Introducción al Hacking ético

Contenidos

1. Un poco de historia.
2. Algunos hackers famosos.
3. La ciberdelincuencia en la actualidad.
4. Conceptos básicos.
5. Tipos de intrusos, código dañinos y ataques.
6. Vulnerabilidades.
7. Tipos de auditoría.
8. Metodología y fases de un test de intrusión.
9. Perfil de un buen hacker, plataformas de aprendizaje y recursos.
10. Retos CTF y cazarecompensas.
11. Herramientas de seguridad y hacking.

Un poco de historia

- En inglés, un ***hack*** es una solución rápida e ingeniosa a un problema.
- Los estudiantes o ingenieros que trabajaban en los primeros desarrollos buscaban constantemente mejorar las soluciones a los problemas que se planteaban.
- Estos pioneros de la informática fueron los primeros ***hackers***.

Un poco de historia

- A finales de los 60 y principios de los 70 nació el ***phreaking:*** pirateo de las comunicaciones telefónicas para realizar llamadas gratuitas o para conectarse a Internet.
- Estos primeros *hackers* estaban movidos por la curiosidad y las ansias de aprender pero sus acciones se consideraban ilegales.
- Uno de estos jóvenes apresado y encarcelado es Loyd Blankednship, más conocido como "***The Mentor***". Tras su detención en 1986, publicó en la revista online *Phrack* el artículo "***The Conscience of a Hacker***", más conocido como el ***Manifiesto Hacker***.

Un poco de historia

- Historia del hacking en España.
  - Libro Hackstory de Mercè Molist (hackstory.es)

Sí, soy un delincuente.

"Mi delito es la curiosidad. Mi delito es juzgar a la gente por lo que dice y por lo que piensa, no por lo que parece. Mi delito es ser más inteligente que vosotros, algo que nunca me perdonaréis. Soy un hacker, y éste es mi manifiesto. Podéis eliminar a algunos de nosotros, pero no a todos... después de todo, somos todos iguales." THE MENTOR

Algunos hackers famosos

- ***John Draper* (Capitán Crunch)**. Famoso por utilizar silbatos de regalo de cajas de cereales para hacer llamadas telefónicas gratuitas en EEUU.
- ***Vladimir Levin***. Accedió al sistema central de Citybank en Nueva York para hacer transferencias por valor de 10 millones de dólares.
- ***Kevin Poulson***. Famoso phreaker que intervino las llamadas de numerosos concursos y ofertas para ganarlas. En la actualidad editor de la revista Wired.
- ***Kevin Mitnick***. Uno de los más famosos de la historia por acceder a sistemas de la NASA y del Departamento de Defensa de los Estados Unidos.

Kevin Mitnick - A Hacker's Story
https://www.youtube.com/watch?v=Qe73tRTksf0

La ciberdelincuencia en la actualidad

Tipo de ciberdelito	2016	2017	2018	2019	2020
Fraude informático	45.894	60.511	88.760	192.375	257.907
Amenazas y coacciones	11.473	11.270	11.906	12.782	14.066
Falsificación informática	2.697	2.961	3.095	4.275	6.289
Acceso e interceptación ilícita	2.579	2.505	2.750	4.004	4.653
Contra el honor	1.524	1.537	1.423	1.422	1.550
Delitos sexuales	1.188	1.312	1.393	1.774	1.783
Interferencia en los datos y en el sistema	1.110	1.102	1.015	1.473	1.590
Contra la propiedad intelectual/industrial	121	109	217	197	125
Contra la salud pública	0	0	0	0	0
TOTAL	66.586	81.307	110.603	218.302	287.963

Fuente: Observatorio Español de Delitos Informáticos
https://oedi.es/estadisticas/

La ciberdelincuencia en la actualidad

DELITOS INFORMÁTICOS

Los hackers holandeses del ciberataque al Ayuntamiento de Sevilla piden hasta cinco millones de euros como rescate

- El grupo LockBit, de origen holandés, ha sido señalado como el autor material de los hechos
- El Ayuntamiento espera que los 'hackers' no tengan los datos de los sevillanos
- Los expertos ya advirtieron de que Sevilla era una de las provincias con más dispositivos vulnerables a los ciberataques

betech | Tecnología, gadgets, móviles, informática y redes

SEGURIDAD

¿Qué es el scraping? El hackeo que le ha costado a Meta una multa de 265 millones de euros

Te contamos en qué consiste la práctica que han usado los malhechores para hacerse con los datos de 533 millones de cuetas de Facebook.

LA VANGUARDIA | Economía

Multa de más de 200 millones a British Airways por el robo de datos a clientes

- Un hackeo desvió a los clientes a una página en la que se quedaban los datos de sus tarjetas

https://cso.computerworld.es/tendencias/las-mayores-multas-sanciones-y-acuerdos-del-mundo-por-violacion-de-datos

La ciberdelincuencia en la actualidad

HACKEO COLOMBIA >

Hackeo masivo en Colombia: "La información de millones de personas está en manos de delincuentes en este momento"

Los portales web de la rama Judicial, el Ministerio de Salud, la Superintendencia de Industria y Comercio y muchas otras entidades siguen caídos por tercer día

El juez envía a prisión al ciberdelincuente Alcasec por vender los datos de más de 500.000 contribuyentes

La Audiencia nacional ha decretado prisión provisional, comunicada e incondicional por un delito continuado de revelación de secretos al joven de 19 años, responsable del hackeo al Punto Neutro Judicial del CGPJ.

La ciberdelincuencia en la actualidad

el Periódico de Aragón

PUBLICIDAD

FIESTAS DEL PILAR 2021 **Los actos del programa que no puedes perderte hoy lunes en Zaragoza**

CIFRAS MILLONARIAS

Twitch sufre un hackeo que filtra el sueldo millonario de Ibai Llanos

CIBERSEGURIDAD

Twitch, la plataforma de 'streaming' de Amazon, sufre un 'hackeo' y se filtran 125 GB con datos sensibles

- Entre los datos filtrados están los ingresos de los creadores de contenido de la plataforma desde 2019, el código fuente de todos sus servicios e información sobre una nueva tienda de videojuegos de Amazon que competiría con Steam

La ciberdelincuencia en la actualidad

GOBIERNO >

El Gobierno denuncia que los móviles de Sánchez y Robles fueron espiados con el programa Pegasus

Los atacantes extrajeron 2,6 gigas de datos del teléfono del presidente y nueve megas de la ministra de Defensa. El Ejecutivo no sabe aún cuál es la información robada y su grado de sensibilidad

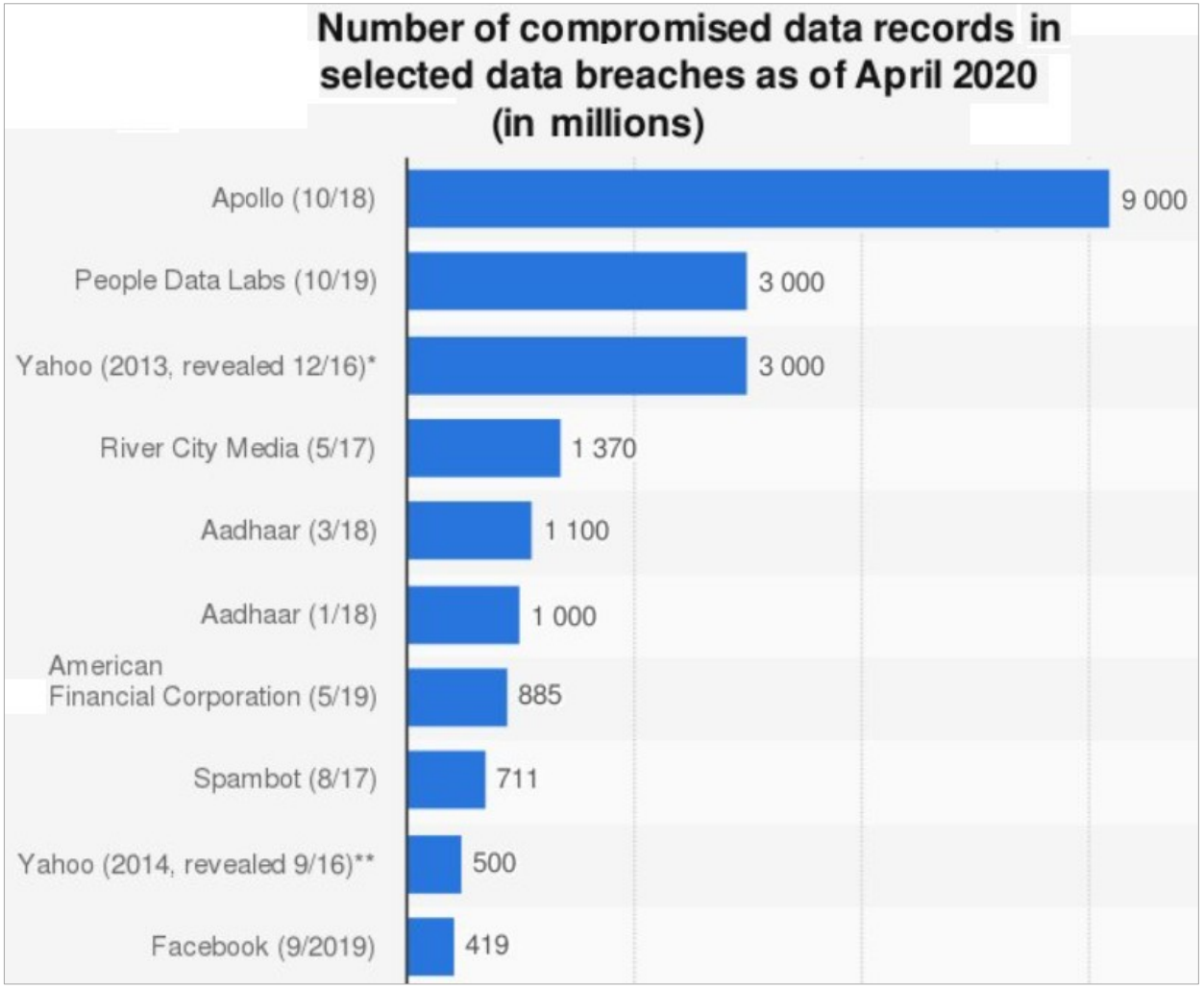
Ecoley

Las multas por Protección de Datos aumentan un 521% durante 2021

* *Las sanciones por fallos de privacidad superan por primera vez los 1.000 millones*

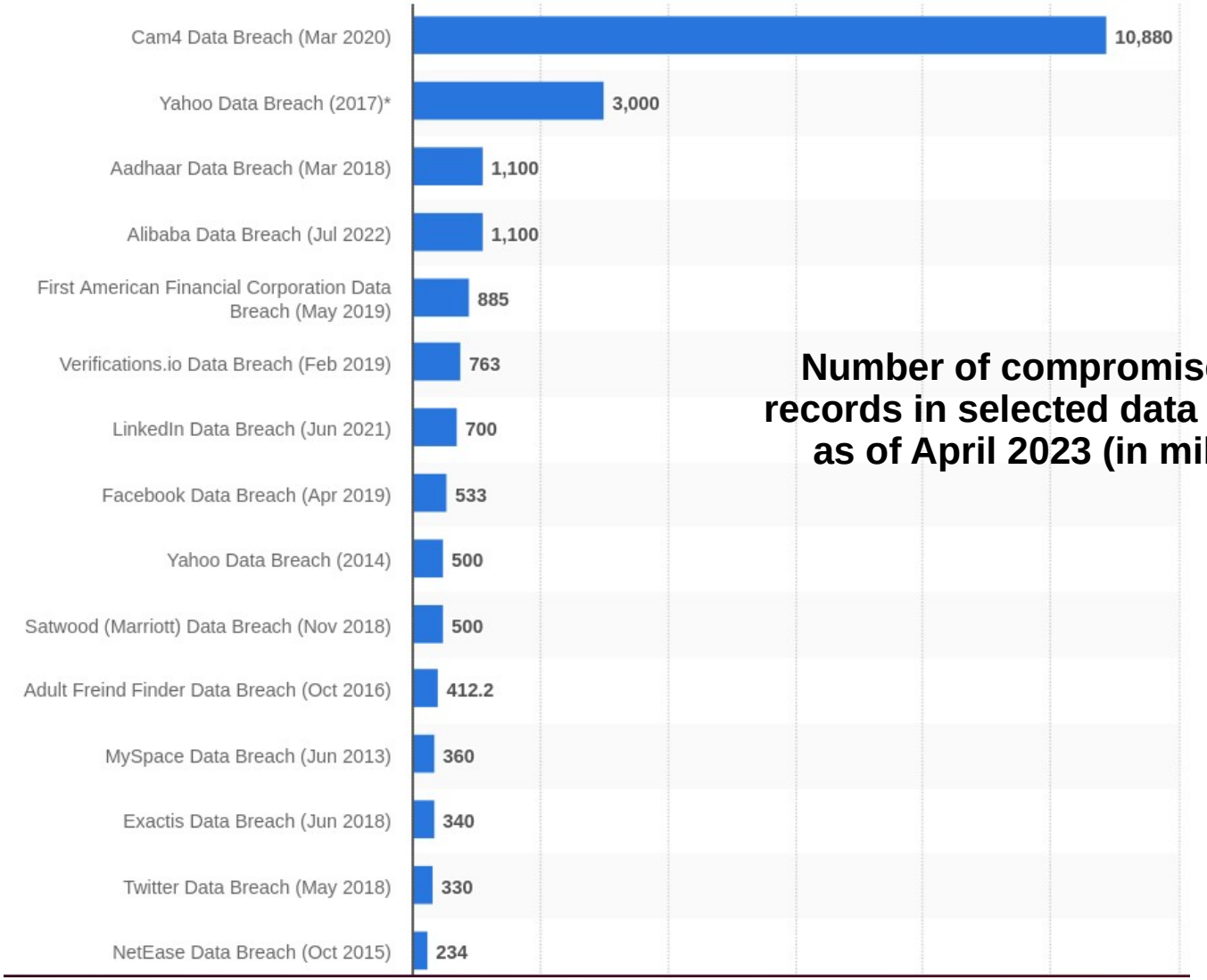
Vídeo de S4vitar sobre el funcionamiento de Pegasus.
https://youtu.be/rABIDoDKGB0

