**CURSO DE ESCANEO ACTIVO Y ANALISIS DE VULNERABILIDADES**

**IP Logger**

Este tipo de herramienta permite capturar la dirección IP de una persona que abre un enlace que se le proporciona.

En el proceso de dirección se obtiene los datos de la persona, como la IP y el navegador.

**Uso de Grabify IP Logger**

1. Ingresa la URL en el campo
2. Clic a botón **Create URL**
3. Aceptar términos de servicios y política de privacidad
4. Ingresaremos a un panel de información, para enviar la URL craqueada clic en **Copy new URL**

**¿Qué información brindará Grabity IP Logger?**

* IP
* Country
* Date/Time
* User Agent
* ISP
* Host Name

**Activar Smart Logger para mayor información. Estos datos se utilizan para rastrear a las personas.**

**¿Qué es ISP?**

ISP en inglés significa Internet Service Provider, refiriéndose a la compañía que provee servicios de internet tanto a clientes personales como a empresas.

**Banner Grabbing**

Consiste en hacer una solicitud a un servicio de internet que este corriendo atrás de un puerto en un servidor. Este banner responde al momento de hacer la solicitud, brinda información cómo qué tecnología esta detrás la versión.

Sirve para identificar vulnerabilidades en las versiones si es que ese servicio esta desactualizado.

**Banner Grabbing en Kali linux**

1. Abrimos la terminal
2. Colocamos netcat [udg.mx](http://udg.mx) 80

**netcat:** Permite conectarnos a un servidor y a un puerto especifico de ese servidor.

[udg.mx](http://udg.mx) : Dominio

**80:** Puerto de protocolo HTTP.

Una aplicación debe de llevar una solicitud consigo para obtener datos.

**HEAD (solicitud) / HTTP (Protocolo) /1.1 (versión)**

**Enumeración de subdominios**

Un [subdomino](https://www.wpbeginner.com/glossary/subdomain/) es la parte previa a un dominio.

Escala de tiempo

El contenido generado por IA puede ser incorrecto.

Sirven para navegar en diferentes secciones de la web.

Enumeración de subdominio en Kali Linux

1. Abrir la terminal
2. Actualizar el sistema e instalar sublist3r

sudo apt-get update && sudo apt-get install sublist3r

1. Colocamos el comando sublust3r para la enumeración de subdominios

sublist3r —domain nayarit.gob.mx

1. Se listara una enumeración de subdominios al dominio principal Texto

   El contenido generado por IA puede ser incorrecto.

Opciones de sublist3r

Texto

El contenido generado por IA puede ser incorrecto.

**Fingerprinting de Aplicaciones Web**

Fingerprinting —> Huella dactilar. Se utiliza para identificar a una persona de manera única a través del mundo.

¿Cómo se identifican?

A través de las membranas en los pulgares, dedos o manos. Estas membranas tienen características únicas y al ser únicas tienen maneras de identificarlas.

whatweb en kali linux

Sintaxis

whatweb option url

Ejemplo

Imagen que contiene Texto

El contenido generado por IA puede ser incorrecto.

El [footprinting](https://www.netacea.com/glossary/footprinting/) en un entorno digital, consiste en identificar a una máquina por medio de los identificadores únicos y versiones de las tecnologías que se ejecutan para su funcionamiento. Por ejemplo dirección ip, versión del servidor web, versión del lenguaje de programación del servidor, país, etc.

Versionado Semántico: <https://semver.org/>

**Identificación Waf**

Un WAF (Web Application Firewall, identifica las conexiones y peticiones) es un sistema de defensa para sitios web, que sirve para bloquear peticiones de tipo malicioso al website, si bien es posible encontrar algunas técnicas para burlar los waf dependiendo de la tecnología y versión de este.

También es posible encontrar:

IDS: Intrusion Detection System.

IPS: Intrusion Prevention System.

Uso de wafw00f en kali linux

Sintaxis

wafw00f url

Ejemplo

Texto

El contenido generado por IA puede ser incorrecto.

¿Qué hace la herramienta?

Hacer pruebas para identificar que firewall esta detrás de una aplicación web.

**Ping y Traceroute**

El Ping sirve para probar la conexión de otros equipos a través de la red.

¿Cómo compruebo la conexión de otros equipos?

El comando para ver si hay comunicación de la máquina es:

ping -option domino/IP

Brinda información sobre el servicio, el SO, ect.

Ejemplo

Texto

El contenido generado por IA puede ser incorrecto.

