



UJAR TECH SOLUTION

NAME: Rithik varma

INTERN ID: UTS1103

TASK 5

Directory Bruteforcing Using Dirb or Gobuster

To discover hidden directories and files on a target web server using brute-force tools like Dirb or Gobuster. This simulates how attackers identify weak or unprotected entry points in web applications

PRACTICAL DESCRIPTION

Problem: - *Explore a Linux machine To discover hidden directories and files on a target web server using brute-force tools like Dirb or Gobuster. This simulates how attackers identify weak or unprotected entry points in web applications.*

Brute Force Attack:-

A brute force attack is when an attacker systematically tries every possible combination of usernames, passwords, or keys until the correct one is found. Think of it as “guessing the lock combination by trying all possibilities.”

Brute Force = Guessing login/passwords or keys.

Key feature of Tool used:

1. Dirb :-

Dirb is a web content scanner used to brute force hidden directories and files on a web server. Many websites leave sensitive directories (/admin, /backup, /test) exposed but not linked.

Dirb = Finds hidden web directories/files (slower).

2. Gobuster:-

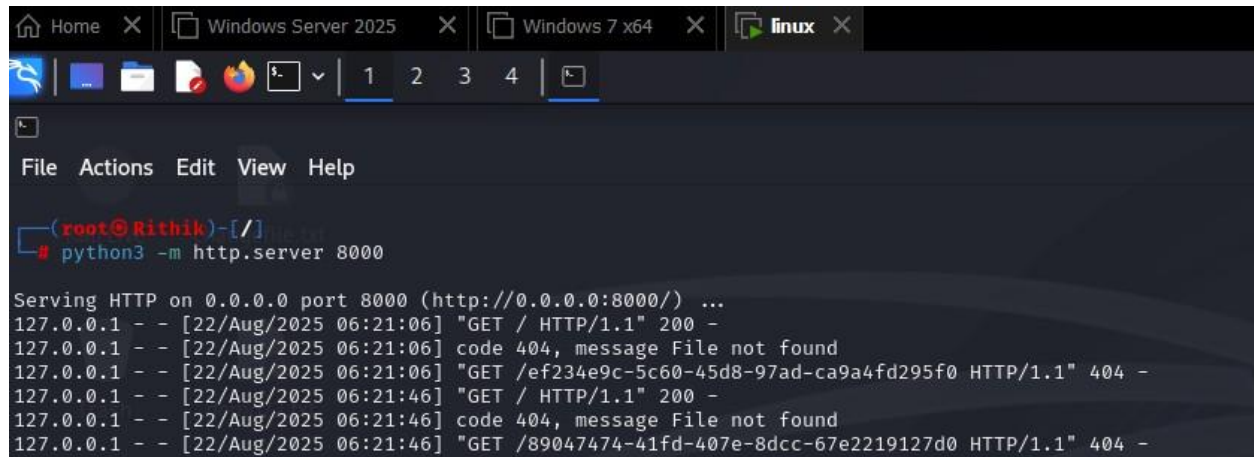
Gobuster is a faster alternative to Dirb written in Go. It can brute force:

- Directories & files on websites (like Dirb).
- DNS subdomains (e.g., mail.example.com, dev.example.com).

Gobuster = Faster tool for directories & subdomains (modern alternative to Dirb).

