Gobuster - The Basics

Gobuster, often used for reconnaissance. Can enumerate web directories, subdomains, and virtual hosts

Gobuster: Introduction

Gobuster is an open-source offensive tool written in Golang

It enumerates web directories, DNS subdomains, vhosts, Amazon S3 buckets, and Google Cloud Storage by brute force, using specific wordlists and handling the incoming responses.

security professionals use this tool for penetration testing, bug bounty hunting, and cyber security assessments.

we can place Gobuster between the reconnaissance and scanning phases

Enumeration
Enumeration is the act of listing all the available resources, whether they are accessible or not. For example, Gobuster enumerates web directories.

Brute Force
Brute force is the act of trying every possibility until a match is found. It is like having ten keys and trying them all on a lock until one fits. Gobuster uses wordlists for this purpose.

Gobuster: Overview

gobuster --help

The help page contains multiple sections:

- **Usage:** Shows the syntax on how to use the command.
- **Available Commands:** Multiple commands are available to aid us in enumerating directories, files, DNS subdomains, Google Cloud Storage buckets, and Amazon AWS S3 buckets. Throughout this room, we will focus on the `dir`, `dns`, and `vhost` commands. We will cover each of them in the following tasks.
- **Flags:** These are specific options we can configure to customize our commands.

Short Flag	Long Flag	Description
`-t`	`--threads`	This flag configures the number of threads to use for the scan. Each of these threads sends out requests with a slight delay. The default number of threads is 10. This number may be slow when using large wordlists. You can increase or decrease the number of threads depending on the available system resources.
`-w`	`--wordlist`	The flag configures a wordlist to use for iterating. Each wordlist entry is attached to the URL you included in the command.
	`--delay`	This flag defines the amount of time to wait between sending requests. Some web servers include mechanisms to detect enumeration by looking at how many requests are received in a certain period of time. We can increase the delay between subsequent requests to make it look like normal web traffic.
	`--debug`	This flag helps us to troubleshoot when our command gives unexpected errors.
`-o`	`--output`	This flag writes the enumeration results to a file we choose.

Example

Let us look at an example of how we would use these commands and flags together to enumerate a web directory:

```
gobuster dir -u "http://www.example.thm/" -w
/usr/share/wordlists/dirb/small.txt -t 64
```

- `gobuster dir` indicates that we will use the directory and file enumeration mode.
- `-u "http://www.example.thm/"` tells Gobuster that the target URL is http://example.thm/.
- `-w /usr/share/wordlists/dirb/small.txt` directs Gobuster to use the *small.txt* wordlist to brute force the web directories. Gobuster will use each entry in the wordlist to form a new URL and send a GET request to that URL. If the first entry of the wordlist were images, Gobuster would send a GET request to http://example.thm/images/.
- `-t 64` sets the number of threads Gobuster will use to 64. This improves the performance drastically.

Use Case: Directory and File Enumeration

Gobuster has a `dir` mode, allowing users to enumerate website directories and their files.

useful when you are performing a penetration test and would like to see what the directory structure of a website is and what files it contains

Gobuster is powerful because it allows you to scan the website and return the status codes. These status codes immediately tell you if you, as an outside user, can request that directory or not.

