AGENT - T

Write-Up by RAHUL DIXIT

IP Address Of Target : **10.10.196.216**

Let’s begin exploiting.

1. Information Gathering

1.1 Ping Request

Let’s try pinging to check whether the target responds to the ping request from our machine.

```
┌──(root㉿kali)-[/home/kali/TryHackMe/Agent]
└─# ping -c 4 10.10.196.216
PING 10.10.196.216 (10.10.196.216) 56(84) bytes of data.
64 bytes from 10.10.196.216: icmp_seq=1 ttl=60 time=249 ms
64 bytes from 10.10.196.216: icmp_seq=2 ttl=60 time=170 ms
64 bytes from 10.10.196.216: icmp_seq=3 ttl=60 time=160 ms
64 bytes from 10.10.196.216: icmp_seq=4 ttl=60 time=211 ms

── 10.10.196.216 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 159.559/197.504/249.337/35.685 ms
```

The target responds to the ping request with a **TTL** of 60 indicating that the OS running is **Linux.**

For all machines running **Linux** their **TTL** value is 64 (60 is nearby approximately to the TTL of 64).

2. Scanning

2.1 Port Scanning

Now let's try scanning for the open ports on the target machine using Nmap.

```
┌──(root㉿kali)-[/home/kali/TryHackMe/Agent]
└─# nmap -p- -Pn -T5 --min-rate=1000 10.10.196.216 -o allPorts.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 19:51 EDT
Warning: 10.10.196.216 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.196.216
Host is up (0.16s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 70.29 seconds
```

After scanning for all the ports that are open on the target, we found 1 port as open.

⚔️ **OPEN PORTS**

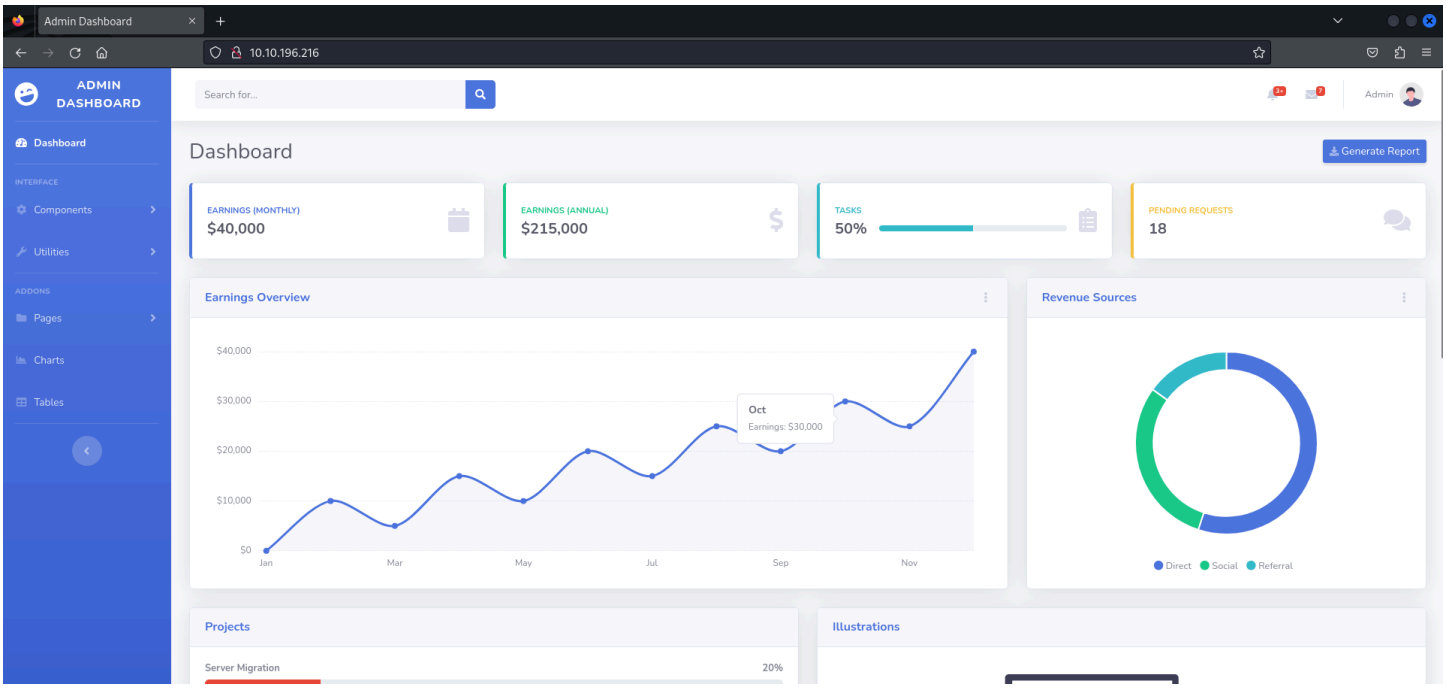
The scan shows PORT **80/TCP**.

