

SUBDOMINIIONS

Enumeración de activos for fun

> WHOAMI

six2dez

> SCREENFETCH



Nombre Alexis Fernández

Lugar Madrid, España

Ocupación Pentester & Bug Hunter

Website pentestbook.six2dez.com

Proyectos reconFTW & OneListForAll

GitHub/Twitter [six2dez/](https://github.com/six2dez)[@six2dez1](https://twitter.com/six2dez1)

> STARTX



DISCLAIMER



Este taller está plagado de Minions sin ningún motivo o relación aparente, ¿por qué? Porque sí, por el mismo motivo que “se nos cae” una comilla simple en cada formulario web, por las risas, qué le vamos a hacer, así somos.

Y de paso, recordad que atacar objetivos sin permiso es ilegal ;)

ÍNDICE

- Objetivo
- Primeros pasos
- Dominios raíz
- Subdominios
- Hosts
- Cloud
- Webs y URLs

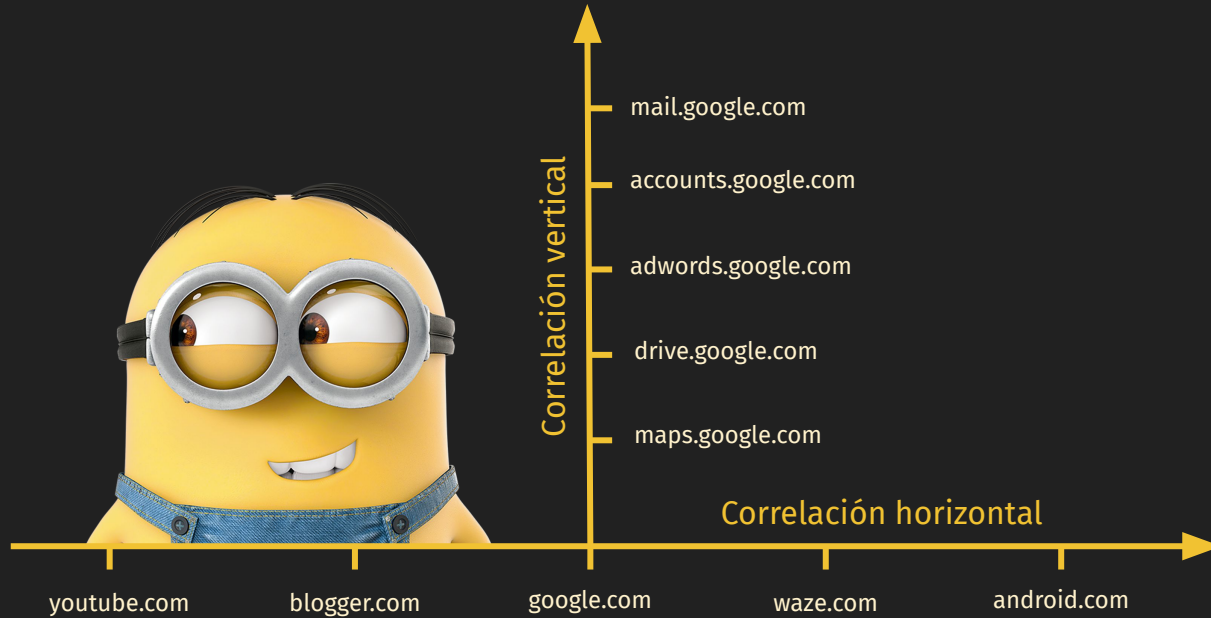


OBJETIVOS

- Tener una “foto” completa del objetivo
- Ampliar el alcance
- Localizar sitios web potencialmente vulnerables
- Encontrar vectores de ataque
- Definir y acotar los principales vectores



PRIMEROS PASOS



PRIMEROS PASOS



- Google
 - Primer vistazo al objetivo
 - “About us”
- Dorks
 - Contenido indexado en buscadores
 - Principalmente Google y GitHub
- Metadatos
 - Documentos ofimáticos indexados que contienen metadatos
- Emails y usuarios
 - Direcciones de email, nombres y apellidos de empleados y posibles usuarios
- Leaks
 - Consulta en DB de brechas conocidas



