

# Inteligencia Activa

Brian Juarez Arguello

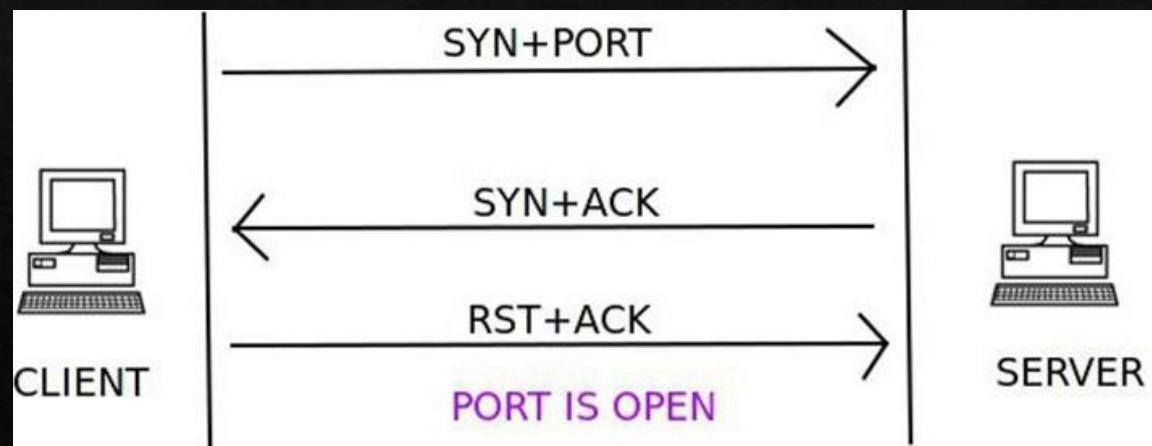
# Análisis de dispositivos y puertos con Nmap

- ❖ El Análisis de dispositivos y puertos con Nmap es una técnica utilizada para escanear y explorar redes informáticas con el objetivo de identificar dispositivos activos en la red, así como los puertos de red que están abiertos y disponibles para la comunicación. Nmap (Network Mapper) es una herramienta de código abierto ampliamente utilizada para realizar este tipo de análisis.
- ❖ El análisis de dispositivos y puertos con Nmap proporciona información valiosa sobre la topología de la red, qué dispositivos están conectados y qué servicios o aplicaciones están en ejecución en esos dispositivos. Esta información es útil para administradores de sistemas, investigadores de seguridad y profesionales de ciberseguridad para comprender la exposición de la red a posibles amenazas y para tomar medidas preventivas.
- ❖ Algunos de los usos comunes del análisis de dispositivos y puertos con Nmap incluyen:
  - ❖ 1. Descubrimiento de dispositivos: Identificar todos los dispositivos activos (como computadoras, servidores, routers, impresoras, etc.) en una red.
  - ❖ 2. Identificación de servicios: Descubrir qué servicios o aplicaciones están siendo ejecutados en los dispositivos y en qué puertos.
  - ❖ 3. Evaluación de seguridad: Identificar posibles puntos débiles o vulnerabilidades en la red al mostrar qué puertos están abiertos y qué servicios son accesibles.
  - ❖ 4. Planificación de red: Ayudar en la planificación y configuración de políticas de seguridad, segmentación de redes y optimización de la infraestructura.
- ❖ Nmap es una herramienta poderosa que puede ejecutar varios tipos de escaneos, como escaneos de puertos TCP, escaneos de puertos UDP, detección de sistemas operativos y más. Sin embargo, es importante tener en cuenta que el uso de Nmap debe realizarse de manera ética y con el permiso del propietario de la red, ya que el escaneo no autorizado de redes puede considerarse un acto ilegal en muchas jurisdicciones.

