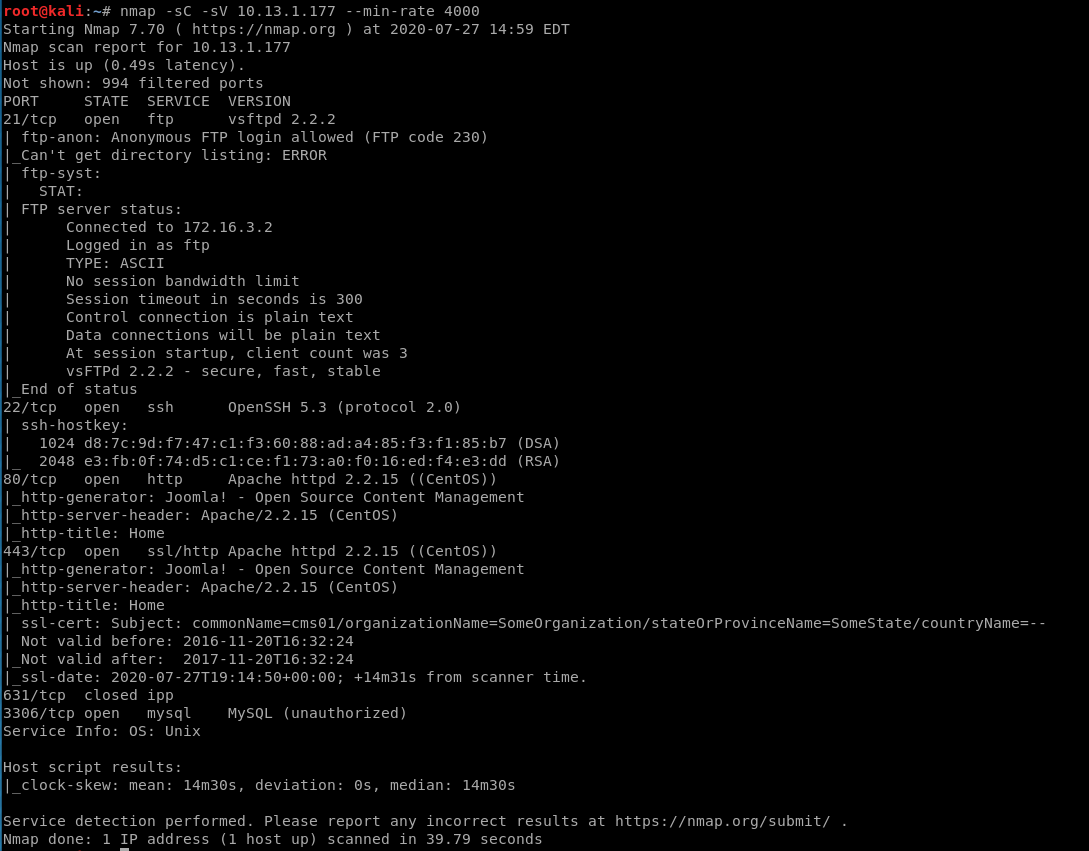
CMS01(10.13.1.177)-GhostIA

Sarah Ferenczi

Enumeration

First, I ran an nmap scan on the IP address to see the open ports.

