

# INTELIGENCIA ACTIVA

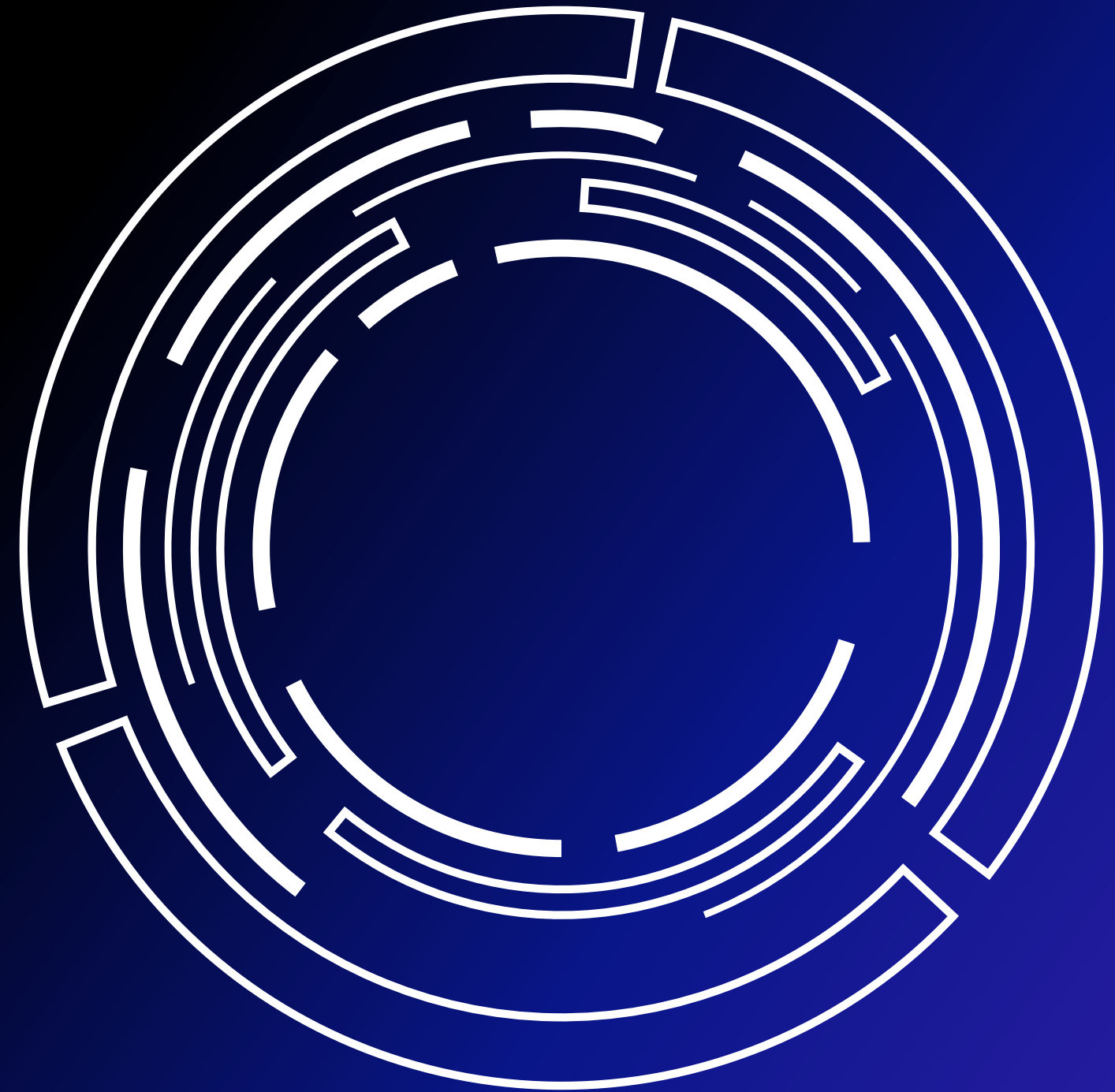
UNIVERSIDAD AUTÓNOMA DE CHIAPAS  
LICENCIATURA EN INGENIERÍA EN DESARROLLO  
Y TECNOLOGÍAS DE  
SOFTWARE

ANÁLISIS DE VULNERABILIDADES  
DOCENTE: DR. LUIS GUTIÉRREZ ALFARO  
RUBEN OCTAVIO RODRÍGUEZ CANO - A200113

7º N

# STEALTH SCAN

Los tipos de Stealth Scan se refiere a aquellos en los que los paquetes designados provocan que el sistema objetivo responda sin tener una conexión completamente establecida. Los hackers utilizan el stealth scan o "escaneo sigiloso" para poder eludir el sistema de detección de intrusiones (IDS), lo que lo convierte en una amenaza muy a tomar en cuenta.





