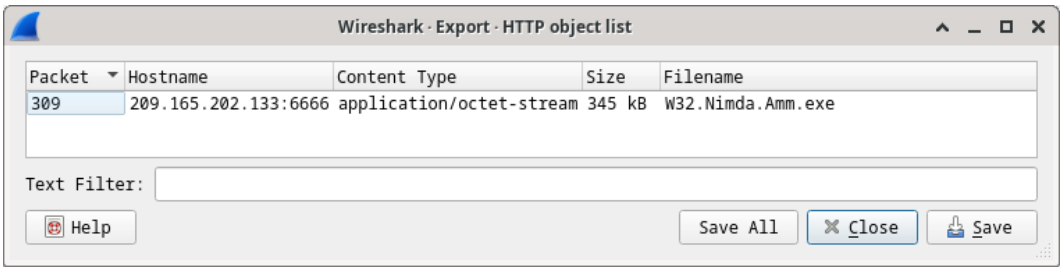
Como los archivos de capturas contiene paquetes relacionados con el tráfico, se puede utilizar un PCAP de una descarga para recuperar un archivo descargado anteriormente. Siga los pasos que se detallan a continuación para utilizar **Wireshark** y recuperar el malware Nimda.

a. En ese cuarto paquete del archivo **nimda.download.pcap**, observe que la solicitud **HTTP GET** se generó desde **209.165.200.235** hacia **209.165.202.133**. En la columna Info (Información) también se ve que de hecho se trata de la solicitud GET correspondiente al archivo.

b. Con el paquete de la solicitud GET seleccionado, diríjase a **File > Export Objects > HTTP** (Archivo > Exportar objetos > HTTP) desde el menú de **Wireshark**.



c. En Wireshark se mostrarán todos los objetos HTTP presentes en el flujo TCP que contiene la solicitud GET. En este caso, el único archivo presente en la captura es **W32.Nimda.Amm.exe**. El archivo aparecerá en pantalla después de algunos segundos.



¿Por qué **W32.Nimda.Amm.exe** es el único archivo presente en la captura?

d. En la ventana **HTTP object list** (Lista de objetos HTTP), seleccione el archivo **W32.Nimda.Amm.exe** y haga clic en **Save As** (Guardar como), en la parte inferior de la pantalla.

e. Haga clic en la flecha hacia la izquierda hasta ver el botón **Home** (Inicio). Haga clic en Home y luego en la carpeta **analyst** (no en la ficha analyst). Guarde el archivo allí.

f. Regrese a su ventana del terminal y asegúrese de que el archivo se haya guardado. Cambie de directorio para ingresar a la carpeta **/home/analyst** y genere una lista de los archivos de la carpeta con el comando **ls -l**.

```
[analyst@secOps pcaps]$ cd /home/analyst
[analyst@secOps ~]$ ls -l
total 364
drwxr-xr-x 2 analyst analyst 4096 Sep 26 2014 Desktop
drwx------ 3 analyst analyst 4096 May 25 11:16 Downloads
drwxr-xr-x 2 analyst analyst 4096 May 22 08:39 extra
drwxr-xr-x 8 analyst analyst 4096 Jun 22 11:38 lab.support.files
drwxr-xr-x 2 analyst analyst 4096 Mar 3 15:56 second_drive
-rw-r--r-- 1 analyst analyst 345088 Jun 22 15:12 W32.Nimda.Amm.exe
[analyst@secOps ~]$
```

¿Se guardó el archivo?

g. El comando **file** proporciona información sobre el tipo de archivo. Utilice el comando file para averiguar un poco más sobre el malware, tal como se indica a continuación:

```
[analyst@secOps ~]$ file W32.Nimda.Amm.exe
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
[analyst@secOps ~]$
```

Tal como se ve arriba, **W32.Nimda.Amm.exe** realmente es un archivo ejecutable de Windows.

En el proceso del análisis de malware, ¿cuál sería un próximo paso probable para un analista especializado en seguridad?