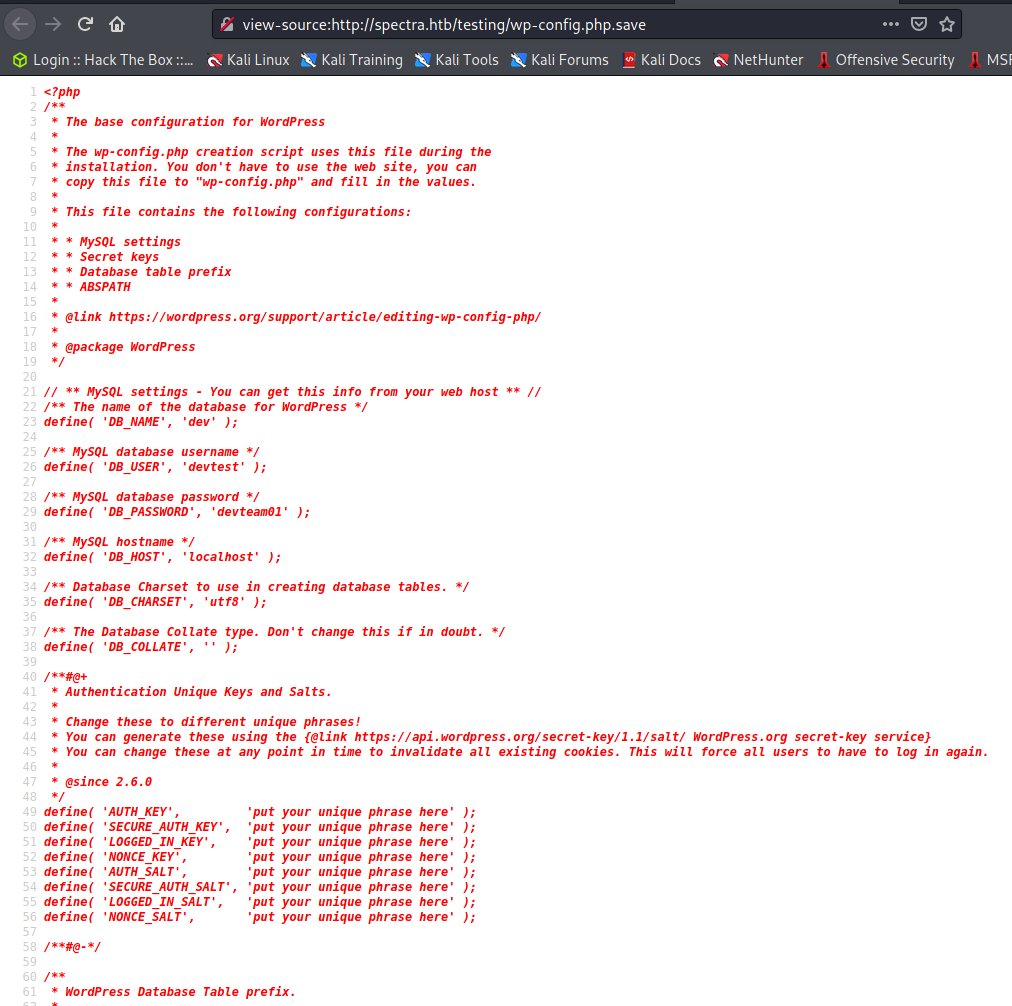
**Spectra**

Difficulty: Easy

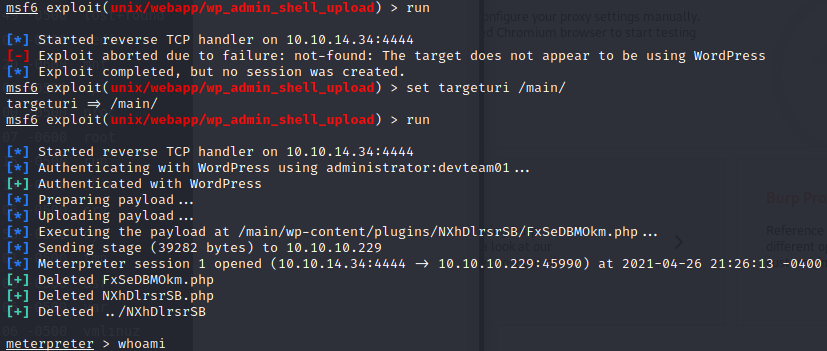
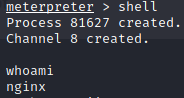
Machine:*Linux*

Nmap

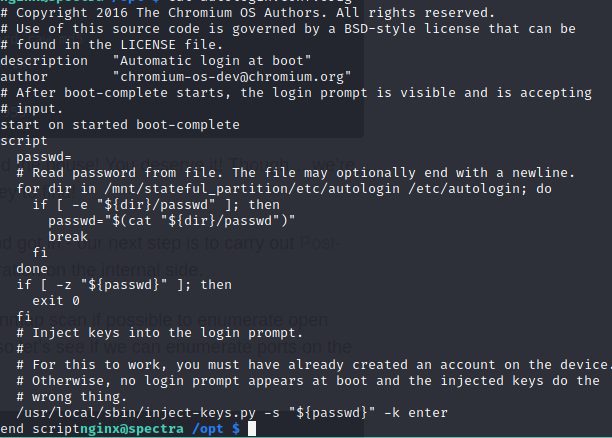
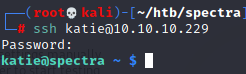
Website

* 
* Can login to wordpress with the following
  + Administrator:devteam01
* The image above also contains mysql database information
  + devtest:devteam01

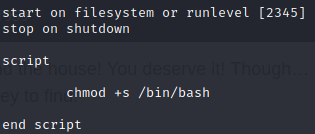
Wordpress

* After logging into the wordpress site and snooping around, I found nothing useful.
* I found an article that helped me get some code execution on the server. It uses the metasploit module “unix/webapp/wp\_admin\_shell\_upload” which requires the admin user for wordpress - the one we have.
  + <https://jhalon.github.io/vulnhub-mr-robot1/>
* 
* Typing “shell” gives us a shell as nginx
  + 

Nginx User

* I went and created my own id\_rsa password file so I can relog in at any time.
* I looked around and found this file called “autologin.conf.orig” in “/opt”
  + 
* It is a strange script. I tried looking around for keys and found nothing. I went through just about every directory that looked interesting to me.
* After searching for a while I went back to the file mentioned above. I then saw a mentioned directory that was new called “/etc/autologin”
* Looking into this directory, I found a file called “passwd.” Printing this file gives us the following
  + SummerHereWeCome!!
    - Please let this be Katie or better yet root
* Trying out this password with the script does not work. Time to try su or ssh
* I logged in a Katie with the above password
  + 

Katie

* Immediately going into privilege finding, I do “sudo -l” and get the following
  + 
* Time to research
* This article looks promising
  + <https://isharaabeythissa.medium.com/sudo-privileges-at-initctl-privileges-escalation-technique-ishara-abeythissa-c9d44ccadcb9>
    - Funny thing about this article, it is using spectra as its example, which is slightly wrong. I noticed this after the fact.
* Following the above article, I went to “/etc/init/” and edited one of the files owned by the “developer” team which Katie is part of. I then put the script mentioned in the above article into test.conf.
  + **
* After doing this, I ran the command
  + *Sudo /sbin/initctl start test*
* Rooted!!

