IES SERRA PERENXISA

GENERALITAT VALENCIANA
Conselleria de Educación, Cultura, Universidades y Empleo

FPCV
Formació Professional Comunitat Valenciana

UNIDAD 1
FUNDAMENTOS DEL HACKING ETICO

DESCARGO DE RESPONSABILIDAD

La información contenida en esta presentación solo es utilizada para fines educativos, tanto el equipo docente, como el centro, no se hacen responsables del uso indebido que se haga de ella.

GLOSARIO

1. DEFINICIONES
2. LEY DEL HACKING
3. TIPOS DE HACKERS
4. FASES DEL HACKING ETICO

1. DEFINICIONES

1.DEFINICIONES - HACKING

El **hacking** podemos definirlo como el arte de hacer que las cosas funcionen de manera diferente a como su diseñaron originalmente.

Es un concepto que podemos aplicar a cualquier tecnología, pero es habitual asociar el término hacking a los sistemas informáticos.

1.DEFINICIONES - HACKING

El término **hacking**, más que referirse a la piratería, es la manipulación de un dispositivo, un software o un artefacto para modificar su comportamiento, encontrar fallos o proponer mejoras.

Por ejemplo: alguien que modifica una lavadora para que funcione mejor que lo hace de fábrica, podemos decir que ha hackeado la lavadora.

1.DEFINICIONES - HACKER

El hacker podemos definirlo como un experto en muchos campos como son las redes, la programación, la electrónica, los sistemas operativos, la seguridad informática, etc.

Es por tanto, un experto multidisciplinar.

El hacker tiene un afán de conocimientos técnicos inagotable y dedica mucho tiempo a la informática y al descubrimiento de vulnerabilidades y fallos de seguridad.

1.DEFINICIONES - HACKER

En los medios de comunicación, es habitual utilizar el término hacker de forma despectiva, incluyendo en este concepto a todos los ciberdelincuentes con fines maliciosos y que realmente encajan dentro de la definición de cracker. De hecho, la propia RAE definía hasta hace poco al hacker como:

1.DEFINICIONES - HACKER

hacker

Artículo | Sinónimos o afines

Voz ingl.

1. m. y f. *Inform.* **jáquer.**

   SIN.: **jáquer**, **pirata**.

Sinónimos o afines de «*hacker*»

- **jáquer**, **pirata**.

Hacker

Artículo Discusión L

Para otros usos de este término, véase Hacker (desambiguación).

El término ***hacker***,[3] hispanizado como **jáquer**[4] o **jacker**,[5] es un concepto con diferentes definiciones que se diferencian principalmente en su amplitud de significado y su enfoque (neutro, negativo o positivo). El *Diccionario de la lengua española* de la ASALE, en su segunda acepción, establece que es una «*persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora*».[6] Existen definiciones más amplias como «*crear, investigar y difundir información de interés general, cumpliendo ser éticamente bueno como criterio diferenciador de crackear. Aunque pudiera usarse en sentido amplio, el uso del término hackear se suele restringir habitualmente a cuando implica informática, computación, software, hardware, reparación y/o modificación*».[7] Según Glider,[8] «*un hacker es un apasionado, un entusiasta, un experto de las nuevas tecnologías, una persona que trata de romper los límites de la tecnología para crear algo superior*»,[9] que considera que poner la

1.DEFINICIONES - CRACKER

Cracker

30 idiomas

Artículo Discusión | Leer Editar Ver historial Herramientas

En este artículo sobre informática se detectaron varios problemas. Por favor, edítalo y/o discute los problemas en la discusión para mejorarlo:

- No tiene una redacción **neutral**. Por favor, modifica los párrafos o secciones que muestran un punto de vista parcial en concordancia con lo esperado en una enciclopedia.
- Carece de **fuentes o referencias** que aparezcan en una fuente acreditada.

Puedes avisar al redactor principal pegando lo siguiente en su página de discusión: `{{sust:Aviso PA|Cracker|noneutral|referencias}} ~~~~`

Para otros usos de este término, véase Cracker (desambiguación).

Para las personas destacadas con un importante conocimiento de informática, véase Hacker.

El término ***cracker*** o **cráquer** (literalmente traducido como **rompedor**, del inglés *to crack*, que significa *romper* o *quebrar*) se utiliza para referirse a las personas que *rompen* o vulneran algún sistema de seguridad informática.[1] Usualmente de forma ilícita, los *crackers* pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta, o por el desafío.[2] Mayormente, se entiende que los crackers se dedican a la edición desautorizada de software propietario. Sin embargo, debe entenderse que si bien los ejecutables binarios son uno de los principales objetivos de estas personas, una aplicación web o cualquier otro sistema informático representan otros tipos de ataques que de igual forma pueden ser considerados actos de *cracking*.

1.DEFINICIONES – HACKER VS CRACKER

Así pues:

Aspecto	Hacker	Cracker
Definición	Experto en informática y redes con gran conocimiento técnico.	Persona que rompe la seguridad de sistemas de forma maliciosa o ilegal.
Objetivo principal	Investigar, aprender, mejorar sistemas, aumentar la seguridad.	Obtener beneficios ilegales, dañar, robar información, piratear software.
Connotación	Puede ser positiva (white hat), neutral o negativa (black hat).	Siempre negativa.
Ejemplos de acción	- Descubrir vulnerabilidades y reportarlas.- Auditar la seguridad de una empresa.- Crear nuevas herramientas.	- Hackear cuentas para robar datos.- Crackear licencias de software.- Infectar con virus o ransomware.
Legalidad	Puede ser legal (seguridad informática) o ilegal (black hat).	Siempre ilegal.
Motivación	Curiosidad, reto intelectual, ética profesional, seguridad.	Beneficio económico, vandalismo, venganza, notoriedad.

1.DEFINICIONES - PENTESTING

El **Pentesting** es la práctica de atacar sistemas con la intención de descubrir fallos y vulnerabilidades para poder mejorar la seguridad y prevenir cualquier ataque malicioso.

Es una palabra formada partir de los términos ingleses "*penetration*" y "*testing*".

El **pentesting** realmente es una forma de hacking, sólo que esta práctica es totalmente legal, ya que cuenta con el consentimiento de los propietarios de los sistemas informáticos que se van a testear.

1.DEFINICIONES - HACKER ÉTICO

El **pentester o hacker ético** es un profesional que emplea las técnicas que utilizan los mismos ciberdelincuentes (crackers o black hat) para descubrir y explotar fallos en el sistema de información de una empresa u organización.

El objetivo es el de emitir un informe de vulnerabilidades encontradas y propuesta de mejoras que ayuden a mejorar la seguridad de los sistemas.

1.DEFINICIONES - HACKER ÉTICO

El **pentester o hacker ético** es un perfil profesional que está en pleno auge

Actualmente, las organizaciones y empresas del todo el mundo necesitan cada vez más expertos en seguridad que les ayuden a defender sus sistemas informáticos de las nuevas ciberamenazas, tanto externas como internas.