Help

gobuster dir --help

Many flags are used to fine-tune the `gobuster dir` command

Flag	Long Flag	Description
`-c`	`--cookies`	This flag configures a cookie to pass along each request, such as a session ID.
`-x`	`--extensions`	This flag specifies which file extensions you want to scan for. E.g., .php, .js
`-H`	`--headers`	This flag configures an entire header to pass along with each request.
`-k`	`--no-tls-validation`	This flag skips the process that checks the certificate when https is used. It often happens for CTF events or test rooms like the ones on THM a self-signed certificate is used. This causes an error during the TLS check.
`-n`	`--no-status`	You can set this flag when you don't want to see status codes of each response received. This helps keep the output on the screen clear.
`-P`	`password`	You can set this flag together with the --username flag to execute authenticated requests. This is handy when you have obtained credentials from a user.
`-s`	`--status-codes`	With this flag, you can configure which status codes of the received responses you want to display, such as 200, or a range like 300-400.
`-b`	`--status-codes-blacklist`	This flag allows you to configure which status codes of the received responses you don't want to display. Configuring this flag overrides the -s flag.
`-U`	`--username`	You can set this flag together with the `--password` flag to execute authenticated requests. This is handy when you have obtained credentials from a user.
`-r`	`--followredirect`	This flags configures Gobuster to follow the redirect that it received as a response to the sent request. A HTTP redirect status code (e.g., 301 or 302) is used to redirect the client to a different URL.

How To Use dir Mode

To run Gobuster in `dir` mode, use the following command format:

```
gobuster dir -u "http://www.example.thm" -w /path/to/wordlist
```

practical example of how to enumerate directories and files with Gobuster `dir` mode:

```
gobuster dir -u "http://www.example.thm" -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -r
```

This command scans all the directories located at *www.example.thm* using the wordlist *directory-list-2.3-medium.txt*. Let's look a bit closer at each part of the command:

- `gobuster dir`: Configures Gobuster to use the directory and file enumeration mode.
- `-u http://www.example.thm`:
- The URL will be the base path where Gobuster starts looking. So, the URL above is using the root web directory. For example, in a typical Apache installation on Linux, this is `/var/www/html`. So if you have a "resources" directory and you want to enumerate that directory, you'd set the URL as `http://www.example.thm/resources`. You can also think of this like `http://www.example.thm/path/to/folder`.
- The URL must contain the protocol used, in this case, HTTP. This is important and required. If you pass the wrong protocol, the scan will fail.
- In the host part of the URL, you can either fill in the IP or the HOSTNAME. However, it is important to mention that when using the IP, you may target a different website than intended. A web server can host multiple websites using one IP (this technique is also called virtual hosting). Use the HOSTNAME if you want to be sure.
- Gobuster does not enumerate recursively. So, if the results show a directory path you are interested in, you will have to enumerate that specific directory.
- `-w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt` configures Gobuster to use the *directory-list-2.3-medium.txt* wordlist to enumerate. Each entry of the wordlist is appended to the configured URL.
- `-r` configures Gobuster to follow the redirect responses received from the sent requests. If a status code 301 was received, Gobuster will navigate to the redirect URL that is included in the response.

a second example where we use the `-x` flag to specify what type of files we want to enumerate:

```
gobuster dir -u "http://www.example.thm" -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .php,.js
```

Task

Enumerate directories of www.offensivetools.thm

I used this gobuster command

```
root@ip-10-81-124-183:~# gobuster dir -u "http://www.offensivetools.thm" -w /usr/share/wordlists/dirbuster/d
irectory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://www.offensivetools.thm
[+] Method:                  GET
[+] Threads:                 10
```

```
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 333]
/home                 (Status: 200) [Size: 8818]
/media                (Status: 301) [Size: 332]
/templates            (Status: 301) [Size: 336]
/modules              (Status: 301) [Size: 334]
/plugins              (Status: 301) [Size: 334]
/includes             (Status: 301) [Size: 335]
/language             (Status: 301) [Size: 335]
/components           (Status: 301) [Size: 337]
/api                  (Status: 301) [Size: 330]
/cache                (Status: 301) [Size: 332]
/libraries            (Status: 403) [Size: 287]
/tmp                  (Status: 301) [Size: 330]
/layouts              (Status: 301) [Size: 334]
/secret               (Status: 301) [Size: 333]
/administrator        (Status: 301) [Size: 340]
```

the secret directory catches my attention

once finding the different directory we can enumerate that by having the path url /[directory name] then also look for specific file types with -x [file type]

```
root@ip-10-81-124-183:~# gobuster dir -u "http://www.offensivetools.thm/secret" -w /usr/share/wordlists/d
uster/directory-list-2.3-medium.txt -x .js
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://www.offensivetools.thm/secret
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              js
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/content              (Status: 301) [Size: 341]
/uploads              (Status: 301) [Size: 341]
/flag.js              (Status: 200) [Size: 22]
```

