Red Team: Summary of Operations

Table of Contents

Exposed Services

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

$ nmap -sV 198.168.1.110

```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-04 08:45 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00054s latency).
Not shown: 995 closed ports
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 12.22 seconds
root@Kali:~#
```

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 netbios-ssn

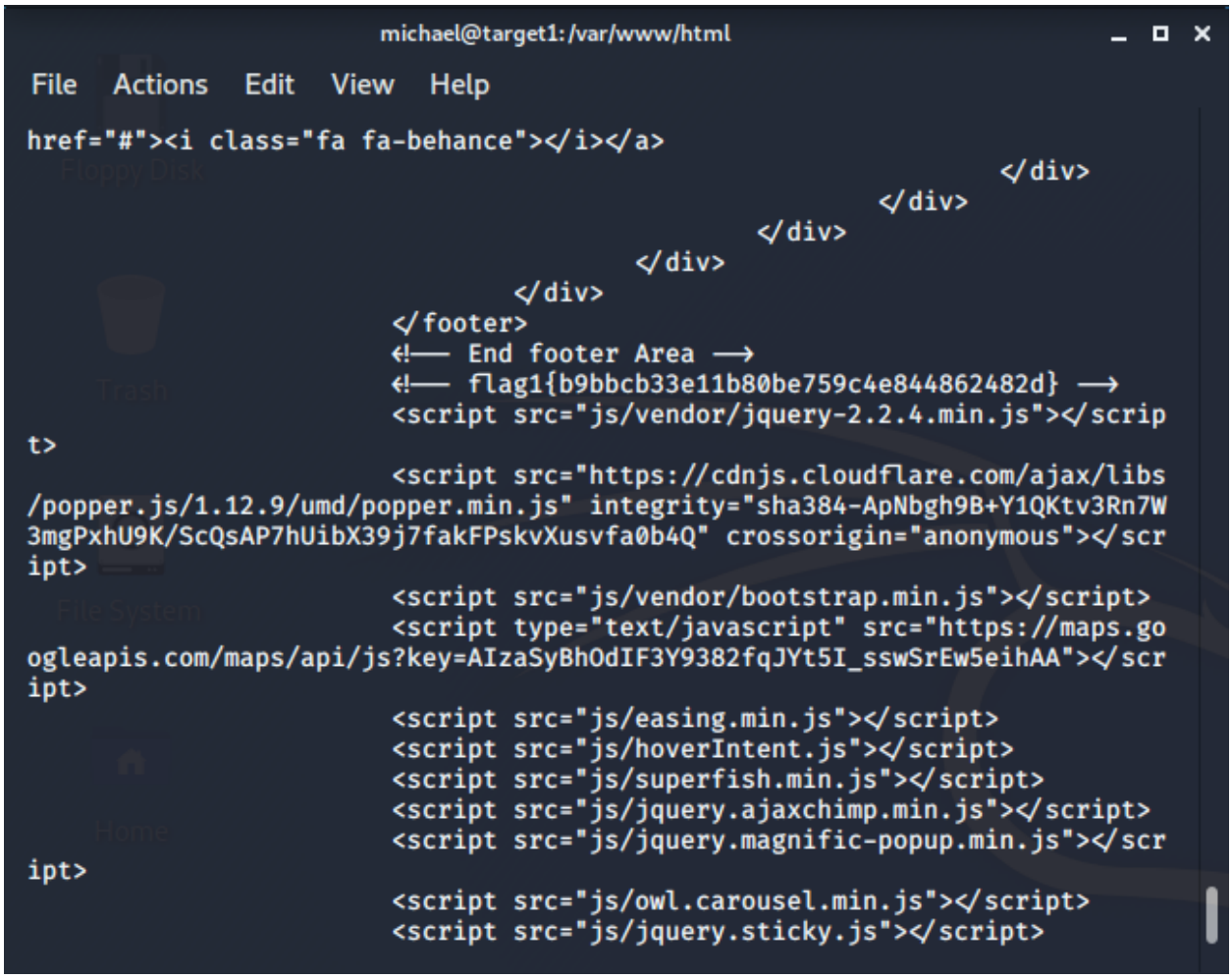
The following vulnerabilities were identified on each target:

- Target 1
    - List of
    - Critical
    - Vulnerabilities

Exploitation

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

- Target 1



- Flag1.txt: b9bbcb33e11b80be759c4e844862482d
  - **Exploit Used**
    - *WPScan*
    - *Wpscan - -url http://192.168.1.110/wordpress - -enumerate u*
    - *$ cd /var/www/html*
    - *ls*
    - *$ cat service.html*

- flag2.txt: fc3fd58dcdad9ab23faca6e9a36e581c

```
michael@target1:~$ ls
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$
```

- **Exploit Used**
  - *Wpscan - -url http://192.168.1.110/wordpress - -enumerate u*
  - *$ cd /var/www/*
  - *ls*
  - *$ cat flag2.txt*