-c 4: Mostrar 4 respuestas ping

ICMP

* Protocolo de mensajes de control de Internet [(ICMP)](https://www.fortinet.com/lat/resources/cyberglossary/internet-control-message-protocol-icmp). Verifica si los datos llegan a su destino y en el momento correcto
* Se usa para diagnosticar problemas en la red

TTL

* Determina cuánto tiempo se debe almacenar en caché una consulta o contenido, en las redes es el tiempo de vida time to live [(TTL).](https://www.fortinet.com/lat/resources/cyberglossary/what-is-ttl)

Traceroute

* Permite ver por dónde pasa un paquete antes de llegar a su destino final (no es una conexión directa, pasa por distintos dispositivos).

Sintaxis

traceroute dominio

Ejemplo

Imagen que contiene Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

En términos de seguridad, sirve para ver si en una organización existen multiples dispositivos antes de salir en internet.

**Nslookup**

Se utiliza principalmente para encontrar la dirección IP que corresponde a un host, o el nombre de dominio que corresponde a una dirección IP (un proceso llamado "Reverse [DNS Lookup](https://www.ionos.com/digitalguide/server/tools/nslookup/)")

Nslookup significa “Name server look up” 💡

Nslookup en Kali Linux

1. Abrir la terminal de linux
2. Colocar nslookup
3. set type=service Interfaz de usuario gráfica, Sitio web

   El contenido generado por IA puede ser incorrecto.
4. Colocar dominio, por ejemplo: >platzi.com Interfaz de usuario gráfica, Texto

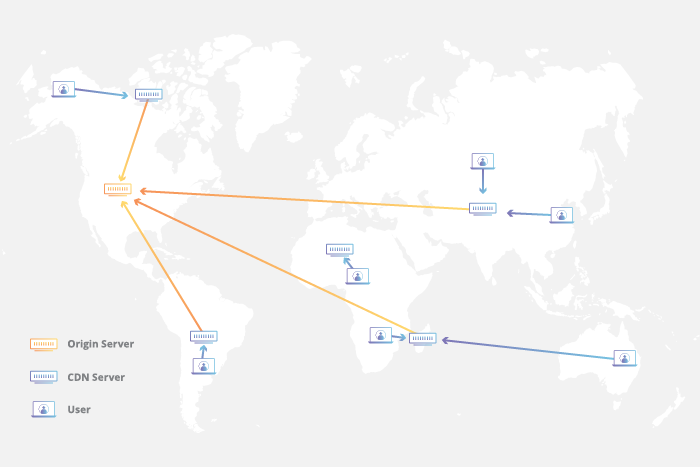
   El contenido generado por IA puede ser incorrecto.

Para salir: ctrl + C

DNS checker

Al realizar un [DNS checker](https://dnschecker.org/) pruebas Nslookup gráficamente y la solicitud se hace a multiples servidores.

Servicios que brinda DNS checker

* A: Dirección IPv4.
* AAAA: Dirección IPv6.
* CNAME: Alias de otro dominio. Se utilizan para asociar nuevos subdominios con dominios ya existentes.
* MX: Lista de servidor de intercambio de correo que se utiliza para el dominio.
* PTR: Punto de terminación de red.
* NS: Hace referencia a qué servidor de nombres es el autorizado para el dominio.
* SOA: Comienzo de autoridad.
* SRV: Hace referencia a un servicio, por ejemplo: TCP.
* TXT: Referencia a un texto.
* SPF: Servidores a qué están autorizados para enviar correos electrónicos.
* CAA: Especifica las posibles autoridades de certificación (CA) para un dominio.
* DS: “Delegation Signer”, sirve para identificar zonas con firmas DNSSEC.
* DNSKEY: Contiene una clave pública para DNSSEC.
* CDN = Content Delivery Network. ****

Dependiendo de los resultados se toma decisiones, para que, posteriormente, salga qué decisión tomar en una auditoria.

**Netdiscover**

Permite identificar dispositivos dentro de una red de manera automática. [Netdiscover](https://www.kali.org/tools/netdiscover/) es una herramienta que se utiliza para reunir toda la información importante sobre la red. Recoge información sobre los clientes conectados y el router

**Uso de Netdiscover en Kali Linux**

1. Abrir la terminal
2. sudo netdiscover
3. Colocar contraseña
4. Automáticamente identificara los dispositivos en la red

**Opciones**

Texto

El contenido generado por IA puede ser incorrecto.

