



# **Universidad Autónoma de Chiapas**

## **Facultad de Contaduría y Administración**

### **Campus I**

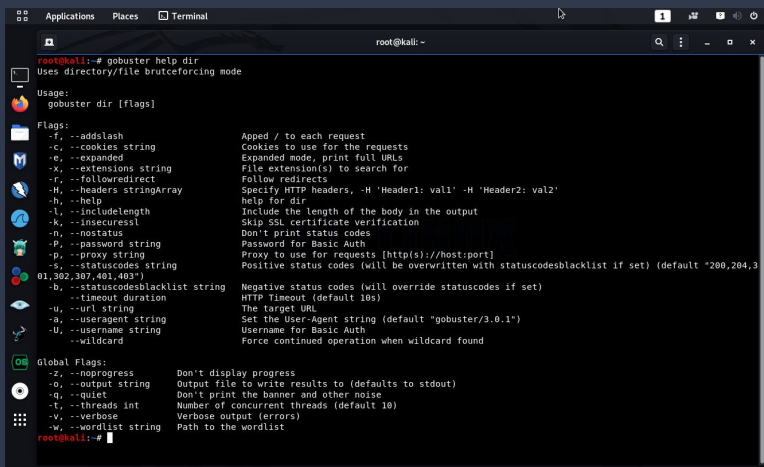
### **Ingeniería en Desarrollo y Tecnologías de Software.**

Materia: Análisis de vulnerabilidades

Alumno: Joahan Jimenez Ramirez 7"N"

Inteligencia Misceláneo:

# Gobuster



```
root@kali:~# gobuster help dir
Uses directory/file bruteforcing mode

Usage:
gobuster dir [flags]

Flags:
  -f, --addslash           Append / to each request
  -C, --cookies string     Cookies to use for the requests
  -e, --expanded           Expanded mode, print full URLs
  -x, --extensions string  File extension(s) to search for
  -r, --followredirect     Follow redirects
  -H, --headers stringArray Specify HTTP headers, -H 'Header1: val1' -H 'Header2: val2'
  -h, --help              help for dir
  -l, --includelength      Include the length of the body in the output
  -k, --insecuressl        Skip SSL certificate verification
  -n, --nostatus           Don't print status codes
  -P, --password string    Password for Basic Auth
  -p, --proxy string       Proxy to use for requests [http(s)://host:port]
  -s, --statuscodes string Positive status codes (will be overwritten with statuscodesblacklist if set) (default "200,204,301,302,307,401,403")
  -b, --statuscodesblacklist string Negative status codes (will override statuscodes if set)
  -t, --timeout duration   HTTP Timeout (default 10s)
  -u, --url string          The target URL
  -s, --useragent string    Set the User-Agent string (default "gobuster/3.0.1")
  -U, --username string     Username for Basic Auth
  -w, --wildcard            Force continued operation when wildcard found

Global Flags:
  -z, --noprogess          Don't display progress
  -o, --output string       Output file to write results to (defaults to stdout)
  -q, --quiet              Don't print the banner and other noise
  -t, --threads int        Number of concurrent threads (default 10)
  -v, --verbose            Verbose output (errors)
  -w, --wordlist string     Path to the wordlist

root@kali:~#
```

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”).

# 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.

# 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.