NMAP Y SUS FUNCIONES

SEGURIDAD INFORMÁTICA

CRISTIAN RIVERA ZAPATA

2022

INDICE

[¿Qué es Nmap? 2](#_Toc96543520)

[Port scanning 3](#_Toc96543521)

[Como usar Nmap 3](#_Toc96543522)

[Tipos de escaneos 3](#_Toc96543523)

[Zenmap 4](#_Toc96543524)

[Estado del puerto para Nmap 4](#_Toc96543525)

[Auditar con NMAP 5](#_Toc96543526)

[WEBGRAFÍA 9](#_Toc96543527)

¿Qué es Nmap?

Nmap, abreviatura de Network Mapper, es una herramienta gratuita y de código abierto para la detección de redes y el análisis de vulnerabilidades. Los administradores de red usan Nmap para identificar dispositivos que se ejecutan en un sistema, descubrir hosts disponibles y los servicios que brindan, encontrar puertos abiertos y detectar riesgos de seguridad. Nmap se puede usar para monitorear hosts individuales, así como grandes redes que abarcan cientos de miles de dispositivos y una gran cantidad de subredes. Aunque Nmap ha evolucionado a lo largo de los años y es muy flexible, es esencialmente una herramienta de exploración de puertos que recopila información mediante el envío de paquetes sin procesar a los puertos del sistema. Escucha las respuestas y determina si el puerto está abierto, cerrado o filtrado de alguna manera. (Otros términos utilizados para el escaneo de puertos incluyen descubrimiento de puertos o enumeración de puertos).

Nmap cuenta con diferentes tipos de escaneos de puertos, ya sea sobre segmentos TCP, datagramas UDP o paquetes ICMP, también permite escanear de forma oculta, dificultando su detección por parte de los firewalls. Por supuesto, podemos escanear ciertos puertos, especialmente entre rangos de puertos, entre rangos de direcciones IP, usando paquetes TCP null, FIN, Xmas y ACK y la posibilidad de SYN para localizar puertos TCP abiertos. Otras de las características que nos ofrece esta herramienta es la posibilidad de hacer un inventario completo de la red e incluso comprobar si un determinado host o servicio sigue funcionando. El programa está diseñado para escanear una gran cantidad de hosts, por lo que, si necesita escanear múltiples objetivos, no tendrá ningún problema.

Este programa es muy flexible, combinas docenas de técnicas avanzadas para escanear hosts y puertos, además permite realizar auditorías a través de NSE (Nmap Search Engine), por lo que es realmente poderoso. Nmap tiene varios estados de puerto que aparecen cuando hacemos un escaneo de puerto. Comprender el significado de cada estado de Nmap es fundamental, ya que cualquier exploración de puertos devolverá un estado diferente.

Port scanning

Los paquetes que Nmap envía devuelven direcciones IP y una gran cantidad de otros datos, lo que le permite identificar todo tipo de atributos de la red, permite crear un perfil o mapa de la red y un inventario de hardware y software.

Nmap emplea protocolos de capa de transporte que incluyen TCP, UDP y SCTP, así como protocolos de soporte como ICMP, utilizados para enviar mensajes de error.

Por ejemplo, la sobrecarga de recursos de UDP es adecuada para la transmisión de vídeo en tiempo real, en la que se sacrifican algunos paquetes perdidos a cambio de velocidad, mientras que los vídeos de transmisión en tiempo no real en YouTube se almacenan en búferes y utilizan el protocolo TCP más lento, aunque más fiable.

Como usar Nmap

Existe una amplia gama de utilidades de monitorización de red gratuitas, así como escáneres de vulnerabilidades de código abierto gratuitos disponibles para administradores de red y auditores de seguridad. Lo que hace que Nmap destaque como la herramienta que los administradores de IT y de redes necesitan conocer es su flexibilidad y potencia. Si un administrador de red recibe una alerta sobre una vulnerabilidad en una versión particular de una aplicación, por ejemplo, puede escanear su red para identificar si esa versión de software se está ejecutando en la red y tomar medidas para parchear o actualizar los hosts relevantes.

Tipos de escaneos

Escaneo Ping / Escaneo ARP: Utiles para conocer qué servidores se encuentran activos. Cuando nos encontramos en una red local se ejecuta un escaneo ARP para obtener información de los servidores activos.

Sondeo de lista: Se realiza una resolución inversa de DNS para obtener los nombres de los equipos. A diferencia del escaneo Ping, con este escaneo no se envía ningún tipo de paquete hacia el objetivo.

Escaneo TCP connect: Realiza una conexión completa con los puertos que están a la escucha (3 way hand shake). Es el escaneo por defecto sino se utilizan privilegios de administrador para ejecutar el TCP SYN.

Zenmap

una interfaz gráfica para Nmap Zenmap es una interfaz gráfica de usuario para Nmap que ofrece cientos de opciones. Permite a los usuarios realizar búsquedas de datos, como guardar escaneos y compararlos, ver mapas de topología de red, ver pantallas de puertos que se ejecutan en un host o en todos los hosts de la red y almacenar escaneos en una base de datos.

