



# Inteligencia Misceláneo

MATERIA: Analisis De Vulnerabilidad





# GOBUSTER



**Es una herramienta utilizada para realizar fuerza bruta a: URLs (directorios y archivos) en sitios web, subdominios DNS (con soporte de comodines) y nombres de hosts virtuales en los servidores web.**

**Esta herramienta tiene tres modalidades:**

**dir: el modelo clásico de fuerza bruta contra directorios**

**dns: el modo de fuerza bruta contra subdominios DNS**

**vhost: el modo de fuerza bruta contra hosts virtuales que no es lo mismo que el DNS.**

# 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 donde se obtienen datos sobre un usuario para hacerse pasar por el y acceder a sus perfiles u otras áreas restringidas de internet o red local pero tambien tiene un componente fisico, ya que esos datos se pueden buscar en la basura tradicional**

**Datos que pueden obtener al buscar en ella son:**

- **codigo de acceso y contraseñas**
- **Numeros de telefono, correos electronicos y direcciones domiciliarias de clientes, socios comerciales, proveedores y familiares .**
- **Diseños de productos, planos y borradores de planos de negocio.**
- **Numeros de tarjeta de credito y cuentas bancarias del personal y clientes comerciales.**
- **CD, DVD, USB Y otros dispositivos de almacenamiento portátiles.**



**Las diferentes técnicas de manipulación que usan los ciberdelicuentes para obtener información confidencial de los usuarios como:**

- **llamadas telefónicas**
- **visitas personales al domicilio de las personas**
- **Aplicación de mensajería instantánea**
- **Correos electrónicos**
- **Redes sociales**

**Los ataques de ingeniería social son muy difíciles de identificar en donde usan diferentes técnicas psicológicas y sociales, distintos tipos de dispositivos y plataformas para engañar a las personas.**

**-Configura la privacidad en las redes sociales para que no queden expuestos tus datos personales.**

**-Usa una contraseña segura**

**-Configura la autenticación en dos pasos para estar alerta de accesos indebidos a tus cuentas.**

**-presta atención a cualquier persona que te pida información personal.**