Determinación de las herramientas de monitorización para detectar vulnerabilidades (Hacking ético)

Elementos esenciales del hacking ético

Más información

- https://www.jesusninoc.com/01/10/curso-de-hacking-con-powershell-contenido/

Diferencias entre hacking, hacking ético, tests de penetración y hacktivismo

Hacking

Un hacker es alguien que descubre las vulnerabilidades de una computadora o un sistema de comunicación e información, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas.□□

Hacking ético

Hacking Ético permite identificar vulnerabilidades en los sistemas de información y comunicaciones aplicando contramedidas para subsanarlas.

Tests de penetración

Los test de penetración sirven para determinar el nivel de seguridad en un equipo, red, aplicaciones, etc.

Métodos de análisis de ejemplo para un test de penetración:

- Network Mapping
- Information Gathering
- CMS Identification
- IDS/IPS Detection
- Open Source Analysis
- Web Crawlers
- Vulnerability Assessent and Exploitation
- Maintaining Access

Network Mapping

El mapeo de redes es el estudio de la conectividad física de las redes, por ejemplo en Internet. El mapeo de red descubre los dispositivos en la red y su conectividad.

Ejemplos de herramientas:

- Nmap
- Netifera

Ejercicios

Detectar información

- https://www.jesusninoc.com/09/04/detectar-el-sistema-ope

rativo-que-tienen-las-direcciones-ip-de-un-rango-utilizando-nmap/

- https://www.jesusninoc.com/09/05/detectar-los-puertos-abiertos-que-tienen-las-direcciones-ip-de-un-rango-utilizando-nmap/
- https://www.jesusninoc.com/09/06/detectar-los-servicios-que-estan-activos-en-las-direcciones-ip-de-un-rango-utilizando-nmap/
- https://www.jesusninoc.com/08/01/detectar-smb-que-estan-activos-en-las-direcciones-ip-de-un-rango-utilizando-nmap/

Análisis de direcciones IP

- Comprobar la conexión a las direcciones IP que están en un fichero
- Mostrar las direcciones IP de un rango variando el segundo, tercer y cuarto octeto
- Mostrar las direcciones IP de un variando el primer, segundo, tercer y cuarto octeto
- Realizar ping a las direcciones IP de un rango
- Realizar ping a las direcciones IP de un rango variando el tercer y cuarto octeto
- Realizar ping a las direcciones IP de un rango y comprobar si están o no activas
- Obtener la dirección MAC de cada IP de un rango

Más información

- https://www.jesusninoc.com/02/11/achilles/
- https://www.jesusninoc.com/02/02/angry-ip/

Information Gathering

«Information Gathering» (también llamada «footprinting») es

una táctica habitual llevada a cabo por los ciberdelincuentes como paso previo al ataque a una entidad. Consiste en recabar la máxima cantidad de información posible de fuentes abiertas (buscadores, redes sociales, sitios web públicos con contenido filtrado o recopilado…). Dicha información permite al atacante elaborar un «perfil» de su objetivo, aumentando así las probabilidades de éxito. De hecho, un atacante empleará el 90% de su tiempo en detallar un buen perfil de su objetivo y un 10% en lanzar el ataque.

Ejemplos de herramientas:

- TheHarvester
- Maltego

CMS Identification

CMS Identification se utiliza para qué CMS está usando un sitio web.

Ejemplos de herramientas:

- BlindElephant
- CMS-Explorer
- WhatWeb
- CMSeek

Ejercicios

Detección de CMS con CMSeek desde Ubuntu y mostrar los resultados en PowerShell

- https://www.jesusninoc.com/06/20/deteccion-de-cms-con-cmseek-desde-ubuntu-y-mostrar-los-resultados-en-powershell/

IDS/IPS Detection

IDS (Intrusion Detection System) o sistema de detección de intrusiones: es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red, es decir, son sistemas que monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas.

