



Universidad Autónoma de Chiapas
Facultad de contaduría y administración, Campus I
Licenciatura en Ingeniería en Desarrollo y Tecnologías de Software

Análisis de Vulnerabilidades
Catedrático: Luis Gutiérrez Alfaro

ACT. 1.1 Investigar los conceptos de vulnerabilidades

Alumno: José Julián Molina Ocaña
Matricula: A200002

Tuxtla Gutiérrez, Chiapas
A
12 de agosto del 2023



conceptos de vulnerabilidades

Herramientas de vulnerabilidades

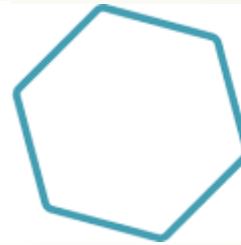


Nmap: Network Mapper (Nmap) es una herramienta de código abierto utilizada para escanear redes y sistemas en busca de hosts y servicios activos. Puede realizar diversos tipos de escaneos, como escaneos de puertos, detección de sistemas operativos y más. Nmap es ampliamente utilizado por administradores de sistemas y profesionales de seguridad para evaluar la seguridad de redes y sistemas.

Joomscan: Joomscan es una herramienta diseñada específicamente para escanear y evaluar la seguridad de sitios web construidos con el sistema de gestión de contenidos Joomla. Realiza pruebas de vulnerabilidad específicas para Joomla, como la detección de versiones vulnerables y posibles problemas de configuración.



WPScan



nessus[®]
Essentials

Wpscan: Similar a Joomscan, WPScan se enfoca en la evaluación de la seguridad de sitios web, pero en este caso, está dirigida a sitios que utilizan WordPress como plataforma. WPScan busca vulnerabilidades conocidas en plugins, temas y la propia instalación de WordPress.

Nessus Essentials: Nessus es una herramienta de evaluación de vulnerabilidades líder en la industria. Existen versiones tanto comerciales como una versión gratuita llamada Nessus Essentials. Permite escanear sistemas en busca de vulnerabilidades conocidas y configuraciones incorrectas que podrían ser explotadas por atacantes.

Vega: Vega es una herramienta de código abierto para realizar pruebas de seguridad en aplicaciones web. Se utiliza para identificar y analizar vulnerabilidades en aplicaciones web mediante la realización de pruebas automatizadas de seguridad, como inyecciones SQL, cross-site scripting (XSS) y más.

Inteligencia Misceláneo.



Gobuster: Gobuster es una herramienta de línea de comandos utilizada para realizar ataques de fuerza bruta o búsqueda de contenido en servidores web. Su función principal es escanear y enumerar directorios y archivos en un sitio web mediante el envío de solicitudes HTTP a diferentes rutas y analizar las respuestas. Esta herramienta es útil para identificar recursos ocultos o mal configurados en un sitio web que podrían ser aprovechados por atacantes.

Inteligencia Misceláneo.



Dumpster Diving: El Dumpster Diving (buceo en la basura) es una técnica de ingeniería social que implica buscar información confidencial o valiosa en la basura o en la eliminación de documentos de una organización. Los atacantes pueden buscar documentos impresos, discos duros, USB u otros medios de almacenamiento que han sido descartados incorrectamente. Esta técnica puede revelar información sensible que podría ser utilizada para ataques posteriores.



Ingeniería Social: La ingeniería social es una técnica utilizada por atacantes para manipular a las personas y obtener información confidencial o realizar acciones no autorizadas. Implica la explotación de la psicología humana y la confianza para obtener acceso a sistemas o información valiosa. Los ataques de ingeniería social pueden incluir pretextos, suplantación de identidad, persuasión y manipulación emocional para engañar a las personas y lograr sus objetivos maliciosos.



Inteligencia Activa se refiere a la recopilación de información utilizando técnicas y herramientas que involucran interacciones directas con sistemas o redes. Esto a menudo incluye el uso de herramientas de escaneo y análisis para obtener detalles específicos sobre dispositivos y servicios.


```
ruvelro@ruvelro-Ubuntu: ~  
ruvelro@ruvelro-Ubuntu:~$ nmap 192.168.1.2  
  
Starting Nmap 6.00 ( http://nmap.org ) at 2013-05-20 12:44 CEST  
Nmap scan report for 192.168.1.2  
Host is up (0.00019s latency).  
Not shown: 995 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
9091/tcp  open  xmltec-xmlmail  
  
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds  
ruvelro@ruvelro-Ubuntu:~$
```