1.DEFINICIONES - TEST DE INTRUSIÓN

El **test de intrusión** o **pentest** es un conjunto de técnicas y métodos para evaluar los niveles de seguridad de un sistema informático.

Realiza una simulación de un ataque real, pero bajo las limitaciones de un contrato que delimita el ámbito y el alcance de dicho test.

1.DEFINICIONES - TEST DE INTRUSIÓN

El test de intrusión conlleva un análisis activo sobre los sistemas de una organización (red, servidores, aplicaciones, etc.) para encontrar posibles vulnerabilidades, explotarlas y reportarlas en un informe final.

Tras realizar el pentest, se presenta esta información en forma de **informe** con una **evaluación precisa de los impactos** potenciales que podrían causar las vulnerabilidades si fueran explotadas por un atacante, que podría ser interno o externo a la organización.

1.DEFINICIONES - TEST DE INTRUSIÓN

El pentest y el análisis de vulnerabilidades y son conceptos diferentes.

Un análisis de vulnerabilidades detecta y clasifica las debilidades del sistema informático de la organización.

El pentesting, es la práctica de probar un sistema informático, para identificar fallos de funcionamiento, configuraciones de seguridad deficientes u otras debilidades con el objetivo de explotarlas.

1.DEFINICIONES - TEST DE INTRUSIÓN

El análisis de vulnerabilidades se limita por tanto, a enumerar los posibles fallos de seguridad mientras que el pentesting, intenta explotarlas y penetrar en el sistema.

El pentesting usa el escaneo de vulnerabilidades como una de las fases previas a la planificación de la estrategia de ataque e intrusión.

1.DEFINICIONES - RED TEAM

Los **Red Teams** emulan a los atacantes reales, utilizando sus mismas tácticas, técnicas y procedimientos (TTP), explotando las vulnerabilidades de los sistemas y aplicaciones y de esta manera entrenar al equipo el *Blue Team y sus* capacidades de detección y respuesta considerando tanto el plano tecnológico, como el procedimental y humano.

Los ejercicios de Red Team son más largos en el tiempo que el pentesting y en algunas empresas muy concienciadas con la seguridad se están realizando de manera continua.

1. DEFINICIONES - BLUE TEAM

El **Blue Team** es el equipo de seguridad que defiende a las organizaciones de ataques de una manera proactiva. Realizan una vigilancia constante, analizando patrones y comportamientos anómalos y trabajan en la mejora continua de la seguridad.

En casos de incidentes, realizan las tareas de respuesta, incluyendo análisis de forense de las máquinas afectadas, trazabilidad de los vectores de ataque, propuesta de soluciones y establecimiento de medidas de detección para futuros casos.

1.DEFINICIONES - PURPLE TEAM

Los **Purple Team** existen en aquellas organizaciones donde no hay suficiente presupuesto para tener ambos equipos e integran las tácticas y controles defensivos del Blue Team con las amenazas y vulnerabilidades encontradas por el Red Team.

Idealmente, no debería ser un equipo, sino una dinámica de cooperación entre Red y Blue Team.

1.DEFINICIONES - ETICA DEL PENTESTING

Para emular la metodología de ataque de un intruso informático y no serlo, ha de haber ética de por medio.

Imaginemos que analizando un sistema encontramos un fallo grave de seguridad, podemos hacerlo público o avisar al fabricante para que antes de comunicarlo a los usuarios, a estos les de tiempo a realizar los cambios necesarios para subsanar este fallo.

La ética **implica** que el **trabajo** y la intervención del profesional en seguridad informática o de la información **no comprometen** de ningún modo los *activos* de la **organización**, que son los valiosos datos con los que ella cuenta.

1.DEFINICIONES - CONDUCTA

El hacker ético debe cumplir unas conductas mínimas como son:

- Hacer su trabajo de la mejor manera posible.
- Respetar el secreto profesional y confidencialidad.
- No hablar mal ni inculpar a un administrador o equipo de programadores.
- No aceptar sobornos.

1.DEFINICIONES - CONDUCTA

El hacker ético debe cumplir unas conductas mínimas como son:

- No manipular o alterar resultados o análisis.
- Delegar tareas específicas en alguien más capacitado.
- No prometer algo imposible de cumplir.
- Ser responsable en su rol y función.
- Manejar los recursos de modo eficiente.

2. LEY DEL HACKING

2. LEY DEL HACKING

Conocida popularmente como "*Ley del hacking*", la reforma de diciembre de 2010 del artículo 197 del Código Penal, prevé **penas de prisión para quien rompa la seguridad de un sistema informático**.

La reforma incluyó los artículos 197 bis hasta 197 quinquies. Destacamos los siguientes aspectos:

abrir_fiscalia.php

2. LEY DEL HACKING

- La reforma sólo afecta a las empresas privadas (el sector público está exento de dichas responsabilidades penales).

- La detección de vulnerabilidades informáticas se convierte en un delito si no hay autorización.

2. LEY DEL HACKING

- El Código Penal sanciona el uso de las nuevas tecnologías de la información para invadir o atentar contra la intimidad de las personas.

- Realizar un acceso no consentido, sin autorización, vulnerando un sistema de autenticación será sancionado.

- El usuario que comete este delito puede ser sancionado con penas de prisión de entre seis meses y dos años.

2. LEY DEL HACKING

- **Las empresas son responsables por los delitos que cometen sus empleados** si se demuestra que no han implantado medidas para evitar este tipo de acciones.

- Pueden ser sancionados tanto la empresa como el empleado.

- Los profesionales dedicados a la ciberseguridad deben conocer esta ley y sus implicaciones y las empresas que los contratan deben asegurarse de ello.

2. LEY DEL HACKING

La ley no hace distinciones entre las intenciones de un delincuente y del simple curioso con conocimientos de seguridad informática, que busca comprobar la fortaleza del sistema sin aprovecharse de ello.

El Código Penal sitúa en el mismo escalafón a un investigador de seguridad que a un delincuente.

2. LEY DEL HACKING

Los empleados de una empresa dedicada a la seguridad informática deben conocer esta ley porque las sanciones que pueden afectar a las empresas son muy distintas:

- desde una multa pequeña
- hasta la propia disolución de la sociedad.

Sancionados serán tanto la empresa como el empleado causante del delito.

3. TIPOS DE HACKERS

3. TIPOS DE HACKERS

- **Hacktivista**: nace de la unión de hacker+activista. Le mueve una ideología política o un sentimiento social. (Wikileaks, Anonymous)

- **Phreaker**: Persona con grandes conocimientos en teléfonos móviles que se dedica a vulnerarlos.

- **Ciberterrorista**: su propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violación a la libre voluntad de las personas. Los fines pueden ser principalmente políticos o religiosos.

3. TIPOS DE HACKERS

- **Cracker**: Es la persona que utiliza sus conocimientos con fines maliciosos.

- **Lammer/ScriptKiddie**: Persona que alardea de ser un hacker / cracker utilizando herramientas desarrolladas por verdaderos hackers.