IPS (Intrusion Prevention System) o sistema de prevención de intrusiones: es un software que se utiliza para proteger a los sistemas de ataques e intrusiones. Su actuación es preventiva.

Ejemplos de herramientas:

- Snort

Open Source Analysis

Inteligencia de fuentes abierta son datos recogidos de fuentes disponibles de forma pública para ser utilizados en un contexto de inteligencia. En la comunidad de inteligencia, el término «abiertas» se refiere a fuentes disponibles públicamente ya sean de pago o gratis.

Ejemplos de herramientas:

- GHDB

Ejercicios

Obtener información de los resultados sobre las búsquedas en Google Hacking Database

- https://www.jesusninoc.com/04/01/obtener-informacion-de-los-resultados-sobre-las-busquedas-en-google-hacking-database/
- https://www.jesusninoc.com/12/06/obtener-el-numero-de-resultados-sobre-busquedas-en-google-hacking-database-ghdb/

Web Crawlers

Un rastreador web, indexador web, indizador web o araña web es una programa informático que inspecciona las páginas del World Wide Web de forma metódica y automatizada.

Ejemplos de herramientas:

- WebShag
- DirBuster

Ejercicios

Recorrer enlaces

- https://www.jesusninoc.com/12/03/recorrer-el-primer-nivel-de-un-sitio-web-y-obtener-informacion-de-todos-los-enlaces-del-sitio/
- https://www.jesusninoc.com/11/14/recorrer-el-segundo-nivel-de-un-sitio-web-y-obtener-informacion-de-todos-los-enlaces/
- https://www.jesusninoc.com/12/05/recorrer-el-segundo-nivel-de-un-sitio-web-y-obtener-todos-los-enlaces-del-sitio/
- https://www.jesusninoc.com/01/13/recorrer-el-segundo-nivel-de-un-sitio-web-obtener-informacion-de-todos-los-enlaces-del-sitio-y-anadir-la-informacion-creando-una-clase-a-un-array/
- https://www.jesusninoc.com/12/06/obtener-los-enlaces-de-una-pagina-web-buscar-si-alguno-contiene-una-cadena-en-concreto-despues-recorrer-ese-enlace-y-detectar-si-se-encuentra-una-palabra-dentro-del-contenido-del-enlace-recorrido/

Recorrer sitios del fichero robots

- https://www.jesusninoc.com/10/19/recorrer-los-enlaces-que-estan-denegados-en-el-fichero-robots-txt/

Vulnerability Assessment and Exploitation

Una evaluación de vulnerabilidad es una revisión sistemática de las debilidades de seguridad en un sistema de información. Evalúa si el sistema es susceptible a vulnerabilidades conocidas, asigna niveles de gravedad a esas vulnerabilidades y recomienda soluciones o mitigación, si es necesario.

Ejemplos de herramientas:

- SqlMap
- Sqlninja
- Absinthe
- Fimap
- Shodan
- W3af
- Nikto

Más información

- https://www.jesusninoc.com/12/04/sqlmap/
- https://www.jesusninoc.com/12/02/sqlninja/
- https://www.jesusninoc.com/12/09/absinthe/
- https://www.jesusninoc.com/04/02/filtros-shodan/
- https://www.jesusninoc.com/01/13/nikto/

Maintaining Access

Después de comprometer con éxito un host, si las reglas de participación lo permiten, con frecuencia es una buena idea asegurarse de que podrá mantener su acceso para un examen más detallado o para penetrar en la red de destino. Esto también garantiza que podrá volver a conectarse con su víctima si está utilizando un exploit único o si bloquea un servicio en el objetivo. En situaciones como estas, es posible que no pueda recuperar el acceso nuevamente hasta que se reinicie el objetivo.

