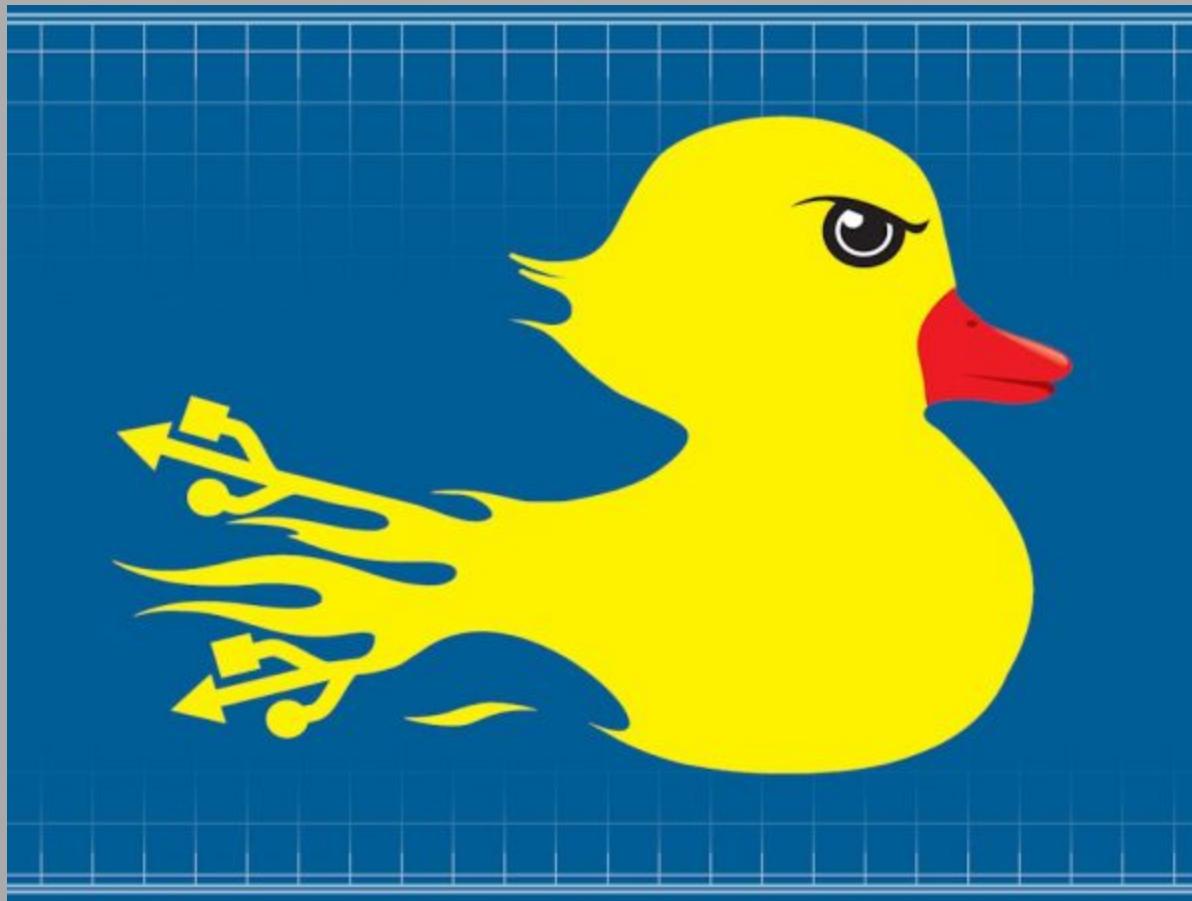


Rubber Ducky



Paula de la Hoz

@Terceranexus6

¿Quién soy? 🖖

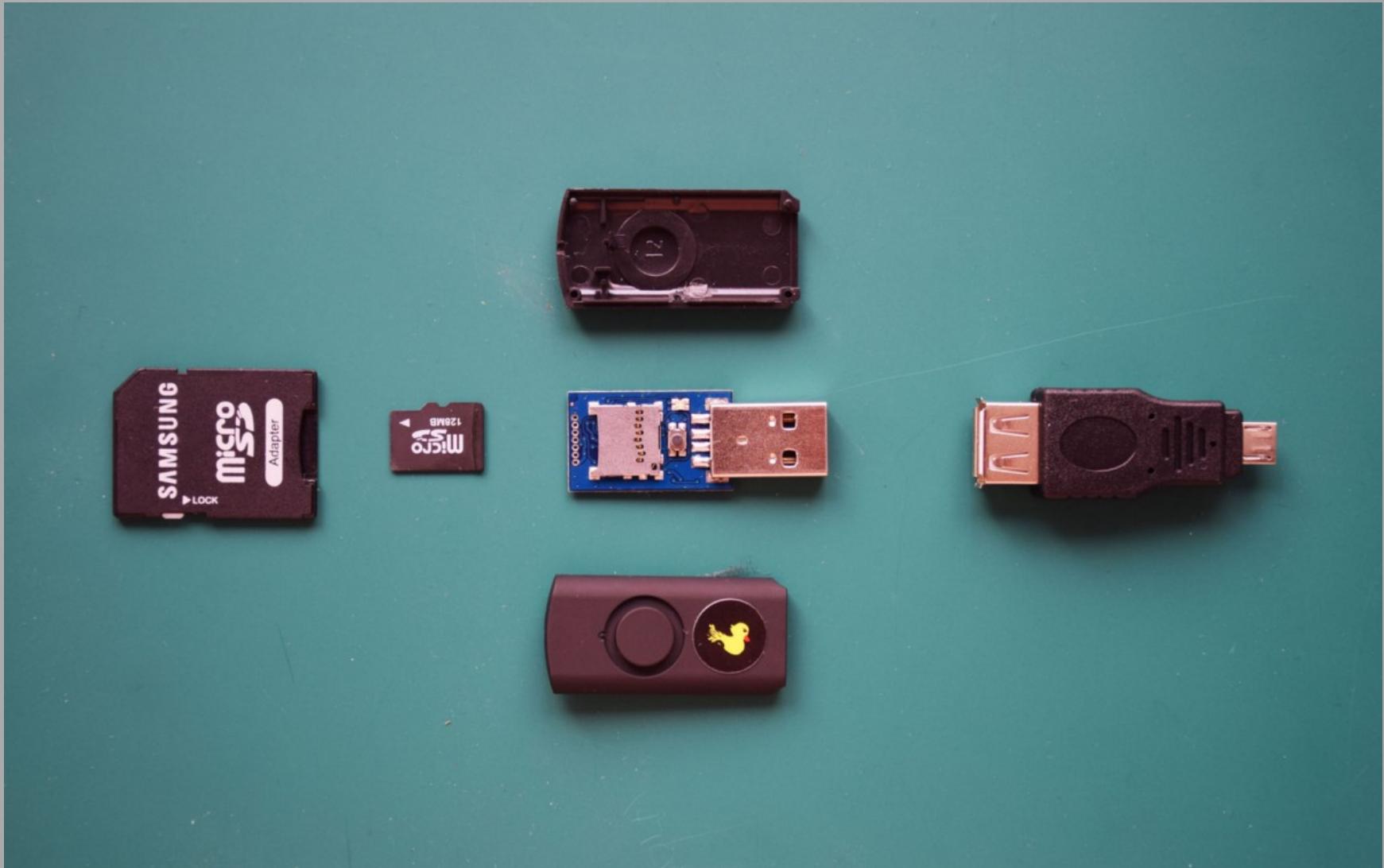
- Estudiante de ingeniería informática
- Programadora Junior
- Activista por los derechos digitales



Índice

- **¿Qué es Rubber Ducky?**
- **¿Cómo funciona?**
 - Procedimiento
 - Ejemplo de programación
- **Pentesting**
 - Concepto
 - Ingeniería social
 - Ética
- **Pros y Contras**
- **Demostración**

¿Qué es Rubber Ducky?



¿Qué es Rubber Ducky?

Rubber Ducky es un pen drive que imita la entrada de un humano por teclado para injectar comandos en ordenadores, móviles y otros sistemas.

¿Cómo funciona?



¿Cómo funciona?

Procedimiento

- 1- Creamos un **programa** con el lenguaje de programación diseñado para el pen.
- 2- **Compilamos** el programa con el compilador online del dispositivo.
- 3- Guardamos el *.bin* en la **micro SD** del pen-drive.
- 4- Metemos la micro SD en el pen-drive, y lo conectamos por **USB** al dispositivo objetivo.
- 5- El pen-drive ejecutará los **comandos** que le hayamos programado imitando entrada por teclado de un humano.

¿Cómo funciona?

