

Trabajar en ciberseguridad 2023

¿Por dónde empezar?



@kriwarez



@kriware



@kriware

\$> whoami

Cristian ‘kriM’ Cantos

Analista de seguridad en Layakk

Entusiasta de la ciberseguridad, la
tecnología e Internet

Amante de memes

Staff RootedCON

En mi tiempo libre (casi nunca) subo
videos a YouTube

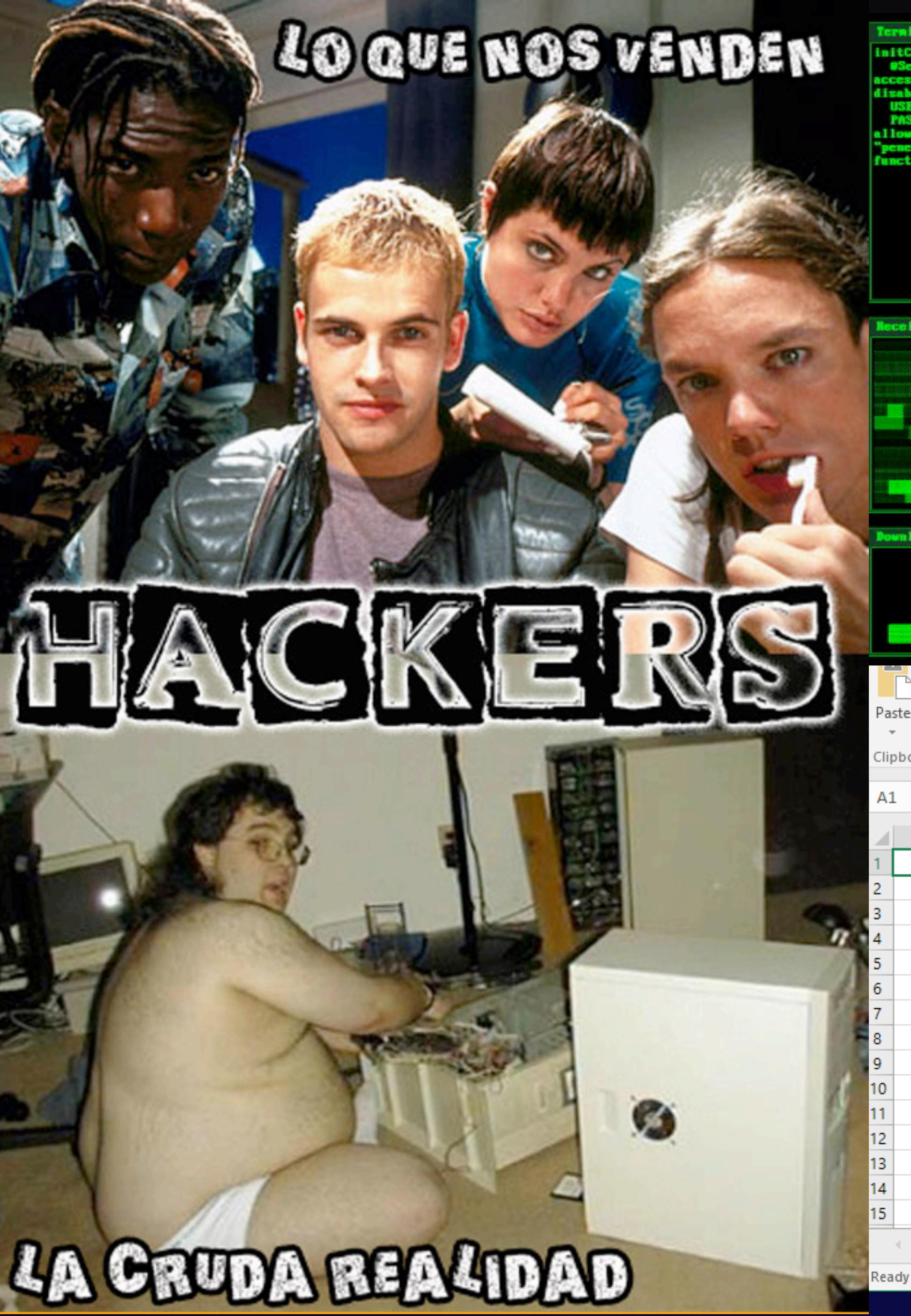


Disclaimer

Todos los recursos aquí son GRATUITOS

Son recursos para gente que empieza

TODO lo que voy a comentar ¡es mi punto de vista!



