Práctica 2: Análisis de una Traza de Paquetes



**INGENIERÍA DE LA CIBERSEGURIDAD**

Octubre 2023

Grado en Ingeniería Informática

Pablo Brasero Martínez. NIA: 100451247

Miguel Castuera García. NIA: 100451285

**Índice**

[**1. trace\_1.pcap**](#_85hsq7ro9oh7) **3**

[a. ¿Cuál es el protocolo de aplicación más prevalente en la traza?](#_fqy39nhxx16x) 3

[b. ¿Cuáles son las direcciones IP y puertos del cliente y el servidor?](#_2v5te7f6klin) 3

[c. ¿Qué tipo y versión de servidor se está ejecutando?](#_x2fqk0slcyaz) 4

[d. Escriba un filtro que muestre el primer paquete TCP de cada flujo en la traza](#_4jn5kbo2v00v) 4

[e. Observando la traza globalmente, ¿cuál cree que es el objetivo del cliente?](#_fmrb4mw3mxru) 4

[**2. trace\_2.pcapng**](#_o9nnfpykp88k) **5**

[a. Describa cuántas conversaciones TCP y UDP hay en la traza y cuántos hosts hay involucrados](#_xhk2f9tg477x) 5

[b. Analizando globalmente la traza, ¿qué está haciendo el host con dirección IP 192.168.5.51?](#_bsx4gy4ymbbp) 5

[c. Enumere todas las técnicas que el host con dirección IP 192.168.5.51 está usando.](#_pvt4brr1rk37) 6

[d. ¿Qué puertos hay abiertos en el host con dirección IP 192.168.5.20?](#_ca7eff6i4qej) 6

[**3. trace\_3.pcapng**](#_hvxs1od4p5yn) **7**

[a. Escriba un filtro que muestre todas las conversaciones HTTP en la traza](#_ptpa4ultx75f) 7

[b. Describa toda la información que pueda averiguar sobre el servidor y el cliente HTTP](#_t1is6wf4qj15) 7

[c. Obtenga las contraseñas (en texto en claro) de las cabeceras HTTP Authorization contenidas en la traza](#_2dnih2577rmu) 8

[**4. trace\_4.pcap**](#_t7e7s7xky6ks) **9**

[a. Esta traza de red contiene una infección por malware de un host Windows. Proporcione la fecha y hora de esta actividad.](#_6wpyydxd6rwb) 9

[b. Indique las direcciones IP y MAC y el nombre del host que es infectado](#_6ntgqcxvj9so) 9

[c. ¿Cuál es el nombre de dominio y la dirección IP del sitio web comprometido?](#_sp1hdvr5vi1n) 9

[d. ¿Cuál es el nombre de dominio e IP del sitio web desde el que se descarga el malware?](#_nv89yfwnoumi) 9

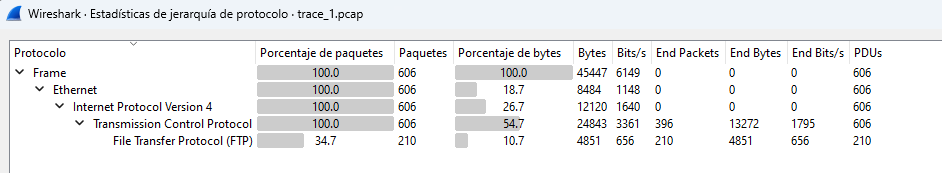
[e. ¿Qué navegador utiliza el host Windows que es infectado?](#_ymtbg3b1pmw1) 9

[f. Tras la infección, el malware utiliza comunicaciones HTTP. ¿Qué método (GET o POST) utiliza?](#_nvu1bd68jbsn) 10

# **trace\_1.pcap**

## ¿Cuál es el protocolo de aplicación más prevalente en la traza?

Para la realización de este apartado, con el archivo cargado en el programa, nos dirigimos al apartado de “Estadísticas” dentro del programa y ahí pulsamos en “Jerarquía de protocolo”, ahí encontraremos la siguiente ventana:



Podemos observar como el protocolo más prevalente es el de Transmisión Control Protocol (TCP)

## ¿Cuáles son las direcciones IP y puertos del cliente y el servidor?

|  | Como se puede observar en esta imagen, todas las comunicaciones están realizadas entre 2 extremos, las ip 192.168.56.1 y la ip  192.168.56.101. Esto nos da a entender que se trata de una comunicación entre cliente y servidor. |
| --- | --- |

Esto se puede confirmar si entramos a la pestaña “Conversaciones” dentro de “Estadísticas”, en la cual veremos la siguiente información:



