INTELIGENCIA MISCELÁNEO

MATERIA: ANALISIS DE VULNERABILIDADES

ALUMNO: SERGIO BENJAMÍN TORRES PÉREZ
GRADO Y GRUPO: 7-N
MATRICULA: A200248
DOCENTE: DR GUTIÉRREZ ALFARO LUIS

GOBUSTER

Gobuster es una herramienta utilizada para realizar fuerza bruta a: URIs (directorios y archivos) en sitios web, subdominios DNS (con soporte de comodines), y nombres de hosts virtuales en los servidores web.
Gobuster tiene tres modos disponibles. “dir”, el modo clásico de fuerza bruta contra directorios, “dns”, el modo de fuerza bruta contra subdominios DNS, y “vhost”, el modo de fuerza bruta contra hosts virtuales (no es lo mismo a “DNS”).

Resumiendo tiene la capacidad de realizar las siguientes enumeraciones:

-URIs (directorios y ficheros) en portales web
-Subdominios DNS con soporte para wildcard
-Nombres de virtual hosts en servidores web
-Buckets S3 de Amazon públicos

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.

«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.