Gobuster

1. Introduction:

- **Gobuster:**
  Gobuster is a fast command-line tool written in Go used for directory brute forcing, DNS enumeration, virtual host discovery, and fuzzing. It is widely used in penetration testing to discover hidden paths and services. It relies on sending many HTTP requests quickly, which makes it powerful but also easily detectable by firewalls.

- **Strengths:**

➔ **Speed and Performance:** Written in Go, Gobuster is highly efficient and supports multi-threading (concurrent requests). This makes it significantly faster than older, similar tools like DirBuster, especially against large wordlists.

➔ **Versatility (Multiple Modes):** It can do much more than just web directory scanning. Its various modes include: **dir** (directories/files), **dns** (subdomains), **vhost** (virtual hosts), **s3** (Amazon S3 buckets), **gcs** (Google Cloud buckets), and **tftp** (TFTP files).

➔ **Customization:** Offers extensive command-line flags to customize the scan, including setting the number of threads (-t), specifying file extensions (-x), filtering by HTTP status codes (-s, -b), and adding delays (--delay).

- **Limitations:**

➔ **Reliance on Wordlists:** As a brute-forcing tool, its effectiveness is **entirely dependent** on the quality and size of the wordlist used. If a directory name is not in the list, Gobuster will not find it.

➔ **Noise and Detection:** Because it sends a large volume of requests in a short period, it is a very **"noisy"** tool. This high volume of traffic can be easily detected and blocked by Web Application Firewalls (WAFs) or intrusion detection systems (IDS).

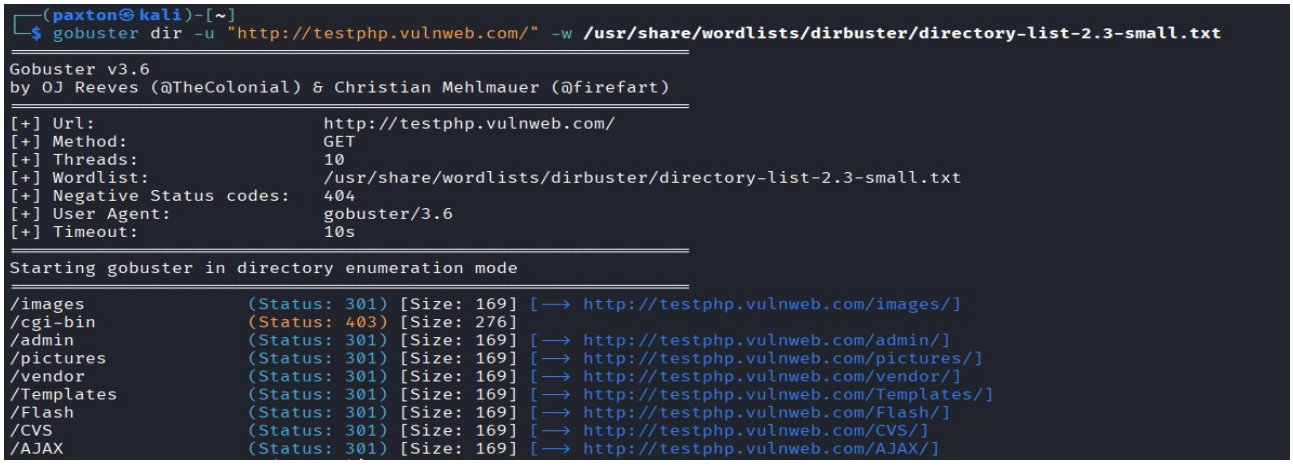
➔ **Can Overwhelm Servers:** If the thread count is set too high, especially against a slow or low-capacity server, Gobuster can inadvertently cause a **Denial of Service (DoS)** condition, crashing or severely degrading the performance of the target application.

2. Directory/File enumeration mode

- **Basic scan**

➔ **Command:** *gobuster dir -u "http://testphp.vulnweb.com/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt*

➔ **Description:** Scans your target URL for hidden directories and files using a wordlist. Useful for discovering admin panels, backup files, and internal paths



- **Scan with file extensions**
- ➔ **Command:** *gobuster dir -u "http://testphp.vulnweb.com/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php,html,txt*
- ➔ **Description:** Adds file extensions to each brute-force attempt. This is used to discover files such as login.php or debug.txt that attackers typically look for.

```
┌──(paxton㉿kali)-[~]
└─$ gobuster dir -u "http://testphp.vulnweb.com/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-small
.txt -x php,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://testphp.vulnweb.com/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/images/]
/index.php            (Status: 200) [Size: 4958]
/search.php           (Status: 200) [Size: 4732]
/cgi-bin              (Status: 403) [Size: 276]
/cgi-bin.html         (Status: 403) [Size: 276]
/login.php            (Status: 200) [Size: 5523]
/product.php          (Status: 200) [Size: 5056]
/disclaimer.php       (Status: 200) [Size: 5524]
/signup.php           (Status: 200) [Size: 6033]
/admin                (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/admin/]
/categories.php       (Status: 200) [Size: 6115]
/cart.php             (Status: 200) [Size: 4903]
/pictures             (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/pictures/]
Progress: 1991 / 350660 (0.57%)
```

