

INTELIGENCIA MISCELÁNEO

MARCOS JAVIER CANCINO HERNÁNDEZ - A200353
ANÁLISIS DE VULNERABILIDADES - 7° "N"





GOBUSTER

- Gobuster es una herramienta de código abierto utilizada en pruebas de penetración y seguridad cibernética. Su objetivo principal es realizar ataques de fuerza bruta o enumeración de directorios en aplicaciones web
- Esto significa que Gobuster intentará adivinar nombres de archivos y directorios mediante el uso de listas predefinidas, lo que podría ayudar a descubrir recursos ocultos o no autorizados en un sitio web. Aunque esta herramienta puede ser valiosa para identificar posibles vulnerabilidades, también puede ser utilizada de manera maliciosa para intentar acceder a áreas restringidas sin permiso.

```
gobuster : bash — Konsole
r00t@r00t-KitPloit:~/KitPloit/gobuster$ ./gobuster -h
Usage:
  gobuster [command]

Available Commands:
  dir      Uses directory/file bruteforcing mode
  dns      Uses DNS subdomain bruteforcing mode
  help     Help about any command
  vhost    Uses VHOST bruteforcing mode

Flags:
  --delay duration    Time each thread waits between requests (e.g. 1500ms)
  -h, --help          help for gobuster
  -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

Use "gobuster [command] --help" for more information about a command.
r00t@r00t-KitPloit:~/KitPloit/gobuster$
```



D U M P S T E R D I V I N G

- El "dumpster diving" (buceo en la basura) es una técnica que implica buscar información valiosa o sensible en la basura de una organización. A menudo, los atacantes o investigadores de seguridad buscan documentos impresos, discos duros, medios de almacenamiento o cualquier otro material que pueda contener información confidencial.
- Aunque puede sonar poco convencional, el "dumpster diving" puede revelar información útil para realizar ataques de ingeniería social o incluso obtener acceso no autorizado a sistemas.





INGENIERIA SOCIAL

- La ingeniería social es una táctica que implica manipular a las personas para obtener información o acceso a sistemas y recursos. Esto puede incluir técnicas como el engaño, la persuasión o la explotación de la confianza para obtener información confidencial, como contraseñas, datos personales o detalles de seguridad.
- La ingeniería social es una de las mayores amenazas para la seguridad cibernética, ya que explota la naturaleza humana y puede ser difícil de detectar.



ESTOS TRES TÉRMINOS REFLEJAN ÁREAS DIFERENTES PERO RELACIONADAS EN EL CAMPO DE LA SEGURIDAD INFORMÁTICA Y LA OBTENCIÓN DE INFORMACIÓN. MIENTRAS QUE GOBUSTER SE CENTRA EN LA EXPLORACIÓN DE APLICACIONES WEB, EL "DUMPSTER DIVING" SE ENFOCA EN LA OBTENCIÓN DE INFORMACIÓN DE DOCUMENTOS FÍSICOS Y MATERIALES DESECHADOS, Y LA INGENIERÍA SOCIAL INVOLUCRA LA MANIPULACIÓN DE PERSONAS PARA OBTENER ACCESO A SISTEMAS O INFORMACIÓN. CADA UNO DE ESTOS CONCEPTOS PUEDE TENER IMPLICACIONES IMPORTANTES EN LA SEGURIDAD CIBERNÉTICA Y LA PROTECCIÓN DE LA INFORMACIÓN.

