$>t3chfest
¿qué quieres aprender?

Informática 64
www.informatica64.com

Pentesting con Metasploit Framework

Pablo González

¿Qué es Metasploit?

Es el caos, puro y bello por fuera, eterno y complejo por dentro, es puro pentesting...

$>t3chfest
¿qué quieres aprender?

Agenda

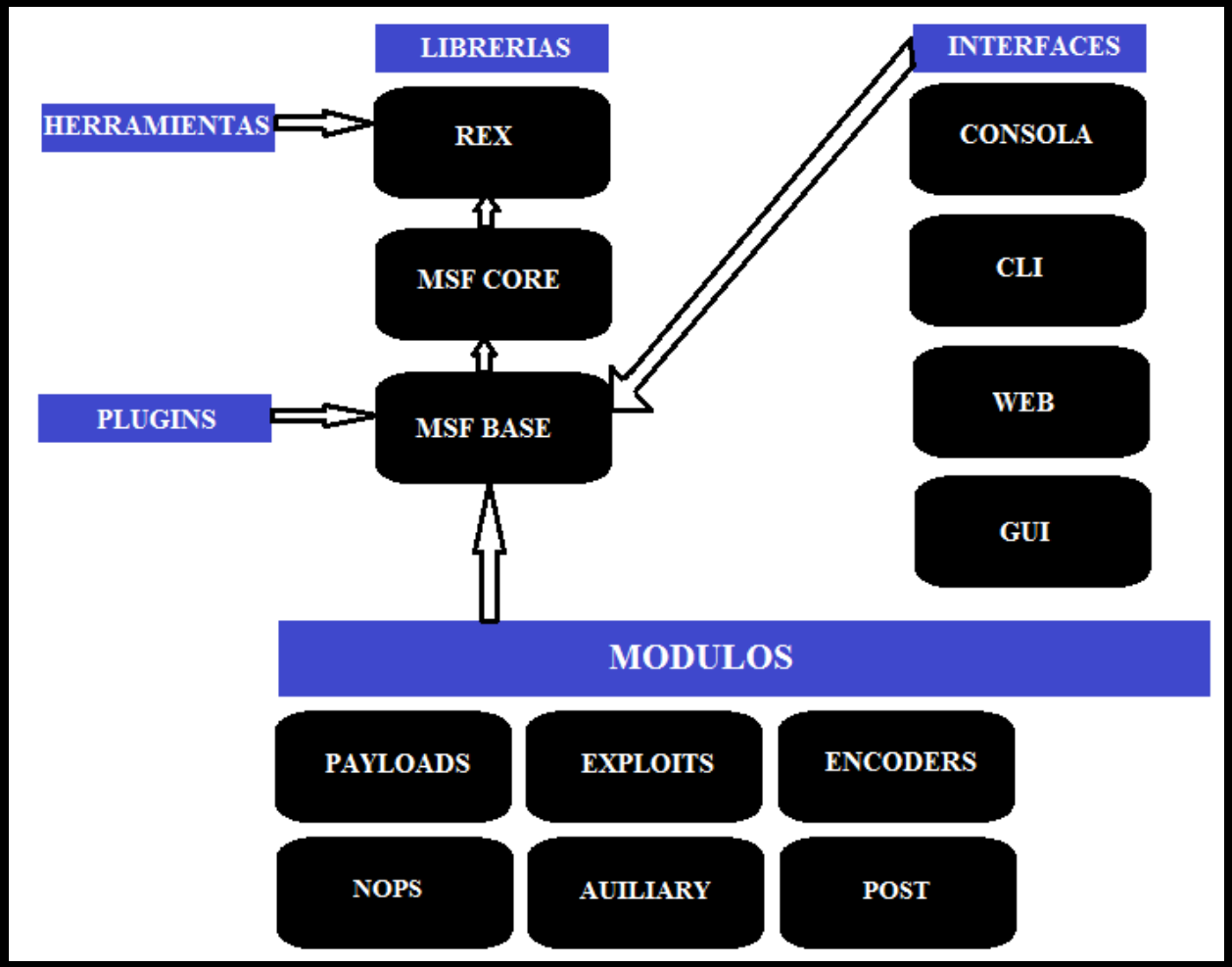
1. Arquitectura de Metasploit
2. Fases de un test de intrusión
3. ¿Dónde participa Metasploit?
4. El arte de la intrusión
5. El bien y el mal...
6. Demo
7. La tienda en casa

Informática 64
www.informatica64.com

$>t3chfest
¿qué quieres aprender?

