

**Centro iFP   
Actividad Evaluabl 2ª Evaluación**

**Memoria Técnica**

**Script de Host activos y Calculadora de direcciones IP en binario.**

**1. Configuración inicial:**



- @echo off: Esta línea desactiva la visualización de los comandos en la consola mientras se ejecuta el script.

- cls: Este comando limpia la pantalla de la consola para una mejor presentación.

**2. Inicio del archivo HTML:**

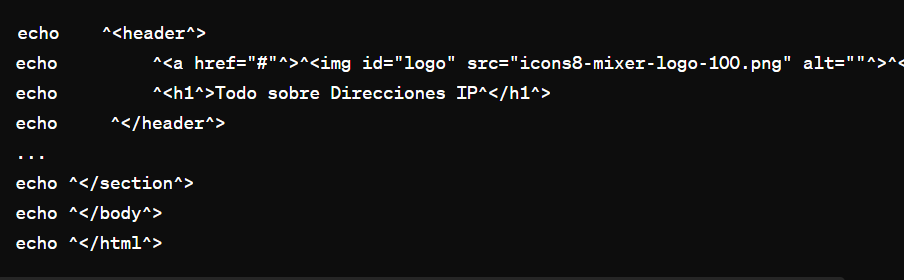


- Se inicia la generación del archivo HTML mediante un bloque de código encapsulado entre paréntesis ( ). Cada echo imprime líneas de código HTML en el archivo resultado.html.



**Centro iFP   
Actividad Evaluabl 2ª Evaluación**

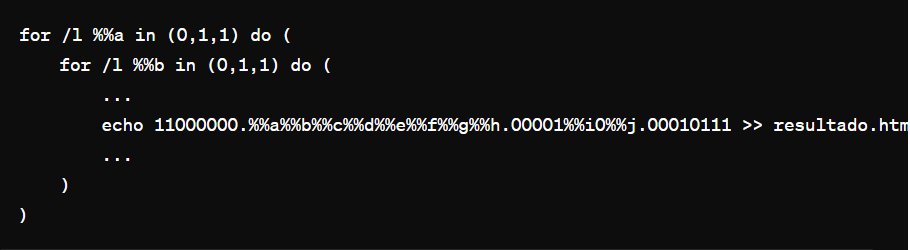
**3. Sección de información sobre las direcciones IP:**



- Sección que incluye información sobre las direcciones IP, como su definición, proceso de obtención, seguridad, y uso en diferentes contextos.

- Se utiliza una combinación de etiquetas HTML para estructurar la información y darle formato adecuado.

**4. Generación de direcciones IP:**



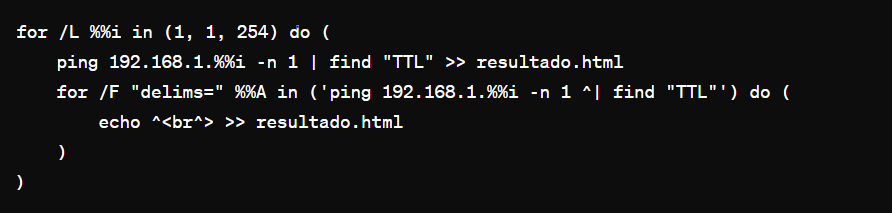
- Se utilizan bucles for anidados para generar direcciones IP de forma dinámica.

- Cada iteración del bucle genera una dirección IP y la agrega al archivo HTML resultado.html.



**Centro iFP   
Actividad Evaluabl 2ª Evaluación**

**5. Escaneo de direcciones IP activas:**



- Se escanean las direcciones IP en un rango específico (192.168.1.1 a 192.168.1.254) para detectar dispositivos activos en la red local.

- Se utiliza el comando ping para enviar un paquete ICMP a cada dirección IP y se busca la cadena "TTL" en la respuesta para determinar la actividad del dispositivo.

- Si se encuentra la cadena "TTL", se asume que la dirección IP está activa y se agrega al archivo HTML.

