Shocker –

As the initial step of enumeration, used **Nmap** tool to enumerate the machine for open ports and services.

Text

Description automatically generated

Opened the Ip on web browser as port 80 is open on the server.

A picture containing graphical user interface

Description automatically generated

Checked the source code of the web page but no luck as there was only a jpg file of the above shown image.

Then used **Gobuster** tool to enumerate the sub-directories of the webpage.

Text

Description automatically generated

The gobuster results reveal a Permission Denied sub directory but it did give a hint of further sub directory.

Also as checked on google for possible vulnerabilities around /cgi-bin/ and Apache,it revealed an excellent vulnerability – Bash Shellshock. Hence our next aim is to find a .sh sub directory which can be used to exploit the vulnerability.

Hence, used **Gobuster** to enumerate files with **“.sh”** extension.

Text

Description automatically generated

As checked online for possible steps to exploit the shellshock vulnerability, found an interesting article -[**https://ethicalhackingguru.com/how-to-exploit-the-shellshock-vulnerability/**](https://ethicalhackingguru.com/how-to-exploit-the-shellshock-vulnerability/)which uses **Burpsuite** to exploit it.

Followed the steps on the above article and forwarded the payload via Burpsuite and simultaneously opened up a listener on the local machine.

Graphical user interface, text, application, email

Description automatically generated

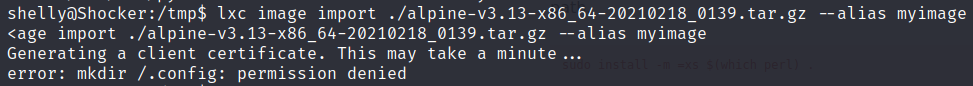
Once received by the server, a reverse shell has been created on our attacking machine as below with **Shelly** user privileges.

Graphical user interface, text

Description automatically generated

As checked the current user privileges, it had **lxd** privileges which can be exploited to escalate our privileges. Followed the steps in the article - <https://www.hackingarticles.in/lxd-privilege-escalation/> .

Yet there seems to be no proper privileges to create a directory and hence the attack failed.



As enumerated more, noticed that any user has access to run perl script on the machine which can be used to exploit the machine further and get root access.

Text

Description automatically generated

GTFobins (<https://gtfobins.github.io/gtfobins/perl/> ) is a popular site which provides such one-liner shell codes to be used to get Sudo access.

Followed the steps and successfully got root access on the machine as shown below -

Text

Description automatically generated

Finally able to capture the root flag and own the machine.

A picture containing graphical user interface

Description automatically generated