

【PathBuster】Gobuster

支援不同的列舉模式，包括fuzzing和dns，但目前，我們只會依賴dir模式，該模式列舉文件和目錄。我們需要使用-u參數指定目標IP，並使用-w參數指定單詞列表。默認運行的線程數是10；我們可以通過使用-t參數設置更低的數字來減少流量。

```
# -t thead
# -u ip
# -w 字典檔
kali@kali:~$ gobuster dir -u 192.168.50.20 -w /usr/share/wordlists/dirb/common.txt -t 5

=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             http://192.168.50.20
[+] Method:          GET
[+] Threads:         5
[+] Wordlist:         /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:      gobuster/3.1.0
[+] Timeout:         10s
=====
2022/03/30 05:16:21 Starting gobuster in directory enumeration mode
=====
/.hta             (Status: 403) [Size: 278]
/.htaccess        (Status: 403) [Size: 278]
/.htpasswd        (Status: 403) [Size: 278]
/css              (Status: 301) [Size: 312] [--> http://192.168.50.20/css/]
/db               (Status: 301) [Size: 311] [--> http://192.168.50.20/db/]
/images           (Status: 301) [Size: 315] [--> http://192.168.50.20/images/]
/index.php        (Status: 302) [Size: 0] [--> ./login.php]
/js               (Status: 301) [Size: 311] [--> http://192.168.50.20/js/]
/server-status    (Status: 403) [Size: 278]
/uploads          (Status: 301) [Size: 316] [--> http://192.168.50.20/uploads/]

=====
2022/03/30 05:18:08 Finished
=====
```

在/usr/share/wordlists/dirb/文件夾中，我們選擇了common.txt單詞列表，找到了十個資源。其中有四個資源由於權限不足而無法訪問（狀態：403）。但是，其餘的六個是可以訪問的，值得進一步調查。

🕒修訂版本 #1

★由 treeman 建立於 9 🍀Q🍀@🍀🍀 2023 01:01:05

🔧由 treeman 更新於 7 🍀@🍀🍀 2024 19:30:26