**Uso**

**Comando**

sudo netdiscover -i eth0 -r IP/MASK -P -N | grep -Eo '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}’

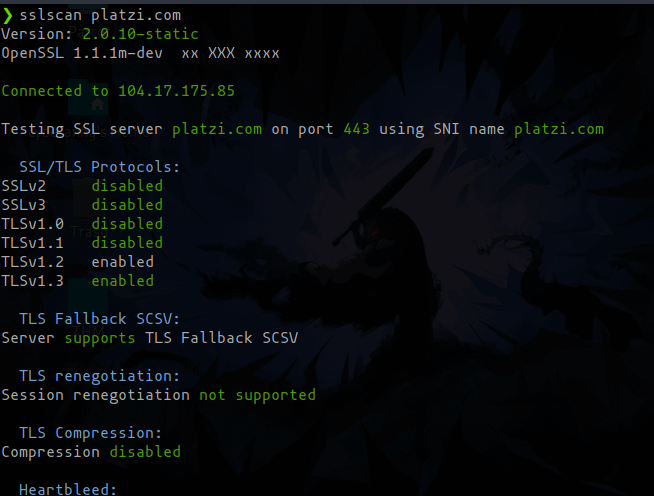
**Explicación del comando** Escala de tiempo

El contenido generado por IA puede ser incorrecto.

**SSLscan**

Permite escanear certificados ssl y obtener información de los mismos. Un [escaneo SSL](https://www.kali.org/tools/sslscan/) es necesario para solucionar problemas de comunicación entre el dispositivo inSync Client y inSync Cloud.

**¿Qué mostrará SSLscan?**

* SSL/TLS Protocols
* TLS Fallback SCSV
* TLS Compression
* Heartbleed (Si es o no vulnerable)
* Supported Server cipher(s)
* Server Key Exchange Group(s)
* SSL Certificate 

**Sintaxis**

sslscan url

**Ejemplo**

sslscan platzi.com

Nota: Se puede obtener información de sub dominos💡

**Enum4Linux**

Permite obtener información a través del protocolo SMB.

Normalmente, hay unidades compartidas SMB en un servidor a las que se puede conectar y utilizar para ver o transferir archivos. SMB a menudo puede ser un gran punto de partida para un atacante que busca descubrir información sensible. Enu4mlinux es una gran herramientas para conseguir informarción SMB.

¿Por qué usar Enu4mlinux?

Es una herramienta utilizada para enumerar los recursos compartidos SMB tanto en sistemas Windows como Linux.

Hace fácil extraer información del objetivo que pertenece a SMB.

Sintaxis

enum4linux -option IP

Ejemplo

enum4linux -a 192.168.0.20

Información importante que brinda Enu4mlinux

Información del grupo

Estado del dispositivo

Información de usuario o contraseñas

Información del Sistema Operativo

**Análisis de dispositivos y puertos con Nmap**

**Cuanto más se conozca el sistema o la red de destino, más opciones se tendrán**, por eso es importante llevar a cabo una enumeración adecuada antes de realizar cualquier intento de explotación.

* [**Nmap**](https://nmap.org/) **es una herramienta de exploración de redes y seguridad / escáner de puertos. Fue diseñada para escanear rápidamente grandes redes, aunque funciona bien contra hosts individuales.**

**¿Cuál es el objetivo de identificar dispositivos y puertos abiertos?**

* Identificar sevicio y sus versiones
* Conocer parte de la topología de red
* Identificar puertos abiertos dentro de la red
* Identificar que sistemas operativos se encuentran en la red

