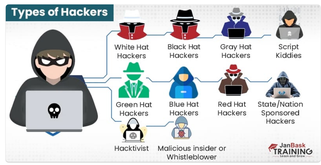
CIBERSEGURIDAD

Hackers

- **White Hat:** son hackers que se apegan a la ética y que trabajan protegiendo sistemas. Generalmente trabajan para empresas de seguridad informática y son contratados para hallar agujeros en los sistemas cibernéticos.
- **Black Hat:** estos hackers o crackers utilizan sus habilidades para romper sistemas de seguridad y entrar a zonas restringidas, infectar redes o apoderarse de ellas; roban identidades, clonan tarjetas, etc. Todo esto para beneficio personal o de terceros, en muchas ocasiones para lucrarse.
- **Grey Hat:** es una mezcla de los anteriores, debido a que puede irrumpir de manera ilegal en los sistemas aunque con buenas intenciones. Pueden penetrar sistemas de seguridad de compañías y luego ofrecer sus servicios para reparar esas fallas. También pueden obtener información relevante de manera ilegal para luego divulgarla a la opinión pública.
- **Blue Hat:** es una persona que trabaja en consultoría informática que presta sus servicios probando los errores de un sistema antes de que sea lanzado al público.
- **Hacktivist:** es una palabra compuesta entre hacker y activista. Hace referencia a la persona que presenta una posición social, ideológica o política usando la tecnología. Un ejemplo claro de hacktivismo es el grupo conocido como Anonymous.
- **Script-kiddie:** es un tipo de hacker que carece de habilidades técnicas y que busca obtener beneficios de un hackeo sin tener los conocimientos para realizarlo. En este grupo también están los noobs o newbies, los novatos en el hackeo con poco conocimiento del mundo de la tecnología. La diferencia está en que los script-kiddies hacen cibervandalismo, propagan software malicioso y no se preocupan por funcionamiento interno de los sistemas.



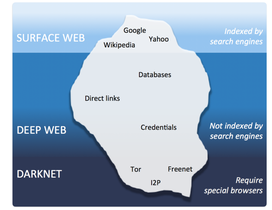
WHOIS

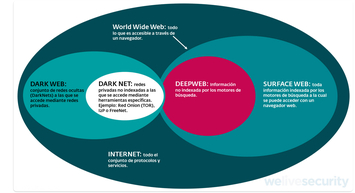
Es un protocolo TCP sirve para efectuar consultas y saber el propietario de un nombre de dominio o una dirección IP en Internet.
Las consultas WHOIS se suele realizar a través de una utilidad para línea de comandos (terminal o consola)

Ciberataque

Es un **ataque** para destruir, eliminar o para obtener acceso sin autorización o utilizar un activo.
Un **ciberataque** o **ataque informático** es cualquier maniobra ofensiva de explotación deliberada que tiene como objetivo tomar el control, desestabilizar o dañar un sistema informático.

Deep Web, Dark Web y Darknet





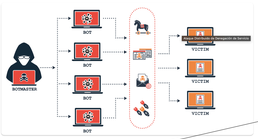
Tipos de amenazas según sus efectos:

Interceptación (escucha o monitorización).
Denegación del servicio (interrupción).
Modificación (manipulación o alteración).
Suplantación (impostura o fabricación).

Surface Web : **Internet tal cual lo conocen la mayoría de los cibernautas**, la web a la que cualquiera puede acceder fácilmente desde cualquier navegador.

DEEP WEB Está disponible, pero **a la que NO puedes acceder de forma pública**. Por una parte, pueden tratarse de páginas convencionales que han sido protegidas por un PAYWALL, pero también archivos guardados en DROPBOX o CORREOS ELECTRÓNICOS.
La componen sitios con un "Disallow" en el archivo robots.txt. Supone el **90%** de la www.

Dark Web : Forma parte de la Deep Web. Sólo se puede acceder mediante aplicaciones específicas.
La porción de Internet que **está intencionalmente oculta a los motores de búsqueda**, usa direcciones IP enmascaradas y es accesible sólo con un navegador web especial. Supone el **0,1 % de la www.**



Ejemplos de debilidades que explota un atacante:

- Obtiene datos del proveedor a través de Whois, como la fecha de caducidad y envía un correo malicioso de renovación de dominio para obtener datos.
- Seguimiento en redes sociales para obtener información, hacer *pishing* mediante ingeniería social...
- Servicios inseguros: Telnet
- Ataques DoS y DDoS con redes zombie
- Redirigir DNS
- Formularios y logins: CAPTCHA y honeypod.