# FINGERPRINTING

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.





# TÉCNICAS DE FINGERPRINTING

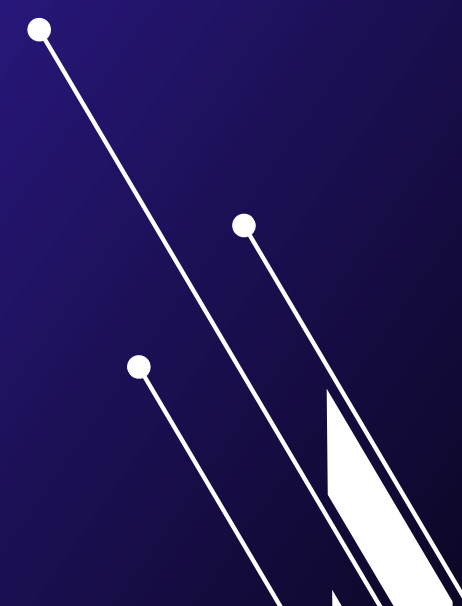
## COOKIES

Es una técnica de seguimiento que consiste en ficheros que se encuentran en el dispositivo del usuario y que son creados por la web de un proveedor de servicios.

Se utilizan para mejorar la experiencia del usuario en la página o analizar estadísticas de ésta. A través de las cookies se puede realizar un perfilado bastante exhaustivo del usuario.

## SNIFFING

Es una técnica que permite escuchar todo lo que ocurre en una determinada red. Pueden obtener todo el tráfico de información que esté circulando en la red en la que esté conectado el dispositivo.