**Sintaxis de nmap**

nmap -Scan-type -option(s) IP

**Ejemplos de escaneo**

**Escaneo básico**

nmap 192.168.0.1/24

**Escaneo**

nmap -sS -sU -p 192.168.0.1

Nota: Dependiendo del escaneo se necesita permisos de super usuario 💡

* -sS →‘Syn Scan’
* -sU → ’UDP Scan’
* -O → ‘Detect OS'
* -sV → 'Dectect service versions'
* -v → 'Verbosidad, se puede usar hasta 3 seguidos'
* -oA → 'Formato principal de guardado de enumeracion'
* -oN → 'Guardar enumeracion en formato Normal'
* -n → 'Eliminas resolucion de DNS'
* -oG → 'Guardar consulta en formato grepable'
* -A → 'Modo agresivo, genera ruido en red pero devuelve toda info'
* -T[1-5] → 'Control velocidad consulta 1 lenta, 5 muy intrusivo'
* -p → 'Escanero de un puerto especifico o rango de puertos'
* -p- → 'Analizar TODOS los puertos'
* --script →'Uso de scripts de la libreria nmap'
* -sT → 'TCP Connect Scan'
* -sN → ‘TCP Null Scan, no maneja banderas en paquete'
* -sF → 'TCP FIN Scan'
* -sX → 'TCP Xmas Scans, por la forma de arbol de navidad que tiene en el paquete'
* -sn → 'Barrido de ping, no escanea solo depende de respuesta ICMP o ARP '
* -Pn → 'Quitamos fase de Discovery, es decir pedimos que no haga ping'
* -iL → 'Indicas uso de un archivo con ips para scanear'
* -sS →‘Syn Scan’
* -sU → ’UDP Scan’
* -O → ‘Detect OS'
* -sV → 'Dectect service versions'
* -v → 'Verbosidad, se puede usar hasta 3 seguidos'
* -oA → 'Formato principal de guardado de enumeracion'
* -oN → 'Guardar enumeracion en formato Normal'
* -n → 'Eliminas resolucion de DNS'
* -oG → 'Guardar consulta en formato grepable'
* -A → 'Modo agresivo, genera ruido en red pero devuelve toda info'

**Parámetros y opciones de escaneo**

En la clase de análisis de dispositivos y puertos con Nmap, se vio que es una herramienta de exploración de redes y seguridad / escáner de puertos.

**Parámetros en nmap**

Un escaneo simple, pero sin embargo recolecita información sensible e importante para el análisis de nuevos vectores de ataque.

nmap -sV -O -v -T3 -p <puertos> IP/Mask

**Parámetros**

-sV: Versiones de los servicios

-O: Versión del Sistema Operativo

-v: Muestra a detalle lo que hace la herramienta

-T: Permite indicar la intensidad del escaneo

-T0: Paranoico (Muy lento) 🚅

-T1: Sigiloso (Más lento) 🛬

-T2: Sostificado (Lento) 🛫

-T3: Normal ✈️

-T4: Agresivo (Más rápido) 🛩️

-T5: Muy agresivo (Insane) 🚀

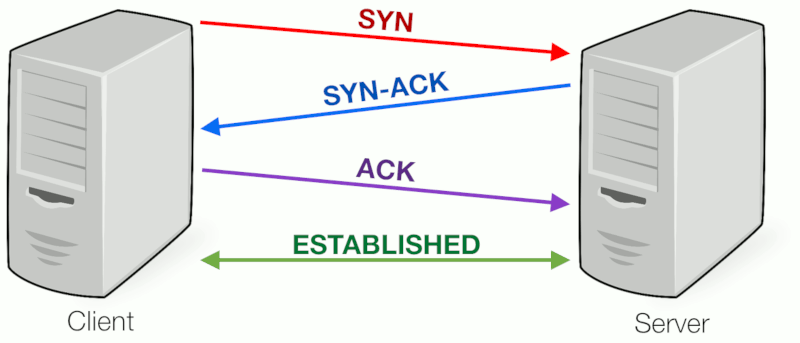
-p: Rango de [puertos](https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/) a escanear

**Full TCP scan vs Stealth scan**

Wireshark Monitorea todos los paquetes que se envían entre el dispositivo y la puerta de enlace, también identifica el broadcast.

**¿Cómo funciona Full TCP scan y Stealth Scan?**

En el protocolo TCP (Capa 4) para establecer conexión utiliza las conexión de

El protocolo TCP para establecer una conexión utiliza 3-Way-Handshake 

Conexión de 3 vías, se envían los paquetes en 3 direcciones

**Full TCP scan**

Completa la conexión 3-way-Handshake (Intrusivo), hace un análisis completo hasta llegar a su conexión.

-sT : Análisis utilizando TCP CONNECT

**Stealth scan**

Realiza la conexión SYN y termina en ACK (Sigiloso, requiere privilegio), hace un análisis solo utilizando TCP SYN

* **El escaneo se llevaba a cabo hasta el segundo paso de la conexión 3-way-Handshake**

-sS : Análisis utilizando TCP SYN

**Fingerprinting con Nmap**

La huella digital [**(Fingerprinting)**](https://ssd.eff.org/en/module/what-fingerprinting) es el proceso por el que un sitio o servicio remoto recopila pequeños fragmentos de información sobre la máquina de un usuario y los une para formar una imagen única, o "huella digital", del dispositivo del usuario.

**¿Cuáles son las formas principales de Fingerprinting?**

Las dos formas principales son: \* **La huella digital del navegador**, donde esta información se entrega a través del navegador cuando un usuario visita sitios remotos. \* **La huella digital del dispositivo**, cuando la información se entrega a través de las aplicaciones que un usuario ha instalado en su dispositivo.