Now let's perform a more insane scan on the specific ports that are open on the target machine.

```
┌──(root㉿kali)-[/home/kali/TryHackMe/Agent]
└─# nmap -p 80 -sCV -Pn -T5 --min-rate=10000 10.10.196.216 -o insaneScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 19:53 EDT
Nmap scan report for 10.10.196.216
Host is up (0.15s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    PHP cli server 5.5 or later (PHP 8.1.0-dev)
|_http-title:  Admin Dashboard

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.02 seconds
```

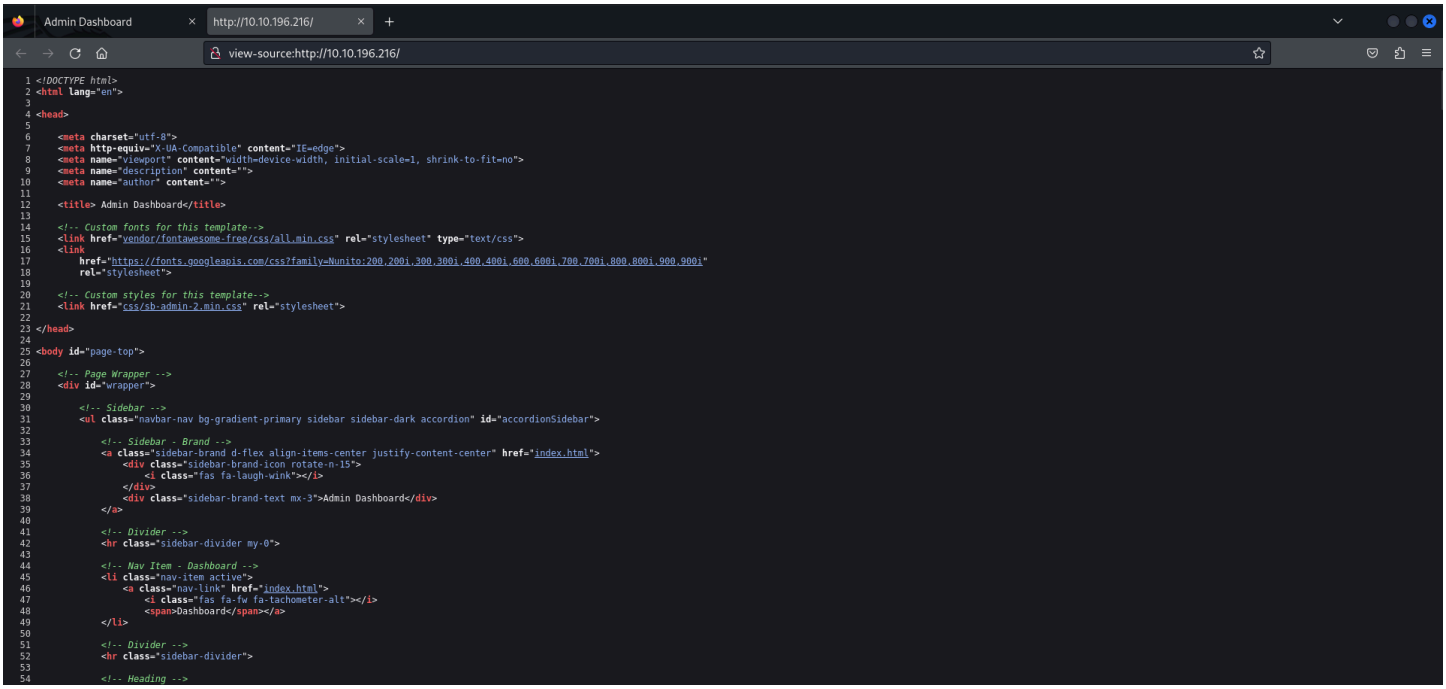
The scan indicates that the HTTP service is running on port **80** of the target machine. The service running on this port is identified as the **PHP CLI server, version 5.5 or later, with PHP 8.1.0-dev**.

Now we have a website let's check whether we can get any sensitive information from the website.



We have this beautiful admin page hosted on the target machine upon looking around nothing seemed functional. Every link ended up with **404** status code indicating the resource was not found.

Let’s check the client-side source code to see if we can find something useful.



Upon analysing the source code there was nothing useful in the source code.

2.2 Directory Enumeration

Now let's enumerate the directories that maybe hidden on the server using PathX.