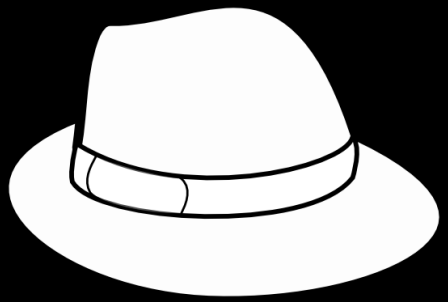
Arquitectura

Informática 64
www.informatica64.com


LIBRERIAS
INTERFACES
HERRAMIENTAS
REX
CONSOLA
MSF CORE
CLI
PLUGINS
MSF BASE
WEB
GUI
MODULOS
PAYLOADS
EXPLOITS
ENCODERS
NOPS
AUILIARY
POST

$>t3chfest
¿qué quieres aprender?

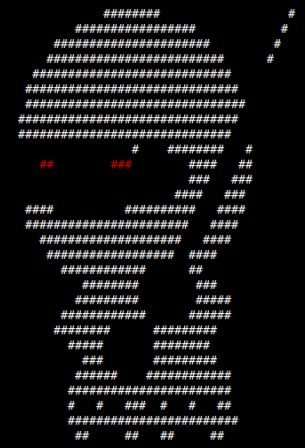
Fases Test Intrusión



Informática 64
www.informatica64.com

Fases

- ✓ Alcance y términos del test de intrusión
- ✓ Recolección de información
- ✓ Análisis de vulnerabilidades
- ✓ Explotación de vulnerabilidades
- ✓ Post-Explotación del sistema
- ✓ Generación de informes



$>t3chfest
¿qué quieres aprender?

¿Dónde participa?

Informática 64
www.informatica64.com

$>t3chfest
¿qué quieres aprender?

Lo importante es...

Participar!!!

- ✓ Recolección de información
- ✓ Análisis de vulnerabilidades
- ✓ Explotación de vulnerabilidades
- ✓ Post-Explotación

Pero incluso... ayuda a generar informes!

Informática 64
www.informatica64.com

$>t3chfest
¿qué quieres aprender?

El arte de la intrusión

Informática 64
www.informatica64.com

¿Arte o Ingeniería?

```
Procedure pentesting;
BEGIN
        writeln('paso 1')
        writeln('paso 2')
        ...
        arte;
END;

Procedure arte;
...
```

$>t3chfest
¿qué quieres aprender?

Ámbito

Explotación vulnerabilidades (pero...)

