TALLER APLICADO DE SEGURIDAD DE LA INFORMACIÓN

Ataques de red, hardware y software

Unidad 1

ESCUELA DE CONSTRUCCIÓN E INGENIERÍA

Director: Marcelo Lucero Yañez

ELABORACIÓN

Experto disciplinar: Eder Moran Heredia

Diseñador instruccional: Antonio Colmenares Prieto

Editora instruccional: María José Fonseca Palacios

VALIDACIÓN

Experto disciplinar: Alex Flores Fuentealba

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Didactic

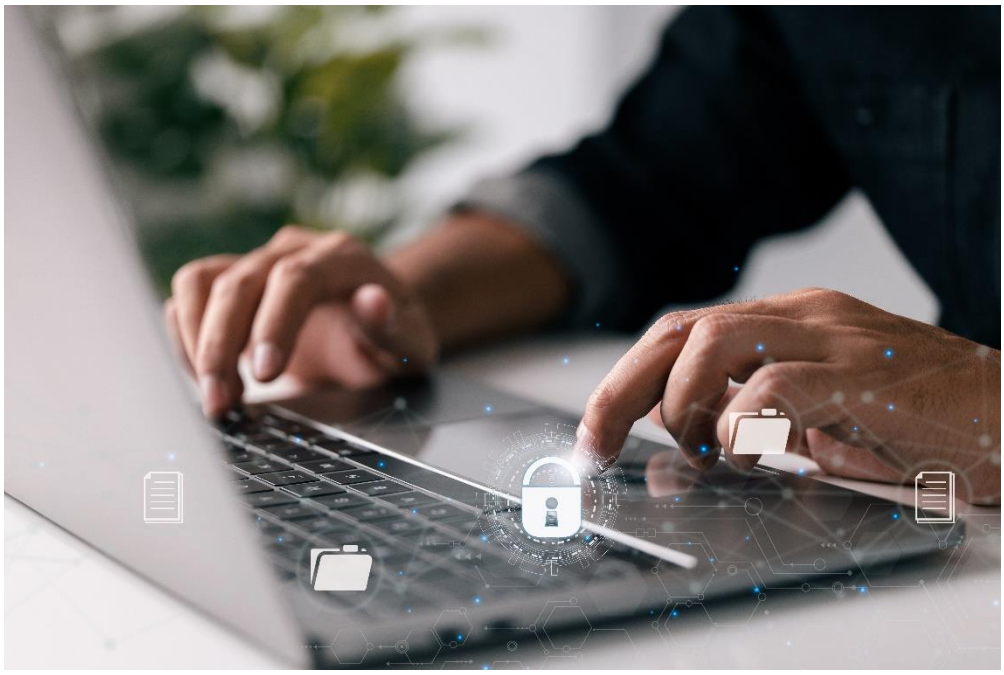
AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Utilizan técnicas de Footprinting asociadas a Ethical Hacking, considerando requerimientos técnicos de la industria.



Introducción

Actualmente, los ataques cibernéticos dirigidos a empresas financieras han causado una gran preocupación en los usuarios y por supuesto en el mundo empresarial. Y considerando que, en los últimos años, ha figurado en las cifras de ciberataques un aumento de incidentes relacionados con la ciberseguridad, tanto en entidades del sector privado, como en el sector público, sin discriminar grandes, medianas y pequeñas empresas, entendiéndose con esto, que los ataques son transversales.

Estos antecedentes, han provocado que las empresas, sea cual sea su rubro, reconozcan que los datos con los que trabajan (datos del personal interno de la empresa, de sus clientes y de proveedores, la información operacional, financiera, información de proyectos de investigación, etc.), son de vital importancia, por lo que deben protegerlos y resguardarlos de los ciberataques, incorporando medidas que incluyen mecanismos de seguridad de la infraestructura crítica, pero muchas de estas empresas no conocen cuáles son las principales vulnerabilidades que existen dentro de la organización. Por lo que, solicitan a un experto realizar un diagnóstico o evaluación de los riesgos y vulnerabilidades que presentan actualmente en la empresa.