3. TIPOS DE HACKERS - BLACK HAT Y WHITE HAT

Un hacker de sombrero negro (**black hat**): son los también llamados badguys en el argot de la seguridad informática.

Los términos de sombrero blanco o negro, son tomados de las películas de Western.

3. TIPOS DE HACKERS - BLACK HAT Y WHITE HAT

También conocidos como *crackers*, muestran sus habilidades en informática rompiendo sistemas de seguridad de computadoras, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas, entre otras muchas cosas utilizando sus destrezas.

En contraposición, el hacker ético o pentester sería el **white hat**.

3. TIPOS DE HACKERS - GREY HAT

Actúa con el espíritu de un white hat ya que intenta descubrir vulnerabilidades e informar de ellas a los dueños de los sistemas, pero a diferencia del hacker ético que ha sido contratado y autorizado para ello, el grey hat actúa por su cuenta sin tener ninguna autorización para ello. Por tanto, **se expone a ser denunciado** e imputado por comisión de delitos.

Muchos hackers éticos han pasado por esta fase alguna vez en su vida, movidos por la curiosidad y el afán de la aprender, ayudar y demostrar sus conocimientos.

3. TIPOS DE HACKERS - GREY HAT

Algunos hackers que se autodenominan white hat, son en realidad grey hat, ya que divulgan los fallos encontrados a la comunidad sin dar tiempo al responsables para que corrija el problema.

Es lo que se conoce como full disclosure frente al responsible disclosure.

3. TIPOS DE HACKERS - GREY HAT

Full Disclosure (Divulgación total)

- **Definición**: publicar **toda la información** de la vulnerabilidad encontrada (incluyendo a veces el código de explotación).
- **Se hace pública inmediatamente**, sin esperar a que el fabricante o empresa la corrija.
- **Ventajas**:
  - Transparencia total.
  - Obliga a la empresa a reaccionar rápido.
  - La comunidad puede colaborar en soluciones.
- **Riesgos**:
  - Atacantes pueden aprovecharse de la información antes de que haya un parche.
  - Puede causar daños masivos.

3. TIPOS DE HACKERS - GREY HAT

Responsible Disclosure (Divulgación responsable)

- **Definición**: notificar privadamente al fabricante o empresa de la vulnerabilidad, dando un plazo de gracia (generalmente 30–90 días) para corregirla.
- **Después del plazo**, se publica el informe (a veces de forma parcial si no hay solución).
- **Ventajas**:
  - Se minimizan los riesgos de explotación inmediata.
  - Permite al fabricante arreglar el problema sin alarma social.
- **Riesgos**:
  - El fabricante puede ignorar la alerta o retrasar el parche.
  - A veces los usuarios permanecen vulnerables mucho tiempo sin saberlo

3. TIPOS DE HACKERS – HACKER FAMOSOS

Kevin Mitnick

También conocido como “El Cóndor”. Calificado como el criminal informático más buscado de la historia.

Sus acciones comenzaron en los 80, siendo famoso por penetrar en entornos muy protegidos.

Fue encarcelado y se le prohibió el uso de cualquier teléfono u ordenador.

3. TIPOS DE HACKERS – HACKER FAMOSOS

Stephen Wozniak

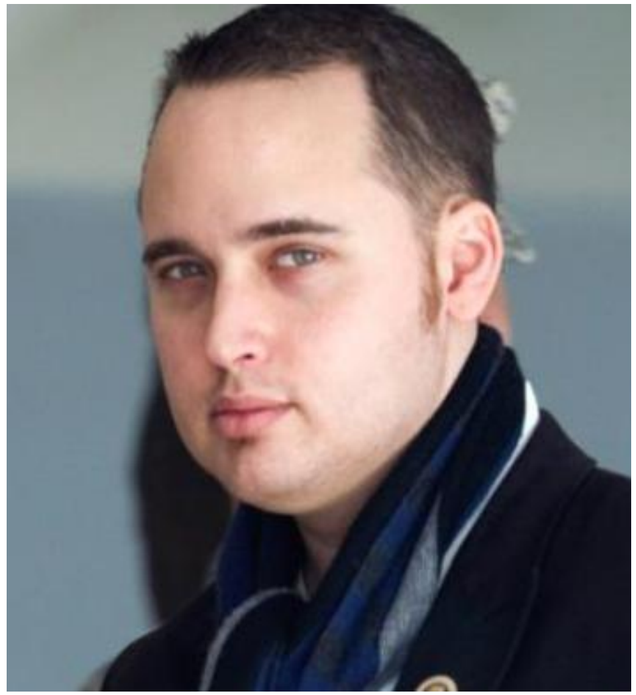
Comenzó su carrera como hacker de sistemas telefónicos para realizar llamadas gratis.

Creo un aparato llamado "Caja azul" que imitaba los distintos tonos usados para realizar llamadas.

Fundó Apple junto a Steve Jobs.

3. TIPOS DE HACKERS – HACKER FAMOSOS

Adrian Lamo



Originario de Boston y conocido como "El hacker vagabundo".

Incluyó su nombre en la lista de expertos de New York Times y penetró en la red de Microsoft.

Se dedicó a buscar vulnerabilidades de la revista Fortune y comunicarles a continuación dichas fallas.

3. TIPOS DE HACKERS – HACKER FAMOSOS

José Luis Huertas

Se infiltró en los sistemas del Consejo General del Poder Judicial, sistemas de la DGT para expedir carnés de conducir, hackear la base de la propia Policía Nacional o acceder a la web de Telecinco, hacerse pasar por Paolo Vasile (consejero delegado de Mediaset España) y robarles 300.000 euros. Llegando a robar, entre otros, los datos de más de 500.000 contribuyentes de la Agencia Tributaria.

4. FASES DEL HACKING ETICO

4. FASES DEL HACKING ETICO

A la hora de realizar una auditoría de seguridad informática, se puede seguir una metodología, aunque generalmente todas coinciden en las siguientes fases:

- Contrato de auditoría
- Recolección de información
- Análisis de vulnerabilidades
- Explotación.
- Post-explotación.
- Presentación de informes y resultados
- Borrado de huellas.

4. FASES DEL HACKING ETICO - CONTRATO

Es la fase previa a la realización de la auditoría propiamente dicha.

En este contrato se define el alcance y términos del test de intrusión y cuáles son los objetivos buscados por el cliente.

Es muy importante en esta fase, informar adecuadamente al cliente en qué consiste un test de intrusión y la información privada de la empresa que puede llegar a manejarse.

4. FASES DEL HACKING ETICO - CONTRATO

Con el contrato, el cliente autoriza al auditor a realizar una intrusión en sus sistemas que, de otra manera, constituiría un delito sin la autorización correspondiente.

El cliente puede imponer ciertas restricciones a la auditoría, que deben incorporarse al contrato y ser tenidas en cuenta por el auditor.
Una vez definido el contrato, debe ser firmado por ambas partes, el cliente y la empresa que realiza la auditoría.

4. FASES DEL HACKING ETICO - RECOPILACION

Esta fase, también conocida como information gathering se recogerá toda la información posible de la organización a auditar.