**6. Apertura del archivo HTML:**



- Finalmente, el script abre el archivo HTML resultado.html en el navegador web predeterminado del sistema.

Finalmente, el script abre el archivo HTML resultado.html en el navegador web predeterminado del sistema.

**Centro iFP   
Actividad Evaluabl 2ª Evaluación**

**Sniffer Captura de tráfico de red.**

**Objetivo:**

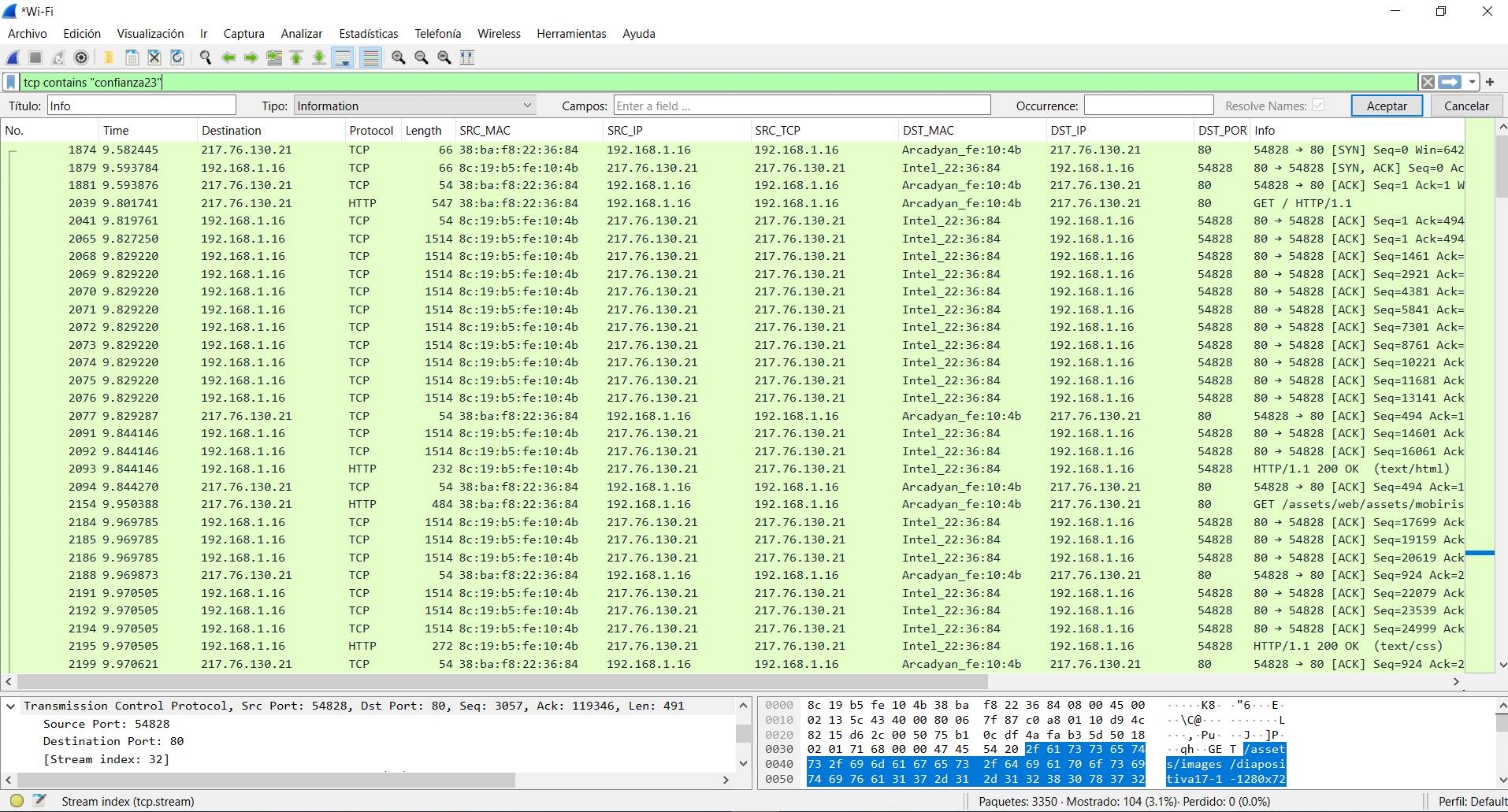
Realizar la captura de tráfico de red local en el equipo, simulando la operación normal de un usuario. Se busca capturar una petición web a la página principal y subpáginas del dominio http://www.confianza23.es.

