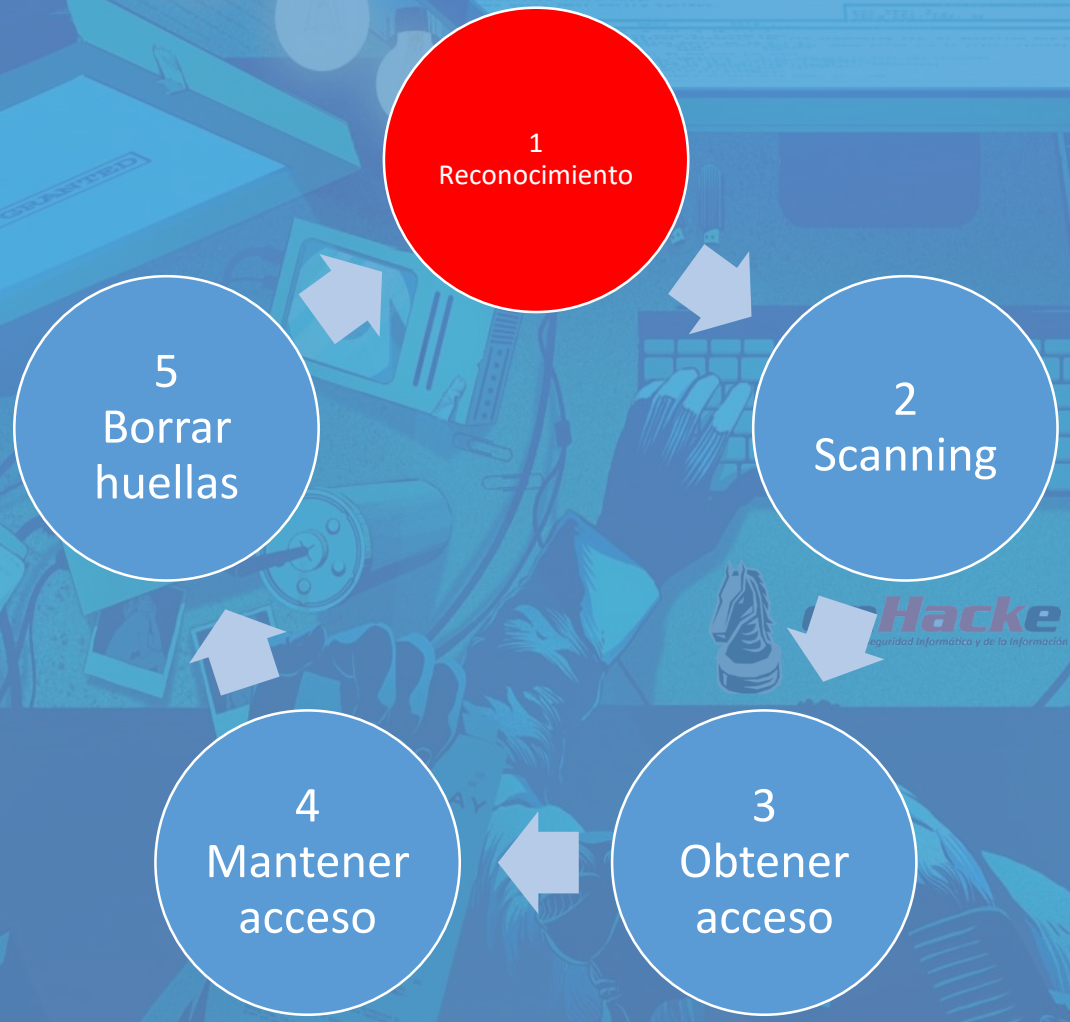
Enhacke Ethical Hacking Certification

GOOGLE HACKING

enHacke
Su aliado en Seguridad Informática y de la Información

Introducción - Reconocimiento



- **Reconocimiento refiere a la fase de preparación donde un atacante busca reunir toda la información posible sobre un objetivo antes de lanzar su ataque.**

GOOGLE HACKING: Ok… que es??

