



TRABAJO FIN DE GRADO
INGENIERÍA EN INFORMÁTICA

Implementación en tiempo real de sistemas de identificación de tráfico de red

Subtítulo del proyecto

Autor

Álvaro Maximino Linares Herrera

Directores

Jesús Esteban Díaz Verdejo



ESCUELA TÉCNICA SUPERIOR DE INGENIERÍAS INFORMÁTICA Y DE
TELECOMUNICACIÓN

—
Granada, 3 de septiembre de 2017



Implementación en tiempo real de sistemas de identificación de tráfico de red

Subtitulo del proyecto

Autor

Álvaro Maximino Linares Herrera

Directores

Jesús Esteban Díaz Verdejo

Implementación en tiempo real de sistemas de identificación de tráfico de red

Álvaro Maximino Linares Herrera

Palabras clave: inspección profunda de paquetes, bro, flujos, identificación, clasificación, red, tráfico

Resumen

La identificación de tráfico en red es realmente importante para aplicaciones de ingeniería de tráfico y de seguridad.

En este trabajo se tratará la creación de un programa para un NMS (Network Monitoring System), en este caso se usará BRO, mediante el cual se pueda resolver el emparejamiento de flujos. BRO consiste en un NMS que funciona mediante el terminal en Linux o Mac, una de las peculiaridades de este programa es que para la creación de scripts que nos permitan extender la funcionalidad de la que dispone, tendremos que usar BRO como lenguaje de programación. Es un lenguaje de scripting, el cual está orientado a eventos, que se lanzan cuando ocurre algo relacionado con el control y análisis de redes, es un lenguaje que para los que vienen de C++, Java o Python, no debe de suponer un gran reto, más allá de acostumbrarse a sus sintaxis. Es un lenguaje potente que al estar orientado a redes nos permite obtener mucha información de los flujos que tenemos en la red o en el archivo que vayamos a analizar. En este trabajo mediante implementaciones offline se verificará la eficacia de esta técnica de clasificación de tráfico.

Project Title: Project Subtitle

First name, Family name (student)

Keywords: Keyword1, Keyword2, Keyword3,

Abstract

Write here the abstract in English.

Yo, **Álvaro Maximino Linares Herrera**, alumno de la titulación TITULACIÓN de la **Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación de la Universidad de Granada**, con DNI 76669401M, autorizo la ubicación de la siguiente copia de mi Trabajo Fin de Grado en la biblioteca del centro para que pueda ser consultada por las personas que lo deseen.

Fdo: Álvaro Maximino Linares Herrera

Granada a 3 de septiembre de 2017.

D. **Jesús Esteban Díaz Verdejo**, Profesor del Área de XXXX del Departamento YYYY de la Universidad de Granada.

Informa:

Que el presente trabajo, titulado *Implementación en tiempo real de sistemas de identificación de tráfico de red*, ha sido realizado bajo su supervisión por **Álvaro Maximino Linares Herrera**, y autorizamos la defensa de dicho trabajo ante el tribunal que corresponda.

Y para que conste, expiden y firman el presente informe en Granada a 3 de septiembre de 2017.

Los directores:

Jesús Esteban Díaz Verdejo	Nombre Apellido1 Apellido2 (tu- tor2)
-----------------------------------	--

Agradecimientos

Poner aquí agradecimientos...

Índice general

1. Introducción	15
1.1. Motivación y antecedentes	15
1.2. Objetivos	18
1.3. Metodología	19
1.4. Estructura de la memoria	20
2. Estado del arte	21
2.1. Identificación de tráfico	21
2.1.1. Técnicas de identificación de tráfico	21
2.1.2. Identificación de tráfico basada en flujos	22
2.1.3. DPI	22
2.2. BRO	22
2.2.1. Funcionalidades básicas de BRO	23
2.2.2. Eventos y trazas	24
2.2.3. Incorporación de funcionalidades	24
2.3. Emparejamiento de flujos	24
2.4. NMS y BRO	25
2.4.1. Requisitos de Bro	26
2.4.2. Gestión de tráfico en Bro	28
2.4.3. Identificación de flujos en Bro (Tipo de flujo/Protocolo)	30
2.4.4. Ejemplo de uso de eventos	31
3. Diseño y arquitectura del sistema	33
3.1. Arquitectura del sistema	33
3.2. Módulo y funciones	33
3.3. Gestión de flujos	33
3.4. Estructura de datos	33
4. Implementación	35
5. Evaluación y pruebas	43

6. Conclusiones y trabajo futuro	45
6.1. Conclusiones	45
6.2. Trabajo futuro	45
Bibliografía	48

Capítulo 1

Introducción

1.1. Motivación y antecedentes

Dada la gran expansión de Internet desde los años 90, la seguridad se ha convertido en algo fundamental. Hoy en día el uso de Internet se ha generalizado tanto que ha llegado a todas las áreas, desde finanzas hasta el envío de pruebas médicas, pasando por compras, redes sociales y demás, por lo tanto se tratan temas de carácter muy privado y personal.

Internet se organiza mediante un modelo de capas. Hay varios modelos de capas, como son el modelo TCP/IP y el modelo OSI. [1]

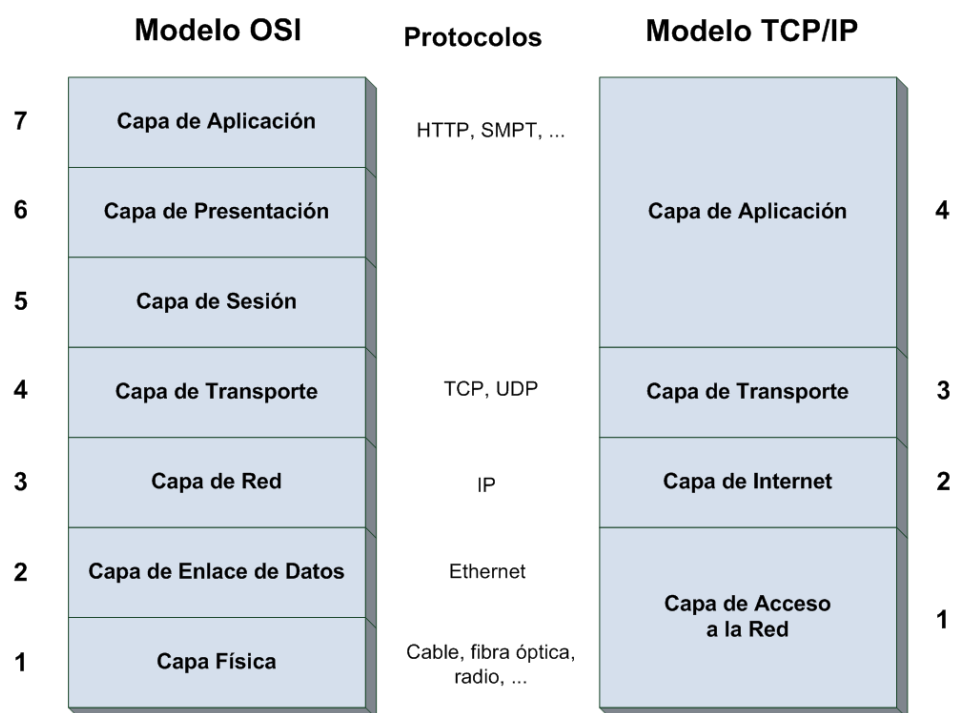


Figura 1.1: Modelos de capas de Internet.

Dentro del modelo TCP/IP, que es el que se seguirá en este proyecto, es importante tener claro las siguientes capas, pues forma parte de los conocimientos básicos para lograr entender el emparejamiento de flujos.

■ Capa de aplicación

En la capa de aplicación se encontrarán las aplicaciones de red y sus protocolos. Los protocolos que se encuentran en esta capa son HTTP, SMTP y FTP.

