UNACH | Universidad Autónoma de Chiapas

FACULTAD DE CONTADURIÁ Y ADMINISTRACIÓN CAMPUS I

Licenciatura en Ingeniería en desarrollo y tecnologías de software

ANALISIS DE VULNERABILIDADES

ACT. 1.1 Investigar los conceptos de vulnerabilidades

CATEDRÁTICO: Dr. Luis Gutiérrez Alfaro

ESTUDIANTE:

Gutiérrez Hernández Cristian - A200256

Semestre: 7° Grupo: “M”

Tuxtla Gutiérrez, Chiapas.

Domingo, 21 de agosto de 2022

Herramientas de vulnerabilidades:

- nmap
- Joomscan
- Wpscan
- Nessus Essentials
- Vega

Inteligencia Misceláneo.

- Gobuster:
- Dumpster Diving
- Ingeniería Social

Inteligencia Activa:

- Análisis de dispositivos y puertos con Nmap
- Parametros opciones de escaneo de nmap
- Full TCP scan
- Stelth Scan
- Fingerprintig
- Zenmap
- Análisis traceroute

Herramientas de vulnerabilidades

Un escáner de vulnerabilidades es un software que evalúa tu red y sistemas en busca de vulnerabilidades e informa los riesgos asociados con ellos.

Los escáneres de vulnerabilidades permiten a las organizaciones cumplir con los estándares de seguridad en evolución al monitorizar y detectar vulnerabilidades y corregirlas para mantener la seguridad de la red. Además, el escaneo de vulnerabilidades es también uno de los primeros pasos en las pruebas de penetración.

Existen diferentes tipos de análisis de vulnerabilidades:

- Análisis de vulnerabilidades externas
- Análisis de vulnerabilidades internas
- Análisis de vulnerabilidades no autenticados
- Análisis de vulnerabilidades autenticados
- Análisis de vulnerabilidades completos
- Análisis de vulnerabilidades limitado

Los escáneres de vulnerabilidades funcionan mediante un mecanismo de tres pasos que converge hacia el objetivo de la organización de identificar las vulnerabilidades y el riesgo que pueden representar.

1. **Detección**: la herramienta de evaluación de vulnerabilidades es realizar una prueba de vulnerabilidad para detectar e identificar posibles superficies de ataque. Te permite determinar las brechas de seguridad en tu red y llenarlas antes de que los atacantes puedan penetrarla.

2. **Clasificación**: en el segundo paso, las vulnerabilidades se clasifican para ayudar a los administradores a priorizar su curso de acción. Estas vulnerabilidades pueden incluir actualizaciones faltantes, errores de secuencia de comandos o anomalías.

3. **Remediación**: generalmente, los escáneres de vulnerabilidades no proporcionan una forma de abordar las vulnerabilidades identificadas automáticamente. Se centran más en supervisar y proporcionar detalles para que los administradores den un paso más. Pero algunos escáneres manejan errores de configuración, lo que ahorra horas de trabajo al administrador al llegar a varios dispositivos simultáneamente.

- Nmap

Es la abreviatura de Network Mapper. Es una herramienta de línea de comandos Linux de código abierto que se utiliza para escanear direcciones IP y puertos en una red y para detectar aplicaciones instaladas.

Permite a los administradores de red encontrar qué dispositivos se ejecutan en su red, descubrir puertos y servicios abiertos y detectar vulnerabilidades.

nos ayuda a trazar rápidamente una red sin comandos o configuraciones sofisticadas. También admite comandos simples (por ejemplo, para verificar si un host está activo) y secuencias de comandos complejas a través del motor de secuencias de comandos Nmap.

Otras características:

- Capacidad para reconocer rápidamente todos los dispositivos, incluidos servidores, enrutadores, conmutadores, dispositivos móviles, etc. en redes únicas o múltiples.

- Ayuda a identificar servicios que se ejecutan en un sistema que incluye servidores web, servidores DNS y otras aplicaciones comunes. Nmap también puede detectar versiones de aplicaciones con una precisión razonable para ayudar a detectar vulnerabilidades existentes.