**Entradas:**

Petición web por HTTP a la web www.confianza23.es, desde navegador, TELNET al puerto 80 u otra petición simulando un acceso web (por ejemplo, wget).

**Salidas:**

1. Formato del Fichero: .pcap o .pcapng con nombre estándar.
2. Campos del Fichero:
3. Dirección MAC de origen (resuelta)
4. Dirección IP de origen
5. Puerto de origen
6. Dirección MAC de destino (no resuelta)
7. Dirección IP de destino
8. Puerto de destino (resuelto)
9. Protocolo
10. Campo de información





**Centro iFP   
Actividad Evaluabl 2ª Evaluación**

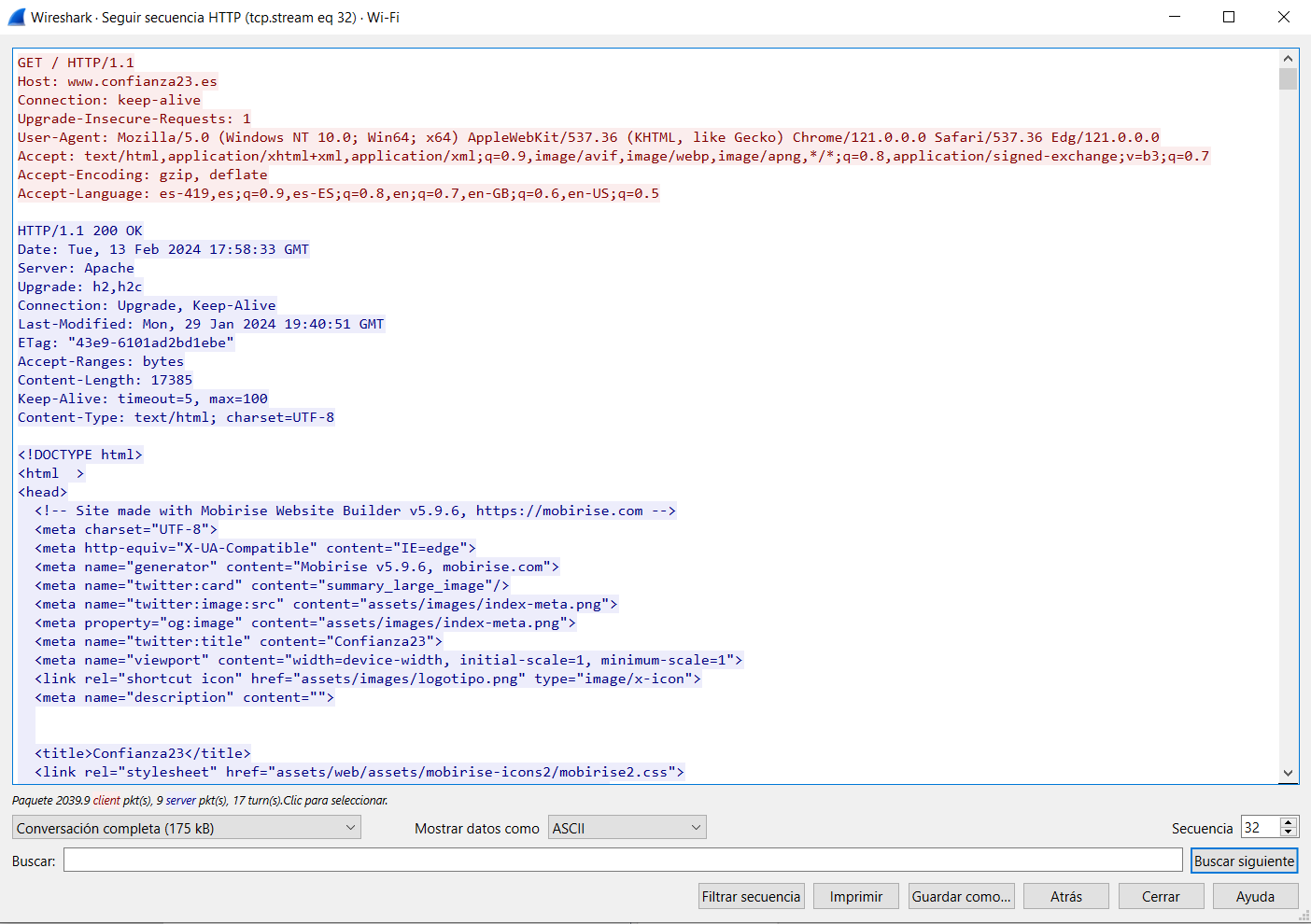
**Contenido del Fichero:**

Solo registros de conexiones en el stream marcado, incluyendo peticiones TCP del triple hanshaking, petición HTTP y respuesta del código HTML.

Filtro para incluir solamente conexiones relevantes, sin ruido de otros streams.

**Adjuntos Requeridos:**

Captura de pantalla del flujo de tráfico web, mostrando la decodificación del protocolo HTTP para ese stream.



Formato de Salida:

Fichero: .pcap o .pcapng

**Filtros Utilizados:**

Documentación detallada de los filtros empleados para la captura y exportación del tráfico.





**Centro iFP   
Actividad Evaluabl 2ª Evaluación**