- El protocolo *HTTP* permite la solicitud y transferencia de documentos web.
- El protocolo *SMTP* permite la transferencia de mensajes de correo electrónico.
- El protocolo *FTP* permite la transferencia de archivos entre dos terminales.

A parte de estos protocolos también corresponde a esta capa el **DNS**, el cual se encarga de traducir los nombres de los sitios web.

Para una información más extensa sobre la capa de aplicación consulte [2]

■ Capa de transporte

La capa de transporte es la encargada de transportar los mensajes de la capa de aplicación. Los protocolos de esta capa son **TCP y UDP**. La principal diferencia y será algo que siempre se debe de tener presente cuando se trabaja con redes es que *TCP* está orientado a garantizar la conexión, mientras que *UDP* no garantiza la conexión.

Para ampliar información sobre esta capa consulte [3]

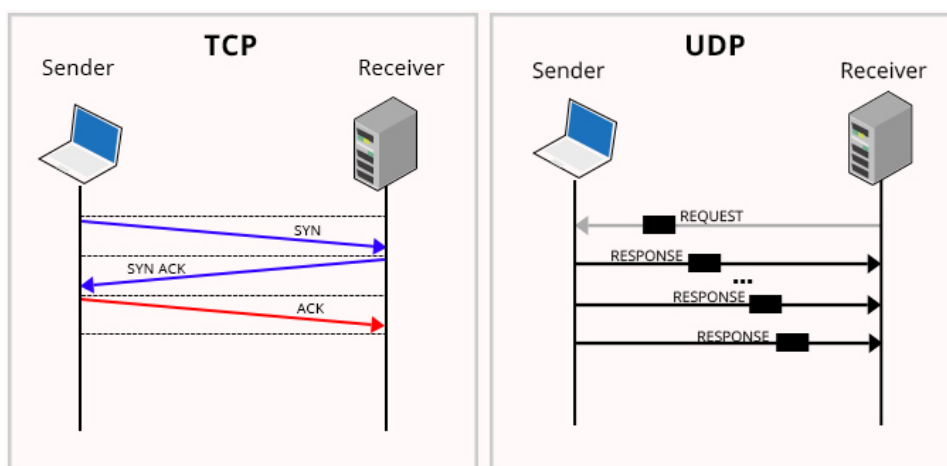


Figura 1.2: Diagrama de conexión de TCP y UDP.

■ Capa de red

En la capa de red es donde se encuentra el protocolo **IP**, el cual es el encargado de especificar el formato de envío entre los routers y los hosts y también el protocolo **ICMP**, el cual es un protocolo de control.

En esencia, esta capa es la que se encarga de transportar los *datagramas* de un *host* a otro.

Para ampliar sus conocimientos sobre la capa de red consulte [4]

En Internet la información que se envía se divide en paquetes. Estos paquetes tienen una IP de origen y otra de destino, así como un puerto de origen y un puerto de destino. Estos paquetes, que contienen parte de la información que se envía por la red, son unidos de nuevo una vez que llegan a su destino, de forma que entonces se dispondrá de la información completa. Dependiendo del tipo de protocolo se tolerarán pérdidas de paquetes o no, para ilustrar esta idea, en una llamada mediante *Skype* se tolera perder algunos paquetes, pues no se notará mucha diferencia. Si se pierden muchos paquetes la imagen se verá borrosa y la voz no se escuchará bien. Ahora en un correo electrónico, no se tolerará perder paquetes, pues entonces no se

obtendrá la información completa. Cuando varios paquetes tienen el mismo origen y el mismo destino se denomina flujo. [5]

De esta forma se llega al emparejamiento de flujos, el cual es muy útil para los NMS, sistemas de monitoreo de red, *Network Monitoring System*, como podría ser BRO [6]. Gracias al uso de estos programas el administrador de sistemas podrá prevenir ataques, como por ejemplo, los de denegación de servicio, DDoS, *Distributed Denial of Service* [7]. Un administrador de sistemas deberá de garantizar que el recurso que facilita y gestiona esté operativo siempre, por lo tanto analizará el tráfico para evitar los posibles ataques, virus, etc.

Existen otras técnicas de clasificación de tráfico, como se puede ver en el artículo del departamento [8], estas técnicas son:

- Clasificación basada en los puertos de la capa de transporte. [9]
- Clasificación basada en el contenido del paquete. [10]
- Clasificación basada en la aplicación de técnicas de aprendizaje automático sobre estadísticas de tráfico. [11]

Hoy en día, las dos primeras técnicas mencionadas no son muy eficaces, pues por ejemplo:

- La primera técnica puede ser burlada fácilmente, haciendo que las conexiones pasen por el puerto 80.
- En la segunda técnica, al tener que acceder a los paquetes, solo bastará con que estos estén encriptados para que no se pueda acceder a dicho paquete. Y también se debe de tener en cuenta que al acceder a los paquetes de una red que no es del propietario de la información es un delito y no respeta la privacidad.

Ahora bien, la tercera técnica si es eficaz y fiable, pero su principal inconveniente es que necesita cierto tiempo para aprender a clasificar de una forma correcta el tráfico.

Por lo tanto es necesario un nuevo método de clasificación, que sea funcional en cualquier circunstancia y sea eficiente desde el principio. Por ello, el método de emparejamiento planteado por el departamento [8] es muy atractivo al ser necesario saber solo las IP's y los puertos, ya que se respeta la seguridad, pues no es necesario acceder a los paquetes para conocer estos detalles. Incluso no sería necesario ser un proveedor de servicios de Internet, ISP, para conocer estos datos.

1.2. Objetivos

En este trabajo se hará uso del NMS mencionado anteriormente, llamado Bro [6], el cual cuenta con su propio lenguaje de scripting. Dicho lenguaje es

de fácil uso y comprensión, además de que está completamente orientado a trabajar con conexiones, teniendo distintos tipos de datos que son realmente útiles. Dicho esto el objetivo del trabajo es desarrollar un módulo para Bro. En este módulo irá implementada la técnica de emparejamiento de flujos, de forma que pueda ser usada en redes fuera de un entorno de laboratorio.

- Para ello será necesario conocer como Bro gestiona los flujos, desde su nacimiento a su muerte.
- También hará falta gestionar las entradas y salidas, aunque al principio se hará uso de un archivo *pcap* de prueba para controlar si todo funciona bien, pudiendo pasar luego a analizar el tráfico de una red online.
- Implementar la función de emparejamiento de flujos.
- Será necesario realizar pruebas al módulo que se pretende desarrollar, de modo que se detecten los errores y se subsanen.

Por último, y fuera de los objetivos más técnicos, el desarrollo de esta memoria también se considera un objetivo, que se tendrá en cuenta dentro de la temporización.

1.3. Metodología

Para realizar este trabajo se establecen una serie de tareas:

- Lectura del artículo del departamento. [8]
- Estudio del uso de Bro y de su lenguaje de scripting.
- Pruebas con el lenguaje propio de Bro.
- Desarrollo del módulo en Bro.
- Pruebas del módulo.
- Desarrollo de la memoria.

Cada tarea anterior se realimentará de la siguiente, el ejemplo más claro es el desarrollo del módulo, que irá cambiando por las pruebas, pues se detectarán los fallos, a su vez habrá que releer el artículo mientras se desarrolla el módulo para asegurarse de que todo se realiza de acuerdo al trabajo previo, etc.

En el siguiente diagrama de Gantt se puede ver una temporización de estas tareas.

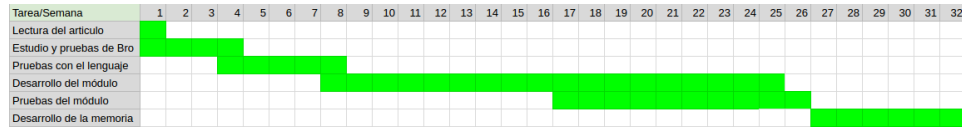


Figura 1.3: Temporización en diagrama de Gantt.

