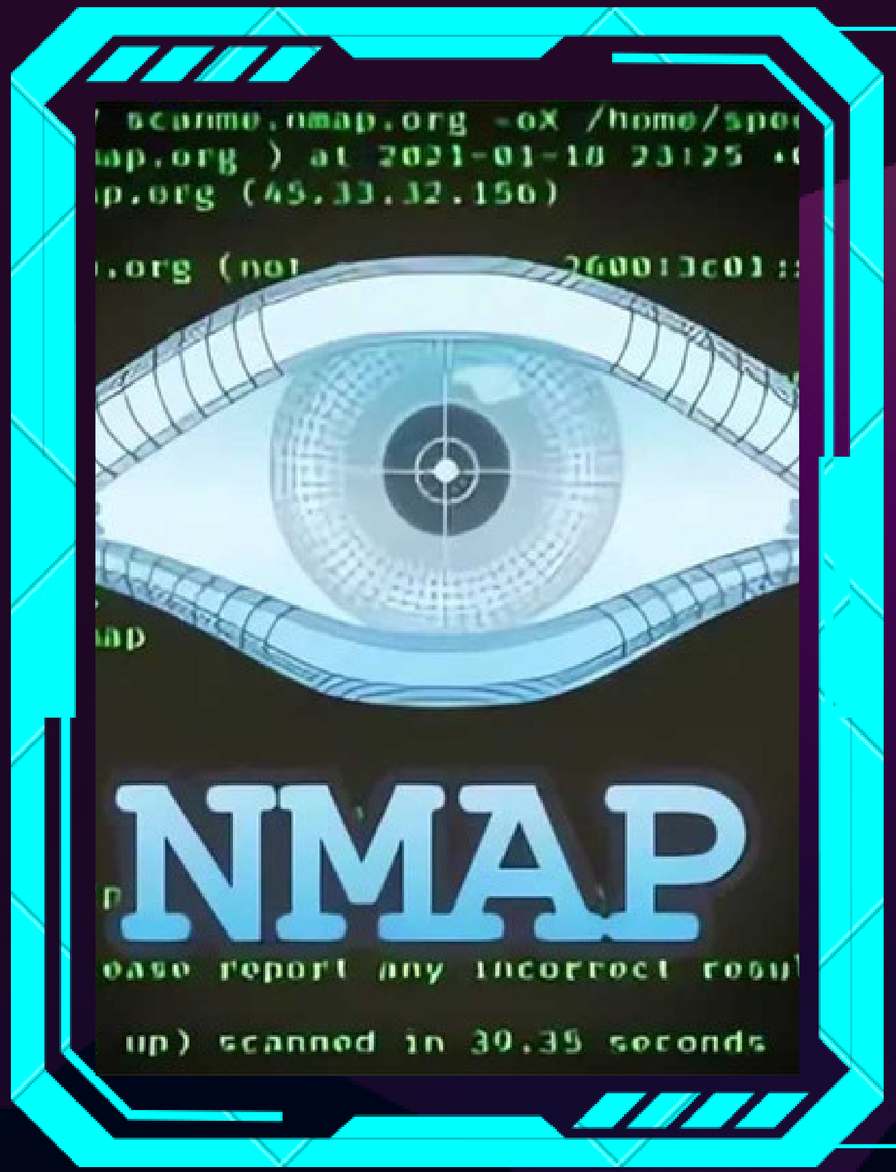
CONCEPTOS DE VULNERABILIDAD

NÉSTOR HORACIO ZEA HERNÁNDEZ 7°M

HERRAMIENTAS DE VULNERABILIDAD

HERRAMIENTAS DE VULNERABILIDAD



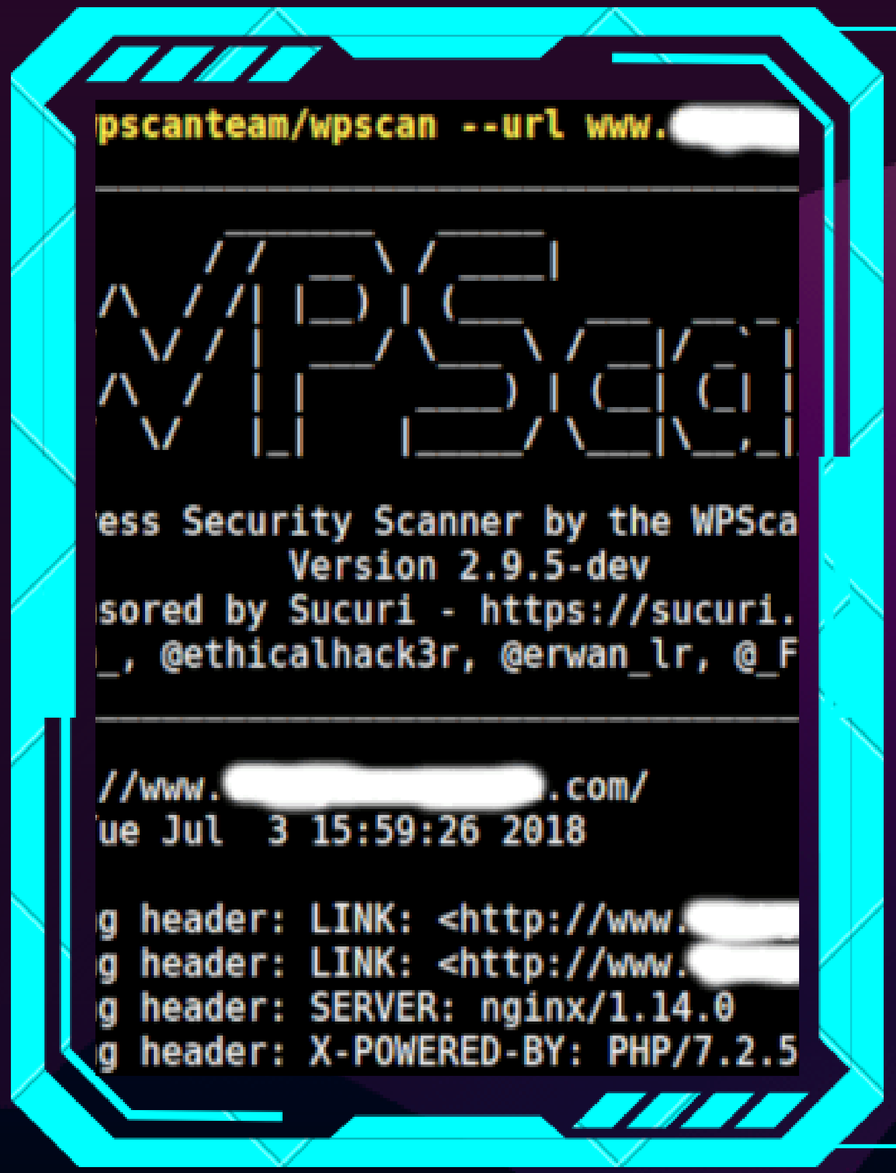
NMAP

Network Mapper es una herramienta de código abierto utilizada para descubrir hosts y servicios en una red, creando un mapa de la topología. Es una herramienta de código abierto creada en 1998 que es muy reconocida en el mundo de seguridad informatica por su funcionalidad de escaneo de redes, puertos y servicios que ha ido mejorando con el correr de los años.

JOOMSCAN

Escáner de seguridad Joomscan es una herramienta de auditoría de sitios web para Joomla. Está escrito en Perl y es capaz de detectar más de 550 vulnerabilidades como inclusiones de archivos, inyecciones de SQL, Defectos de RFI, BIA, Defecto XSS, inyección ciega de SQL, protección de directorios y otros. Es una herramienta específicamente diseñada para escanear y evaluar la seguridad de sitios web construidos en el CMS Joomla.