**Network\_Scanner\_Escaneador\_de\_red.**

**Pasos:**

**1. Definición del Alcance del Escaneo:**

- Identificar el rango de direcciones IP de las distintas salas (por ejemplo, 192.168.128.0 / 22).

- Establecer la ruta predeterminada (por ejemplo, 192.168.128.1).



**2. Utilización de la Herramienta Nmap:**

- Descargar e instalar la versión apropiada de Nmap para tu sistema operativo (Windows/Linux).

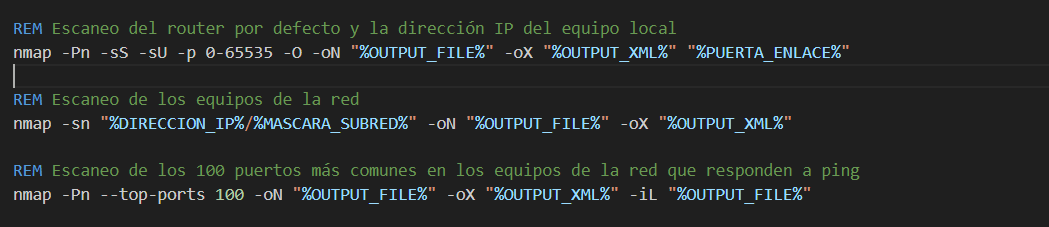
- Considerar utilizar el entorno gráfico Zenmap para facilitar la configuración y visualización de los escaneos.

**3. Configuración de Parámetros de Escaneo:**

- Seleccionar los niveles de escaneo apropiados según los requisitos del ejercicio.

- Utilizar las combinaciones de parámetros de escaneo proporcionadas como referencia (por ejemplo, Intense scan, Quick scan, etc.).

- Personalizar los parámetros según el alcance y las necesidades específicas del ejercicio.





**Centro iFP   
Actividad Evaluabl 2ª Evaluación**

**4. Ejecución del Escaneo:**

- Ejecutar Nmap con los parámetros configurados en el rango de direcciones IP especificado.

- Supervisar el progreso del escaneo y asegurarse de que se estén capturando los datos requeridos.

