



EuskalHack Security Congress IX



CTF as a Service

Mikel Izal (mikel.izal@unavarra.es)
Cátedra de Ciberseguridad
Universidad Pública de Navarra



CTF as a Service



About us...

Hace unos 4 años... en una universidad cerca de aquí...

Universidad Pública de Navarra > área de ingeniería telemática
CTFs para aprendizaje y motivación > ciberseguridad, hacking, red team...

- ex-alumnos en la National Cyber League
- prácticas en modo CTF
- club de hacking de la UPNA (the Hacker's C0nclav3)
- Máster de Ciberseguridad en UPNA
- Navarra Cybersecurity Center >> Cátedra de Ciberseguridad (2025+)



CTF as a Service





CTF as a Service



Un buen reto de Capture the Flag

>>> Busca curiosidad

- Un reto a primera vista imposible de conseguir
- Usa 1 habilidad/concepto
- Sin distracciones
- Sin guessing

Hay escenarios más realistas

>>> Busca realismo

- Reconocimiento y decidir que atacar
- Ingeniería social
- cyber-ranges más que CTFs

¿Cómo convertimos retos en infraestructura?



CTF as a Service



One-slide challenge

```
Adivina el numero entre 0 y 10000000  
r= 42  
era 805536  
concentrate mas...
```

```
print('Adivina el numero entre 0 y 10000000')  
respuesta=int(input('r= '))  
  
random.seed(int(time()))  
x=random.randint(0,10000000)  
  
print(f'era {x}')  
if x==respuesta :  
    print('muy bien tu clarividencia')  
    print_flag()  
else:  
    print('concentrate mas...')
```



CTF as a Service



Distribuyendo retos

Reto autocontenido

Servidor en docker

web / php / js

python / binario con socat

máquinas unix en docker

...

Definicion docker-compose.yml

escenarios con varios dockers

+scripts de soporte

Download and use...

```
reto1
├── docker-compose.yml
├── _flag.txt
├── py
│   └── reto.py
├── prepare.bash
├── start.bash
└── stop.bash
```

docker-compose.yml

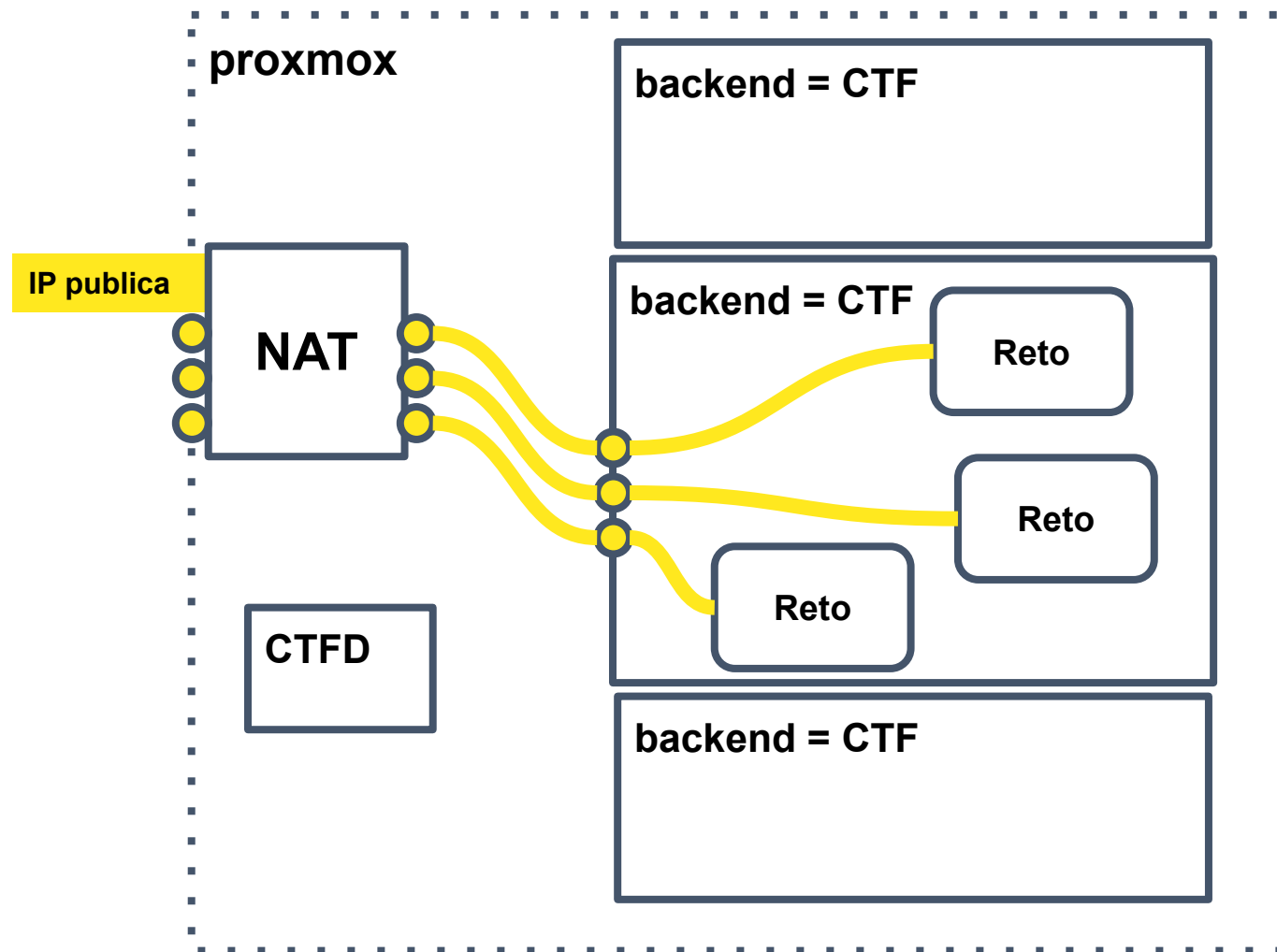
```
services:
  pyapp:
    image: simplepy
    volumes:
      - ./py:/py:ro
      - ./_flag.txt:/flag/flag.txt
    ports:
      - ${PORT}:22001
    command: sh -c "socat TCP-LISTEN:22001,reuseaddr,
      fork EXEC:'python3 /py/reto.py'"
```