- Es un termino con el cual la comunidad se refiere a las búsquedas y consultas complejas que se le hacen a google y a su creacion
- Tiene como objetivo filtrar la información valiosa para el hacker de modo que pueda utilizarla para recolectar información acerca del objetivo auditado
- Viéndolo desde el lado oscuro, puede ser utilizado para detectar webs vulnerables a distintos factores de ataque o bien para encontrar información que descuidadamente ha sido indexada
- Principalmente se refiere al uso inteligente e imaginativo de los operadores de google

Que se puede encontrar con google hacking

- Vulnerabilidades de servidor
- Mensajes de error que brindan información de mas
- Archivos con passwords
- Directorios con información sensible
- Portales de logeo donde se revela información del sistema
- Paginas de registro o de configuración donde se revela información de dispositivos de la red donde se encuentra el objetivo
- Información sensible

Fundamentos

LOGICA BASICA DE LA BUSQUEDA

- La busqueda se hace de izquierda a derecha
- Tratar de usar logica de MAYOR a menor
- Usar lenguaje TARZAN: YO TARZAN TU JANE (sin caracteres ni tildes)
- Google busca por paginas nuevas siempre y usa algoritmos avanzados para analizar el contenido de cada pagina y sus links

BUSQUEDAS INICIALES DE EJEMPLO

- Compro laptop
- Compro una laptop
  - UNA es considerado un termino superfluo
  - Varias preposiciones también son consideradas de igual manera
- “compro una laptop”
  - La frase en comillas es denominada: BUSQUEDA LITERAL y le indica a google que busque el resultado tal cual sin modificaciones, permutaciones o combinaciones de palabras.
- “compro una laptop” –hp
  - En este caso se utiliza el signo menos (–) para filtrar o restringir un resultado
- Compro +una laptop
  - En este caso se está reforzando de otra forma el termino superfluo mediante el signo mas (+)

COMODINES

- Comodín de palabra
  - “compro laptop nueva”
  - “* laptop nueva”
  - “compro * nueva”
  - “compro laptop *”
- Comodín de carácter
  - m.trix
- El comodín de palabra * solamente funciona en una búsqueda literal
- El comodín carácter puede ir en cualquier palabra, en cualquier parte de la palabra

Anonimato

- Al hacer consultas directamente a un servidor web, la dirección IP de la máquina origen queda grabada o registrada
- Para evitar esto, se puede hacer uso de google
- El cache de google provee anonimato
  - Puedes ver la pagina sin ni siquiera conectarte al webserver del objetivo
  - Si no hay conexión al servidor, no hay pruebas de tu investigación
- Servicio de traducción de google
  - Funciona también como servidor proxy cuando se utiliza el servicio de traducción de google
  - Si se traduce una pagina mediante este servicio, google obtiene la pagina del webserver con el ip de google, la traduce y luego la muestra

Operadores avanzados

A TENER EN CUENTA

- La caja de texto de google en realidad es una ejecutador de comandos, solamente que en vez de comandos al estilo sistema operativo, le damos palabra que toma como términos de búsqueda.
- Un operador le define a google que se va a utilizar un comando
- Este comando tiene que ser acompañado de un termino de búsqueda necesariamente
- La sintaxis es operador:termino
- Fijarse como entre el operador y el termino hay : (dos puntos) pero no hay espacio
- Si google encuentra un espacio, pensará que se trata de un termino de búsqueda adicional