Estado del puerto para Nmap

Abierta: la aplicación acepta activamente conexiones TCP o UDP. El puerto está abierto y disponible, y los evaluadores de penetración podrán explotar el sistema utilizando este puerto abierto. Este es el estado predeterminado si no tenemos ningún firewall que bloquee el acceso.

Cerrado: se puede acceder al puerto cerrado porque responde a Nmap, pero no se ejecuta ninguna aplicación en el puerto. Es útil para descubrir que un host está activo o como parte del descubrimiento de un sistema operativo. Para los administradores del sistema, se recomienda usar un firewall para filtrar estos puertos para que no se pueda acceder a ellos. Para los probadores de penetración, es recomendable mantener estos puertos "cerrados" para su posterior análisis en caso de que pongan nuevos servicios.

Filtered: en este estado Nmap no puede determinar si el puerto está abierto, porque hay un firewall filtrando los paquetes de Nmap en dicho puerto. Estos puertos filtrados son los que aparecerán cuando tengamos un firewall activado. Nmap intentará en varias ocasiones intentar conectar, lo que hace que el escaneo de puertos sea bastante lento.

Open| Filtered: Nmap no sabe si el puerto está abierto o filtrado. Esto ocurre porque el puerto abierto no envía ninguna respuesta, y dicha falta de respuesta podría ser por el firewall. Este estado aparece cuando usamos UDP y IP, y utilizamos escaneos FIN, NULL y Xmas.

Closed | Filtered: en este estado no se sabe si el puerto está cerrado o filtrado. Solo se usa este estado en el IP Idle Scan.

Auditar con NMAP

Ventajas:

Es una herramienta muy poderosa en sus dos versiones GUI (Interfaz gráfica de usuario) y CLI (Interfaz de línea de comando), esta tiene opciones para realizar escaneos muy difícilmente detectables por las “victimas” o supervisores de red. Escanea cualquier rango de puertos que desees e incluso detecta el sistema operativo de la víctima, dando lugar a que el hacker identifique más claramente como puede acceder al equipo remoto.

A continuación, se mostrarán algunas pruebas que se pueden realizar con esta herramienta:

* Escanear puertos

Escaneo básico

* Comando:

nmap -vv cleveritgroup.com

-vv significa salida detallada. Muestra lo que está sucediendo durante el escaneo.

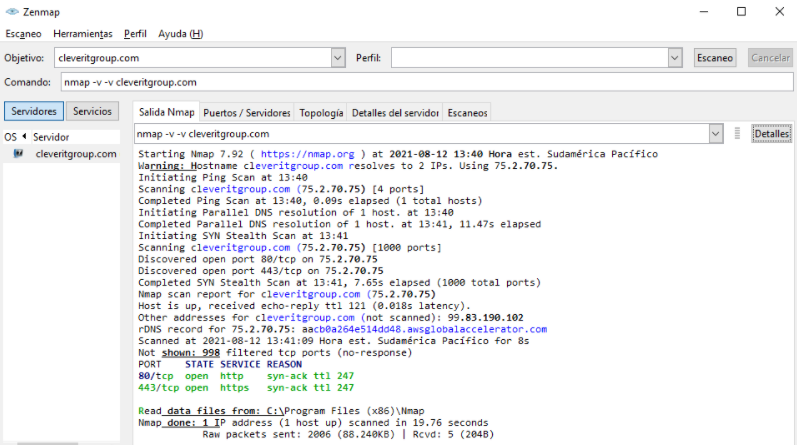


Ilustración 1

* Ingresar el número de puerto

Comando:

-nmap -vv 1-5000 cleveritgroup.com

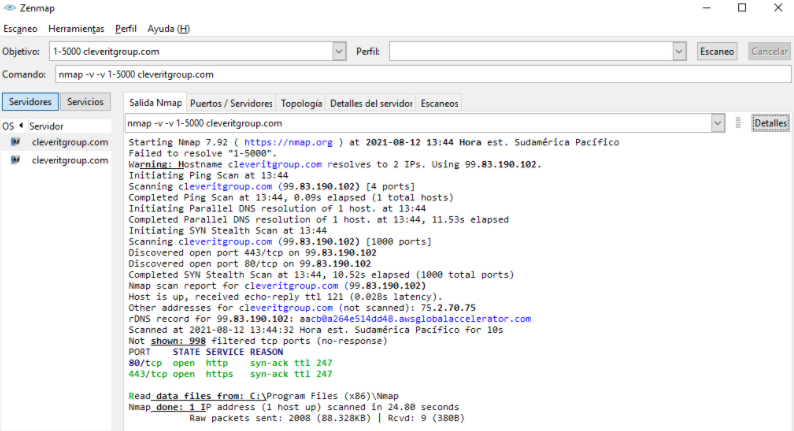


Ilustración 2

* Detectar el Sistema operativo

Comando:

-nmap -v -Pn -o cleveritgroup.com

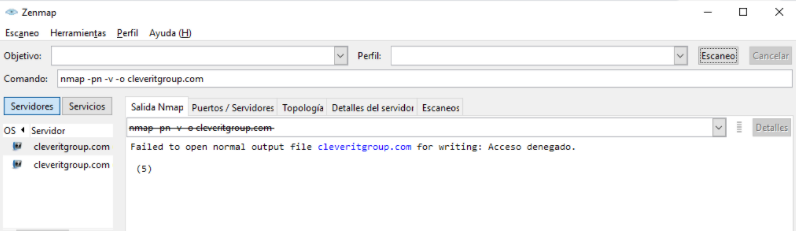


Ilustración 3

Detectar si es vulnerable a ataque DoS

Comando:

-nmap --script dos -Pn cleveritgroup.com

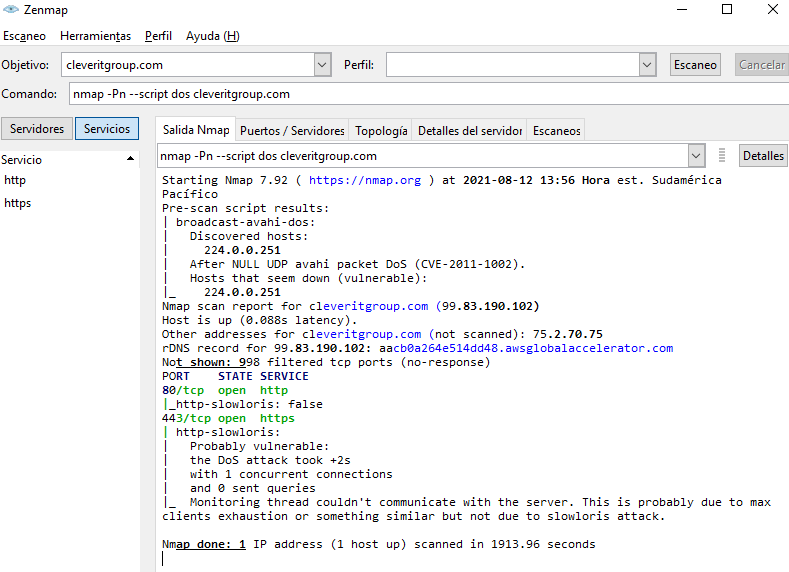


Ilustración 4

Descubrir vulnerabilidades

Comando:

-nmap -Pn –script vuln cleveritgroup.com

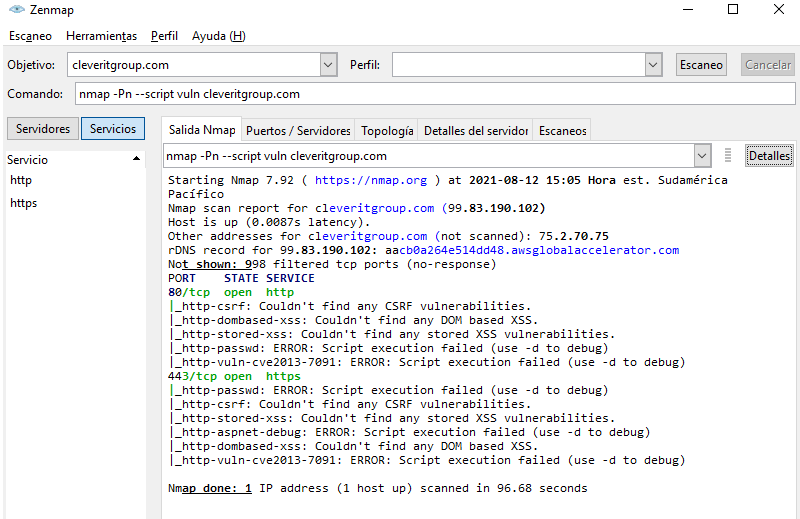


Ilustración 5

Para visualizar los resultados puede dirigirse a la pestaña que se llama Salida Nmap y de acuerdo con el resultado que obtenga si existe o no una vulnerabilidad puede a su criterio dar un informe de resultados.



Ilustración 6

Concluyendo con este tutorial sacado de un repositorio de seguridad de un foro en internet, se puede decir que nos permite saber que es lo que está expuesto de una red debido a que es ese el primer paso para protegerla, no permite saber si se encuentran puertos extraños que estén abiertos ya que se suponen que deben estar cerrados, ya que serían entradas a atacantes e incluso virus. Mientras se controle más el sistema, menos oportunidad existe para romperlo.

WEBGRAFÍA

* <https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/>
* <https://www.marindelafuente.com.ar/que-es-nmap-por-que-necesitas-este-mapeador-de-red/>
* <https://es.wikipedia.org/wiki/Nmap>
* <https://nmap.org/man/es/index.html>
* <https://dojoconfpa.org/nmap-network-mapper/>
* <https://www.cleveritgroup.com/blog/analisis-de-vulnerabilidades-con-nmap>