**DETECCIÓN DE SISTEMA OPERATIVO:**

* -**O:** Opción para permitir detección del sistema operativo.
* **–-osscan-limit:** Opción para limitar detección del sistema operativo a objetivos mas “fáciles”
* **–-osscan-guess:** Intentar adivinar el sistema operativo de manera más agresiva.

**DETECCIÓN DE SERVICIOS/VERSIÓN:**

* -**sV:** Probar puertos abiertos para determinar información de servicios/versión.
* **–-version-intensity :** Desde 0 (ligero) hasta 9 (probar todas las versiones)
* **–-version-light:** Limitarse a solo las pruebas de combinaciones mas probables de encontrarse (intensidad 2)
* **–-version-all:** Probar cada posible combinación (intensidad 9)–version-trace: Mostrar la actividad detallada del proceso de escaneo de versiones.

**Comando para detectar sistema operativo del servidor y servicios ejecutándose en un dominio (Fingerprinting)**

sudo nmap -O --osscan-guess -sV --version -all dominio

**Escaneo agresivo con Zenmap**

[Zenmap](https://geek-university.com/what-is-zenmap/) es una interfaz gráfica gratuita y de código abierto para Nmap

**Características de Zenmap**

* Puede mostrar la salida normal de Nmap, pero también puede organizar su visualización para mostrar todos los puertos de un host o todos los hosts que ejecutan un servicio en particular.
* Resume los detalles sobre un solo host o un escaneo de com en una pantalla conveniente. Incluso puede utilizar Zenmap para dibujar un mapa topológico de las redes descubiertas.
* Puede utilizar Zenmap para mostrar gráficamente las diferencias entre dos escaneos. Esto puede ayudar a rastrear los nuevos hosts o servicios que aparecen en sus redes, o los existentes que caen.
* Puede utilizar los perfiles de comando de Zenmap para ejecutar el mismo escaneo más de una vez.

**¿Cómo usar Zenmap?**

1. Elegir el tipo de perfil para el escaneo (Intense scan). Una vez elegido el perfil, se coloca el comando que viene por defecto
2. En objetivo colocar IP a escaner
3. Clic a botón **Escaneo**

**Nota 💡**

* En la parte izquierda se mostrará los dispositivos que fueron detectados dentro de la red que fue escaneada
* Al seleccionar la red se pueden ver los puertos abiertos
* El signo de interrogación indica que no se puedo identificar el dispositivo
* En la sección de “Topología” se podrá ver todos los dispositivos que se identificaron. Si queremos interpretar cada uno de los símbolos, dar clic al botón de **Leyenda.**

**Análisis de Traceroute**

[Traceroute](https://www.fortinet.com/lat/resources/cyberglossary/traceroutes) permite ver por dónde pasa un paquete antes de llegar a su destino final (no es una conexión directa, pasa por distintos dispositivos).

**El análisis de estos datos es de información**, ya que no se obtiene el permiso para escanear o hacer auditoria de pentesting a ninguno de los dispositivos por el cual pasa un paquete antes de llegar a su destino final.

**¿Qué hace Traceroute?**

* Funciona al enviar paquetes de Protocolo de mensajes de control de Internet (ICMP), y cada enrutador involucrado en la transferencia de datos recibe estos paquetes. Los paquetes de ICMP proporcionan información sobre si los enrutadores utilizados en la transmisión pueden transferir los datos de manera efectiva.

**¿Cuál es la diferencia entre Ping y Traceroute?**

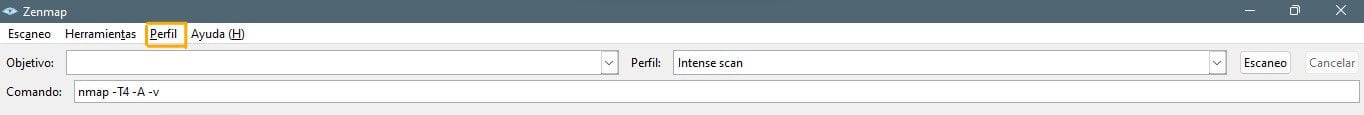
* El ping **indica si es accesible** y el tiempo que toma para trasmitir y recibir datos, traceroute **detalla la información precisa de la ruta.**

**Creación de perfiles de escaneo en Zenmap**

Puede **mostrar la salida normal de Nmap,** pero también puede **organizar su visualización** para mostrar todos los puertos de un host o todos los hosts que ejecutan un servicio en particular.