Infra para CTFs

Estructura básica de CTF

- Múltiples retos en un git
 - **git clone** y usar en tu máquina
 - o despliegue en infra
 - CTFD para la puntuación
-
- 1 CTF > 1 backend > 1 git





CTF as a Service



Evolución de la infraestructura

- Preparación y preview de los retos
 - >> git y scripts
- Dudas y caídas durante el juego. (Está funcionando el reto X?)
 - >> scripts de pruebas y autosolución
- Es suficiente una instancia de cada reto?
 - >> Persistencia tras la conexión?
 - >> En prácticas quieres separación
 - >> Entorno hostil ... el día que probamos en CTFTime



CTF as a Service



Ejemplo de reto con persistencia

```
<?php    session_start();
if (isset($_POST['nombre'])) { $_SESSION['nombre'] = $_POST['nombre']; }
$nombre = $_SESSION['nombre'] ?? 'desconocido';    ?>

<p>Hola <?= htmlspecialchars($nombre) ?>, estas en una sesion</p>
<form method="post"> <input type="text" name="nombre">
<input type="submit" value="Cambiar nombre"> </form>

[<a href="?content=news">noticias</a>][<a href="index_php">ver index.php</a>]

<?php
if (isset($_GET['content']) && strpos($_GET['content'], 'flag') === false) {
?><hr>
<pre> <?php include($_GET['content']); ?> </pre>
<?php } ?>
```

