Active Discovery

Juan Rodríguez

CYBER SEC 42

@juanrodr

CYBER SEC 42

CYBER SEC 42

42madrid_liga_cybersec – 21 abr.

darodrig 19:19

Importante para los asistentes del taller. Desde seguridad del distrito ha llegado una alerta de tráfico malicioso. Nos piden que detengáis inmediatamente vuestros servicios de hosting (ngrok) si aún están en pie. Una cosa es experimentar con la tecnología y otra lanzar ataques dirigidos y almacenar contraseñas reales. No es una broma. No queremos que haya que dejar de hacer este tipo de cosas por irresponsabilidades de los estudiantes. Gracias.

🚨 ⚠️ 36 reacciones

CYBER SEC 42

Tarea de hoy

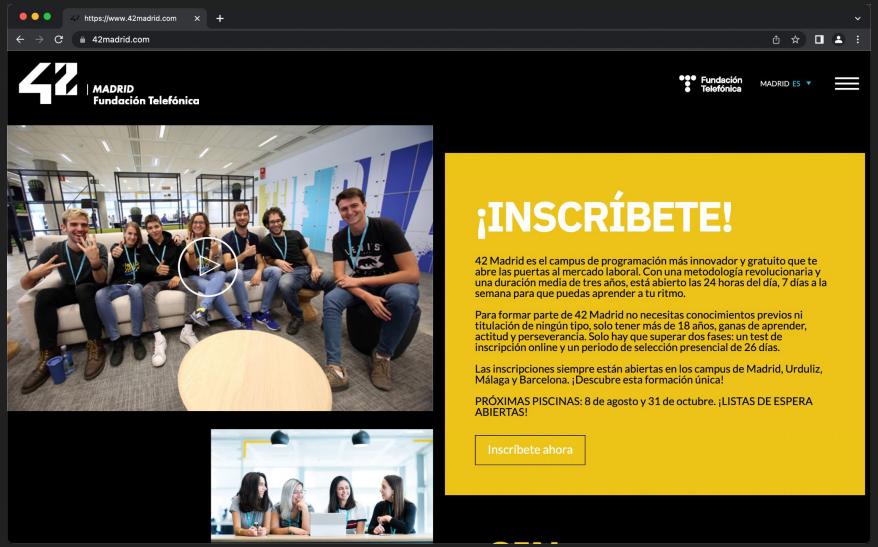
1. Qué es el descrubrimiento activo
2. Web o Infraestructura
3. Qué tienen las webs
4. Herramientas
5. Infraestructura
6. Herramientas

CYBER SEC 42

Active Discovery

CYBER SEC 42

Diferenciación



CYBER SEC 42

Páginas Web

https://subdomain.domain.extension:port/route?parametros=hd

CYBER SEC 42

Domains

https://subdomain.domain.extension

- Ping
- Dig
- Nslookup
- Whois

CYBER SEC 42

Subdomains

https://subdomain.domain.extension

Sublist3r: https://github.com/aboul3la/Sublist3r

CYBER SEC 42

Routes

https://domain.extension/route

- Crawlers
- wfuzz

Wappalyzer

Netcat y Nmap

Nuclei

https://github.com/projectdiscovery/nuclei

Muchas gracias!

CYBER SEC 42