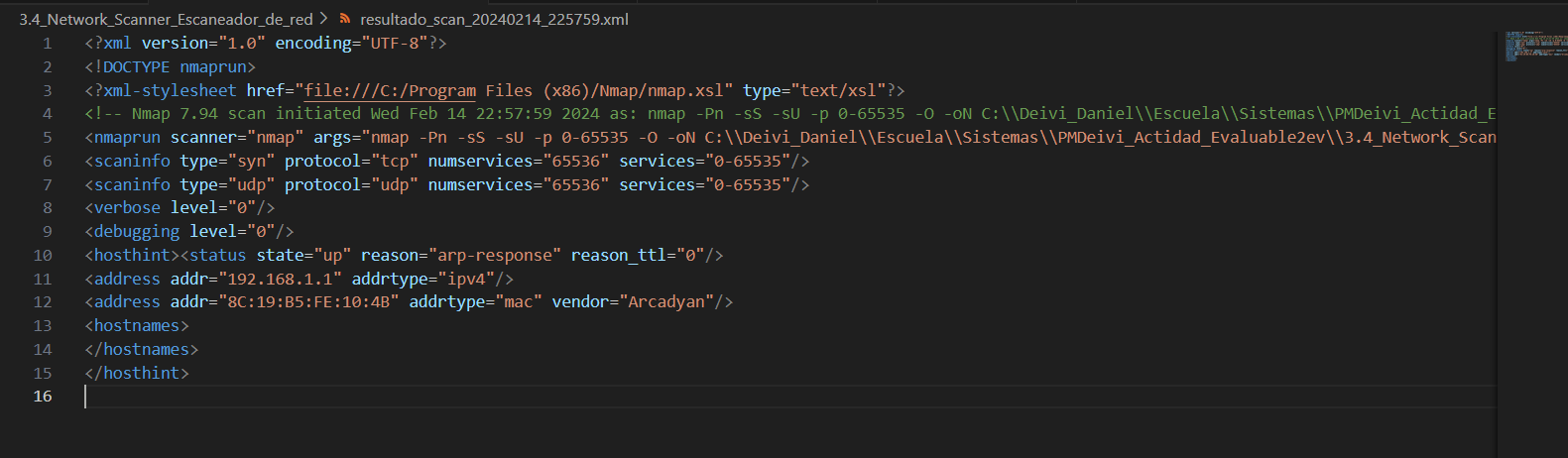
**5. Análisis de Resultados:**

- Revisar los resultados del escaneo y analizar la información recopilada.

- Identificar los equipos visibles a nivel IP que responden al ping ICMP.

- Revisar el listado completo de todos los puertos TCP y UDP para los equipos que responden al ping, junto con su estado (abierto, cerrado, filtrado).

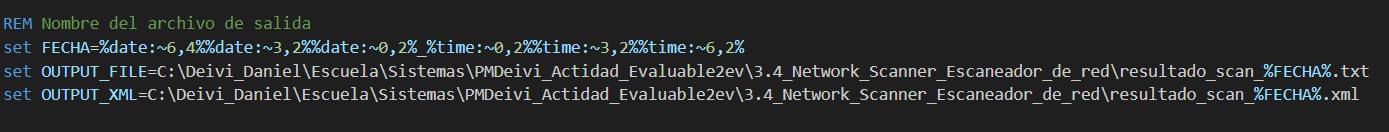
- Identificar el servicio más probable en ejecución en cada puerto según el estándar de mapeo de puertos con servicios de la IANA.



**6. Generación de Salidas:**

- Redireccionar la salida estándar de pantalla a un fichero ASCII.

Generar un fichero XML con los resultados del escaneo.





**Centro iFP   
Actividad Evaluabl 2ª Evaluación**



**Centro iFP   
Actividad Evaluabl 2ª Evaluación**



**Centro iFP   
Actividad Evaluabl 2ª Evaluación**



**Centro iFP   
Actividad Evaluabl 2ª Evaluación**



**Centro iFP   
Actividad Evaluabl 2ª Evaluación**