La ciberdelincuencia en la actualidad



Fuente: statista.com

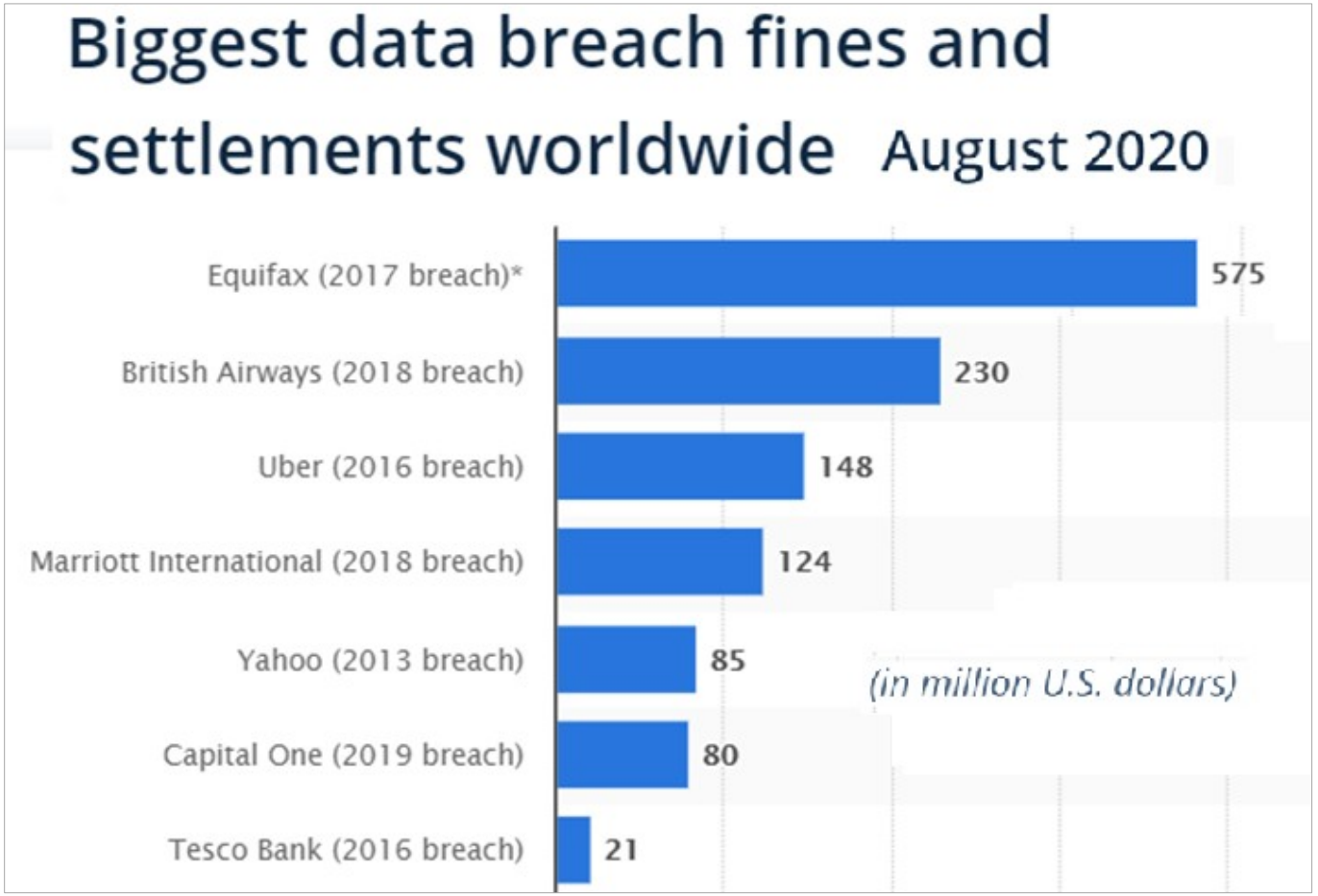
La ciberdelincuencia en la actualidad



Number of compromised data records in selected data breaches as of April 2023 (in millions)

https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/

La ciberdelincuencia en la actualidad



https://www.statista.com/statistics/1170520/worldwide-data-breach-fines-settlements/

La ciberdelincuencia en la actualidad

- La demanda de profesionales formados en ciberseguridad ha crecido enormemente, si bien, no lo ha hecho al mismo ritmo que los delitos.
- Hay una falta de personal con titulaciones y experiencia suficiente con respecto a los perfiles que requieren las empresas.
- Según el INCIBE, la demanda de talento doblará a la oferta en el año 2024, con una estimación de más de 83.000 profesionales necesarios.

https://www.incibe.es/sala-prensa/notas-prensa/demanda-talento-ciberseguridad-doblara-oferta-2024-alcanzar-cifra-mas-83000

Conceptos básicos

- **Seguridad informática**: Conjunto de medidas de prevención, detección y corrección, orientadas a proteger la **confidencialidad**, **integridad** y **disponibilidad** de la información.
- Estos tres aspectos de la información se conocen como principios de la seguridad informática.
- **Seguridad defensiva**: su objetivo es proteger la información y los recursos de la organización.
- **Seguridad ofensiva**: técnicas y procedimientos para vulnerar los controles y poner en riesgo alguno de principios mencionados.

Conceptos básicos

- Principios de la seguridad informática:
  - **Confidencialidad** (*confidentiality*). Se ocupa de garantizar que la información solo pueda ser conocida por las personas autorizadas.
  - **Integridad** (*integrity*). Esta característica posibilita que la información no pueda ser alterada o modificada sin permiso o de forma accidental.
  - **Disponibilidad** (*availability*). Se garantiza que la información estará accesible por un sistema o por usuarios autorizados a ello.

Conceptos básicos

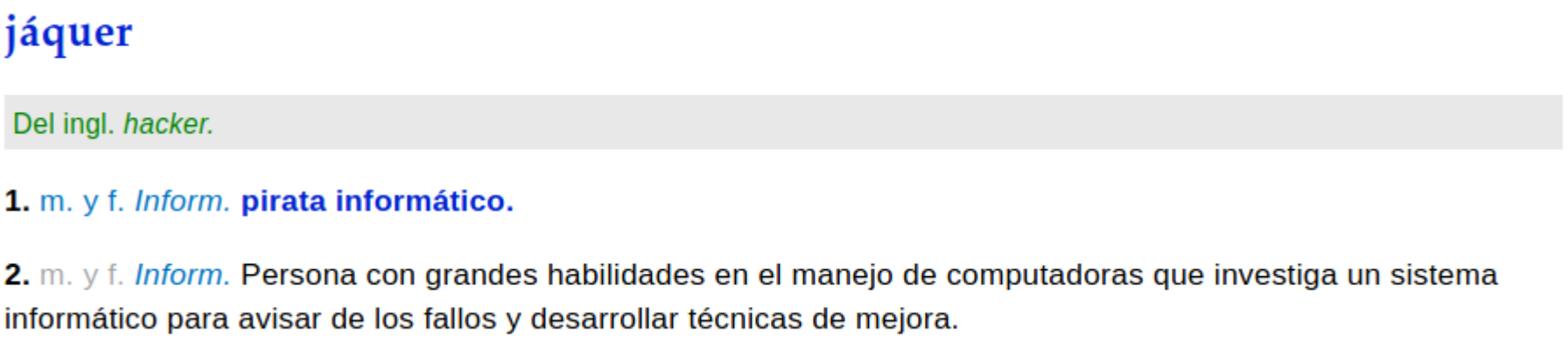
- Otros principios de la seguridad informática:
  - **Autenticación**. Se garantiza la identidad del creador del mensaje. Se consigue usando factores de autenticación.
  - **No repudio**. No se puede negar que el mensaje ha sido enviado por el emisor (**no repudio de origen**) y/o recibido por el destinatario (**no repudio de destino**).

Conceptos básicos

- Medidas de seguridad. Atendiendo al momento de la actuación:
  - **Seguridad activa**. Aquellas medidas que tratan de prevenir algún daño en un sistema informático.
  - **Seguridad pasiva**. Aquellas medidas que tratan de reparar o minimizar un daño que se ha producido en un sistema informático.
- Medidas de seguridad. Atendiendo al elemento que se protege:
  - **Seguridad física**. Aquellas medidas que tratan de proteger el hardware de los sistemas informáticos.
  - **Seguridad lógica**. Aquellas medidas que tratan de proteger el software de los sistemas informáticos.

Conceptos básicos

- ***Hacker*** o **jáquer** según la RAE.
  - **Pirata informático**: “Persona que accede ilegalmente a sistemas informáticos ajenos para apropiárselos u obtener información secreta.”.
  - “Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora.”



jáquer

Del ingl. *hacker*.

1. m. y f. *Inform.* **pirata informático.**

2. m. y f. *Inform.* Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora.

Conceptos básicos

- **Código penal**: Artículos 197 a 201.
  - **Art. 197bis.1**: "El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años."
  - **Art. 197.bis.2**: "El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses."

Conceptos básicos

- **Código penal**: Artículos 197 a 201.
  - **Art. 197bis.1**: "El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos conte ismo o se mant le quien tenga el leg a de prisión de se
  - **Art. 1** ios o instru ado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses."

IMPRESCINDIBLE

AUTORIZACIÓN Y CONTRATO

Conceptos básicos

GRAVE VULNERABILIDAD/

El Ministerio de Justicia denuncia al hacker que descubrió el fallo en LexNET

El Ministerio de Justicia, con Rafael Catalá a la cabeza, ha decidido denunciar al joven hacker que a finales de julio desveló una de las vulnerabilidades más graves jamás descubierta en el sistema informático que usa la Justicia.

Tipos de hacker

Gray Hats

Who work for both, offensively and defensively

White Hats

Security analyst, or individuals with hacking skills using them for defensive purpose

Black Hats

Hacker with malicious and destructive activities with extraordinary skills (Crackers)

Script Kiddies

Unskilled hackers, hacking systems using tools made by real hackers

HACKER

Suicide Hackers

They are those who aim for destruction without worrying about punishment

Hacktivist

Hackers promoting political agenda traditionally by defacing or disabling websites

State Sponsored Hackers

Security analyst, or individuals with hacking skills using them for defensive purpose

Cyber Terrorists

Skilled, motivated by religious or political beliefs attacking on large scale to create fear

Tipos de intrusos y motivaciones

- ***Cracker***. Buscan provocar daños y obtener beneficios de forma ilegal. Ligado a los años 80 cuando desarrollaban *cracks* y *keygens* para el software propietario.
- ***Phreaker***. Acceso a Internet a través de redes telefónicas (*blue boxes*).
- ***Spammer***. Envío masivo de emails.
- ***Lamers*** ("*wannabes*"): *script-kiddies*. Usan herramientas obtenidas de Internet sin tener conocimientos técnicos.
- **Personal interno** (*insiders*). Pueden causar daños de forma voluntaria o involuntaria.
- **Ex-empleados**. Pueden actuar como venganza.
- **Pirata**. Pirateo de software y otros.
- **Escritor de virus**. Escriben virus informáticos como pasatiempo o para obtener beneficios económicos o sabotear sistemas.

Códigos dañinos (*malware*)

- ***Malware*** (*malicious software*): programa desarrollado para causar daños o introducirse de forma no autorizada en algún sistema informático.
- **Técnicas de propagación** que emplean.
  - Tiendas de aplicaciones móviles.
  - Usar software que se sabe activará el antivirus (activador de Windows, Spotify pirata).
  - Ficheros comprimidos con contraseña.
  - ***Stegomalware***. El malware oculto en un fichero aparentemente legítimo se reconstruye dinámicamente.
  - ***Fileless*** o ***in-memory*** malware. Solo existe en la memoria en tiempo de ejecución, no se distribuye en ficheros ni se almacena en el disco duro del sistema, por lo que el análisis forense posterior es muy complicado.

