



JU

conceptos de vulnerabilidades



Analisis de Vulnerabilidades

UNIVERSIDAD AUTONOMA DE CHIAPAS

Jesus Salvador Hernandez Zarate 7° M

26 DE ENERO DE 2024 TUXTLA GUTIERREZ
CHIAPAS

Herramientas de Vulnerabilidades:

IV

✓ Nmap

“Network Mapper” es una herramienta open source de línea de comandos de linux que se utiliza para escanear direcciones IP y puertos de red para detectar aplicaciones instaladas. Nmap permite a los administradores de red encontrar qué dispositivos se están ejecutando en su red, descubrir puertos y servicios abiertos y detectar vulnerabilidades.

✓ Joomscan

Es una herramienta de escaneo de vulnerabilidades de código abierto, que está escrita en en perl. Cuando un sitio web está siendo creado los desarrolladores, conscientes o no, hacen algunos errores en el código. Un hacker puede tomar ventaja de las vulnerabilidades y acceder a la información del website. Joomscan es una herramienta.

✓ WPscan

Es un software open source para Kali Linux, diseñado para escanear vulnerabilidades y fallos en un sitio web de WordPress. WPScan es una poderosa herramienta con la capacidad de brindar información a detalle sobre una página web. Con ella es posible auditar sistemas, verificar su estado y corregir fallos.



Herramientas de Vulnerabilidades:

IV

✓ Nessus Essentials

Es un escáner de vulnerabilidades que permite escanear la red doméstica personal a alta velocidad, evaluaciones a profundidad o buscar vulnerabilidades de forma automatizada. Está enfocado a analizar las redes informáticas. Es capaz de detectar puertos abiertos, versiones de los servicios y las vulnerabilidades de estos, así como indicarlas.

Vega



Diremos que es un escáner y plataforma de código abierto de pruebas de seguridad para páginas web con el propósito de testear la seguridad de dichas aplicaciones. Vega es capaz de encontrar y validar inyecciones SQL, Cross-Site Scripting, información sensible que fue revelada inadvertidamente, entre otras vulnerabilidades. Está escrito en Java, cuenta GUI y se ejecuta en sistemas operativos Linux, OS X y Windows.





JU



Inteligencia Miscelanea



Genera una rutina.

Lo definimos como una técnica de manipulación que se aprovecha del fallo humano para recabar información privada o acceder a sistemas u objetos de valor. Estas técnicas suelen hacer que los usuarios desprevenidos expongan datos, propaguen malware u otorguen acceso a sistemas restringidos. Esta técnica se basa en cómo actúan y piensan las personas.



Gobuster.

Es una herramienta que permite la identificación de contenido web como directorios o ficheros que puedan estar accesibles u ocultos en una página web. Estilo lo realiza por medio de solicitudes http con un diccionario o por fuerza bruta, y detectará la existencia de las mismas en función del código respuesta obtenido. A resumidas cuentas, Gobuster es capaz de realizar.



Dumpster Diving

Es una técnica usada para recabar información que podría conllevar un ataque o obtener acceso a una computadora de una red desde los ítems eliminados. Esta técnica no está limitada a la búsqueda de información simple como códigos de acceso o contraseñas escritas en notas. Información aparentemente inocente como la lista del teléfono, calendarios o cuadros de información puede ayudar al atacante a usar técnicas de ingeniería social para obtener acceso a la red.

Inteligencia Activa

Análisis Traceroute

Es una herramienta inteligente de línea de comandos para trazar el path de un paquete de IP que cruza una o varias redes. Desarrollado originalmente para plataformas UNIX, ahora también está incluido en la mayoría de sistemas operativos, con la implementación de Windows conocida como “tracert”.

Fingerprinting.

Es un tipo de recolección de datos que requiere de la interacción en el sistema analizado. Por ende, el fingerprinting puede dejar un rastro sobre las direcciones IP desde las que se realiza el análisis. Por medio del fingerprinting se puede indagar para obtener información sobre direcciones IP, navegadores web, sistemas operativos, proveedores de servicios, entre otros.

Zenmap

Es la interfaz gráfica oficial de Nmap. Es una aplicación multiplataforma de código abierto que pretende facilitar el uso de Nmap para principiantes, que a su vez provee características avanzadas para los usuarios más experimentados. Los scanners usados con regularidad pueden ser guardados en perfiles para volver sus ejecuciones repetidas más sencillas. El creador de comandos permite la creación interactiva de líneas de comando NMap. Los resultados de los escáneres pueden ser observados posteriormente.

Inteligencia Activa

JU

◆ Analisis de dispositivos y puertos con nmap

El análisis de puertos es el acto de testear varios puertos remotamente para determinar en qué estado se encuentran. El estado más llamativo de un puerto es el abierto, el cual nos indica que una aplicación está siendo escuchada y acepta conexiones en el puerto. En el análisis de puertos nmap los divide en seis estados., abierto, cerrado, con filtro, abierto con filtro, sin filtro y cerrado sin filtro. Por otro lado en el análisis o descubrimiento de dispositivos los usuarios pueden saltarse el descubrimiento completamente con un escaneo de lista (-sl) o al deshabilitar el descubrimiento de host (-pn), o involucrar a la red con combinaciones arbitrarias de multi puerto TXP SYN/ACK, UDP, SCTP Sondas INIT e ICMP.

◆ Stealth Scan

- Es la opción de escaneo por default. Esta puede realizarse rápidamente, escanea miles de puertos por segundo en una red raída no obstaculizada por firewalls intrusivos. SYN scan es relativamente discreto y sigiloso, ya que este nunca completa conexiones TCP. Este también funciona contra cualquier otra pila TCP compatible que, dependiendo de la idiosincrasia de plataformas específicas como Nmap FIN/NULL/XMAS y los escaneos inactivos, también lo hace. Además permite una diferenciación confiable entre estados de puertos.

◆ Full TXP Scan

Es otra opción de escaneo cuando el Stealth scan no es posible. En lugar de recibir paquetes en raw como la mayoría de otros tipos de escaneo, Nmap pregunta al sistema operativo subyacente para establecer una conexión con la máquina y puerto objetivo al generar problemas en la llamada de conexión del sistema. Este es el mismo sistema que llama a los navegadores web, clientes p2p y la mayoría de aplicaciones habilitadas para la red que se utilizan para establecer una conexión.

Parámetros y opciones de escaneo con nmap

◆ Especificación de puertos y orden de análisis

-F: Analizar solo los puertos listados en el archivo nmap-services

◆ Detección de sistemas operativos

--osscan-limit: Limita la detección de SO a objetivos prometedores

◆ Detección de servicios

--version-light: Limita a las sondas más probables

◆ Temporizado y rendimiento

--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <msecs> Indica el tiempo de ida y vuelta de la sonda.

◆ Especificación de objetivo

--exclude <sist1[,sist2][,sist3],...> Excluye ciertos sistemas o redes

◆ Descubrimiento de Hosts

-PS/PA/PU [lista de puertos]: Análisis TCP SYN, ACK o UDP de los puertos indicados.

◆ Técnicas de análisis

-sN/sF/sX: Análisis TCP Null, FIN, Xmas

◆ Evasión y falsificación de cortafuegos

-S <Dirección_IP> Falsificar la dirección IP origen

◆ Salida

-d[nivel]: Fijar o incrementar el nivel de depuración