

Preignition



Álvaro Delgado Hernández

```
(root@kali)-[/home/alvadelg]
# nmap -sS -p- -sV -O -A --top-ports 100 -oN scan.txt 10.129.40.221

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-13 15:30 CET
Nmap scan report for 10.129.40.221
Host is up (0.044s latency).
Not shown: 99 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Welcome to nginx!
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.0
OS details: Linux 5.0, Linux 5.0 - 5.14
Network Distance: 2 hops

TRACEROUTE (using port 3389/tcp)
HOP RTT      ADDRESS
1   43.68 ms 10.10.14.1
2   43.99 ms 10.129.40.221

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.38 seconds
```

`nmap -sS -p- -sV -O -A --top-ports 100 -oN scan.txt <target-ip>`

Explanation of Each Argument

`-sS`: SYN Scan

This performs a TCP SYN scan, which is a stealthy scan method. It sends SYN packets and waits for SYN-ACK responses, allowing you to discover open ports without completing the TCP handshake.

`-p-`: Scan All Ports

This option tells Nmap to scan all 65,535 TCP ports instead of just the default 1,000 ports.

`-sV`: Version Detection

This option tells Nmap to detect the versions of the services running on open ports.

`-O`: OS Detection

This flag enables OS detection, allowing Nmap to determine the operating system of the target host.

-A: Aggressive Scan

This enables several advanced and intrusive options, including OS detection (-O), version detection (-sV), script scanning (-sC), and traceroute.

--top-ports 100: Scan Top 100 Ports

This option tells Nmap to scan the top 100 most commonly used ports. It might be redundant in this context because -p- already includes all ports.

-oN scan.txt: Output to a File

This option specifies that the scan results should be saved in normal format to a file named scan.txt.

Directory Brute-forcing is a technique used to check a lot of paths on a web server to find hidden pages. Which is another name for this? (i) Local File Inclusion, (ii) dir busting, (iii) hash cracking.

dir busting

What switch do we use for nmap's scan to specify that we want to perform version detection

-sV

What does Nmap report is the service identified as running on port 80/tcp?

Http

What switch do we use to specify to Gobuster we want to perform dir busting specifically?

nginx 1.14.2

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	nginx 1.14.2

```
(root@kali)-[/home/alvadelg]
# gobuster dir -u http://10.129.40.221 -w /usr/share/dirb/wordlists/common.
txt -x php,js

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.129.40.221
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,js
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/admin.php (Status: 200) [Size: 999]
/admin.php (Status: 200) [Size: 999]
Progress: 13842 / 13845 (99.98%)

Finished: //nmap.org/submit/
```

`gobuster dir -u http://10.129.40.221 -w /usr/share/dirb/wordlist/common.txt -x php,js`

Explanation of Each Argument

`gobuster dir:`

This tells Gobuster to use the directory brute-forcing mode, which is designed to find hidden directories and files on the web server.

`-u http://10.129.40.221:`

This specifies the URL of the target website.

`-w /usr/share/dirb/wordlist/common.txt:`

This indicates the wordlist to use for brute-forcing. In this case, the common.txt wordlist from the dirb directory. This wordlist contains common directory and file names that are often found on web servers.

`-x php,js:`

This option specifies the file extensions to append to each word in the wordlist when searching for directories and files. In this case, it will check for .php and .js files.

What switch do we use to specify to Gobuster we want to perform dir busting specifically?

Dir

When using gobuster to dir bust, what switch do we add to make sure it finds PHP pages?

-x php

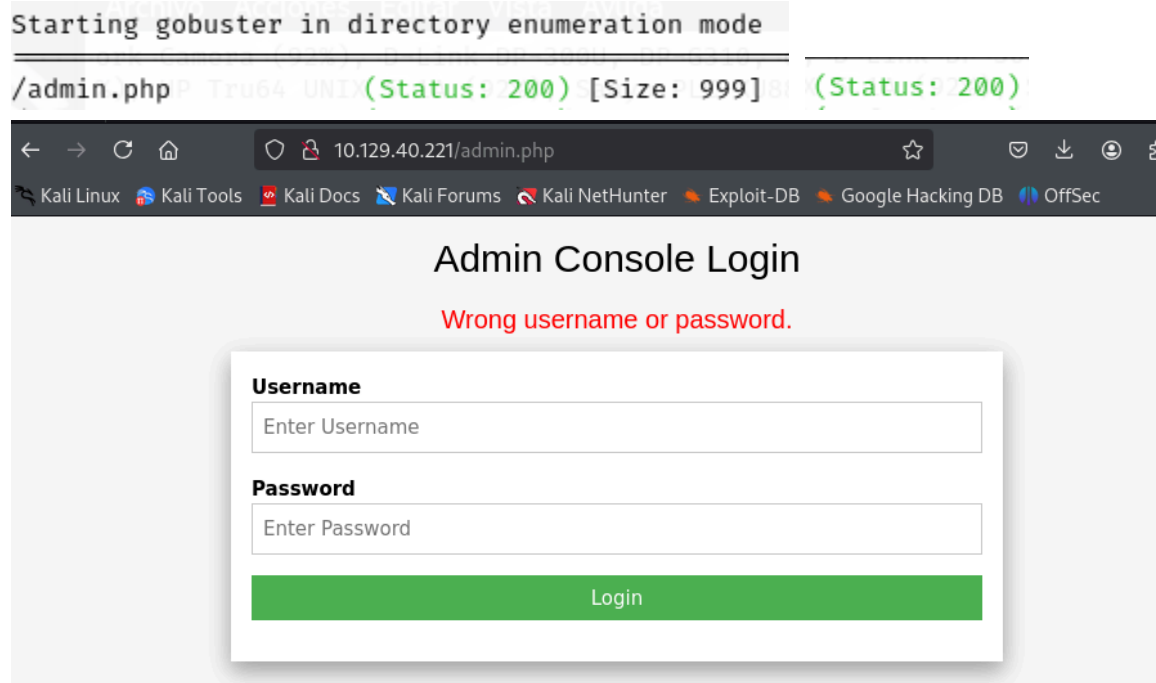
We can see that we have an /admin.php:

What page is found during our dir busting activities?

admin.php

What is the HTTP status code reported by Gobuster for the discovered page?

200



Let's try admin as the user and admin as the password.

