

UNIVERSIDAD AUTÓNOMA DE CHIAPAS

LICENCAITURA EN INGENIERIA EN DESARROLLO Y TECNOLOGÍAS DE SOFTWARE

Materia: Análisis de vulnerabilidades

Docente: Dr.Luis Gutiérrez Alfaro

Actividad: Investigar los conceptos de
vulnerabilidades-Inteligencia activa

Alumno: Elian Guadalupe Díaz Balcázar

A200178

7° "N"



TUXTLA GUTIERREZ CHIAPAS A 15 DE
AGOSTO DEL 2023

Inteligencia activa.

01 Análisis de dispositivos y puertos con Nmap

02 Parámetros opciones de escaneo de nmap

03 Full TCP scan

04 Stealth Scan

05 Fingerprinting

06 Zenmap

07 Análisis traceroute



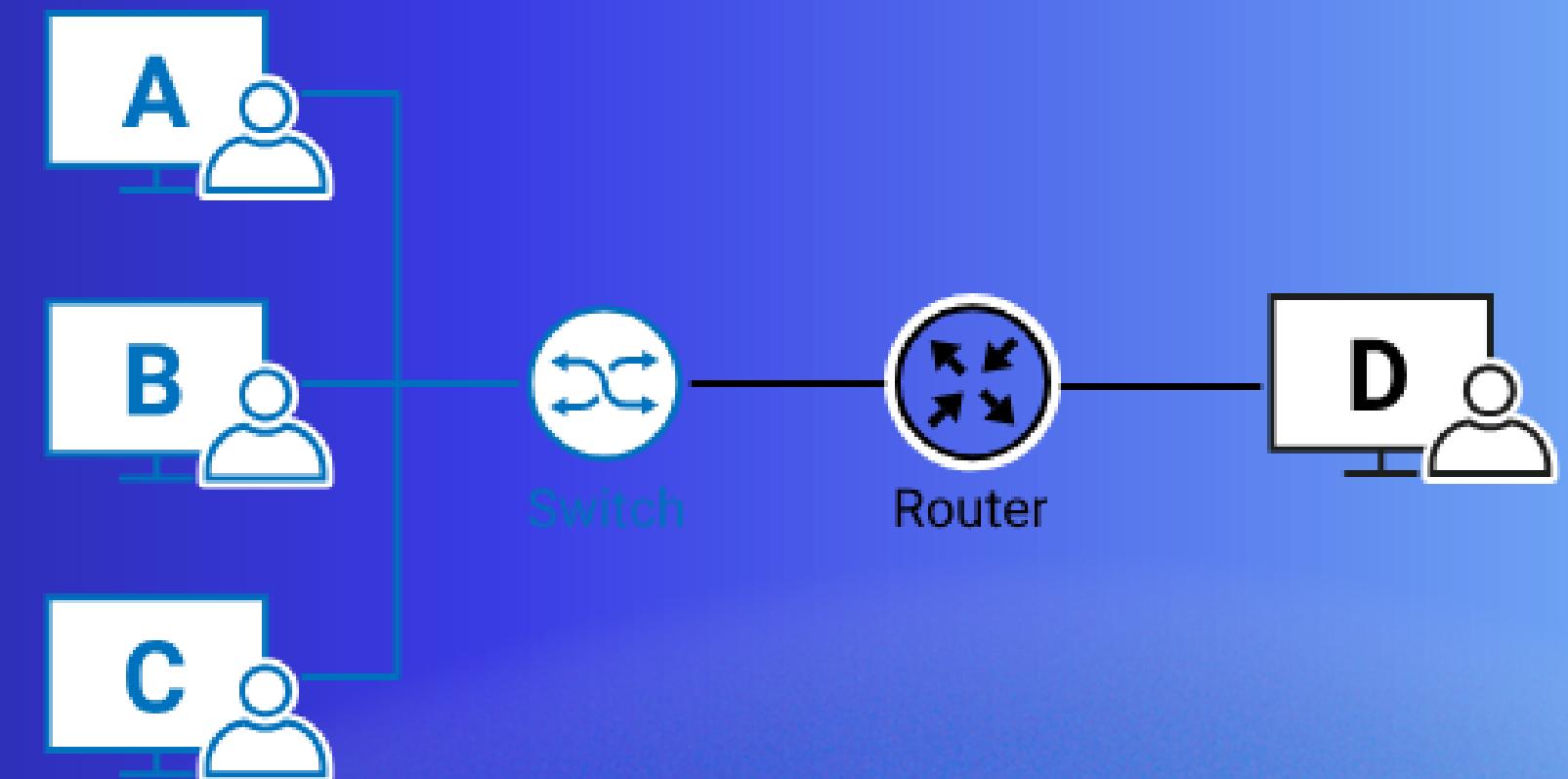


Análisis de dispositivos y puertos con Nmap

Sirve de guía a un administrador de red para descubrir vulnerabilidades y tener controlado todo lo que sucede en una red. Esta aplicación es fundamental para poder mantener un control de la red, detectando cualquier acceso no autorizado tanto a una red doméstica como en grandes redes con miles de dispositivos y subredes.