- Puede encontrar información sobre el sistema operativo que se ejecuta en dispositivos. Puede proporcionar información detallada como las versiones del sistema operativo, lo que facilita la planificación de enfoques adicionales durante las pruebas de penetración.
- Durante la auditoría de seguridad y el escaneo de vulnerabilidad, se puede usar Nmap para atacar sistemas usando scripts existentes del motor de script de Nmap.

- Tiene una interfaz gráfica de usuario llamada Zenmap. Le ayuda a desarrollar asignaciones visuales de una red para una mejor usabilidad e informes.

- 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.

- WPScan

WPScan es un software de código abierto para Kali Linux, diseñado para escanear vulnerabilidades y fallos en un sitio web de WordPress. WPScan es una herramienta muy poderosa y capaz de darte información detallada sobre una página web. Con ella, puedes auditar sistemas, verificar su estado y corregir cada fallo que encuentres antes de que lo aproveche un delincuente.

El programa te enumerará una lista con los nombres de los usuarios, los plugins y los temas vulnerables del sitio web. Con esta información podrías hacer un ataque de fuerza bruta para probar distintas contraseñas con los nombres de usuario, pues, en ocasiones, las contraseñas pueden ser muy inseguras y hallarse de este modo.

- Nessus Essentials

Nessus es un escáner de vulnerabilidades de red, es decir, una herramienta de seguridad que busca debilidades en los sistemas informáticos y redes. Fue creado por Renaud Deraison en 1998 y es una de las soluciones de seguridad más populares y utilizadas en todo el mundo.

Nessus se utiliza para identificar y analizar vulnerabilidades de seguridad en sistemas operativos, aplicaciones y dispositivos de red. Es capaz de escanear todo tipo de dispositivos, desde servidores hasta dispositivos móviles, routers y firewalls.

- Vega

Vega es un programa dedicado a la seguridad de las páginas web, el cual es un programa que permite saber todas las vulnerabilidades que tiene un sitio web para que después tu mismo puedas corregirlas. Aunque no esté integrado nativamente en Kali Linux, es de esos programas que se integran bien con la temática de este sistema operativo, ya que es un sistema operativo dedicado a todo lo que concierne a la seguridad informática.

Vega puede ayudarle a encontrar y validar la inyección de SQL, Cross-Site Scripting (XSS), reveló inadvertidamente información sensible, y otras vulnerabilidades. Vega incluye un escáner automatizado para pruebas rápidas y un proxy de intercepción para inspection.

Inteligencia Miseláneo

- Gobuster, un escáner de registros escrito en Go Language. Gobuster puede ser una implementación Go de esas herramientas y se puede obtener en un conveniente formato de línea de comandos. El beneficio principal que Gobuster tiene sobre otros escáneres de directorios es la velocidad. Como lenguaje de programación, se entiende que Go es rápido. Sin embargo, la falta de exploración recursiva de directorios. Para los directorios, de un nivel bastante profundo, se necesitará otro escaneo, desafortunadamente.

Gobuster es una herramienta de línea de comandos utilizada en pruebas de penetración para realizar ataques de fuerza bruta o enumeración de rutas/directorios en aplicaciones web. Busca nombres de archivos y directorios mediante solicitudes HTTP.

- Dumpster Diving

En su Guía de ciberataques, Incibe y OSI definen el dumpster diving como “el proceso de buscar en nuestra basura para obtener información útil sobre nuestra persona o empresa que luego pueda utilizarse contra nosotros para otro tipo de ataques”.

Buscando en los documentos impresos que tiramos a una papelera o un contenedor, los ciberdelincuentes esperan encontrar números de tarjetas bancarias, contactos o anotaciones con credenciales. En algunos casos, incluso buscan dispositivos electrónicos que los usuarios arrojan a la basura para intentar extraer información que no haya sido borrada.

- La Ingeniería Social es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Éstas contemplan entre otras cosas: la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo), pudiendo ser o no del interés de la persona objetivo.