Escanear utilizando una conexión TCP

nmap -sT 192.168.0.1

Escanear utilizando una escan SYN (por defecto)

nmap -sS 192.168.1.1

Escanear los puertos UDP

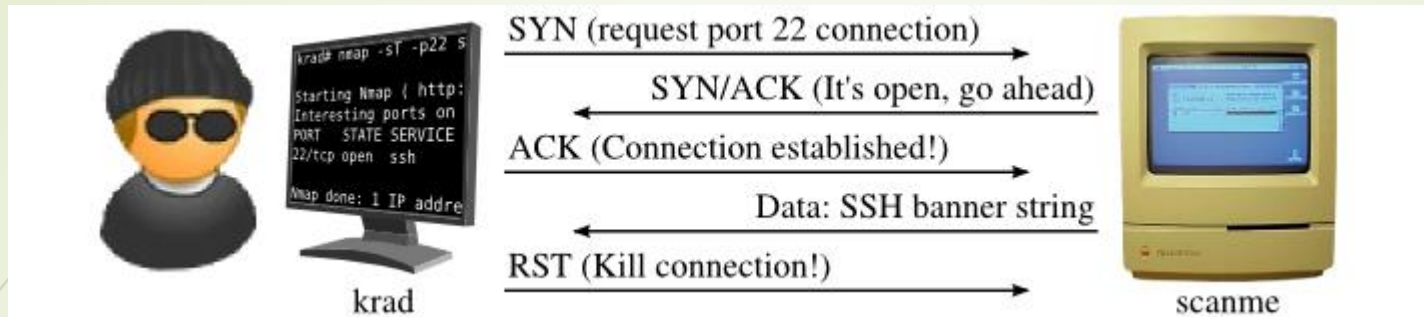
nmap -sU -p 123,161,162 192.168.0.1

Escanear puertos ignorando el discovery

nmap -Pn -F 192.168.0.1

Análisis de dispositivos y puertos con Nmap: Nmap (Network Mapper) es una herramienta de código abierto ampliamente utilizada para descubrir dispositivos y servicios en una red. Permite escanear rangos de direcciones IP para identificar hosts activos y los puertos que están abiertos en esos hosts. Esto es útil para comprender la topología de la red y evaluar posibles puntos de entrada.

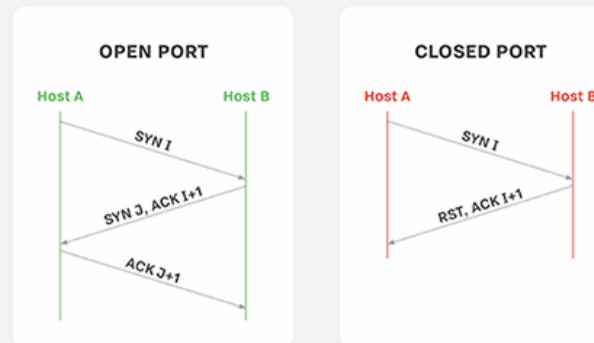
Parámetros y opciones de escaneo de Nmap: Nmap ofrece una amplia gama de parámetros y opciones de escaneo que permiten a los usuarios personalizar sus escaneos. Algunos ejemplos de opciones son el escaneo de puertos específicos, el escaneo rápido, la detección de sistemas operativos y más.

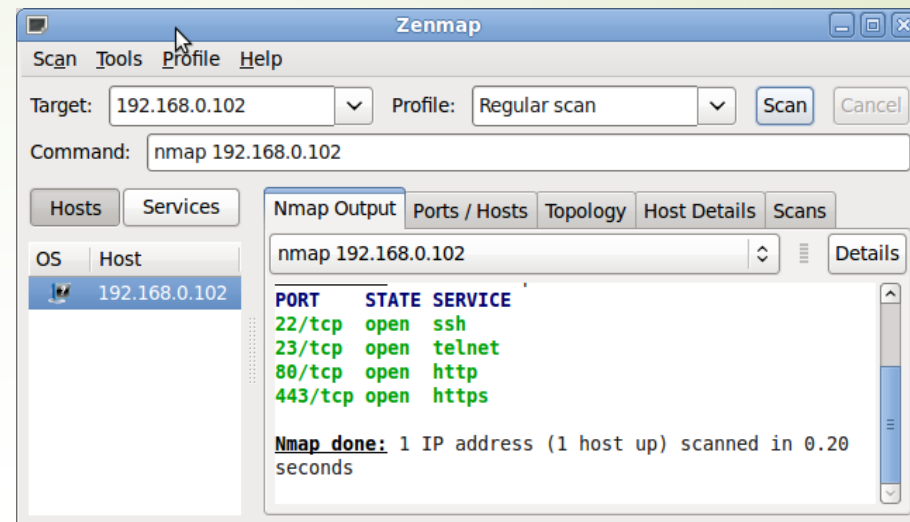


Full TCP Scan: Este tipo de escaneo en Nmap, también conocido como "TCP Connect Scan", intenta establecer una conexión TCP completa con cada puerto en el rango especificado. Es un método preciso pero puede ser más lento y más detectable por sistemas de defensa.

