PreIgnition

Machine Information

Task Name - **Basic Directory Enumeration On Vulnerable Server.**
IP address - 10.129.107.219
Difficulty - very easy
Operating System - Linux/Unix TTL-63

Enumeration

Tools used - ping, nmap, gobuster

Commands executed - ping 10.129.107.219, nmap -sV 10.129.107.219, gobuster dir -w ~/Desktop/common.txt -u 10.129.107.219, man gobuster.

Output and Findings :

Output section

1.ping : ping 10.129.107.219

```
PING 10.129.107.219 (10.129.107.219) 56(84) bytes of data.
64 bytes from 10.129.107.219: icmp_seq=1 ttl=63 time=229 ms
64 bytes from 10.129.107.219: icmp_seq=2 ttl=63 time=231 ms
64 bytes from 10.129.107.219: icmp_seq=3 ttl=63 time=230 ms
64 bytes from 10.129.107.219: icmp_seq=4 ttl=63 time=230 ms
64 bytes from 10.129.107.219: icmp_seq=5 ttl=63 time=248 ms
64 bytes from 10.129.107.219: icmp_seq=6 ttl=63 time=232 ms
64 bytes from 10.129.107.219: icmp_seq=7 ttl=63 time=231 ms
64 bytes from 10.129.107.219: icmp_seq=8 ttl=63 time=230 ms
64 bytes from 10.129.107.219: icmp_seq=9 ttl=63 time=231 ms
64 bytes from 10.129.107.219: icmp_seq=10 ttl=63 time=233 ms
^C
--- 10.129.107.219 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9054ms
rtt min/avg/max/mdev = 229.357/232.522/247.680/5.123 ms
```

2.nmap : nmap -sV 10.129.107.219

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-25 08:59 CDT
Nmap scan report for 10.129.107.219
Host is up (0.70s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.75 seconds
```

3. gobuster : gobuster dir -w ~/Desktop/common.txt -u 10.129.107.219

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.107.219
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /root/Desktop/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin.php           (Status: 200) [Size: 999]
Progress: 776 / 4615 (16.81%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 776 / 4615 (16.81%)
===============================================================
Finished
===============================================================
```

4. man gobuster : check mannual page of gobuster tool

Findings Section :

-Connection was alive with ping utility tool
-Found http-80 open port
-Found admin.php directory on server using gobuster
-typed http://10.129.107.219/admin.php in url
-Admin console opened
-logged with default credentials (admin, admin)
-Got Root Flag

Exploitation/Initial Foothold

Vulnerability Identified - **The administrative interface was publicly accessible on browser. Default Credentials are used to log in admin console page. Successfully logged-in . Found Root Flag**.

Exploit steps -
step 1 - open terminal in kali.
step 2 - check target ip was reachable or not. check for operating system running on target.
step 3 - scan the target to find the service version, open ports and other info.
step 4 - install gobuster tool to enumerating directories on target .(which conccluded that it was a nginx server on target).
step 5 - enumerate the directories. check for any imp directories were found.
step 6 - Here , **admin.php** was found on scanning.
step 7 - loggin the target with found directory. (http://tar ip/admin.php) . admin console opened.
step 8 - login with default credentials that are specified in **Findings section.**
step 9 - Boom , Got root flag. Successfully Pwned machine.