**Tengo una sesión
con sus cookies
Si no voy al mismo
servidor la perderé**

**Ejecución de código de
fichero que contenga
PHP**

**¿¿Pero de donde saco
un fichero con el PHP
que yo quiero??**



CTF as a Service



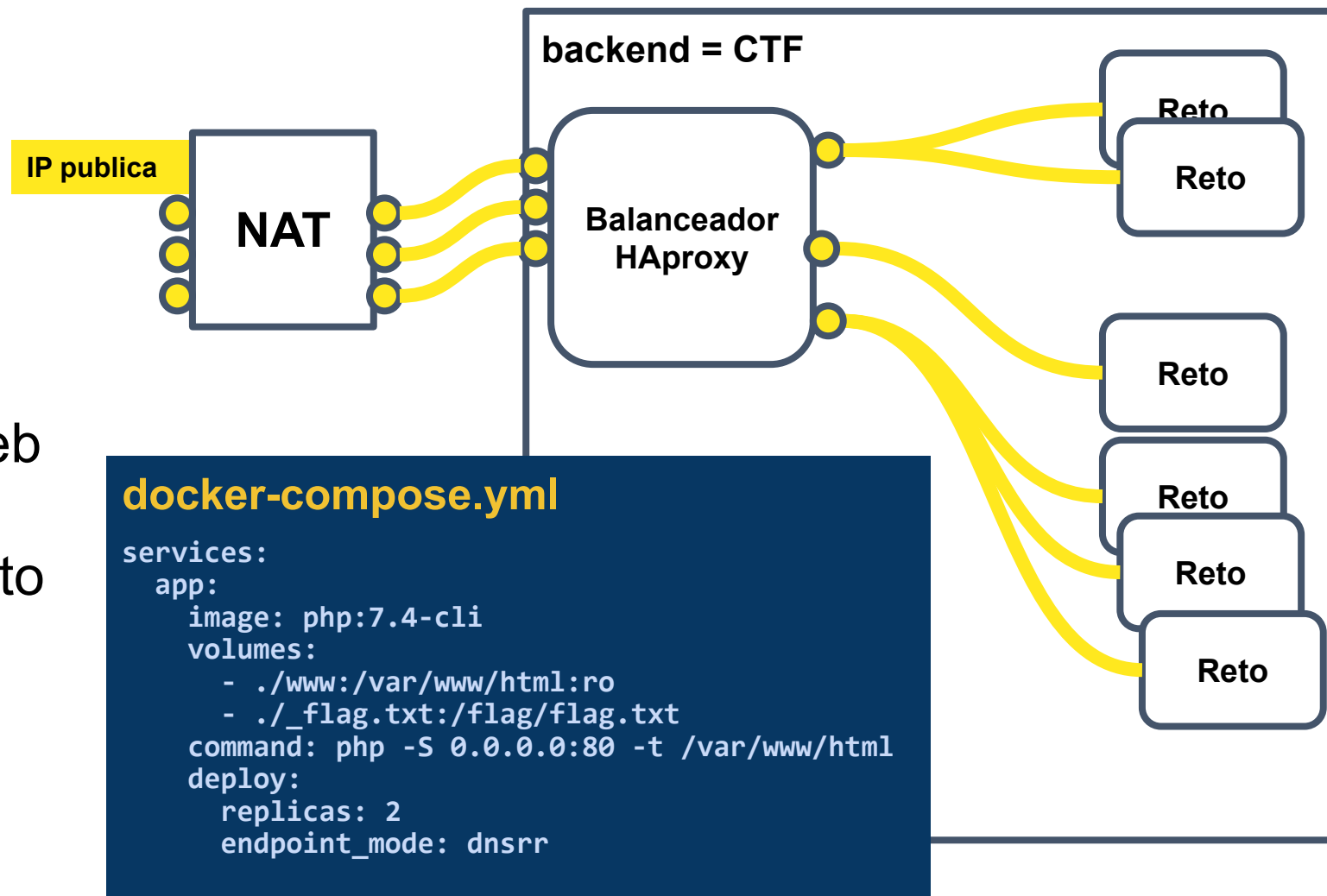
Multi-instancia

docker swarm
con DNSrr