Con está información, podemos asumir que el la Dirección A es el cliente y la Dirección B es el servidor. Esto es así puesto que en el concepto de redes que estamos tratando, el cliente el siempre el que establece la conversación y envía el primer paquete, cosa que podemos observar al fijarnos en la primera captura, viendo que la primera source es la dirección 192.168.56.1 es decir la Dirección A

## ¿Qué tipo y versión de servidor se está ejecutando?

El tipo y versión del servidor se puede identificar por las respuestas que envía el servidor al cliente, por lo que podemos determinar esto gracias a la línea 4 de información de la comunicación:

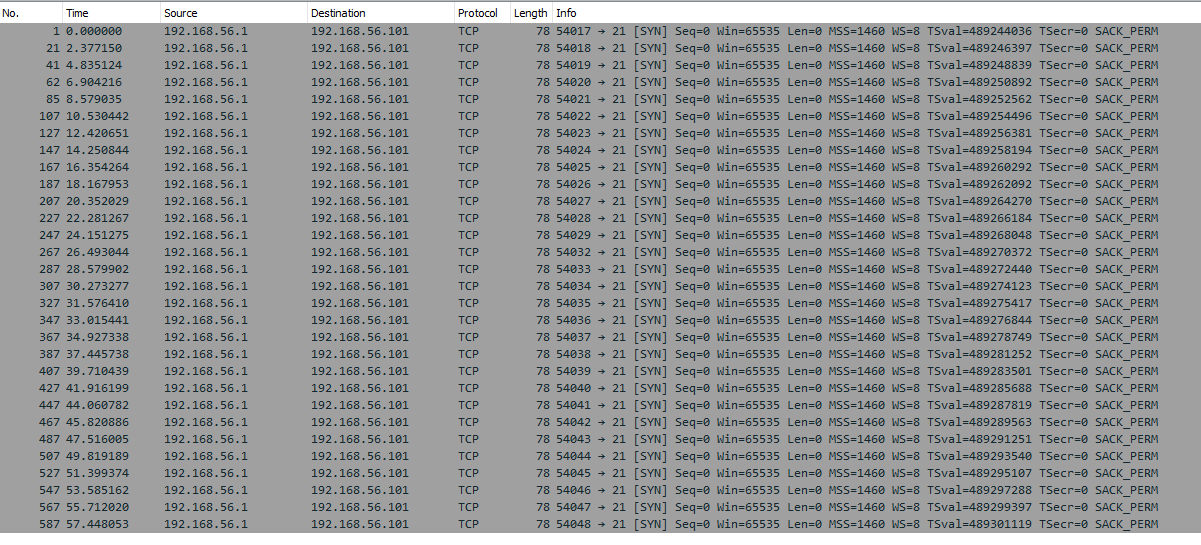


Con esta información podemos conocer que se trata de un servidor redmine FTP server en la versión 6.4.0.

## Escriba un filtro que muestre el primer paquete TCP de cada flujo en la traza

Tras hacer una breve investigación sobre cómo se pueden observar los primeros paquetes TCP de cada flujo, hemos descubierto que aquellos paquetes que tienen el flag SYN activado y el flag ACK desactivado son típicamente los primeros paquetes en cada flujo TCP. Por lo que el filtro que hemos optado por aplicar ha sido el siguiente:

tcp.flags.syn == 1 && tcp.flags.ack == 0

Esto nos ha devuelto la siguiente información:  


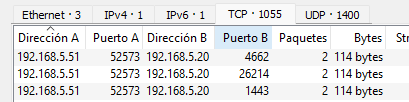
## Observando la traza globalmente, ¿cuál cree que es el objetivo del cliente?

El cliente está realizando un ataque de fuerza bruta para adivinar la contraseña del usuario bro del servidor y se puede observar que es un ataque numérico. El comando QUIT lo puede estar utilizando para evitar medidas de seguridad del servidor. Por ejemplo, algunos sistemas implementan medidas de seguridad que bloquean una cuenta o IP después de un número específico de intentos fallidos.

# **trace\_2.pcapng**

## Describa cuántas conversaciones TCP y UDP hay en la traza y cuántos hosts hay involucrados

De la misma manera que en el ejercicio anterior, si entramos a la pestaña “Conversaciones” dentro de “Estadísticas” podremos observar la siguiente información:



Tras esta captura podemos determinar que a través de TCP hay 1055 y UDP hay 1400, por lo tanto hay un total de 2455 conversaciones entre ambos.