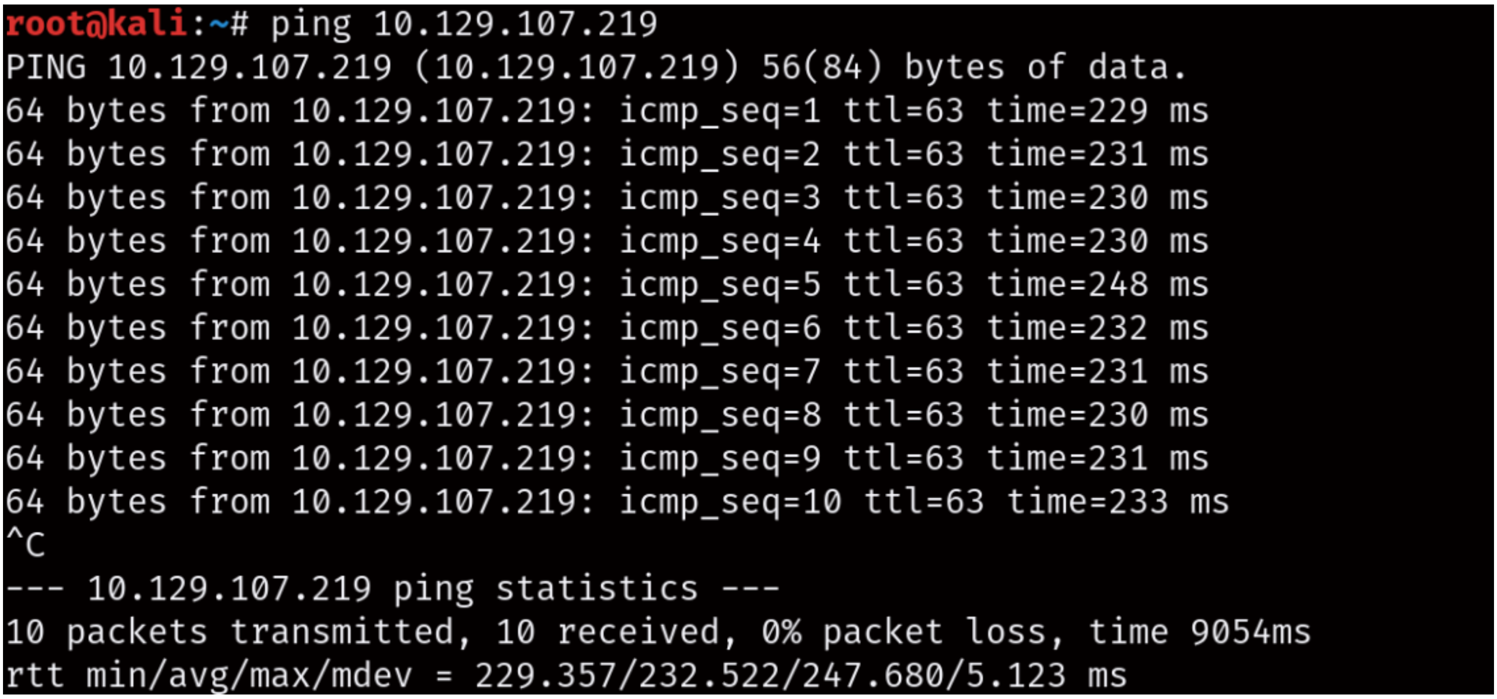
- No shell were obtained in this task.

Privilege Escalation

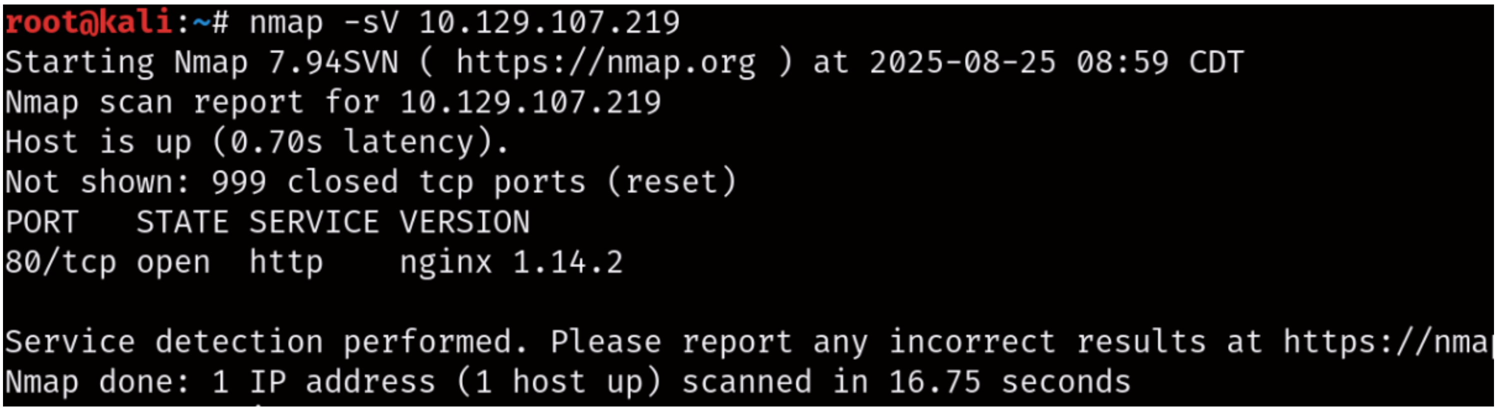
- **Low level privilege accessed with default credentials.**

Proofs & Flags

Screenshots:

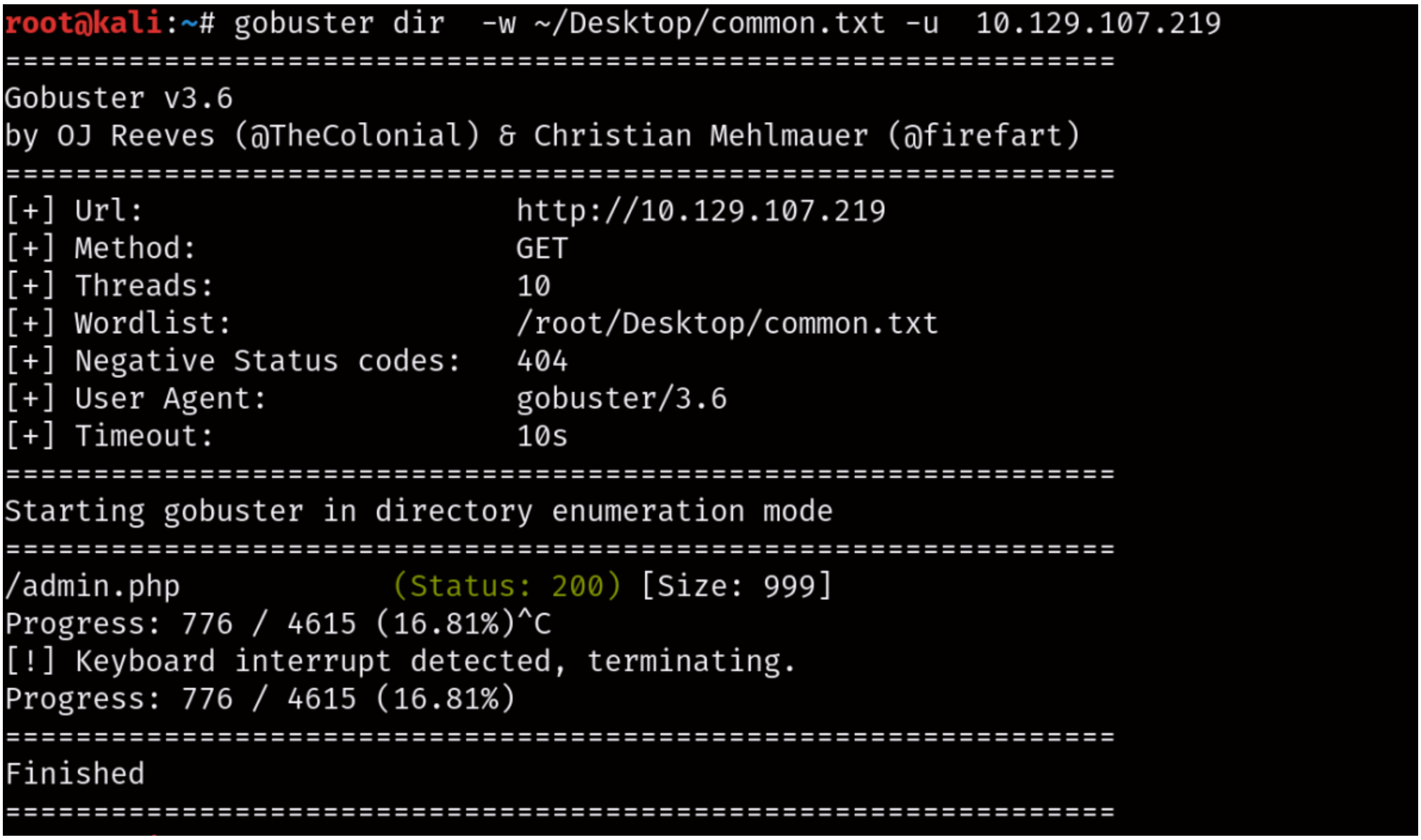


```
root@kali:~# ping 10.129.107.219
PING 10.129.107.219 (10.129.107.219) 56(84) bytes of data.
64 bytes from 10.129.107.219: icmp_seq=1 ttl=63 time=229 ms
64 bytes from 10.129.107.219: icmp_seq=2 ttl=63 time=231 ms
64 bytes from 10.129.107.219: icmp_seq=3 ttl=63 time=230 ms
64 bytes from 10.129.107.219: icmp_seq=4 ttl=63 time=230 ms
64 bytes from 10.129.107.219: icmp_seq=5 ttl=63 time=248 ms
64 bytes from 10.129.107.219: icmp_seq=6 ttl=63 time=232 ms
64 bytes from 10.129.107.219: icmp_seq=7 ttl=63 time=231 ms
64 bytes from 10.129.107.219: icmp_seq=8 ttl=63 time=230 ms
64 bytes from 10.129.107.219: icmp_seq=9 ttl=63 time=231 ms
64 bytes from 10.129.107.219: icmp_seq=10 ttl=63 time=233 ms
^C
--- 10.129.107.219 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9054ms
rtt min/avg/max/mdev = 229.357/232.522/247.680/5.123 ms
```

