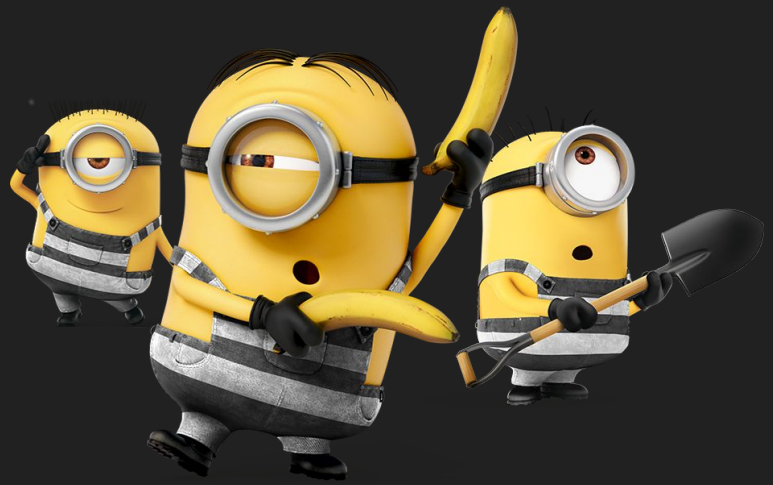


SUBDOMINIONS

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/@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 ;)

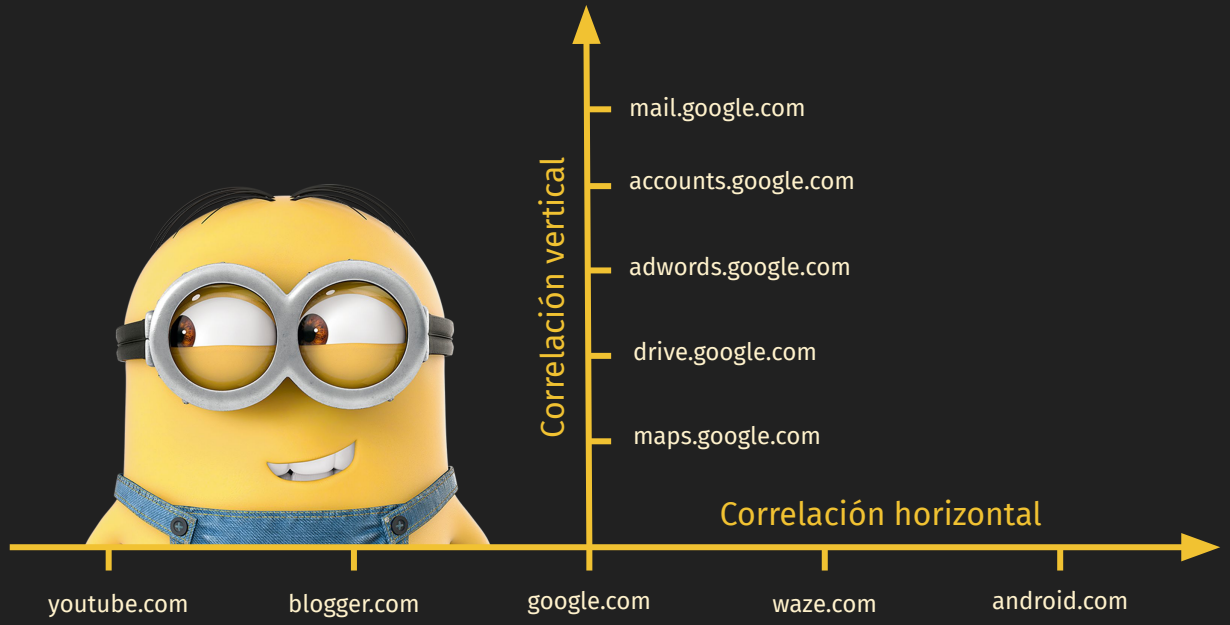
ÍNDICE

- 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
  - Múltiples servicios
  - Info no actualizada
  - Info duplicada
  - Modelo gasto tokens/datos
- Crtsh
  - DB info certificados
  - Creada para detectar fraudes
  - Solo info de webs con certificados
- Resolución DNS

Subdominios

- Fuerza bruta DNS
  - En base a diccionarios
  - Cuello de botella
  - Lento pero único
  - Permutaciones y alteraciones
    - Generar dicts en base a resultados
    - Espacio en disco
- Crawling
  - Pasivo
  - Activo
- 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