
# Universidad Autónoma de Chiapas

## Facultad de Contaduría y Administración

## Campus I

### Ingeniería en Desarrollo y Tecnologías de Software.

Materia: Análisis de vulnerabilidades

Alumno: Joahan Jimenez Ramirez 7”N”

Inteligencia Activa:

# Análisis de dispositivos y puertos con Nmap

Nmap es la mejor herramienta de escaneo de puertos y descubrimiento de hosts que existe actualmente. Nmap nos permitirá obtener una gran cantidad de información sobre los equipos de nuestra red, es capaz de escanear qué hosts están levantados, e incluso comprobar si tienen algún puerto abierto, si están filtrando los puertos (tienen un firewall activado), e incluso saber qué sistema operativo está utilizando un determinado objetivo.

# 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

El escaneo de conexión TCP es el tipo de escaneo TCP predeterminado cuando el escaneo SYN no es una opción. Este es el caso cuando un usuario no tiene privilegios de paquetes sin procesar o está escaneando redes IPv6. En lugar de escribir paquetes sin procesar como lo hacen la mayoría de los otros tipos de escaneo, Nmap le pide al sistema operativo subyacente que establezca una conexión con la máquina y el puerto de destino mediante la emisión de una connectllamada al sistema.

# Stelth Scan

Un escaneo sigiloso (a veces conocido como escaneo semiabierto) es muy parecido a un escaneo completamente abierto con una pequeña diferencia que lo hace menos sospechoso en el dispositivo de la víctima. La principal diferencia es que no se produce un protocolo de enlace de tres vías TCP completo. Mirando el siguiente diagrama, el iniciador (dispositivo A) enviaría un paquete TCP SYN al dispositivo B con el fin de determinar si un puerto está abierto.

# Fingerprintig

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 la interfaz gráfica de usuario oficial de Nmap Security Scanner. Es una aplicación multiplataforma (Linux, Windows, Mac OS X, BSD, etc.) gratuita y de código abierto que tiene como objetivo hacer que Nmap sea fácil de usar para los principiantes al tiempo que proporciona funciones avanzadas para usuarios experimentados de Nmap. Los escaneos de uso frecuente se pueden guardar como perfiles para que sean fáciles de ejecutar repetidamente.

# Análisis tracerote

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.