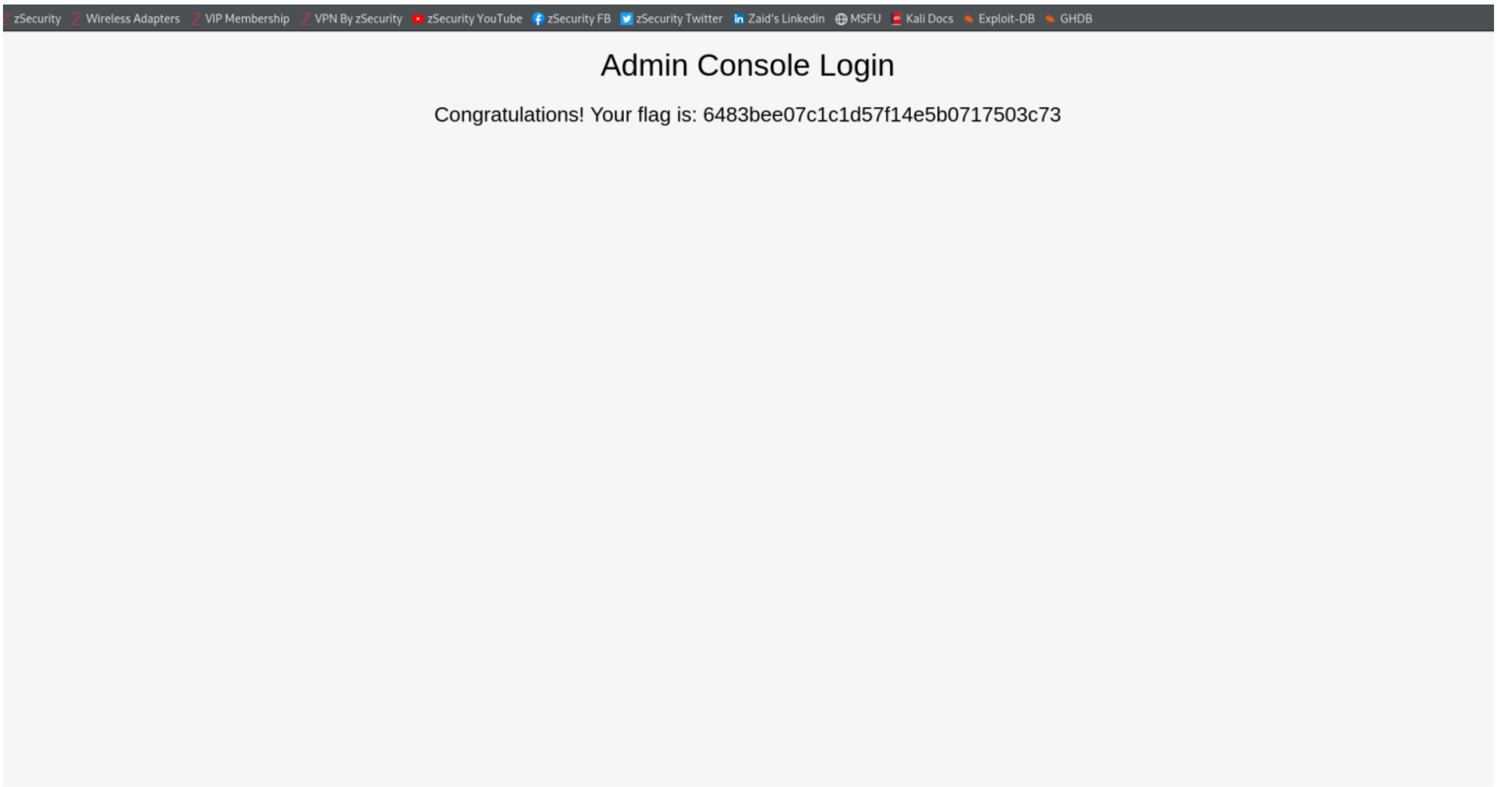


```
root@kali:~# nmap -sV 10.129.107.219
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-25 08:59 CDT
Nmap scan report for 10.129.107.219
Host is up (0.70s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.2

Service detection performed. Please report any incorrect results at https://nma
Nmap done: 1 IP address (1 host up) scanned in 16.75 seconds
```



```
root@kali:~# gobuster dir  -w ~/Desktop/common.txt -u  10.129.107.219
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.107.219
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /root/Desktop/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin.php            (Status: 200) [Size: 999]
Progress: 776 / 4615 (16.81%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 776 / 4615 (16.81%)
===============================================================
Finished
===============================================================
```



Admin Console Login

Congratulations! Your flag is: 6483bee07c1c1d57f14e5b0717503c73

Mitigation

1.Change the default credentials.
2.Limit the login attempts to prevent brute force.
3.enable Multi Factor Authentication.
4.Restrict access to admin interface.
5.Update server and use HTTPS protocol
6.Conduct regular security audits.