Ejemplos de herramientas:

- Weevely
- Msfvenom

Más información

- https://www.jesusninoc.com/10/09/windows-post-exploitation-cmdlets-execution-powershell/

Hacktivismo

Hacktivismo (acrónimo de hacker y activismo también conocido como ciberactivismo) se entiende normalmente «la utilización no-violenta de herramientas digitales persiguiendo fines políticos; estas herramientas incluyen desfiguraciones de webs, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales, sabotajes virtuales y desarrollo de software».

Recolección de permisos y autorizaciones previos a un test de intrusión

Fundamental obtener los permisos antes de realizar un test de intrusión.

Fases del hacking

El hacking ético actúa a partir de un esquema que se divide en cinco fases:

- Firma de un acuerdo.
- Investigación de los sistemas.
- Elaboración de plan de ataque.
- Descubrimiento de vías de acceso y vulnerabilidades.
- Prueba de la teoría y de la resistencia de la empresa en su seguridad.

Auditorías de caja negra y de caja blanca

Existen varios procedimientos para las auditorías:

- Caja negra: procedimiento para comprobar requisitos funcionales desde el exterior del programa.
- Caja blanca: tipo de pruebas de software que se realiza sobre las funciones internas de un programa.
- Enfoque aleatorio: elaboración de casos de prueba a partir de modelos obtenidos estadísticamente.

Ejemplos

- https://www.jesusninoc.com/03/14/ejercicios-de-powershel

l-registrar-una-accion-cuando-se-cree-un-usuario-register-wmievent/

Documentación de vulnerabilidades

Cada fallo encontrado hay que documentarlo para poner solución a dicho problema mediante un parche (actualización o procedimiento similar).

Clasificación de herramientas de seguridad y hacking

Algunas herramientas ya están vistas en el apartado anterior cuando se trataba los «Tests de penetración».

Hay muchas herramientas relacionadas con los siguientes campos de la seguridad y el hacking:

- Ofuscación
- Fuerza bruta
- Análisis forense

Más información

- https://www.jesusninoc.com/03/11/thumbnail-database-viewer/
- https://www.jesusninoc.com/01/18/malzilla-malware-hunting-tool/
- https://www.jesusninoc.com/03/11/thc-hydra/

ClearNet, Deep Web, Dark Web, Darknets. Conocimiento, diferencias y herramientas de acceso: Tor. ZeroNet, FreeNet

ClearNet

Clearnet es un término que normalmente se refiere a Internet de acceso público. A veces, «clearnet» se utiliza como sinónimo de «web superficial», excluyendo tanto la darknet como la deep web.

Deep Web

Consiste en la parte de Internet profunda, internet invisible o internet oculta es el contenido de internet que no está indexado por los motores de búsqueda convencionales, debido a diversos factores. El término se atribuye al informático Mike Bergman. Es el opuesto al Internet superficial.

Darknets

El concepto de red oscura, también conocido por su nombre original en inglés darknet, ha ido evolucionando con el tiempo desde su definición original, dada por unos investigadores de Microsoft. A la fecha de este artículo, el término darknet no tiene una definición universalmente aceptada.

Dark Web

La dark web o internet oscura es el contenido de la World Wide Web que existe en darknets, redes que se superponen a la internet pública y requieren de software específico y configuraciones o autorización para acceder.

ZeroNet

ZeroNet es una red de internet descentralizada, donde los usuarios se conectan a través del protocolo p2p.

FreeNet

Freenet es una red de distribución de información descentralizada y resistente a la censura diseñada originalmente por Ian Clarke.

Tor

Tor es un proyecto cuyo objetivo principal es el desarrollo de una red de comunicaciones distribuida de baja latencia y superpuesta sobre internet, en la que el encaminamiento de los mensajes intercambiados.

Ejercicio

Crear un dominio .onion utilizando Tor

- https://www.jesusninoc.com/02/01/crear-un-dominio-onion/
- https://www.jesusninoc.com/02/20/crear-un-dominio-en-la-deep-web-de-forma-facil-y-sencilla/
