**Red Team: Summary of Operations**

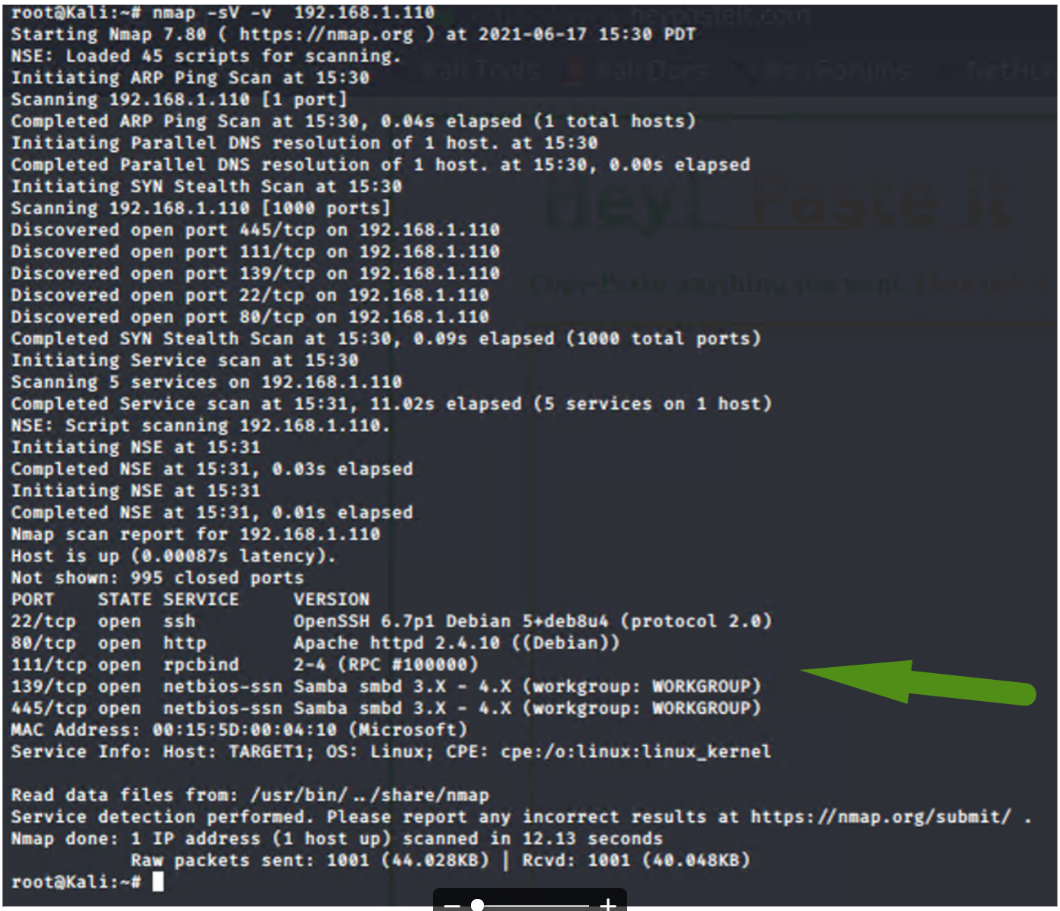
**Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

# Exposed Services

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

$ nmap –sV –v 192.168.1.110



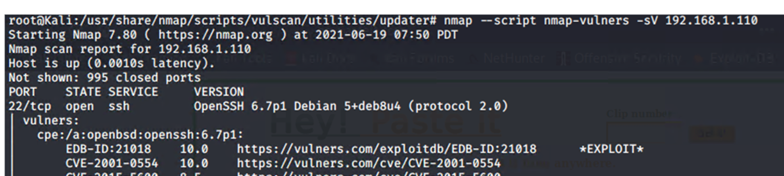
This scan identifies the services below as potential points of entry:

| Service | Port | State | OS Version |  
|-------------|---------|-------|----------------------------------------------|  
| SSH | 22/TCP | OPEN | OpenSSH 6.7p1 Debian 5 deb8u4 (protocol 2.0) |  
| HTTP | 80/TCP | OPEN | Apache httpd 2.4.10 ((Debian)) |  
| RPCBIND | 111/TCP | OPEN | 2-4 (RPC #100000) |  
| NETBIOS-SSN | 139/TCP | OPEN | Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |  
| NETBIOS-SSN | 445/TCP | OPEN | Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |

# Critical Vulnerabilities

#### Port 22/TCP

/tcp  open  ssh         OpenSSH 6.7p1 Debian 5 deb8u4 (protocol 2.0)  
CVE-2001-0554   Severity -> 10.0  
CVE-2015-5600   Severity -> 8.5



#### Port 80/TCP

80/tcp  open  http        Apache httpd 2.4.10 ((Debian))  
  
CVE-2017-7679   Severity -> 7.5  
CVE-2017-7668   Severity -> 7.5  
CVE-2017-3169   Severity -> 7.5