The image shows a Microsoft Excel spreadsheet titled "Final". The content of the spreadsheet consists of several windows from a penetration testing or network monitoring application. These windows include:

- A terminal window showing connection details to a server at 32.3.211.0.
- A "Directory" window listing files in a directory structure under "storage": models, contestperiod.exe, ctrl.exe, entry.bin, fb.init, report_bug.ad, user.exe, routes, error.ad, info.bin, submit.exe, and crack.
- A "Transfer" window showing a file transfer progress bar with a speed of 604MB/s and a timestamp of 15:47:0.
- A "Compiler" window displaying a grid of characters (A-Z, 0-9, symbols) in a hex-like format.
- A "Access" window with a large "PERMISSION" watermark.
- A "Crash" window showing a pixelated error screen.
- A "Load" window showing a progress bar for "Downloading Critical Data" at 77%.
- A "Script" window listing various modules: Process, crack.exe, buffer, trans.exe, cache, and penet.
- A "Countdown" window showing a green progress bar.
- An "Upload" window showing a blank area for file upload.

The Excel ribbon and toolbar are visible at the top, and the standard Excel grid is visible below the windows.



MUCHO POR APRENDER



TODAVÍA TIENES

Requisitos Hardware



Requisitos Hardware

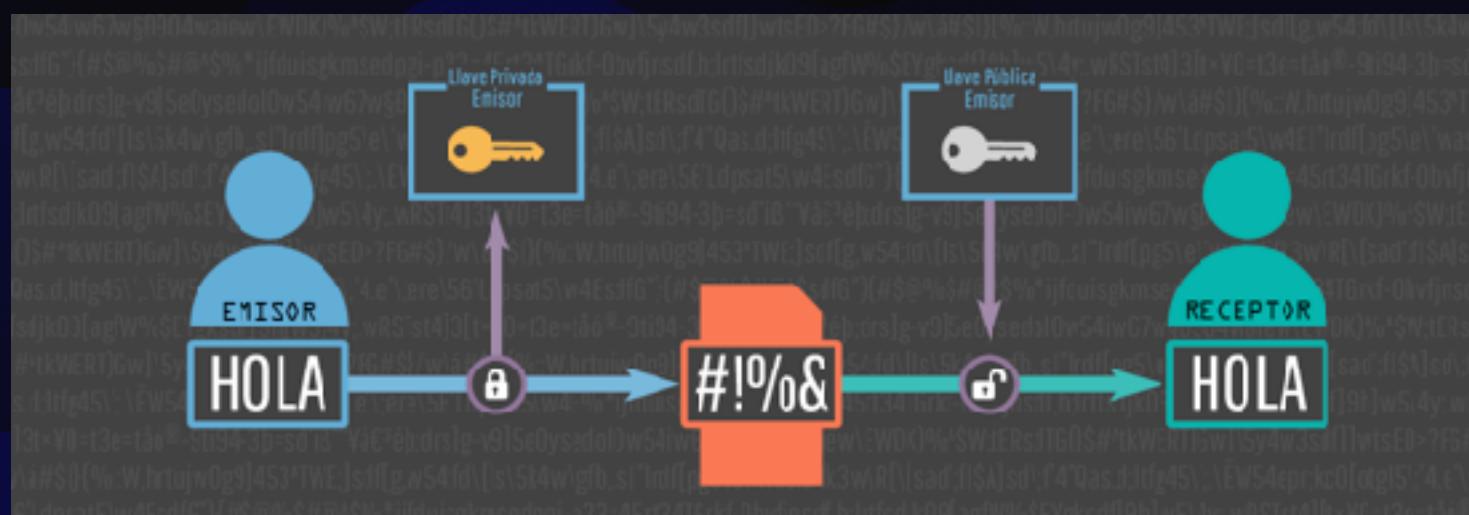
Mis recomendaciones

- Pórtatil/Sobremesa
- 8/16 GB de RAM (16 altamente recomendable)
- Un ratón cualquiera
- Procesador cuando más mejor (i5 sería lo mejor)