Incluye los procesos de *footprinting*, *fingerprinting* y *enumeración*. La información se puede obtener mediante ingeniería social, fuentes abiertas (OSSINT), medios de comunicación, redes sociales, hacking de buscadores, whois, etc

4. FASES DEL HACKING ETICO - RECOPILACION

Footprinting: también llamada reconocimiento pasivo porque se obtiene información de la organización objetivo, pero sin interactuar con sus sistemas.

Esta primera fase propone recolectar información pública como rangos de direcciones IP, dominios, direcciones de correo, etc.

Es una fase menos importante cuando el entorno es interno, por ejemplo en una auditoría interna a una empresa.

4. FASES DEL HACKING ETICO - RECOPILACION

Fingerprinting: también llamada reconocimiento activo pues se realiza directamente contra los sistemas de la organización.

Esta fase permite al auditor analizar los servicios localizados en la fase de footprint y conseguir información detallada de ellos.

El análisis de puertos abiertos, el análisis de mecanismos de protección y la obtención de versiones de sistemas operativos y aplicaciones y servicios se realiza en esta fase.

4. FASES DEL HACKING ETICO - RECOPILACION

Enumeración: el atacante realiza conexiones con el sistema objetivo para conseguir información más detallada como lista de hosts, dispositivos, usuarios y grupos LDAP, email, ftp, SIP(Protocolo de Inicio de Sesión en VoIP), etc.

4. FASES DEL HACKING ETICO - FOOTPRINTING

Algunas de las fuentes utilizadas por el footprinting son:

- Buscadores
- Redes sociales
- Sitios Web
- Email
- Inteligencia competitiva
- WHOIS
- DNS
- Red
- Ingeniería social

4. FASES DEL HACKING ETICO – GOOGLE DORKING

Google Dorking es la práctica de utilizar Google para encontrar aplicaciones web y servidores vulnerables mediante el uso de las capacidades nativas del motor de búsqueda de Google.

Algunas opciones avanzadas se pueden utilizar para buscar un tema específico mediante la búsqueda.

Google Search Operators - Google Guide
Búsqueda avanzada de Google

4. FASES DEL HACKING ETICO – GOOGLE DORKING

CETI 25/26

Operador (concepto)	Descripción (qué hace)	Ejemplo seguro (uso defensivo / educativo)
`site:`	Restringe resultados a un dominio o subdominio concreto. Útil para revisar qué contenido de tu dominio está indexado públicamente.	`site:tu-dominio.com` — revisar páginas indexadas de tu propio sitio.
`filetype:` / `ext:`	Filtra resultados por tipo de archivo (PDF, XLSX, DOCX, etc.). Útil para encontrar documentos publicados accidentalmente.	`site:tu-dominio.com filetype:pdf` — identificar PDFs públicos en tu dominio.
`intitle:`	Busca páginas que contienen el término en el título HTML. Puede ayudar a localizar páginas con ciertos encabezados públicos.	`site:tu-dominio.com intitle:"informe anual"` — localizar documentos públicos titulados “informe anual”.
`inurl:`	Busca páginas con un texto concreto en la URL. En contexto defensivo, sirve para detectar rutas no deseadas que hayas desplegado.	`site:tu-dominio.com inurl:"/backup"` — detectar URL públicas que incluyan “backup” (si existen en tu dominio).
`cache:`	Muestra la versión en caché que Google tiene de una página. Útil para comprobar cómo Google indexó una página y si persisten datos que ya borraste.	`cache:tu-dominio.com/pagina` — ver la copia en caché de una página propia.
`robots.txt` (concepto)	Permite comprobar si el `robots.txt` de un dominio está accesible públicamente y qué instrucciones contiene. Útil para auditar exclusiones que hayas configurado.	`site:tu-dominio.com robots.txt` — comprobar el robots.txt de tu dominio.
`author:` / `group:` (metadatos)	Busca páginas que contengan metadatos de autor o grupo. Útil para localizar documentos publicados con información de identidad.	`site:tu-dominio.com "Autor: Nombre"` — verificar documentos que incluyan metadatos propios.
`related:`	Encuentra páginas relacionadas con una URL. Útil para entender el ecosistema de contenido alrededor de tu sitio.	`related:tu-dominio.com` — explorar sitios relacionados (análisis competitivo/defensivo).
`allintext:` / `allinurl:`	Fuerzan la búsqueda de varios términos solo en el texto o en la URL. En defensa, ayudan a comprobar si frases sensibles aparecen públicas.	`site:tu-dominio.com allintext:"clave interna"` — buscar frases concretas en tu sitio.

4. FASES DEL HACKING ETICO – GOOGLE HACKING DATABASE

Google Dorking es una combinación de técnicas de hacking para encontrar agujeros de seguridad dentro de la red de una organización utilizando la búsqueda de Google y otras aplicaciones de Google.

El Google Hacking fue popularizado por Johnny Long.

Él clasificó las consultas en una base de datos conocida como Google Hacking Database (GHDB).

4. FASES DEL HACKING ETICO – GOOGLE HACKING DATABASE

Esta información puede ser sensible y no estar disponible públicamente.

A través de www.exploit-db.com, se puede buscar en GHDB o navegar por la categoría de GHDB.

Google Hacking Database (GHDB) - Google Dorks, OSINT, Recon

4. FASES DEL HACKING ETICO – RRSS

Las redes sociales son una de las mejores fuentes de información.

Las redes sociales más populares pueden hacer bastante fácil encontrar a alguien y conocerlo, incluyendo su información personal básica, así como también información confidencial.

4. FASES DEL HACKING ETICO – RRSS

Las funciones avanzadas en estos sitios de redes sociales también proporcionan información actualizada.

Un ejemplo de footprinting a través de redes sociales puede ser encontrar a alguien en Facebook, X, LinkedIn, Instagram, TickTock... y conoces sus hábitos y lugares.

4. FASES DEL HACKING ETICO – RRSS

Las redes sociales más populares pueden hacer bastante fácil encontrar a alguien y conocerlo, incluyendo su información personal básica, así como también información confidencial.

