Informe de Análisis de Tráfico - Wireshark Challenge

Curso "Introducción al Análisis de Redes" – Security Blue Team

---

Tabla de contenidos

---

1. Resumen ejecutivo

Se analizaron dos capturas de tráfico (.pcap) suministradas por el curso gratuito de Security Blue Team para adquirir destrezas básicas en Wireshark. Las actividades consistieron en aplicar filtros, explorar estadísticas y extraer indicadores clave como protocolos, direcciones IP, credenciales y puertos utilizados por un atacante.

---

2. Objetivo

- **Desarrollar familiaridad práctica** con la interfaz de Wireshark.
- **Aplicar filtros** (display & estadísticos) para responder preguntas dirigidas.
- **Identificar** artefactos relevantes: protocolos, IPs, puertos, contraseñas, nombres de archivo.

---

3. Entorno y herramientas

Elemento	Descripción
Sistema operativo	**Kali Linux 2024.2** (VM)
Analizador de paquetes	**Wireshark 4.2.x** (preinstalado en Kali)
Capturas analizadas	pcap1.pcap, pcap2.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. **Apertura** de cada .pcap en Wireshark.
2. **Aplicación de filtros rápidos** en la barra *Display Filter* (icmp, dns, ftp, etc.).
3. **Uso de menús estadísticos** (Statistics › Endpoints, Protocol Hierarchy) para identificar hosts y cargas de bytes.
4. **Seguimiento de flujos** (Follow TCP/HTTP Stream) para inspeccionar credenciales y nombres de archivo.
5. **Documentación** de cada hallazgo con captura de pantalla (ver Anexos) y breve explicación.

---

5. Resultados

5.1 PCAP 1

#	Pregunta	Procedimiento	Respuesta
1	**¿Qué protocolo se utilizó en el puerto 3942?**	Statistics › Endpoints › UDP → clic derecho sobre puerto 3942 → *Apply as filter › Selected*	**SSDP**
2	**¿Cuál es la IP del host al que**	Filtro icmp → observar solicitudes Echo (ping)	**8.8.4.4**

	se hizo ping dos veces?		
3	**¿Cuántos paquetes "DNS Query Response" fueron capturados?**	Filtro dns → seleccionar 1.er paquete con "Standard query response" → Apply as filter › Selected	**90 paquetes**
4	**¿Qué host envió la mayor cantidad de bytes?**	Statistics › Endpoints › IPv4 → ordenar por *Bytes* (Tx) descendente	**115.178.9.18**

5.2 PCAP 2

#	Pregunta	Procedimiento	Respuesta
1	**Contraseña de WebAdmin**	Filtro http → paquete ID 2141 (GET password.txt) → *Follow HTTP Stream*	**sbt123**
2	**Versión del servidor FTP del atacante**	Filtro ftp and ip.src == 192.168.56.1 → paquete 4243 → campo *Server Version* en cabecera FTP	**pyftpdlib 1.5.5**
3	**Puerto usado para acceder al host Windows (192.168.56.103)**	Filtro ip.src == 192.168.56.1 and ip.dst == 192.168.56.103 and tcp.flags.ack == 1 → primer paquete	**8081**
4	**Archivo confidencial extraído**	Paquete 4130 → *Follow TCP Stream* → búsqueda de "confidencial"	**Información_del_empleado_CONFIDENCIAL.txt**
5	**Archivo de log creado a las 04:51 AM**	Mismo flujo TCP → búsqueda ".log"	**LogFile.log**

6. Conclusiones y lecciones aprendidas

- Los filtros de Wireshark permiten **aislar rápidamente** conversaciones relevantes (por protocolo, IP o banderas).
- El menú **Protocol Hierarchy** agiliza la identificación de servicios inusuales sin revisar todo el tráfico.
- El **seguimiento de flujos** (TCP/HTTP) es clave para extraer credenciales y nombres de archivo sin reconstruir manualmente las tramas.
- Practicar con .pcap seguros en un entorno aislado brinda confianza antes de analizar capturas reales potencialmente hostiles.

---

7. Recomendaciones

1. Mantener **listas personalizadas de filtros** para agilizar futuros análisis (e.g., http.request, dns.flags.response == 1).
2. Automatizar la exportación de estadísticas con tshark dentro de scripts de línea de comandos para laboratorios repetitivos.
3. Documentar siempre evidencias con **hashes de archivos** .pcap y capturas de pantalla fechadas, para trazabilidad.

---

8. Referencias

- Security Blue Team – *Introduction to Network Analysis* (curso gratuito).
- Wireshark User Guide, v4.2.
- RFC 792 (ICMP), RFC 1035 (DNS).

---

9. Anexos

Nota: Las siguientes imágenes se incluyen en la carpeta images/ del repositorio.

#	Figura	Descripción
1	A-1	Aplicación de filtro UDP 3942 mostrando tráfico SSDP
2	A-2	Solicitudes ICMP Echo a 8.8.4.4
3	A-3	Estadística de Endpoints IPv4 con orden de bytes transmitidos (vista 1)
4	A-4	Estadística de Endpoints IPv4 con orden de bytes transmitidos (vista 2)
5	A-5	Endpoints IPv4 ordenados por bytes transmitidos (115.178.9.18 en primer lugar)
6	A-6	HTTP Stream – GET /password.txt (muestra usuario WebAdmin)
7	A-7	HTTP Stream – Respuesta que revela sbt123
8	A-8	Vista del tráfico HTTP completo para confirmar la credencial
9	A-9	Cabecera FTP con versión pyftpdlib 1.5.5
10	A-10	Primer paquete TCP al puerto 8081 (SYN o ACK inicial)
11	A-11	TCP Stream con Información_del_empleado_CONFIDENCIAL.txt
12	A-12	TCP Stream identificando LogFile.log a las 04:51 AM