Las bases de la ciberseguridad

Las bases de la ciberseguridad

Criptografía



Sistemas



Redes



Programación

```
document.getElementById(div).innerHTML = '';
else if (i==2)
{
    var atpos=inputs[i].indexOf('@');
    var dotpos=inputs[i].lastIndexOf('.');
    if (atpos<1 || dotpos<atpos+2 || dotpos>inputs[i].length-2)
        document.getElementById('errEmail').innerHTML = 'Email address is invalid';
}
```

Puestos/Disciplinas de trabajo en la ciberseguridad

Otro Disclaimer

Elegir un área no te ata para siempre, nunca es tarde para cambiar

PRINCIPALES ROLES EN EL SECTOR DE LA CIBERSEGURIDAD

RED TEAM

Auditorias de seguridad

Descubrir vulnerabilidades

Pruebas de penetración



BLUE TEAM

Monitorización de sistemas

Análisis forense

Respuesta ante incidentes



Pentester / Pentesting

¿Qué es?

- Los que “hackean”
- Intrusión en Sistemas/Infraestructuras
- Los proyectos de Pentesting son de corta duración y muy acotados

¿Donde aprender?

- Existen cientos de miles de recursos en internet. Es la disciplina MÁS popular
- Hack The Box, TryHackMe, Vulnhub, OWASP TOP 10...
- Comunidades en Telegram: HackPlayers, Follow The White Rabbit...
- Chuletarios: book.hacktricks.xyz, ired.team, the-pentesting-guide.marmeus.com