Recordar que Zenmap **puede utilizar los perfiles de comando para ejecutar el mismo escaneo más de una vez ✨**

**Perfil de escaneo**

1. Abrir Zenmap
2. Clic a la sección de **Perfil** 
3. Clic a Nuevo perfil o comando (o ctrl + P) Interfaz de usuario gráfica, Texto, Aplicación

   El contenido generado por IA puede ser incorrecto.
4. Aparecerá la ventada de Editar Perfil Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

   El contenido generado por IA puede ser incorrecto.
5. Indicar qué parámetros se desea escanear. Interfaz de usuario gráfica, Aplicación

   El contenido generado por IA puede ser incorrecto.

Para finalizar, clic a **Guardar cambios.**

1. Una vez guardados los cambios, le damos a Perfil y se visualizará el escaneo guardado

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

**El tipo de escaneo se realiza en base a las necesidades o de lo que se requiere escanear, para dejarlo listo para cuando se necesite.** 🧭

**Nmap Scripting Engine**

Se conoce como [script](https://www.significados.com/script/) a un texto que consta de una serie de instrucciones que deben de seguir. En programación se usa este término para referise al **código fuente escrito en algún tipo de lenguaje interpretado** (casi siempre).

Cuando se ejecuta un [script](https://www.linuxadictos.com/que-es-script.html), será el intérprete **el que interprete las ordenes**

**Algunos scripts funcionales:**

* http-enum: Enumera los directorios utilizados por las aplicaciones y servidores web más populares.
* http-errors: Este script rastrea el sitio web y devuelve las páginas de error.
* http-title: Muestra el título de la página por defecto de un servidor web.
* nmap -p22 --script ssh-brute.nse --script-args
* userdb=,passdb=
* nmap -script=smb-brute
* nmap -script=smb-enum-users
* nmap -Pn -n -vv --script banner
* nmap -Pn -n -vv --script malware
* nmap -Pn -n -vv --script vuln

<https://nmap.org/nsedoc/scripts/>

**Gobuster**

Gobuster es una herramienta que **permite llevar a cabo solicitudes a una aplicación web, realiza una enumeración de directorios que no se encuentras visibles** o no se encuentran accesible para los usuarios.

**Gobuster en Kali Linux**

**Para saber si está instalado Gobuster**

gobuster version o gobuster

**Actualizar si no esta en su versión más reciente** 💡

**Instalación de Gobuster**

sudo apt-get install gobuster

**Sintaxis**

gobuster commands -flag

gobuster commands -flag /wordlist domain

**Ejemplo**

gobuster dir -t 20 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

**Dir**

este es el modo para enumerar los directorios del sitio web, los directorios con lo que va despues de la diagonal al terminar el nombre del sitio.

**Otra herramienta para la enumeración de directorios**

[**Dirsearch**](https://github.com/maurosoria/dirsearch) **- Web path scanner**

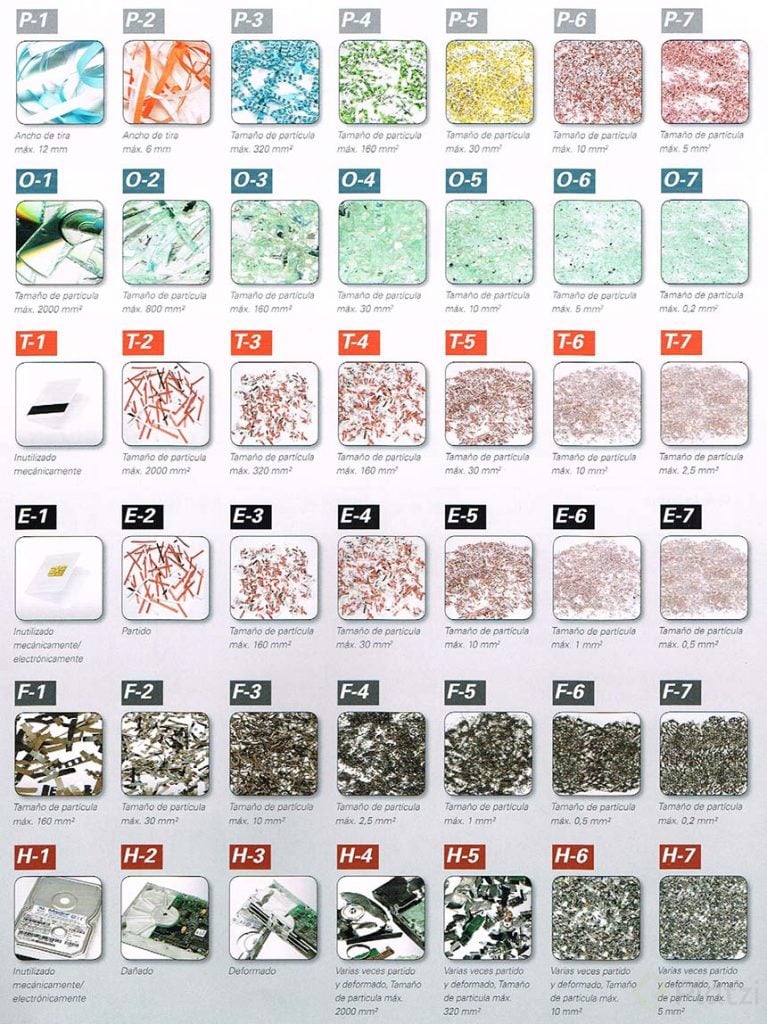
[Es una herramienta avanzada](https://esgeeks.com/guia-completa-uso-dirsearch/?feed_id=5703&_unique_id=6076249cc271f) de línea de comandos diseñada para forzar directorios y archivos en servidores web, también conocida como escáner de rutas web