Lista de operadores avanzados

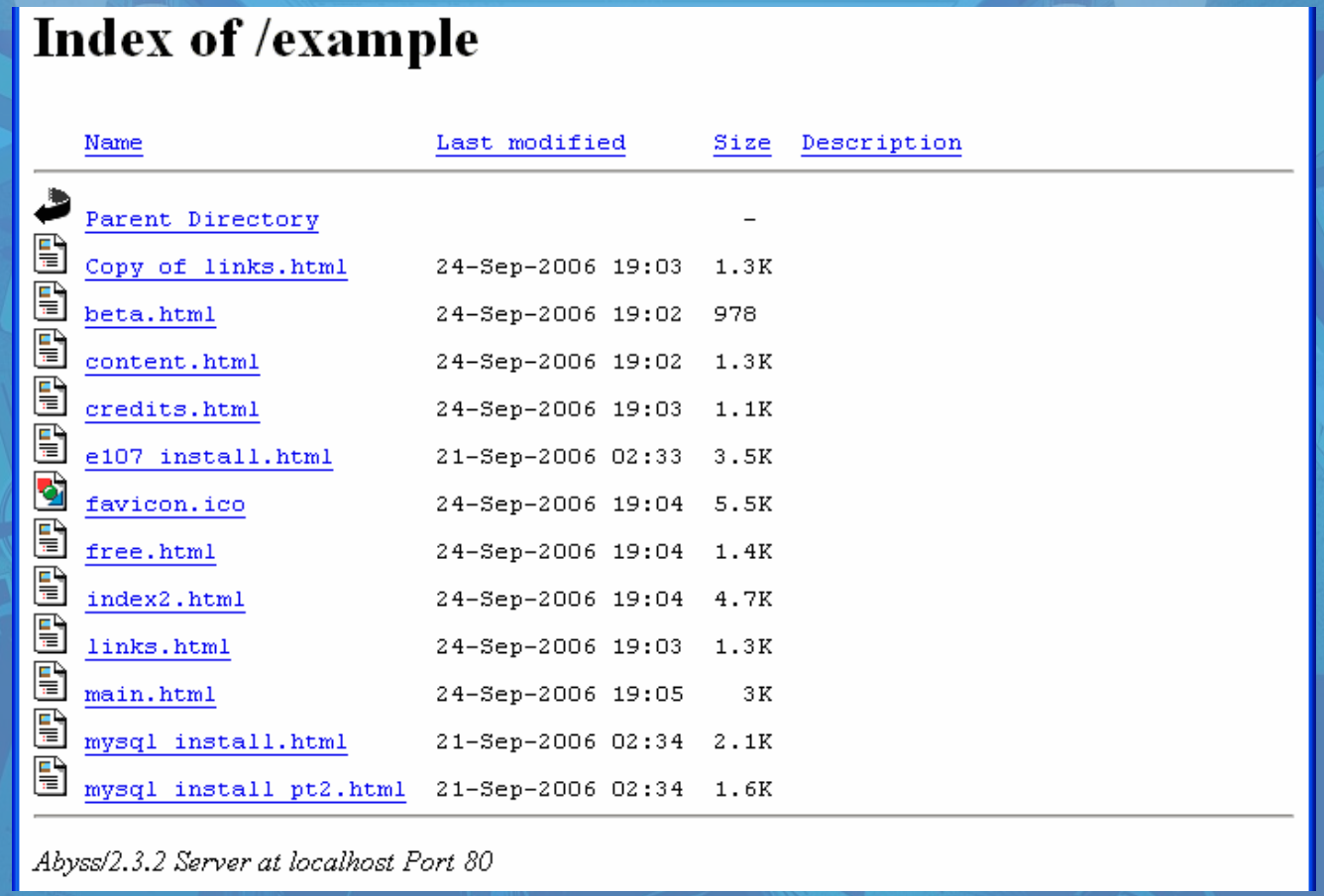
site:	**Permite restringir búsqueda a dominios y subdominios**
intitle:	**Busca en la barra de titulo mostrada en los resultados**
inurl:	**Busca la palabra clave en la url de los resultados**
filetype:	**Permite buscar tipos de archivo ejem:doc, pdf, xls**
ext:	**Busca por extensiones de archivo**
( )	**Sirve para agrupar 2 o más términos de busqueda**
| OR lógico	**Expresa en la búsqueda que puede buscar UNO u OTRO término.**

Buscando vulnerabilidades

Listado de directorios

- Tiene como definido aquellas paginas que presentan una lista de los archivos y directorios que están contenidos en el servidor web
- Esta característica la tienen los servidores web para una interacción usuario-archivo eficiente
- Importante: usualmente tienen como titulo una descripción del directorio
- Es parecido al servicio del ftp visto desde el explorador web

Listado de directorios



Index of /example

	Name	Last modified	Size	Description
	Parent Directory		-	
	Copy of links.html	24-Sep-2006 19:03	1.3K	
	beta.html	24-Sep-2006 19:02	978	
	content.html	24-Sep-2006 19:02	1.3K	
	credits.html	24-Sep-2006 19:03	1.1K	
	e107 install.html	21-Sep-2006 02:33	3.5K	
	favicon.ico	24-Sep-2006 19:04	5.5K	
	free.html	24-Sep-2006 19:04	1.4K	
	index2.html	24-Sep-2006 19:04	4.7K	
	links.html	24-Sep-2006 19:03	1.3K	
	main.html	24-Sep-2006 19:05	3K	
	mysql install.html	21-Sep-2006 02:34	2.1K	
	mysql install pt2.html	21-Sep-2006 02:34	1.6K	