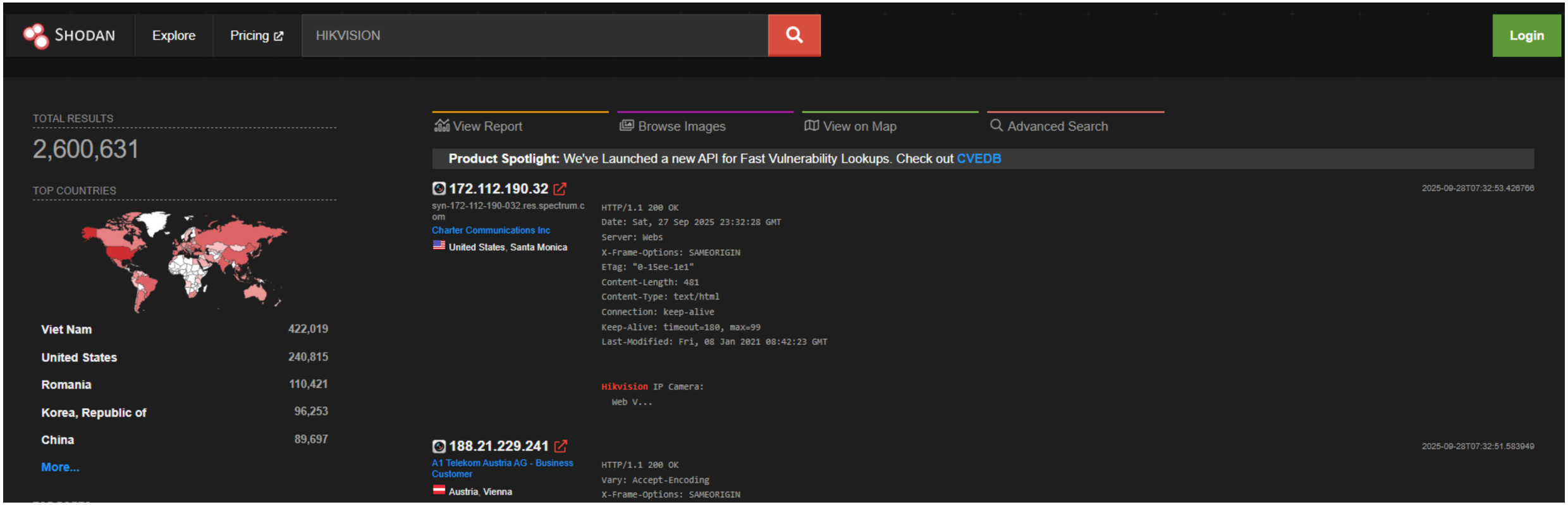
Las funciones avanzadas en estos sitios de redes sociales también proporcionan información actualizada.

4. FASES DEL HACKING ETICO – RRSS

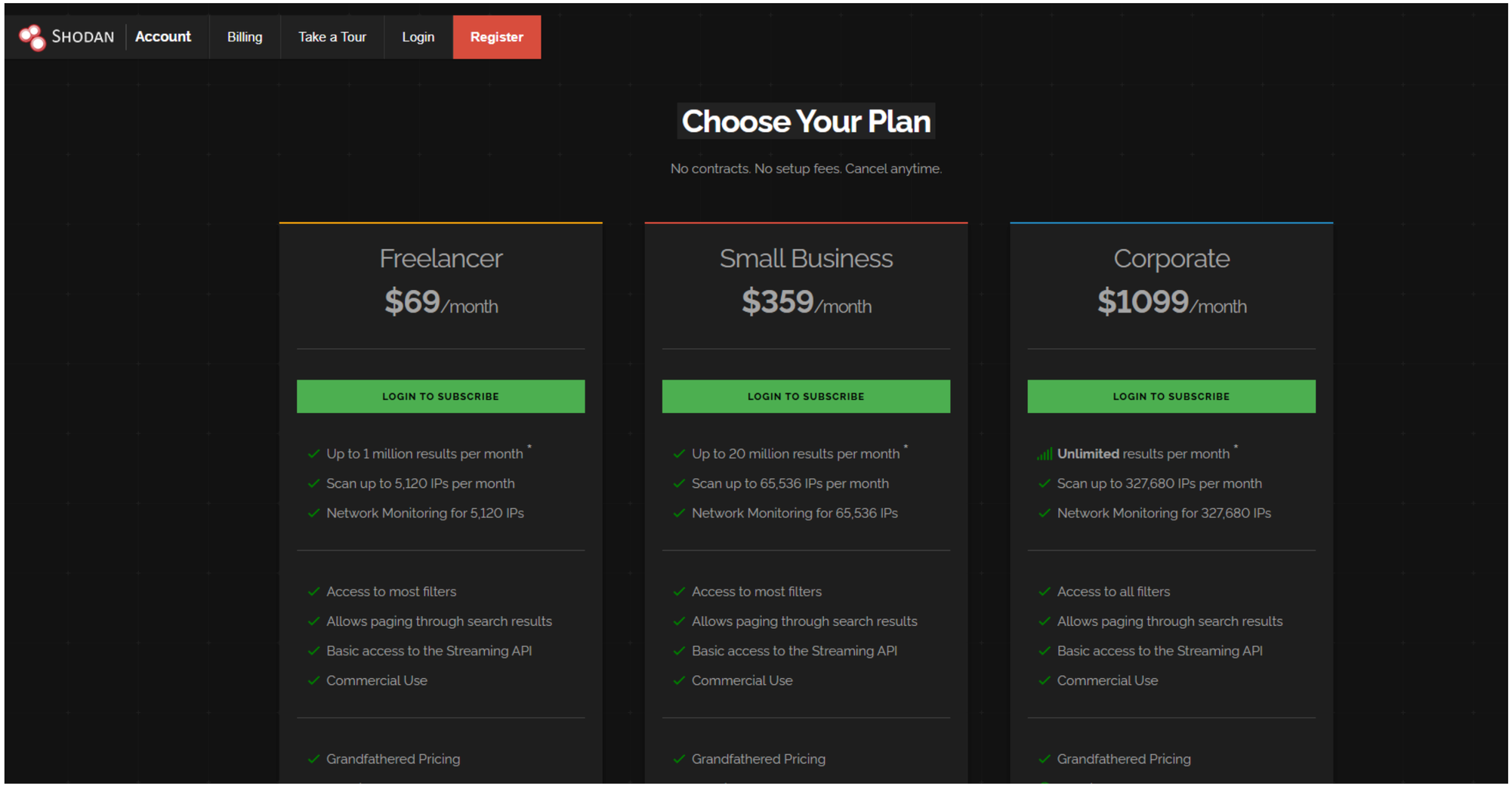
- Contactos
- E-mail
- Fecha nacimiento
- Localización
- Información laboral
- Información sobre un objetivo como información personal y laboral
- Estrategias para realizar ingeniería social
- Información personal más reciente
- Localización más reciente
- Información de amigos y familiares
- Actividades de interés
- Información relacionada con tecnología
- Información de próximos eventos
- Información relacionada con plataformas y tecnologías usadas por el objetivo
- Localización del objetivo
- Listado de amigos, familiares y/o empleados.
- Naturaleza y características del negocio

4. FASES DEL HACKING ETICO – SHODAN

Shodan como buscador especial, ya que permite encontrar por todo Internet dispositivos conectados como routers, servidores, cámaras IP, IoT y otros dispositivos usando una variedad de filtros.



4. FASES DEL HACKING ETICO – SHODAN



4. FASES DEL HACKING ETICO – SHODAN

El website footprinting incluye el seguimiento y la investigación de la página web oficial de la organización objetivo para obtener información como:

- versión de software en ejecución
- sistemas operativos
- Subdirectorios
- base de datos
- información de secuencias de commandos
- otros detalles.

