

Análisis de
Vulnerabilidades

Vulnerabilidades

Conceptos

Fátima De Los Santos Fiallo

LIDTS 7º M

Tuxtla Gutiérrez, Chis.
fatima.santos27@unach.mx

15 de Agosto 2023



Herramientas de vulnerabilidades

Realizar pruebas para verificar las vulnerabilidades del sistema, posibles fugas de información, amenazas potenciales, todo esto teniendo en cuenta también el factor humano y sus fallos.

Nmap: Explorar la red y realizar auditorías de seguridad, esta herramienta utiliza paquetes IP para determinar que equipos

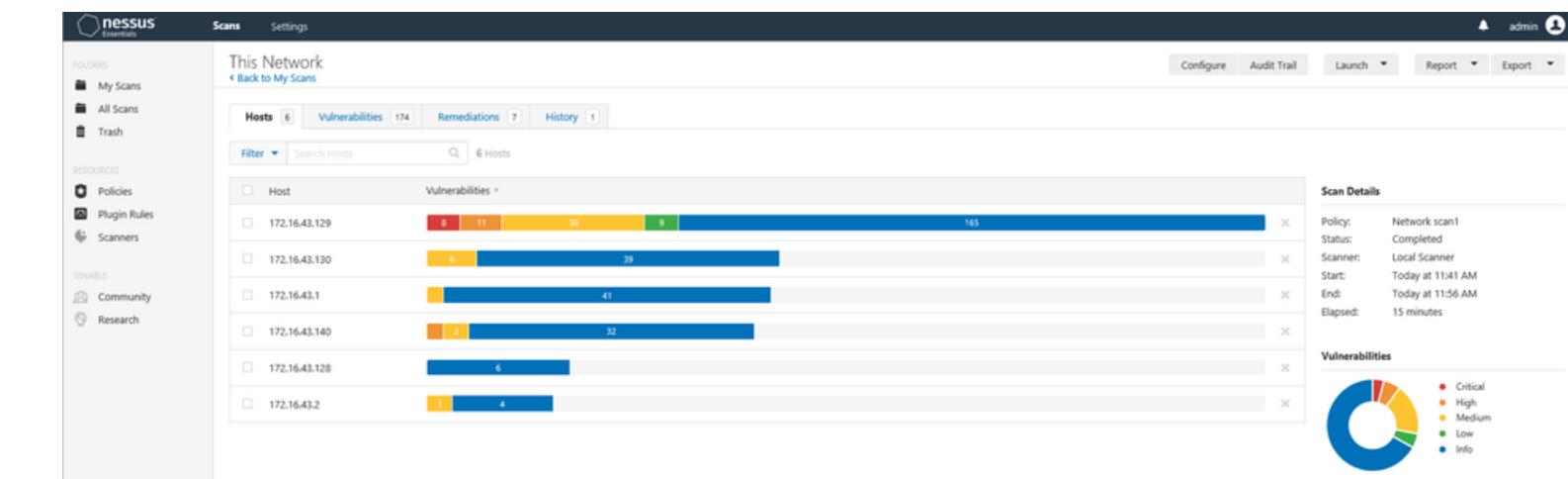
01 se encuentran disponibles en una red, se puede determinar los servicios como son nombre y versión de la aplicación, sistemas operativos, tipos de cortafuegos que se están ejecutando.

02 **Joomscan:** Indicar información de la versión de PHP así como también detalles sobre el tipo de servidor en un análisis automático de los plugins instalados.

03 **Wpscan:** Identificar el tema activo y los diversos problemas de seguridad que pueda contener en un análisis rápido del sitio web.

04 **Nessus Essentials:** Utilizar la interfaz de usuario de Nessus a través del navegador web, habrá que arrancar el servicio con el comando /etc/init.d/nessusd start

05 **Vega:** Interfaz sencilla, fácil de utilizar, en la que cualquier usuario, puede realizar un análisis sin disponer de conocimientos en ese campo y visualizar la información de estos.



```
(dachman@dachman) ~]$ wpscan -h
\\WPSCAN\\
Wordpress Security Scanner by the WPScan Team
Version 3.8.20
 @_WPScan_, @_ethicalhack3r, @_erwan_lr, @_firegart

Usage: wpscan [options]
--url URL

-h, --help
--hh
--version
-v, --verbose
--[no-]banner

The URL of the blog to scan
Allowed Protocols: http, https
Default Protocol if none provided: http
This option is mandatory unless update or help or hh or ver
Display the simple help and exit
Display the full help and exit
Display the version and exit
Verbose mode
Whether or not to display the banner
```



Inteligencia Misceláneo



- 01 **Gobuster:** Tiene tres modos disponibles. “dir”, el modo clásico de fuerza bruta contra directorios, “dns”, el modo de fuerza bruta contra subdominios DNS, y “vhost”, el modo de fuerza bruta contra hosts virtuales (no es lo mismo a “DNS”).
- 02 **Dumpster Diving:** Técnica de hacking en la que alguien busca en tu basura información sensible. Si hay algo sospechoso entre esos archivos (como un nombre de archivo que parece una “contraseña” sin extensión), lo más probable es que sea malicioso.
- 03 **Ingeniería Social:** Utilizan la confianza de las personas para obtener acceso a un sistema o red. Cuando un atacante hace esto, suele utilizar técnicas de manipulación psicológica como el phishing, entre otras.



