





Conceptos de vulnerabilidades

Por Cedrick Marcial Quintero

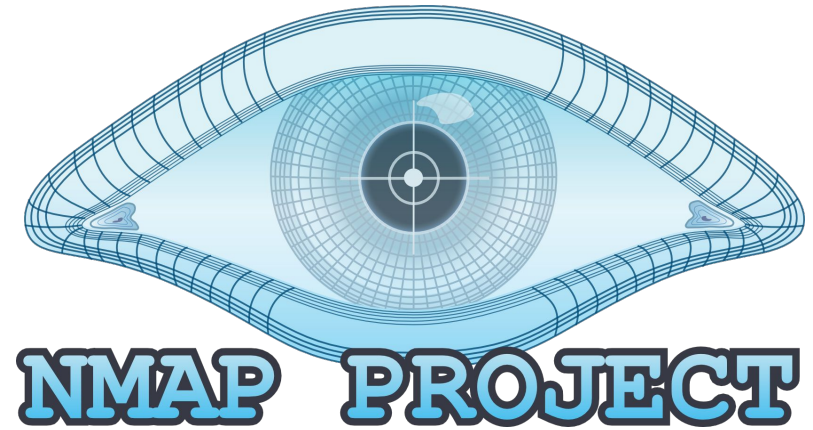




Herramientas de vulnerabilidades

Nmap

Este es un software de código, multi propósito el cual sirve para hacer desde el rastreo de puertos en una computadora, hasta hacer cómputo forense por medio de lo que es el finger-painting, esta es una herramienta la cual es bastante versátil pero la cual esta mucho mas orientada a lo que es el escaneo y detección de vulnerabilidades.



Joomscan

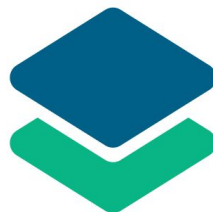
Este es un software hecho por un equipo independiente y de uso libre el cual está enfocado en en la búsqueda de vulnerabilidades en páginas web desarrolladas en joomla, los procesos que este software usa están automatizados, puesto que los desarrolladores buscaban que fuera lo más práctico y accesible para desarrolladores web.



WPScan

Es una herramienta la cual fue desarrollada con las mismas intenciones que JoomScan, sin embargo esta está enfocada al análisis de lo que son páginas desarrolladas en Wordpress.

Este software requiere de forma obligatoria ejecutarse en kali linux.



WPScan

Nessus Essentials

Nessus Essentials es parte de una familia de distintos softwares de seguridad, desarrollados por la empresa Tenable. Esta herramienta en específico está orientada a lo que es el escaneo de vulnerabilidades de forma local/Una red doméstica. Esta es una herramienta pensada para estudio y prácticas, en comparación a los otros modelos del mismo Nessus que cuentan con herramientas sofisticadas.



VEGA

Este es un programa de código abierto el cual está expresamente hecho el análisis de seguridad de páginas web, no está orientado hacia ninguna tecnología como WordPress o Joomla, lo que hace que sea compatible con mas servicios de alojamiento web. Cabe resaltar que este software también permite lo que es el análisis y protección de bases de datos (SQL).



OPEN SOURCE WEB APPLICATION VULNERABILITY SCANNER, PROXY AND PLATFORM



Inteligencia Misceláneo

Gobuster

Esta es una herramienta la cual accede a directorios y archivos, pertenecientes a sitios web o Dns's, esta logra acceder a estos datos por medio de distintos scripts automatizados los cuales vulnerar el los datos por medio de la fuerza bruta.

Dumpster Diving

Esta no es una práctica propia de la informática. Esta consiste en excavar y buscar dentro la basura de un individuo objetivo con el objetivo de buscar información la cual nos pueda ser de utilidad, o nos de pistas e una vulnerabilidad.

Ingeniería Social

Este consiste en la obtención de datos importantes por medio de engaños, con frecuencia este tipo de engaños los podemos encontrar en emails los cuales a simple vista provienen de fuentes confiables o inofensivos, pero que los correos de remitente, no tiene nada que ver con el correo



Inteligencia Activa

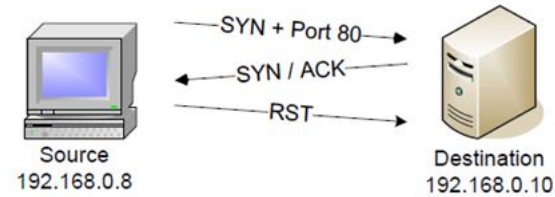
Análisis de dispositivos y puertos con Nmap

Cuando hablamos de esto nos referimos a hacer un reconocimiento de nuestro objetivo con la herramienta Nmap, implica el conocer los distintos puertos que tiene y en cuales podemos vulnerar, tener una noción de la implementación de la topología de red que tiene, e identificar qué servicios y versiones del mismo tiene.



Full TCP Scan

Este es un tipo de escaneo en el cual se realiza una conexión directa con el servidor, con la cual se puede hacer el análisis del objetivo, este tipo de escaneo se suele hacer cuando una conexión SYN no es funcional.