- **Show only specific status codes**
- ➔ **Command:**
  1st Command: *gobuster dir -u "http://testphp.vulnweb.com/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -s 200,301*
  2nd Command: *gobuster dir -u "http://testphp.vulnweb.com/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -s 200,301 -b ""*
- ➔ **Description:** Filters results to only show valid responses from some status code. Helps you focus on real directories and ignore noise.
- ➔ **Issue in 1st command:** When I use 1st command , i got some issues and i researched and found that: By default, Gobuster automatically uses a **status-code-blacklist** (which typically excludes codes like **404 Not Found**, **403 Forbidden**, etc.). You cannot use both the allowed list (-s) and the default blacklist simultaneously, as they conflict.

```
┌──(paxton㉿kali)-[~]
└─$ gobuster dir -u "http://testphp.vulnweb.com/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-small
.txt -s 200,301
Error: error on parsing arguments: status-codes ("200,301") and status-codes-blacklist ("404") are both set
- please set only one. status-codes-blacklist is set by default so you might want to disable it by supplying
 an empty string.
```

→ **Solution in 2nd Command:** To solve this, you need to tell Gobuster to **disable the default blacklist** when you supply your own list of allowed codes using the -s flag. You do this by setting the blacklist to an empty string with the **-b** or **--status-codes-blacklist** flag.

```
┌──(paxton㉿kali)-[~]
└─$ gobuster dir -u "http://testphp.vulnweb.com/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-small
.txt -s 200,301 -b ""
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:            http://testphp.vulnweb.com/
[+] Method:         GET
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Status codes:   200,301
[+] User Agent:     gobuster/3.6
[+] Timeout:        10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/images/]
/admin                (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/admin/]
/pictures             (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/pictures/]
/vendor               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/vendor/]
/Templates            (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/Templates/]
/Flash                (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/Flash/]
/CVS                  (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/CVS/]
/AJAX                 (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/AJAX/]
Progress: 11521 / 87665 (13.14%)
```

