Manual del Usuario – Packet Sniffer “NetSpy”

Versión 1.0

Equipo 4

Esparza Torres Miguel Angel	272437
Mojica Lamas Gustavo Andrés	348175
Muñoz López Bruno Santiago	280023
Vázquez Reyes Diego Alonso	348545

17/12/2024

Índice

1. Introducción

1.1 Breve Descripción del Software

"NetSpy" es un software *Packet Sniffer* diseñado para capturar, analizar y registrar datos transmitidos a través de una red. Utiliza librerías como “pcap” y una interfaz gráfica basada en *ncurses* para facilitar la visualización y manipulación de datos.

Aplicaciones Principales:

- Diagnóstico y resolución de problemas de red.

- Análisis de seguridad y detección de tráfico sospechoso.

- Monitoreo y filtrado de paquetes.

- Exportación de datos capturados para análisis posterior.

1.2 Objetivo del Documento

El objetivo de este manual es proporcionar una guía clara y detallada para instalar, configurar y utilizar "NetSpy". Este documento permite que cualquier usuario pueda capturar y analizar paquetes de red de manera efectiva.

1.3 Público Objetivo

Este manual está dirigido a:

- Estudiantes interesados en redes de computadoras.

- Técnicos y administradores de redes.

- Profesionales en análisis de seguridad informática.

2. Requisitos del Sistema

2.1 Hardware

- Procesador: Intel Core i3 o equivalente.

- Memoria RAM: 4 GB (8 GB recomendados).

- Espacio en Disco Duro: 500 MB libres.

2.2 Software

- Sistema Operativo Compatible: Linux (Ubuntu 20.04 o superior).

- Dependencias:

  - libpcap-dev.

  - ncurses.

  - Compilador gcc.

3. Instalación

3.1 Descarga del Software

1. Clona el repositorio desde: https://github.com/WeroML/proyectopacketsniffer.

2. Accede al directorio del proyecto (esto depende de donde hayas guardado el programa, se deberá acceder a dicha ruta desde una terminal).

3.2 Ejecución del Script de Instalación

1. Asegúrate de que el archivo install_netspy.sh esté en el directorio del proyecto.

2. Dale permisos de ejecución al script:

   “chmod +x install_netspy.sh”

3. Ejecuta el script como superusuario:

   “sudo ./install_netspy.sh”

3.3 Verificación de la Instalación

1. Ejecuta el programa (Tener una terminal de 140x40):

   “sudo ./netspy”

2. Verifica que la interfaz principal cargue correctamente y que puedas seleccionar adaptadores de red.

4. Guía de Uso

4.1 Interfaz Principal

El programa utiliza varias ventanas:

- Ventana Principal: Muestra el estado del programa (captura activa/inactiva) y las opciones disponibles.

- Ventana de Paquetes: Lista los paquetes capturados en tiempo real.

- Ventana de Detalles: Muestra información detallada de un paquete seleccionado.

- Ventana RAW: Visualiza datos crudos del paquete en formato hexadecimal.

Controles principales:

- `ESPACIO`: Iniciar/Detener captura de paquetes.

- `F`: Configurar filtros.

- `N`: Desactivar filtros activos.

- `P`: Seleccionar un paquete para ver detalles.

- `X`: Exportar datos a un archivo CSV.

- `Q`: Salir del programa.

4.2 Funciones Principales

1. Captura de Paquetes:
   - Selecciona el adaptador de red y presiona `ESPACIO` para iniciar la captura.
2. Filtrado:
   - Usa `F` para elegir filtros por IP, protocolo o puerto.
3. Visualización Detallada:
   - Presiona `P` y selecciona un paquete para ver información detallada en las ventanas.
4. Exportación:
   - Presiona `X` para guardar los datos capturados en un archivo CSV.

4.3 Ejemplo Práctico

1. Inicia el programa.

2. Presiona `ESPACIO` para capturar paquetes.

3. Aplica un filtro (por ejemplo, IP origen) usando `F`.

4. Selecciona un paquete con `P` y examina sus detalles.

5. Exporta los resultados a CSV con `X`.

5. Solución de Problemas (Troubleshooting)

Problemas Comunes y Soluciones

- El programa no se ejecuta: Verifica que tengas permisos de superusuario (sudo).

- No captura paquetes: Asegúrate de que el adaptador de red esté configurado correctamente.

- Errores al aplicar filtros: Verifica que los valores ingresados sean válidos (ej. IP o protocolos).

6. Preguntas Frecuentes

1. ¿Qué protocolos soporta el software?

   - TCP, UDP, ICMP, entre otros.

2. ¿Puedo exportar capturas a Wireshark?

   - Sí, los datos exportados en CSV pueden ser analizados con otras herramientas.

7. Créditos y Contacto

Equipo 4.

Contacto: Equipo 4.

Reconocimientos: Uso de librerías libpcap y ncurses.