Stegomalware en APTs modernos. Técnicas y contramedidas. Charla de Alfonso Muñoz en las XIV Jornadas STIC del CCN-CERT

https://youtu.be/hGhufb2C_7Y

Códigos dañinos (*malware*)

- Podemos clasificar los virus en función de sus características:
  - ***Exploit***. Aprovecha las vulnerabilidades del software para comprometer el sistema. La acción maliciosa que realiza el exploit es lo que se conoce como ***payload***.
  - **Virus**. Su código se acopla en un programa legítimo y cuando se ejecuta, el código dañino se replica en otros programas y ficheros del ordenador.
  - ***Ransomware***. Una vez infecta los sistemas, encripta la información relevante y solicita un rescate para recuperar la información.
  - ***Spyware***. Su acción consiste en recopilar la actividad que realiza el usuario para enviarla al ciberdelincuente.
  - ***Adware***. Normalmente inocuo o inofensivo pero molesto, que consiste en mostrar anuncios y publicidad de forma constante, a través de lo cual los ciberdelincuentes obtienen beneficio económico.
  - **Troyanos**. Programas aparentemente inofensivos que tienen oculto un código malicioso.
  - ***Rootkits***. Un tipo de troyano que facilitan el control del sistema informático con privilegios de administración.
  - ***Keylogger***. Registra todas las teclas que se han pulsado en el sistema.
  - **Gusanos**. Programas que se autopropagan por las redes de ordenadores infectando a todos los equipos conectados a ellas.
  - **Bacterias**. Son programas diseñados para consumir la memoria del sistema creando múltiples copias de sí mismo.
  - **Bombas lógicas**. Programa que permanece oculto hasta que se cumplen las condiciones predefinidas para su activación.
  - ***Cryptojacking***. Su propósito es el minado de criptomonedas aprovechando el hardware de los equipos infectados.

Códigos dañinos (*malware*)

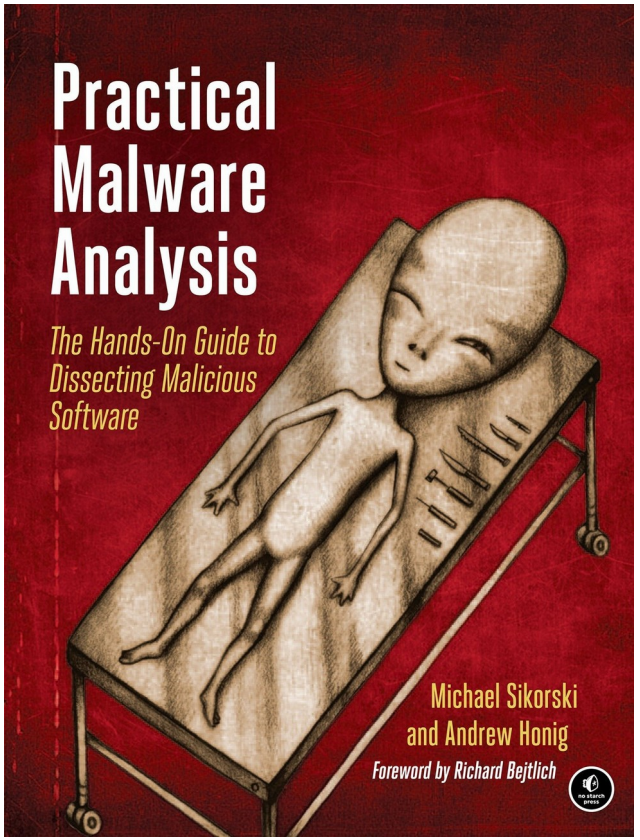
- Algunos de los virus más famosos de la historia.
  - **Brain** (1986). Considerado el primer virus difundido fuera de un laboratorio. Desarrollado en Pakistan infectaba el sector de arranque de los disquetes.
  - **Stoned** (1987). Otro virus pionero, infectaba el sector de arranque del disco duro.
  - **Jerusalem** (1987). También conocido como “Viernes 13” ya que se desencadenaba en esa fecha. Borraba los ficheros que infectaba.
  - **Gusano de Morris** (1988). Provocó que toda la red ARPANET colapsara ya que ralentizaba los ordeandores infectados y conectados a la misma.
  - **Michelangelo** (1992). Infectaba el sector de arranque de los disquetes y el MBR y actuaba el 6 de marzo, el aniversario del nacimiento del pintor y escultor.
  - **Concept** (1995). Primer virus de macro de Office.
  - **Laroux y AccesiV** (1998). Primeros virus de macro de Excel y Access respectivamente.
  - **Strange Brew** (1998). Primer virus desarrollado en lenguaje Java.
  - **Chernobyl o CIH** (1999). Virus que formateaba el disco duro y podía ocasionar daños en el hardware ya que intentaba reescribir la BIOS del equipo.
  - **Melissa** (marzo de 1999). Consiguió infectar 4 millones de ordenadores en 3 días. Se propagaba a través del correo electrónico.
  - **Loveletter o I Love You** (mayo de 2000). Escrito en VB Script, infectó a 40 millones de ordenadores en tan solo 6 horas.
  - **Stuxnet** (septiembre de 2010). Una de las primeras armas para la guerra cibernética. Infectaba sistemas y procesos críticos aprovechando hasta 4 vulnerabilidades “zero-day”.
  - **Wannacry** (mayo de 2017). Ransomware que infectó unos 200.000 dispositivos en pocas horas. El ataque se detuvo gracias a la activación del interruptor de parada del malware, descubierto por Marcus Hutchins y que consistía en el registro de un dominio de Internet.

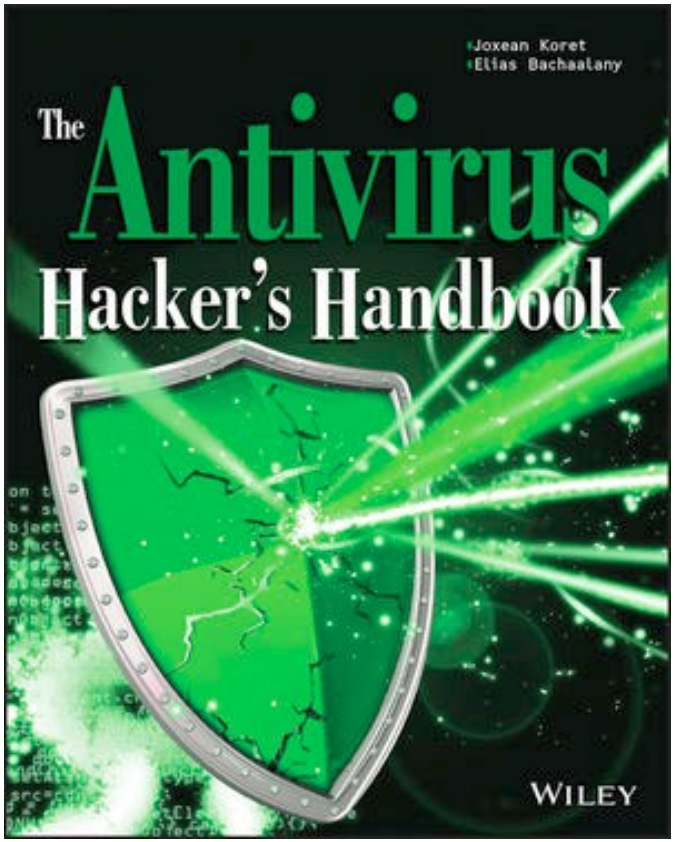
Códigos dañinos (malware)

- **Análisis de malware**. Es uno de los trabajos de un experto en ciberseguridad.
  - **Any.Run** es un servicio online para el análisis dinámico de malware, empleando *sandboxes*.
  - **Malvuln** es un proyecto que busca descubrir vulnerabilidades en el malware.
  - El proyecto **VX-Unnderground** publica el código fuente de todo tipo de malware, junto a artículos de investigación.
  - **REMnux** es una distribución específica basada en Linux para análisis de malware.

Códigos dañinos (malware)

Análisis de malware. Es uno de los trabajos de un experto en ciberseguridad.





Tipos de ataques

- Guía de Ciberataques de la OSI.
- **Ataques a contraseñas**.
  - Fuerza bruta.
  - Ataque por diccionario.
- **Ataques por ingeniería social**.
  - *Phishing*, *Vishing* y *Smishing*.
  - *Baiting* o Gancho (ejemplo: *clickbait*).
  - *Shoulder surfing* (mirando por encima del hombro).
  - *Dumpster Diving* (rebuscando en la basura).
  - *Spam* (correo no deseado).
  - Fraudes online.

Tipos de ataques

- **Ataques a las conexiones**.
  - Ataques DDoS (*Distributed Denial of Service*).
  - Ataque de intermediario (*Man in the Middle,* MitM).
  - Ataques de suplantación (*Spoofing*).
    - *IP Spoofing*.
    - *Web Spoofing*.
    - *Email Spoofing*.
    - *DNS Spoofing*.
  - Escucha de conexiones (*sniffing*).
  - Redes trampa (Wifi falsas – *RogueAP*).

https://www.genbeta.com/seguridad/google-cloud-bloquea-mayor-ataque-ddos-historia-tres-veces-mayor-que-record-establecido-hace-justo-ano

Tipos de ataques

- **Ataques por malware**.
  - Virus.
  - *Adware* o anuncios maliciosos.
  - *Spyware* (software espía).
  - Troyanos (*backdoors*, *keyloggers*, *stealers*, *ransomware*).
  - Gusano.
  - *Rootkit.*
  - *Botnets* (redes zombi).
  - *Rogueware* o el falso antivirus.
  - *Criptojacking*.
  - Apps maliciosas.

Tipos de ataques

- **Ataques a la cadena de suministro** (*supply chain*).
  - Buscan vulnerar los sistemas de un tercero que pertenece a la cadena de suministro del objetivo principal.
  - La corporación objetivo confía en los productos que adquiere de ese proveedor y las revisiones de seguridad que realiza sobre estos son escasas o nulas.
  - Hackeo de **SolarWind**, una empresa de desarrollo de software proveedora de importantes agencias gubernamentales de EE.UU, en su software Orion que usa más de 18.000 empresas.
  - Las medidas para evitar este tipo de ataques van encaminadas a implantar lo que se conoce como **Zero Trust Security**, o seguridad de confianza nula, cuyo concepto principal es "***nunca confiar, siempre comprobar***".

https://csrc.nist.gov/News/2022/planning-for-a-zero-trust-architecture-white-paper

Tipos de ataques

- **Ataques invisibles en el código fuente** (*trojan source*).
  - Aprovecha una vulnerabilidad de los compiladores en el tratamiento que hacen de los caracteres de control Unicode
  - Hacen que el código sea reordenado por el compilador, por lo que el comportamiento final del programa es distinto al esperado.

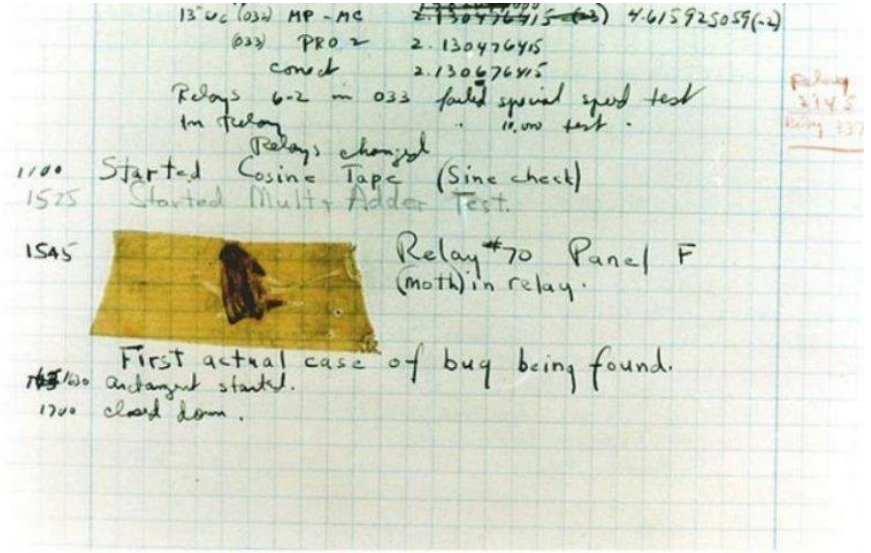
```
public class TrojanSource {
    public static void main(String[] args) {
        String accessLevel = "user";
        if (accessLevel != "userRLO LRI// Check if adminPDI LRI") {
            System.out.println("You are an admin.");
        /* end admin only RLO { LRI*/
    }
}
```

```
public class TrojanSource {
    public static void main(String[] args) {
        String accessLevel = "user";
        if (accessLevel != "user") { // Check if admin
            System.out.println("You are an admin.");
        }
    }
}
```

https://trojansource.codes/

Vulnerabilidades

- Primer fallo informático: el 9 de septiembre de 1945 en el laboratorio de cálculo de la U.de Harvard. Grace Murray Hopper trabajaba como programadora del ordenador Mark II cuando intentaba averiguar la causa de un fallo.
- Descubrió que era debido a la presencia de una polilla, un bicho(***bug***).