balanceo HAproxy
sticky sessions

tcp por src retos no web
http cookies dinámicas web

Replicas configurables por reto





CTF as a Service



orquestación

proxmox

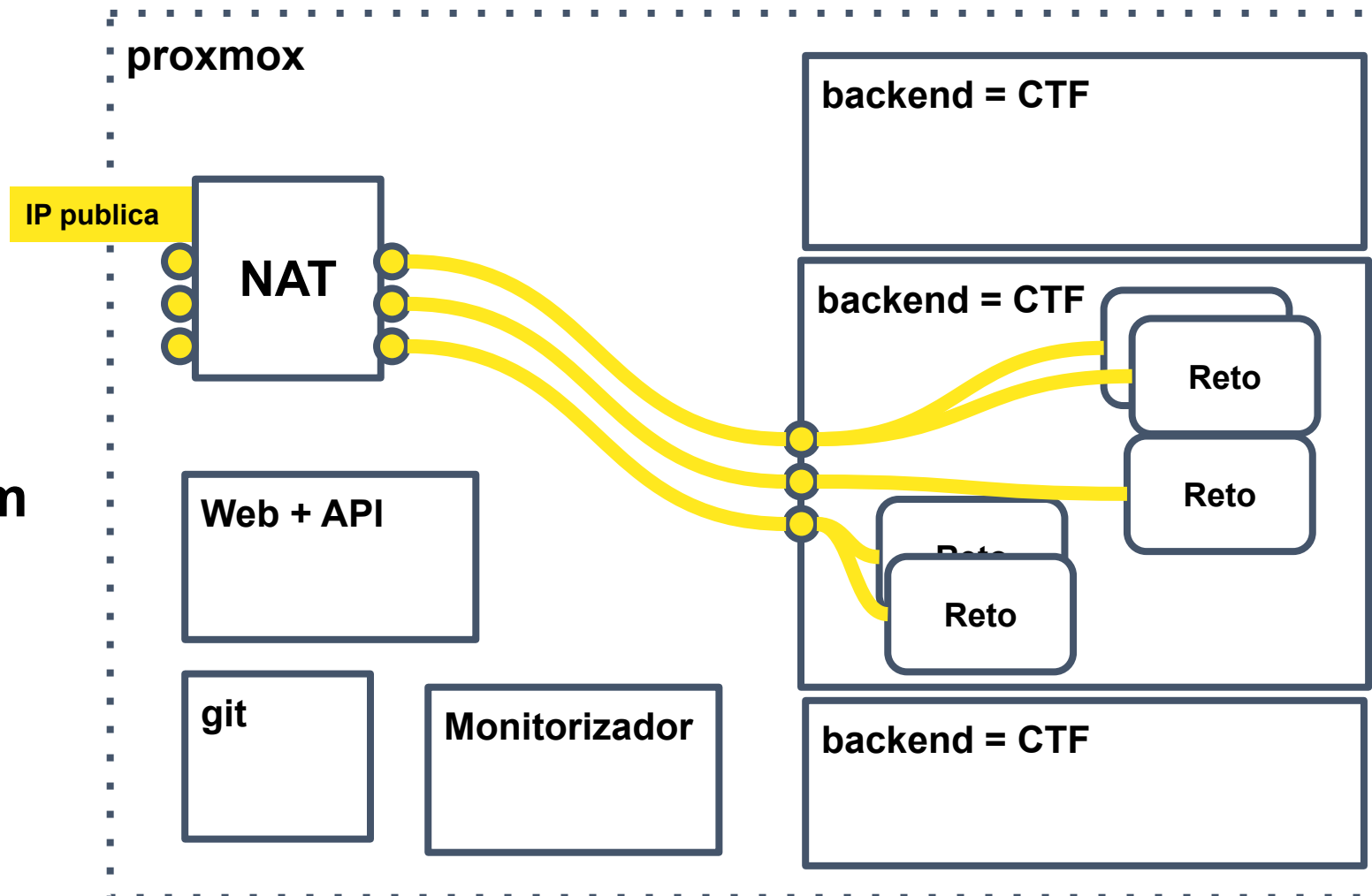
terraform/ansible

git

retos en docker

balanceo HAproxy + swarm

y frontend?...