# Parametros opciones de escaneo de nmap

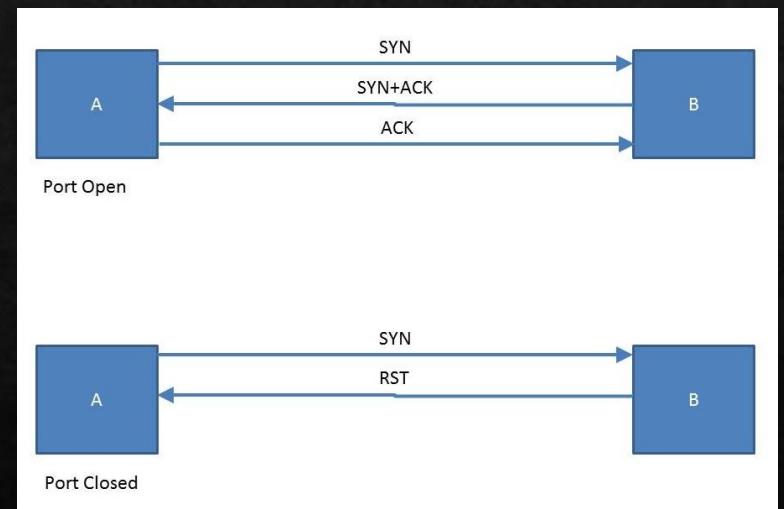
## Listado de parámetros de Nmap

- ❖ Seleccionar objetivos: Direcciones o rangos IP, nombres de sistemas, redes, etc.
- ❖ Descubrir sistemas.
- ❖ Técnicas de análisis de puertos.
- ❖ Puertos a analizar y orden de análisis.
- ❖ Duración y ejecución:
- ❖ Detección de servicios y versiones.
- ❖ Evasión de Firewalls/IDS.



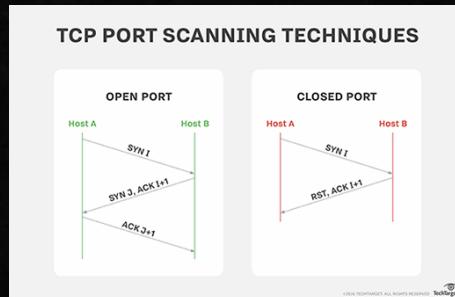
# Full TCP scan

- ❖ TCP FIN Scan: Es una técnica de exploración de puertos que consiste en enviar un paquete FIN a un puerto determinado, con lo cual deberíamos recibir un paquete de reset (RST) si dicho puerto esta cerrado. Esta técnica se aplica principalmente sobre implementaciones de pilas TCP/IP de sistemas Unix. 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 valida. El FIN Scan esta pensado para trabajar únicamente con sistemas operacionales que tengan implementaciones de TCP/IP con respecto al documento RFC 793. El FIN Scan tiene como particularidad identificar el estado de un puerto la manera en que reacciona el host víctima con respecto a una petición de cierre de conexión en un puerto TCP.
- ❖ Para saber si el puerto esta cerrado o no, el proceso de TCP FIN Scan debe de hacer lo siguiente:
- ❖ Supongamos la comunicación entre un host A y B
  - ❖ • El host A manda una petición FIN al host B
  - ❖ • Si Host B responde con una petición RST/ACK, el puerto esta cerrado
  - ❖ • Si host B no responde, posiblemente el puerto esta abierto.
- ❖ Este tipo de exploración de puertos, es silenciosa y en muchas ocasiones no es registrada por Firewall o IDS, así que puede ser usada por atacantes informáticos.



# Stelth Scan

- ❖ Los tipos de escaneo sigiloso son aquellos en los que los indicadores de paquetes hacen que el sistema de destino responda sin tener una conexión completamente establecida. Los piratas informáticos utilizan el escaneo sigiloso para eludir el sistema de detección de intrusos ( IDS ), lo que lo convierte en una amenaza importante. Por lo tanto, es importante que los administradores de sistemas ejecuten escaneos ocultos en sus sistemas para probar el firewall y la funcionalidad del IDS.
- ❖ Algunos Stelth Scan comunes incluyen lo siguiente:
- ❖ Escaneos FIN (terminados). Estos envían paquetes FIN con un conjunto de banderas. Si se devuelve un RST, el puerto se considera abierto; si no se recibe nada, se considera cerrado.
- ❖ Escaneos NULL. Estos no establecen ningún indicador en el paquete TCP. En otras palabras, el encabezado del indicador TCP se establece en 0 y los protocolos de respuesta son los mismos que los escaneos FIN.
- ❖ Escaneos de Navidad. Estos utilizan banderas FIN, URG (urgente) y PSH (push), que iluminan el paquete como un árbol de Navidad. Si se recibe un RST empaquetado, el puerto se considera cerrado; ninguna respuesta indica un estado abierto o filtrado. Un error ICMP inalcanzable también indica un puerto filtrado.