Vulnerabilidades

- **Vulnerabilidades en el software**.
  - Errores de programación en el código fuente.
  - Fallos de configuración.
  - Agujeros intencionados o ***backdoors***.
  - Ocurren a todos los niveles del sistema informático (un elemento vulnerable compromete todo el sistema): servidor web, aplicación web, librería de terceros (***log4shell***, ***spring4shell***).
  - Una vez en el sistema, si el S.O. no está actualizado el atacante puede escalar privilegios (***pwnkit***, ***hivenightmare***).
  - Errores en el uso de la criptografía (***zerologon***).

https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

Vulnerabilidades

- **Vulnerabilidades en el hardware**.
  - ***Meltdown*** y ***Spectre*** aprovechan una vulnerabilidad en la ejecución fuera de orden y en la ejecución especulativa del código en los procesadores.
  - ***Retbleed***, una vulnerabilidad en el sistema ***retpoline*** diseñado para proteger los ataques de *Spectre*.
  - ***Rowhammer***, afecta a memorias DDR DRAM y que permite modificar bits de la memoria.
  - Vulnerabilidades en consolas de videojuegos (***FreeHDBoot***, ***FreeDVDBoot***).

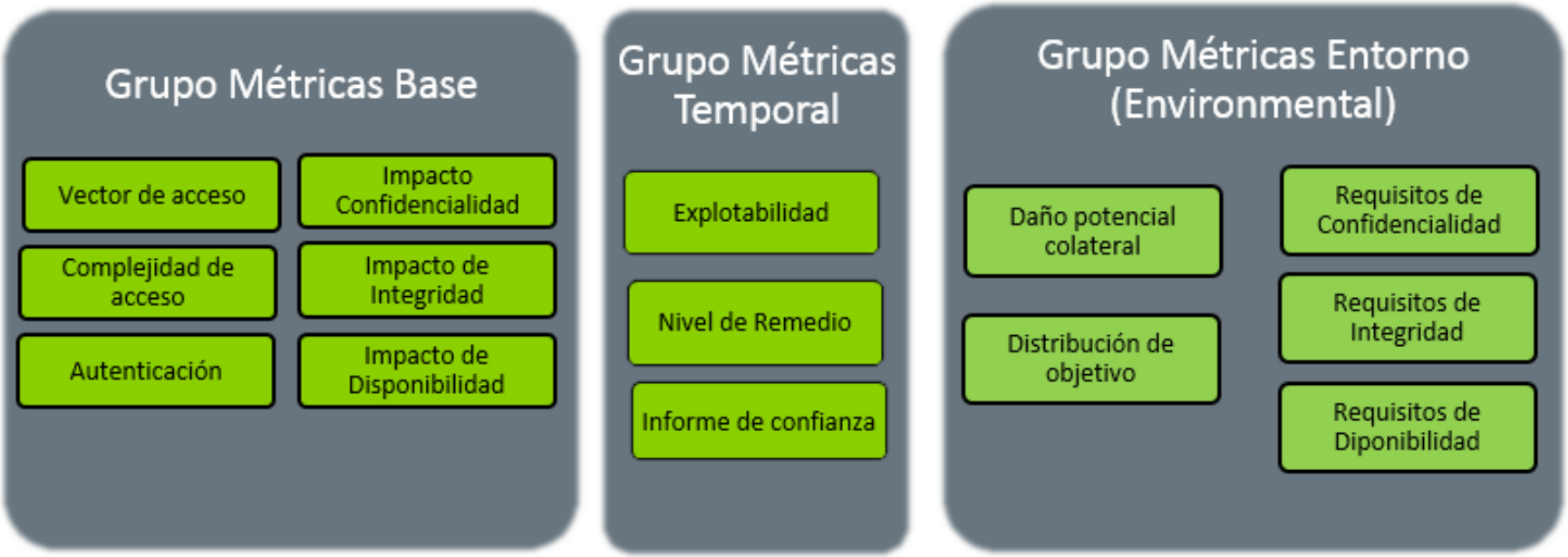
https://meltdownattack.com/

Documentación de vulnerabilidades

- **CVE** (*Common Vulnerabilities and Exposures*). Provee una lista para identificar vulnerabilidades de seguridad a las que se le asigna un número. Ej: CVE-2014-0160.
- **CVSS** (*Common Vulnerability Scoring System*). Sistema de puntuación que valora la gravedad de una vulnerabilidad.
- **CWE** (*Common Weakness Enumeration*). Lista de fallos o debilidades software/hardware que permite identificarlas y clasificarlas.

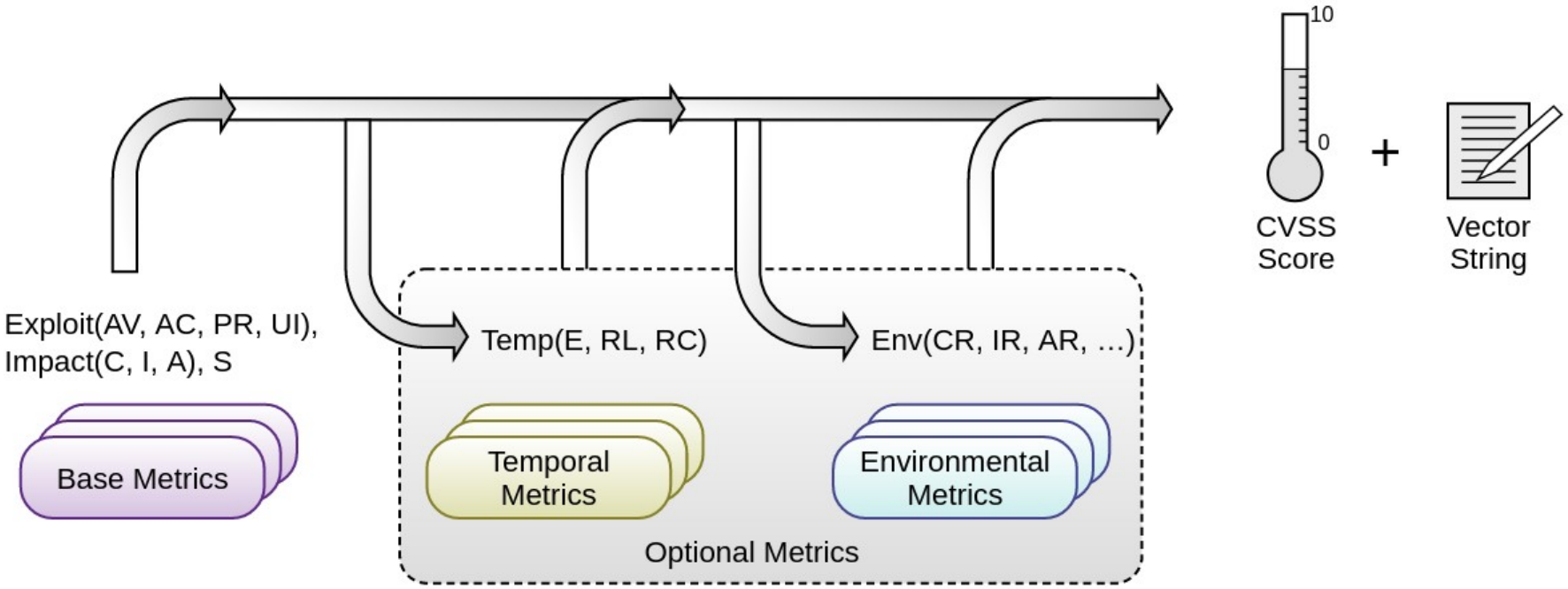
Documentación de vulnerabilidades

- Metodología para el cálculo del CVSS



Documentación de vulnerabilidades

- Metodología para el cálculo del CVSS



Documentación de vulnerabilidades

Elementos de la calculadora CVSS 3.1.

Grupo Base:

Access Vector (AV). Valores: [L,A,N] (Local, Adjacent, Network
Access Complexity (AC). Valores [H,M,L] (High, Medium, Low)
Authentication (Au). Valores [M,S,N] (Multiple, Single, None)
Confidenciality Impact (C) . Valores [N,P,C] (None, Partial, Complete)
Integrity Impact (I). Valores [N,P,C] (None, Partial, Complete)
Availability Impact (A). Valores [N,P,C] (None, Partial, Complete)

Grupo Temporal:

Exploitability (E). Valores: [U,POC,F,H,ND] (Unproven, Proof-of-Concept, Functional Exploit, High, Not Defined)
Remediation Level (RL). Valores: [OF,TF,W,U,ND] (Official Fix, Temporary Fix, Workaround, Unavailable, Not Defined)
Report Confidence (RC). Valores: [UC,UR,C,ND] (Unconfirmed, Uncorroborated, Confirmed, Not Defined)

Grupo Entorno Usuario:

Collateral Damage Potential (CDP). Valores: [N,L,LM,MH,H,ND] (None, Low, Low Medium, Medium High, High, Not Defined)
Target Distribution (TD). Valores: :[N,L,M,H,ND] (None, Low, Medium, High, Not Defined)
Security Requirements (CR, IR, AR). Valores: [L,M,H,ND] (Low, Medium, High, Not Defined)

Tipos de auditoría

- **Auditoría de caja negra**.
  - Permite al auditor tomar el rol de un hacker que no conoce ninguna característica del interior de la organización.
  - Se comienza recopilando todo tipo de información (pública) sobre el objetivo → ***Information Gathering***.
- **Auditoría de caja blanca**. Se asume el rol de un usuario interno de la organización con acceso parcial o total a los sistemas internos o críticos de la misma.
  - Revisión de sistemas, configuraciones, políticas…
  - Permite el uso de herramientas de automatización.
- **Auditoría de caja gris**. Se dispone de una visión limitada del interior de la organización sin acceso a sistemas o recursos críticos.

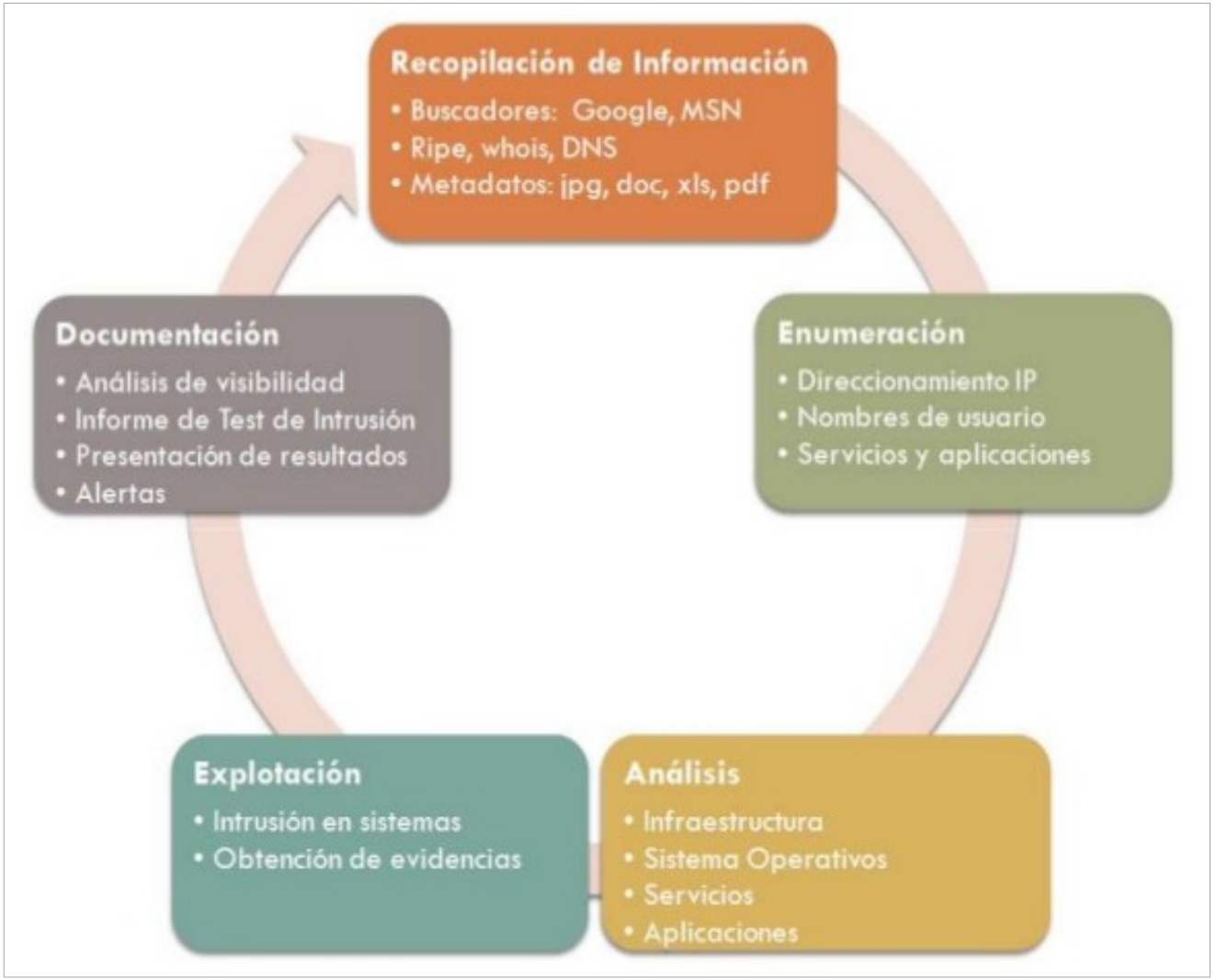
Tipos de auditoría

- **Auditoría perimetral**. Permite conocer el estado de seguridad del perímetro. El objetivo es obtener acceso a la red interna.
- **Auditoría interna**. Proporcionan información del estado de seguridad de los distintos segmentos de la red. El auditor toma el rol de un empleado que trabaje en uno de los segmentos o de un invitado que se conecta a la red corporativa.
- **Auditoría interna con privilegios**. El auditor dispone de privilegios para comprobar configuraciones, revisar código fuente...