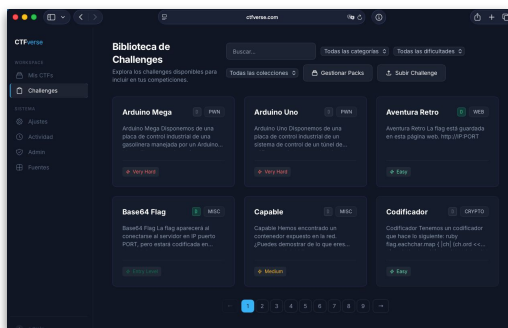


CTF as a Service

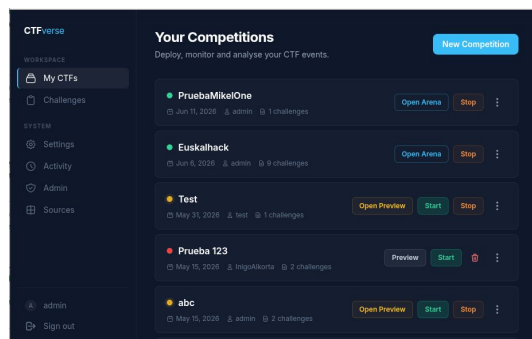


CTFVERSE.COM

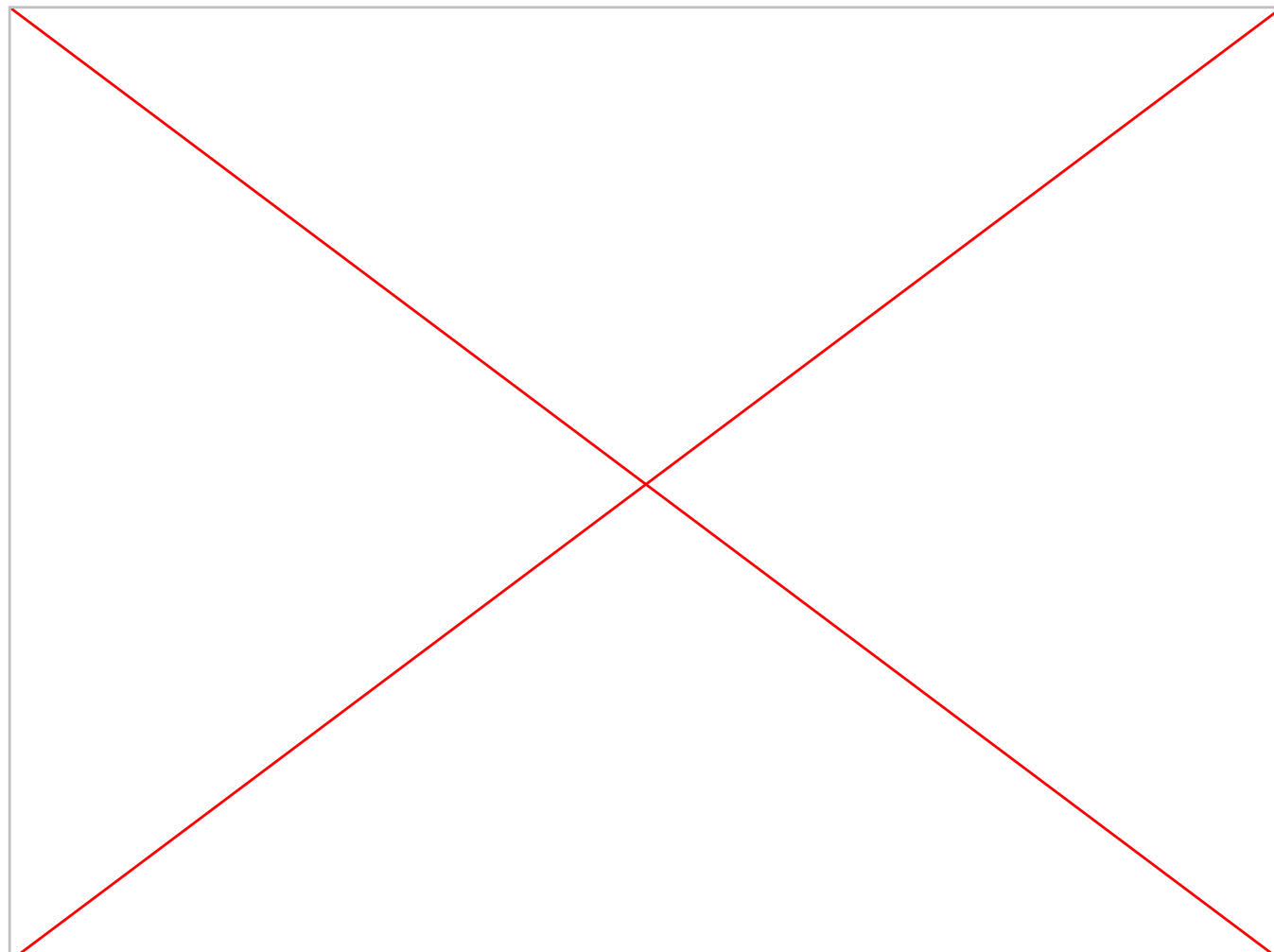
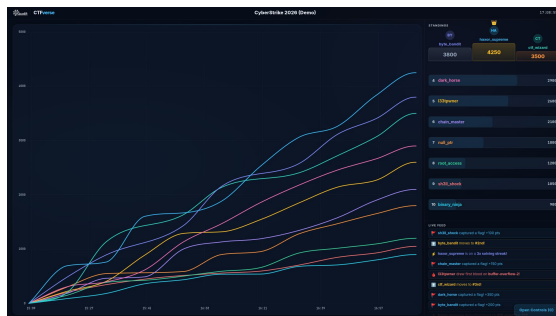
Gestión de retos



Creación de CTFs



Scoreboard





CTF as a Service



Conclusiones

- CTFs para motivar la entrada en ciberseguridad ofensiva
- Filosofía e infraestructura CTF as a service

Future lines...

- Una instancia por jugador?
- Escenarios de ataque y defensa? Cyber-range?
- Evitar o integrar la IA? (construyendo retos, resolviendo retos)



CTF as a Service



¡MUCHAS GRACIAS!
ESKERRIK ASKO!



<https://ctfverse.com>