1. Footprinting: Objetivos

Es la instancia previa a la intención de ejecutar una intrusión a un sistema por medio de alguien que no tiene autorización. Esto también es utilizado en las empresas por profesionales de seguridad informática, para realizar comprobaciones de seguridad. La recolección de información implica llevar adelante una tarea previa y minuciosa de inteligencia, recolectando datos relacionados con el objetivo o algún componente que se relacione a éste. Esta fase está conformada principalmente por la investigación y el análisis.

Un sistema informático está compuesto por incontables piezas, por lo tanto, el agujero de seguridad inicial puede encontrarse en cualquier nivel desde una falla humana, una falla en la infraestructura (es decir, falla técnica), una falla en la lógica e incluso a raíz de una falla en agentes externos involucrados, como puede ser un proveedor de internet, de hosting, una sucursal que tenga una red desprotegida, etcétera.

Los datos que buscan los intrusos antes de producir un ataque se pueden relacionar con algún empleado (de cualquier rango, ya sea un ejecutivo o un operario), mediante un sistema o parte de un sistema o con una operación o procedimiento que nos permita la intervención de un sistema. También puede ser que se busque, en una primera instancia, un sitio web, una dirección IP, una aplicación, una red, un servicio (por ejemplo, un puerto que se encuentre abierto y sirva para autenticación),

un protocolo en particular, un descuido en la programación o la administración de los sistemas, un documento, un directorio, una plataforma o cualquier dato de ubicación física de la empresa organizacional. Desde ya que, si un intruso tiene la posibilidad de conseguir en primera instancia algún logan (acceso), lo hará sin dudarlo, ya que esto permitirá escalar privilegios de forma rápida.

En esta etapa no interesa si el dato es de suma importancia o insignificante, todo es útil a la hora de escalar un sistema, así como para la planificación (simulación de ataque o chequeo).

Antes de proceder con la simulación de un ataque, debemos hacernos algunas preguntas útiles, por ejemplo:

1.- ¿Qué información tenemos acerca del objetivo?

2.- ¿Dónde se encuentran sus redes, sus sitios, por dónde fluye la información de la organización?

3.- ¿Qué partes conforman mi objetivo?

4.- ¿Qué sistemas posee la organización y cómo se conforman?

5.- ¿Cómo se llaman los integrantes de la organización? ¿Qué otros datos de estos tenemos?

6.- ¿Quiénes son los empleados? ¿De qué forma trabajan? ¿Desde dónde trabajan?

7.- ¿Qué información de los empleados existe en internet?

Para poder comenzar a realizar un ataque o una simulación del mismo, es necesario comenzar por el primer paso: saber con qué plataformas trabaja la organización y conocer algunos usuarios del sistema. En este punto, es necesario realizar una diferenciación entre "plataforma", "arquitectura" y "sistema operativo". Estos tres términos no hacen referencia a lo mismo: la plataforma es el sistema que sirve como base para que funcione el hardware, la arquitectura debe ser interna del hardware y es a quién va dirigido el sistema operativo, y el sistema operativo es el que alberga todas las operaciones de sistemas.

Como ya estudiamos, vamos a llamar footprinting (huella) a la recolección de información. Existen infinidad de métodos para recolectar información; cada atacante y cada profesional de la seguridad informática tiene su propia metodología y recursos en medio de una búsqueda de información. Mientras mayor e ingeniosa sea esta búsqueda, se tendrá mayor posibilidad de dar con un descuido, un objetivo o con una pista para comenzar a trabajar. Por ejemplo, alguien (un atacante) que tenga en su poder algunas o varias bases de datos de ISP (proveedores de internet) cuenta con una ventaja sobre el resto, ya que allí, seguramente, haya mucha información útil relacionada con el objetivo, que comprometa al sistema o parte de él.

En esta fase, un atacante tiene mucha ventaja, incluso por encima del profesional de seguridad informática, ya que pueden utilizar técnicas o recursos no éticos para la realizar la recolección o extracción de información. Si el profesional de seguridad tiene conocimiento de estas

ventajas y sabe cómo lidiar con ellas, puede estar seguro de tener un sistema protegido y controlado.

