Instituto Politécnico Nacional

Escuela Superior de Cómputo

Olguín Martínez José Arturo

Grupo: 5CV4

Redes de computadoras

Analizador de protocolos de red

¿QUÉ ES UN SNIFFER?

Un sniffer de red, también conocido como analizador de paquetes, es una herramienta de software o hardware diseñada para monitorizar y capturar el tráfico de datos que circula por una red. Su función principal es permitir a los administradores y profesionales de TI observar y analizar la información que se envía y recibe a través de la red.

Los sniffers operan principalmente en la capa de enlace de datos del modelo OSI. Capturan cada paquete que transita por la red, lo decodifican y presentan los datos en un formato comprensible.

Esto permite a los técnicos diagnosticar problemas, identificar cuellos de botella en el rendimiento y detectar intrusiones

TIPOS DE SNIFFER

- Sniffers Activos: Estos envían solicitudes a dispositivos en la red y analizan las respuestas. Son comúnmente utilizados en pruebas de penetración.
- Sniffers Pasivos: Se limitan a escuchar el tráfico sin interferir, siendo más comunes debido a su naturaleza no intrusiva

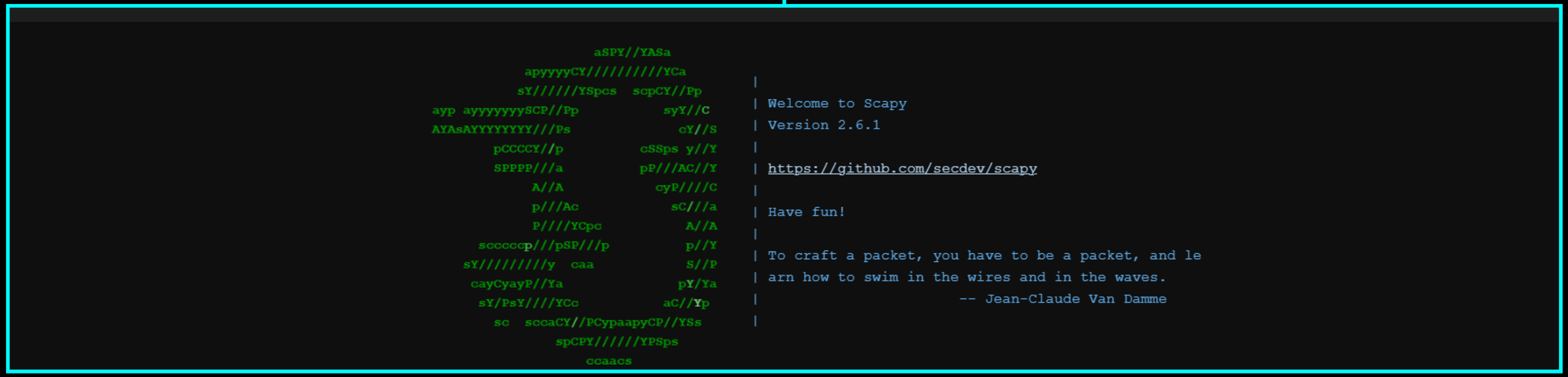
USOS COMUNES

- Identificación de Problemas: Ayudan a diagnosticar fallos en la red.
- Detección de Intrusiones: Monitorean el tráfico para identificar accesos no autorizados.
- Desarrollo de Protocolos: Facilitan el análisis y mejora de protocolos existentes.
- Seguridad: Se utilizan para proteger redes al detectar actividades sospechosas

RIESGOS DE UN SNIFFER

Los sniffer aunque son importantes para la seguridad también puede ser usado de forma maliciosa.
Por ejemplo, un hacker puede emplear un sniffer para interceptar datos sensibles como contraseñas o información personal, especialmente en redes desprotegidas.

Esto subraya la importancia de implementar medidas de seguridad adecuadas para proteger la información transmitida en redes públicas o inseguras.



SCAPY

Scapy es una librería de Python muy poderosa y flexible, se usa para la manipulación de paquetes de red. Esta fue diseñada para permitir a los usuarios construir, enviar, recibir y analizar paquetes de red de manera detallada.

Scapy destaca debido a su enfoque en el control preciso de paquetes. Mientras que otras librerías como Pyshark y Tshark permiten establecer conexiones y manejar protocolos a nivel de aplicación, Scapy opera en un nivel más bajo, ofreciendo capacidades de construcción y manipulación de paquetes a nivel de red.

SCAPY

Características principales:

1. Manipulación de paquetes: Puedes construir paquetes desde cero o modificar los existentes.
2. Soporte para múltiples protocolos: Compatible con una amplia gama de protocolos de red (TCP, UDP, ICMP, ARP, DNS, etc.).
3. Envío y recepción de paquetes: Permite enviar paquetes personalizados y capturar las respuestas.
4. Ampliamente extensible: Puedes crear tus propios protocolos o modificar los existentes.
5. Interactividad: Ideal para tareas de prueba y experimentación en redes.

Ventajas:

- Gran flexibilidad en la construcción y manipulación de paquetes.
- Ideal para simulaciones de red y pruebas de seguridad.
- Permite realizar ataques de prueba éticos (como ARP spoofing).

Desventajas:

- Menor enfoque en el análisis profundo y detallado de capturas de tráfico existentes.
- Puede ser más complicado para usuarios principiantes.

PYSHARK

Características principales:

1. Lectura de archivos pcap: Puedes analizar capturas de tráfico guardadas previamente.
2. Captura en tiempo real: También permite capturar tráfico en vivo directamente desde una interfaz de red.
3. Enfoque en análisis: Facilita la extracción de información como direcciones IP, puertos y datos específicos de protocolos.
4. Integración con TShark: Hereda el poder del motor de análisis de Wireshark.

Ventajas:

- Excelente para el análisis detallado de tráfico de red.
- Fácil de usar si estás familiarizado con Wireshark.
- Soporte para filtrado avanzado de paquetes (basado en filtros de TShark).

Desventajas:

- No permite modificar ni enviar paquetes.
- Depende de TShark, por lo que necesitas instalarlo previamente.

REQUISITOS PARA SCAPY

```
# Proyecto_Redes_Sniffer

# scapy opera de forma normal en linux, tratar de ejecutar en maquina linux

# Si no es una maquina linux se debe instalar Scapy

# Es necesario tener instalado Python a partir de la version 2.5.0+
```

```
# Si no se tiene instalado scapy ejecutar #
## pip install scapy

from scapy.all import sniff, PcapReader, wrpcap, IP, TCP, UDP

```

BIBLIOTECAS PARA SCAPY

GRACIAS