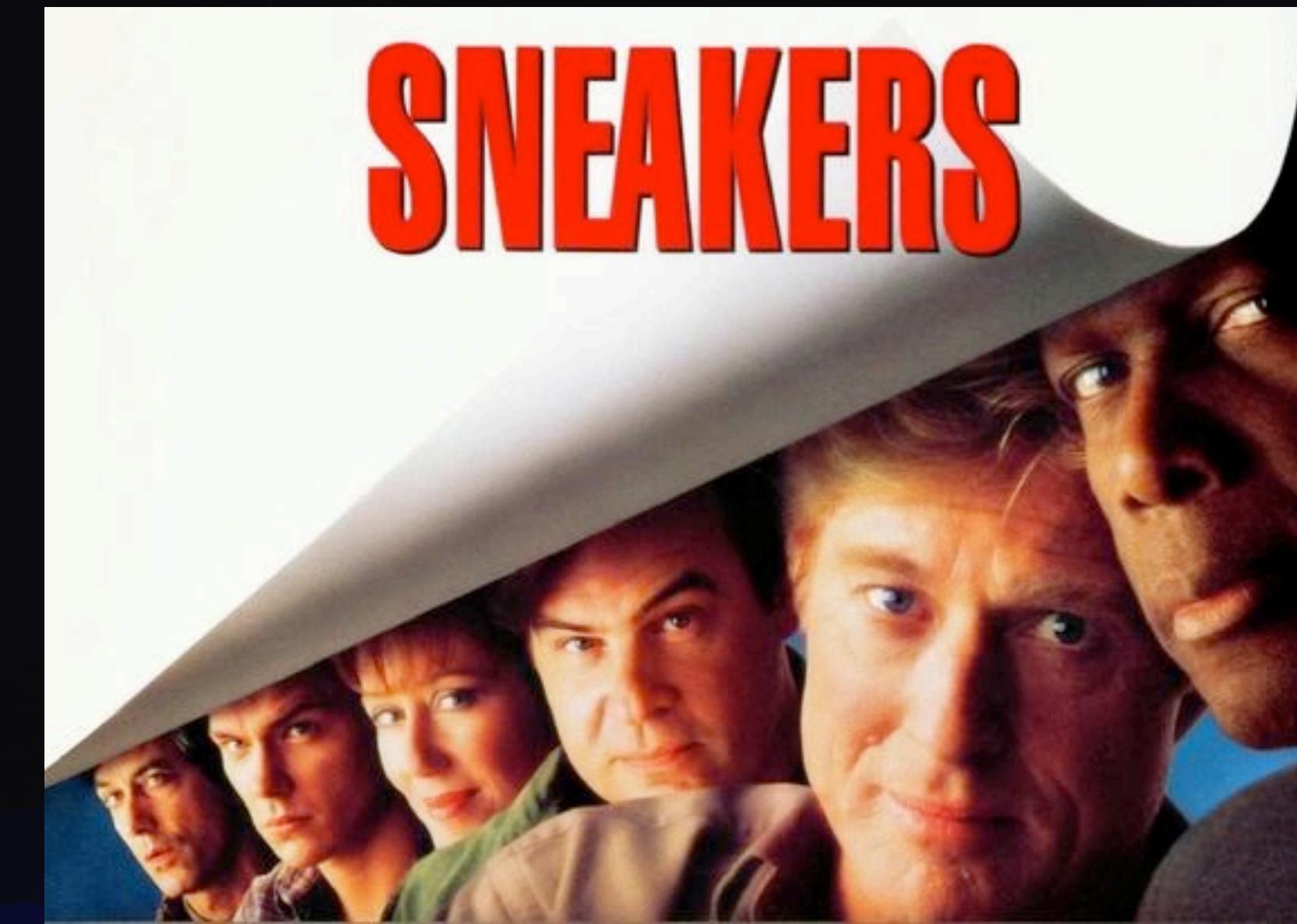
RedTeamer / Red Team

¿Qué es?

- Los que “hackean”, pero un paso más allá
- Intrusión en todos los sentidos (incluso física)
- Engañar a la gente para que te deje entrar o haga click en un link
- Proyectos de larga duración (meses)
- Hackean una central eléctrica <https://www.youtube.com/watch?v=pL9q2IOZ1Fw>

¿Qué/Donde aprender?

- Lockpicking – LockPickingLawyer en YouTube
- Ingeniería Social – Charla RootedCon de Ruth Sala & Carmen Torrano: <https://www.youtube.com/watch?v=UWG5kKL45yU>



Reverser/Reversing y Exploiter/Exploiting

¿Qué es?

- Ver como funcionan/comportan las cosas
- Análisis de binarios
- Análisis de Malware
- Desarrollo de programas para explotar vulnerabilidades (Exploiting)
- Curva de aprendizaje Alta

¿Donde aprender?

- Canal Telegram CrackLatinos
- Links de Recursos para empezar en el canal de TG: <https://t.me/clsinfo>

Hardware Hacking

¿Qué es?

- Hackear cacharros y cosas IoT
- Necesitas conocimientos de electrónica básica
- AliExpress es tu amigo para comprar los cacharros
- Mucho Reversing de Firmware

¿Donde aprender?

- Puedes empezar con proyectos de electrónica básica: <https://www.luisllamas.es/?s=arduino>
- Ernesto Sanchez & Joel Serna - Hardware Hacking y uso de la herramienta... [RootedCON2019-ESP] – <https://www.youtube.com/watch?v=vcBYey01CeY>