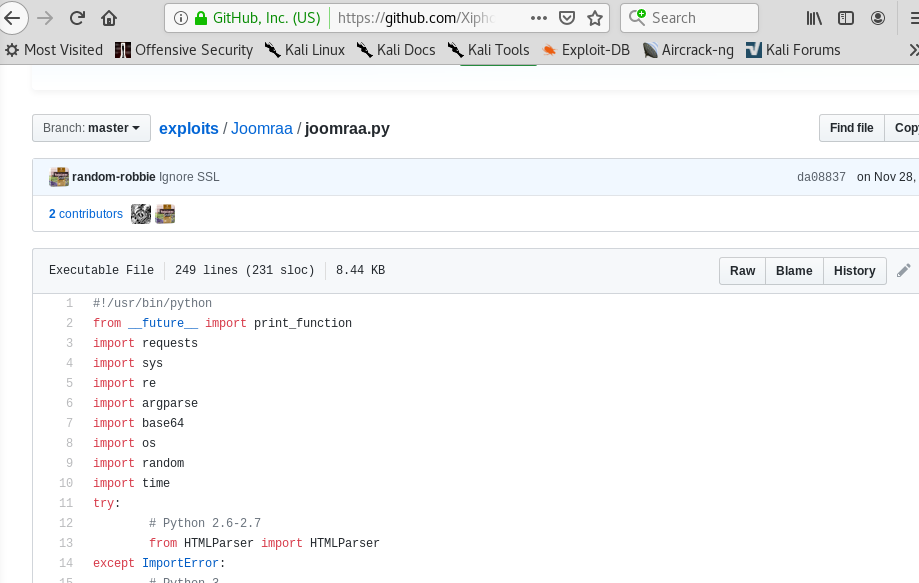


The first thing I noticed was port 80, which navigated to a webpage. Because Joomla is known to be highly vulnerable, I decided to navigate to the webpage to see what vulnerabilities are on there.

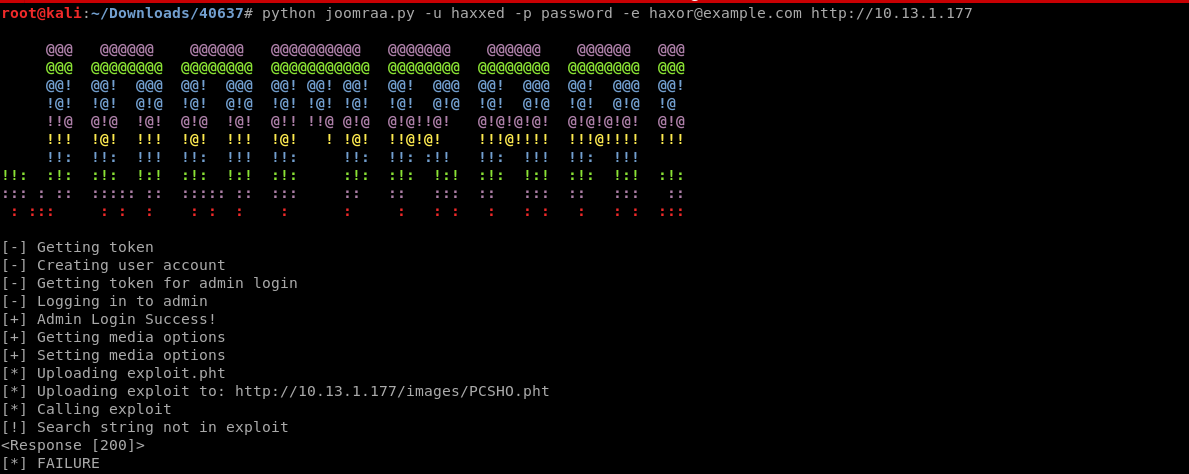


Exploitation

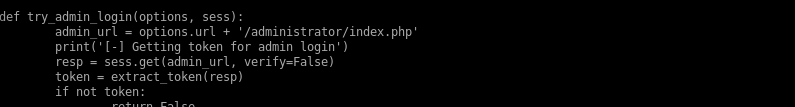
Navigating there, I noticed that the version number was 3.6.3. From this, I decided to go and look up any known vulnerabilities to this version that could benefit me in some way.



