When scanning we see the ports
ftp
ssh
http

We visit http but see nothing interesting.
Do gobuster scan to find
/files
When visiting we get directory listning
ftp
image.jpg
notice.txt

Then we try ftp as anonymous user
ftp anonymous@<target ip>
and no password
This lets us in and it seems to contain the same contents as the /files on the website.
We then try to navigate to ftp folder in ftp and do put shell.php.
When going to the ftp folder on the website we now see the shell.php on there.
We can now click it and listen for a reverse shell with netcat.
Now stabilise the shell according to nc shell stabilisation.
Now we get the first ingredient in a text file.
Next we go to /home and see user lennie, but we cannot access the folder.
Back to the / folder.
Here we see incidents folder which contains a .pcapng file. Download this and open with wireshark on kali,
In wireshark we follow the tcp stream and scroll through different streams.
On one stream we see a linux terminal and at one point a password is tried.
We then try to ssh into lennie with this password and that works! ssh lennie@<ip>
Now we have access to lennie and get the user flag.
Then in scripts we see a planner.sh file which seems to first echo some stuff into a txt file and then run another .sh file.
When inspecting this other .sh file we see that lennie has access to it and we can modify that. We try inputing a reverse shell to our machine and close it.
Then we inspect the crontab and see that planner runs automatically so we can now open a listener on kali.
Now after a while we get a root shell from the reverse shell and can get the root flag!