- <https://hackaday.com/2018/11/19/how-the-xbox-was-hacked/>

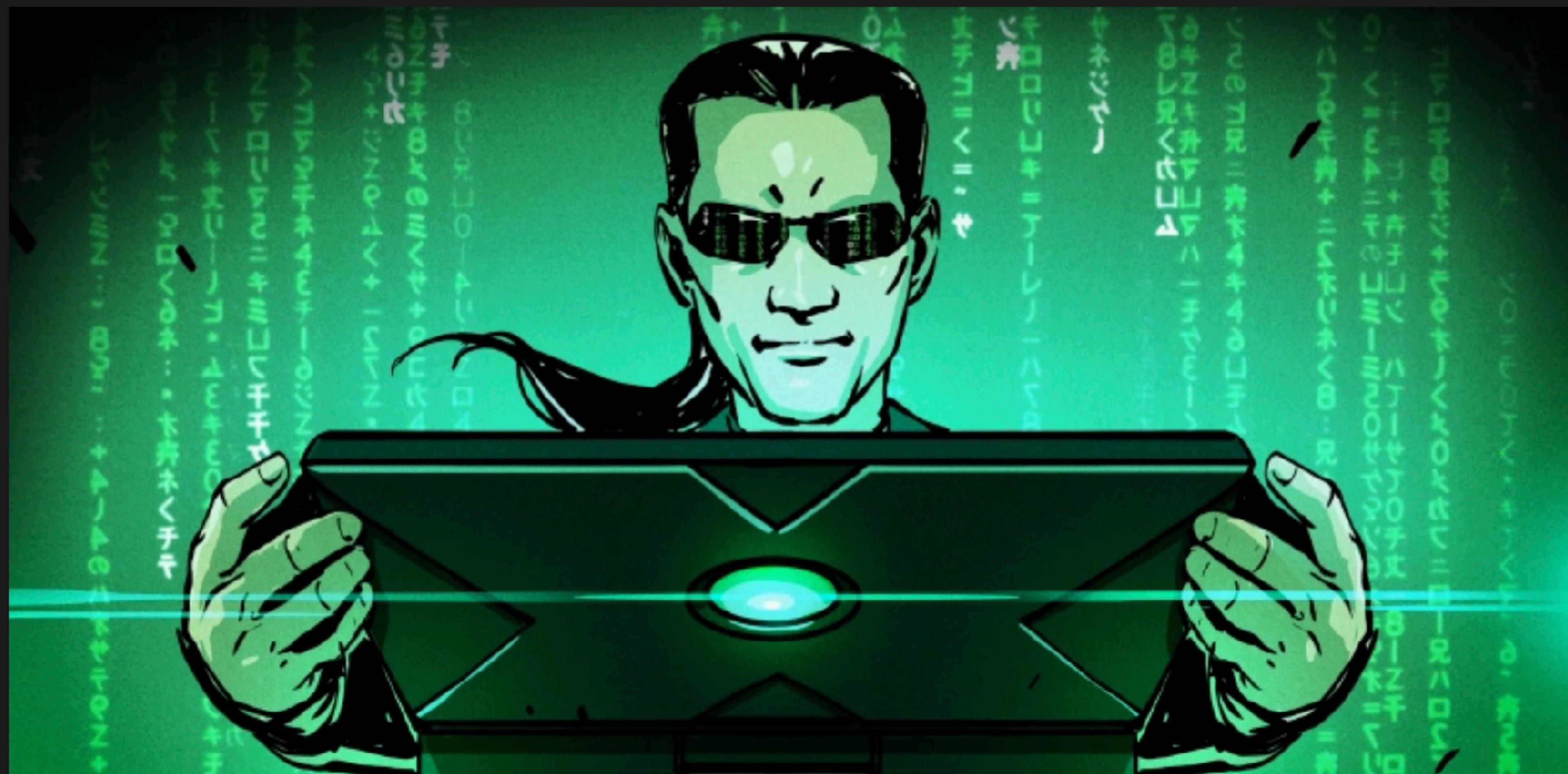
HOW THE XBOX WAS HACKED

by: **Drew Littrell**

38 Comments

f t Y d

November 19, 2018



DFIR / Forense / Peritaje

¿Qué es?

- Digital Forensics & Incident Response
- Los hackers que llegan cuando te han hackeado
- Analizan lo ocurrido, clonadoras, volcados de memoria, análisis de redes, forense a equipos informáticos...
- Peritaje informático, Juicios, Explicarle a un Juez cosas de bytes

Mas Info:

- Charla RootedCON 2019 – C.Tascon & J Carlos Diaz & J. Urtiaga - Incident Response Story Tellin – <https://www.youtube.com/watch?v=wE5gxH174tg>
- Charla RootedCON 2020 – Antonio Sanz – <https://www.youtube.com/watch?v=m2NA2yneQ3c>
- Comentario Pineado en el grupo Telegram Forense: de <https://t.me/forense> lleno de retos, cheat sheet forense



OSINT / Data Analyst

¿Qué es?