Comandos

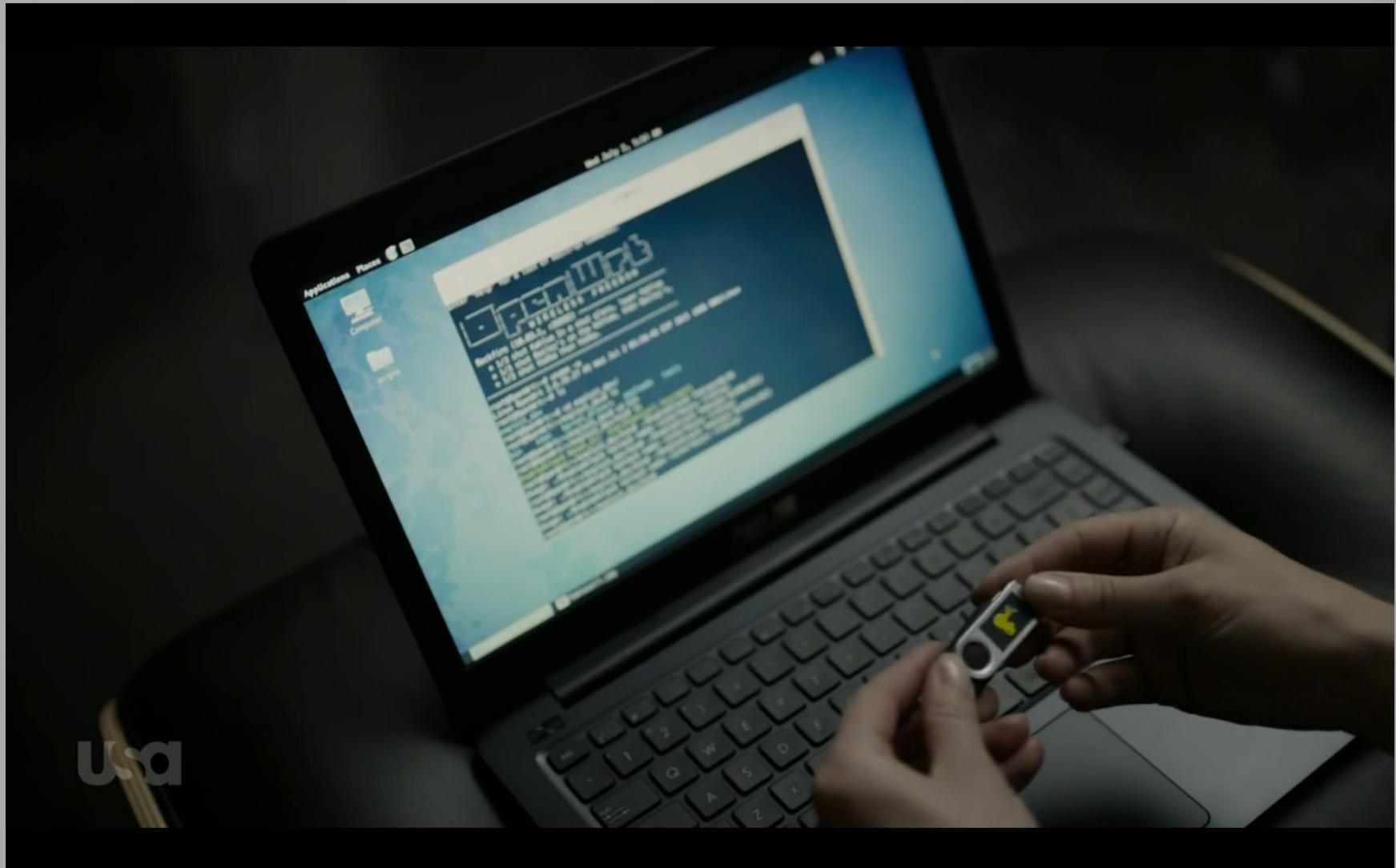
DELAY x–Retraso en milisegundos
STRING xyz–escribir
GUI–system
GUI r–Windows cmd
UP | UPARROW–tecla arriba
DOWN | DOWNARROW–tecla abajo
LEFT | LEFTARROW–tecla izda
RIGHT | RIGHTARROW–tecla derecha
CAPS | CAPSLOCK–Bloquear mayusc
ENTER–Enter
SPACE–Espacio
REPEAT x–repetir comandos anteriores X veces.

¿Cómo funciona?

Ejemplo de programación (linux)

```
DELAY 300 //espera 300 ms
GUI t      //abre terminal [S]+t
DELAY 750 //espera 750 ms
STRING cd //escribe cd en la terminal
DELAY 200
ENTER      //ejecuta Enter
DELAY 200
STRING loquesea...
// y así ejecutamos los comandos que queremos
```

Pentesting



Pentesting



Concepto

Del inglés "*penetration test*", consiste en una prueba controlada para **testear la seguridad** de un sistema. Hay muchas técnicas de pentesting, dependiendo del objetivo.

En nuestro caso se requiere una mezcla de **habilidad técnica**, para programar el ataque, e *ingeniería social*.

Pentesting

Ingeniería social

La capacidad de usar **habilidades no técnicas**, si no sociales (forma de **hablar**, de vestir, psicología, contexto, etc) para alcanzar un objetivo, en nuestro caso de testeo de **seguridad** informática.



Pentesting

Ética 😈

En informática, aún siendo una especialidad técnica, está tan presente en nuestras vidas, que requiere un control moral y ético en muchos aspectos.

La seguridad, concretamente, necesita un control ético especialmente alto.

Pros y Contras de Rubber Ducky



PROS

- Es una herramienta fácil de transportar y pasa **desapercibida**.
- Muy **flexible** a la hora de ser programada.
- **Documentación** completa y colaborativa en [GITHUB](#).

CONTRAS

- Requiere **acceso físico** al sistema.
- Está limitado a acciones por comando sin una **interacción** directa del programador.
- Se debe conocer bien el sistema a testear (poca portabilidad)

Demostración 

¿Preguntas? 