I found the flag.js file and now we can use curl on the path and directory of that flag.js file to read that script

```
root@ip-10-81-124-183:~# curl www.offensivetools.thm/secret/flag.js
THM{ReconWasASuccess}
root@ip-10-81-124-183:~#
```

Use Case: Subdomain Enumeration

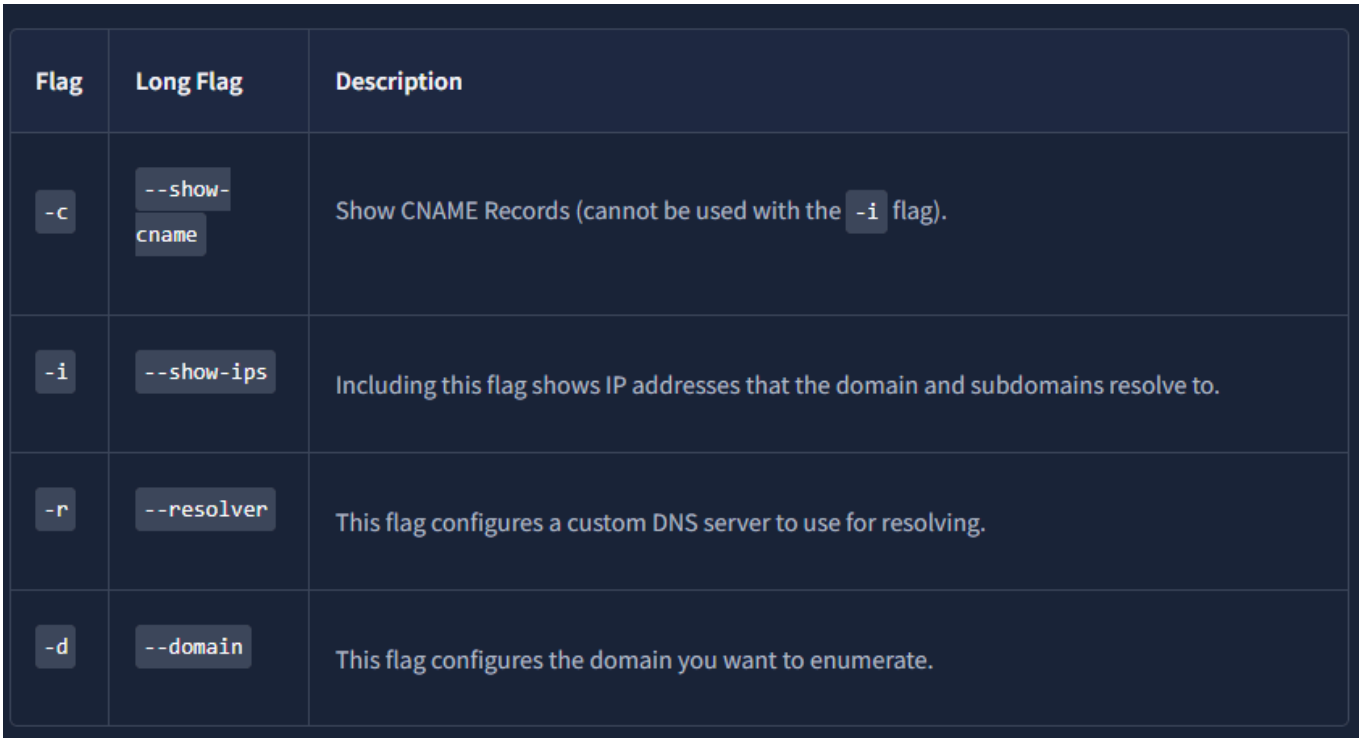
`dns` mode allows Gobuster to brute force subdomains.