HERRAMIENTAS DE VULNERABILIDAD



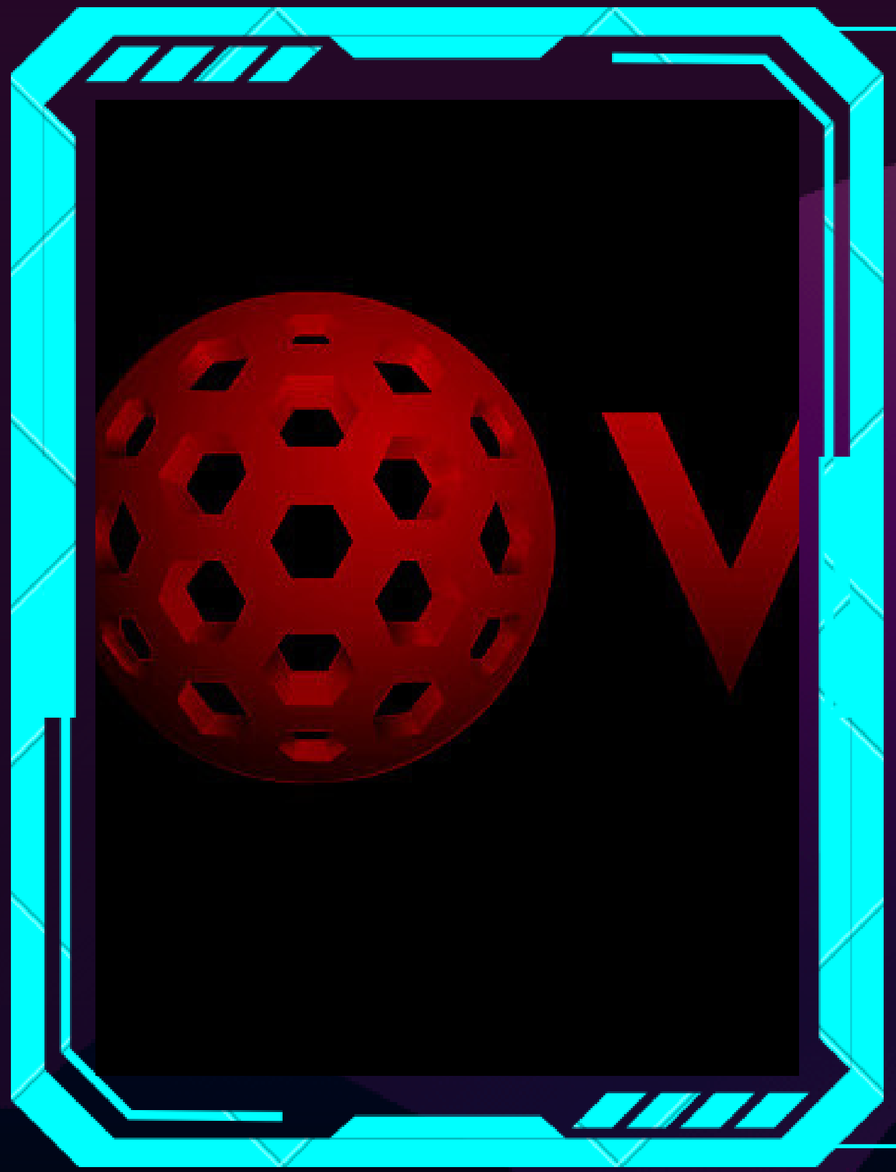
WPSCAN

Es una herramienta diseñada para evaluar la seguridad de sitios web basados en WordPress. Escanea sitios en busca de vulnerabilidades en el CMS, plugins y temas utilizados en la instalación. Es una herramienta muy útil para comprobar las vulnerabilidades y puntos débiles de tu sitio Wordpress. Las irregularidades y problemas en Wordpress cada vez son más comunes. Así podemos decir que es un plugin pero que no elimina los objetos sospechosos, sino que ayuda al usuario a identificarlos para eliminarlos por completo.

NESSUS ESSENTIALS

Es una herramienta utilizada principalmente para escanear vulnerabilidades, es desarrollada y mantenida por Tenable. Tiene un motor para escanear los objetivos que se basa en plugins.
Es una herramienta de escaneo de vulnerabilidades que identifica debilidades en sistemas y aplicaciones.