Este proyecto no necesita de ningún gasto, pues Bro [6] proporciona sus binarios de forma gratuita. El módulo será subido a GitHub [12] con licencia de software libre, por lo que cualquiera podrá usarlo o modificarlo en el futuro. El único *gasto* es el de un ordenador con Linux, o bien con Mac OS X, pues de momento no está disponible para Windows. [13]

1.4. Estructura de la memoria

Esta memoria se organizará de la siguiente forma:

- En el capítulo 2 se hablará de todos los fundamentos teóricos y tecnológicos sobre los que se basa el proyecto.
- En el capítulo 3 se contará cómo se pretende resolver el problema expuesto.
- En el capítulo 4 se encontrará detallado cómo se han implementado los diferentes módulos.
- En el capítulo 5 se realizarán las pruebas, para comprobar que todo funciona como estaba previsto, tanto a nivel funcional como a nivel de aplicación.
- En el último capítulo se hablará de las conclusiones recogidas a lo largo de este proyecto y las posibles opciones que tiene para seguir trabajando sobre él.

Capítulo 2

Estado del arte

Aquí se encontrará la parte teórica del proyecto. Se desglosará en que consiste la identificación de tráfico y las distintas técnicas que existen. También se hablará de Bro [6], el NMS que se usará para llevar a cabo el desarrollo del módulo. Se introducirá en que consiste, cómo gestiona los eventos y sus funcionalidades, así como la posibilidad de ampliar estas.

Por último se presentará de forma teórica en que consiste el emparejamiento de flujos y de qué forma se podría usar para identificar el tráfico.

2.1. Identificación de tráfico

La identificación de tráfico, por si sola, no clasifica el tráfico. Solamente proporciona información obtenida de los paquetes. Esta información puede ser obtenida con distintas técnicas, las cuales se detallarán a continuación.

2.1.1. Técnicas de identificación de tráfico

Existen varias técnicas de identificación de tráfico, cómo se pudo ver en el capítulo de introducción. Ahora serán explicadas de una forma más detallada.

Clasificación basada en los puertos de la capa de transporte. [9]

Esta clasificación consiste en clasificar el tráfico dependiendo de los puertos de la capa de transporte, fue diseñada por IANA [14]. IANA es la organización que se encarga de asignar los protocolos de Internet, algunos nombres de dominios y coordinar la asignación de direcciones IP.

Entonces, IANA es quien asigna el número de puerto a los distintos protocolos, haciendo que se pueda clasificar el tráfico por el número de puerto al que se envía. Este sistema tiene el inconveniente de que ahora mismo, se están desarrollando multitud de aplicaciones web, las cuales se conectan mediante el puerto 80, es decir, mediante el protocolo HTTP. Pero esto no

es cierto, pues se puede hacer que cualquier aplicación envíe información por el puerto 80, sin que sea HTTP, lo cual daría una mala clasificación.

2.1.2. Identificación de tráfico basada en flujos

Clasificación basada en la aplicación de técnicas de aprendizaje automático sobre estadísticas de tráfico [11], se aplica sobre flujos.

Esta clasificación es muy sencilla. Consta de algoritmos de aprendizaje automático, los cuales se dedican a realizar análisis estadísticos. De esta forma aprenden las características determinadas de los flujos. Este tipo de clasificación tiene un porcentaje de acierto del 95 %, según se puede leer en el artículo [8].

2.1.3. DPI

Clasificación basada en el contenido del paquete o DPI. [10]

Esta técnica de clasificación consiste en analizar los paquetes, más allá de su cabecera. La Inspección Profunda de Paquetes, DPI por sus siglas en inglés, *Deep Packet Inspection*. Esta técnica lo que hace es analizar todos los paquetes en busca de cadenas que se repitan, además de las IP's y los puertos. Una vez que tiene una cadena, la usa para buscar paquetes que tienen ese patrón, de esta forma establece la clasificación.

Esta técnica es útil para buscar virus, intrusiones y demás. Suele ser usada por los proveedores de servicios de Internet, ISP, por sus siglas en inglés *Internet Service Provider* y grandes empresas. Se puede decir que es una técnica que no respeta la privacidad, pues entra dentro de la información del paquete, más allá de la cabecera. Aunque en el caso de una gran empresa si puede hacerse, pues si se está en la red propia no es delito mirar la información. En algunos países, como Alemania, donde es ilegal el uso de *torrents*, las autoridades pueden pedir información al proveedor de servicios sobre uno de sus clientes, si cree que este está infringiendo la red, por lo que esta técnica es ideal para este tipo de cometidos.

Esta técnica también es ideal para saber si se está siendo atacado. [15]

2.2. BRO

Bro [6], es un analizador de tráfico de red de código abierto. Al ser de código abierto permite ser usado por quien lo desee sin necesidad de pagar licencias. Funciona sobre sistemas basados en Linux y Mac OS X. Una de sus principales características es la posibilidad de buscar amenazas en la red que se esté monitorizando.

Bro incorpora la posibilidad de introducir funcionalidades nuevas, mediante la programación en su propio lenguaje de *scripting*, del mismo nom-

bre. Esto se desarrollará más adelante y en la parte de implementación se podrá ver cómo se desarrolla y algunos ejemplos de código escrito en Bro.

No tiene interfaz gráfica, por lo que su gestión se realiza desde la línea de comandos. Este aspecto para el usuario que no esté familiarizado con la consola de Linux puede suponer un problema. Pero uno de sus principales ventajas es la rapidez con la que analiza los ficheros pcap. **RELEER**



Figura 2.1: Logo de Bro.

2.2.1. Funcionalidades básicas de BRO

La funcionalidad más básica de Bro, es el análisis del tráfico de la red en la cual se esté ejecutando. Mientras que se encuentra ejecutándose, genera registros o *logs* en texto plano que se podrán leer. Pero hay que tener cuidado y guardarlos fuera de la carpeta en la que se generan o se irán reescribiendo cuando vaya analizando más tráfico. Algunos *logs* que se generan son los siguientes.

- *dnpd.log*. Consiste en un resumen de los protocolos encontrados en puertos que no son estándar.
- *dns.log*. Contendrá toda la actividad correspondiente al *DNS*
- *ftp.log*. Un registro de la actividad a nivel de sesión de *FTP*.
- *files.log*. Un resumen con los archivos transferidos a través de una red. Incluye protocolos *HTTP*, *FTP* y *SMTP*.
- *http.log*. Registro de toda la actividad *HTTP* con sus réplicas.
- *ssl.log*. Un registro de las sesiones *SSL*, incluidos los certificados que se utilizan.
- *weird.log*. En este *log* se guarda la información correspondiente a actividad inesperada o rara a nivel de protocolo. Al analizar gran cantidad de tráfico no es muy útil, pues ocurren muchas cosas raras, pero a pequeña escala es bastante interesante para detectar intrusiones y demás.
- *conn.log*. Aquí se puede ver la información correspondiente a conexiones *TCP*, *UDP* e *ICMP*.

Para más información sobre *logs* generados por una monitorización de Bro lea [16].

2.2.2. Eventos y trazas

2.2.3. Incorporación de funcionalidades

2.3. Emparejamiento de flujos

El emparejamiento de flujos, por si mismo, sólo identifica el tráfico, por lo tanto se necesitará otra técnica para clasificar el tráfico.

AQUI EMPIEZA LO ANTIGUO, REHACER

La idea de la que partimos es la siguiente: Los flujos son un conjunto de paquetes que comparten la misma información, IP de origen, IP de destino y los puertos de origen y destino, aparte de esta información también tienen un tiempo de inicio, relativo al *timestamp* del primer paquete del flujo y una duración. Con estos datos ya podemos empezar a trabajar en el emparejamiento, pues si dos flujos comparten las IP's de origen y destino y los puertos de origen y destino ya serían candidatos a la comparación.