2. Metodología del Footprinting

2.1 Consultas a bases de datos

Es la recolección de datos previa a un ataque comienza, generalmente, en algún tipo de base de datos. Cuando son realizadas por intrusos, estas recolecciones, en muchas ocasiones, no es legal. Un ejemplo relacionado a la consulta a una base de datos de forma ilegal puede ser el caso anteriormente mencionado en el que se tiene acceso a la base de datos completa de un ISP, donde figuran datos personales, passwords (contraseñas), direcciones, IP, etcétera.

Luego de cotejar la información contenida en dicha base de datos (por ejemplo, datos personales) con la realidad, el atacante tratará de utilizar como passwords sus números de identificación, sus fechas de nacimiento, oficios, los propios passwords volcados en la base de datos, etcétera, pero lo hará en las cuentas de correo de las empresas que estén expuestas en dicha base de datos o en algún otro servicio que requiera autenticación, como puede ser un FTP, un login de sistema online, SSH, etcétera.

Basándose en los datos contenidos en esa base, un intruso también puede intentar descifrar la entropía y composición de las contraseñas. Tomemos un ejemplo: supongamos que en su cuenta personal la víctima

posee una pregunta secreta en relación al libro ángeles y demonios y el atacante encuentra en un foro que a esa persona le interesa ese libro. Entonces probará diferentes claves, por ejemplo, "angel", "demonio", "Rober", "Langdon", "vaticano", etcétera. Diferentes análisis confirman que, años atrás, el usuario utilizaba en sus cuentas de IPS claves como maradona10, para lo cual el intruso probará otras claves que se relacionen con ella, por ejemplo, "Maradona", "dios", "manodedios", "diegoarmando", etcétera, tratando así de dar con alguna forma actual o evolucionada de la clave. ¿Y esto por qué? Porque tiene posibilidad que hoy en día también las utilice o las haya heredado y las use en otras aplicaciones de ingreso. Incluso los datos personales se utilizan para deducir accesos, por ejemplo, nombre y apellido, y obtener así usuarios, además de passwords.

Un típico ejemplo es el USERID de las cuentas de correo corporativo e institucionales, formados muchas veces por la primera letra del nombre y seguido del apellido. Información de este tipo sirve para sacar aún más información desde otros lugares. El intruso, con esta información, buscará a su vez más información en bases de datos ilegales, como tarjetas de crédito, aportes jubilatorios, padrones, entidades privadas, información de servidores previamente atacados, etcétera. Para cualquier intruso, una fuente de passwords o datos personales es atemporal, ya que por más vieja que sea la base de datos, puede cobrar relevancia en un futuro y ser de utilidad.

Es muy común que más allá del análisis íntegro de la organización o del sitio institucional del objetivo, se busque información en otros portales,

sitios relacionados a postulaciones laborales (por la cantidad de CV), información de riesgos crediticios, si existen automóviles, reimpresión de patentes, blogs, foros, comunidades online, juicios, eventos, registros de dominios, si posee o está registrado en portales de educación, guías, redes sociales, etcétera.

Como podemos ver, la lista de lugares desde donde obtener información y armar bases de datos es muy extensa. Existen infinidades de bases de datos que se encuentran online, ya que los organismos que las manejan no ven los riesgos que es tener esa información al alcance de cualquier persona. Un ejemplo puede ser la base de datos de mapas donde se puede encontrar la fachada de la casa de una persona u organización, el sitio web de AFIP, donde está la constancia de inscripción, el sitio CUIT online donde se da información personal de alguien, etcétera. Todas estas formas de recolección de datos son pasivas.

Por otro lado, una recolección de información mucho menos pasiva, ligada a base de datos, resulta intrusiva. Por ejemplo, si el intruso programa o utiliza lo que se conoce como "massrooter" (una combinación de escaneo con exploit remoto permitiendo el ingreso dentro de servidores y realizar la extracción de datos de forma secuencial a mucha velocidad) para barrer rangos de direcciones IP.

Estos datos se acumulan para ser utilizados en un futuro, aprovechando la intrusión, se procede a instalar algunas de las siguientes cosas:

Backdoors on the fly: son "puertas traseras" que se dejan abiertas para poder ingresar cuando se desee, sin despertar sospechas. Estas no dejan abierto ningún puerto o algo remotamente detectable como para saber que existen.