Prectical of Brute ForceTools using Kali Linux :-

We have used python3 -m http.server

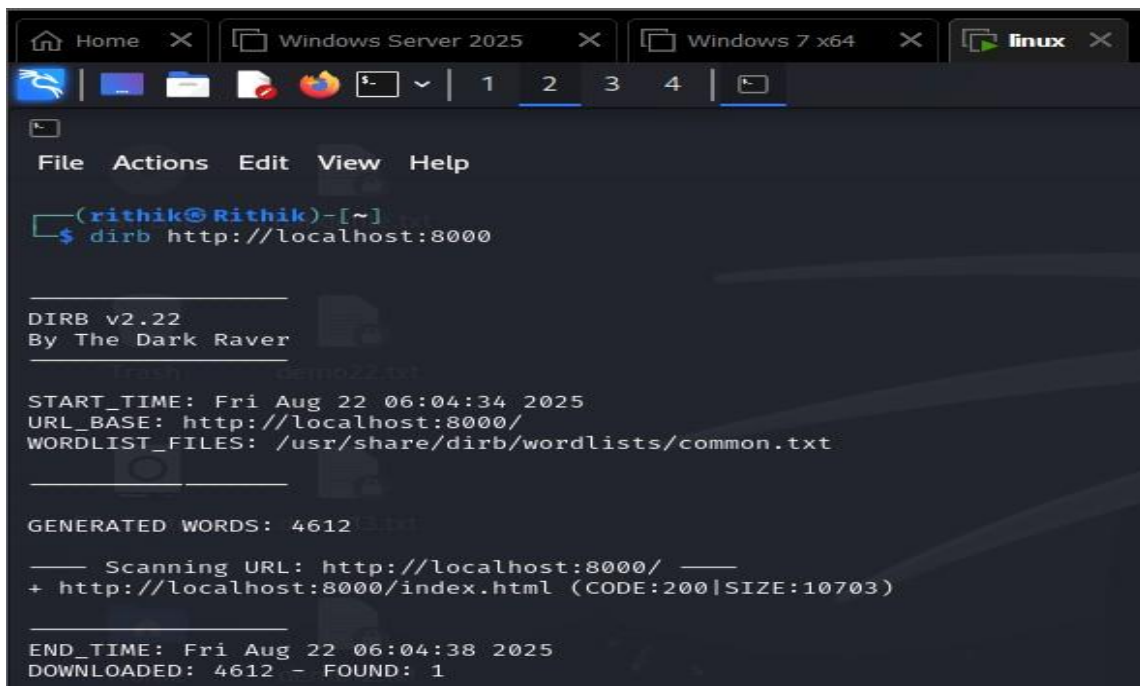


```
File Actions Edit View Help

(root@Rithik)-[/]
# python3 -m http.server 8000

Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
127.0.0.1 - - [22/Aug/2025 06:21:06] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [22/Aug/2025 06:21:06] code 404, message File not found
127.0.0.1 - - [22/Aug/2025 06:21:06] "GET /ef234e9c-5c60-45d8-97ad-ca9a4fd295f0 HTTP/1.1" 404 -
127.0.0.1 - - [22/Aug/2025 06:21:46] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [22/Aug/2025 06:21:46] code 404, message File not found
127.0.0.1 - - [22/Aug/2025 06:21:46] "GET /89047474-41fd-407e-8dcc-67e2219127d0 HTTP/1.1" 404 -
```

- **DRIB:-**



```
File Actions Edit View Help

(rithik@Rithik)-[~]
$ dirb http://localhost:8000

____
DIRB v2.22
By The Dark Raver
____

START_TIME: Fri Aug 22 06:04:34 2025
URL_BASE: http://localhost:8000/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

____

GENERATED WORDS: 4612

____ Scanning URL: http://localhost:8000/ ____
+ http://localhost:8000/index.html (CODE:200|SIZE:10703)

____

END_TIME: Fri Aug 22 06:04:38 2025
DOWNLOADED: 4612 - FOUND: 1
```

```

(rithik@Rithik)-[~]
$ dirb http://localhost:8000 /usr/share/wordlists/dirb/common.txt

_____|_____|
DIRB v2.22
By The Dark Raver

START_TIME: Fri Aug 22 06:05:31 2025
URL_BASE: http://localhost:8000/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

_____|_____|

GENERATED WORDS: 4612

— Scanning URL: http://localhost:8000/ —
+ http://localhost:8000/index.html (CODE:200|SIZE:10703)

_____|_____|

END_TIME: Fri Aug 22 06:05:35 2025
DOWNLOADED: 4612 - FOUND: 1

```

- **Gobuster:-**

```

File Actions Edit View Help

(rithik@Rithik)-[/home/rithik]
# gobuster dir -u http://localhost:8000 -w /usr/share/wordlists/dirb/common.txt

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://localhost:8000
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/index.html (Status: 200) [Size: 10703]
Progress: 4614 / 4615 (99.98%)
=====
Finished
=====

```

```
(root@Rithik)-[/home/rithik]
# touch mylist.txt

(root@Rithik)-[/home/rithik]
# echo "admin
login
backup
config
secret
" > mylist.txt

(root@Rithik)-[/home/rithik]
# gobuster dir -u http://localhost:8000 -w mylist.txt

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://localhost:8000
[+] Method: GET
[+] Threads: 10
[+] Wordlist: mylist.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
Progress: 6 / 7 (85.71%)
=====
Finished
=====
```

In the above image there is txt file(mylist.txt) contain text which is used to scan with gobuster .

Captured results and analyzed HTTP response codes:

- *200 OK → Accessible directory/file.*
- *403 Forbidden → Directory/file exists but access is restricted.*
- *404 Not Found → Doesn't exist.*
- *301/302 Redirect → Redirect to another page.*

Directory/File	Status Code	Notes
<i>/admin</i>	<i>200 OK</i>	<i>Admin panel discovered</i>
<i>/uploads</i>	<i>403</i>	<i>Forbidden Directory exists but restricted</i>
<i>/backup</i>	<i>200 OK</i>	<i>Sensitive backup folder</i>
<i>/secret.txt</i>	<i>200 OK</i>	<i>Exposed text file</i>

Conclusion :-

*Directory bruteforcing revealed several hidden endpoints on the target web server. Such findings demonstrate why **directory enumeration** is a critical step in web penetration testing, as attackers can exploit these weak points if not properly secured.*