Desmitificando a los hacker

<<@BySepa 2022>>

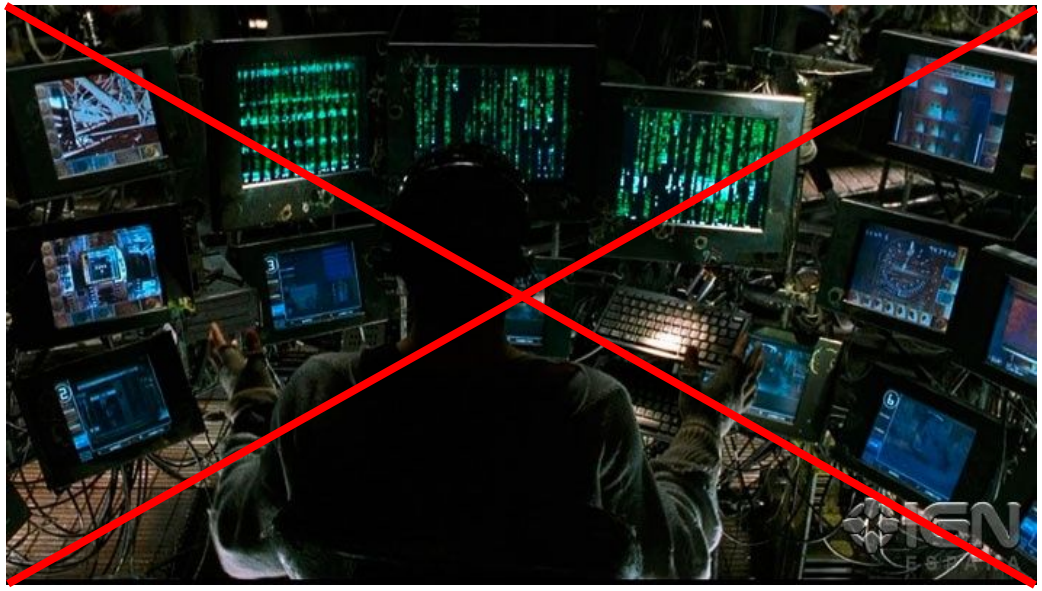
<<@BySepa 2022>>

¿QUIENES SON?

Un ***hacker*** es alguien que descubre las vulnerabilidades de una computadora o un sistema de comunicación e información, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas. Los hackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta o por el desafío.

Wikipedia.org

La realidad hacker



Fuente: Matrix

Fuente: Mr. Robot

Los hackers

“Los hackers son buenos, los crackers son malos”

– Un amigo de Sepa

“El Cracker” “El Hacktivista” “El Hacker”

Los hackers

Tipos:

- **Informáticos** >> Esta presentación va orientada a ellos <<
- Electrónicos -de hardware-
- Radioaficionados -señales de radio-
- De telecomunicaciones -enlaces punta a punta, wifi, etc.-
- Ingeniería Social -estudian a las personas y sus defectos-
- Sistemas de seguridad físicos -cámaras, molinetes, tarjetas de acceso, etc.-
- Industriales -petróleo, plantaciones, gas, agua, electricidad, etc.-
- IOT -heladeras, lavarropas, microondas, etc.-
- Políticos / activistas -actividades basadas en ideales-
- Medios de pagos -tarjetas-
- etc.

Cinematografía

- Antitrust.
- Cypher.
- Eagle Eye.
- Enemigo público.
- Firewall.
- **Hackers.**
- **Juegos de guerra.**
- La Red.
- La Red 2.0.
- Live Free or Die Hard.
- **Matrix.**
- **Piratas de Silicon Valley**
- Sneakers.
- **Swordfish.**
- Take Down.
- Tron: Legacy.
- Untraceable.
- Weird Science.
- **Mr Robot.**
- CSI: Cyber.

¿Cómo te inicias en el mundo hacker?

Lo **primero**, y lo que yo creo fundamental, es el preguntarse ¿porque? ¿como?

- ¿porque esta aplicación hace esto?.
- ¿que pasa si cuando esta web me pide mi número de dni le pongo caracteres especiales?.
- ¿como viajan los datos de mi computadora hasta el servidor).
- ¿como anda el wifi?

Lo **segundo**, y no por eso menos fundamental, leer y experimentar

- Casi todo está en Internet.
- Participar en grupos.
- Armar laboratorios o entornos de prueba. No solo software, también investigar el hardware.
- Jugar en sitios como Hack The Box donde nos dan desafíos.
- Hacer cursos, certificaciones o una carrera universitaria acorde.