Sirve para:

- **Mapear una red.**
- **Identificar servicios en ejecución**
- **Realizar una auditoría de seguridad**
- **Detectar sistemas operativos**





Parametros opciones de escaneo de nmap

Descubrir sistemas.

- PS n tcp syn ping
- PA n ping TCP ACK
- PU n ping UDP
- PM Netmask Req
- PP Timestamp Req
- PE Echo Req
- SL análisis de listado
- PO ping por protocolo
- PN No hacer ping
- n no hacer DNS
- R Resolver DNS en todos los sistemas objetivo
- traceroute: trazar ruta al sistema (para topologías de red)
- sP realizar ping, igual que con -PP -PM -PS443 -PA80

Técnicas de análisis de puertos

- sS análisis TCP SYN
- sT análisis TCP CONNECT
- sU análisis UDP
- sY análisis SCTP INIT
- sZ COOKIE ECHO de SCTP
- sO protocolo IP
- sW ventana TCP -sN
- sF -sX NULL, FIN, XMAS
- sA TCP ACK

Puertos a analizar y orden de análisis

- p n-mrango**
- p- todos los puertos**
- p n,m,z especificados**
- p U:n-m,z T:n,m U para UDP, T para TCP**
- F rápido, los 100 comunes**
- top-ports n analizar los puertos más utilizados**
- r no aleatorio**

Duración y ejecución:

- T0 paranoico
- T1 sigiloso
- T2 sofisticado
- T3 normal
- T4 agresivo
- T5 locura
- min-hostgroup
- max-hostgroup
- min-rate
- max-rate
- min-parallelism
- max-parallelism
- min-rtt-timeout
- max-rtt-timeout
- initial-rtt-timeout
- max-retries
- host-timeout -scan-delay

Detección de servicios y versiones

- sV: detección de la versión de servicios
- all-ports no excluir puertos
- version-all probar cada exploración
- version-trace rastrear la actividad del análisis de versión
- O activar detección del S. Operativo
- fuzzy adivinar detección del SO
- max-os-tries establecer número máximo de intentos contra el sistema objetivo

Evasión de Firewalls/IDS

- f fragmentar paquetes
- D d1,d2 encubrir análisis con señuelos
- S ip falsear dirección origen
- g source falsear puerto origen
- randomize-hosts orden
- spoof-mac mac cambiar MAC de origen

Parámetros de nivel de detalle y depuración

- v Incrementar el nivel de detalle
- reason motivos por sistema y puerto
- d (1-9) establecer nivel de depuración
- packet-trace ruta de paquetes

Otras opciones

- resume file continuar análisis abortado (tomando formatos de salida con -oN o -oG)
- 6 activar análisis IPV6
- A agresivo, igual que con -O -sV -sC -traceroute

Opciones interactivas

- v/V aumentar/disminuir nivel de detalle del análisis
- d/D aumentar/disminuir nivel de depuración
- p/P activar/desactivar traza de paquetes

Scripts

- sC realizar análisis con los scripts por defecto
- script file ejecutar script (o todos)
- script-args n=v proporcionar argumentos
- script-trace mostrar comunicación entrante y saliente



Full TCP 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.



Fingerprinting

El *fingerprinting* permite una investigación más meticulosa y exhaustiva de un sistema, pero a la vez es una técnica más intrusiva y puede dejar rastro. Por seguridad, es mejor aplicarlo solo en sistemas informáticos en los que se tenga autorización. En este post, nos concentraremos en explicarte qué es *fingerprinting* y cómo se utiliza en ciberseguridad.



Zenmap

Es una interfaz gráfica gratuita y de código abierto para Nmap

Características de Zenmap

- Puede mostrar la salida normal de Nmap, pero también puede organizar su visualización para mostrar todos los puertos de un host o todos los hosts que ejecutan un servicio en particular.
- Resume los detalles sobre un solo host o un escaneo de com en una pantalla conveniente. Incluso puede utilizar Zenmap para dibujar un mapa topológico de las redes descubiertas.
- Puede utilizar Zenmap para mostrar gráficamente las diferencias entre dos escaneos. Esto puede ayudar a rastrear los nuevos hosts o servicios que aparecen en sus redes, o los existentes que caen.
- Puede utilizar los perfiles de comando de Zenmap para ejecutar el mismo escaneo más de una vez.

¿Cómo usar Zenmap?

1. Elegir el tipo de perfil para el escaneo (Intense scan). Una vez elegido el perfil, se coloca el comando que viene por defecto
2. En objetivo colocar IP a escanear
3. Clic a botón Escaneo



Análisis 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.

¿Cuál es la diferencia entre Ping y Traceroute?

- El ping indica si es accesible y el tiempo que toma para trasmisitir y recibir datos, traceroute detalla la información precisa de la ruta.