

## **REPORTE**

Guerra Leyva Rene  
Ruiz Morua Eduardo

### **Describe a profundidad cómo funciona la biblioteca pcap.**

La librería pcap es una API que se utiliza para la captura de paquetes que está recibiendo una tarjeta de red.

### **¿Cuales son las principales vulnerabilidades de seguridad del protocolo http?**

Que es muy fácil poder agarrar los paquetes de datos que una computadora está recibiendo al utilizar pcap para poder interceptarlos y esto puede ocasionar que al momento que de estar recibiendo contraseñas uno fácilmente las pueda conseguir si no está cifrado.

### **Principales ataques informáticos que explotan el protocolo http. Da una breve descripción de cada uno.**

#### **Ataque man in the middle:**

Se trata de interceptar los datos que se están enviando y recibiendo de un servidor.

#### **Ataque DDoS:**

Se trata de saturar los puertos con cantidades grandes de flujo de información sobrecargando el servidor e impidiendo que los usuarios se conecten a él.

**Además de las preguntas, se debe agregar un pequeño reporte de las particularidades de su código, como son:**

**¿Cuál es el flujo del programa?**

El proceso es elegir el dispositivo de red al que vamos a interceptar, empezamos a capturar con libpcap e imprimimos en pantalla el paquete interceptado y los datos que este contenga.

### **Principales problemas que se encontraron y cómo los solucionaron**

El principal problema convertir el paquete que se encontraba en hexadecimal y convertirlo a structs con los headers de tamaño correcto para imprimir correctamente los campos de los paquetes. Lo solucionamos leyendo el RFC de HTTP y la documentación de pcap que nos dieron una idea clara de en qué parte se van separando los campos.

### **Problemas que no fueron solucionados.**

A veces imprime en terminal caracteres no reconocibles.