Binarios troyanizados: el intruso, con suficientes conocimientos, suele sustituir de forma manual algunos archivos binarios (ps, lsof o ls) para poder esconder archivos o procesos propios dentro del sistema operativo. Cuando los mismos sean utilizados, el administrador del sistema no se dará cuenta de su existencia y de que son nuevos dentro del servidor atacado.

Rootkits: es una serie o kit de aplicaciones que se usa para la mantención de privilegios de administrador o root dentro de un servidor, no se instala de forma tan artesanal y sirve para mantener procesos ocultos y utilizarlos como puerta de entrada. Existen para todos los sistemas operativos.

Sniffers: son capturadores de logins o paquetes.

Los archivos más recolectados por esta técnica intrusiva son los shadows (sombras) de los servidores Linux y los SAM de los servidores Windows (estos poseen cuentas de sistema y passwords cifrados). Estos también se pueden comprometer por medio de descuidos del Administrador, no solo por fallas de software. Un ejemplo muy común es la famosa cuenta de SQL, por defecto "sa", sin clave asignada. Si el administrador del sistema deja sin actualizar su servidor por un corto período, el atacante puede aprovechar alguna vulnerabilidad existente y conocida por

desactualización, ingresar y comprometer el sistema sin dejar rastro alguno.

2.2 Footprinting through search engines

Buscadores

Son la mejor fuente de clasificación, análisis, búsqueda y caché de información, tanto confidencial como no confidencial sobre un objetivo. AltaVista fue el buscador preferido en los 90, le siguió Yahoo! cerca del año 2000 y hoy en día es Google por excelencia. Previamente, nos introducimos ya de manera breve en Google Hacking, es decir, la técnica para utilizar el famoso buscador y encontrar datos relevantes del objetivo. Veamos una lista bastante completa de búsquedas determinadas que se pueden hacer para encontrar información. Puede ser de archivos con información sensible, configuraciones, bases de datos internas, detalles de vulnerabilidades, avisos, usuarios, entradas, login, directorios privados, errores típicos de un sistema operativo o aplicación, etcétera.

Tabla 1. Buscadores

" " (comillas): buscar frase exacta.	inurl o allinurl: la expresión buscada está en la url.
and or not: operadores lógicos "y" o "no".	site: solo busca resultados dentro de la web que va detrás de "site:".
+ y -: incluir y excluir. Ej.: jaguar -coches: busca la palabra "jaguar", pero omite las webs con la palabra "coches".	filetype: solo busca archivos de un tipo (doc, xls, txt…).
* (asterisco): comodín, cualquier palabra, pero una sola palabra.	link: solo busca en páginas que tienen un link a una determinada web.
. (punto): comodín, cualquier palabra, una o muchas.	inanchor: solo busca en páginas que tienen en el texto de enlace la expresión buscada.
intitle o allintitle: la expresión buscada está en el título.	cache: muestra el resultado en la caché de Google de una página web.
related: busca webs relacionadas con una determinada palabra.	

Tabla 1. Buscadores.

Fuente: Moran. E. (2022)

Combinando estos operadores, el atacante puede obtener siete tipos de información distinta.

2.3 Google hacking base de datos

A continuación, se describen los grupos de información y se resaltan los códigos que hay que colocar en el cuadro de búsquedas de Google:

1.- Ficheros con usuarios y contraseñas lo que permite al atacante entrar directamente en tu web.

1. ext:pwd inurl:(service | authors | administrators | users) "# -FrontPage-" Usuarios y claves de administradores, para modificar la web. Se ven directamente en Google, sin necesidad de entrar en la página.

2. filetype:sql "# dumping data for table" "`PASSWORD` varchar" Bases de datos sql volcadas completas, tienen datos de usuarios y contraseñas.

3. intitle:"index of" "Index of /" password.txt Servidores con un archivo llamado password.txt. Se puede centrar por países con site:.ar o por páginas educativas con site:.edu

4. filetype:inc intext:mysql_connect password -please -could -port Google nos da más de 2.000 usuarios y contraseñas de bases de datos MySQL.

5. filetype:sql "MySQL dump" (pass | password | passwd | pwd) Más contraseñas disponibles en bases de datos.