4. FASES DEL HACKING ETICO – SHODAN

Esta información puede ser recopilada por el servicios como netcraft.com o mediante el uso de herramientas software como Burp Suite, Zaproxy, Nmap, Website Informer, Firebug, Httrack y otros.

Estas herramientas pueden extraer información como el tipo de conexión y el estado y la última información de modificación.

Al obtener este tipo de información, un atacante puede examinar el código fuente, los detalles del desarrollador, la estructura del sistema de archivos o las secuencias de comandos.

4. FASES DEL HACKING ETICO – WEBSITE FOOTPRINTING

El website footprinting incluye el seguimiento y la investigación de la página web oficial de la organización objetivo para obtener información como versión de software en ejecución, sistemas operativos, subdirectorios, base de datos, información de secuencias de comandos y otros detalles.

4. FASES DEL HACKING ETICO – WEBSITE FOOTPRINTING

Esta información puede ser recopilada por el servicios como netcraft.com o mediante el uso de herramientas software como Burp Suite, Zaproxy, Nmap, Website Informer, Firebug, Httrack y otros.

4. FASES DEL HACKING ETICO – WEBSITE FOOTPRINTING

Estas herramientas pueden extraer información como el tipo de conexión y el estado y la última información de modificación.

Al obtener este tipo de información, un atacante puede examinar el código fuente, los detalles del desarrollador, la estructura del sistema de archivos o las secuencias de comandos

4. FASES DEL HACKING ETICO – EMAIL FOOTPRINTING

El contenido y el cuerpo de los mensajes de correo electrónico proporcionan información valiosa.

Este contenido puede incluir información de hardware y software, credenciales de usuario, información de dispositivos de seguridad y de red, información financiera…

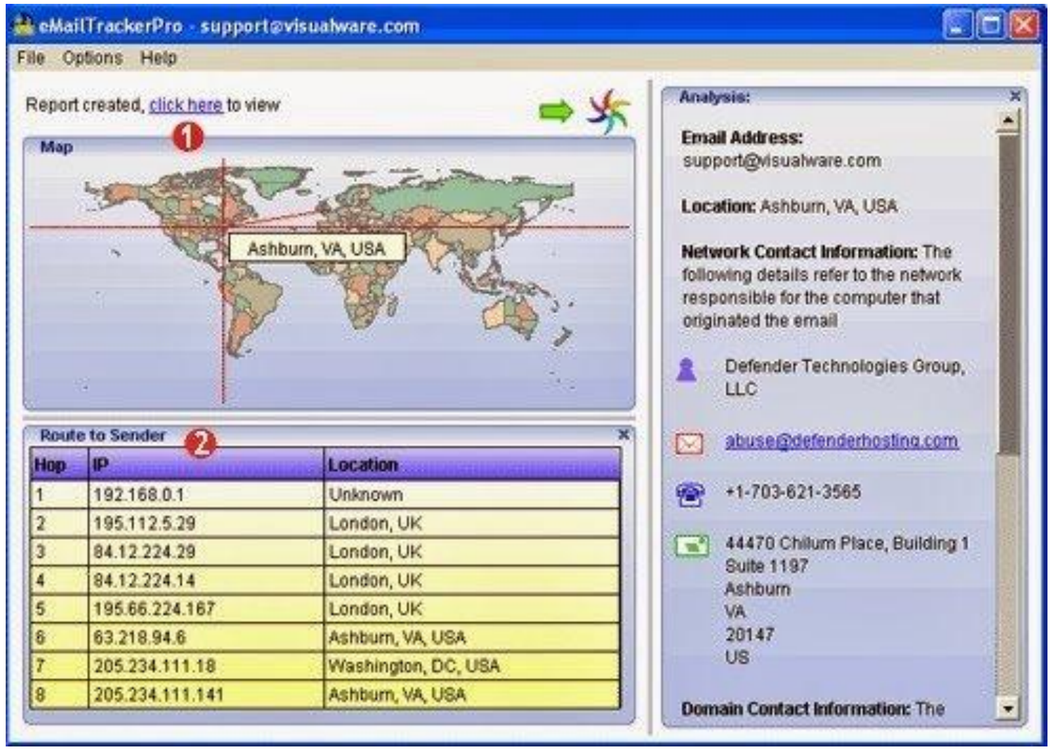
4. FASES DEL HACKING ETICO – EMAIL FOOTPRINTING

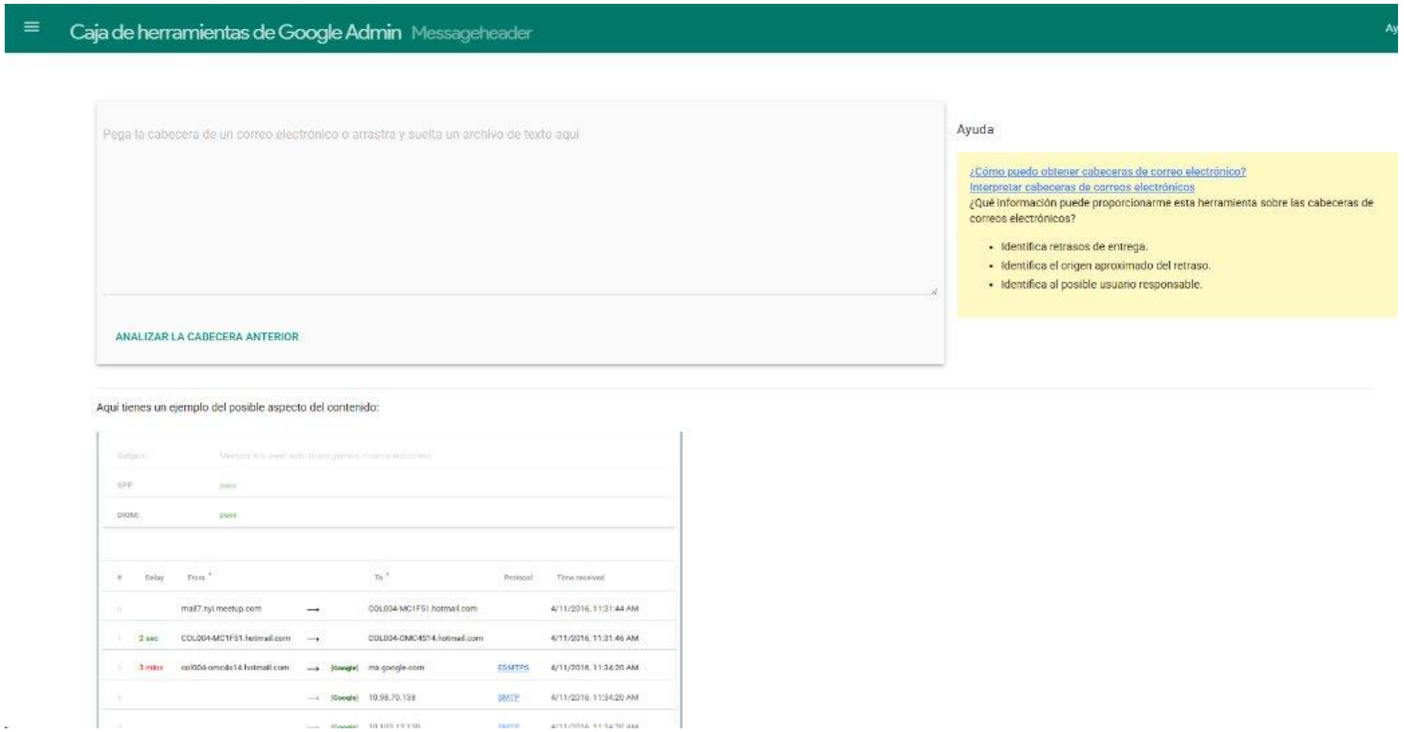
Por otra parte, las cabeceras (headers) de los mensajes pueden revelar la siguiente información:

- Dirección IP de destino / remitente
- Servidor de correo del remitente
- Información de fecha y hora
- Información del sistema de autenticación del servidor de correo

4. FASES DEL HACKING ETICO – EMAIL FOOTPRINTING

Las cabeceras se pueden analizar manualmente pero hay herramientas que lo hacen como Email Tracker Pro, Google Toolbox Messageheader, Polite Mail, Email Lookup, etc.





4. FASES DEL HACKING ETICO – WHOIS

WHOIS es un servicio que ayuda a obtener información sobre el nombre dedominio, su propietario, rangos de direcciones IP, servidores de nombres de dominio y otro tipo de información.

Los registros regionales de Internet (RIR) mantienen la base de datos de WHOIS.

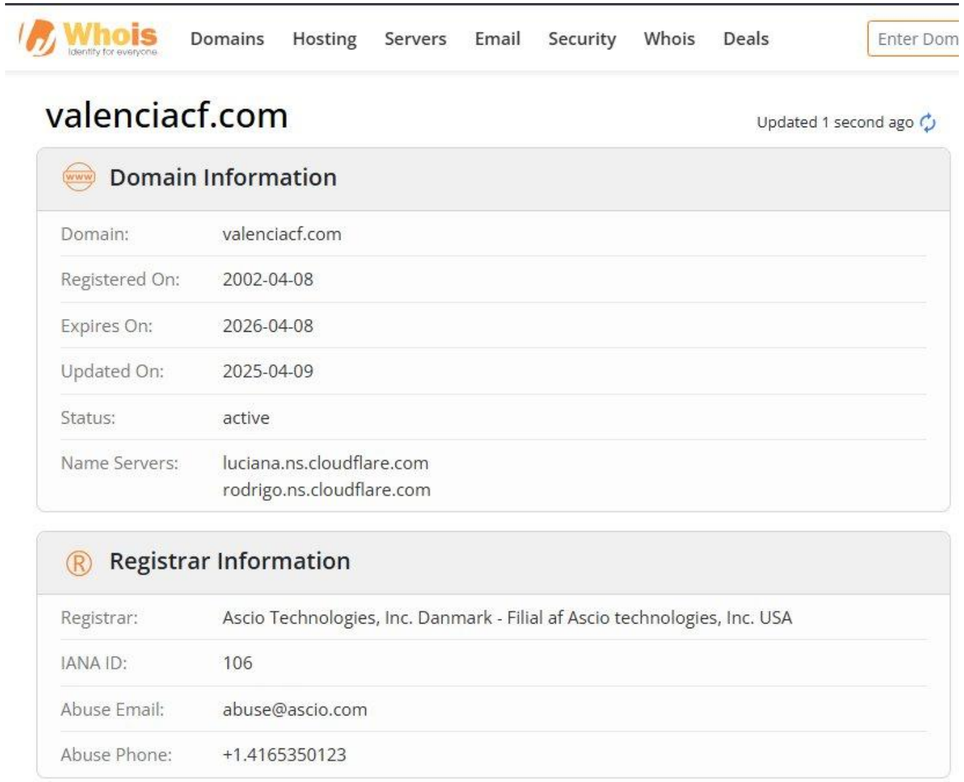
4. FASES DEL HACKING ETICO – WHOIS

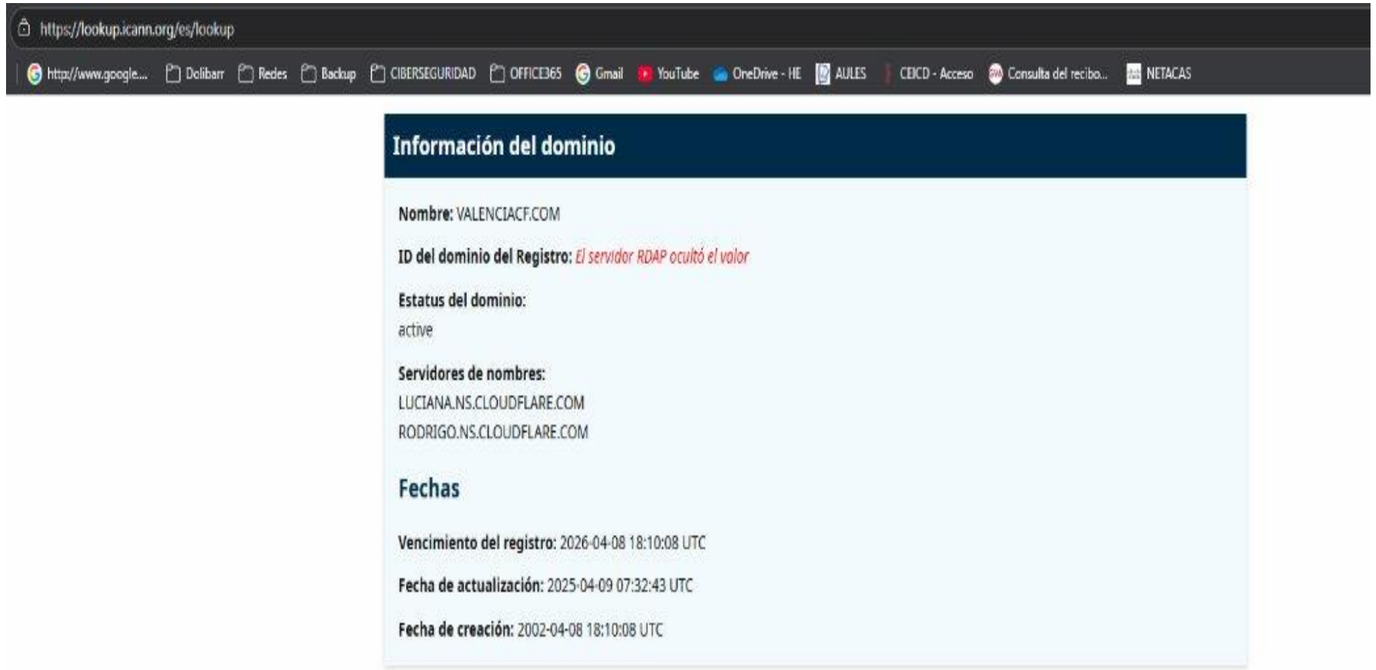
Son cinco los RIR a nivel mundial:

- AfriNIC: África
- ARIN: USA, Canadá, partes del Caribe y la Antártida
- APNIC: Asia, Australia, Nueva Zelanda
- LACNIC: Latino América y el resto del Caribe
- RIPE NCC: Europa, Rusia, países del Este y Asia Central

Whois es un protocolo cliente/servidor sobre el puerto 43/tcp y se utiliza con un cliente de consola o gráfico aunque también se puede consultar la información del whois mediante sitios web.