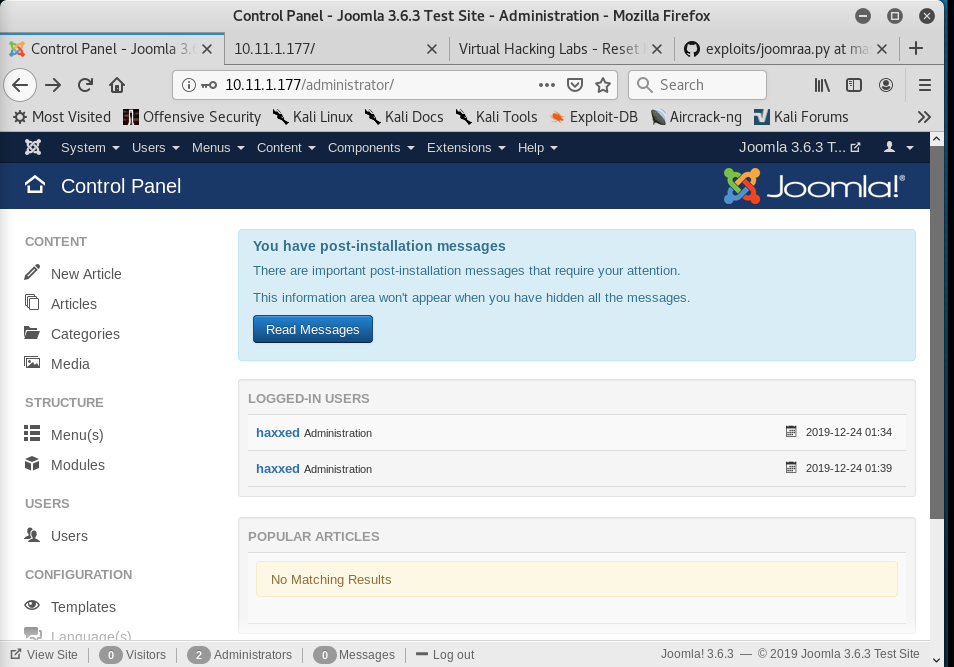
From there, I came across this exploit off of GitHub that creates an administrator account. With that, I decided to run it.



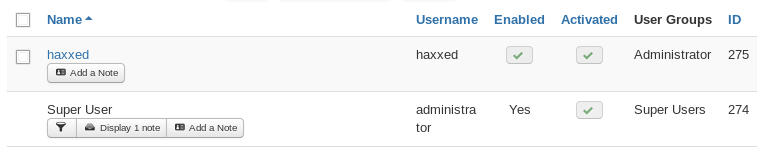
I decided to run the code, however, at the very end, the code crashed due to it being unable to upload a .pht file because of the website blocking all files with the .pht extension in them. However, I still have the authentication for an administrator account.

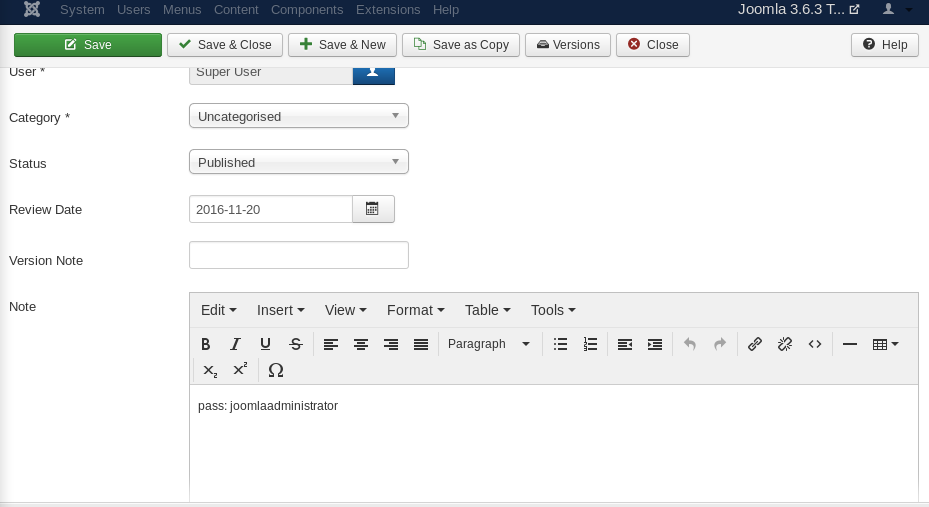


As we can see in the code, the directory to administrator login is in there. So I headed over to the administrator login page.



Using the credentials I made, I went ahead and logged in as an admin.