2. Páginas con formularios de acceso (típica ventana que pide usuario y contraseña para entrar): lo que les permite realizar un ataque de diccionario (con listas de usuarios y contraseñas más frecuente combinados).

1. "You have requested access to a restricted area of our website. Please authenticate yourself to continue." Puerta de entrada a la administración de la web.

2. inurl:":10000" webmin, Webmin es un programa que permite administrar vía web remotamente un servidor Linux por el puerto 10000, esta búsqueda nos da muchos servidores que lo tienen activado.

3. "VNC Desktop" inurl":5800" VNC es un programa que permite administrar remotamente la web y corre en el puerto 5800 por defecto.

4. intitle:"vnc viewer for java" otra forma de acceder a gente que tiene instalado VNC.

5. inurl:/admin/login.asp allintitle:Outlook Web Access Logon Login, que permite al hacker ver los correos de una empresa.

3. Ficheros con nombres de usuario o mensajes de error que revelan el nombre de usuario:

1. "access denied for user" "using password" "general error" -inurl:phpbb "sql error" Foros php que dan errores. Nos dan el nombre del usuario y a veces también la IP del servidor.

4. Detección de la versión servidor de la web o versiones productos vulnerables:

Si el servidor web o alguno de los programas instalados en el mismo no son la última versión, casi siempre tienen agujeros de seguridad. Las versiones habitualmente salen para actualizar los agujeros de seguridad. Basta buscar en Google el exploit para poder entrar en el servidor.

1. SquirrelMail version 1.4.4" inurl:src ext:php Una versión muy mala y fácilmente accesible del gestor de correo.

2. intitle:index.of "Apache/*" "server at" Busca servidores Apache. Poniendo en lugar del * una versión con vulnerabilidades, el hacker sabe en qué servidores puede entrar.

3. intitle:index.of "Microsoft-IIS/* server at" Igual que el anterior, con sus versiones correspondientes.

5. Dispositivos hardware online (ver webcams y cámaras de vigilancia o manejar impresoras remotamente):

Con ellos puedes espiar remotamente, ver qué se imprime en una empresa, etcétera:

1. camera linksys inurl:main.cgi cámaras disponibles para que un atacante nos vea. No hace falta contraseña para entrar.

2. inurl:"ViewerFrame?Mode=" cámaras disponibles para espiar sin necesidad de contraseña.

3. “active webcam page” inurl:8080 Más cámaras disponibles en el puerto 8080.

4. intitle:”toshiba network camera - User Login”

5. intitle:”ivista main page”

6. intitle:”i-catcher console” “please visit”

7. inurl:webarch/mainframe.cgi Impresoras listas para administrar remotamente.

8. intitle:”network print server” filetype:shtm

6. Ficheros con información sensible o directorios sensibles de un servidor:

1. “phone* * *” “address *” “e-mail” intitle:”curriculum vitae” Obtenemos teléfono, nombre, mail y dirección postal.

2. filetype:ctt Archivos con listas de e-mails.

3. “robots.txt” “disallow:” filetype:txt En el archivo robots.txt el webmaster dice qué partes de su web no quiere que Google muestre, es decir, la información más confidencial de la web.

4. allintitle:restricted filetype:doc site:gov Encontrar información “interesante” en sitios de Gobiernos. Se puede cambiar “restricted” por “top secret” o “confidential”. Y “doc” por “pdf” o “txt”. O “gov” por “mil”.

5. passwords | contraseñas | login | contraseña filetype:txt site:web.com Busca contraseñas y logins en documentos txt de la web web.com. Se puede ir cambiando el filetype o la web, para tener resultados diferentes.

6. inurl:intranet filetype:doc confidential

7. "Index of" / "chat/logs" Logs de chats almacenados en servidores.

8. index.of.dcim carpetas con fotos para descargar gratis. Esta búsqueda muestra personas que han subido las carpetas de fotos a una web.

9. intitle:index.of "parent directory" Listado de directorios de un servidor, para ver las carpetas y explorarlas.

10. intitle:"index of" "Index of /"

11. intitle:"index of" inurl:"admin"

7. Información de apoyo al acceso:

1. "Microsoft (R) Windows * (TM) Version * DrWtsn32 Copyright (C)" ext:log

2. inurl:":8080" -intext:8080 Servidores que ejecutan servicios en el puerto 8080.