During a penetration test, checking the subdomains of your target's top domain is essential. Just because something is patched in the regular domain, it doesn't mean it is also patched in

the subdomain.

Help

gobuster dns --help



Flag	Long Flag	Description
`-c`	`--show-cname`	Show CNAME Records (cannot be used with the `-i` flag).
`-i`	`--show-ips`	Including this flag shows IP addresses that the domain and subdomains resolve to.
`-r`	`--resolver`	This flag configures a custom DNS server to use for resolving.
`-d`	`--domain`	This flag configures the domain you want to enumerate.

How to Use dns Mode

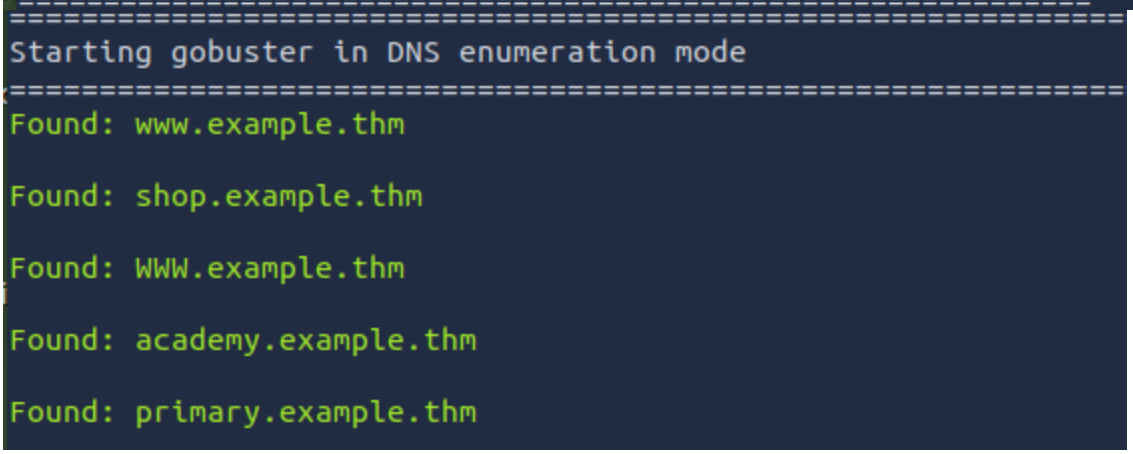
To run Gobuster in dns mode, use the following command syntax:
`gobuster dns -d example.thm -w /path/to/wordlist`

Let us look at an example of how to enumerate subdomains with Gobuster dns mode:

```
gobuster dns -d example.thm -w
/usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
```

- `gobuster dns` enumerates subdomains on the configured domain.
- `-d example.thm` sets the target to the *example.thm* domain.
- `-w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt` sets the wordlist to s*ubdomains-top1million-5000.txt*. Gobuster uses each entry of this list to construct a new DNS query. If the first entry of this list is 'all', the query would be *all.example.thm.*

```
root@ip-10-81-114-100:~# gobuster dns -d example.thm -w /usr/share/wordlists/Se
Lists/Discovery/DNS/subdomains-top1million-5000.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     example.thm
[+] Threads:    10
[+] Timeout:    1s
[+] Wordlist:   /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1mill
on-5000.txt
===============================================================
Starting gobuster in DNS enumeration mode
===============================================================
```



this lists the different subdomains

I then enumerated the subdomains of the offensivetools.thm domain and found 5 subdomains

```
root@ip-10-81-114-100:~# gobuster dns -d offensivetools.thm -w /usr/share/wordlists/SecLists/Discovery/DNS/
ubdomains-top1million-5000.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     offensivetools.thm
[+] Threads:    10
[+] Timeout:    1s
[+] Wordlist:   /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
===============================================================
Starting gobuster in DNS enumeration mode
===============================================================
Found: www.offensivetools.thm

Found: forum.offensivetools.thm

Found: store.offensivetools.thm

Found: WWW.offensivetools.thm

Found: primary.offensivetools.thm
```

Use Case: Vhost Enumeration

`vhost` mode allows Gobuster to brute force virtual hosts

Virtual hosts are different websites on the same machine.