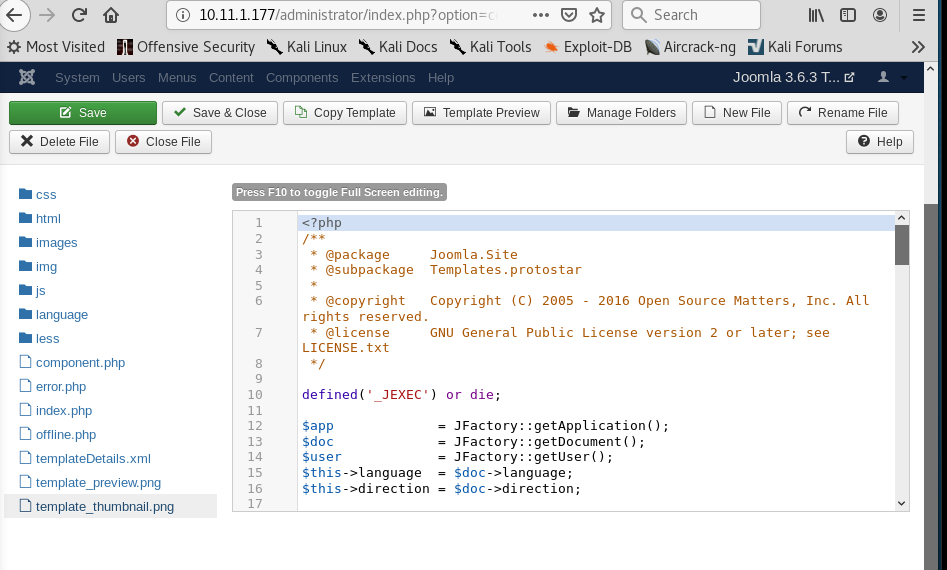




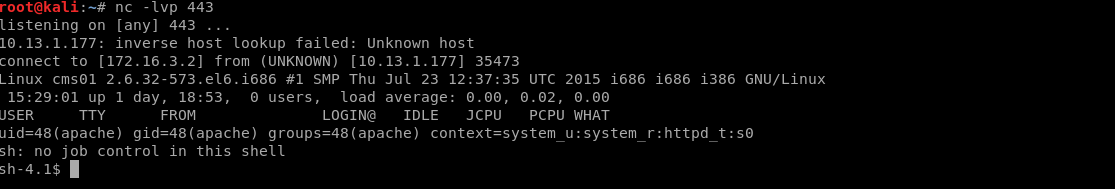
After some digging around, I found a note from the administrator in regards to the password. With my current access, I cannot do anything to the page as seen before, so I can edit the webpage once I access the Super User account.

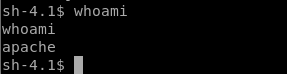


With the credentials I have just obtained, I went ahead and logged in with them.



From there, I headed to the bottom of the page where Configuration was located, clicked on Templates>Templates>protostar>index.php in order to edit the page. From there, I replaced the code with a php reverse shell and used an already open port to listen on, which in my case, was port 443. Clicked Save and view site at the bottom.



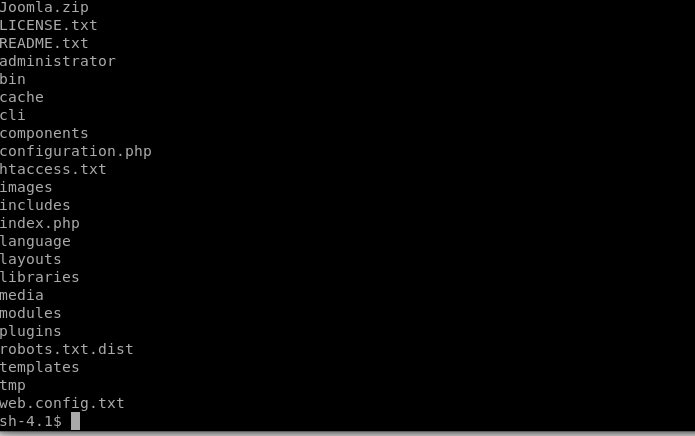


And from there, I got my shell.

Privilege Escalation



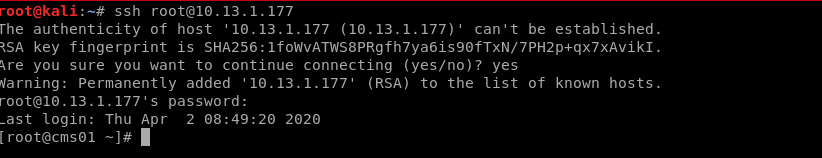
Being apache, I have limited privileges still. From there, I navigated to var/www/html to look for any potential credentials.



After poking around, in configuration.php, I noticed some credentials for root.



From there, I decided to ssh into root with the credentials given here.



From there, we can get the key

cvxdxsy3cjhhbk0zbfuf