





# Inteligencia Activa

**MATERIA: ANALISIS DE VULNERABILIDADES**  
**ALUMNO: SERGIO BENJAMÍN TORRES PÉREZ**  
**GRADO Y GRUPO: 7-N**  
**MATRICULA: A200248**  
**DOCENTE: DR GUTIÉRREZ ALFARO LUIS**



# -Análisis de dispositivos y puertos con nmap

## -Parametros opciones de escaneo de nmap

Monitorizar una red es una tarea muy importante para todo administrador de sistemas, pues permite conocer lo que ocurre, que dispositivos están conectados, que IPs y puertos están siendo utilizados y mucha otra información para mantener la seguridad de la red.

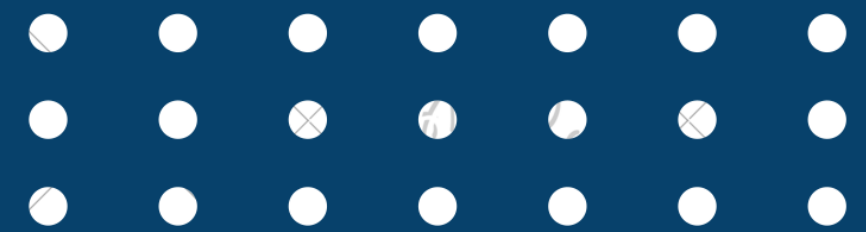
Entre las herramientas de análisis de puertos y monitorización de redes, nmap es una de las más utilizadas gracias a su gran versatilidad y usabilidad, pero vamos a empezar desde el principio.

### **Escaneo del sistema operativo**

Además de los servicios y sus versiones, Nmap puede proporcionar información sobre el sistema operativo subyacente mediante huellas dactilares de TCP/IP. Nmap también intentará encontrar el tiempo de actividad del sistema durante una exploración del sistema operativo.



# Full TCP scan



Un "Full TPC scan" (escaneo completo de TPC) se refiere a un análisis exhaustivo y detallado de las amenazas, vulnerabilidades o actividades maliciosas en una red o sistema utilizando técnicas de inteligencia activa. TPC generalmente se refiere a "Transmission Control Protocol" (Protocolo de Control de Transmisión), que es un protocolo de comunicación utilizado en Internet para transmitir datos de manera confiable entre dispositivos.

En el contexto de seguridad cibernética, un escaneo de TPC completo implica la búsqueda minuciosa de posibles debilidades o problemas de seguridad en las comunicaciones y conexiones utilizando este protocolo. Puede involucrar la detección de puertos abiertos, la identificación de servicios y aplicaciones en ejecución, y la evaluación de posibles riesgos para garantizar que la red o sistema estén protegidos contra posibles amenazas.



# Stealth scans

Los tipos de escaneo sigiloso son aquellos en los que las banderas de paquetes hacen que el sistema objetivo responda sin tener una conexión completamente establecida. Los hackers utilizan el escaneo sigiloso para eludir el sistema de detección de intrusos (IDS), lo que lo convierte en una gran amenaza.

Algunas exploraciones furtivas comunes son las siguientes:

FIN scans (finalizados). Estos envían paquetes FIN con una bandera establecida. Si se devuelve un RST, el puerto se considera abierto; si no se recibe nada, se considera cerrado.

NULL scans. No establecen ninguna bandera en el paquete TCP. En otras palabras, la cabecera de banderas TCP se establece en 0, y los protocolos de respuesta son los mismos que los escaneos FIN.

Xmas scans. Utilizan las banderas FIN, URG (urgente) y PSH (push), que iluminan el paquete como un árbol de Navidad. Si se recibe un paquete RST, el puerto se considera cerrado; la ausencia de respuesta indica un estado abierto o filtrado. Un error ICMP unreachable también indica un puerto filtrado.



