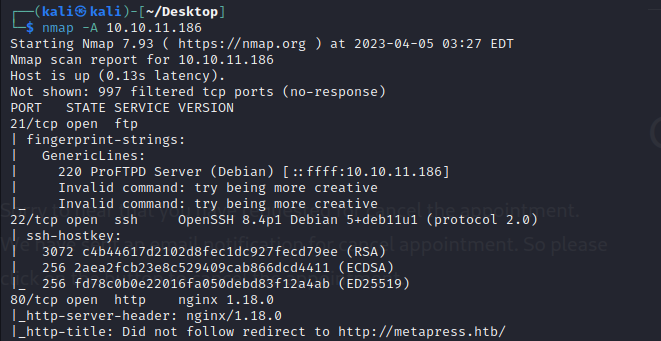
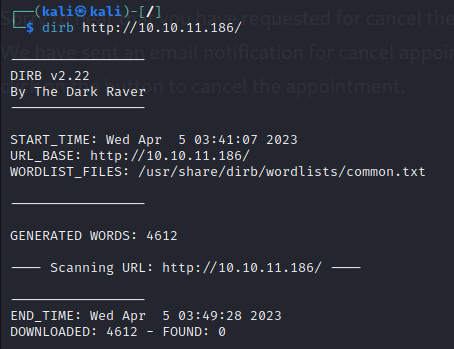
I first scanned with nmap the ip of the machine



Seeing that the 80 port was open, I tried connecting to the site which gave a 302 Found page.

The “follow redirect to …” part I’ve seen before in a writeup and the solution was to put it into the hosts file and associate it with the machine’s ip. After doing that, I could access the site.

I tried scanning the site with dirb



but it didn’t find anything, I’ll try scanning again later using the host name if I can’t find any other leads.

Clicking through the website, no page seemed interesting.

I tried going to the /admin page and the WordPress login page opened. The default login credentials for WordPress didn’t work.

I couldn’t find any cookies that might help:



The only thing that seemed to me to be a lead was the search bar:



So I tried searching for “/” in case I could do a path transversal

The search retrieved a list of pages on the site, so the path transversal might work.

Among those pages I could find:

<http://metapress.htb/cancel-payment/>

<http://metapress.htb/cancel-appointment/>

<http://metapress.htb/thank-you/>

Normally you would get redirected to those pages by other means, so accessing them like this might provide useful

Dirb seems to work on the host name, the dump of dirb scan results is saved in dirb-dump.txt

Registering on the site might provide a vulnerable cookie

Why does the site say to login through the events page specifically?

After registering for an event I got redirected to

<http://metapress.htb/thank-you/?appointment_id=Mg==>

So it seems like that /thank-you page can take an “appointment\_id” parameter

Dirb found the following url:

<http://metapress.htb/xmlrpc.php>

Accessing it through the browser displays:



This is a remote procedure call protocol. Googling it shows that the protocol might be dangerous and potentially vulnerable.