HERRAMIENTAS DE VULNERABILIDAD

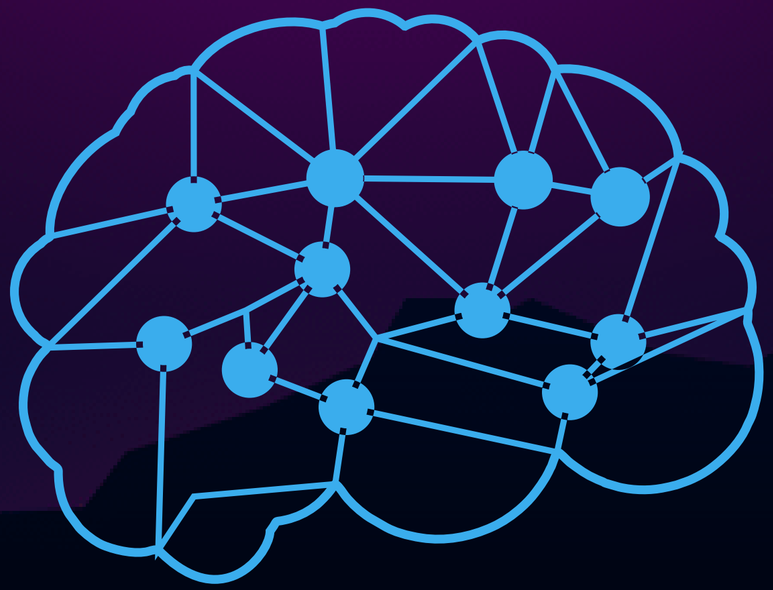


VEGA

Es una plataforma de pruebas de seguridad web que se utiliza para evaluar la seguridad de aplicaciones web. Puede realizar escaneos de seguridad automatizados e identificar vulnerabilidades.

Esta herramienta realiza diversas funciones tales como: ·Análisis de Vulnerabilidades ·Crawler (copia del sitio web) ·Análisis de contenido · Modificación manual de paquete HTTP (proxy) La herramienta tiene módulos para realizar ataques típicos del OWASP como XSS, SQL Injection, Directorio transversal, URL Injection, detección de errores, etc

INTELIGENCIA MISCELÁNEA



INTELIGENCIA MISCELÁNEA

GOBUSTER

Es una herramienta de línea de comandos utilizada para realizar ataques de fuerza bruta o enumeración de directorios y archivos en un sitio web. También ayuda a descubrir contenido oculto o archivos/directorios mal configurados en servicios web. Gobuster es una herramienta utilizada para realizar fuerza bruta a: URIs (directorios y archivos) en sitios web, subdominios DNS (con soporte de comodines), y nombres de hosts virtuales en los servidores web.

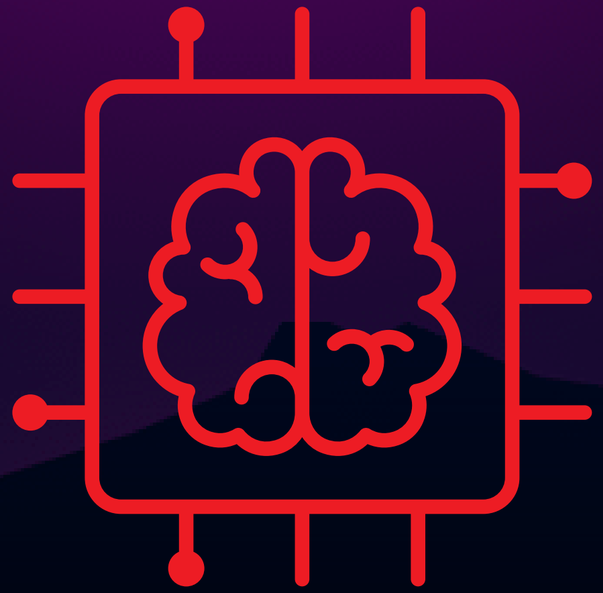
DUMPSTER DIVING

Se refiere a la práctica de buscar información valiosa, como contraseñas o documentos confidenciales, en la basura física o digital de una organización.

INGENIERÍA SOCIAL

La ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados. Además, los hackers pueden tratar de aprovecharse de la falta de conocimiento de un usuario; debido a la velocidad a la que avanza la tecnología, numerosos consumidores y trabajadores no son conscientes del valor real de los datos personales y no saben con certeza cuál es la mejor manera de proteger esta información.

