
```
  gobuster [command]

Available commands:
  dir         Uses directory/file enumeration mode
  dns         Uses DNS subdomain enumeration mode
  fuzz        Uses fuzzing mode
  help        Help about any command
  s3          Uses aws bucket enumeration mode
  version     shows the current version
  vhost       Uses VHOST enumeration mode

Flags:
      --delay duration    Time each thread waits between requests (e.g. 1500ms)
  -h, --help              help for gobuster
      --no-error          Don't display errors
  -z, --no-progress       Don't display progress
  -o, --output string     Output file to write results to (defaults to stdout)
  -p, --pattern string    File containing replacement patters
  -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
```

Wordlists

Gobuster needs wordlists. One of the essential flags for gobuster is `-w` . Wordlists can be obtained from various places. Depending on the individual setup, wordlists may be preinstalled or found within other packages, including wordlists from Dirb or Dirbuster. The ultimate source and "Pentesters friend" is **SecLists** - https://github.com/danielmiessler/SecLists which is a compilation of numerous lists held in one location.

Gobuster DIR command

The DIR mode is used for finding hidden directories and files.

To find additional flags available to use `gobuster dir --help`


```
Usage:
  gobuster dir [flags]

Flags:
  -f, --add-slash                     Append / to each request
  -c, --cookies string                Cookies to use for the requests
  -d, --discover-backup               Upon finding a file search for backup files
      --exclude-length ints           exclude the following content length (completely ignc
  -e, --expanded                      Expanded mode, print full URLs
  -x, --extensions string             File extension(s) to search for
  -r, --follow-redirect               Follow redirects
  -H, --headers stringArray           Specify HTTP headers, -H 'Header1: val1' -H 'Header2:
  -h, --help                          help for dir
      --hide-length                   Hide the length of the body in the output
  -m, --method string                 Use the following HTTP method (default "GET")
  -n, --no-status                     Don't print status codes
  -k, --no-tls-validation             Skip TLS certificate verification
  -P, --password string               Password for Basic Auth
      --proxy string                  Proxy to use for requests [http(s)://host:port]
      --random-agent                  Use a random User-Agent string
  -s, --status-codes string           Positive status codes (will be overwritten with statu
  -b, --status-codes-blacklist string Negative status codes (will override status-codes if
      --timeout duration              HTTP Timeout (default 10s)
  -u, --url string                    The target URL
  -a, --useragent string              Set the User-Agent string (default "gobuster/3.1.0")
  -U, --username string               Username for Basic Auth
      --wildcard                      Force continued operation when wildcard found

Global Flags:
      --delay duration    Time each thread waits between requests (e.g. 1500ms)
      --no-error          Don't display errors
  -z, --no-progress       Don't display progress
  -o, --output string     Output file to write results to (defaults to stdout)
  -p, --pattern string    File containing replacement patterns
  -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
```

Flags

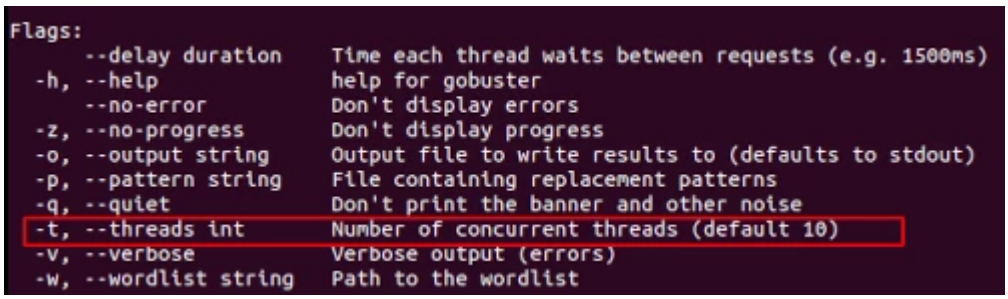
The 2 flags required to run a basic scan are `-u -w`. This example uses `common.txt` from the SecList

```
===============================================================
[+] Url:                     https://example.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /wordlists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/03/01 10:34:16 Starting gobuster in directory enumeration mode
===============================================================
/assets
/css
/download
```

Not too many results and was quite heavy on the system processess. Results depend on the wordlist selected. It is worth working out which one is best for the job. The length of time depends on how large the wordlist is. It can also be worth creating a wordlist specific to the job at hand using a variety of resources.

Threads

Gobuster is fast, with hundreds of requests being sent using the default 10 threads. This speeds can create problems with the system it is running on. It could be beneficial to drop this down to 4.



Additionally it can be helpful to use the flag `--delay duration Time each thread waits between requests (e.g. 1500ms).` For example `--delay 1s` in other words, if threads is set to 4 and --delay to 1s, this will send 4 requests per second.

```
user@matrix:$ gobuster dir -u https://example.com -w /wordlists/Discovery/Web-Content/directc

===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://example.co.uk/
[+] Method:                  GET
[+] Threads:                 4
[+] Delay:                   1s
[+] Wordlist:                /wordlists/Discovery/Web-Content/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/03/08 12:12:19 Starting gobuster in directory enumeration mode
===============================================================
/admin
/aux
===============================================================
2022/03/08 12:46:57 Finished
===============================================================
```

Took a while, but by filtering the results to an output file its easy to see and retain for future enumerating, what was located. A few more interesting results this time.

```
/admin                (Status: 302) [Size: 0] [--> /login.jsp]
/aux                  (Status: 200) [Size: 0
/robots.txt           (Status: 200) [Size: 0]
/images               (Status: 302) [Size: 0] [--> /images/]
/lpt1                 (Status: 200) [Size: 0]
/static               (Status: 302) [Size: 0] [--> /static/]
/util                 (Status: 302) [Size: 0] [--> /util/]
```