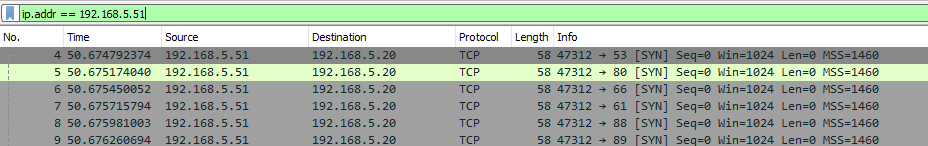
| Las direcciones de los hosts involucrados son: | 192.168.5.51 |
| --- | --- |
| 192.168.5.20 |

## Analizando globalmente la traza, ¿qué está haciendo el host con dirección IP 192.168.5.51?

Usando el siguiente código filtraremos únicamente por los paquetes enviados desde esa dirección con el siguiente código:

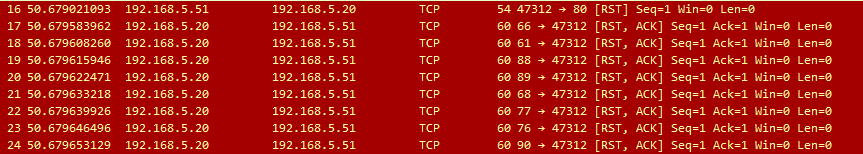
ip.addr == 192.168.5.51

Con esto obtendremos la siguiente información:



De estos datos podemos obtener información como que el host está intentando realizar conexiones con el host destino puesto que la información que se envía en cada paquete contiene la flag SYN, la cual indica una solicitud para establecer una nueva conexión.

También podemos observar que todas esas conexiones están siendo rechazadas por el host destino gracias a estas líneas de información:



En estas líneas podemos observar como el paquete destino está rechazando las conexiones gracias a las flags RST y ACK. Puesto que la flag RST es utilizada para reiniciar la conexión, nos está indicando que 192.168.5.20 está rechazando o cerrando las conexiones iniciadas por 192.168.5.51.

## Enumere todas las técnicas que el host con dirección IP 192.168.5.51 está usando.

En primer lugar, podemos observar que todos este host está usando 3 protocolos diferentes, UDP, TCP e ICMP

También podemos ver que a lo largo de todos los envíos que realiza la información contiene las siguientes flags:

* SYN (Sincronizar): Se utiliza durante el establecimiento de una conexión TCP. Es el primer paquete enviado en el proceso de "three-way handshake" y solicita la apertura de una conexión.
* ACK:(Reconocimiento): Se utiliza para reconocer la recepción de paquetes. También es parte del proceso de "three-way handshake" que establece una conexión TCP.
* FIN (Finalizar): Se utiliza para indicar el cierre de una conexión. Un host envía un paquete con la flag FIN para señalar que ha terminado de enviar datos.
* PSH (Push): Se utiliza para instruir al receptor a enviar inmediatamente los datos al nivel de aplicación, en lugar de almacenarlos en un búfer.
* URG (Urgente): Se utiliza para señalar que los datos deben ser procesados de manera urgente. Funciona junto con un campo de "puntero urgente" para especificar qué datos son urgentes.

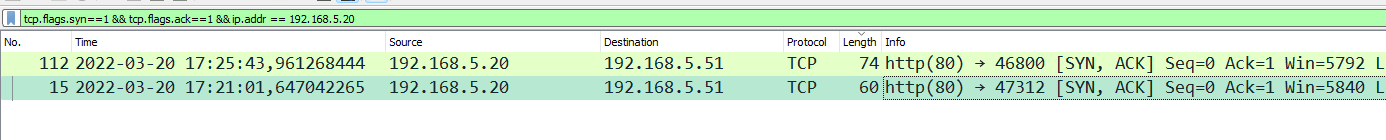
## ¿Qué puertos hay abiertos en el host con dirección IP 192.168.5.20?

Usando el siguiente filtro:

tcp.flags.syn==1 && tcp.flags.ack==1 && ip.addr == 192.168.5.20

El filtro se divide en 3 partes diferentes:

* **tcp.flags.syn==1:** Esta parte del filtro busca paquetes TCP donde el flag SYN está establecido. Este flag se usa al inicio de una conexión TCP significa que el paquete es una solicitud de inicio de conexión TCP.
* **tcp.flags.ack==1:** Esta parte del filtro se enfoca en los paquetes TCP donde el flag ACK está establecido. Este flag se usa para reconocer la recepción de paquetes. Específicamente, un paquete SYN-ACK es enviado como respuesta a un paquete SYN, indicando que el puerto está escuchando y disponible para la conexión.
* **ip.addr == 192.168.5.20:** Esta parte del filtro limita la búsqueda a paquetes que tienen la dirección IP “192.168.5.20”

Habiendo usado ese filtro encontramos el siguiente resultado:  
Con este resultado, podemos acceder a los 2 paquetes de la traza que cumplen el filtro. Accediendo a ambos paquetes podemos observar que ambos paquetes han sido enviados desde el puerto 80 lo que nos da a entender que este puerto es el único que está abierto.  