Abyss/2.3.2 Server at localhost Port 80

Peligros del listado de directorios

- Usualmente son mostrados accidentalmente (en algunos casos si el index no esta o ha sido invalidado)
- En algunas configuraciones viene por defecto
- Si no hay una buena configuracion, muestra TODO. No diferencia entre lo publico y lo que deberia ser confidencial
- No previene de acceso no consentido
- Pueden dar informacion adicional que puede ayudar al atacante a saber mas sobre el sistema objetivo

Ubicando los listados

- “Index of,” o “index of”
  - Esto es lo que se muestra en el titulo de las paginas vulnerables que muestran el listado de directorios
- Intitle:index.of
  - Se le puede agregar mas factores de busqueda para filtrar y hacer mas exactos los resultados
- Intitle:index.of “parent directory”
- Intitle:index.of “name size”
- Directorios
  - Intitle:index.of.admin
  - Intitle:index.of inurl:admin
- Archivos
  - Intitle:index.of ws_ftp.log

version del webserver

- El hacker sabra plantear mejor su ataque si sabe la version exacta de software que corre el webserver
- Se puede sacar esa informacion conectandose al puerto 80 del servidor y haciendo un request
- En algunos listados de directorios tambien aparece la informacion del servidor web
  - Muchas veces esta informacion es falseada
- Intitle:index.of “server at”
- Tambien se puede sacar informacion acerca del sistema operativo o del sistema que gestiona la web
  - Palabras como “powered by” , “developed by”

Directory traversal

- El objetivo es hallar el listado de directorio pero de informacion donde no hay ninguna intencion de que sea publica
- Intitle:index.of inurl:"/admin/*"
  - Recordemos que el * es el comodin de google y que solo puede ser usado en busquedas literales
  - Busqueda literal: " "
- Si se entra al directorio principal, es muy probable que se tenga acceso al resto de directorios
- Se puede hacer en forma manual a traves de al URL, usando nombres relacionados (si hay mala configuracion)
- También se puede hacer uso de herramientas automatizadas o scripts

Mensajes de error

- Pueden revelar mucha informacion acerca del objetivo
- Se les da muy poca importancia porque son eso: “mensajes de error”, pero muchos desarrolladores no tienen idea de la cantidad de informacion que estos pueden revelar (sistema operativo, tecnologia de desarrollo web, arquitectura de la red, informacion de la BD, informacion de usuarios, etc)
- Intitle:error → ademas hay que agregarle imaginacion

Otras...

nombre	definición	palabras que pueden ayudar en la búsqueda
login	para encontrar páginas de logueo o autenticación	login | logon
usuarios	conseguir usuarios del sistema objetivo	username | userid | employee.id | "your username is"
		usuario | usuarioid | idusuario | empleado | codempleado | empleadoid
contraseñas	conseguir palabras claves, listados de contraseñas o palabras utilizadas en sistemas de autenticación del sistema objetivo	password | passcode | "your password is"
		contraseña | contrasena | contrasenia | clave | "su clave es"
		intext:(password | passcode | pass) intext:(username | userid | user)
registros	algunos registros de windows que revelan informacion	filetype:reg intext:"internet account manager"
paneles de administracion	para localizar paginas administrativas o portales de administración	"please contact your * administrator"
		admin | administrator
		"admin login"

Tecnologias web

- En alguna ocasión vamos a querer encontrar paginas web especificas a un tipo de tecnologia
  - Paginas desarrolladas en asp, php, html…
  - Ejemplo: site:victima.com filetype:asp
- Tambien se puede excluir este tipo de resultados con el objetivo de descubrir informacion mas interesante
  - Ejemplo: site:victima.com –ext:html –ext:htm -ext:shtml –ext:asp –ext:php
  - El operador ext: es parecido a filetype: y le hemos puesto el signo negativo (-) delante para que excluya estas extensiones de nuestra busqueda de paginas del dominio victima.com

Archivos temporales o de respaldo

- Aunque haya muchos posibles terminos para encontrar y listar archivos temporales o de respaldo, es recomendable hacer una busqueda con terminos comunes
- Terminos de busqueda: inurl:temp | inurl:tmp | inurl:backup | inurl:bak
  - Estos terminos deben ser combinados con site:
  - Esta busqueda, al usar el inurl tambien ubica los archivos con estas terminaciones
    - Ejemplo: index.html.bak
  - Encontrando archivos de backup
    - Intitle:index.of index.php.bak
    - Inurl:index.php.bak