CAPTCHA

Qué es Telnet

El nombre de Telnet proviene del acrónimo **Telecomunication Network**, y básicamente un **protocolo de red TCP/IP** que es utilizado desde 1960 para **establecer conexiones remotas con otros ordenadores**, servidores, y dispositivos con un sistema compatible en el acceso mediante este sistema de comunicación. De forma predeterminada se utiliza el **puerto de conexión 23**.

Además del propio protocolo, **también recibe este nombre el programa que lo utiliza** para establecer la propia conexión. Para acceder a la otra máquina de forma remota, debemos utilizar un terminal, por ejemplo, Símbolo del sistema de Windows, o el Terminal de Linux. De esta forma podremos interactuar en la máquina remota navegando por sus archivos, ejecutando otros comandos internos, si tenemos permiso, y monitorizar el estado de la propia máquina sin la necesidad de ir físicamente al lugar en donde se encuentra.

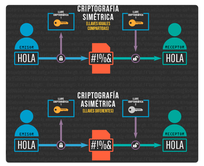
Además de ser utilizado en sistemas MSDOS y Windows, **también es compatible con sistemas Basados en UNIX, como Mac y Linux, y FreeBSD.** Con este protocolo, también seremos capaces de **comprobar la conectividad de otras máquinas** y comprobar si tienen determinados puertos abiertos al exterior. Esto es algo que veremos en un momento.

Telnet es un **protocolo de red TCP/IP** utilizado para **establecer conexiones remotas con otros ordenadores.** De forma predeterminada se utiliza el **puerto de conexión 23**.

¿Qué es un Honeypot?

Tenemos que tener claro que un Honeypot, más conocido como "sistema trampa" o "señuelo", está ubicado en una red o sistema informático para que su objetivo sea evitar un posible ataque al sistema informático.

CRIPTOGRAFIA, CLAVE PUBLICA - CALVE PRIVADA



La criptografía asimétrica

En cuanto al procedimiento, **el destinatario genera ambas claves y comunica la clave pública al emisor** del mensaje quien, por su parte, tiene ahora la opción de cifrar el mensaje.

Una vez que se haya enviado el mensaje, **solo se podrá descifrar con la clave privada**, de manera que si el mensaje cifrado es interceptado, la información del mensaje permanecerá oculta2 . Además, los métodos criptográficos garantizan que esa pareja de claves solo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Protocolo	Publicación
SSL 1.0	No publicado
SSL 2.0	1995
SSL 3.0	1996
TLS 1.0	1999
TLS 1.1	2006
TLS 1.2	2008
TLS 1.3	2018

Seguridad de la capa de transporte

TLS - Seguridad de la capa de transporte
SSL - Capa de puertos seguros

Son protocolos criptográficos, que proporcionan comunicaciones seguras por una red (internet).

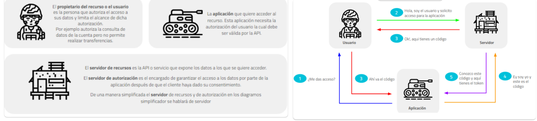
Que es OpenID

Que es OpenID

- Estándar de identificación digital descentralizado
- Puede ser verificado por cualquier servidor que soporte el protocolo
- A diferencia de otras arquitecturas Single Sign-On, OpenId no especifica el mecanismo de autenticación.
- Solo necesitan disponer de un identificador creado en un servidor que verifique OpenID,
- Autenticación de Perfil Simple (Single Profile Authentication)
  - One ID, aceptado en cualquier lugar
- Un protocolo
  - Like HTTP, no es un API
- Un estandar abierto
  - Código abierto, Nadie es propiertario (pero tiene una Fundación que prove un framework legal)

Que es OAuth

Open Authorization es un estándar abierto que permite flujos simples de autorización para sitios web o aplicaciones informáticas



¿Qué es la autenticación multifactor - AMF

La autenticación multifactor es un método de autenticación electrónica en el que se requieren dos o más factores (p.ej. una contraseña y una huella dactilar) para que un usuario tenga acceso a una página web o aplicación.
Estos factores pueden ser de conocimiento (algo que el usuario pueda saber), de características inherentes (algo que el usuario pueda ser) o de posesión (algo que el usuario pueda tener). La MFA está diseñada para ser más segura que un simple inicio de sesión utilizando un identificador y una contraseña, protegiendo al usuario del robo de identidad y del fraude.

