# Reporte

García Romo Claudia Fernanda
Marquez Cortés Francisco Javier
Taboada Magallanes Ricardo

## 1. Describe a profundidad la biblioteca pcap.

-Es una interfaz por medio de la cual se pueden capturar y transmitir paquetes a través de la red. Es un driver que extiende el sistema operativo para para proveer aceeso de bajo nivel a la red y es utilizada para acceder a las capas de bajo nivel de la red.

## 2.¿Cuáles son las principales vulnerabilidades de seguridad del protocolo http?

### Vulnerabilidad 1 -CVE-2009-0086 -

Una Vulnerabilidad con ejecución remota de código exite en la manera que Windows HTTP Services especifica el valor que está regresando para un remoto Web Server.

### Vulnerabilidad 2 - CVE-2009-0089 -

Una suplantación de la vulnerabilidad existe en Windows HTTP Services como un resultado de la incompleta validación de la distinción de nombre en un certificado digital. Cuando se combina con otros ataques, tales como DNS spoofing ", esto puede permitir a un atacante con éxito el falso certificado digital de un sitio Web para cualquier aplicación que utiliza Windows HTTP Services.

### Vulnerabilidad 3 -CVE-2009-0550 -

Una vulnerabilidad de ejecución remota de código existe en la forma en que Windows HTTP Services maneja credenciales cuando un usuario se conecta a un servidor Web del atacante. Esta vulnerabilidad permite aun atacante producir las credenciales

de los usuarios y ejecutar código en contexto del usuario conectado, si un usuario está conectado como usuario administrativo.

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

Vulnerabilidades del servidor Web. Este tipo es cada vez más atípico ya que la mayoría de los desarrolladores de servidores Web han aumentado su seguridad con los años;

- Manipulación de URL, incluida la modificación manual de parámetros de URL para modificar el comportamiento esperado del servidor Web;
- Aprovechamiento de las debilidades de los identificadores de sesión y sistemas de autenticación;
- Inyección de código HTML y Secuencia de comandos entre sitios;
- Inyección de comandos SQL.

## Reporte de Particularidades