DEMO OSINT



DOMINIOS

- Información del dominio principal
 - bgp.he.net - ASNs
 - domainbigdata.com
 - viewdns.info
 - whoisxmlapi.com
- Registrants
 - Nombre
 - Organización
 - Email
- Reverse whois
- Google Analytics ID
- Favicon Hash



demo dominios



SUBDOMINIOS

- Pasivo
 - Servicios de terceros
 - Modelo gasto tokens/datos
- Crtsh
- Resolución DNS
- DNS BF
 - Permutaciones y alteraciones
- Crawling
- Registros DNS
- Google Analytics ID



DEMO SUBDOMINIOS



HOSTS



- Resolución IP de subdominios
- Resolución inversa de IPs
- IP CloudFlare
- Escaneo de puertos
 - Pasivo
 - Activo
- Versiones de software vulnerable

DEMO HOSTS



CLOUD

- Localización de activos cloud
 - Fuerza bruta palabras clave
- Buckets S3
- IPs pertenecientes a proveedores
- Redirecciones DNS



DEMO CLOUD



WEB Y URLS

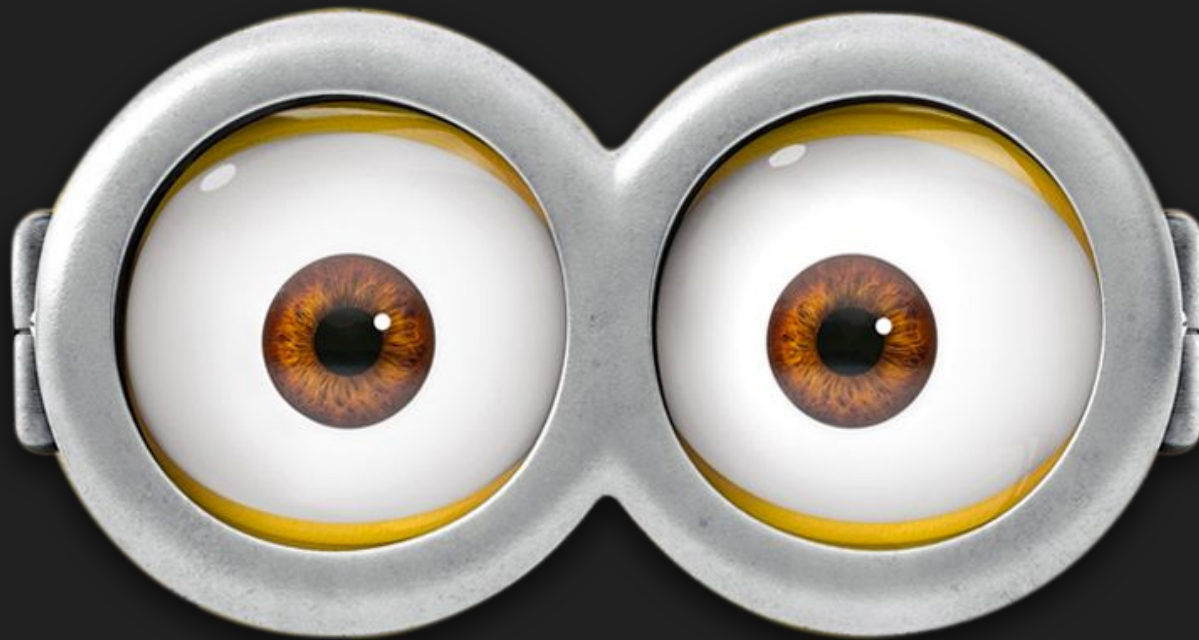
- Resolución web de subdominios
- Análisis puertos web no comunes
- Identificación tecnologías
 - WAF
 - CMS
- Capturas de imágenes web
- Fuzzing
- Extracción URLs
 - Crawling
 - Wayback Machine
 - VirusTotal
 - GitHub
- Procesamiento URL
 - Filtros
 - Patrones
 - Análisis JS
 - Clasificación



DEMO WEB Y URLS



PREGUNTAS



GRACIAS