# TRACEROUTE

## DEFINICION

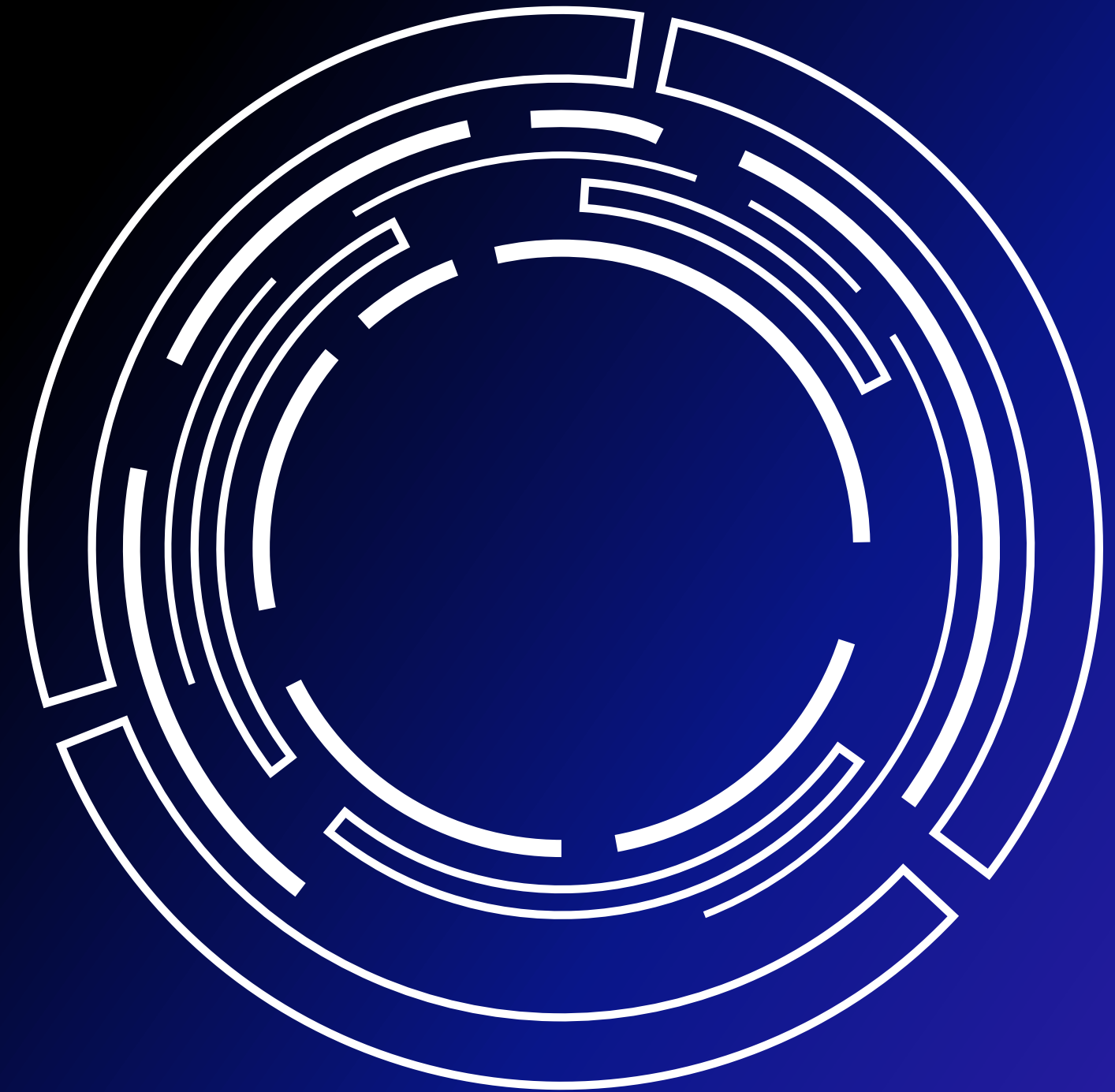
El comando Tracert se ejecuta en la consola de símbolo de sistema en los sistemas operativos Windows. Gracias a este comando, podremos seguir la pista a los paquetes que vienen desde un host. Cuando ejecutamos el comando «Tracert» obtenemos una estadística de la latencia de red de esos paquetes, lo que es una estimación de la distancia (en saltos) a la que están los extremos de la comunicación.

## TRaceroute

La herramienta traceroute es exactamente la misma que el tracert, pero se denomina de otra forma, aunque internamente puede hacer uso de diferentes protocolos, ya que en algunos sistemas operativos se hace uso del protocolo ICMP Echo Request/reply, y en otros de hace uso de mensajes UDP directamente para comprobar cuántos saltos hay de un equipo a otro.

# ZENMAP

Zenmap se define como la interfaz gráfica de usuario oficial de Nmap, que permite usar el programa de manera práctica, cómoda, clara y más organizada. Esta interfaz es ideal para expertos y principiantes, aunque también depende del gusto y hay quienes prefieren su uso directamente en la consola.





# FULL TCP SCAN

## TCP Connect Scan

Es un proceso de exploración de puertos el cual necesita el intercambio de tres vías para poder realizar de forma completa la e

Se llama Connect Scan, ya que implementa una llamada al sistema de tipo Connect, para así saber de forma rápida el estado del puerto. Exploración de puertos.

## TCP SYN Scan

Es una técnica donde solo se envían paquetes del tipo SYN (inicio de conexión), por cada uno de los puertos que se quieren analizar. Al recibir como respuesta un paquete RST/ACK significa que no existe ningún servicio que escuche por este puerto. Por el contrario, si se recibe un paquete SYN/ACK, podemos afirmar la existencia de un servicio asociado a dicho puerto TCP y en este caso se enviará un paquete RST/ACK para no establecer la conexión y no ser registrados por el sistema objetivo.

## TCP Null scan

Este tipo de exploración pone a cero todos los indicadores de la cabecera TCP, por lo tanto la exploración debería recibir como resultado un paquete de reset (RST) en los puertos no activos. No es recomendable usar este tipo de exploración de puertos con Sistemas Microsoft, ya que la información que se devolverá será un poco confusa y poco válida. Este tipo de exploración es Recomendable llevarlo a la práctica en sistemas de tipo UNIX, LINUX y \*.BSD