

# Informe de Análisis de Tráfico -TCPDump

Curso “Introducción al Análisis de Redes” – Security Blue Team

---

## Tabla de contenidos

1. [Resumen ejecutivo](#)
  2. [Objetivo](#)
  3. [Entorno y herramientas](#)
  4. [Metodología](#)
  5. [Resultados](#)
    - [5.1 PCAP4](#)
    - [5.2 PCAP5](#)
  6. [Conclusiones y lecciones aprendidas](#)
  7. [Recomendaciones](#)
  8. [Referencias](#)
  9. [Anexos](#)
- 

## 1. Resumen ejecutivo

Se analizaron dos capturas de tráfico (.pcap), (PCAP 4 y PCAP 5) suministradas por el curso gratuito de Security Blue Team para adquirir destrezas básicas en TCPDump. Las actividades consistieron en filtrado de paquetes, conteo rápido y extracción de metadatos (versiones de software, nombres de archivos, puertos y marcas de tiempo).

---

## 2. Objetivo

- Dominar filtros y contadores básicos de TCPDump.
  - Replicar consultas típicas de Wireshark en CLI.
  - Documentar comandos + resultados para futura automatización.
-

### 3. Entorno y herramientas

Elemento	Descripción
Sistema operativo	Kali Linux 2024.2 (VM)
Analizador de paquetes	tcpdump v4.99.x
Capturas analizadas	pcap4.pcap, pcap5.pcap (descargadas del portal del curso)
Conectividad	Red NAT (sin exposición directa a Internet)
Consideraciones de seguridad	Archivos verificados por Security Blue Team como no maliciosos; descarga efectuada en VM aislada por precaución.

### 4. Metodología

#### 1. Visión general preliminar

- `tcpdump -nn -vv -r <pcap>` para identificar protocolos, puertos y hosts predominantes sin resolución DNS.
- Registro de tiempo total y tamaño de cada captura para dimensionar el ejercicio.

#### 2. Diseño de filtros específicos

- **Capa 3/4** → Selectores `udp`, `tcp`, `ip[8]==TTL`, `tcp[tcpflags]&0x12==0x12`.
- **Capa 7 / Strings** → `-A + grep -Ei 'png|zip|openssh|chrome'`.
- Validación de cada filtro con `--count` para medir impacto antes de volcar datos.

#### 3. Extracción de indicadores

- Métricas de volumen (`--count`, `wc -l`) y temporales (`-tttt`) para series cronológicas.
- Conversión de campos binarios → hex o decimal (e.g., checksum, flags) con `printf "%x"` y `bc`.

#### 4. Verificación cruzada

- Comparación de salidas con Wireshark (*ground truth*) en caso de dudas (p. ej. checksum `0xCFD3`).
- Uso de *tshark* para confirmaciones rápidas (`tshark -r <pcap> -Y 'ip.ttl==38'`).

5. **Documentación** de cada hallazgo con captura de pantalla (ver Anexos) y breve explicación.

## 5. Resultados

### 5.1 PCAP 4

#	Pregunta	Procedimiento	Respuesta
1	Paquetes UDP capturados	<code>tcpdump -r SBT-PCAP4.pcap udp   wc -l</code>	<b>3290</b>
2	Paquetes TCP con <b>**SYN + ACK**</b>	<code>tcpdump -r SBT-PCAP4.pcap 'tcp[tcpflags] &amp; (tcp-syn tcp-ack) == (tcp-syn tcp-ack)'   wc -l</code>	<b>20</b>
3	Versión de <b>**Chrome**</b> hacia <b>*securityblue.team*</b>	<code>tcpdump -A -r SBT-PCAP5.pcap   grep -E "Chrome securityblue.team"</code>	<b>80.0.3987.87</b>
4	Paquetes con <b>**TTL 38**</b>	<code>tcpdump -r SBT-PCAP4.pcap 'ip[8]==38'   wc -l</code>	<b>710</b>

### 5.2 PCAP 5

#	Pregunta	Procedimiento	Respuesta
1	Archivo <b>** .png **</b> servido por <b>192.168.56.111</b>	<code>tcpdump -vvv -r SBT-PCAP5.pcap   grep OpenSSH</code>	<b><i>proprietary.png</i></b>
2	Versión de <b>**OpenSSH**</b> del servidor	<code>tcpdump -vv -r SBT-PCAP5.pcap \   grep OpenSSH</code>	<b>7.9p1</b>
3	Puerto que sirve el archivo <b>** .zip **</b>	<code>tcpdump -A -n -l -r SBT-PCAP5.pcap   grep ".zip"</code>	<b>3016</b>
4	Timestamp del paquete con checksum TCP <b>**53203 (0xCFD3)**</b>	<code>tcpdump -x -r SBT-PCAP5.pcap "tcp[16:2]=5302"</code>	<b>06:04:46.207925</b>

---

## 6. Conclusiones y lecciones aprendidas

- ``tcpdump --count`` agiliza métricas (no hace *\*dump\** completo).
  - ``-A`` es imprescindible para extraer nombres de archivos en HTTP.
  - Filtrar flags con valores hex/dec (``0x12 → 18``) evita confusión.
  - Hallar checksums específicos requiere combinar salida hex (``-x``) + pipes a ``grep``.
- 

## 7. Recomendaciones

1. Crear un *\*\*cheat-sheet\*\** de flags TCP, offsets IP y ejemplos.
  2. Automatizar reportes con pequeños scripts Bash (``tshark`` + ``awk/wc``).
  3. Revisar ``tcpdump -x -s0`` para análisis de checksums y firmas binarias.
- 

## 8. Referencias

- Security Blue Team – *\*Network Analysis Training (Beginner)\**
  - Manuales ``tcpdump(8)`` y ``grep(1)``
  - Baeldung – “Grep show surrounding lines”
- 

## 9. Anexos

Las capturas de pantalla *\*\*A-1 ... A-12\*\** que ilustran cada pregunta se encuentran en la carpeta ``Imagenes/`` del repositorio.

Cada imagen está enlazada en el README para consulta rápida.