80/tcp open http Apache httpd 2.4.10 ((Debian))

|\_http-server-header: Apache/2.4.10 (Debian)

| vulners:

| cpe:/a:apache:http\_server:2.4.10:

| CVE-2017-7679 7.5 https://vulners.com/cve/CVE-2017-7679

| CVE-2017-7668 7.5 https://vulners.com/cve/CVE-2017-7668

| CVE-2017-3169 7.5 https://vulners.com/cve/CVE-2017-3169

#### No vulnerabilities found for ports 111, 139, 445 with the nmap command.

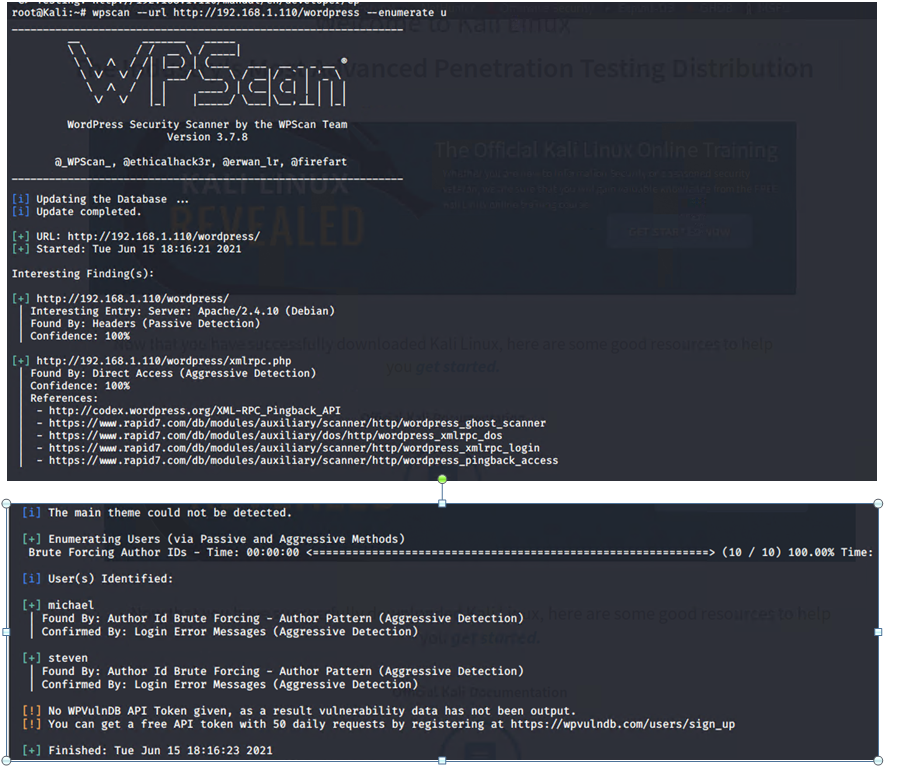
# Exploitation

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

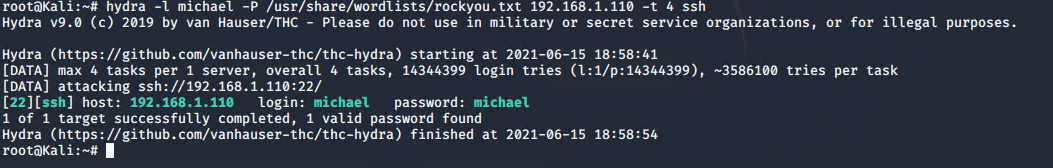
#### Flag2

-Exploit Used /Command run

* WPscan -to identify users



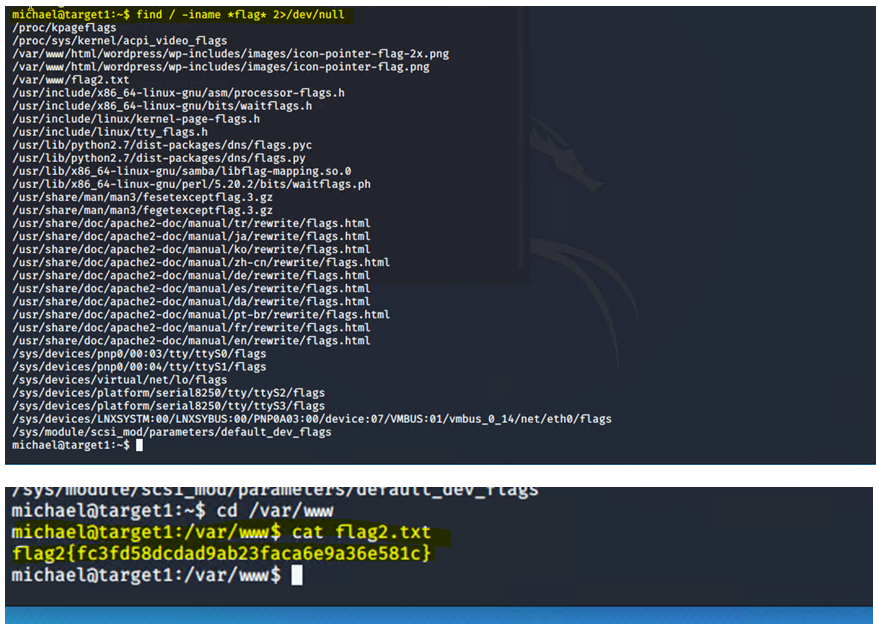
* Hydra – to get password to log in as user