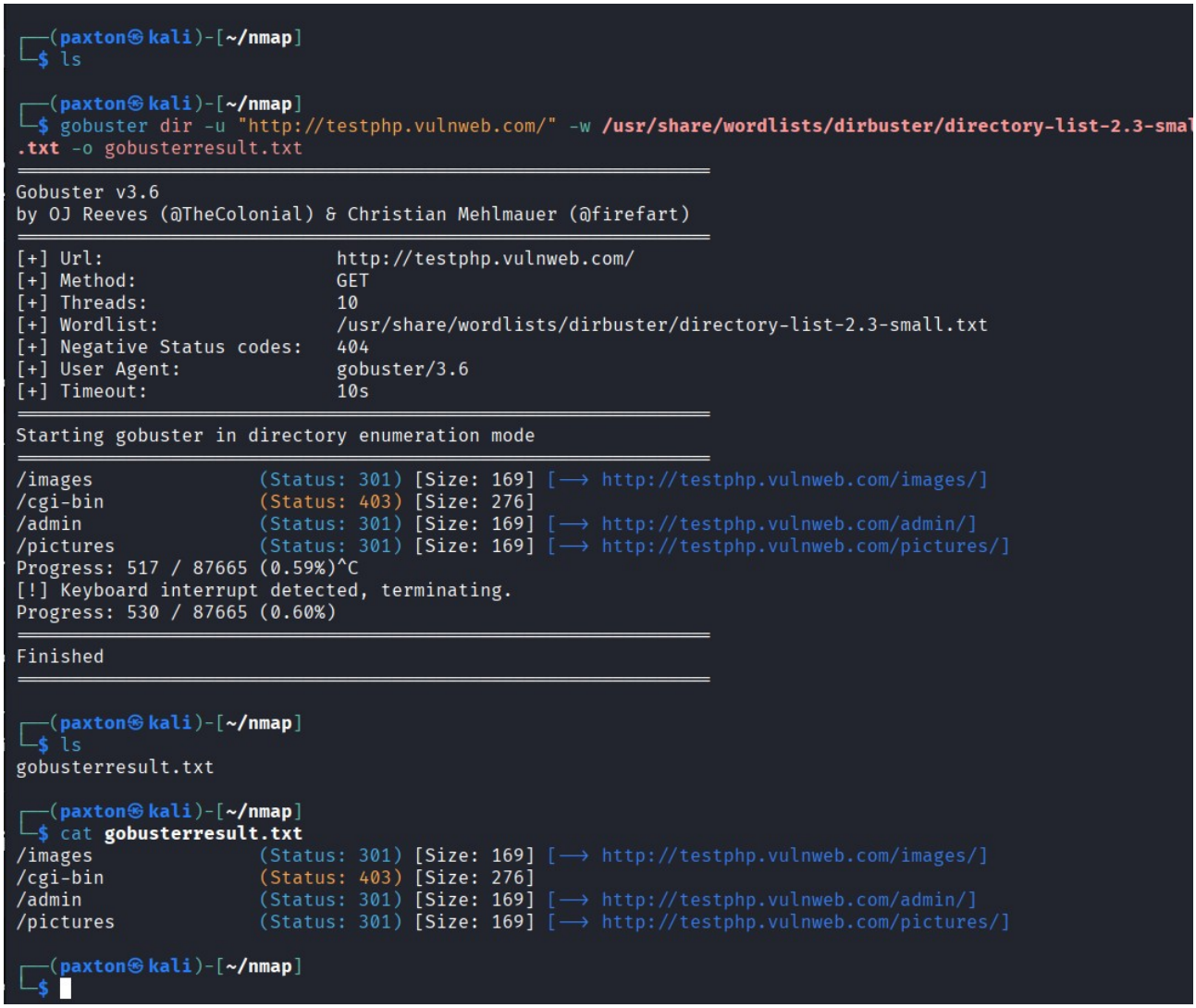
- **Hide specific status codes**

→ **Command:** *gobuster dir -u "http://testphp.vulnweb.com/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -b 404,403*

→ **Description:** Blacklists unwanted status codes so they don't appear in the output. This makes the results cleaner and easier to analyze.

```
┌──(paxton㉿kali)-[~]
└─$ gobuster dir -u "http://testphp.vulnweb.com/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-small
.txt -b 404,403
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                    http://testphp.vulnweb.com/
[+] Method:                 GET
[+] Threads:                10
[+] Wordlist:               /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:  404,403
[+] User Agent:             gobuster/3.6
[+] Timeout:                10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/images/]
/admin                (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/admin/]
/pictures             (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/pictures/]
/vendor               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/vendor/]
/styles               (Status: 500) [Size: 177]
/Templates            (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/Templates/]
/Flash                (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/Flash/]
/CVS                  (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/CVS/]
/AJAX                 (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/AJAX/]
/secured              (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/secured/]
/bar4-r               (Status: 500) [Size: 177]
/myaol                (Status: 500) [Size: 177]
/symnasmb             (Status: 500) [Size: 177]
/ani                  (Status: 500) [Size: 177]
/22007                (Status: 500) [Size: 177]
/indx                 (Status: 500) [Size: 177]
/index-fr             (Status: 500) [Size: 177]
```

- **Save results to file**
- ➔ **Command:** *gobuster dir -u "http://testphp.vulnweb.com/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -o gobusterresult.txt*
- ➔ **Description:** Stores the scan output in a text file for documentation and future analysis. This is good for keeping logs of your own tests.



- **Increase threads (Faster scan)**
- ➔ **Command:** *gobuster dir -u target.com -w wordlist.txt -t 50*
- ➔ **Description:** Increases the number of threads to speed up the scan. Higher threads produce faster results but also increase firewall detection likelihood. Default is *-t 10*

3. DNS Enumeration (dns mode)

- **Basic dns scan**
- ➔ **Command:** *gobuster dns -d google.com -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt*
- ➔ **Description:** Discovers subdomains under your domain using brute forcing. Useful to identify hidden services like dev.yourlab.com or admin.yourlab.com.

```
┌──(paxton㉿kali)-[~/nmap]
└─$ gobuster dns -d google.com -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     google.com
[+] Threads:    10
[+] Timeout:    1s
[+] Wordlist:   /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
===============================================================
Starting gobuster in DNS enumeration mode
===============================================================
Found: smtp.google.com

Found: www.google.com

Found: mail.google.com

Found: ns1.google.com

Found: ns2.google.com

Found: ns.google.com

Found: m.google.com

Found: blog.google.com

Found: ns3.google.com

Found: admin.google.com

Found: vpn.google.com

Found: mobile.google.com

Found: support.google.com
```

