🧾 Gobuster Ultimate Professional Cheat Sheet

🔹 1. Introduction

- **Tool:** Gobuster
- **Use Case:** Directory/File, DNS, and VHost brute forcing
- **Why Gobuster?**
  - Faster than Dirb (written in Go)
  - Supports multiple modes (dir, dns, vhost, s3, fuzz)
  - Works with custom wordlists

🔹 2. Basic Syntax

```
gobuster <mode> -u <URL> -w <wordlist> [options]
```

Modes:

- dir → Directory/File brute forcing
- dns → DNS subdomain brute forcing
- vhost → Virtual host discovery
- s3 → AWS S3 bucket enumeration
- fuzz → Generic fuzzing

🔹 3. Directory Brute Force (dir mode)

Basic Scan

```
gobuster dir -u http://target.com -w /usr/share/wordlists/dirb/common.txt
```

With File Extensions

```
gobuster dir -u http://target.com -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt
```

Ignore SSL Errors (HTTPS)

```
gobuster dir -u https://target.com -w wordlist.txt -k
```

🔹 4. DNS Subdomain Enumeration (dns mode)

Basic Subdomain Scan

```
gobuster dns -d target.com -w /usr/share/wordlists/dns/subdomains-top1million-5000.txt
```

With a Specific Resolver

```
gobuster dns -d target.com -w wordlist.txt -r 8.8.8.8
```

◆ 5. VHost Enumeration (vhost mode)

```
gobuster vhost -u http://target.com -w /usr/share/wordlists/vhosts.txt
```

◆ 6. Useful Options

Option	Description
-u	Target URL
-w	Wordlist path
-x	File extensions (comma-separated)
-t	Threads (default: 10)
-s	Status codes to show (e.g., 200,204,301,302)
--timeout	Request timeout
-r	Custom DNS resolver
-k	Skip SSL certificate check

◆ 7. Advanced Usage

Save Results to File

```
gobuster dir -u http://target.com -w wordlist.txt -o results.txt
```

Exclude Status Codes

```
gobuster dir -u http://target.com -w wordlist.txt -b 404,403
```

Increase Threads for Speed

```
gobuster dir -u http://target.com -w wordlist.txt -t 50
```

Add Cookies (Authenticated Fuzzing)

```
gobuster dir -u http://target.com -w wordlist.txt --cookies "PHPSESSID=abcd1234"
```

🔹 8. Tips & Notes

- **Common Wordlists:**
  - /usr/share/wordlists/dirb/common.txt
  - /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
  - SecLists/Discovery/Web-Content/
- **Pairing:**
  - Use with **Nikto** for vulnerabilities
  - Use with **Burp Suite Intruder** for deeper fuzzing
- **When to Use Gobuster over Dirb:**
  - For faster scans
  - For advanced modes (DNS, VHost, Fuzz)