Para comparar los flujos lo que haremos será aplicar la siguiente fórmula:

$$F(x, y) = \begin{cases} G(x, y), & NIP(x, y) \geq 1 \\ -\infty, & \text{en otro caso} \end{cases}$$

Donde tenemos que $G(x, y)$ es:

$$G(x, y) = |NIP(x, y) - 1| + 1 / (dp1(x, y) + k1) + 1 / (dp2(x, y) + k1) + 1 / (dt(x, y) + k2)$$

Tenemos que \mathbf{x} e \mathbf{y} son los flujos a comparar, $\mathbf{NIP}(\mathbf{x}, \mathbf{y})$ es el número de veces que tenemos almacenado flujos similares, por lo cual siempre será uno, como mínimo. $\mathbf{dp1}(\mathbf{x}, \mathbf{y})$ son los puertos de origen de los dos flujos, que al comparar siempre flujos que tienen los mismos puertos serán siempre el mismo puerto. $\mathbf{dp2}(\mathbf{x}, \mathbf{y})$ son los puertos de destino, que como en el caso anterior siempre serán el mismo puerto. $\mathbf{k1}$ y $\mathbf{k2}$ son constantes definidas antes de ejecutar el programa, estando estas normalmente en los trabajos realizados anteriormente estas constantes suelen estar definidas entre 1 y 10000 y, por último, \mathbf{dt} es la diferencia de tiempo entre los **timestamps** de los dos flujos.

Con esta fórmula obtendremos un número que podremos comparar con un

umbral que estará definido a la hora de ejecutar el programa, si el umbral definido es pequeño tendremos más flujos almacenados, si el umbral es más grande serán menos los flujos que serán emparejables y por tanto almacenados para trabajar con ellos. [8]

2.4. NMS y BRO

Bro es un NMS, Network Monitoring System, cuya principal actividad es analizar el tráfico de una red para la búsqueda de amenazas. Una de las muchas peculiaridades de Bro es que usa un lenguaje propio, llamado también Bro, el cual tiene similitudes con *Python* y *Java*, y se gestiona mediante **eventos**. En el caso de este trabajo se utilizará dicho lenguaje, el cual en un principio puede parecer difícil, pues no disponemos de más documentación que la propia de la web de Bro [6], pero que acaba siendo bastante útil para la tarea que queremos, pues tiene un tipo de dato llamado *connection*, el cual está relacionado con los flujos, siendo al final este tipo el que representa al propio flujo. En este tipo se establecen bastantes datos que nos serán útiles, como la IP de origen, la de destino, así como los puertos y sus protocolos, también guarda la información de la duración así como el *timestamp* y más información que, en este caso, no será relevante, como la *historia del flujo*, donde se nos informa del tipo de paquetes que contiene e incluso el *número de paquetes* de los que consta el flujo.

EVENTOS

En el caso de los eventos, también nos facilitarán el trabajo, pues tenemos eventos que gestionan todo lo que tiene que ver con los flujos, desde cuando aparece un nuevo flujo el cual no tenemos identificado previamente, lo cual para nuestro trabajo es fundamental, pues nos hace el programa más eficiente, ya que cada vez que se lanza ese evento significa que tenemos que añadir ese flujo a la lista de flujos comparables, sin tener que compararlo con los que tengamos previamente almacenados. También tenemos flujos que nos indicarán cuando un flujo esté a punto de morir, siendo el momento de eliminarlo de la lista de comparables y, en caso de tener flujos con los que éste ha sido comparado, pasará el primero de estos a reemplazar el flujo que va a morir en la lista de comparables, de ésta forma nos evitamos tener que estar comprobando la duración del flujo para eliminarlo manualmente. Con todo esto conseguimos un programa eficiente en cuanto a tiempo y que, gracias a estos eventos, va a identificar los dos protocolos de la capa de transporte, siendo estos **TCP** y **UDP**. Cabe destacar que los eventos de *UDP* empleados en nuestro programa son muy costoso, por lo tanto en caso de tener mucho tráfico *UDP*, siendo de dos tipos distinto **reply** y **request**, puede hacer que el análisis tarde más tiempo del deseado, pero el programa

suele funcionar en una horquilla de tiempo bastante aceptable en términos de rendimiento para el análisis del tráfico, aunque cabe destacar que en nuestro caso analizamos archivos, no tráfico en tiempo real. En el apartado *Implementación* se hablará sobre los eventos usados con más detalle.

Bro también nos otorga una gran cantidad de **logs** en los cuales él mismo puede llegar a clasificar el tráfico dependiendo del protocolo que se use, siendo algunos ejemplos, *HTTP*, *DNS*, *SSL*, *etc.* pero no nos interesa, pues se tratan de protocolos de la capa de aplicación. Aunque como en nuestro caso usamos la información contenida en un archivo **pcap**, la información de los protocolos de la capa de aplicación, dependerá de si han sido cargados los *scripts* correspondientes cuando se realizó la captura del tráfico, pues en los flujos de Bro la información relativa a *HTTP*, *DNS*, *etc.* es opcional, siendo únicamente obligatorio, en lo relativo a puertos que se informe de si pertenece a *TCP*, *UDP* o *ICMP*.

Bro trabaja sobre Linux y sobre la terminal por lo tanto será necesario leer la documentación para saber que opciones nos interesa tener activadas cuando vayamos a analizar el tráfico, pues al no tener interfaz gráfica nos puede ocurrir que no tengamos activado lo que queramos y otras cosas que no precisamos si estén activas.

También es digno de mención que la información que hay en la red sobre Bro es bastante escasa, quedando casi exclusivamente la información que se puede encontrar en la web de Bro [6], por lo tanto a la hora de alguna duda, la web será nuestra principal opción y en caso de no encontrar lo que queramos tendremos que hacer bastantes pruebas hasta dar con la clave. También podemos realizar una búsqueda por *GitHub* para coger ideas de cómo podemos resolver nuestras dudas. Aquí por ejemplo se puede encontrar información sobre cómo operar tablas con vectores de la manera correcta [17].

2.4.1. Requisitos de Bro

Podemos descargar los binarios y el código fuente desde la web de Bro [13], pero en mi caso después de experimentar ciertos fallos con ésta instalación, recomiendo seguir la instalación de Bro de su web en el apartado de instalación [18], pues allí nos guía a una instalación que es más fácil de mantener actualizada, ya que descargamos el código fuente directamente del **repositorio de GitHub**, por lo cual si hay algún cambio importante, con alguna mejora interesante la podremos tener casi directamente a nuestra disposición.

Para la instalación con los archivos de *GitHub*, tendremos que hacer lo siguiente:

```
sudo apt-get install cmake make gcc g++ flex bison libpcap-dev libssl-dev python-dev swig zlib1g-dev
```

Una vez que terminemos de instalar todo lo del comando anterior tendremos todos los prerequisites para la instalación de Bro, ahora clonamos el *repositorio de GitHub* en nuestro ordenador:

```
git clone --recursive git://git.bro.org/bro
```

Cuando termine de descargarlo nos metemos en la carpeta y ejecutamos lo siguiente:

```
./configure  
make  
make install
```

De esta forma ya tendremos instalado Bro en nuestro ordenador y podremos empezar a usarlo.