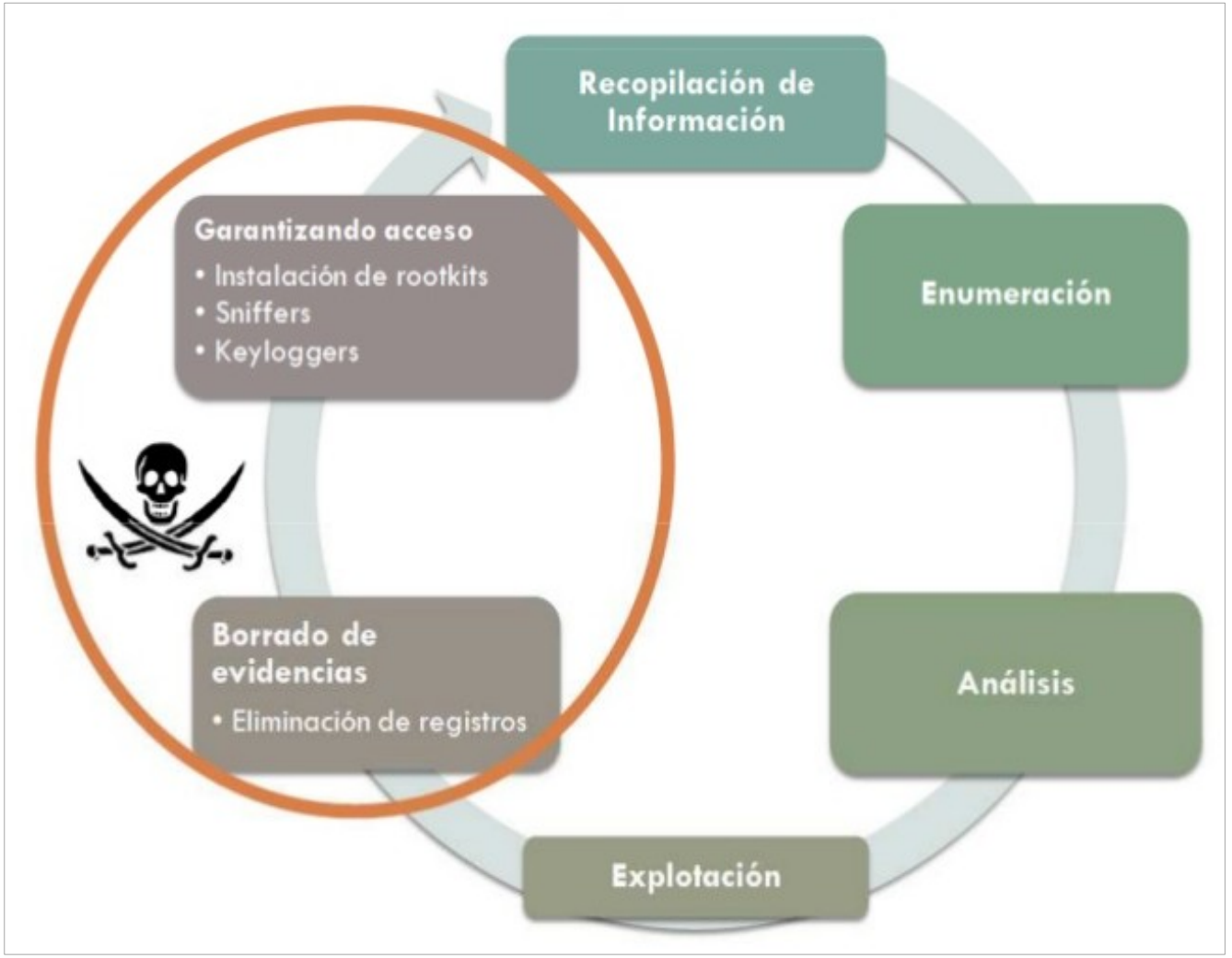
Tipos de auditoría

- **Auditoría web**. Evalúa la seguridad de la web. Puede ser de forma externa sin permisos (perimetral), con permisos de un usuario con credenciales (interna) o auditando el código fuente (caja blanca).
- **Auditoría de aplicaciones móviles**. Permite conocer el grado de seguridad de las apps de la empresa. Se puede realizar a diferentes niveles como en el caso de la web.
- **Auditoría wireless y VOIP**. Permite conocer el estado de seguridad de las comunicaciones inalámbricas y de voz.
- **Prueba de estrés DoS/DDoS**. Se evalúa la fortaleza de la infraestructura ante situaciones de alta carga.

Fases de un pentest



Fases de una intrusión



Metodologías de pentesting

- Estándares y modelos (Penetration Testing Methodologies).
  - OSSTMM (*Open Source Security Testing Methodology Manual*).
  - OWISAM (*Open Wireless Security Assesment Methodology*).
  - Guías del OWASP:
    - WSTG (*Web Security Testing Guide*).
    - MSTG (*Mobile Security Testing Guide*).
    - *Firmware Security Testing Methodology*.
  - PTES (*Penetration Testing Execution Standard*).
  - PCI DSS (*Payment Card Industry Data Security Standard*).
  - PTF (*Penetration Testing Framework*).
  - *Techinical Guide to Information Security Testing and Assessment* y el *CyberSecurity Framework* del NIST.
  - CAF (*Cyber Assement Framework*).

Metodologías de pentesting

- OSSTMM (***Open Source Security Testing Methodology Manual***).
  - Manual libre y gratuito desarrollado por el ISECOM (*Institute for SECurity and Open Methodologies*).
  - 15 capítulos donde se explican cómo llevar a cabo las pruebas de auditoría en distintos ámbitos (humana, física, wireless, redes…).

Metodologías de pentesting

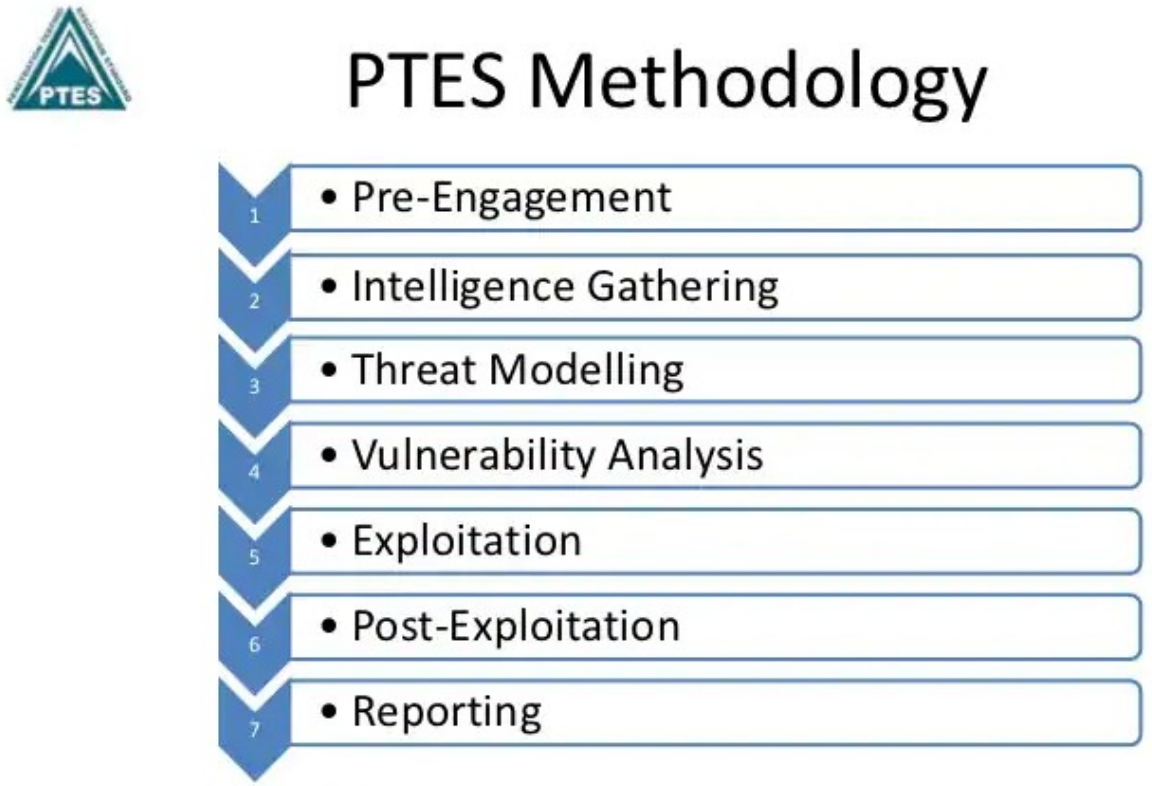
- OWISAM (***Open Wireless Security Assesment Methodology***).
  - Objetivo: “poner en común con la comunidad los controles de seguridad que se deben verificar sobre redes de comunicaciones inalámbricas y definir una metodología abierta y colaborativa que ayude a administradores de redes, administradores de sistemas y a analistas de seguridad informática a identificar riesgos, a minimizar el impacto de los ataques informáticos y a garantizar la protección de las infraestructuras Wireless basadas en el estándar 802.11”.

Metodologías de pentesting

- **OWASP** (*Open Web Application Security Project*). Es un proyecto de código abierto dedicado a determinar las vulnerabilidades en el software
  - ***Web Security Testing Guide***. Guía para auditar aplicaciones y servicios web. El OWASP Top 10 recoge las 10 vulnerabilidades más frecuentes localizadas en auditorías.
  - ***Mobile Security Testing Guide***. Guía para la auditoría de seguridad de aplicaciones móviles y la ingeniería inversa de estas.