La Ingeniería Social se sustenta en un sencillo principio: “el usuario es el eslabón más débil”. Dado que no hay un solo sistema en el mundo que no dependa de un ser humano, la Ingeniería Social es una vulnerabilidad universal e independiente de la plataforma tecnológica.

Inteligencia Activa

- Análisis de dispositivos y puertos con Nmap.

Nmap nos permitirá obtener una gran cantidad de información sobre los equipos de nuestra red, es capaz de escanear qué hosts están levantados, e incluso comprobar si tienen algún puerto abierto, si están filtrando los puertos (tienen un firewall activado), e incluso saber qué sistema operativo está utilizando un determinado objetivo.

- Parametros opciones de escaneo de nmap

Nmap es una herramienta de exploración de red y escáner de seguridad que permite realizar diferentes tipos de escaneos, como:

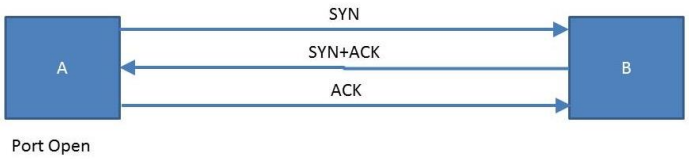
- Escaneos de ping: Detectan si los objetivos están en línea, pero no escanean los puertos. Se pueden hacer con las opciones -Pn o -PT
- Escaneos de puertos: Detectan los puertos abiertos, cerrados o filtrados en los objetivos. Se pueden hacer con las opciones -sS, -sU, -sT, entre otras.
- Escaneos de servicios: Identifican los servicios y versiones que se ejecutan en los puertos abiertos. Se pueden hacer con las opciones -sV o -A

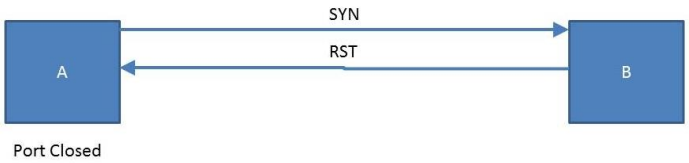
- Full TCP scan

De todos los escaneos, el escaneo abierto completo es muy fácil de visualizar y entender, ya que ya lo hemos visto. Un escaneo abierto completo establece un protocolo de enlace TCP de tres vías antes de realizar cualquier escaneo de puertos en el sistema de destino, con el objetivo de determinar su estado si están abiertos y cerrados.

Este tipo de escaneo puede determinar rápidamente si un puerto está abierto o cerrado porque establece un protocolo de enlace TCP de tres vías con el destino.

Cuando el iniciado ya no desea comunicarse con el destino, el iniciado enviará un paquete TCP FIN para que el destino sepa que desea finalizar correctamente la sesión:





Un escaneo TCP completo es un tipo de escaneo que intenta establecer una conexión TCP con cada puerto del objetivo, esperando una respuesta y cerrando la conexión tan pronto como se ha establecido. Es un método lento pero confiable para detectar los puertos abiertos. Para hacer un escaneo TCP completo con Nmap, puedes usar la opción -sT seguida de la dirección IP o el rango de red que quieres escanear. Por ejemplo:

nmap -sT 192.168.1.1

nmap -sT 192.168.1.0/24

- Stelth Scan

TCP SYN (Stealth) Scan (-sS)

El escaneo SYN es la opción de escaneo predeterminada y más popular para siempre razón. Se puede realizar rápidamente, escaneando miles de puertos por En segundo lugar, en una red rápida no obstaculizada por firewalls intrusivos. Análisis SYN es relativamente discreto y sigiloso, ya que nunca completa TCP Conexiones. También funciona contra cualquier pila TCP compatible en lugar de que depender de idiosincrasias de plataformas específicas como la de Nmap Los escaneos FIN / NULL / Xmas, Maimon y idle lo hacen. También permite claro, Diferenciación fiable entre , , y estados.openclosedfiltered