**Dumpster Diving**

Dumpster Diving o Trashing **consiste en explorar la basura con el objetivo de buscar/recolectar información valiosa**, como: - USB - Discos óptimos - Documentos - Discos duros - Estados de cuenta - Información del empleado

**GDPR**

[General Data Protection Regulation (GDPR)](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_es) **este reglamento incluye cómo deshacer de manera eficaz y correcta la basura de una empresa u organización, asignando niveles dependiendo de su importancia.**



Es uno de los [ataque de ingeniería social.](https://platzi.com/clases/2238-ingenieria-social/37095-ejemplos-de-ataques-de-ingenieria-social-pretextin/)

**Ingeniería Social**

La disciplina que consiste en **extraer datos sin que la víctima se percate** y **lograr la confianza para luego engañarlas** y **manipularlas** para el beneficio propio de quien la implementa, se le conoce como **ingeniería social.**

Consiste en aprovechar las habilidades sociales de la persona, realizando una recolección de datos activas.

**¿Por qué funciona la ingeniería social?**

Para que la ingeniería social sea efectiva, se necesita tres elementos fundamentales:

* Todos tienen **atención selectiva**
* Todos suelen **distraerse** con algo
* La **confianza**

**Las personas son el eslabón más débil**, es extremadamente **difícil de detectar cuando no existe IDS (Intrusion Detection System) para la falta de sentido de común o ignoracia.**

**¿Qué se puede recolectar?**

* Información a través de medios sociales
* Información de acceso wifi en algún establecimiento
* Complementar información
* Crear una identidad falsa
* Encontrar otros vectores de ataque

**Nmap**

Cuanto más se conozca el sistema o la red de destino, más opciones se tendrán. Para buscar vulnerabilidades de manera automática con nmap, se utiliza el siguiente comando:

sudo nmap -A -v -T4 —script=vuln IP/Mask

1. -A: Identificar el dispositivo y sus versiones
2. -v: Verbosidad
3. T4: Escaneo Agresivo
4. —script=vuln: Es la categoría para identificar vulnerabilidades

**No busca vulnerabilidades**

nmap **no es una herramienta especializada para el análisis de vulnerabilidades,** solo se usan los script para detectar p ver si tiene vulnerabilidades 💡

**Sintaxis**

—script=categoría

**Ejemplo**

—script=vuln

**Joomscan**

Permite buscar vulnerabilidades de manera automática en aplicaciones web que tengan el SMS Joomla.

El script JoomScan, es una aplicación que ejecutada desde consola (a través de interface web) y que **permite localizar vulnerabilidades web conocidas para Joomla. Está escrita en Perl (como todo buen script que se precie) y permite la actualización por** [**SVN**](https://www.perforce.com/blog/vcs/what-svn) **(subversion).**

**Instalación**

1. Actualizar el sistema

sudo apt upgrade

sudo apt update

1. Instalación de Joomscan

sudo apt-get install joomscan

**Para comprobar la instalación ejecutar el comando:** joomscan

**Sintaxis**

joomla -option url

**Ejemplo**

joomla -ec --url https://www.poncitlan.gob.mx

**-ec:** Enumeración de componentes

**Nota 💡**

**Si la instalación de joomla se encuentra en una carpeta, hay que indicar la carpeta donde se encuentra.**

joomla -ec --url https://www.poncitlan.gob.mx/ruta-de-carpeta-joomla

**Wpscan**

Permite escanear vulnerabilidades en aplicaciones web, este escáner es especializado para aplicaciones web que estén hechas en WordPress.