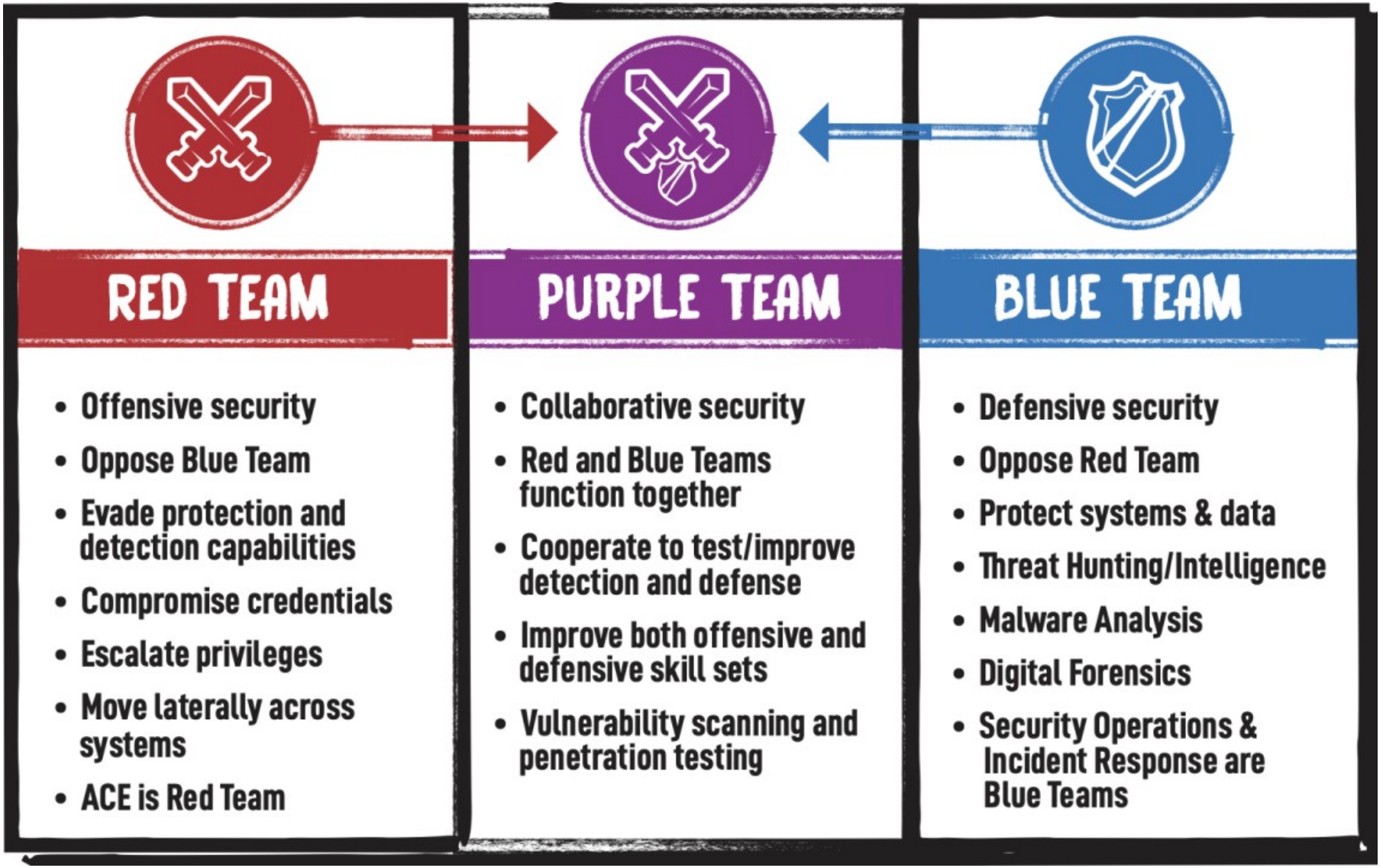
Metodologías de pentesting

- **PTES** (*Penetration Testing Execution Standard*).

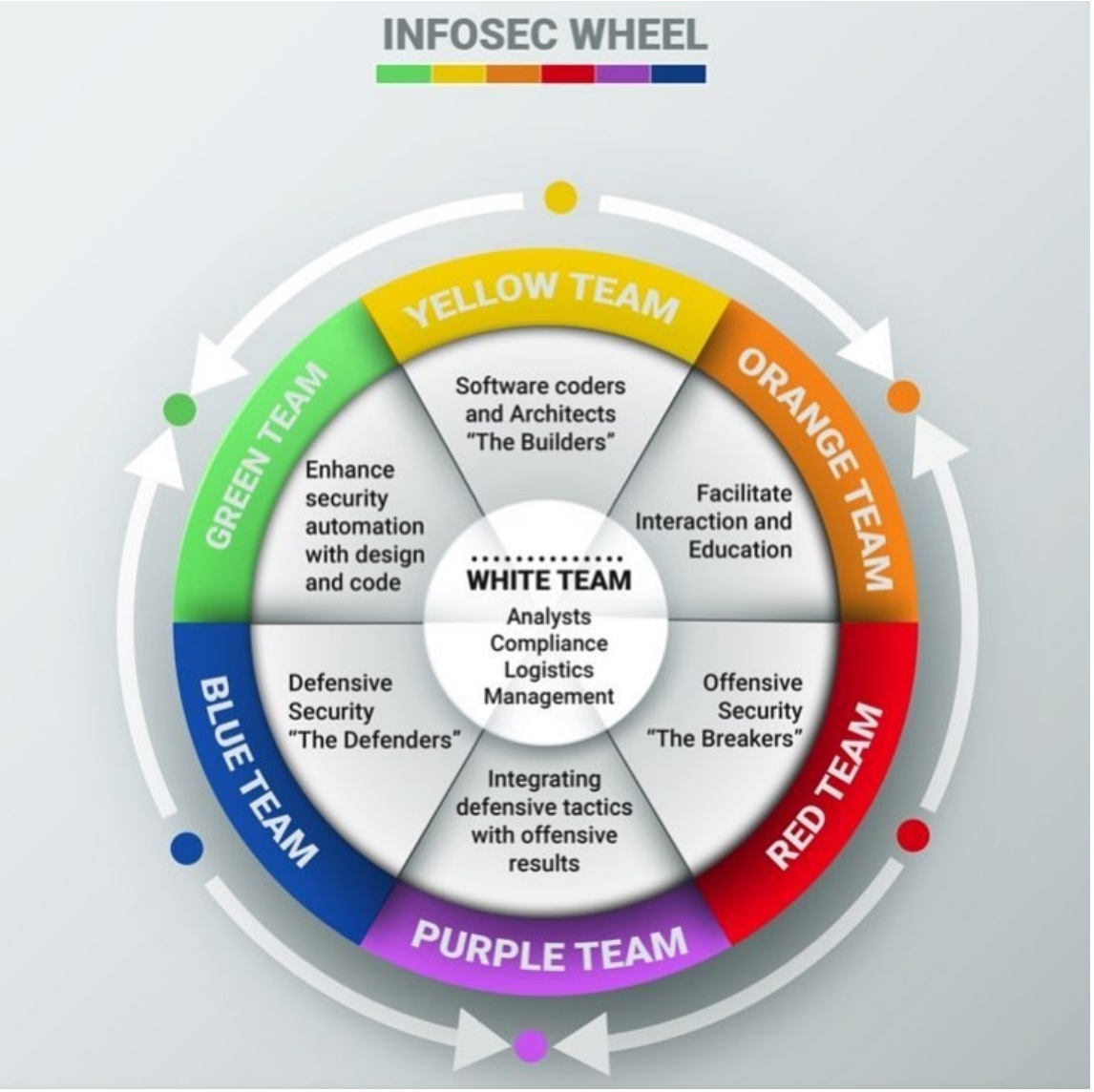


Equipos de seguridad

Equipos de seguridad



Equipos de seguridad



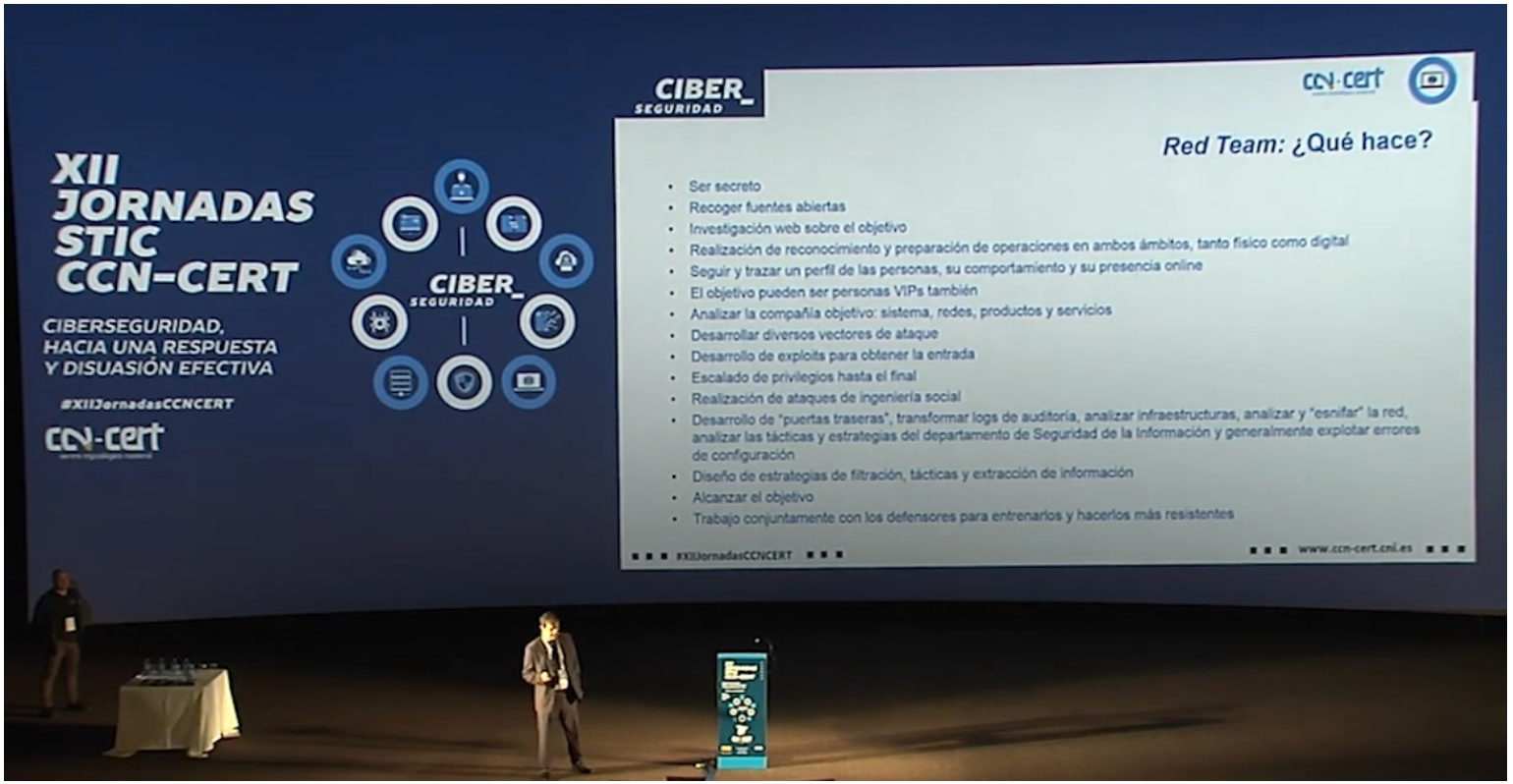
Pentesting vs Red Teaming

- A menudo ambos términos se confunden o se usan indistintamente pero hay diferencias importantes.
  - **Pentest**: Orientado a una acción concreta sobre un objetivo en un tiempo reducido.
  - **Red Team**:
    - Ejercicio continuo y constante que trata de probar las defensas del objetivo evitando ser descubiertos. Conlleva un proceso de planificación y actuación a más largo plazo.
    - Emula el *modus operandi* de grupos organizados (matriz de Tácticas, Técnicas y Procedimientos de Mittre Att&ck).

Pentesting vs Red Teaming

XII JORNADAS STIC CCN-CERT

Red Team como herramienta de protección frente APTs (Layakk)
https://www.youtube.com/watch?v=IJoi-hjS8Koç



