Introducción:

En esta práctica el alumno llevara a cabo la primera fase del hacking “reconocimiento” con ayuda de herramientas como OSINT Framework y técnicas de Google Hacking. Esta etapa es fundamental, ya que se obtiene información relevante de los objetivos a través de fuentes abiertas o públicas.

El objetivo de esta práctica es conocer los principios del reconocimiento y como obtener información de forma sencilla y sobre todo completar el reto número #1 del SANS Holiday Hack Challenge y agregar sus conclusiones en el reporte final.

En pocas palabras es buscar información el Google, generalmente con fines maliciosos.

Herramientas de trabajo:

- Google Hacking

https://www.exploit-db.com/google-hacking-database

- OSINT Framework

https://osintframework.com/

Una de las formas más sencillas de encontrar sitios vulnerables se conoce como Google Hacking o Dork. Un dork es una búsqueda especifica que encuentra sitios web que cumplen los parámetros proporcionados por Google.

A. Jugando con Google dorks:

Comandos:

- ✔ **Intitle o allintitle:** la expresión es buscada en el título de la página.
- ✔ **inurl o allinurl:** la expresión buscada está en la URL (dirección).
- ✔ **Intext:** Búsqueda por texto principal.
- ✔ **site:** Se limita a buscar resultados dentro de la web que va dentro de “site:”
- ✔ **filetype:** sólo busca archivos de un tipo (doc, xls, txt…)
- ✔ **link:** sólo busca en páginas que tienen un link a una determinada web
- ✔ **inanchor:** sólo busca en páginas que tienen en el texto de enlace la expresión buscada.
- ✔ **cache:** Muestra el resultado en la cache de Google de una página web.

- ✔ **related:** busca webs relacionadas con una determinada.

Operadores:

- **and or not:** Operadores lógicos “y” o “no”
- **“ (comillas):** Si se desea buscar una palabra o frase exacta.
- **+ y -:** incluir y excluir. Ej: jaguar -coches: busca la palabra “jaguar”, pero omite las webs con la palabra “coches”
- **(asterisco):** comodín, cualquier palabra, pero una sola palabra
- **. (punto):** comodín, cualquier palabra, una o muchas

Ejemplos:

- inurl:index.php?id=
- inurl:admin.php?id=
- inurl:show.php?id=
- inurl:article.php?ID=

http://www.suesupriano.com/article.php?id=25

http://www.suesupriano.com/article.php?id=25 order by 8

Obtener Log de Wordpress.

- inurl:/uploads/wc-logs/

https://winkeyless.kr/wp-content/uploads/wc-logs/

Obtener archivos con usuarios y passwords.

- intitle: "index of" "Index Of/" password.txt

Obtener credenciales en csv.

- intitle:"index of" users.csv | credentials.csv | accounts.csv

http://lakewaleshigh.com/wp-content/uploads/2015/08/

Obtener Dump de MYSQL.

- filetype:sql “MySQLdump”(pass|password|passwd|pwd)

http://www.conveyortransmission.com/media/documents/7930-d60522533.sql

Archivos de invernación en Windows.

- intitle:"index of" "hiberfil.sys"

https://www.burntwoodgroup.com/wp-content/uploads/2016/09/download.htm

https://atlantis-zero.net/root/

Cámaras

- inurl:/view.shtml intitle:"AXIS"

http://68.116.33.170:4002/view/view.shtml?imagepath=/mjpg/video.mjpg&size=4

http://194.150.15.187/view/view.shtml?videos=&size=1

http://97.76.183.58:4000/CgiStart?page=Single&Language=0

http://131.123.154.200/videostream.cgi?user=testvisit&pwd=1234

- inurl:”ViewerFrame?Mode=”

http://184.183.28.12:4000/ViewerFrame?Mode=Motion&Language=0

http://210.155.223.251/CgiStart?page=Single&Mode=Refresh&Language=1

http://shiretoko.miemasu.net/CgiStart?page=Single&Mode=Motion

Utilización de CKeditor

- index of /ckeditor

http://protectioncivile07.org/ckeditor/

http://www.truefittandhill.com.sg/ckeditor/

Configuración de contenedores dockers

- intitle:"docker" intitle:"index of" config

Obtener Curriculum vitae:

- “teléfono * * *” “dirección *” “e-mail” intitle:”curriculum vitae”

B. Probando OSINT Framework

https://osintframework.com/

Herramientas para probar:

- Namecheckr

https://www.namecheckr.com/

- Intel Techniques

https://inteltechniques.com/osint/username.html

- Namevine

https://namevine.com/

- Amazon wishlist

https://www.amazon.com/gp/registry/search.html/?ie=UTF8&type=wishlist

Obtención de información en Github

Para este ejercicio se debe obtener información de un usuario de Github con el comando:

Información de un solo sitio

- site:github.com <juan>

Con el usuario obtenido anteriormente revisamos su información pública en el Api de Github.

- https://api.github.com/users/joanby/events/public

Revisando la información se puede visualizar un correo electrónico:

- juangabriel@frogames.es

Se utiliza la página Pipl, el cual es un buscador de Internet especializado en redes sociales con el objetivo de adquirir más información.

- https://pipl.com/

Se utiliza la herramienta hunter para buscar más correos de la página obtenida.

- https://hunter.io/search

Con los correos obtenidos verificamos la existencia del mismo con:

- https://verify-email.org/

Si el correo se encuentra en la filtración de Ashley Madison.

- https://ashley.cynic.al/

Por último, se puede revisar si los correos electrónicos han sido víctimas de una brecha de seguridad.

- https://haveibeenpwned.com/

Obtener información de la página:

http://whois.domaintools.com

https://toolbar.netcraft.com

http://www.spyonweb.com/

https://dnsdumpster.com/

https://dnstwister.report

Obteniendo usuario de Twitter

https://inteltechniques.com/osint/instagram.html

site:twitter.com "Juan Gabriel Gomila" "instagram.com/p"

Ubicación de los tweets del usuario @Joan_By

http://geosocialfootprint.com/

Extra: Tweets en tiempo real

https://onemilliontweetmap.com/

https://www.omnisci.com/demos/tweetmap/

Extra: Zone-h

Es un repositorio que contiene más de dos millones de copias de web defacements de todo el mundo.

http://zone-h.org

Extra: Obtener usuarios en Tinder.

https://www.gotinder.com/@juan