



# INTELIGENCIA MISCELÁNEO.

Brian Juarez Arguello



# Gobuster

- Gobuster es una herramienta de código abierto diseñado para la enumeración de directorios y archivos en servidores web. Su función principal es ayudar en la búsqueda y descubrimiento de rutas ocultas, archivos y subdirectorios en sitios web. Es una herramienta popular entre los profesionales de seguridad informática y los pentesters (testers de penetración) para evaluar la superficie de ataque de un sitio web y descubrir posibles vulnerabilidades. Las principales características de Gobuster incluyen:
  - Enumeración de directorios: Gobuster puede realizar una búsqueda exhaustiva de directorios y subdirectorios en un servidor web. Esto puede ser útil para identificar áreas del sitio que no están enlazadas públicamente pero que aún son accesibles.

# Dumpster Diving

- En ciberseguridad, el término inglés dumpster diving consiste en investigar la «basura» de una persona u organización para encontrar información que pueda ser utilizada para atacar una red informática.
- En muchas ocasiones, el dumpster diving trata de obtener datos sobre un usuario para hacerse pasar por él y acceder a sus perfiles u otras áreas restringidas de Internet o red local. Aunque también tiene un componente físico, ya que esos datos se pueden buscar en la basura tradicional.
- «La basura de un hombre es el tesoro de otro»
- Los ciberdelincuentes obtienen información sensible a través de nuestra «basura» para infiltrarse en la red o copiar la identidad de un empleado. Entre los datos que los ciberdelincuentes pueden obtener al buscar en ella están:
  - Códigos de acceso y contraseñas.
  - Números de teléfono, correos electrónicos y direcciones domiciliarias de clientes, socios comerciales, proveedores y familiares.
  - Diseños de productos, planos y borradores de planes de negocio.
  - Números de tarjetas de crédito y cuentas bancarias del personal y clientes comerciales.
  - CD, DVD, USB y otros dispositivos de almacenamiento portátiles.



# Ingeniería Social

- Se llama ingeniería social a las diferentes técnicas de manipulación que usan los ciberdelincuentes para obtener información confidencial de los usuarios.
- Los ciberdelincuentes engañan a sus víctimas haciéndose pasar por otra persona. Por ejemplo, se hacen pasar por familiares, personas de soporte técnico, compañeros de trabajo o personas de confianza. El objetivo de este engaño es apropiarse de datos personales, contraseñas o suplantar la identidad de la persona engañada.
- ¿Qué canales utilizan los ciberdelincuentes para los ataques de ingeniería social?
- Los ciberdelincuentes manipulan y engañan a las personas a través de:
  - llamadas telefónicas
  - visitas personales al domicilio de las personas
  - aplicaciones de mensajería instantánea
  - correos electrónicos
  - redes sociales