Stealth Scan: También llamado "TCP SYN Scan" o "Half-Open Scan", este escaneo utiliza paquetes SYN para intentar establecer una conexión pero no completa la conexión TCP. Es más rápido y menos intrusivo que un escaneo completo, pero podría ser detectado por sistemas de seguridad.

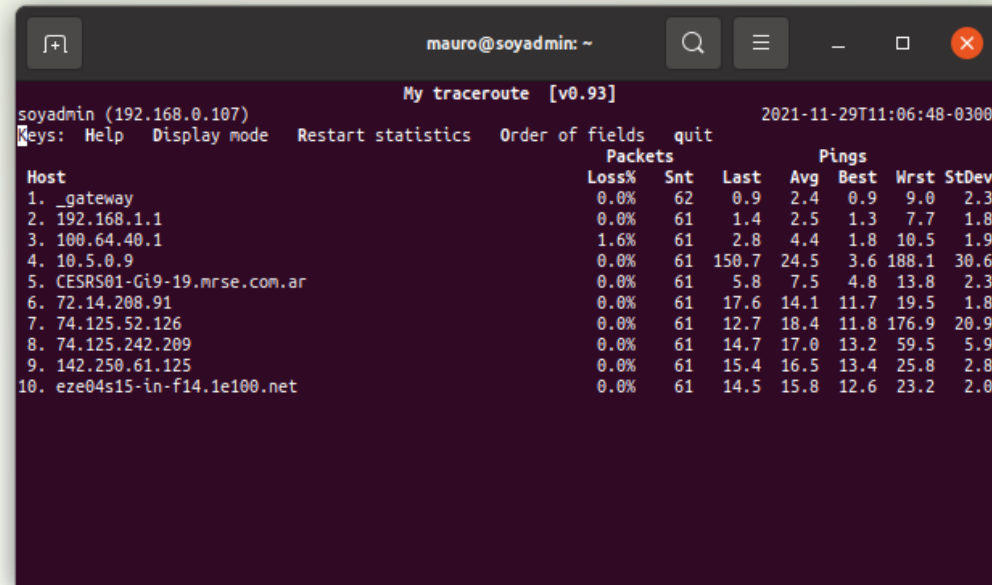
TCP PORT SCANNING TECHNIQUES





Fingerprinting (Identificación de huellas): En el contexto de la ciberseguridad, el fingerprinting se refiere a la técnica de identificar sistemas operativos, servicios y versiones específicas que se ejecutan en un host objetivo. Esto se puede lograr analizando respuestas a solicitudes de escaneo y comparándolas con bases de datos de huellas digitales.

Zenmap: Zenmap es la interfaz gráfica de usuario (GUI) para Nmap. Proporciona una forma más fácil de utilizar Nmap y visualizar los resultados de los escaneos. Permite a los usuarios configurar escaneos, ver los resultados en un formato más legible y realizar análisis básicos de los datos recopilados.



```
mauro@soyadmin: ~  
My traceroute [v0.93] 2021-11-29T11:06:48-0300  
Keys: Help  Display mode  Restart statistics  Order of fields  quit  
Host      Loss%  Snt  Last  Avg  Best  Wrst  StDev  
1. _gateway 0.0%   62   0.9   2.4  0.9   9.0   2.3  
2. 192.168.1.1 0.0%   61   1.4   2.5  1.3   7.7   1.8  
3. 100.64.40.1 1.6%   61   2.8   4.4  1.8  10.5   1.9  
4. 10.5.0.9 0.0%   61 150.7 24.5  3.6 188.1 30.6  
5. CESRS01-Gi9-19.mrse.com.ar 0.0%   61   5.8   7.5  4.8  13.8   2.3  
6. 72.14.208.91 0.0%   61 17.6 14.1 11.7 19.5   1.8  
7. 74.125.52.126 0.0%   61 12.7 18.4 11.8 176.9 20.9  
8. 74.125.242.209 0.0%   61 14.7 17.0 13.2 59.5   5.9  
9. 142.250.61.125 0.0%   61 15.4 16.5 13.4 25.8   2.8  
10. eze04s15-in-f14.1e100.net 0.0%   61 14.5 15.8 12.6 23.2   2.0
```

Análisis traceroute: Traceroute es una herramienta que rastrea la ruta que sigue un paquete de datos desde tu dispositivo a un destino específico en una red. Muestra todos los saltos intermedios (routers) que el paquete hace para llegar a su destino final. Esto puede ser útil para diagnosticar problemas de conectividad y entender la topología de una red.