The difference between `vhost` and `dns` mode is in the way Gobuster scans:

- `vhost` mode will navigate to the URL created by combining the configured HOSTNAME (-u flag) with an entry of a wordlist.
- `dns` mode will do a DNS lookup to the FQDN created by combining the configured domain name (-d flag) with an entry of a wordlist.

Help

gobuster vhost --help

Short Flag	Long Flag	Description
`-u`	`--url`	Specifies the base URL (target domain) for brute-forcing virtual hostnames.
	`--append-domain`	Appends the base domain to each word in the wordlist (e.g., word.example.com).
`-m`	`--method`	Specifies the HTTP method to use for the requests (e.g., GET, POST).
	`--domain`	Appends a domain to each wordlist entry to form a valid hostname (useful if not provided explicitly).
	`--exclude-length`	Excludes results based on the length of the response body (useful to filter out unwanted responses).
`-r`	`--follow-redirect`	Follows HTTP redirects (useful for cases where subdomains may redirect).

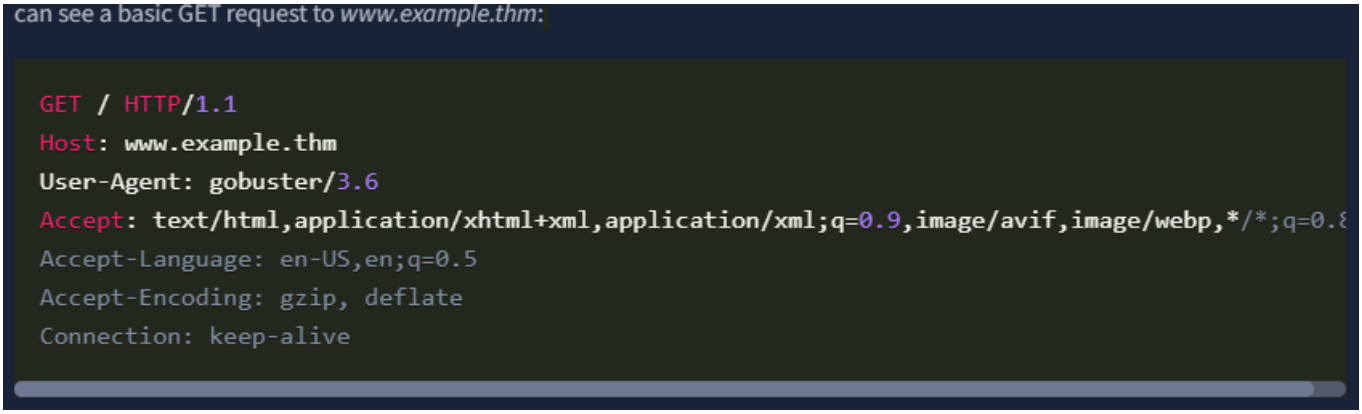
How To Use vhost Mode

To run Gobuster in `vhost` mode, type the following command:

```
gobuster vhost -u "http://example.thm" -w /path/to/wordlist
```

```
root@ip-10-81-114-100:~# gobuster vhost -u "http://10.81.144.28" --domain example.thm -w /usr/share/wordlist
s/SecLists/Discovery/DNS/subdomains-top1million-5000.txt --append-domain --exclude-length 250-320
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:              http://10.81.144.28
[+] Method:           GET
[+] Threads:          10
[+] Wordlist:         /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:       gobuster/3.6
[+] Timeout:          10s
[+] Append Domain:    true
[+] Exclude Length:   300,313,316,253,281,285,289,271,274,288,312,298,319,320,292,305,308,250,258,263,282,27
8,287,297,303,299,311,318,252,261,270,295,291,275,290,302,254,260,264,293,301,309,257,265,272,296,280,286,29
4,317,277,279,315,255,266,314,304,251,256,273,284,268,307,276,283,306,310,259,262,267,269
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: blog.example.thm Status: 200 [Size: 1493]
Found: shop.example.thm Status: 200 [Size: 2983]
Found: academy.example.thm Status: 200 [Size: 434]
Found: WWW.example.thm Status: 200 [Size: 84352]
Found: www.example.thm Status: 200 [Size: 84352]
Progress: 4997 / 4998 (99.98%)
===============================================================
Finished
===============================================================
```

