Embebidos

Proyecto final: Monitoreo de tráfico en una red local

Equipo: Verónica López, Miguel Guzmán, Roxanna Morales y David Osorio

Introducción.

En el siguiente reporte se muestra el desarrollo del proyecto de monitoreo de una red local para detectar los dispositivos conectados y los paquetes enviados con el fin de presentar dicha información al usuario final mediante una aplicación.

La principal finalidad de ésta aplicación es la de mostrar los logs generados por el monitor de la red, constituido por una Raspberry pi B como instrumento físico con la ayudada del programa Tcpdump y el demonio NetMonServd, ver figura 1.





**SCAN NETWORK APP**

Figura 1. Diseño de la arquitectura del proyecto.

Tcpdump es una herramienta utilizada mediante líneas de comandos que permite el análisis del tráfico que circula en la red. La misma captura en tiempo real los paquetes enviados y recibidos por el ordenador conectado.

Desarrollo.

**Código.**

A continuación, se muestran algunos de los comandos que se usan en el código para lograr la obtención de los datos.

El código se compila con el siguiente comando:

gcc -o NetMonServd NetMonServd.c linked\_list.c

El monitoreo del tráfico se inicia con el siguiente commando:

pi@raspberrypi:~/tcpdump/tcpdump $ sudo ./networkMon.sh

y los logs se almacenan en ./tcp\_logs

Los archivos que se generan con los datos son netMonReport.log, tcpmon.log y tcpmon.log\_p. El archivo que contiene el log de la actividad de red es netMonReport.log, el siguiente es un ejemplo de la información que se obtiene:

-------------------------------------------

Mac Sender: 70:03:7e:86:92:f2

IP Sender: dns1-LEON-megacable.com.mx.domain

Mac Receiver: dc:a6:32:0b:3e:db

IP Receiver: 192.168.0.12.46368

Package Count: 1

Bytes Number: 624

First Time: Sat Nov 30 17:19:36

Last Time: Sat Nov 30 17:19:36

-------------------------------------------

Mac Sender: dc:a6:32:0b:3e:db

IP Sender: 192.168.0.12.46368

Mac Receiver: 70:03:7e:86:92:f2

IP Receiver: dns1-LEON-megacable.com.mx.domain

Package Count: 1

Bytes Number: 524

First Time: Sat Nov 30 17:19:36

Last Time: Sat Nov 30 17:19:36

-------------------------------------------

Finalmente, para detener el monitoreo de la red se ejecuta el siguiente comando:

pi@raspberrypi:~/tcpdump/tcpdump $ sudo ./networkMonEnd.sh

**Aplicación.**

La aplicación está compuesta únicamente con dos páginas, una que es la página de bienvenida (ver la figura 2) y la pagina donde se muestra la información de los logs de una forma más digerible para el usuario (de la figura 3).

A screenshot of a cell phone

Description automatically generated

Figura 2. Página inicial.

A screenshot of a cell phone

Description automatically generated

Figura 3. Página secundaria.

En la página de bienvenida se tiene un menú oculto que se muestra cuando se da click al icono ; el cual se encuentra en la esquina superior izquierda. Para ver una imagen del menú ve la figura 4.



Liga a la pagina donde se muestra la información de los logs

Figura. 3

Figura 4. Menú de la página inicial.

En la página donde se muestra la información de los logs encontramos varios elementos como son dos gráficas y una tabla con la información del log. La primera gráfica es de pastel donde se muestra la relación dispositivo y número de paquetes enviados. La segunda es una gráfica de barras donde se muestra la relación del dispositivo y el número de bytes enviados. La tabla muestra la información del archivo generado por el demonio NetMonServd, donde se puede ver más a detalle lo mostrado en las gráficas, ver la figura 5 y 6.

A screenshot of a cell phone

Description automatically generated

Figura 5. Relación de dispositivo contra paquetes enviados y dispositivo contra bytes enviados.

A screenshot of a social media post

Description automatically generated

Figura 6. Información detallada del log procesado.

La solución está basada en el patrón de diseño MVC, y está construido en el marco de trabajo NoteJS que está basado en el lenguaje JavaScript, en la figura 7 se puede observar cómo está la estructura de las carpetas y en donde se encuentra cada componente de la solución.

A screenshot of a video game

Description automatically generated

Figura 7. Estructura de la aplicación.