El escaneo SYN se puede solicitar pasando la opción a Nmap. Requiere privilegios de paquetes sin formato, y es el valor predeterminado Escaneo TCP cuando están disponibles. Entonces, cuando se ejecuta Nmap como root o Administrador, generalmente se omite. Este valor predeterminado El comportamiento del análisis SYN se muestra en el ejemplo 5.1, que busca un puerto en cada uno de los tres estados principales.-sS-sS

Ejemplo 5.1. Un escaneo SYN que muestra tres estados de puerto

```
krad# nmap -p22,113,139 scanme.nmap.org

Starting Nmap ( https://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
PORT    STATE    SERVICE
22/tcp  open     ssh
113/tcp closed   auth
139/tcp filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

- Fingerprintig

Dentro de la ciberseguridad, Footprinting es la primera forma para que los evaluadores de penetración puedan recoger información sobre hardware o red.

Se trata de un procedimiento de exploración con el que podemos conocer a nuestro enemigo. Para que ese procedimiento de penetración sea completo, debemos acumular toda la información posible. La huella se puede hacer de forma activa o pasiva.

Realizar una evaluación de la web de una empresa con su autorización es un ejemplo de la huella pasiva e intentar acceder a información sensible utilizando la ingeniería social es un ejemplo de la recopilación activa de información.

Hay dos tipos de footprinting como se detalla a continuación.

- Huella activa: significa realizar una huella al ponerse en contacto directo con la máquina de destino.
- Huella pasiva: la impresión pasiva del pie significa recopilar información de un sistema ubicado a una distancia remota del atacante.

A través del Footprinting podemos conocer:

- Sistema operativo de la máquina de destino.
- Cortafuegos
- Dirección IP
- Mapa de red
- Configuraciones de seguridad de la máquina de destino
- Identificación de correo electrónico, contraseña
- Configuraciones de servidor
- URLs
- VPN

- Zenmap

Zenmap es la GUI oficial de Nmap Security Scanner. Es una multiplataforma (Linux, Windows, Mac OS X, BSD, etc.) Aplicación gratuita y de código abierto que tiene como objetivo hacer que Nmap sea fácil de usar para los principiantes mientras proporciona funciones avanzadas para usuarios experimentados de Nmap. Exploraciones de uso frecuente se pueden guardar como perfiles para que sean fáciles de ejecutar repetidamente. Un El creador de comandos permite la creación interactiva del comando Nmap lineas. Los resultados del análisis se pueden guardar y ver más tarde. Resultados de análisis guardados se pueden comparar entre sí para ver en qué se diferencian. Los resultados de los escaneos recientes se almacenan en una base de datos en la que se pueden realizar búsquedas.

- Traceroute

Traceroute o tracert es un comando que ejecuta funciones de diagnóstico de red en sistemas operativos informáticos.

En general, ambos comandos funcionan igual. La diferencia radica en el sistema operativo: mientras que Linux y macOS utilizan el comando traceroute, Windows utiliza tracert.

El comando traceroute envía tres paquetes de sondeo a través de la red y supervisa cómo llegan al destino.

Un paquete de sondeo pasará por varios dispositivos, como routers y conmutadores, para llegar a la dirección IP de destino en un proceso denominado salto (hop). El comando traceroute mapea cada salto dentro de la ruta junto con su tiempo de ida y vuelta (RTT).

El registro también puede incluir otros detalles, como el nombre del dispositivo y la dirección IP de cada salto.

El comando traceroute tiene una funcionalidad similar al comando ping. Sin embargo, a diferencia del comando ping, traceroute permite una resolución de problemas más fácil en una red grande con más dispositivos como routers intermedios y puentes.