- OSINT = Open Source INTelligence.
- Datos → Información → Conocimiento → Inteligencia
- Análisis de datos en fuentes abiertas
- Investigación de persona/identidades en internet
- Para el análisis de datos Python es tu amigo

Ideas para aprender:

- Solicitar acceso a la API de Twitter y procesar datos que te interesen
- Google Dorks, Web Scraping
- Visualización de datos (Pilar ELK)



SOC Analyst

¿Qué es?

- SOC = Security Operation Center
- Monitorización y gestión de eventos
- Expertos en temas de logs
- Usan SIEM = Security Information and Event Management

Mas Info en:

- Vacaciones en la costa del SOC – Marta López – <https://www.youtube.com/watch?v=fhauGr9CCHY>
- Todo a SIEM – Marta López RootedCON2020 – https://www.youtube.com/watch?v=9wfMx_z1GW8



Threat Hunting

¿Qué es?

- Defensa ProActiva
- Búsqueda constante de comportamientos maliciosos
- Parten de pequeñas hipótesis que podrían ser malware
- Anticipación ante amenazas
- Monitorización e Instrumentalización a nivel de sistema operativo (les mola SYSMON)

Mas Info en:

- Hunting Malware using process behaviour - Roberto Amado [RootedCON2020-ES] – <https://www.youtube.com/watch?v=1aRDEljZaSA>



BugHunter / Bug Bounty

¿Qué es?

- Hackers que trabajan por su cuenta para encontrar bugs en grandes organizaciones
- Se ha puesto de moda en los últimos años por plataformas como HackerOne, Intigritti, BugCrowd...
- Si quieras dedicarte a esto necesitas experiencia en automatización de procesos
- Tienes que ser el primero en encontrar los bugs porque los sino RIP \$\$

Mas Info:

- [BugBounty Workshop The SpInquisitors Way - A. Fernandes, J. Domingo, R.Fernandez](https://www.youtube.com/watch?v=jHWUkYzMf6k) — <https://www.youtube.com/watch?v=jHWUkYzMf6k>
- [Offensive DevOops: Automatizando bounties usando "la nube"... - Borja Berástegui \[RootedCON2020-ES\]](https://www.youtube.com/watch?v=q11eBk_k6DA) — https://www.youtube.com/watch?v=q11eBk_k6DA
- [JAIME PEÑALBA - The Worst Bug Bounty Ever... \[Rooted CON 2017 - ESP\]](https://www.youtube.com/watch?v=pf1TZn1YnXA) — <https://www.youtube.com/watch?v=pf1TZn1YnXA>
- Comunidad en Español de Bug bounty: <https://t.me/bugbountyes>