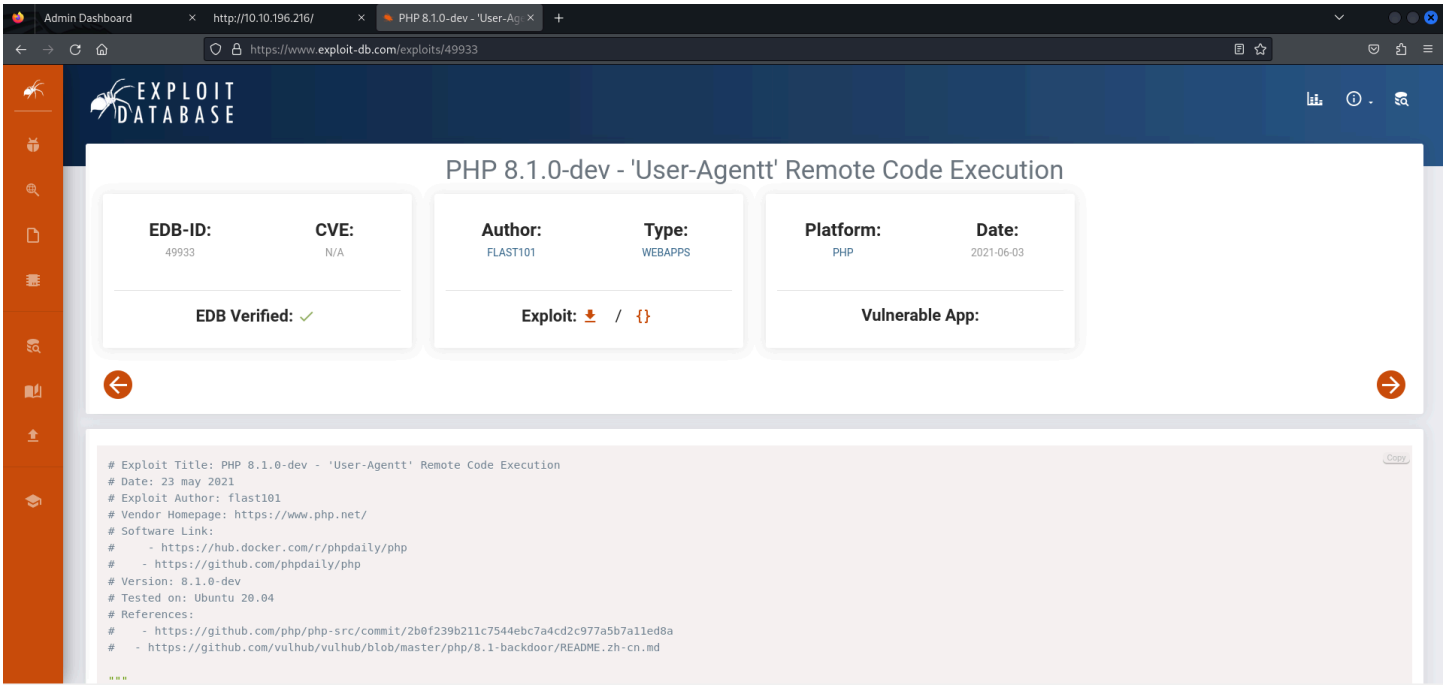
```
┌──(root㉿kali)-[/home/kali/TryHackMe/Agent]
└─# python PathX.py --url http://10.10.196.216 --wordlist /usr/share/wordlists/dirb/small.txt --mode sub -o TryHackMe/Agent/dir.txt --rate-limit 64

   ___      _   _  __  _  _
  / _ \___ _/ /_/ /_ | |/ /
 / ___/ _ `/ __/ __ \|   /
/_/   \_,_/\__/_/ /_/_/|_|

v1.0.0 - BETA
By @syncattacker
──────────────────────────────────────────────────
METHOD : GET
URL : http://10.10.196.216
TIMEOUT : 10
RATE LIMIT : 64
STATUS CODE : 200-209, 300-309, 401, 403
──────────────────────────────────────────────────
[INFO] [19:57:45] TOTAL REQUESTS : 959
[INFO] [19:58:04] ELAPSED TIME : 18.59
[ERROR] [19:58:04] ERRORS ENCOUNTERED : 959
```

On enumerating for directories it seems that nothing was found as the tool **PathX** ended up with errors in the requests sent, enumerating in 18.59 seconds.

2.3 Known Exploit Lookup

Now let's look if we can find any exploits on the version of **PHP** that we found in the scanning phase.

Upon searching on exploit-db, got an exploit for **PHP 8.1.0-dev** the exact version used by our target.



Let’s download and run this exploit and check if we can compromise the target with **RCE** and capture the flag.

3. Gaining Access

3.1 RCE via User-Agent Header

Executed the script and passed the target URL, commands and boom 💥. We compromised the target.

Happy Hacking ⚔️! @exploitslayer