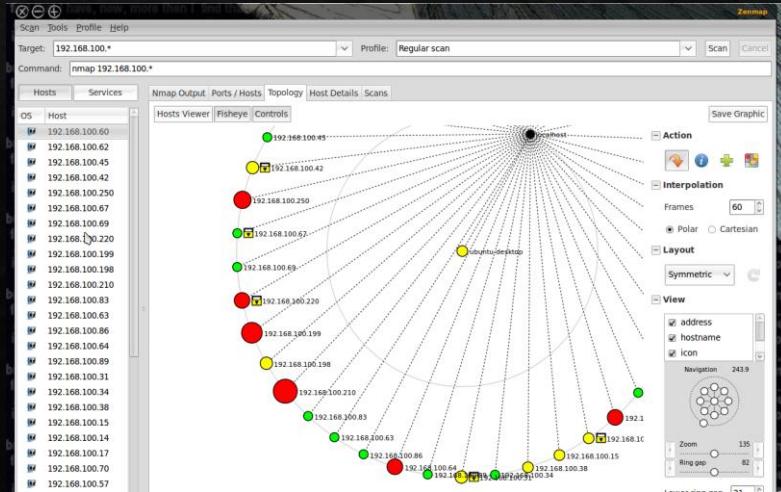
# Fingerprinting

- ❖ 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.
- ❖ 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. A continuación, te ofrecemos una lista de este tipo de actividades que ponen en riesgo tu ciberseguridad y la de tu organización:
  - ❖ Ransomware
  - ❖ Malware
  - ❖ Ataque Botnet
  - ❖ Estafa de Inversión
  - ❖ Estafa de la factura falsa
  - ❖ Vishing
  - ❖ Smishing
  - ❖ Fraude del CEO



# 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.
- ❖ Zenmap es excelente para los principiantes que desean probar las capacidades de Nmap sin pasar por una interfaz de línea de comandos.



# Tracert

- ❖ 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.
- ❖ Aunque Windows lo denomina «tracert», en sistemas operativos basados en UNIX, el nombre de esta herramienta que viene por defecto se denomina «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 se hace uso de mensajes UDP directamente para comprobar cuántos saltos hay de un equipo a otro.

- ❖ Estamos ante una opción de diagnóstico para detectar posibles problemas en la conexión. Por ejemplo si estamos intentando conectar con un equipo que hay en nuestra red y no podemos, así como cualquier tipo de servidor, como podría ser mismamente RedesZone.net o cualquier otra página web con la que estemos teniendo problemas para acceder.
- ❖ Al enviar estos paquetes vamos a obtener cierta información estadística que nos puede ayudar a solucionar esos problemas que mencionamos. Actúa básicamente como eso, como una herramienta nativa del sistema operativo que nos va a mostrar datos relevantes de la conexión.

```
Microsoft Windows [Versión 10.0.18363.476]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\osesp>tracert www.redeszone.net

Traza a la dirección cec02.esc.edgetcdn.com [185.103.39.27]
sobre un máximo de 30 saltos:

 1    2 ms      2 ms      2 ms  www.adsl.vf [192.168.0.1]
 2    4 ms      4 ms      4 ms  static-10-0-235-87.ipcom.comunitel.net [87.235.0.10]
 3    4 ms      4 ms      4 ms  10.183.74.21
 4    *      541 ms    597 ms  172.29.80.9
 5    *          *      5 ms   172.29.1.102
 6   15 ms     14 ms    14 ms  172.29.1.101
 7   15 ms     14 ms    15 ms  xe1-de-cix-mad.airenetworks.es [185.1.68.4]
 8   15 ms     14 ms    15 ms  10.50.1.131
 9   15 ms     14 ms    15 ms  185.103.39.27

Traza completa.

C:\Users\osesp>
```