3. intitle:index.of ws_ftp.log Logs de acceso por FTP, que incluyen las rutas locales de los archivos que se suben y horas de subida.

4. site:sitio.com -site:www.sitio.com Sirve para conocer subdominios, intranets, dominios para la gestión del correo, etcétera.

5. intitle:"the page cannot be found" "please * * following" "Internet * Services" Permite saber el tipo de servidor. (Gonzalez, A. (s.f.). https://acortar.link/wOrBWj).

2.4 Website footprinting

El Website Footprinting es un conjunto de técnicas para obtener información del sitio web que será auditado a través de su monitoreo. Los piratas informáticos pueden mapear todo el sitio web del objetivo sin ser notados.

El Website Footprinting brinda información sobre:

- Software.
- Sistema operativo.
- Subdirectorios.
- Información del contacto.
- Plataforma de secuencias de comandos.
- Detalles de consulta.

Al examinar los encabezados del sitio web, es posible obtener la siguiente información:

- Tipo de contenido.
- Rangos de aceptación.
- Estado de conexión.
- Información de última modificación.
- X-powered-by Información.
- Información del servidor web.

Existen formas adicionales de recopilar información a través del código fuente HTML y el análisis de cookies. Al examinar el código fuente HTML, es posible extraer información de los comentarios en el código, así como obtener información sobre la estructura del sistema de archivos al observar los enlaces y las etiquetas de imagen.

Las cookies también pueden revelar información importante sobre el software que se ejecuta en el servidor y su comportamiento. Además, al inspeccionar las sesiones, es posible identificar las plataformas de secuencias de comandos.

Hay programas diseñados para ayudar en la huella del sitio web. Estos programas se denominan arañas web y navegan metódicamente por un sitio web en busca de información específica. La información recopilada de esta manera puede ayudar a los atacantes a realizar ataques de ingeniería social.

Uno de los Softwares más utilizados para estas funciones es NMAP ya que sirve para:

- Auditar la seguridad de un dispositivo o firewall identificando las conexiones de red que se pueden realizar a través de él.
- Identificar puertos abiertos en un host de destino en preparación para la auditoría.
- Inventariar las redes, mapeo de redes, mantenimiento y gestión de activos.
- Auditar la seguridad de una red mediante la identificación de nuevos servidores.
- Generar tráfico a hosts en una red, análisis de respuesta y medición del tiempo de respuesta.
- Encontrar y explotar vulnerabilidades en una red.
- Realizar Consultas DNS y búsqueda de subdominios.

Existen otras herramientas online para realizar Website Footprinting, a continuación algunas:

HERRAMIENTA	WEB	DESCRIPCION
DNSstuff	https://tools.dnsstuff.com/	Kit de múltiples herramientas para extraer información de las redes, servidores o cualquier otro recurso IP, de manera de saber si dispositivo se encuentra funcionando en forma correcta.
SamSpade	https://tools.wordtothewise.com/	Herramienta de tipo WHOIS
NetCraft	https://www.netcraft.com/	El producto Netcraft ofrece análisis de servidores y alojamiento web, incluyendo detección del tipo de servidor web y del sistema operativo que posee.
Whois	https://www.whois.org/	Herramienta de tipo WHOIS

Tabla 2. Herramientas online para realizar Website Footprinting.

Fuente: Moran. E. (2022)

Como también software para Footprinting:

Metagoofil: Es un software que permite la extracción de metadatos de documentos públicos (pdf, doc, xls, ppt, docx, pptx, xlsx).

FOCA: realiza lo mismo que Metagoofil, pero tiene funciones más avanzadas

Dmitry: Es un programa de linux basado en línea de comando, el cual permite obtener información de un host, desde algo tan básico como un Whois hasta informes de funcionamiento o escaneo de puertos.

SpyderFoot: Es un producto que facilita de gran manera el footprinting, ya que obtiene información sobre sub-dominios, versión del web server, dominios similares, bloques de red (Netblocks) y correos.

DNSenum: Es un kit de herramientas automatizada para las extracciones de información de servidores DNS y entradas DNS.