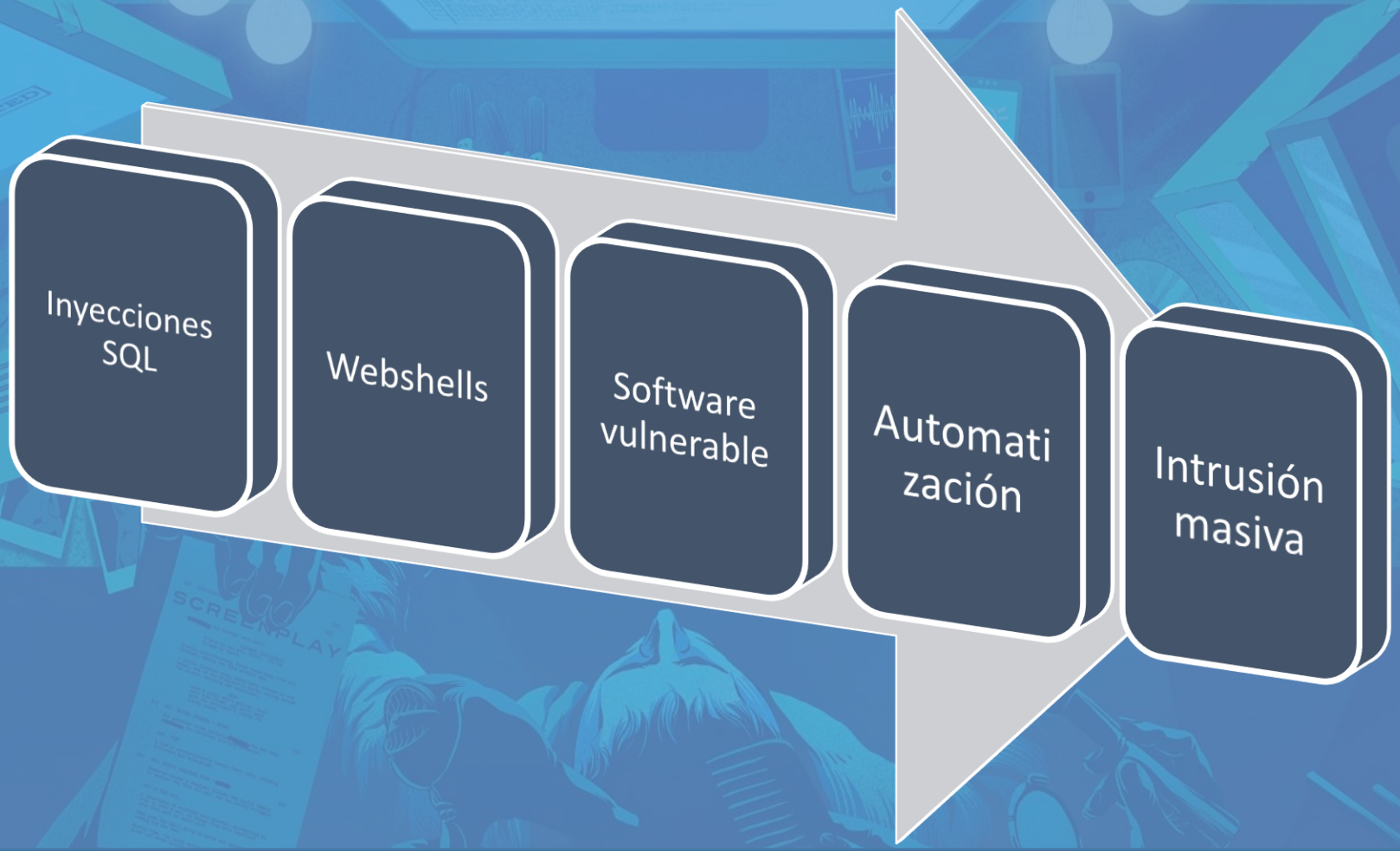
HERRAMIENTAS

DONDE PUEDO CONSEGUIR MAS INFORMACION

- GHDB
  - JOHNNY LONG – hackers for charity
    - http://www.hackersforcharity.org/ghdb/
  - Google Hacking Data Base
    - https://www.exploit-db.com/google-hacking-database/

Google dorks & google dorking & google attacks

Ataques por google



Enhacke Ethical Hacking Certification

GOOGLE HACKING

enHacke
Su aliado en Seguridad Informática y de la Información