Red Team: Summary of Operations

Table of Contents

Exposed Services

Nmap scan results for each machine reveals the below services

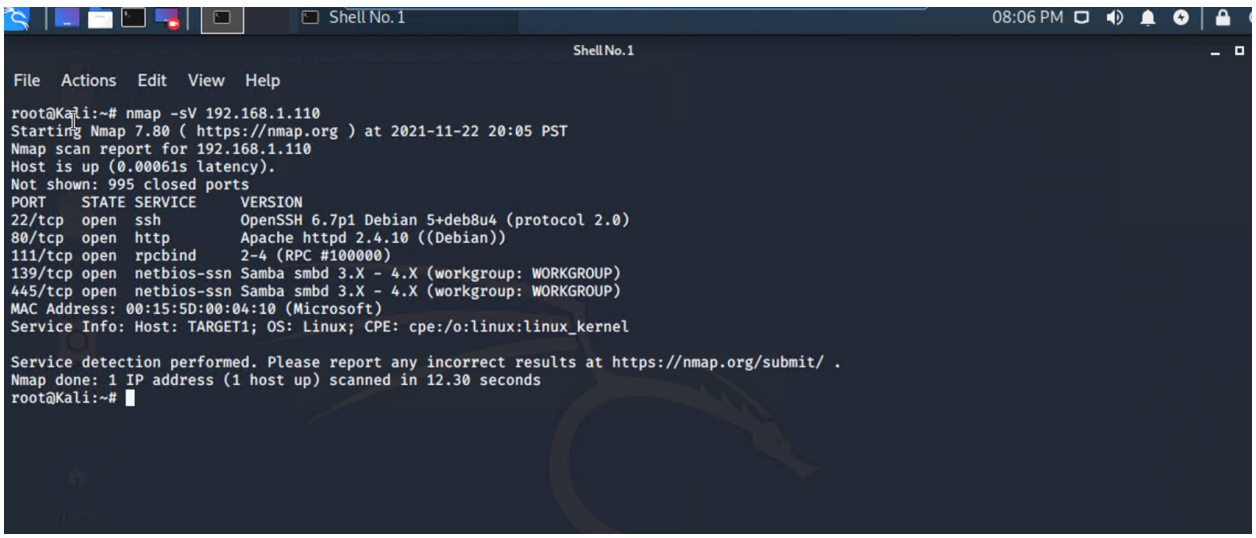
Nmap -sP 192.168.1.1-255 reveals 192.168.1.110 and 192.168.1.115

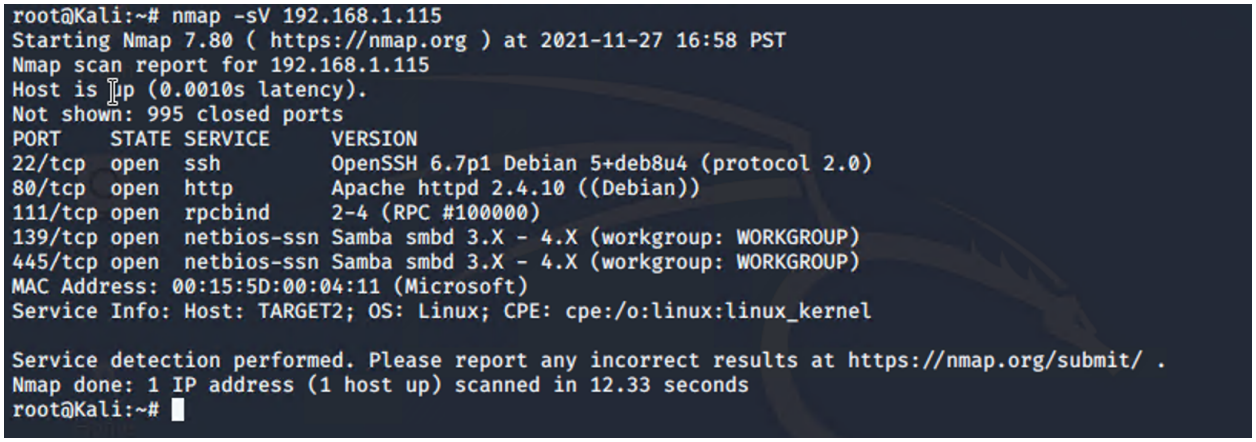
TODO: Fill out the information below.

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

$ nmap ... # TODO: Add command to Scan Target 1
  # TODO: Insert scan output

```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind     2-4 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.38 seconds
root@Kali:~# nmap -sP 192.168.1.225
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-27 15:02 PST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.46 seconds
root@Kali:~# nmap -sP 192.168.1.1-255
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-27 15:03 PST
Nmap scan report for 192.168.1.1
Host is up (0.00068s latency).
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Nmap scan report for 192.168.1.100
Host is up (0.00090s latency).
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Nmap scan report for 192.168.1.105
Host is up (0.00078s latency).
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Nmap scan report for 192.168.1.110
Host is up (0.00093s latency).
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Nmap scan report for 192.168.1.115
Host is up (0.0020s latency).
MAC Address: 00:15:5D:00:04:11 (Microsoft)
Nmap scan report for 192.168.1.90
Host is up.
Nmap done: 255 IP addresses (6 hosts up) scanned in 3.59 seconds
root@Kali:~#
::1             ff02::2         ip6-allrouters  ip6-loopback    localhost
ff02::1         ip6-allnodes    ip6-localhost   Kali
root@Kali:~# s4
```





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

- Target 1
    - List of Exposed Services
    - Port 22 ssh
    - Port 80 http
    - Port 111 rpcbind
    - Port 139 netbios-ssn
    - Port 445 netbios-ssn

TODO: Fill out the list below. Include severity, and CVE numbers, if possible.