* SSH into user’s profile



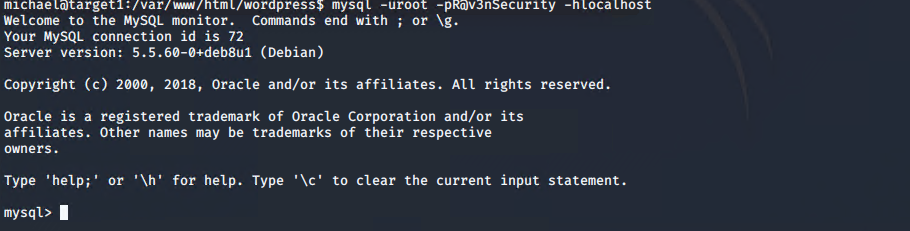
* Use, find command to look for files with name “flag” and then cat into the file.



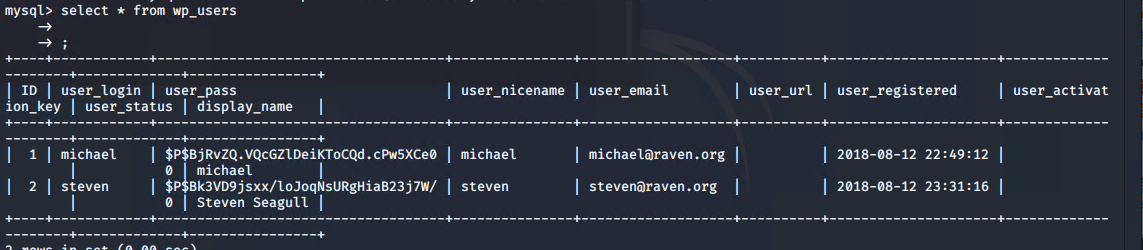
#### Flag 4

-Exploit Used/Command run

* Using credentials found in flag 2, logged on to MySQL



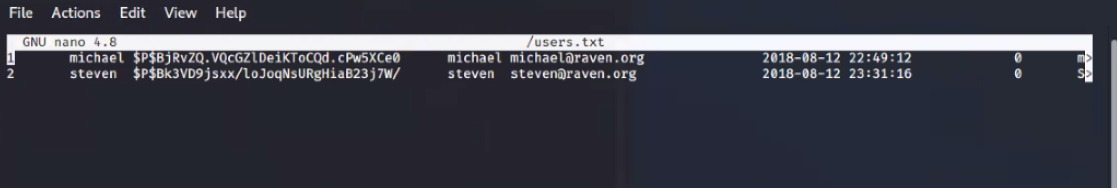
* Connected to db to get user hash

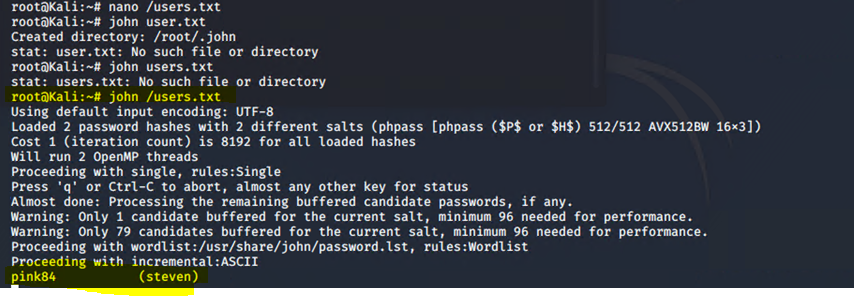


* Save user hash found, to local folder

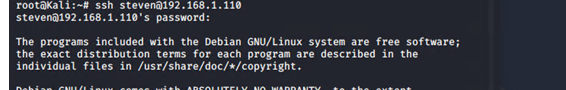


* Format file to use John the ripper, to crack password





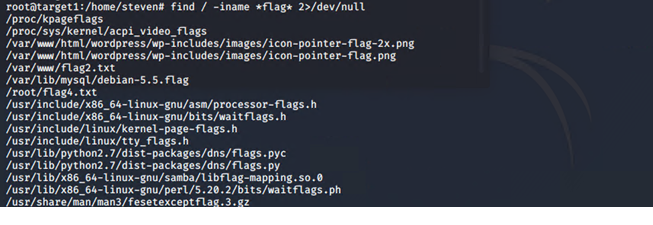
* Ssh into profile of user found



* Use python to get into users root folder



* Use, find command to look for files with name “flag” and then cat into the file.



* cd into folder where the flag file is found and cat into the file.