Other DIR flag examples

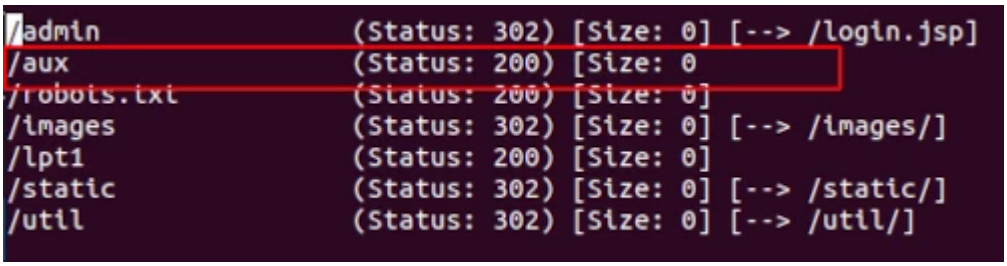
The results above show status codes. To exclude status codes use `-n`

```
user@matrix:$ gobuster dir -u https://example.com -w /wordlists/Discovery/Web-Content
```


```
user@matrix:$ gobuster dir -u https://example.com -w /wordlists/Discovery/Web-Content
```

Continue enumerating

Continue to enumerate results to find as much information as possible. Run gobuster again with the results found and see what else appears. Keep digging to locate those hidden directories.




```
$ gobuster dir -u https://example.com/aux -w /wordlists/Discovery/Web-Content/big.txt
```

Gobuster DNS command

Use the DNS command to **discover subdomains** with Gobuster. To see the options and flags available specifically for the DNS command use: `gobuster dns --help`

```
user@matrix:$ gobuster dns --help
Uses DNS subdomain enumeration mode

Usage:
  gobuster dns [flags]

Flags:
  -d, --domain string      The target domain
  -h, --help               help for dns
  -r, --resolver string    Use custom DNS server (format server.com or server.com:port)
```


```
  -z, --no-progress       Don't display progress
  -o, --output string     Output file to write results to (defaults to stdout)
  -p, --pattern string    File containing replacement patterns
  -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
```

DNS example

```
$ gobuster dns -q -r 8.8.8.8 -d example.com -w wordlists/Discovery/DNS/subdomains-top
```

Breaking this down.

`dns` mode
`-q` --quiet : Don't print the banner and other noise
`-r` --resolver string : Use custom DNS server (format server.com or server.com:port)
`-d` --domain string
`-w` --wordlist string : Path to the wordlist
`-t` --threads
`--delay` -- delay duration
`-o` --output string : Output file to write results to (defaults to stdout)

Using another of the Seclists wordlists `/wordlists/Discovery/DNS/subdomains-top1million-5000.txt`.

Results

In this case, as the flag `-q` for quiet mode was used, only the results are shown, the Gobuster banner and other information are removed.

```
Found: www.example.com
Found: nagios.example.com
```


```
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     example.com
[+] Threads:    4
[+] Delay:      1s
[+] Resolver:   8.8.8.8
[+] Timeout:    1s
[+] Wordlist:   /home/wordlists/subdomains-top1million-5000.txt
===============================================================
2022/03/18 16:20:35 Starting gobuster in DNS enumeration mode
===============================================================

Found: www.example.com
Found: nagios.example.com
Found: dev.example.com
Found: auto.example.com

===============================================================
2022/03/18 16:20:37 Finished
===============================================================
```

Gobuster VHost command

The vhost command discovers Virtual host names on target web servers. Virtual hosting is a technique for hosting multiple domain names on a single server.

Exposing hostnames on a server may reveal supplementary web content belonging to the target. Vhost checks if the subdomains exist by visiting the formed URL and cross-checking the IP address.

To brute-force virtual hosts, use the same wordlists as for DNS brute-forcing subdomains.

Similar to brute forcing subdomains eg. url = example.com, vhost looks for dev.example.com or beta.example.com etc.

For options and flags available use `gobuster vhost --help`


```
Usage:
  gobuster vhost [flags]

Flags:
  -c, --cookies string        Cookies to use for the requests
  -r, --follow-redirect       Follow redirects
  -H, --headers stringArray   Specify HTTP headers, -H 'Header1: val1' -H 'Header2: v
  -h, --help                  help for vhost
  -m, --method string         Use the following HTTP method (default "GET")
  -k, --no-tls-validation     Skip TLS certificate verification
  -P, --password string       Password for Basic Auth
      --proxy string          Proxy to use for requests [http(s)://host:port]
      --random-agent          Use a random User-Agent string
      --timeout duration      HTTP Timeout (default 10s)
  -u, --url string            The target URL
  -a, --useragent string      Set the User-Agent string (default "gobuster/3.1.0")
  -U, --username string       Username for Basic Auth

Global Flags:
      --delay duration    Time each thread waits between requests (e.g. 1500ms)
      --no-error          Don't display errors
  -z, --no-progress       Don't display progress
  -o, --output string     Output file to write results to (defaults to stdout)
  -p, --pattern string    File containing replacement patterns
  -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
```

As shown above the Global flags are the same as for the all modes. Again, the 2 essential flags are the `-u` URL and `-w` wordlist. Not essential but useful `-o` output file and `-t` threads, `-q` for quiet mode to show the results only.

Vhost example

```
user@matrix:$ gobuster vhost -u https://example.com -t 50 -w /wordlists/Discovery/DNS/subdoma
```