The following vulnerabilities were identified on each target:

- Target 1
    - List of Critical Vulnerabilities

Port 22 is open, this enable us to ssh

Port 80 is open, this enables us to have access to http server

TODO: Include vulnerability scan results to prove the identified vulnerabilities.

Exploitation

TODO: Fill out the details below. Include screenshots where possible.

Wpscan --url http://192.168.1.110/wordpress -eu

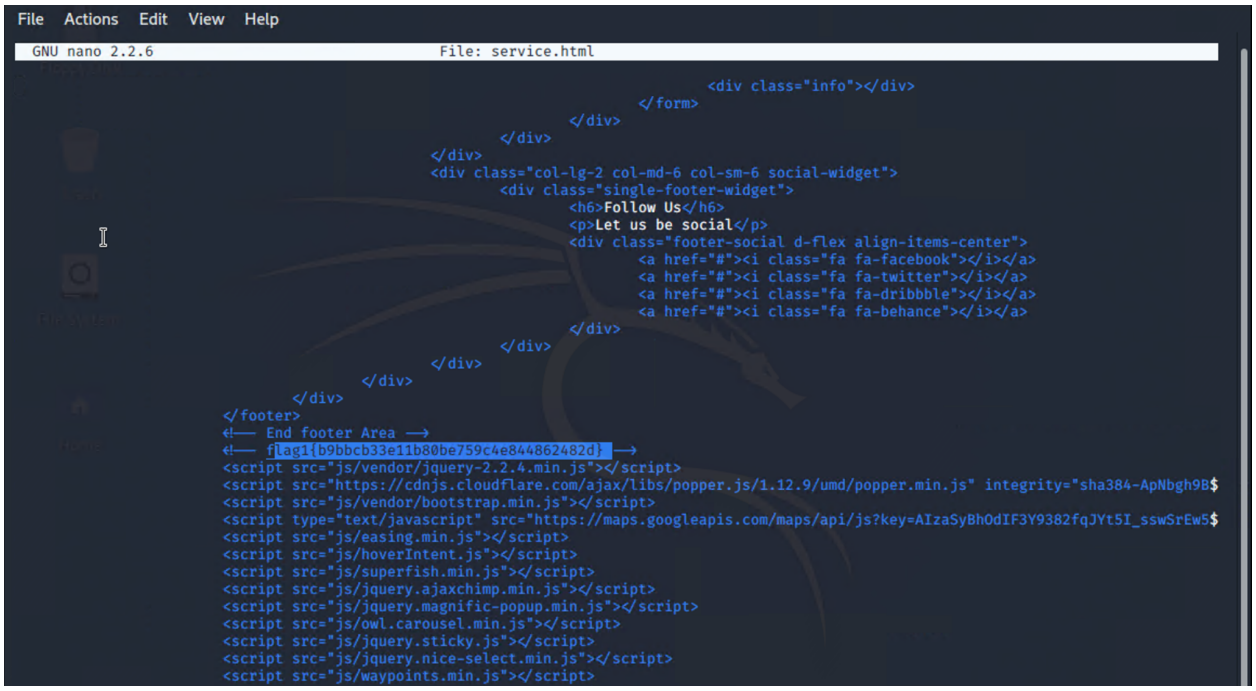
```
[i] User(s) Identified:

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up
```

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

- Target 1
    - flag1.txt: *TODO:* flag1{b9bbcb33e11b80be759c4e844862482d}
    -
        - **Exploit Used**

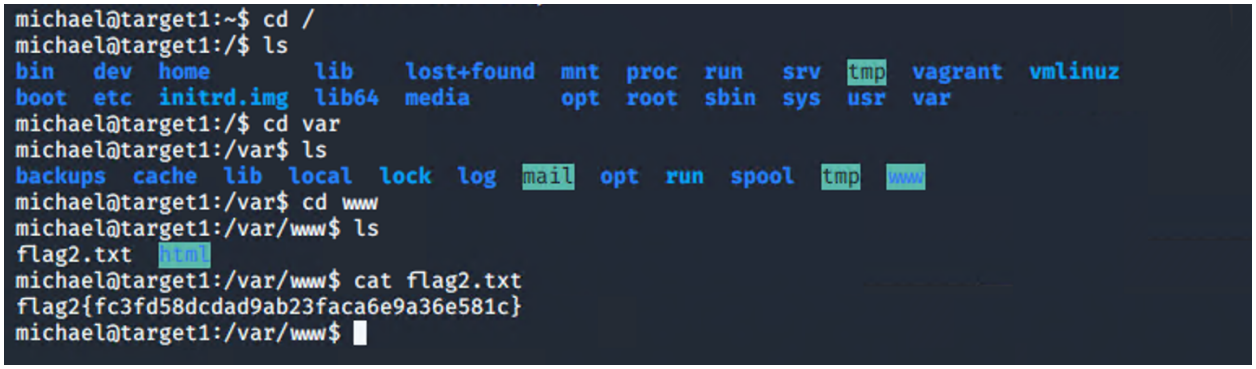
```
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:
Permission denied, please try again.
michael@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Thu Nov 25 13:16:00 2021 from 192.168.1.90
michael@target1:~$
```

```
michael@target1:~$ cd /
michael@target1:/$ ls
bin   dev  home        lib    lost+found  mnt  proc  run   srv  tmp  vagrant  vmlinuz
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  var
michael@target1:/$ cd var
michael@target1:/var$ ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
michael@target1:/var$ cd www
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```



- *TODO: Identify the exploit used*
- *TODO: Include the command run*

- flag2.txt: *TODO:* flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
-
  - **Exploit Used**



- *TODO: Identify the exploit used*
- *TODO: Include the command run*