Ahora para usarlo tendremos que hacer lo siguiente, lo primero será **ajustar el PATH** de nuestro terminal, para ello, tendremos que ejecutar en nuestro terminal lo siguiente:

```
export PATH=/usr/local/bro/bin:$PATH
```

Es importante hacerlo, pues sino obtendremos un error diciendo que Bro no se encuentra instalado. Una vez hecho esto, podemos empezar realizando un script sencillo y probar a ejecutarlo, un ejemplo de script sencillo es el que se ve en el apartado *Ejemplo de uso de evento*, supongamos que el script se llama *prueba.bro*, para lanzarlo tendremos que hacer lo siguiente:

```
~$ bro -b -r pcap/nitroba.pcap scripts/bro-flows/prueba.bro
```

En este caso dentro de la carpeta Bro que se genera cuando clonamos el repositorio he creado una carpeta llamada scripts, para tener todos los scripts

allí guardados, por lo tanto al encontrarnos en la carpeta raíz de Bro, tendremos que ponerlo en la ruta, la opción *-b* que ponemos en la orden es solo para este ejemplo, lo que hace es no cargar los scripts que se encuentran en el directorio *base/*. Como necesitamos leer de un archivo *pcap*, tenemos que poner la opción *-r*, que indica a Bro que tiene un archivo de datos que leer, al igual que con los scripts, también hemos creado una carpeta *pcap* en la cual guardamos los archivos *pcap* que queramos leer. Una vez que lo ejecutemos se nos mostrará en el terminal un mensaje cada vez que se genere un flujo nuevo, cuando se exceda el timeout también y cuando un flujo vaya a ser eliminado de la memoria.

2.4.2. Gestión de tráfico en Bro

Nacimiento y muerte de flujos

En Bro el **nacimiento de un flujo** es controlado por un evento, dicho de otro modo, cuando aparece un nuevo flujo se lanza un evento, de ésta forma podremos controlar cuando un flujo nuevo aparece y podremos analizar toda su información en este evento o en los siguientes antes de que el flujo muera, o en el caso de tenerlo almacenado, antes de eliminarlo, pues una vez que lo eliminemos no podremos recuperarlo, por lo tanto para el análisis detallado del tráfico es interesante guardarlo.

La muerte de un flujo funciona también por eventos, siendo activado el evento cuando el flujo está a punto de morir, por lo tanto todavía podremos operar sobre él, por ejemplo, podremos decidir si queremos que el flujo sea eliminado o seguir guardándolo para análisis estadísticos, realizar una comparación para ver si tenemos más flujos con sus características para reemplazarlo, etc.

Por lo tanto como se comentó en apartados anteriores en Bro la mayor parte de la información se gestiona con eventos, lo cual facilita enormemente el trabajo que tenemos por delante.

Marcas temporales

Es interesante remarcar el uso de los **timestamps**, pues como ya se sabe son una variable importante que usaremos en la comparación, esta variable es necesaria para emparejar los flujos, cierto es que los datos más importantes son las IP's y los puertos, pues si no son iguales no procederemos a aplicar la fórmula necesaria para el emparejamiento, pero llegado el momento también podríamos comparar los *timestamps* para comprobar si son distintos, pues en caso de que sean iguales podríamos desechar la comparación, pues básicamente sería comparar el mismo flujo, por algún error de programación y esto nos haría el programa más eficiente.

En Bro, como lenguaje de programación, volvemos a encontrarnos con un tipo de dato propio para la gestión de estos datos, en este caso el tipo es `time` [19], cuyo nombre es de por sí muy indicativo de lo que va a contener. La peculiaridad de este tipo de dato es que el tiempo viene dado en valor absoluto, por lo cual tendremos que formatearlo para representarlo, aunque no será necesario si solamente queremos operar con él. Bro dispone de funciones para pasar de `double` a `time`, **`double_to_time`**, obtener el tiempo actual, **`current_time`**, y por último también disponemos de una función para obtener el tiempo del último paquete procesado, **`network_time`**, obteniendo así su *timestamp*, aunque parezca que necesita estar procesando de manera online para usar esta función no es así, pues también sirve para los archivos de datos de tráfico de red guardados, como los archivos *pcap* que usaremos nosotros para el emparejamiento. Para mostrar correctamente el valor del tiempo podemos usar **`strftime`**, lo cual nos formateará el tiempo y lo mostrará acorde a lo que le indiquemos en la cabecera de la función. También contamos con el caso contrario, es decir, pasar de `string` a `time`, para ello tendremos que usar la función **`strptime`**.

Para acabar tenemos una de las funciones más importantes que es **`time_to_double`**, que sirve para pasar un tipo `time` a `double`, haciendo más fácil operar con él.

Listado de flujos activos

Para mantener un **listado de flujos activos** haremos uso de un contenedor para almacenarlos y haremos uso de los eventos de Bro para gestionarlos. Primero, cuando se generen flujos que previamente no habíamos visto los guardaremos para compararlos, si aparecen flujos que ya tenemos reconocidos, los compararemos con los almacenados y si nos interesa los guardaremos, y por último cuando Bro nos indique que algún flujo va a ser eliminado de la memoria y por lo tanto ese flujo ya no estará activo una vez que el evento termine, por lo tanto tendremos que operar con el flujo antes de que el evento termine, para ello veremos si hay algún candidato a ocupar su puesto en el listado de flujos emparejados y lo eliminamos del listado de flujos comparables.

Para mantener un listado de flujos activos Bro nos proporciona varias formas. La primera es usar un **vector**, el cual es fácil de usar si venimos de lenguajes como *C++*, podremos incluir datos usando los corchetes, `[]`, indicando el índice dentro de ellos, para borrar un elemento usaremos *delete* y para consultar el tamaño del vector usaremos `—v—`, pero sin embargo por si sólo es muy **ineficiente** para almacenar datos del tipo `connection`, pues solo dispone de índices numéricos.

Otro tipo para almacenar datos es **set**, el cual para borrar y consultar el tamaño es igual que para los vectores, sin embargo, para agregar datos tendremos que usar *add se[s]*, estando entre los corchetes lo que queremos almacenar, aunque también podemos almacenar datos redifiniendo el set, por ejemplo, *s1 = set(1,2,3)*. El set también es **ineficiente**, aunque menos, pues en un índice, aunque podemos guardar varios elementos estos tienen que ser únicos y corremos el riesgo de eliminar los datos almacenados al insertar nuevos datos.

Por último podemos usar un tipo *table*, que es básicamente un *map*, de los que se usan en *C++*, pudiendo hacerlos bastante interesantes, pues podemos hacer un **table de connection de vector** o de set de connection, por lo tanto esta será la forma que usaremos para almacenar el listado de flujos activos, pues nos da bastante versatilidad a la hora de manejar el listado de los flujos, porque podemos acceder por índice a la lista de todos los flujos que comparten datos, haciendo que sea una tarea bastante asequible, en términos de eficiencia.

2.4.3. Identificación de flujos en Bro (Tipo de flujo/Protocolo)

Como ya se explicó en otro apartado, Bro consta del tipo *connection* [20] para referirse y tratar los flujos, por lo tanto cómo en el flujo hay información sobre el protocolo que usa, podemos consultarlo haciendo referencia al flujo que estamos tratando. Hay que destacar que dentro de *connection*, en *history*, existe otro tipo llamado *Conn::Info* [21] que extiende aún más los datos de *connection*, y siendo capaz sus datos de crear los *logs* de lo que estamos analizando, por lo que podremos generar un log con los protocolos que son usados en la sesión. Cabe destacar que mostrando la información del puerto mediante el tipo *port*, el *string* que nos muestra lleva el número del puerto y el protocolo al que pertenece, pudiendo así extraer si es *TCP* o *UDP*. Aunque si lo que queremos es obtener solamente el protocolo de transporte al que pertenece el flujo podemos hacer uso de la función *get_port_transport_proto* [22].

Es destacable que el tipo de dato *port* soporta la comparación, lo cual será usado en el programa.

También en las múltiples extensiones de Bro encontramos un analizador de protocolos, *protocol analyzer* [?], el cual dispone de varias funciones interesantes para el análisis de protocolos, pero que nosotros no usaremos.

Después de lo expuesto en esta sección podemos decir que a partir del pro-

toloco al que nos indique el flujo que pertenece, podremos clasificar mejor el tipo de flujo que estamos tratando.