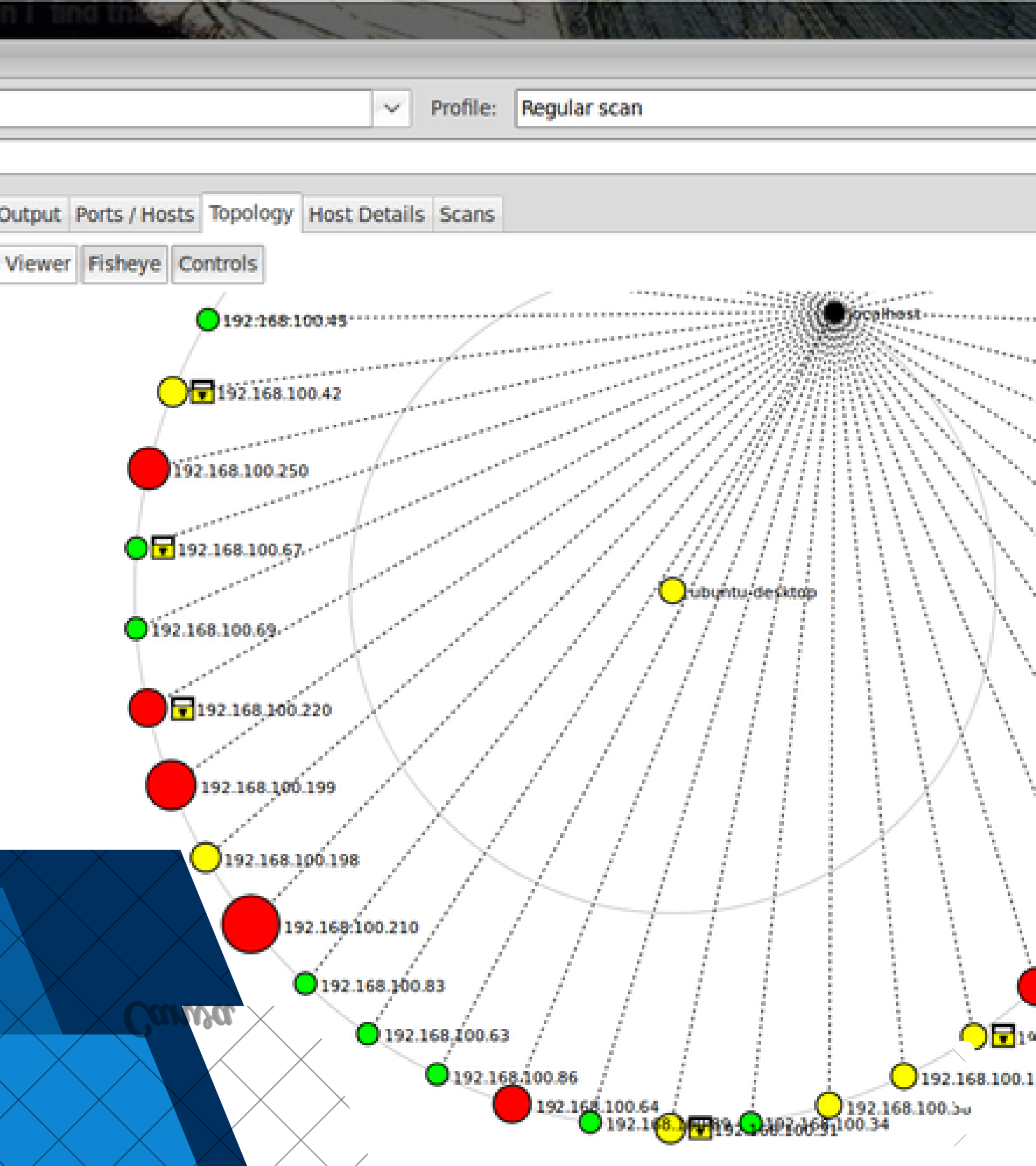
# Fingerprintig

El fingerprinting o la huella digital es toda aquella información sistemática que dejamos sobre un dispositivo informático cada vez que lo utilizamos.

Los datos obtenidos permiten determinar de manera inequívoca el dispositivo empleado y, de esta forma, poder llegar a perfilar y conocer la actividad del usuario, ya sea una persona física o jurídica.

Es decir, el fingersprinting es una técnica que permite obtener información de una persona o empresa a través de los sistemas informáticos. Muchas entidades buscan monitorizar la actividad de los usuarios, algunas para realizar un mejor marketing con publicidad personalizada, otras para detectar posibles actividades fraudulentas o delictivas en Internet.





# Zenmap

Zenmap es una interfaz gráfica de usuario para Nmap. Es un software gratuito y de código abierto que te ayuda a comenzar a utilizar Nmap. Además de proporcionar mapeos de red visuales, Zenmap también te permite guardar y buscar tus escaneos para uso futuro. Además de proporcionar mapeos de red visuales, Zenmap también te permite guardar y buscar tus escaneos para uso futuro.



# Análisis traceroute

Traceroute permite ver por dónde pasa un paquete antes de llegar a su destino final (no es una conexión directa, pasa por distintos dispositivos).

El análisis de estos datos es de información, ya que no se obtiene el permiso para escanear o hacer auditoria de pentesting a ninguno de los dispositivos por el cual pasa un paquete antes de llegar a su destino final.



## ¿Qué hace Traceroute?

Funciona al enviar paquetes de Protocolo de mensajes de control de Internet (ICMP), y cada enrutador involucrado en la transferencia de datos recibe estos paquetes. Los paquetes de ICMP proporcionan información sobre si los enrutadores utilizados en la transmisión pueden transferir los datos de manera efectiva.