Inteligencia Activa

```
Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

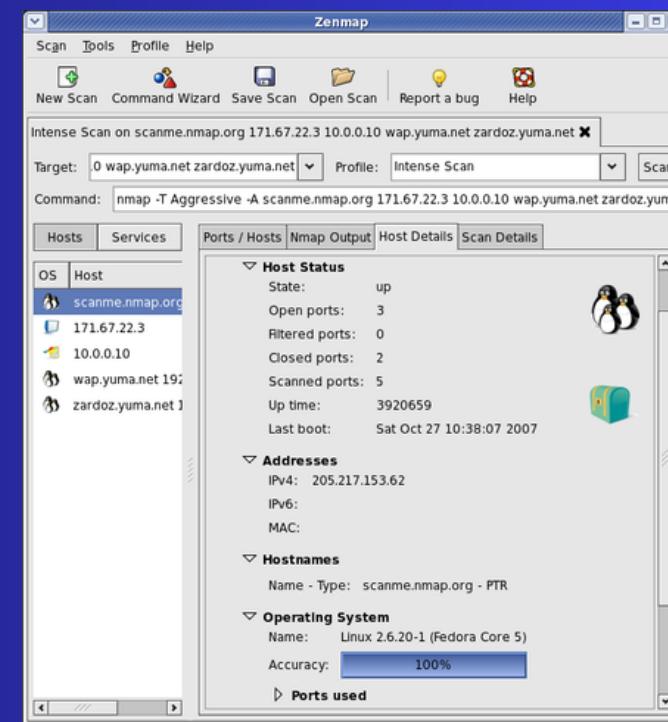
C:\Users\Matt>tracert 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:

 1  <1 ms    <1 ms    <1 ms  192.168.10.254
 2  4 ms     7 ms     1 ms  n4l-akl-internet.mdr-bng1.as45177.net.nz [14.1.43.222]
 3  1 ms     1 ms     1 ms  ae3-1303.mdr-cr1.as45177.net.nz [120.136.0.131]
 4  24 ms    24 ms    25 ms  xe-4-0-1-0.sy3-cr1.as45177.net.au [120.136.0.118]
 5  24 ms    24 ms    24 ms  as15169-ip-119.cust.sy3-cr1.as45177.net.au [120.136.0.119]
 6  25 ms    25 ms    25 ms  216.239.40.233
 7  25 ms    25 ms    25 ms  216.239.40.255
 8  25 ms    25 ms    25 ms  google-public-dns-a.google.com [8.8.8.8]

Trace complete.

C:\Users\Matt>
```



```
Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Matt>tracert 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:

 1  <1 ms    <1 ms    <1 ms  192.168.10.254
 2  4 ms     7 ms     1 ms  n4l-akl-internet.mdr-bng1.as45177.net.nz [14.1.43.222]
 3  1 ms     1 ms     1 ms  ae3-1303.mdr-cr1.as45177.net.nz [120.136.0.131]
 4  24 ms    24 ms    25 ms  xe-4-0-1-0.sy3-cr1.as45177.net.au [120.136.0.118]
 5  24 ms    24 ms    24 ms  as15169-ip-119.cust.sy3-cr1.as45177.net.au [120.136.0.119]
 6  25 ms    25 ms    25 ms  216.239.40.233
 7  25 ms    25 ms    25 ms  216.239.40.255
 8  25 ms    25 ms    25 ms  google-public-dns-a.google.com [8.8.8.8]

Trace complete.

C:\Users\Matt>
```

Análisis de dispositivos y puertos con Nmap

Abierto, cerrado, filtrado, no filtrado, abierto/filtrado, cerrado/filtrado.

Parámetros opciones de escaneo de nmap

```
sudo apt install nmap
nmap [ip]
nmap 192.168.1.2
nmap -p [rango] [ip]
nmap -p 20-200 192.168.1.2
```

Full TCP scan

Nmap le pide al sistema operativo subyacente que establezca una conexión con la máquina y el puerto de destino mediante la emisión de una connect llamada al sistema.

Stealth Scan

la **-sS** opción a Nmap. Requiere privilegios de paquete sin procesar, y es el escaneo TCP predeterminado cuando están disponibles. Entonces, cuando se ejecuta Nmap como raíz o administrador, **-sS** generalmente se omite.

Fingerprinting

técnica de seguimiento le permite identificar posibles ciberataques de phishing, entre otras y mejorar su protección de datos.

Zenmap

Los resultados del escaneo se pueden guardar y ver más tarde.

Análisis traceroute determina la ruta a un destino mediante el envío de paquetes ICMP al destino

Bibliografía

<https://nmap.org>

<https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/>

<https://keepcoding.io/blog/que-es-fingerprinting-ciberseguridad/#Fingerprinting>