2.4.4. Ejemplo de uso de eventos

Ahora que tenemos algunos conceptos claros pondremos el ejemplo de un programa en el cual se lanza un evento cada vez que aparece un flujo nuevo.

```
1  ## Para todo tipo de conexiones, ya sean TCP, UDP o ICMP. Este evento
   salta con cada nueva
2  ## conexion, con el primer paquete de una conexion desconocida, por lo
   que mirando el
3  ## documento generado vemos que esto es un nuevo flujo.
4  event new_connection(c: connection)
5  {
6
7      if ( connection_exists( c$id ) ) {
8          print fmt("Nueva conexion establecida Timestamp: %s desde %s a %
              s", strftime("%Y/%M/%d %H:%m:%S", network_time()),
              c$id$orig_h, c$id$resp_h);
9          print fmt("Protocolo del puerto: %s", get_port_transport_proto(
              c$id$orig_p));
10         print fmt("Informacion de las 4 tuplas del paquete: %s", c$id);
11     } else {
12         print fmt("La conexion ya existe");
13         print fmt("
               -----
               ");
14     }
15 }
16
17 ## Solo disponible para conexiones TCP, se genera cuando no hay
   actividad en un
18 ## periodo de tiempo determinado.
19 event connection_timeout(c: connection)
20 {
21     print fmt("Conexion TCP ha excedido el timeout: %s",c$id);
22 }
23
24 ## Este evento salta para todo tipo de conexion, se da cuando el
   estado interno
25 ## esta a punto de eliminarse de memoria
26 event connection_state_remove(c: connection)
27 {
28
29     print fmt("Conexion de %s a %s a punto de ser eliminada de la
               memoria", c$id$orig_h, c$id$resp_h);
30 }
31 }
```

Algunos comentarios sobre este código. Como habrá podido notar en el lenguaje *Bro* los comentarios se realizan con dos almohadillas, `##`, los `print` son como en la gran mayoría de lenguajes, con la particularidad de que si

vamos a mostrar un *string* debemos de indicar que va formateado mediante *fmt*, *%s* es para mostrar el *string*, tal y como se hace en *C* con los datos de tipo *int* mostrándolo con *%i*, por ejemplo. Por último para acceder a la distinta información que contiene el tipo de dato debemos de usar *\$*, esto es parecido a como accedemos en *Java* a los datos de las clases.

Aunque el código está comentado merece la pena hacer algunas valoraciones sobre los eventos usados, el evento **new_connection** es muy útil, pues se ejecuta cada vez que llega un flujo que no ha sido usado antes y además reconoce *TCP*, *UDP* e *ICMP*. El evento **connection_timeout** aunque sólo sirva para flujos del protocolo *TCP* es bastante útil para empezar a trabajar sobre Bro, pues sirve para empezar a comprender como funcionan los eventos. Por último el evento **connection_state_removed** se lanza para *TCP*, *UDP* e *ICMP* cuando los flujos están a punto de morir, por lo tanto tiene un gran valor para eliminar de memoria los flujos que ya no nos interesan porque no están activos, y si este evento no se lanza no serán eliminados, en caso de que los flujos estén guardados.

Capítulo 3

Diseño y arquitectura del sistema

- 3.1. Arquitectura del sistema
- 3.2. Módulo y funciones
- 3.3. Gestión de flujos
- 3.4. Estructura de datos

Capítulo 4

Implementación

Ahora vamos a proceder a explicar cómo se ha solucionado los problemas propuestos, siendo estos explicados a través del programa que se ha realizado, quedando así más clara la explicación.

Lo primero será mostrar que estructura se ha utilizado para almacenar los flujos.

```
1
2 ## Tablas para guardar los flujos que son emparejados
3 global collection: table[addr, addr, port, port] of vector of
   connection &synchronized;
4 global collection_added: table[addr, addr, port, port] of vector of
   connection;
5
6 ## El umbral: "Comparar la constante 'k', que es el umbral que fijare
   con el resultado que devuelve la funcion,
7 ## si es mas grande el resultado que 'k' se puede decir que los dos
   flujos son iguales, si es mas pequenio podemos decir que los dos
   flujos no son iguales"
8 ## resultado del umbral que calculamos
9 global umbral: double;
10
11 ## Definimos el umbral, de manera global para hacer las comparaciones
12 global k=10;
```

En este primer código tenemos que:

- Vamos a guardar los flujos en una tabla *collection* que tiene como índices dos direcciones IP y dos puertos, y a partir de estos índices tendremos un *vector de connection*.
- La tabla *collection_added* está destinada para guardar los flujos que son emparejados.
- El *umbral*, que será una variable global, y será donde almacenemos el

resultado de la función de comparación.

- k es el umbral que definimos nosotros al principio, que será el que usemos como referencia para saber si dos flujos son emparejables o no.

```

1  ## funcion para la comparacion de los flujos , c1 el flujo que esta el
    primero en el vector de la tabla y c2 para el flujo que es
    candidato a ser emparejado
2
3  function emparejamiento(c1: connection , c2: connection ):double {
4
5      ## Aniadimos variables para comprobar en la tabla , sin hacer bucle
6      local orig = c1$id$orig_h;
7      local dest = c1$id$resp_h;
8      local po = c1$id$orig_p;
9      local pd = c1$id$resp_p;
10
11     local Nip = |collection[orig,dest,po,pd]|; ## Variable para saber
        cuantas conexiones tenemos
12     local Po1: count; ## Puerto origen del primer flujo
13     local Po2: count; ## Puerto origen del segundo flujo
14     local Pd1: count; ## Puerto destino del primer flujo
15     local Pd2: count; ## Puerto destino del segundo flujo
16     local k1 = 1; ## Variable fija
17     local k2 = 10; ## Variable fija
18     local dt: double; ## Variable para la diferencia de los tiempos
19     local resultado = 0.0; ## Lo iniciamos a 0
20
21     print c1$uid;
22     print c2$uid;
23
24     print fmt("Numero de Nip en table: %d", Nip);
25     informacion_coincidencia(c1,c2);
26     print fmt("Tiempo de inicio del flujo: %s", |c1$start_time|);
27     print fmt("Tiempo de inicio del flujo: %s", |c2$start_time|);
28     ## Para dp1 y dp2 que son l-norm usamos la "Manhattan norm" que dice
        lo siguiente: SAD(x1,x2) = sumatoria(x1i - x2i)
29     ## k1 y k2 son dos variables que nosotros le ponemos de forma manual
        , en este caso las pondremos como locales con 1 y 10
        respectivamente
30     ## dt es la diferencia de tiempo entre los time stamp de los
        primeros flujos de los flujos
31     ## el tipo time se supone que es como un double, por lo tanto
        podremos restarlos sin problemas
32     ## para la comparacion de puertos primero tendremos que hacer uso de
        la funcion port_to_count [https://www.bro.org/sphinx/scripts/
        base/bif/bro.bif.bro.html#id-port-to-count]
33     ## la cual nos pasa el puerto, que recordamos que va tambien con un
        string en el cual se nos dice que tipo es, a un
34     ## valor numerico que si podremos restar sin problemas
35     ## La funcion quedaria asi: (Nip-1)+(1/(dp1+k1))+(1/(dp2+k1))+(1/(dt
        +k2))
36     Po1=port_to_count(c1$id$orig_p);
37     Pd1=port_to_count(c1$id$resp_p);
38     Po2=port_to_count(c2$id$orig_p);
39     Pd2=port_to_count(c2$id$resp_p);
40     ## local t1: double;
41     ## local t2: double;
42     ## t1 = time_to_double(c1$start_time);
43     ## t2 = time_to_double(c2$start_time);