**Escáner de vulnerabilidades de WordPress**

Es una herramienta de pruebas de penetración utilizada para escanear [vulnerabilidades en sitios web con WordPress.](https://www.golinuxcloud.com/wpscan-wordpress-vulnerability-scanner/#What_is_WPScan) Utiliza la Base de Datos de Vulnerabilidades de WordPress de WPScan, que existe desde 2014, para escanear vulnerabilidades de WordPress, vulnerabilidades de plugins y vulnerabilidades de temas. Imagen que contiene jugador, pelota, golpear, balanceando

El contenido generado por IA puede ser incorrecto.

**Sintaxis**

wpscan -option --url

**Ejemplo**

wpscan -e —url dominio

**Creación de cuenta en Wpscan**

1. Ingresar a [WPScan](https://wpscan.com/)
2. Crear cuenta
3. Ingresar datos personales para la creación de la cuenta en WPScan
4. Iniciar sesión
5. Copiar el **API Token** que aparece en el panel de control de usuario

**Comando para ingresar API Token**

wpscan -e --url dominio --api-token token

**¿Qué sucede si no se utiliza una API Key en WPscan?**

El software trabaja con normalidad, solo que **no enumera las vulnerabilidades identificadas**

**Nessus Essentials**

Escáner de vulnerabilidades [Nessus Essentials](https://www.tenable.com/products/nessus/nessus-essentials) **permite escanear la red doméstica personal con la misma alta velocidad, evaluaciones a profundidad o buscar vulnerabilidades de forma automatizada.**

**Esta enfocado a analizar las redes informáticas** (Todo lo que tenga sistema operativo, como sistemas embebidos, dispositivos considerados como parte del IoT, etc.)

**¿Qué escanea?**

* Puertos abiertos
* Versiones de los servicios
* Detecta e indica las vulnerabilidades de cada dispositivo y puertos

**Nessus no esta especializado en aplicaciones web** 🚩

**Importante 💡**

Se debe crear una cuenta **para obtener la clave para la versión essentials.**

Al dar clic a empezar, se va a redireccionar a la sección para descargar Nessus.

* Buscar versión para el SO ha utilizar

Una vez ejecutado y aceptado los términos, activar el código (Revisar la bandeja de correos) Interfaz de usuario gráfica, Sitio web

El contenido generado por IA puede ser incorrecto.

Después se creara una cuenta de usuario o iniciar sesión si ya se ha creado la cuenta.

Para crear un nuevo escaneo, clic a **New Scan** Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

**Basic Network Scan**

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

**¿Qué se identifica?**

* Los dispositivos de la red
* Puertos abiertos
* Vulnerabilidades (de los puertos abiertos que estén)

**¿Cómo se realiza el scaneo?**

Al dar clic aparecerá la configuración para el escaneo.

**Apartados obligatorios:**

* Nombre
* Targets (Aquí se coloca la IP a escanear)

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

Una vez configurado, clic a **Save** y se abrirá un nuevo panel de los dispositivos vulnerables.

**Nota 💡**

* La versión gratuita esta limitada comparada a la versión empresarial.

**Vega**

Encuentra vulnerabilidades en la web, vulnerabilidades web hechas en cualquier tecnología web, prueba las ruta, archivos o parámetros en **busca de vulnerabilidades genéricas.**

*Realiza un escaneo de vulnerabilidades en general.*

**Software necesarios antes de instalar Vega**

* Java
* Java Developer kit

**Instalación de Vega**

1. Descargar paquete de Vega desde la página oficial Interfaz de usuario gráfica, Texto

   El contenido generado por IA puede ser incorrecto.
2. Elegir opción de descarga dependiendo el Sistema Operativo.
3. Ejecutar el programa para su instalación
4. Una vez que se haya ejecutado, aparecerá la interfaz gráfica de Vega

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

**¿Cómo comenzar un escaneo con Vega?**

1. Clic a **Star new scan (**botón izquierdo superior**)** o **ctrl + N**
2. Pegar **url** a escanear
3. Clic a **Finish** o **Next** para agregar más opciones de escaneo

Al realizar un escaneo es normal que se encuentren falsos positivos, son vulnerabilidades detectadas, pero, **cuando se realiza la prueba de verificación resulta ser falsa la información, que no es vulnerable.**

**Tipos de alerta**

* High 🔴
* Medium 🟠
* Low 🟢
* Info 🔵