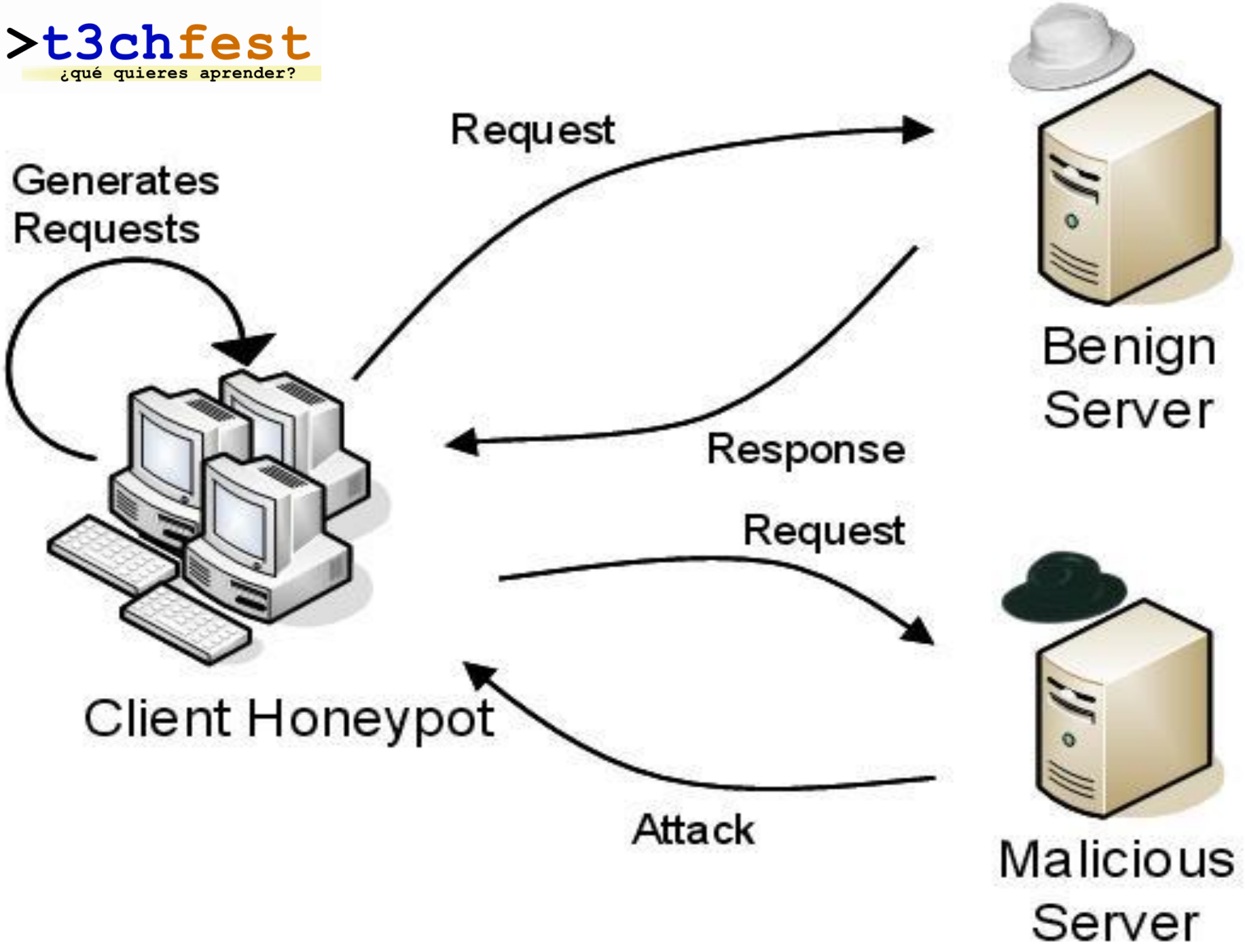
Best and Worst Practices

Informática 64
www.informatica64.com

Elección del payload

Más de 250 payloads...

Son nuestras cartas... ¿Siempre usaremos al rey?


Request
Generates Requests
Benign Server
Response
Request
Client Honeypot
Attack
Malicious Server

Client Side Attack!

Dark Shadows, ¿Cómo hago para que hagan peticiones a mí?

- ✓ Mailing? (spam??)
- ✓ Foros...
- ✓ Páginas web hackeadas...
- ✓ Publicaciones en Internet
- ✓ Acortadores...
- ✓ Ataques locales (DNS Spoof)

$>t3chfest
¿qué quieres aprender?

El bien y el mal...

Informática 64
www.informatica64.com

$>t3chfest
¿qué quieres aprender?

El límite

Debemos ser éticos... ¿Lo somos?

La delgada línea...

Podemos utilizar los ataques client-side para: (muchas, muchas cosas)

- ✓ Distribución malware...
- ✓ Payloads permanentes con MSF!

Informática 64
www.informatica64.com

$>t3chfest
¿qué quieres aprender?

Demo: A jugar!