```



```

44 dt=(|c1$start_time| - |c2$start_time|);
45
46
47 ## print fmt("Tiempo paquete 1: %s", t1);
48 ## print fmt("Tiempo paquete 2: %s", t2);
49 print fmt("Diferencia de tiempo: %s", dt);
50
51 resultado=(Nip-1)+(1/((Po1-Po2)+k1))+(1/((Pd1-Pd2)+k1))+(1/(dt+k2));
52
53 return resultado;
54
55 }

```

En este trozo de código se muestra la función que se usa para devolver el resultado de la función de comparación. El resultado siempre es comparado con el umbral que hemos definido antes de lanzar el programa, y una vez que se usa esta función quiere decir que son *comparables*, pero no sabemos todavía si son *emparejables*. Si son emparejables lo sabremos solamente después de que hayamos ejecutado la función y se realice la comparación con el umbral. Para que quede más claro aquí está el código de la comparación con el umbral.

```

1 . . .
2
3     umbral=emparejamiento(c1,c);
4     print fmt("connection_finished");
5     if(umbral>k){
6         ## Si el umbral calculado es mayor que el umbral de comparacion
7         lo aniadimos
8         print fmt("Si son emparejables TCP"); ## Mostramos TCP para
9         saber en que evento se han calculado
10        collection[orig,dest,po,pd][|collection[orig,dest,po,pd]|] = c;
11        informacion_coincidencia(c1, c);
12        if( [orig,dest,po,pd] !in collection_added ){
13            collection_added[orig,dest,po,pd]=vector(c);
14            print fmt("Aniadimos una nueva conexion al vector de
15            coincidencias");
16        } else {
17            ## Si ya esta, lo aniadimos
18            collection_added[orig,dest,po,pd][|collection_added[orig,dest,
19            po,pd]|] = c;
20            print fmt("Ya esta en vector de coincidencias y lo aniadimos")
21            ;
22        }
23    } else{
24        ## Si el umbral calculado es menor que el umbral de comparacion
25        no lo aniadimos
26        print fmt("No son emparejables TCP");
27    }
28 . . .

```

En este ejemplo se calcularía para las conexiones de tipo *TCP*.

La comparación se dará cuando Bro reconozca un flujo de un determinado tipo de protocolo, en nuestro caso será mediante los eventos destinados a reconocer los tipos de protocolos de la *capa de transporte*. Dichos eventos son:

- `connection_established`, el cual se lanza cuando Bro localiza un SYN-ACK que corresponda a un handshake de TCP.
- `connection_finished`, el cual lanza Bro cuando una conexión TCP finaliza de forma normal.
- `udp_request`, el cual se lanza cuando Bro localiza un flujo que corresponde con UDP lanzado desde el origen.
- `udp_reply`, que es lanzado por Bro cuando localiza una respuesta a un flujo del anterior evento.
- `icmp_echo_request`, lanzado por Bro cuando localiza un flujo de tipo ICMP de echo.
- `icmp_echo_reply`, el cual es lanzado por Bro cuando localiza una respuesta a los flujos del evento anterior.

Dentro de estos eventos descritos se realiza la comprobación de que dos flujos se pueden comparar, ya que tienen los mismos IP's y puertos de origen y destino. Una vez en la función de comparación se almacenarán dichos puertos, pasándolos al tipo count para su uso en la función, se establecerán dos constantes, se calculará la diferencia de tiempo y en una variable se almacenará el número de flujos que hay con esos datos. Cuando realicemos esto, aplicaremos la función de cálculo y podremos decir si los flujos son emparejables.

Para mostrar la información de los flujos tenemos dos opciones, de las cuales mostramos el código a continuación:

```
1
2 ## Creo funcion auxiliar para ver la informacion del flujos que son
   coincidentes
3
4 function informacion_coincidencia(c: connection, p: connection){
5   print fmt("Informacion del primer flujo IPo: %s , Po: %s , IPd: %s ,
       Pd: %s ", c$Id$orig-h, c$Id$orig-p, c$Id$resp-h,
       c$Id$resp-p);
6   print fmt("Informacion del flujo coincidente IPo: %s , Po: %s ,
       IPd: %s , Pd: %s ", p$Id$orig-h, p$Id$orig-p, p$Id$resp-h,
       p$Id$resp-p);
7 }
```

```

8
9  ## Funcion auxiliar para mostrar la informacion de un solo flujo
10
11 function informacion_flujo(c: connection){
12     print fmt("Informacion del flujo aniadido IPo: %s , Po: %s , IPd:
        %s , Pd: %s, uid: %s ", c$Id$orig-h, c$Id$orig-p, c$Id$resp-h,
        c$Id$resp-p, c$uid);
13 }

```

La función `informacion_flujo` sirve para mostrar la información del flujo relativa a las IP's y a los puertos que contiene, así como el *UID* del flujo, que es el identificador único que se le asigna automáticamente a cada flujo.

Por su parte la función `informacion_coincidencia` sirve para mostrar la información de dos flujos a la vez, mostrando sus IP's y sus puertos. Esta función será usada para mostrar la información de los dos flujos que son emparejables, siendo el primero de ellos el que se usa para comparar siempre y el segundo es el nuevo flujo que se ha detectado. De esta forma tan sencilla se puede mostrar toda la información interesante sin tener que recorrer al final de la ejecución del programa toda la *tabla de connection*.

Para eliminar los flujos que, por su *timestamp* estén a punto de morir, Bro nos da la opción mediante un evento de gestionar que hacer antes de que sean eliminados de la memoria, dicho evento es:

- `connection_state_removed`, evento que se lanza cuando un flujo activo va a ser eliminado de la memoria.

Cabe destacar que el borrado no es todavía operativo, por lo que en el script puede que este evento esté comentado.

```

1
2  ## Generated when a connections internal state is about to be
   removed from memory. Bro generates this event reliably
3  ## once for every connection when it is about to delete the internal
   state. As such, the event is well-suited for
4  ## script-level cleanup that needs to be performed for every
   connection.
5  ## This event is generated not only for TCP sessions but also for UDP
   and ICMP flows.
6
7  event connection_state_remove(c: connection){
8
9     local orig = c$Id$orig-h;
10    local dest = c$Id$resp-h;
11    local po = c$Id$orig-p;
12    local pd = c$Id$resp-p;
13    local coleccion = collection[orig,dest,po,pd];
14    local tama=|coleccion|;
15

```

```

16
17     for(j in coleccion){
18         if(j+1 >= tama){
19             if(tama==1){
20                 collection [ orig , dest , po , pd ] = vector () ;
21             }
22             if(j+1==tama){
23                 delete collection [ orig , dest , po , pd ] [ tama ]; ## Aqui esta el
                    error
24             }
25             break;
26         } else {
27             collection [ orig , dest , po , pd ] [ j ] = coleccion [ j + 1 ];
28         }
29     }
30
31     print fmt("Terminamos copia y borrado...");
32
33 }

```

En este evento lo que tratamos de hacer es, antes de eliminarlo de la memoria, ver si existe algún flujo que pueda ocupar su lugar siendo el flujo referencia a la hora de comparar flujos. Básicamente lo que hace es comprobar si el tamaño es mayor que 1. Si es 1 solamente tendremos que borrar el vector contenido en la posición de la tabla, y si tenemos que es mayor, tendremos que borrar el primero y mover todos una posición hacia atrás. Nos interesa que este evento funcione, pues si los *timestamps* de dos flujos tienen mucha diferencia los daremos como que no son comparables, cuando si se van actualizando, tendremos más posibilidades de que la clasificación sea correcta.