# **trace\_3.pcapng**

## Escriba un filtro que muestre todas las conversaciones HTTP en la traza

El filtro que te muestra únicamente todos los paquetes http es muy sencillo, únicamente se debe escribir esto en la barra de filtros:

http

De esta manera te aparecerán únicamente los paquetes asociados con el protocolo HTTP.

## Describa toda la información que pueda averiguar sobre el servidor y el cliente HTTP

* **IP:**

En primer lugar lo primero que observamos son las direcciones IP, 192.168.5.51 para el cliente y 192.168.5.20 para el servidor.

* **Cliente:**

En segundo lugar, podemos ver la actividad que realiza el cliente, este realiza múltiples solicitudes GET a distintas rutas y recursos, vemos que intenta acceder a ciertas rutas o archivos que requieren de autenticación, como se puede observar en la siguiente imagen:

También podemos observar que el cliente intenta acceder a rutas o archivos a través de las siguientes acciones:



* **Servidor:**

En tercer lugar, en cuanto al servidor podemos observar que devuelve 3 respuestas diferentes, la mencionada anteriormente 401 que indica que se requiere de autenticación para acceder al recurso, la 200, que indica una respuesta exitosa y la 304 que indica que el recurso que se ha solicitado no ha cambiado desde la última vez que se solicitó.







* **Recursos solicitados:**

Por último lugar podemos ver todos los recursos a los que se ha accedido o se ha intentado acceder. Estos recursos son los siguientes:

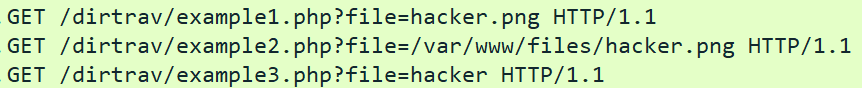
* Rutas de bootstrap:



* Favicon:



* Rutas o archivos de pruebas:



* Rutas o archivos “hacker”:



## Obtenga las contraseñas (en texto en claro) de las cabeceras HTTP Authorization contenidas en la traza

En primer lugar para conseguir filtrar y obtener estos paquetes hemos creado el siguiente filtro:

http and http.authorization

Esto nos permitirá filtrar por paquetes HTTP Authorization. Una vez filtrados, si accedemos a la información detallada de cada paquete vamos a observar las siguientes combinaciones usuario-contraseña:

| **Usuario** | **Contraseña** |
| --- | --- |
| profesor | 234235235 |
| profesor2 | facilona |
| profesor | claveprofesor |
| profesor2 | fallo |
| profesor2 | facil |

# **trace\_4.pcap**

## Esta traza de red contiene una infección por malware de un host Windows. Proporcione la fecha y hora de esta actividad.

Analizando la traza 4 hemos descubierto que la infección se produce en el paquete 1300:



La fecha de esta actividad es la siguiente:

-Formato CET



-Formato UTC



## Indique las direcciones IP y MAC y el nombre del host que es infectado

De la imagen anterior podemos obtener la siguiente información. La IP del host infectado, sería 192.168.204.137, la dirección MAC es 00:0c:29:9d:b8:6d y su hostname es 38NTRGDFQKR­PC.

## ¿Cuál es el nombre de dominio y la dirección IP del sitio web comprometido?

El nombre de dominio desde el que se hace la redirección que provoca la descarga el malware es [*www.excelforum.com*](http://www.excelforum.com) con IP 69.167.155.134 ya que es la web comprometida.

  
En esta captura vemos el nombre del host y su respectiva IP.

## ¿Cuál es el nombre de dominio e IP del sitio web desde el que se descarga el malware?

El sitio web desde el que se descarga el malware es *digiwebname.in* como se puede observar en el host de la sección de Hypertext Transfer Protocol del paquete con el malware y el resto de posibles playloads. Su ip es 205.234.186.111.

## ¿Qué navegador utiliza el host Windows que es infectado?

Gracias nuevamente a la información detallada de los paquetes en la sección de Hypertext Transfer Protocol podemos ver las cabeceras de la solicitud HTTP, con esta información obtenemos la siguiente imagen:   
  
En esta imagen se puede observar como el navegador que el host Windows está usando es Mozilla.

## Tras la infección, el malware utiliza comunicaciones HTTP. ¿Qué método (GET o POST) utiliza?

Tras la infección el malware utiliza el método GET para la descarga de varios playloads de la misma web(digiwebname.in):