INTELIGENCIA ACTIVA



INTELIGENCIA ACTIVA

ANÁLISIS DE DISPOSITIVOS Y PUERTOS CON NMAP

Utilizando Nmap, se realiza un escaneo en una red para identificar dispositivos activos y los puertos abiertos en esos dispositivos. Este tipo de ataque también se conoce como port scan. Básicamente lo que hace un atacante es analizar de forma automática todos los puertos de un equipo, como por ejemplo un ordenador, que esté conectado a la red. Lo que buscan es detectar posibles puertos abiertos y cuáles podrían tener protocolos de seguridad deficientes.

PARÁMETROS Y OPCIONES DE ESCANEO DE NMAP

Nmap ofrece una variedad de opciones de escaneo, como escaneos TCP, UDP, scripts personalizados, etc. Los parámetros permiten ajustar el alcance y la profundidad del escaneo

FULL TCP SCAN

Un "Full TCP Scan" es un término no oficial que a menudo se usa para referirse a un escaneo exhaustivo de todos los puertos TCP en un objetivo. En el contexto de Nmap, puedes lograr esto utilizando el parámetro -p-, que escaneará todos los 65535 puertos TCP posibles en el rango.

INTELIGENCIA ACTIVA

STEALTH SCAN

El término "Stealth Scan" se refiere a un tipo específico de escaneo de puertos en el que el escáner intenta ser lo más discreto posible, evitando que el objetivo detecte el escaneo. Un escaneo sigiloso, como “Stealth Scan” en Nmap, utiliza técnicas para ocultar el escaneo y parecer menos intrusivo para el objetivo.

FINGERPRINTING

En seguridad informática, el fingerprinting implica identificar el sistema operativo, software y versiones utilizadas en un objetivo, Esto puede ayudar a los atacantes a seleccionar vulnerabilidades específicas para explotar. se refiere al proceso de recopilar información detallada sobre un sistema o servicio específico en una red para determinar su versión, configuración y otros detalles relevantes. Esto se hace a menudo con el objetivo de identificar las vulnerabilidades y posibles puntos débiles en un sistema para fines de análisis de seguridad.

ZENMAP

Zenmap es una interfaz gráfica de usuario (GUI) para Nmap (Network Mapper), que es una herramienta de código abierto utilizada para el escaneo de redes y la detección de dispositivos y servicios en una red. Zenmap proporciona una manera más visual y amigable de utilizar Nmap, lo que hace que la configuración y ejecución de escaneos sea más accesible para usuarios menos familiarizados con la línea de comandos..

ANÁLISIS TRACEROUTE

El análisis de "traceroute" es una técnica utilizada para rastrear la ruta que sigue un paquete de datos a través de una red, desde el origen hasta el destino. Esta técnica es útil para entender cómo se enrutan los datos a través de diferentes dispositivos y nodos en Internet y para identificar posibles problemas de latencia o congestión en la red.Es una herramienta utilizada para rastrear la ruta que sigue un paquete de datos desde una fuente hasta un destino en una red. También ayuda a identificar los nodos intermedios por los que pasa el tráfico y a diagnosticar problemas de conectividad

```
C:\Users\Bhishu>tracert 8.8.8.8

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

  1     3 ms     1 ms     1 ms  192.168.101.1
  2     4 ms     2 ms     3 ms  103.41.174.145
  3     5 ms     2 ms     2 ms  103.41.174.140
  4     5 ms     2 ms     3 ms  103.10.28.34
  5     3 ms     3 ms     3 ms  ae0-bg2.vianet.com.np [110.44.112.66]
  6     8 ms     6 ms     7 ms  125.19.67.33
  7    48 ms    39 ms    44 ms  116.119.106.142
  8    47 ms    46 ms    45 ms  142.250.169.206
  9   270 ms    70 ms    70 ms  142.250.209.73
 10    54 ms    54 ms    53 ms  142.251.55.75
 11    53 ms    53 ms    54 ms  dns.google [8.8.8.8]
```


THANK YOU