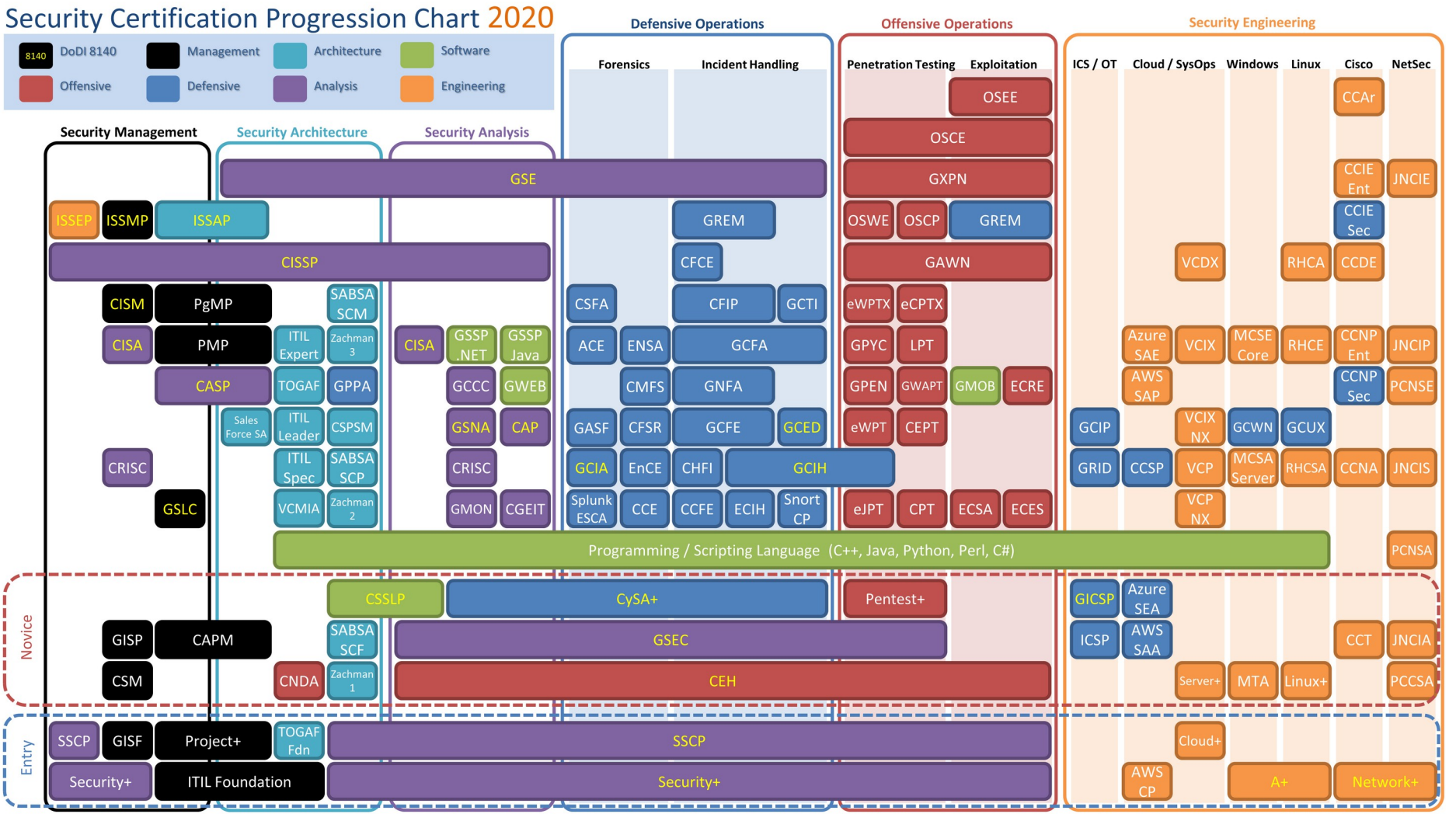
Perfil de un buen hacker

https://johnjhacking.com/blog/the-oscp-preperation-guide-2020/

Perfil de un buen hacker

- **Conocimientos técnicos avanzados** de:
  - Administración de sistemas operativos.
  - Redes de ordenadores y protocolos de red.
  - Lenguajes de programación y scripting.
  - Arquitecturas de computadores y ensamblador.
- **Otras cualidades** o habilidades:
  - Capacidad investigadora y de autoaprendizaje.
  - Comunicación, dominio de idiomas.
  - Escritura y documentación, políticas de seguridad.

Certificaciones de seguridad



https://www.reddit.com/r/cybersecurity/comments/e23ffz/security_certification_progression_chart_2020/

CTF (Capture The Flag)

- Los retos basados en CTF son una herramienta poderosa para el aprendizaje de las diferentes técnicas y disciplinas del hacking.
- Se realizan en entornos de prueba controlados organizados a modo de competición o por hobby.
- Categorías:
  - **Jeopardy**. Conjunto de retos de diferentes tipos que otorgan una serie de puntos tras su resolución (encontrar la flag o bandera) en función del nivel de dificultad de cada ejercicio. La resolución de unos retos libera otros para seguir avanzando en la competición y cuando termina el tiempo estipulado, gana quien ha acumulado más puntos.
  - **Ataque y defensa**. Cada equipo de participantes tiene un servidor/red con vulnerabilidades que debe proteger para que el equipo contrario no consiga acceder. Se dan puntos tanto de ataque como de defensa y gana el equipo que logre mejor puntuación.
  - **Mixto**. Wargame, hardware y otros.

CTF (Capture The Flag)

- Tipos de retos:
  - **Análisis Forense [Forensics]**: Lo más común; imágenes de memoria, de discos duros o capturas de red, las cuales almacenan diferentes tipos de información.
  - **Criptografía [Crypto]**: Textos cifrados mediante un criptosistema determinado.
  - **Esteganografía [Stego]**: Imágenes, sonidos o vídeos que ocultan información en su interior.
  - **Explotación [Pwn]**: Descubrimiento de vulnerabilidades en un servidor.
  - **Ingeniería Inversa [Reversing]**: Inferir en el funcionamiento del software. Lo más común, binarios de Windows y Linux.
  - **Programación [PPC]**: También conocidos como PPC (*Professional Programming & Coding*), desafíos en los que se requiere desarrollar un programa o script que realice una determinada tarea.
  - **Web**: Descubrimiento de vulnerabilidades en una aplicación Web.
  - **Reconocimiento [Recon]**: Búsqueda de la bandera en distintos sitios de Internet. Para resolverlo se ofrecen pistas, tal como el nombre de una persona.

CTF (Capture The Flag)

- Plataformas para realizar CTFs:
  - **CTF Time**. Plataforma en la que se anuncian diferentes eventos donde hay CTFs y Write Ups.
  - Root me. Sitio de entrenamiento con diversos retos adaptados por niveles para probar las habilidades en hacking.
  - Hack me. Es un sitio web donde cada usuario puede colgar sus aplicaciones web vulnerables, un proyecto destinado a fines educativos o de investigación.
  - Wechall. Sitio con retos y enlaces a otras web de CTFs.
  - Una al mes. Un reto mensual by Hispasec.
  - Atenea. Plataforma creada por el CCN-CERT. Tiene retos además de una "academia" para aprender sobre las distintas disciplinas.
  - PicoCTF. Plataforma de la Universidad Carnegie Mellon enfocada a retos para alumnado de secundaria pero con retos interesantes y de diferentes niveles.
  - Hack The Box. Plataforma con laboratorios para practicar pentesting.
  - Try Hack Me. Similar a Hack The Box, con laboratorios guiados enfocados al aprendizaje.

CTF (Capture The Flag)

- CTFs prestigiosos:
  - **Defcon CTF** (Order-of-Overflow).
  - **PlaidCTF** (Plaid Parliament of Pwning).
  - **0ctf** (Tencent y Keenlabs).
  - **Google CTF** (Google).
  - **C3CTF** (Chaos Computer Club).

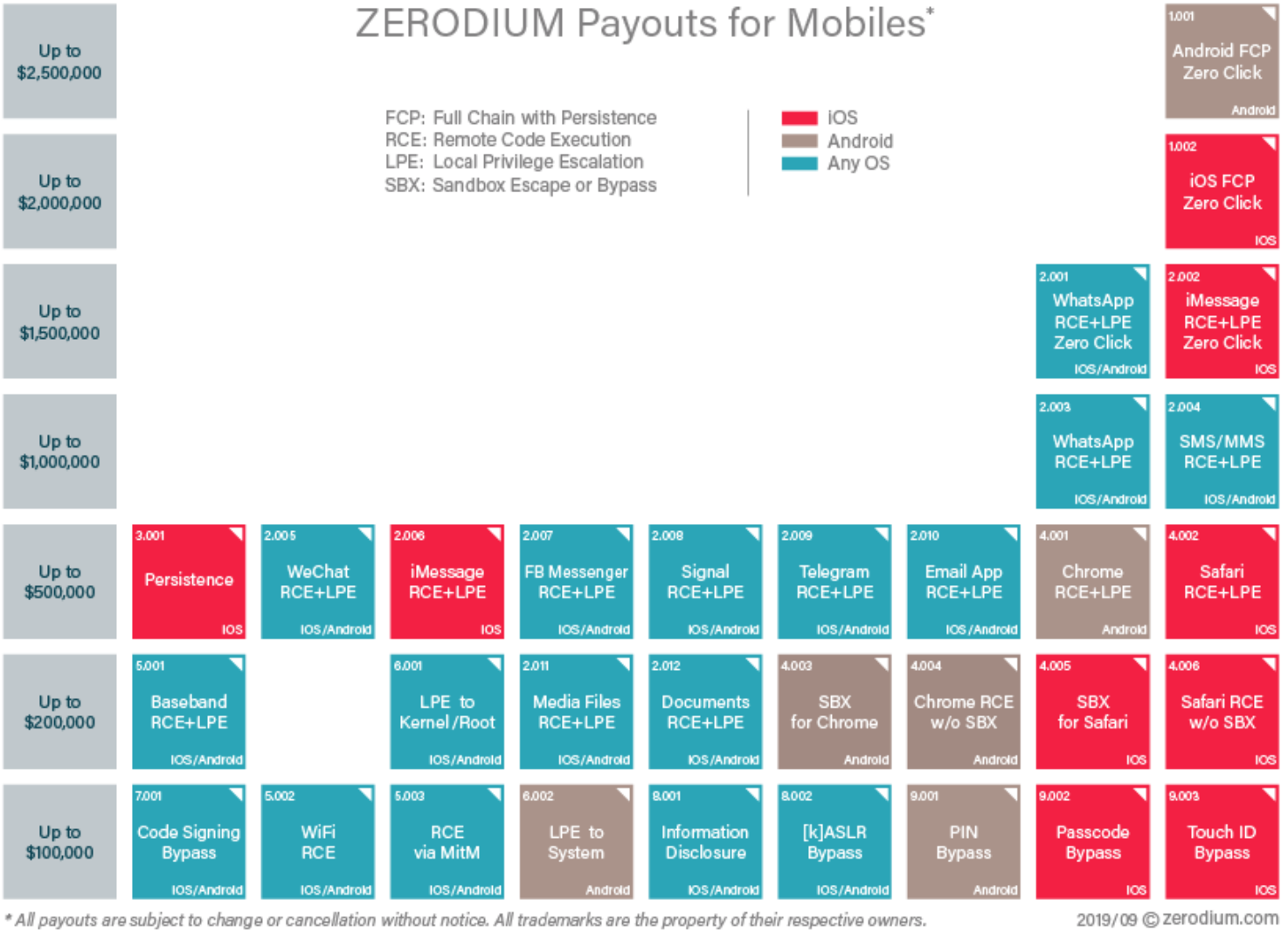
CTF (Capture The Flag)

- Plataformas para organizar y crear CTFs:
  - **CTFd**. https://github.com/CTFd/CTFd
  - **Mellivora**. https://github.com/Nakiami/mellivora
  - **Facebook CTF**. https://github.com/facebookarchive/fbctf

Bug bounty (cazarecompensas)

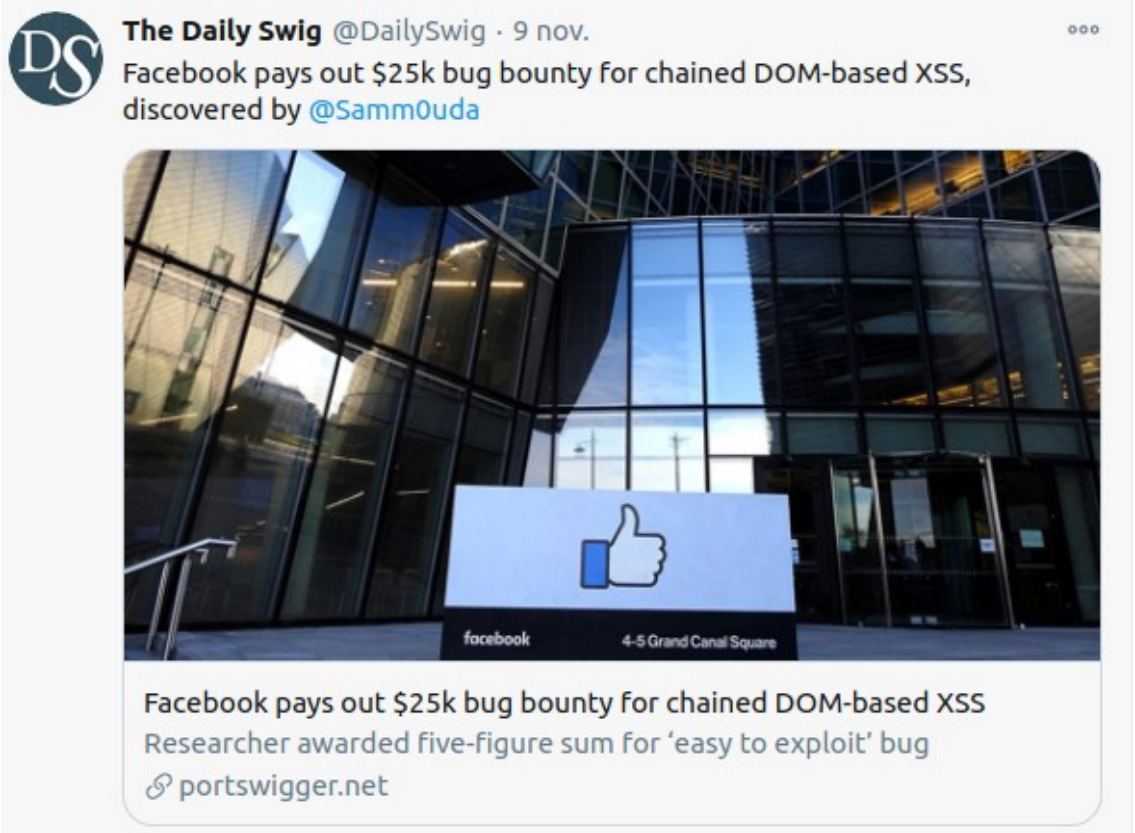
- Programas de recompensas a través de webs en las que empresas, fabricantes, etc., pagan una cantidad económica por reportar bugs.
- Plataformas más importantes:
  - Bugcrowd.
  - Hackerone.
  - Zerodium.
  - Zero day initiative.
  - Synack.
  - Epic Bounties.
  - Immunefi.
  - Intigriti.

