Laboratorio
FUNDAMENTOS DE CIBERSEGURIDAD
Profesor: Juan Ignacio Iturbe A.

Laboratorio 1. Reconocimiento

Introducción

El reconocimiento no es más que los pasos tomados para recopilar evidencia e información sobre los objetivos que desea atacar. Puede ser de naturaleza pasiva o activa. El reconocimiento pasivo implica la recopilación de información sobre su objetivo sin su conocimiento, mientras que el reconocimiento activo utiliza herramientas y técnicas que pueden o no descubrirse, pero pone sus actividades como hacker en mayor riesgo de descubrimiento. Otra forma de verlo es desde una perspectiva de red: activa es aquella que pone a propósito paquetes, o comunicaciones específicas, en una conexión a su objetivo, mientras que pasivo no.

Por ejemplo, imagine que su prueba de penetración, también conocida como pentest, acaba de comenzar y usted no sabe nada acerca de la organización objetivo. Pasivamente, puede simplemente observar el exterior del edificio durante un par de días para conocer los hábitos de los empleados y ver qué medidas de seguridad física se aplican. Activamente, puede simplemente caminar hasta la entrada o la caseta de vigilancia e intentar abrir la puerta (o la puerta). En cualquier caso, está aprendiendo información valiosa, pero con el reconocimiento pasivo no está realizando ninguna acción para indicar a los demás que usted está viendo. Algunos ejemplos de acciones que podrían tomarse durante esta fase son la ingeniería social, el buceo en basureros y el sniffing de redes.[1]

Ejemplo: https://www.youtube.com/watch?v=QMG_GeI90rI

Objetivo general

Descubrir y evaluar la arquitectura tecnológica interna de una organización a partir de información recolectada de fuentes públicas.

Instrucciones generales

- Elija una página web objetivo.
- Se requieren pantallazos que evidencien lo desarrollado.
- Puede utilizar otras herramientas alternativas, si es que las sugeridas no funcionan o no entregan la información que se requiere.
- Con la información recopilada desarrolle un modelado de amenazas (DFD's) sobre la

[1] El presente texto introductorio es una traducción libre de un extracto del libro de Walker, Matt. CEH Certified Ethical Hacker All-in-One Exam Guide, Fourth Edition. McGraw-Hill Education.

arquitectura a la cual se enfrenta. Incluirla y explicarla en la sección de desarrollo.

Etapas del desarrollo

1. Buscar y describir información de forma pasiva sobre el sitio definido
    a. Información en su sitio web
    b. Información en los perfiles de las personas que trabajan allí (ej. linkedin y otras redes sociales)
    c. Busque perfiles a contratar de la empresa en cuestión. Ej. Se busca persona que sea experta en el manejo de Windows Server 2012, Microsoft SQL Server 2016 y servicios de respaldo AWS.
    d. Google, Yahoo y Twitter ofrecen también servicios de alerta, sobre cuando la información es actualizada o cambia. Estos envían las alertas al correo electrónico.
    e. Utilice https://www.netcraft.com/ También puede instalar su toolbar (Chrome y Firefox)
2. Google Hacking (utilice al menos 5 formas de buscar información):
    a. En el buscador Google utilice cadenas de búsqueda como filetype:doc, “intitle:index of” passwd, info:www.xxx.cl, intitle:login, all intitle:login password, inurl: passwd, link, related, site, etc. www.hackersforcharity.org/ghdb/,
    b. Tambien utilizar www.google.com/advanced_search,
3. Footprinting del sitio web y el correo
    a. Averigua información desde las cabeceras y cookies. Utiliza herramientas como burp suite, firebug, Ej: https://website.informer.com/
    b. Copia la página web completa a tu sistema (mirror), con alguna de las siguientes herramientas.
        i. www.httrack.com
        ii. www.tenmax.com
        iii. GNU Wget
        iv. http://spadixbd.com
        v. También puedes buscar información en www.archive.org
    c. Busca información en el HTML de la página web. Por ejemplo en los campos “Hidden”.
    d. Busca información en las cabeceras de correos.
4. Footprinting del DNS
    a. Utilice nslookup
    b. Utilice dig
5. Footprinting de red:
    a. Utilice al menos 3 de las siguientes herramientas sugeridas (puede utilizar

otras):

i. https://www.arin.net/
ii. Utilice tracert
iii. Magic NetTrace
iv. Network Pinger[2]
v. GEO Spider
vi. Ping Plotter
vii. OSR Framework (https://github.com/i3visio/osrframework)

b. Utilice al menos 5 herramientas: https://mxtoolbox.com/NetworkTools.aspx

6. Investigue otras herramientas de reconocimiento:
   a. 5 herramientas adicionales para la realización de reconocimiento (leer advertencia).
   b. Indique qué información útil pudo obtener con estas herramientas.

Contenido del video (15 a 20 minutos máximo)

1. Introducción
2. Desarrollo
3. Análisis de los resultados obtenidos y recomendaciones
4. Conclusión
5. Bibliografía

ADVERTENCIA.

Este laboratorio es de RECONOCIMIENTO PASIVO. El grupo que aplique herramientas de reconocimiento activo sobre una máquina en producción sin autorización, será calificado con la nota mínima.

[2] No usar el modo mapeador de red.

Rúbrica

Descripción	**Puntaje**
Presenta introducción	40
Búsqueda de información de forma pasiva	30
Se utilizan correctamente y de forma pasiva las herramientas Google hacking	10
Se utilizan correctamente y de forma pasiva las herramientas Footprinting del DNS	10
Se utilizan correctamente y de forma pasiva las herramientas Footprinting de red (3 herramientas)	10
Se utilizan correctamente y de forma pasiva las herramientas Footprinting de red (mxtoolbox)	10
El DFD se desarrolla de acuerdo a la evidencia obtenida	25
El DFD se construye de acuerdo a lo indicado en clases	15
Analiza los resultados obtenidos en función de la evidencia	40
Desarrolla conclusión de acuerdo a los resultados obtenidos	40
Incluye bibliografía	20
Investiga e indica otras herramientas para realizar reconocimiento	40
Incluye evidencia que sustenta la información obtenida.	30
Se respeta el tiempo de la presentación (15 a 20 minutos máximo, entre la introducción, desarrollo y conclusión).	10
Cada integrante del grupo presenta de forma proporcional al tiempo.	10
Se indica el integrante del grupo que está hablando en cada momento.	10
El video presenta esquemas y figuras de acuerdo al contenido.	10
El audio del video es claro.	10