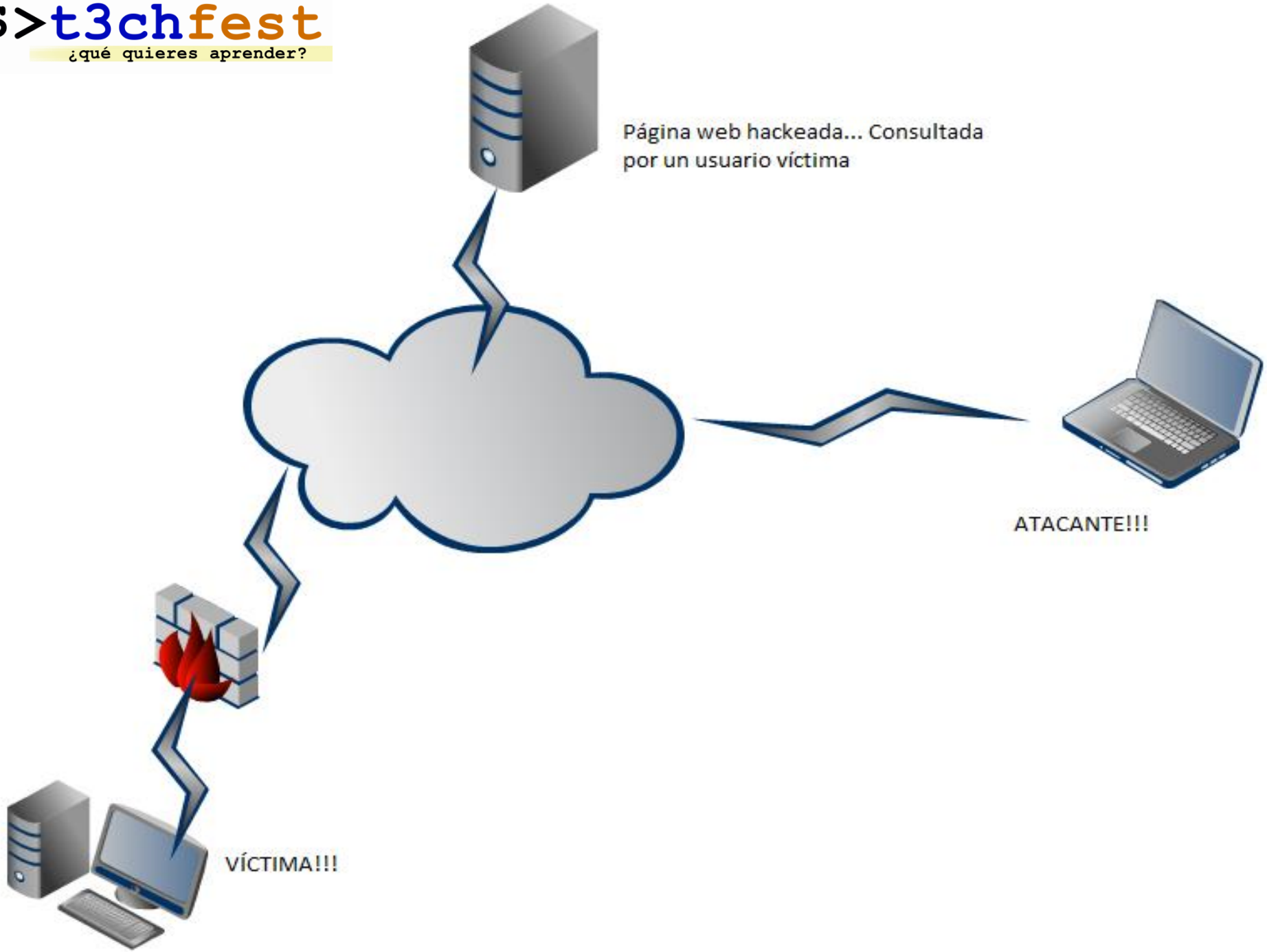
Informática 64
www.informatica64.com

¿Qué vamos a hacer?

Escenario: (idea del mundo real... ^^)

1. Página hackeada...
2. Iframe que apunte a 1 server con MSF
3. Lanzamiento de exploits contra cliente
4. Obtenemos el control...
5. ¿Troyanizamos? (distribución malware)

$>t3chfest
¿qué quieres aprender?



$>t3chfest
¿qué quieres aprender?

Informática 64
www.informatica64.com

$>t3chfest
¿qué quieres aprender?

La tienda en casa

Informática 64
www.informatica64.com

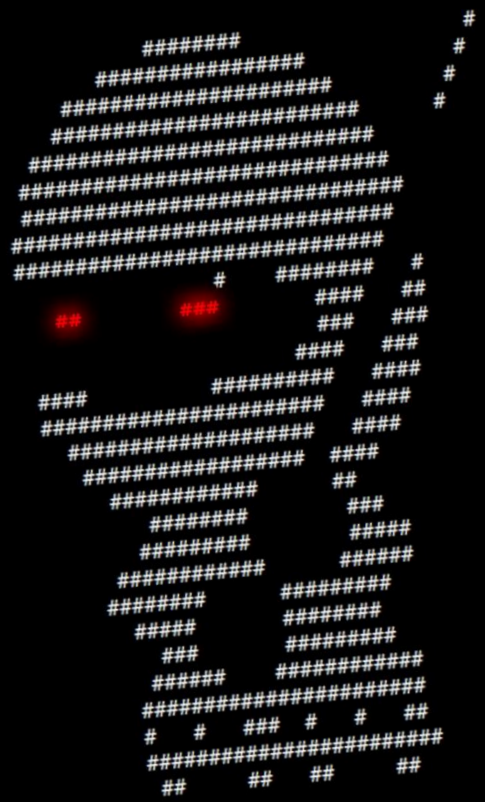
$>t3chfest

¿qué quieres aprender

A

...y han t

Metasploi



..

Informática64
www.informatica64.com

Informática64
www.informatica64.com

$>t3chfest
¿qué quieres aprender?

Informática 64
www.informatica64.com