ORGANISMOS

Conoce INCIBE
INSTITUTO NACIONAL DE CIBERSEGURIDAD

INCIBE trabaja para afianzar la confianza digital, elevar la ciberseguridad y la resiliencia y contribuir al mercado digital de manera que se impulse el uso seguro del ciberespacio en España.

El Instituto Nacional de Ciberseguridad de España (INCIBE), anteriormente Instituto Nacional de Tecnologías de la Comunicación, es una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.

Con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE contribuye a construir ciberseguridad a nivel nacional e internacional.

Que es un Token

Qué es un token y cómo funciona
www.hiveblockchain.com

Diferencia Entre Tokens Y Criptomoneda
criptoton.com

Qué es un token

Un token es un **objeto físico o digital** que **tiene valor en cierto contexto o para determinada comunidad**, aunque su propia materialidad no contenga ese valor en sí.

Las **fichas de casino**, por ejemplo, son solo pedazos de plástico de distintos colores, pero **representan cantidades de dinero**. Algunas, hasta millones de dólares, aunque fabricar una de ellas cueste apenas centavos.

Eso hacen los tokens: **representan otra cosa, están en su lugar**. ¿Por qué? Hay muchos motivos: la **comodidad**, la **seguridad**, la **facilidad de transportarlos o transferirlos**.

En el mundo cripto, los tokens se generan a partir de piezas de **código de programación**, en formato de **smart contracts** que corren sobre la **blockchain**. Estos "contratos inteligentes" son porciones de código de computadoras que determinan **las reglas o el funcionamiento de una herramienta o de una plataforma cripto**.

Tokens y criptomonedas

En 2009, cuando fue creada por Satoshi Nakamoto, **Bitcoin se convirtió en la primera criptomoneda**. De inmediato, muchos otros entusiastas de la seguridad digital, las nuevas economías y los desarrollos tecnológicos se lanzaron a crear las suyas propias.

Una de ellas fue **Ethereum**, creación del joven programador ruso Vitalik Buterin, una red que entre otras cosas permite que que distintas personas, organizaciones o empresas puedan crear **sus propias criptomonedas, sus propios tokens**, sus propias maneras de **medir valor en un proyecto cripto**. Fue recién entonces que **token** se convirtió en un concepto popular en el mundo cripto.

Actualmente, **token y criptomoneda son utilizados como sinónimos**. En definitiva, **ETH** es el token de Ethereum, **BTC** el de Bitcoin y **DAI** el de MakerDAO. Sin embargo, en la distinción señala que **las criptomonedas tienen blockchain propia**, mientras que los tokens se emiten en otra blockchain, como Ethereum.

Además, tené en cuenta que existen otros tipos de tokens cripto que no son criptomonedas. El ejemplo más obvio son los **NFT, literalmente "tokens no fungibles"**, un formato que te permite obtener **desde coleccionables hasta arte digital o personajes de videojuegos**.

Estándares de tokens

- **ERC-20:** se trata del estándar más popular. Son tokens fungibles (es decir que se pueden intercambiar entre ellos) e implementan una API para su desarrollo a través de smart contracts. Este estándar permite la interacción de los smart contracts y las DApps, facilitando la creación de un ecosistema interoperable.
- **ERC-721:** es el estándar más utilizado para la creación de **NFT**. Este estándar permite implementar características únicas a cada unidad, haciendo que sean únicos y no se puedan cambiar por otro.
- **ERC-1155:** Se trata de un tipo de token que puede mezclar las características de los tokens ERC-20 y de los ERC-721.
- **SLP:** el estándar nativo del ecosistema Solana. Este tiene una característica única y es que suelen ser compatibles con los de estándares ERC-20 y ERC-721.
- **BEP-20**: este es el estándar de Binance Smart Chain (BSC) y ofrece un framework flexible para el desarrollo de utility tokens, stablecoins y hasta NFT.
- **TRC-10 y TRC-20:** este el estándar nativo de la red Tron, con capacidad multi-smart contract y algunas características únicas como bajas tarifas de gas o la interoperabilidad.
- **ERC-20 Waves:** se trata de una versión del estándar de Ethereum desarrollada por Waves para la elaboración de aplicaciones descentralizadas de nivel empresarial. Ofrece capacidades de interoperabilidad con diferentes protocolos y exchanges.
- **NEP-5:** este es el estándar de los tokens nativos de la blockchain NEO. Este estándar tiene una particularidad y es que todos los tokens contribuyen de alguna forma al desarrollo y ampliación del ecosistema NEO.

Estándar de tokens ERC – Qué son y qué tipos hay.
blog.bitpanda.com/es/estandar-tokens-erc-que-son-y-que-tipos-hay/