Lo **tercero**, no aflojar y estar todo el tiempo actualizando

- Leer noticias todos los días, para poder adelantarse a lo que puede venir.
- Buscar nuevas metodologías de explotación.
- Compartir con los demás las cosas que aprendemos.

¿De qué trabajan los hackers?

Un hacker puede trabajar de cualquier cosa, pero casi siempre se lo relaciona a los siguientes trabajos:

- Ciberseguridad
  - RedTeam / Seguridad ofensiva
  - BlueTeam / Seguridad defensiva / SOC
  - CSIRT
  - Ciberinteligencia
  - Pentesters
- Seguridad informática / de la información
  - Gobierno de datos
  - Arquitectura de seguridad
  - Operaciones de seguridad
- Networking / Telecomunicaciones
- IT
  - Administración
  - Soporte
- Desarrollo

¿De qué trabajan los hackers?

En empresas u organizaciones los hackers se los relaciona a tres áreas:

- Ciberseguridad
- Seguridad Informática o de la información
- Auditoría

¿Cuales son las tareas habituales de un hacker?

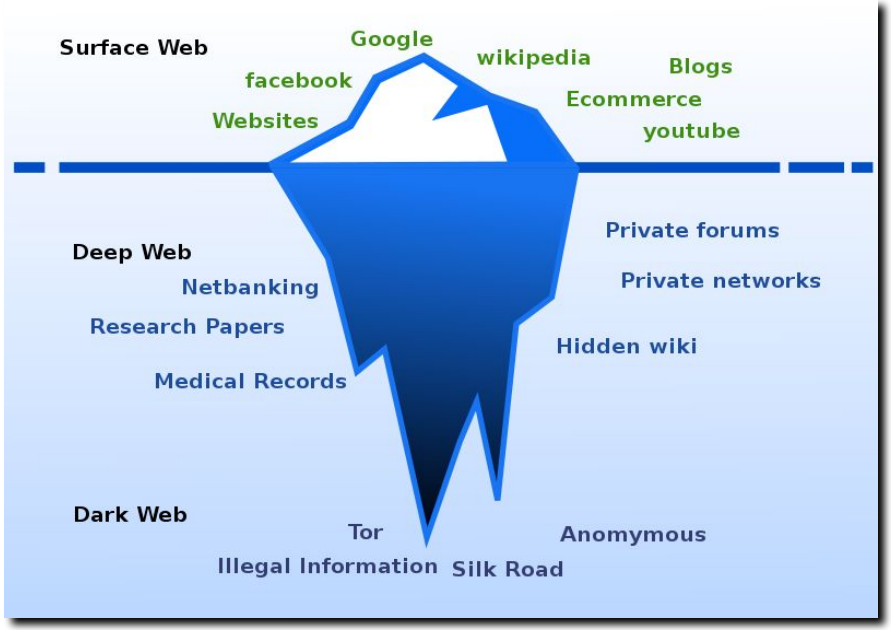
En la mayoría de los casos las empresas contratan hackers para algunas tareas tales como la investigación de incidentes de seguridad, el descubrimiento de vulnerabilidades sobre aplicaciones o infraestructura, la resolución y el seguimiento de vulnerabilidades conocidas, la realización de políticas y procedimientos de seguridad para todos los empleados de la empres u organización, seguridad defensiva (alarmas de seguridad, logs, etc.), operaciones de seguridad (Antivirus, Firewall, WAF, IPS/IDP, Escudo anti-DDoS, etc.) y más…

¿En qué tipo de empresas contratan hackers?

Suelen ser empresas u organizaciones de cualquier finalidad grandes, también existen empresas medianas o chicas pero en este caso es cuando dichas empresas su negocio es la Ciberseguridad.
Las grandes consultoras (las llamadas Big4) son grandes empleadores de hackers y obviamente todas las empresas relacionadas a Internet (Facebook, Microsoft, RedHat, Claro, Telefónica, AT&T, etc.)

Deepweb & Darkweb

El típico gráfico de Iceberg



Deep

Es la Internet que todos conocemos pero no se indexan sus sitios (no se encuentran los sitios en buscadores).

Dark

Corre sobre Internet y no tiene indexación. Presenta un modelo de seguridad en capas (tipo cebolla).