Source	Destination	Summary
[192.168.0.8]	[192.168.0.10]	TCP: D=80 S=57283 SYN SEQ=2360927338 LEN=0 WIN=3072
[192.168.0.10]	[192.168.0.8]	TCP: D=57283 S=80 SYN ACK =2360927339 SEQ=1622899389
[192.168.0.8]	[192.168.0.10]	TCP: D=80 S=57283 RST WIN=0

Stealth Scan

Los escaneo sigilosos con aquellos en los cuales se ha una comunicación con el dispositivo objetivo pero sin la conexión está establecida por completo, esto se logra haciendo una conexión la cual pueda eludir los sistemas de detección de intrusos o IDS.

```
(kali@kali)-[~/Desktop]
$ sudo nmap -v -sS -Pn 10.10.232.201
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-04 07:54 EDT
Initiating Parallel DNS resolution of 1 host. at 07:54
Completed Parallel DNS resolution of 1 host. at 07:54, 0.02s elapsed
Initiating SYN Stealth Scan at 07:54
Scanning 10.10.232.201 [1000 ports]
Discovered open port 80/tcp on 10.10.232.201
Discovered open port 135/tcp on 10.10.232.201
Discovered open port 21/tcp on 10.10.232.201
Discovered open port 53/tcp on 10.10.232.201
Discovered open port 3389/tcp on 10.10.232.201
Completed SYN Stealth Scan at 07:54, 10.32s elapsed (1000 total ports)
Nmap scan report for 10.10.232.201
Host is up (0.17s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
135/tcp   open  msrpc
3389/tcp  open  ms-wbt-server

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.55 seconds
Raw packets sent: 2001 (88.044KB) | Rcvd: 11 (484B)
```

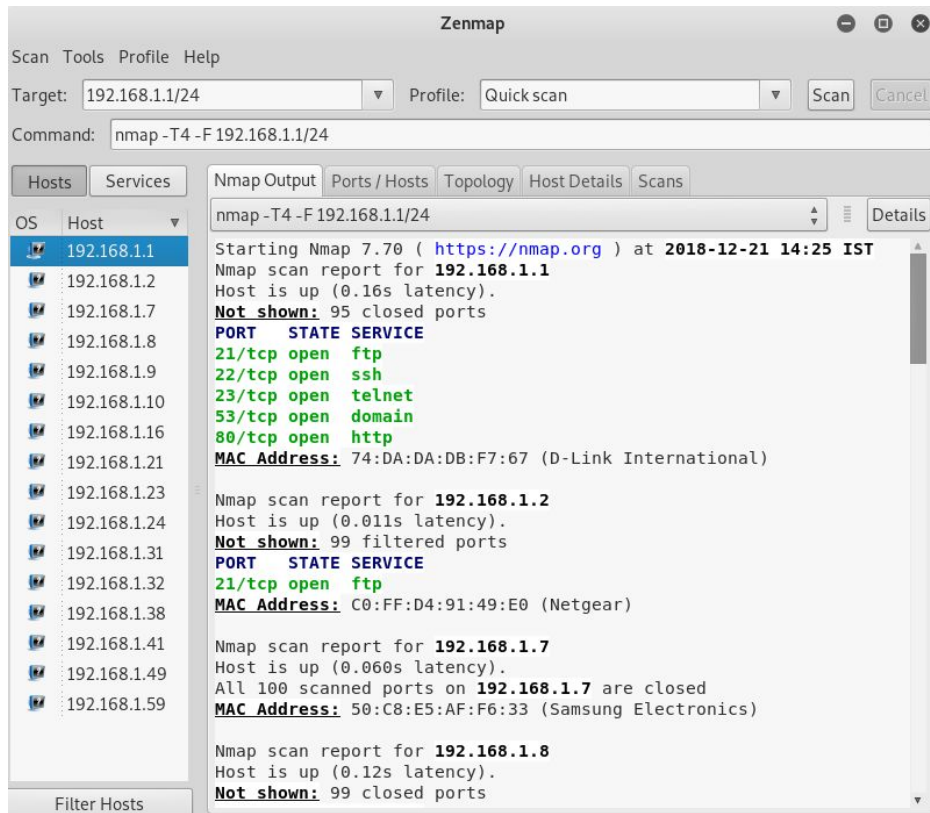
Fingerprinting

Este concepto hace alusión a todos los rastros y residuos que podemos encontrar en un dispositivo electrónico que pueden dejar los distintos programas y elementos que se trabajen dentro del mismo.



Zenmap

Esta es una interfaz gráfica la cual puede ser implementada en Nmap, la principal característica es que esta brinda herramientas las cuales facilitan el uso de Nmap, aunado a esto esta herramienta es recomendado para usar a todos aquellos los cuales empiezan a usar Nmap.



Análisis traceroute

Este es un método de análisis el cual permite diagnosticar problemas de red y conexión de una red local, este puede ser ejecutado de forma directa desde la consola de windows por medio del comando de Tracert, sin embargo en sistemas como GNU/Linux o Mac posee el nombre de Traceroute.

```
C:\WINDOWS\system32\cmd. x + v
Microsoft Windows [Versión 10.0.22621.2134]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\CEDRICK>Tracert

Uso: tracert [-d] [-h saltos_máximos] [-j lista_de_hosts] [-w tiempo_de_espera]
        [-R] [-S srcaddr] [-4] [-6] nombre_destino

Opciones:
    -d                No convierte direcciones en nombres de hosts.
    -h saltos_máximos Máxima cantidad de saltos en la búsqueda del objetivo.
    -j lista-host     Enrutamiento relajado de origen a lo largo de la
                     lista de hosts (solo IPv4).
    -w tiempo_espera  Tiempo de espera en milisegundos para esperar cada
                     respuesta.
    -R                Seguir la ruta de retorno (solo IPv6).
    -S srcaddr        Dirección de origen para utilizar (solo IPv6).
    -4                Forzar usando IPv4.
    -6                Forzar usando IPv6.
```