Referencias

- Analiza la seguridad de tu página web con Vega. (n.d.). ReDIGIT Blog. Retrieved August 14, 2023, from https://blog.redigit.es/analiza-la-seguridad-de-tu-pagina-web-con-vega/

- FunInformatique, P. P. (2021, May 28). ¿Cómo instalar Kali Linux en Windows? (Para principiantes). FunInformatique. https://www.funinformatique.com/es/hacer-que-kali-linux-funcione-en-windows-con-vmware/

- Los 5 principales escáneres de vulnerabilidades para patrullar las redes. (2021, April 29). Ciberseguridad. https://ciberseguridad.com/herramientas/software/escaneres-vulnerabilidades/

- ¿Qué es WPScan? (2022, June 10). KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-wpscan-ciberseguridad/

- ¿Qués es NMAP? (2023, January 16). Genuino Cloud | Correo electrónico corporativo; GenuinoCloud. https://genuinocloud.com/blog/que-es-nmap/

- Sepulveda, M. (2023, February 23). Que es Nessus y como utilizarlo. El Club de la Ciberseguridad. https://ciberseguridad.club/que-es-nessus-y-como-utilizarlo/

- VEGA EN KALI LINUX. (2018, May 4). Creadpag.com. https://www.creadpag.com/2018/05/vega-en-kali-linux.html

- Bajrami, V. (2020, March 31). Running a quick NMAP scan to inventory my network. Enable Sysadmin; Red Hat, Inc. https://www.redhat.com/sysadmin/quick-nmap-inventory

- BlackeyeB. (2023, April 23). Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos. freecodecamp.org. https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/

- De Luz, S. (2021, January 18). Realiza escaneos de puertos con Nmap a cualquier servidor o sistema. RedesZone. https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/

- Greyrat, R. (n.d.). Gobuster: herramientas de prueba de penetración en Kali Tools. Barcelonageeks.com. Retrieved August 14, 2023, from https://barcelonageeks.com/gobuster-herramientas-de-prueba-de-penetracion-en-kali-tools/

- How to scan an entire network using Nmap? (n.d.). Ask Ubuntu. Retrieved August 14, 2023, from https://askubuntu.com/questions/377787/how-to-scan-an-entire-network-using-nmap

- Layne, J. (2023, April 30). Tipos de escaneos Nmap 2023. Ablison. https://ablison.com/es/tipos-de-escaneos-nmap/

- nmap scan (part of UDP but full range TCP). (n.d.). Stack Overflow. Retrieved August 14, 2023, from https://stackoverflow.com/questions/41020016/nmap-scan-part-of-udp-but-full-range-tcp

- Valades, B. (2021, August 24). Dumpster diving: ¿qué es y cómo proteger nuestra información? Se urilatam. https://www.segurilatam.com/actualidad/ingenieria-social-dumpster-diving-que-es-y-como-proteger-nuestra-informacion_20210824.html

- Full Open/TCP connect scans. Retrieved August 15, 2023, from https://subscription.packtpub.com/book/security/9781788995177/4/ch04lvl1sec37/full-opentcp-connect-scans

- Footprinting y Fingerprinting. (2019, December 9). Ciberseguridad. https://ciberseguridad.com/amenzas/footprinting-fingerprinting/

- Infante, D. C. H. (2023, May 31). Comando Traceroute: Cómo usarlo e interpretarlo. Tutoriales Hostinger. https://www.hostinger.mx/tutoriales/comando-traceroute

- Sistemas, S. (2016, November 21). Comando tracert para diagnosticar conexiones de red (Traceroute). Solvetic. https://www.solvetic.com/tutoriales/article/3281-comando-tracert-conexiones-de-red-windows-traceroute/

- TCP SYN (Stealth) Scan (-sS). (n.d.). Nmap.org. Retrieved August 15, 2023, from https://nmap.org/book/synscan.html

- Valades, B. (2021, August 24). Dumpster diving: ¿qué es y cómo proteger nuestra información? Segurilatam. https://www.segurilatam.com/actualidad/ingenieria-social-dumpster-diving-que-es-y-como-proteger-nuestra-informacion_20210824.html

- Zenmap - Official cross-platform Nmap Security Scanner GUI. (n.d.). Nmap.org. Retrieved August 15, 2023, from https://nmap.org/zenmap/