UNIVERSIDAD AUTÓNOMA DE CHIAPAS

SUBCOMPETENCIA 1

7° “M”

ANALISIS DE VULNERABILIDADES

ACT 1.1: INVESTIGAR LOS CONCEPTOS DE VULNERABILIDADES

ESTUDIANTE: JESUS SALVADOR HERNANDEZ ZARATE

PROFESOR: DR. LUIS GUTIERREZ ALFARO

Herramientas de Vulnerabilidades:

- 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.

  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: 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.

- 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.

Inteligencia Miscelánea.

- 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.

- Ingeniería Social. 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.

Inteligencia Activa.

- Análisis 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 maps 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, también llamado ping scan, va más allá de una simple solicitud eco ICMP de paquetes asociados con la ubicua herramienta ping. 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.

- Parámetros opciones de escaneo con nmap. Existen muchos parámetros a los que podemos acudir a la hiora de realizar un análisis con Nmap. Estos pueden variar dependiendo de la función que buscamos realizar. Algunas son:

    - 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: Análisi TCP Null, FIN, Xmas
    - Especificación de puertos y orden de análisis
        - -F: Analizar solos 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 <msegs> Indica el tiempo de ida y vuelta de la sonda.
    - Evasión y falsificación de cortafuegos.
        - -S <Dirección_IP> Falsificar la dirección IP origen
    - Salida
        - -d[nivel]: Fijar o incrementar el nivel de depuración
- Full TCP 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.

- 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.

- 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.

- 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”.

Referencias bibliográficas.

BlackeyeB. (2023, 27 abril). *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/

Jaouari, E. (2023, 2 diciembre). *Joomscan: Detectar y proteger vulnerabilidades en un sitio Joomla | FunInformatique*. FunInformatique. https://www.funinformatique.com/es/joomscan-c%C3%B3mo-detectar-fallas-en-un-sitio-joomla/

KeepCoding, R. (2023b, enero 23). ¿Qué es WPSCAN? | KeepCoding Bootcamps. *KeepCoding Bootcamps*. https://keepcoding.io/blog/que-es-wpscan-ciberseguridad/

Vega Vulnerability Scanner. (s. f.). https://subgraph.com/vega/

Bytemind. (2022, 11 enero). *Enumeración por fuerza bruta con gobuster*. Byte Mind. https://byte-mind.net/enumeracion-por-fuerza-bruta-con-gobuster/

Wright, G. (2021, 6 abril). *Dumpster Diving*. Security. https://www.techtarget.com/searchsecurity/definition/dumpster-diving

¿Qué es la ingeniería social? (2024, 18 enero). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

Chapter 4. Port Scanning Overview | NMAP Network Scanning. (s. f.). https://nmap.org/book/port-scanning.html#port-scanning-what-is-it

Resumen de opciones | Guía de referencia de NMAP (Página de manual). (s. f.). https://nmap.org/man/es/man-briefoptions.html

TCP Connect Scan (-ST) | NMAP Network Scanning. (s. f.). https://nmap.org/book/scan-methods-connect-scan.html

OS Detection | NMAP Network Scanning. (s. f.). https://nmap.org/book/man-os-detection.html

Keary, T., & Keary, T. (2023, 27 abril). *The Definitive Guide to NMAP: Scanning Basics Tutorial*. Comparitech. https://www.comparitech.com/net-admin/the-definitive-guide-to-nmap/

TCP SYN (Stealth) Scan (-SS) | NMAP Network Scanning. (s. f.). https://nmap.org/book/synscan.html

KeepCoding, R. (2023d, octubre 5). ¿Qué es ZenMap? | KeepCoding Bootcamps. *KeepCoding Bootcamps*. https://keepcoding.io/blog/que-es-zenmap-ciberseguridad/

ZenMap - Official Cross-platform NMAP Security Scanner GUI. (s. f.). https://nmap.org/zenmap/

Grimmick, R. (2023, 6 abril). What is Traceroute? How It Works and How to Read Results. *Varonis*. https://www.varonis.com/blog/what-is-traceroute

Host Discovery | NMAP Network Scanning. (s. f.). https://nmap.org/book/man-host-discovery.html

KeepCoding, R. (2023d, mayo 3). ¿Qué es fingerprinting? | KeepCoding Bootcamps. *KeepCoding Bootcamps*. https://keepcoding.io/blog/que-es-fingerprinting-ciberseguridad/

Daniel, F. D. C. (s. f.). *Nessus Essentials*. Platzi. https://platzi.com/clases/2984-inteligencia-activa/49345-nessus-essentials/#:~:text=Esc%C3%A1ner%20de%20vulnerabilidades%20Nessus%20Essentials,buscar%20vulnerabilidades%20de%20forma%20automatizada.