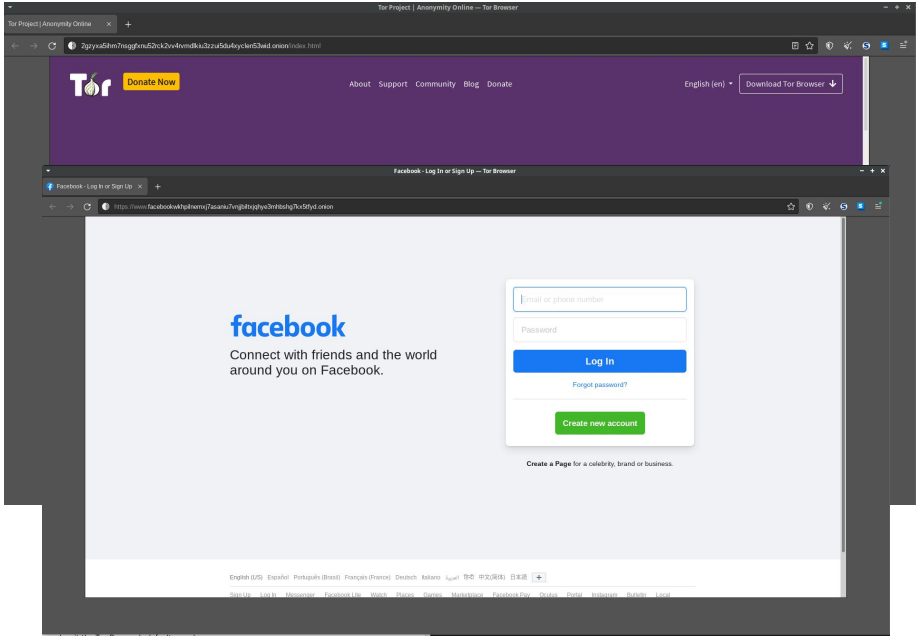
Las redes más comunes:

1. **Freenet - https://freenetproject.org/**
2. **I2P - https://geti2p.net/es/**
3. **Tor - https://www.torproject.org/**
4. ZeroNet - https://zeronet.io/
5. GNUnet - https://gnunet.org/en/

Deepweb y darkweb

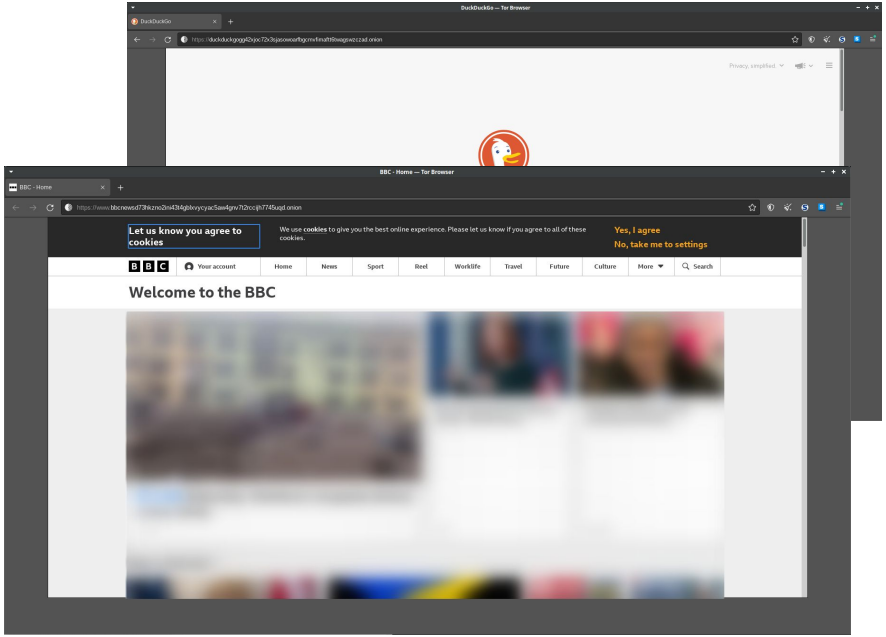
No hay que tenerle miedo, las redes de por si no son malas, todo depende para que se usen.

TorProject http://2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion



Facebook https://www.facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion/

DuckDuckGo https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/



BBC https://www.bbcnewsd73hkzno2ini43t4gblxvycyac5aw4gnv7t2rccijh7745uqd.onion/

¿Dudas ? ¿Preguntas ?

Sitios de interés

- Wikipedia
- Google
- Shodan
- The Hacker News
- Zdnet/Security
- MuySeguridad
- Una al día - Hispasec
- Tor Project
- Incibe
- CISA / NSA
- SecNewsAr - Telegram
- El Blog De Sepa ;)

¡ Gracias por el aguante !

Dudas y consultas por TW: @BySepaTW

Canal de Twitch: @BySepa

Instagram: @BySepa