|1



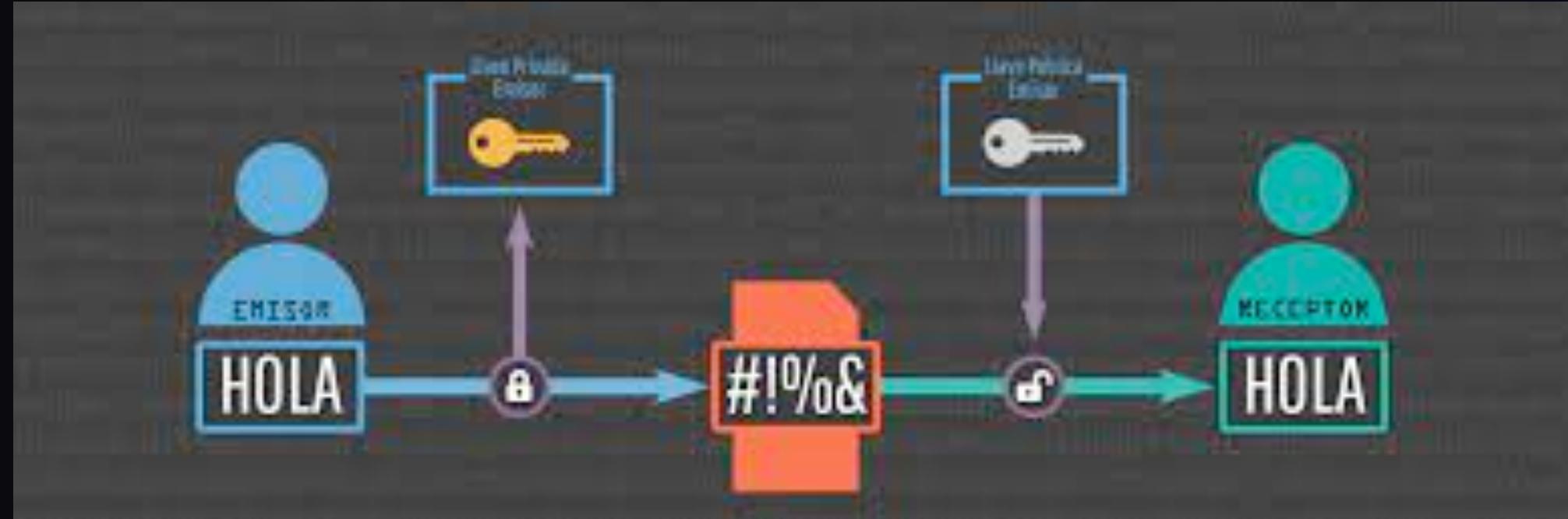
Criptoanalista/Criptografía

¿Qué es?

- Analizar algoritmos criptográficos
- Analizar implementación de productos de estos algoritmos
- Se necesita buena base matemática
- Necesario para dedicarse a la Ciberseguridad, no te escapas de ella, esta en todos lados

¿Donde aprender?

- <https://cryptohack.org/>
- El proyecto Criptored de Alfonso Muñoz y Jorge Ramió – <https://t.me/criptored> (también en Discord)



Bonus Track

Más posibles trabajos en este mundo

- BlockChain Security
 - <https://cryptozombies.io/>
 - Aprender Solidity, lenguaje de programación Ethereum
 - Rust para Solana
- Desarrollo Seguro
 - <https://thehackerway.com/2021/06/07/practica-desarrollo-seguro-con-owasp-secure-coding-dojo/>
 - Legal
 - Charlas Jorge Bermudez en RootedCON: https://www.youtube.com/watch?v=QoE0A_jKRWU
 - FCSE. Policía Nacional & Guardia Civil
 - Grupos de Delitos Telemáticos: <https://www.youtube.com/watch?v=LQHc2NvOMKQ>



Bonus Track Vol. II

Más recursos para empezar

- Redes
 - Aprende TCP/IP <https://www.coursera.org/learn/tcpip>
- Sistemas
 - Aprende Linux y Bash
 - Introducción a Linux: <https://www.edx.org/es/course/introduccion-a-linux>
 - An in-depth exploration of the art of shell scripting: <https://tldp.org/LDP/abs/html/>
 - Programación
 - Aprende python y luego C
 - Curso Python desde 0 de Pildoras Informáticas: <https://www.youtube.com/watch?v=G2FCfQj-9ig&list=PLU8oAlHdN5BlvPxziopYZRd55pdqFwkeS>