Traceroute: Es un Utilitario de línea de comandos que se usa para determinar la ruta que toma un paquete IP para lograr su destino final. Puede trazar el número de routers por donde se trasladan los paquetes y el tiempo en tránsito del traslado entre dos routers.

NSLookup: Es una herramienta utilizada para saber si el DNS está resolviendo correctamente los nombres de dominio y las direcciones IPs.

Cierre

Después de revisado el contenido de la semana, podemos extraer los siguientes factores claves:

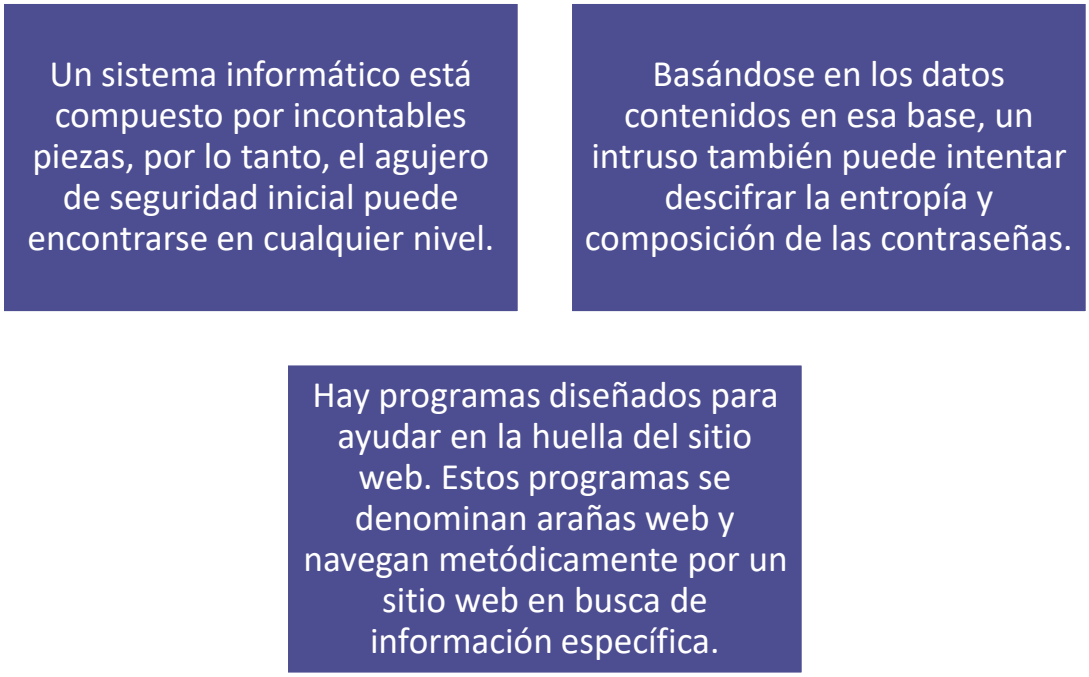


Figura 1. Ideas claves semana 2.

Fuente: Moran, E. (2020)

Referencias

Bassi, A. (2021). SQLInjection parte 1. Recuperado de https://nohaybackup.blogspot.com/

Gonzalez, A. (s.f). Google Hacking & Dorks (46 ejemplos): cómo consigue un hacker contraseñas usando sólo Google. Google puede ser tu peor enemigo. Recuperado de https://antoniogonzalezm.es/tag/intitlei-catcher-console-please-visit/

Haycanal. (s.f.). Los ataques y vulnerabilidades en dispositivos móviles crecen en septiembre. Recuperado de https://haycanal.com/noticias/8250/los-ataques-y-vulnerabilidades-en-dispositivos-moviles-crecen-en-septiembre

Kaspersky. (s.f). Amenazas a la seguridad móvil para Android. Recuperado de https://www.kaspersky.es/resource-center/threats/mobile

Wikipedia. (s.f.). Escáner de puertos. Recuperado de https://es.wikipedia.org/wiki/Esc%C3%A1ner_de_puertos

Stam, S. (Octubre 2020). Repasando #ciberseguridad de la semana 28 de Septiembre de 2020. En Pentass. Recuperado de https://blog.pentass.com/repasando-ciberseguridad-de-la-semana-28-de-septiembre-de-2020/