Para añadir flujos a la tabla de conexiones, tenemos un evento dedicado a ello:

- `new_connection`, Bro lanza este evento cada vez que detecta un flujo que era desconocido.

```

1 ## Cada vez que entra un nuevo flujo compruebo que si esta en la tabla
2 ## Este evento se lanza con cada nueva conexion de un flujo que no sea
   conocido, pero al borrarlo de memoria ser desconocido aunque ya
   lo tengamos en la tabla
3 ## Generated for every new connection. This event is raised with the
   first packet of a previously unknown connection. Bro uses a flow-
   based definition of connection here that includes not only
   TCP sessions but also UDP and ICMP flows.
4
5 event new_connection(c: connection){
6
7     local orig = c$id$orig_h;
8     local dest = c$id$resp_h;
9     local po = c$id$orig_p;

```

```
10 local pd = c$id$resp_p;  
11 print fmt("new_connection");  
12  
13 if( [orig,dest,po,pd] !in collection ){  
14  
15     ## Si no estan los valores clave del flujo lo creamos  
16     collection[orig,dest,po,pd]=vector(c);  
17     informacion_flujo(c);  
18     print fmt("A adimos una nueva conexion");  
19  
20 } else {  
21  
22     ## Si ya esta, lo a adimos  
23     collection[orig,dest,po,pd][collection[orig,dest,po,pd]] = c;  
24     informacion_flujo(c);  
25     print fmt("Ya esta y la a adimos");  
26  
27 }  
28  
29 }
```

Lo que se realiza en este evento es ver si en la tabla global tenemos ya almacenado un flujo de esas características. Si no tenemos uno igual creamos en la tabla para los valores de las IP's origen, destino y puertos de origen y destino un nuevo vector que contenga solamente este nuevo flujo. En caso de que si tengamos los valores ya almacenados solamente tendremos que añadir al final del vector el nuevo flujo. En ambos casos mostraremos la información del flujo.

Por último usamos dos eventos en el programa para ver cuando se lanza y cuando finaliza el programa:

- bro_init, evento que se lanza cuando iniciamos Bro.
- bro_done, evento que se lanza cuando Bro va a terminar.

```
1 ## Evento que se lanza cuando se inicia BRO  
2  
3 event bro_init(){  
4  
5     print fmt("Hora de inicio: %s", current_time());  
6  
7 }  
8  
9 ## Evento que se genera cuando BRO va a tenerminar  
10  
11 event bro_done(){  
12  
13  
14     print fmt("Hora de finalizacion: %s", current_time());  
15  
16 }
```

En el primer evento, que es el que se lanza cuando Bro se ejecuta, mostramos la hora de inicio. En el segundo evento, que solamente se ejecuta cuando Bro va a finalizar, mostramos la hora de finalización.

Capítulo 5

Evaluación y pruebas

Capítulo 6

Conclusiones y trabajo futuro

6.1. Conclusiones

Después de lo visto anteriormente se puede llegar a la conclusión de que mediante un NMS, al cual mediante la agregación de funcionalidades, se le proporciona la capacidad de clasificar el tráfico de una red mediante emparejamiento de flujos. En nuestro caso los protocolos analizados son solamente **TCP y UDP**, es decir, los protocolos de la capa de transporte y en algunos casos también el protocolo ICMP.

Fue muy sencillo poder mostrar los datos de los flujos, pues que se disponga de un tipo de dato que almacene todos los datos correspondientes al flujo hace que trabajar con ello sea muy fácil, incluso mostrar el de todos los flujos que pasan por el programa, y que el rendimiento no se vea afectado. Puede considerarse un inconveniente que no disponga de interfaz, pues en el terminal se puede llegar a confundir las cosas dependiendo de la velocidad con la que saque la información, que sea un lenguaje basado en eventos también puede llegar a ser un problema a la hora de mostrar la información, pues puede ser que estemos mostrando la información de dos flujos que estamos comparando de tipo UDP por ejemplo, y que salte un evento de TCP y se muestre mientras todavía se está mostrando la información del evento de UDP.

6.2. Trabajo futuro

Obviamente este programa al solo poder emparejar flujos mediante el protocolo de transporte se puede quedar corto a la hora de querer obtener un análisis más exhaustivo, de modo que inspeccionemos los paquetes de una forma más profunda, de modo que a este programa se le puede agregar

más funcionalidades haciendo que sea más completo, y clasifiquen además los flujos por el tipo de protocolo en la capa de aplicación pertenecen, con esto nos referimos a *HTTP*, *SMTP*, *FTP*, *DNS* y *demás*. Esto podría llegar a realizarse analizando más detenidamente los puertos. Esta extensión se podría realizar con algunos clasificadores de puertos que ya están realizados y se pueden encontrar con cierta facilidad en *GitHub*.

Bibliografía

- [1] James F. Kurose and Keith W. Rose. *Redes de computadores un enfoque descendente*. Pearson, 2010.
- [2] James F. Kurose and Keith W. Rose. *Redes de computadores un enfoque descendente*, chapter 2. Pearson, 2010.
- [3] James F. Kurose and Keith W. Rose. *Redes de computadores un enfoque descendente*, chapter 3. Pearson, 2010.
- [4] James F. Kurose and Keith W. Rose. *Redes de computadores un enfoque descendente*, chapter 4. Pearson, 2010.
- [5] James F. Kurose and Keith W. Rose. *Redes de computadores un enfoque descendente*, chapter 1. Pearson, 2010.
- [6] Bro Team. Bro indice, . URL <https://www.bro.org>.
- [7] James F. Kurose and Keith W. Rose. *Redes de computadores un enfoque descendente*, page 55. Pearson, 2010.
- [8] José Camacho, Pablo Padilla, Pedro García-Teodoro, and Jesús Díaz-Verdejo. A generalizable dynamic flow pairing method for traffic classification.
- [9] Internet Assigned Numbers Authority (IANA). Service name and transport protocol port number registry. URL <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>.
- [10] Christian Fuchs. Implications of deep packet inspection (dpi) internet surveillance for society. URL <http://fuchs.uti.at/wp-content/uploads/DPI.pdf>.
- [11] Thuy T.T. Nguyen and Grenville Armitage. A survey of techniques for internet traffic classification using machine learning. URL <http://ieeexplore.ieee.org/document/4738466/?reload=true>.

- [12] Álvaro Maximino Linares Herrera. Repositorio del trabajo con bro. URL <https://github.com/Lynares/bro-flows>.
- [13] Bro Team. Descarga de bro, . URL <https://www.bro.org/download/index.html>.
- [14] Kim Davies. Una introducción a iana. URL <https://www.iana.org/about/presentations/davies-atlarge-iana101-paper-080929-es.pdf>.
- [15] Dr. Thomas Porter. The perils of deep packet inspection. URL <https://www.symantec.com/connect/articles/perils-deep-packet-inspection>.
- [16] Bro Team. Arquitectura de bro, . URL <https://www.bro.org/sphinx/script-reference/log-files.html>.
- [17] securitykitten. Finding beacons with bro. URL <https://gist.github.com/securitykitten/a7edcee0932c556d5e26>.
- [18] Bro Team. Instalación de bro, . URL <https://www.bro.org/sphinx/install/index.html>.
- [19] Bro Team. Tipo time, . URL <https://www.bro.org/sphinx/script-reference/types.html?highlight=time#type-time>.
- [20] Bro Team. Tipo connection, . URL <https://www.bro.org/sphinx/scripts/base/init-bare.bro.html#type-connection>.
- [21] Bro Team. Tipo conn, . URL <https://www.bro.org/sphinx/scripts/base/protocols/conn/main.bro.html#type-Conn::Info>.
- [22] Bro Team. Función get_port_transport_proto, . URL https://www.bro.org/sphinx/scripts/base/bif/bro.bif.bro.html#id-get_port_transport_proto.
- [23] Bro Team. Web de bro, . URL <https://www.bro.org/sphinx/intro/index.html>.
- [24] Bro Team. Analizadores de protocolos, . URL <https://www.bro.org/sphinx/script-reference/proto-analyzers.html>.
- [25] Bro Team. Arquitectura de bro, . URL <https://www.bro.org/sphinx/intro/index.html#architecture>.