4. FASES DEL HACKING ETICO – WHOIS





https://lookup.icann.org/es/lookup

4. FASES DEL HACKING ETICO – DNS

La información de búsqueda de DNS es útil para identificar un host dentrode una red.

Tipos de registros para almacenar la información de un dominio.

- **Registro A / AAAA**: registro que contiene la dirección IP de un dominio.
- **Registro CNAME**: reenvía un dominio o subdominio a otro dominio.
- **Registro MX**: dirige el correo a un servidor de correo electrónico.

4. FASES DEL HACKING ETICO – DNS

Tipos de registros para almacenar la información de un dominio. (Cont.)

- **Registro TXT**: Almacenar notas de texto en el registro. Estos registros se suelen utilizar para la seguridad del correo electrónico.
- **Registro NS**: almacena el servidor de nombres para una entrada DNS.
- **Registro SOA**: almacena la información del administrador sobre un dominio.
- **Registro SRV**: especifica un puerto para servicios específicos.
- **Registro PTR**: proporciona un nombre de dominio en búsquedas inversas.

4. FASES DEL HACKING ETICO – DNS

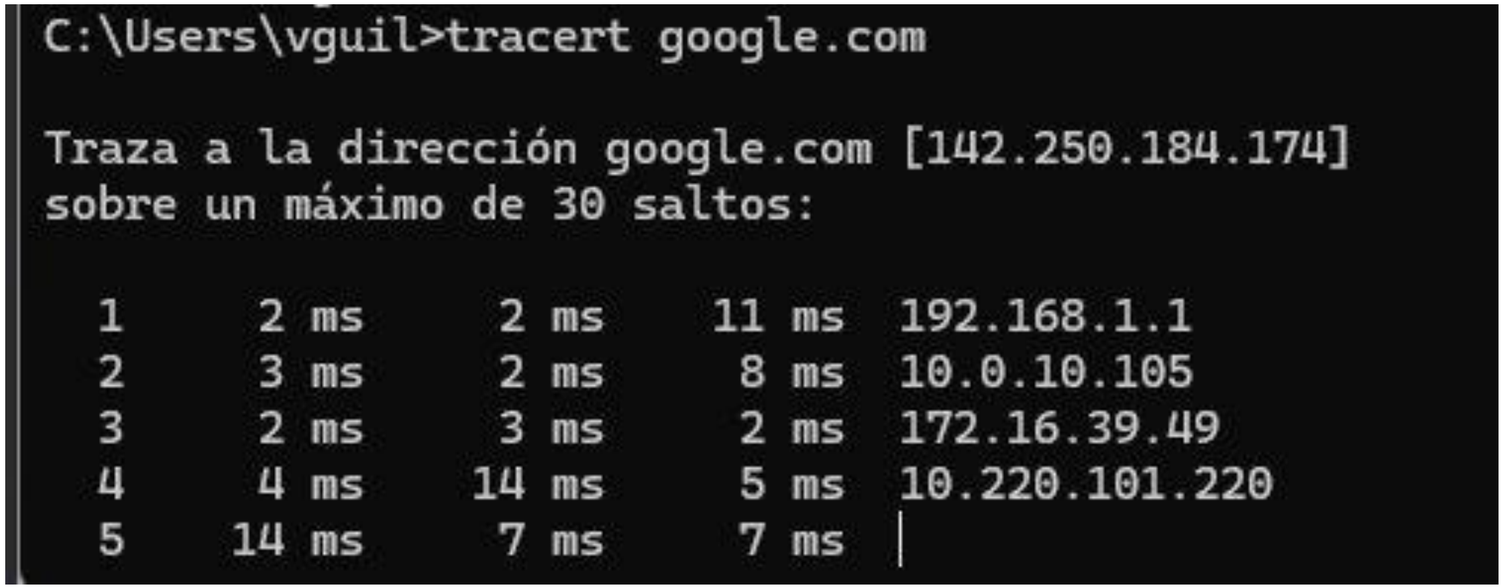
Para consultar la información pública de un dominio DNS, se pueden usar las herramientas de consola *nslookup*, *host* o *dig,* pero también hay muchas herramientas online que pueden hacer este tipo de consultas de la base de datos DNS, como son:

- https://tools.dnsstuff.com/
- https://dnschecker.org/all-tools.php
- https://viewdns.info/
- https://toolbox.googleapps.com/apps/dig/
- https://mxtoolbox.com/DnsLookup.aspx
- https://centralops.net/co/
- http://www.dnsqueries.com

4. FASES DEL HACKING ETICO – DNS

Con el footprinting de red y usando herramientas como traceroute, tracert o mtr podemos obtener valiosa información como:

- Rangos de red
- Nombres de hosts
- Equipos expuestos
- Mapa de la red



4. FASES DEL HACKING ETICO – INGENIERIA SOCIAL

En footprinting, uno de los componentes más fáciles de hackear es el propio ser humano, conocido como la Capa 8.

Podemos recopilar información de un ser humano con bastante más facilidad que obtener información de los propios sistemas.

4. FASES DEL HACKING ETICO – INGENIERIA SOCIAL

Usando Ingeniería Social, algunas técnicas básicas de ingeniería social son:

- Eavesdropping: escucha de conversaciones
- Shoulder Surfing: mirar por encima del hombro
- Dumpster Diving o trashing: buscar en la basura o papeleras
- Phishing: suplantar identidades para obtener información

4. FASES DEL HACKING ETICO – FINGERPRINTING

Esta técnica consiste en recolectar información de forma activa directamente de los sistemas informáticos de una persona o empresa para conocer más sobre su comportamiento y configuración.

4. FASES DEL HACKING ETICO – FINGERPRINTING

Existen muchas técnicas y herramientas pero principalmente se utilizan:

- Escaneo de la red.
- Escaneo de puertos.
- Banner grabbing (detectar versiones del software).

Una de las herramientas más usadas en esta fase es nmap y sus variantes gráficas como zenmap. Algunas otras son hping3, NetScan Tools, Network Topology Mapper, etc.

4. FASES DEL HACKING ETICO – ENUMERACION

Con la enumeración, se intenta obtener información más detallada como:

- Información sobre la red
- Recursos de red
- Rutas de red
- Información SNMP y DNS
- Usuarios y grupos, etc.

4. FASES DEL HACKING ETICO – ENUMERACION

Esta información confidencial es necesaria para acceder poste riormente al sistema.

Para la enumeración se hacen uso de diferentes herramientas y técnicas de forma activa.