don't have a fully set up DNS infrastructure. This requires us to give in extra flags like `--domain` and `--append-domain`. We need to look at the web requests Gobuster sends to understand better how these flags work.



Gobuster will send multiple requests, each time changing the `Host:` part of the request. The value of `Host:` in this example is *www.example.thm*. We can break this down into three parts:

- `www`: This is the subdomain. This is the part that Gobuster will fill in with each entry of the configured wordlist.
- `.example`: This is the second-level domain. You can configure this with the `--domain` flag (this needs to be configured together with the top-level domain).
- `.thm`: This is the top-level domain. You can configure this with the `--domain` flag (this needs to be configured together with the second-level domain).

Now that we know how Gobuster sends its request, let's break down the command and examine each flag more closely:

- `gobuster vhost` instructs Gobuster to enumerate virtual hosts.
- `-u "http://10.81.144.28"` sets the URL to browse to 10.81.144.28.
- `-w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt` configures Gobuster to use the *subdomains-top1million-5000.txt* wordlist. Gobuster appends each entry in the wordlist to the configured domain. If no domain is explicitly configured with the `--domain` flag, Gobuster will extract it from the URL. E.g., *test.example.thm*, *help.example.thm*, etc. If any subdomains are found, Gobuster will report them to you in the terminal.
- `--domain example.thm` sets the top- and second-level domains in the `Hostname:` part of the request to *example.thm*.
- `--append-domain` appends the configured domain to each entry in the wordlist. If this flag is not configured, the set hostname would be *www*, *blog*, etc. This will cause the command to work incorrectly and display false positives.
- `--exclude-length` filters the responses we get from the sent web requests. With this flag, we can filter out the false positives. If you run the command without this flag, you will notice you will get a lot of false positives like "Found: Orion.example.thm Status: 404 [Size: 279]" or "Found: pm.example.thm Status: 404 [Size: 276]". These false positives typically have a similar response size, so we can use this to filter out most false positives. We expect to get a 200 OK response back to have a true positive. There are, however, exceptions, but it is not in the scope of this room to go deeper into these.

I ran the command with offensivetools.thm domain and found 4 vhosts have the status code 200

```
root@ip-10-81-114-100:~# gobuster vhost -u "http://10.81.144.28" --domain offensivetools.thm -w /usr/share/w
ordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt --append-domain --exclude-length 250-320
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:              http://10.81.144.28
[+] Method:           GET
[+] Threads:          10
[+] Wordlist:         /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:       gobuster/3.6
[+] Timeout:          10s
[+] Append Domain:    true
[+] Exclude Length:   252,275,290,299,250,282,292,253,263,266,295,271,293,311,306,260,262,273,281,288,300,30
3,308,259,270,286,296,297,264,298,305,309,251,313,318,320,269,278,280,310,317,312,316,265,268,274,285,302,25
4,257,289,294,319,272,291,301,307,314,258,261,267,276,284,256,279,283,255,277,287,304,315
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: forum.offensivetools.thm Status: 200 [Size: 2635]
Found: store.offensivetools.thm Status: 200 [Size: 3014]
Found: secret.offensivetools.thm Status: 200 [Size: 1550]
Found: WWW.offensivetools.thm Status: 200 [Size: 8806]
Found: www.offensivetools.thm Status: 200 [Size: 8806]

===============================================================
Finished
===============================================================
```