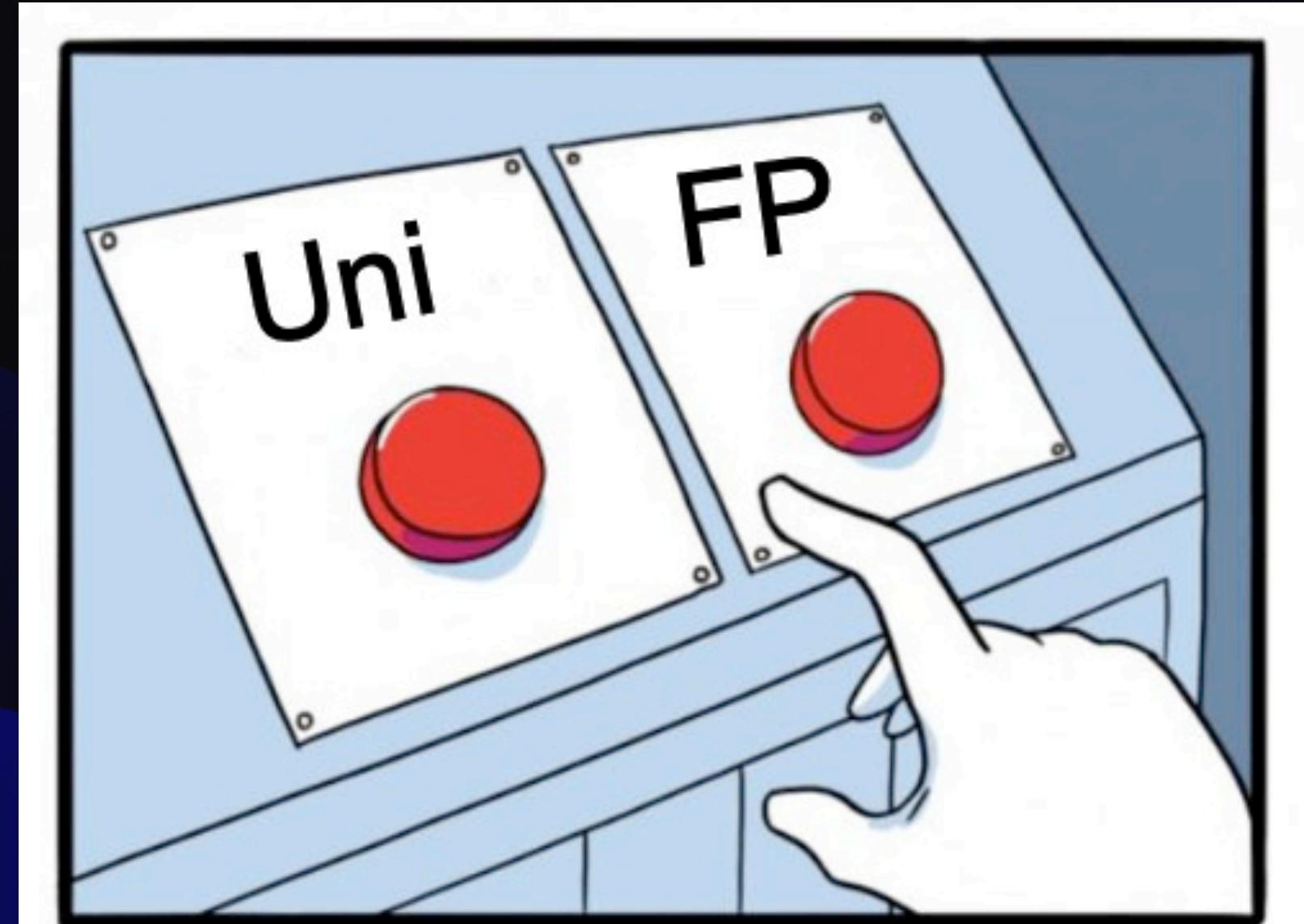


Sueldos en España

- https://docs.google.com/spreadsheets/d/1oM4mGrjv_VyWKE0nvnb5LAV_TGIQHm8gPbkCzWBnt_0/edit#gid=1461376371

Universidad VS. NO Universidad

- Altamente recomendado ir a la uni (my opinion)
- Si quieres trabajar lo antes posible es mejor opción una Formación profesional relacionada (ASIR y derivados...)
- Analiza tu situación, nadie te va a dar la respuesta correcta



Tips para encontrar trabajo

- Ir a conferencias (RootedCON, NavajaNegra, H-CON...)
 - En LATAM: EkoParty, DragonJar, 8dot8
- Hazte un Blog
- Crear un repositorio en GitHub
- Seguir a gente relevante del sector en Twitter
 - <https://twitter.com/kriwarez/status/1612172411511754752?s=46&t=crPI-jgA-oFt-BDP7-Tdw>
- Entrar a comunidades de Discord/Telegram
- Resolver retos (CTFs, HackTheBox, TryHackMe...)



Fin



@kriwarez



/kriware



@kriware