Bug bounty (cazarecompensas)



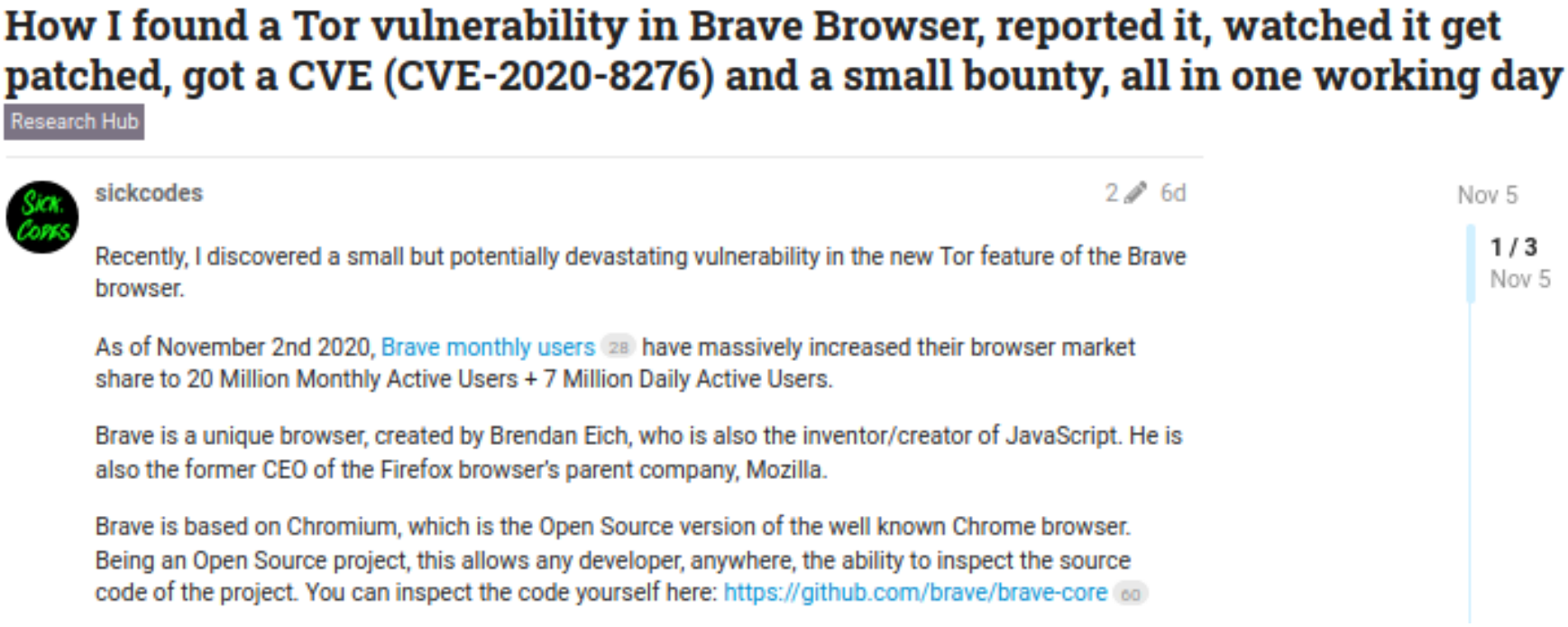
Bug bounty (cazarecompensas)

- Un ejemplo real:
  - @Samm0uda - https://ysamm.com/



Bug bounty (cazarecompensas)

- Un ejemplo real:
  - Una vulnerabilidad en el navegador Brave.



How I found a Tor vulnerability in Brave Browser, reported it, watched it get patched, got a CVE (CVE-2020-8276) and a small bounty, all in one working day

Research Hub

sickcodes — 2 — 6d — Nov 5

Recently, I discovered a small but potentially devastating vulnerability in the new Tor feature of the Brave browser.

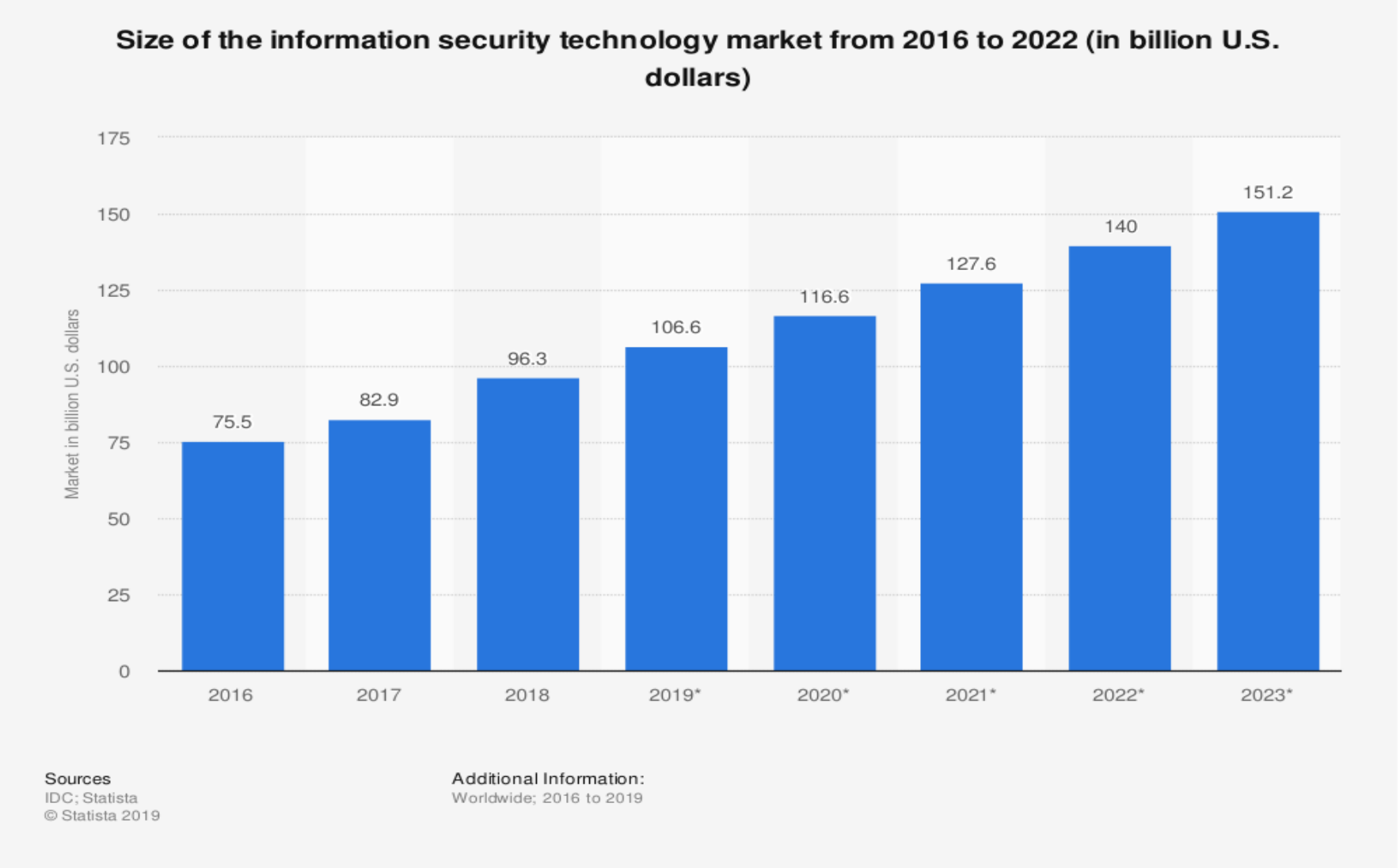
As of November 2nd 2020, Brave monthly users 28 have massively increased their browser market share to 20 Million Monthly Active Users + 7 Million Daily Active Users.

Brave is a unique browser, created by Brendan Eich, who is also the inventor/creator of JavaScript. He is also the former CEO of the Firefox browser's parent company, Mozilla.

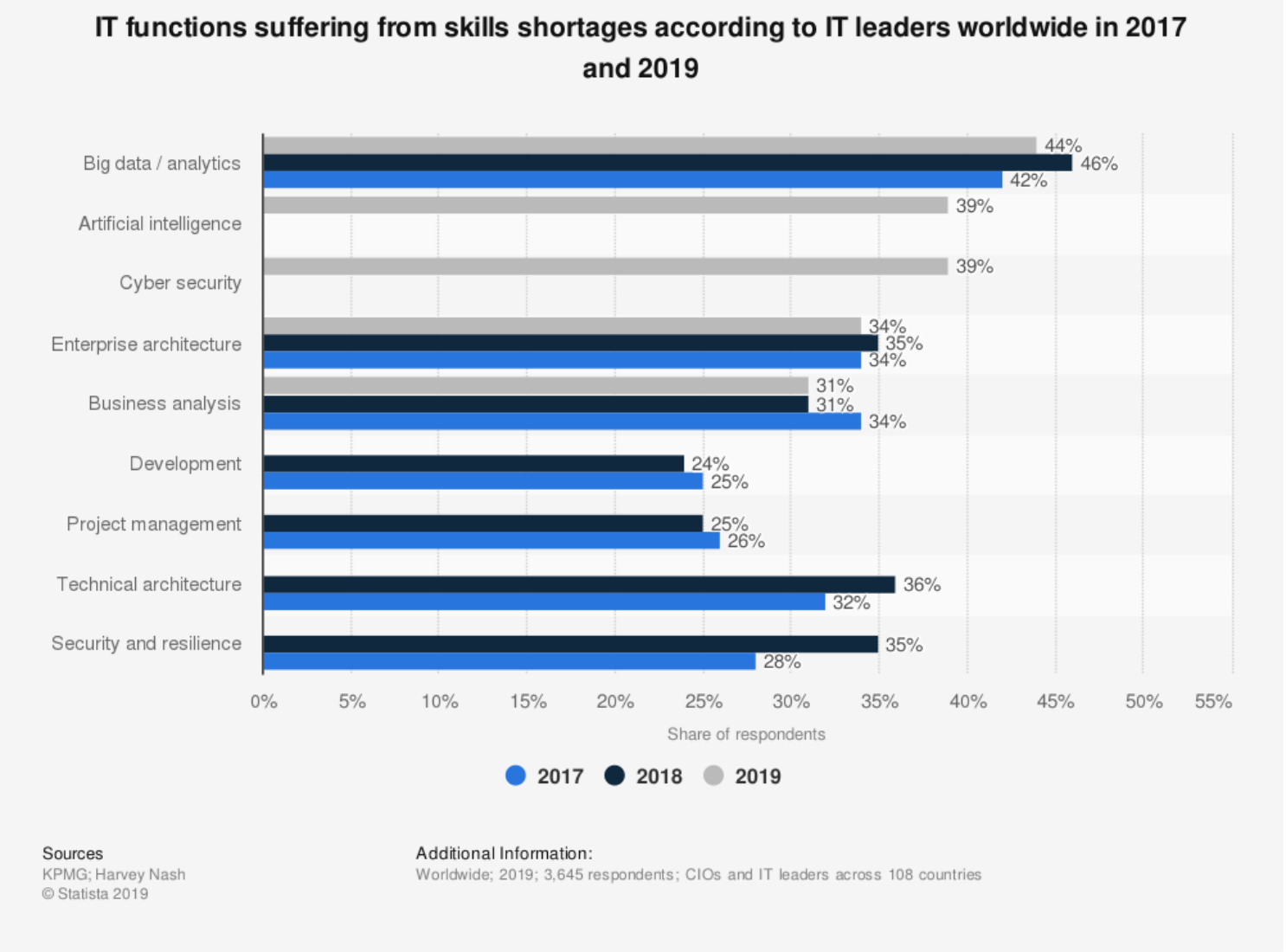
Brave is based on Chromium, which is the Open Source version of the well known Chrome browser. Being an Open Source project, this allows any developer, anywhere, the ability to inspect the source code of the project. You can inspect the code yourself here: https://github.com/brave/brave-core 60

1 / 3
Nov 5

Oportunidades laborales



Oportunidades laborales



Herramientas de hacking

- Distribuciones para hacking:
  - Kali Linux.
  - Parrot Security OS.
  - BackBox.
  - BlackArch.
  - Commando VM.
  - Tails.

Herramientas de hacking

- Laboratorios y máquinas vulnerables:
  - Hack The Box.
  - TryHackMe.
  - HackMyVM.
  - Vulnhub.
  - Metasploitable 2 y 3.
  - OverTheWire WarGames.
  - OWASP Samurai Web Testing Framework.

Introducción al Hacking ético

¿Dudas o preguntas?