ENUMERAÇÃO → DIRETÓRIOS

GOBUSTER

gobuster dir --url [ip_address]:[port] -w

Diretórios	..seclists/Discovery/Web-Content/common.txt
	..seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt

Want Server return	..seclists/../ --status-codes [http_code]
Don't want Server return	..seclists/../ --status-codes-blacklist [http_code]

O *primeiro*, quando usado, os códigos listados IRÃO aparecer nos resultados
O *segundo*, quando usado, os códigos listados NÃO IRÃO aparecer nos resultados
Útil para reduzir ruído
Excluir códigos HTTP pode ocultar informações úteis em alguns testes
Escolha códigos a excluir conforme o objetivo da enumeração
Códigos comuns: 200,204,301,302,307,401,403

Buscar arquivos de backup	--discover-backup

Instrui o Gobuster a, ao encontrar um arquivo/endpoint válido
Automaticamente testar variações comuns de arquivos de backup desse recurso
Gera mais requisições
Pode aumentar os falsos positivos. Conferir manualmente

Adicionar extensões em uma wordlist	--extensions

Faz apendizar de uma lista de extensões às entradas da wordlist
A lista é vírgula-separada: -x php,html,js
Pode ser com ou sem o ponto, como: php e .php
Extensões comuns:

- **web comuns:** php,html,asp,aspx,jsp,cfm
- **estáticos / front:** js,css,txt,md,json,xml
- **config/credenciais:** env,sql,db,ini,conf,inc
- **backups & compressos:** bak,old,orig,zip,tar.gz,tar,gz,rar
- **logs / dumps:** log,dump,sql

Muitas extensões + wordlist grande → explode o número de requisições e aumenta chance de bloqueio/false-positives
Faça rodadas com cada um dos tipos de extensões

Seguir respostas de redirecionamento	--follow-redirect

Instrui o Gobuster a seguir respostas de redirecionamento (3xx) recebidas durante a enumeração

Em vez de só listar o redirect (ex.: 302 com Location), o Gobuster tenta o recurso apontado pelo redirecionamento e reportar o resultado final

Útil para identificar redirect chains que escondem recursos ou para confirmar que um endpoint realmente leva a algo acessível

Valide manualmente se o comportamento for crítico