- **Show IP in output**
- ➔ **Command:** *gobuster dns -d google.com -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -i*
- ➔ **Description:** Adds IP addresses to each discovered subdomain. This helps map your internal lab topology.

```
┌──(paxton㉿kali)-[~/nmap]
└─$ gobuster dns -d google.com -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -i
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     google.com
[+] Threads:    10
[+] Show IPs:   true
[+] Timeout:    1s
[+] Wordlist:   /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
===============================================================
Starting gobuster in DNS enumeration mode
===============================================================
Found: www.google.com [142.250.76.68,2404:6800:4002:810::2004]

Found: smtp.google.com [172.217.194.26,142.251.10.26,172.253.118.27,172.253.118.26,172.217.194.27,2404:6800:4003:c
04::1a,2404:6800:4003:c04::1b,2404:6800:4003:c05::1a,2404:6800:4003:c05::1b]

Found: mail.google.com [142.250.182.37,2404:6800:4002:802::2005]

Found: ns1.google.com [216.239.32.10,2001:4860:4802:32::a]

Found: ns2.google.com [216.239.34.10,2001:4860:4802:34::a]

Found: ns.google.com [216.239.32.10]

Found: m.google.com [142.250.67.75,2404:6800:4002:806::200b]

Found: blog.google.com [142.250.67.73,2404:6800:4002:823::2009]
```

4. Virtual host enumeration (vhost mode)

- **Vhost scan**

➔ **Command:** *gobuster vhost -u target.com -w wordlist.txt*

➔ **Description:** Attempts to discover websites hosted on the same server IP using different Host headers. Useful for testing multi-site environments in your own lab.

5. Fuzzing mode (fuzz)

- **Simple path fuzzing**

➔ **Command:** *gobuster fuzz -u "http://testphp.vulnweb.com/FUZZ/index.php" -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -s 200,301,302 -b ""*

➔ **Description: R**eplaces FUZZ in the URL with each word in the list to find dynamic resources. This is used to map API routes or custom endpoints.

6. Firewall-Aware scanning

- **Reduce speed to avoid rate-limiting**

➔ **Command:** *gobuster dir -u http://yourlab.com -w wordlist.txt -t 5*

➔ **Description:** Lower threading reduces the number of requests per second. Firewalls are less likely to flag slow, human-like traffic.

- **Add delay between requests**

➔ **Command:** *gobuster dir -u "http://testphp.vulnweb.com/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt --delay 200ms*

➔ **Description:** A delay of 200 milliseconds mimics natural browsing behavior. This helps you learn how WAF heuristics interpret traffic pacing.

```
┌──(paxton㉿kali)-[~]
└─$ gobuster dir -u "http://testphp.vulnweb.com/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt --delay 200ms
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://testphp.vulnweb.com/
[+] Method:                  GET
[+] Threads:                 10
[+] Delay:                   200ms
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/images/]
/cgi-bin              (Status: 403) [Size: 276]
/admin                (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/admin/]
/pictures             (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/pictures/]
/vendor               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/vendor/]
```

- **Change user-agent**

➔ **Command:** *gobuster dir -u "http://testphp.vulnweb.com/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt –random-agent or gobuster dir -u http://yourlab.com -w wordlist.txt -a "Mozilla/5.0 (Windows NT 10.0)"*

➔ **Description:** Many firewalls flag default scanner user-agents. Using a common browser string lets you test WAF behavior safely without offensive impersonation.

- **Use HEAD instead of get**

➔ **Command:** *gobuster dir -u "http://testphp.vulnweb.com/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt --method HEAD -b 404,500*

➔ **Description:** HEAD requests only return headers, not the full webpage body. This reduces bandwidth usage and makes requests appear lighter to firewalls.

```
┌──(paxton㉿kali)-[~]
└─$ gobuster dir -u "http://testphp.vulnweb.com/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt --method HEAD -b 404,500
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://testphp.vulnweb.com/
[+] Method:                  HEAD
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   500,404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 0] [--> http://testphp.vulnweb.com/images/]
/cgi-bin              (Status: 403) [Size: 0]
/admin                (Status: 301) [Size: 0] [--> http://testphp.vulnweb.com/admin/]
/pictures             (Status: 301) [Size: 0] [--> http://testphp.vulnweb.com/pictures/]
/vendor               (Status: 301) [Size: 0] [--> http://testphp.vulnweb.com/vendor/]
```

- **Use proxy (Burpsuite)**

➔ **Command:** *gobuster dir -u http://yourlab.com -w wordlist.txt --proxy http://127.0.0.1:8080*

➔ **Description:** Sends all Gobuster traffic through Burp Suite, allowing you to throttle, inspect, or modify requests. This is perfect for learning how firewalls interpret request headers.