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:

```bash
$ nmap ... # TODO: nmap -sV 192.168.1.110


```

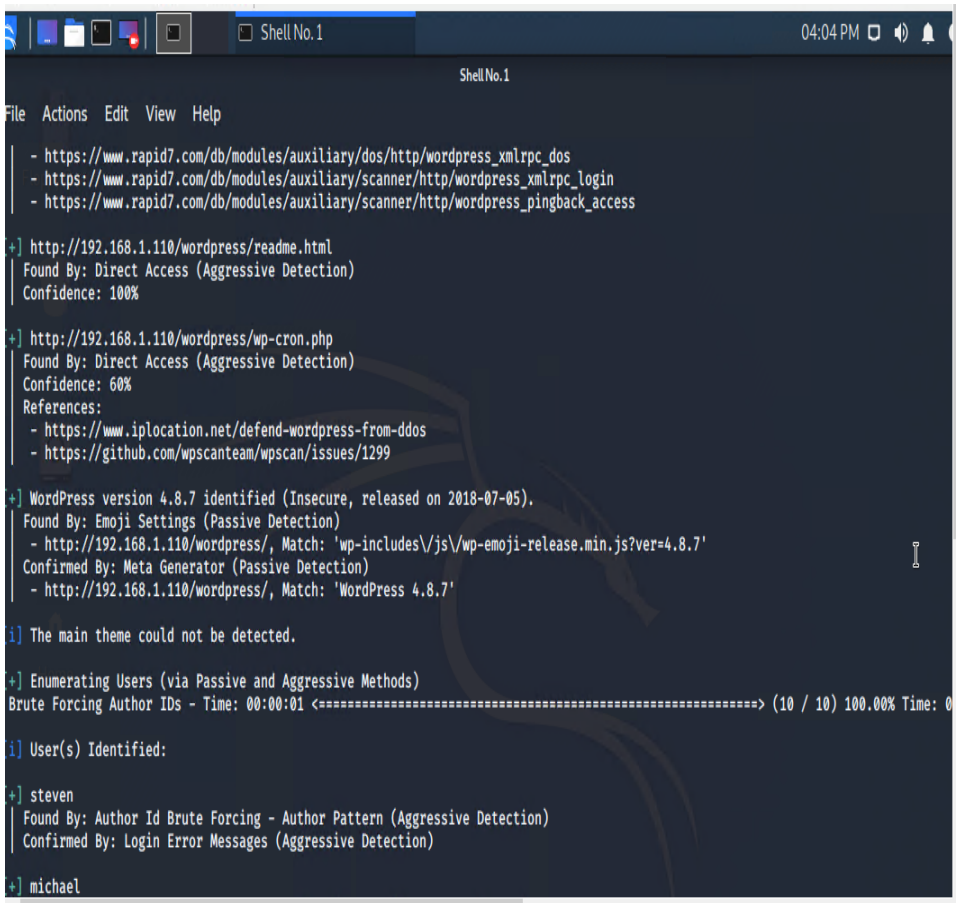
This scan identifies the services below as potential points of entry:
- Target 1
  - List of
  - Exposed Services : ssh, http, rcpbind, netbios-ssn,

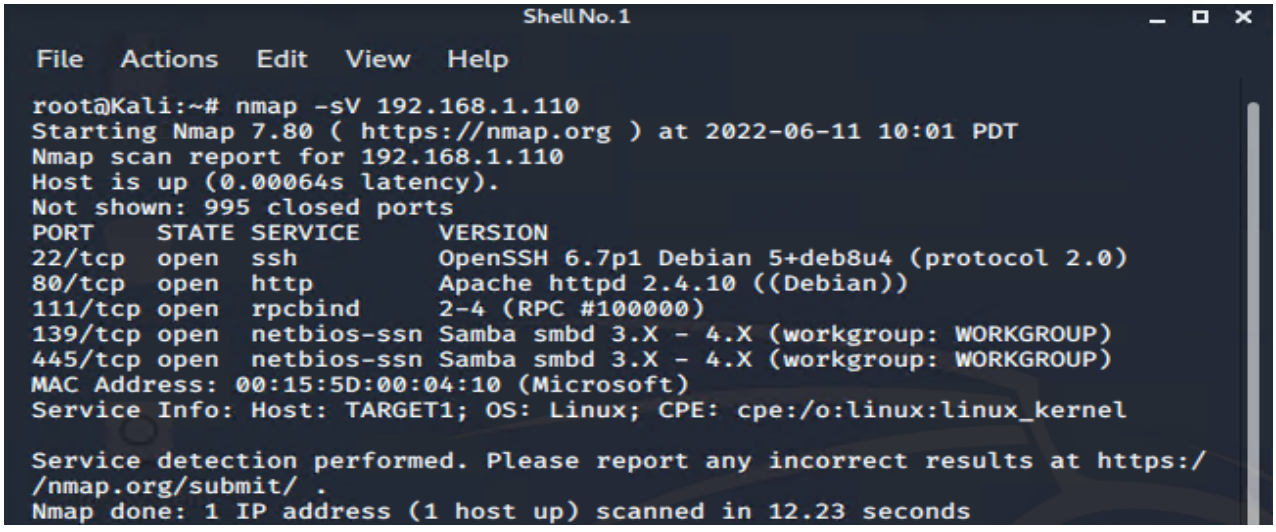
Fill out the list below. Include severity, and CVE numbers, if possible._

The following vulnerabilities were identified on each target:
- Target 1
  - List of
  - Critical
  - Vulnerabilities:

User Enumeration- CVE-2009-2335: Allowed for us to discover usernames. Severity of 5.0.
Weak Password Requirements- CWE-521- This allowed us to easily guess Michael's password. Severity of 8.1.
Wordpress Config File Exposed- CVE-2021-24692 – This allowed us to access the config file without any further authentication. Severity 6.5.
Privilege Escalation- CVE-2018-1000030- Using sudo -l showed us privilege that allowed us to run python command to escalate privileges. Severity 3.6.

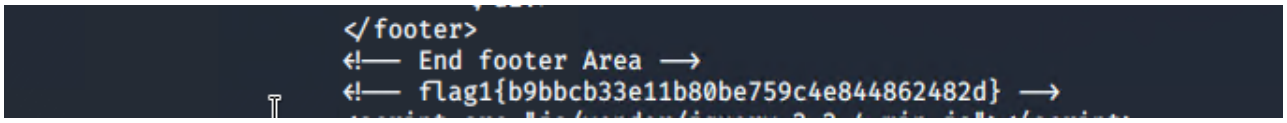
Include vulnerability scan results to prove the identified vulnerabilities._


Shell No. 1
04:04 PM
Shell No. 1
File Actions Edit View Help
- https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
- https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
- https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access
[+] http://192.168.1.110/wordpress/readme.html
Found By: Direct Access (Aggressive Detection)
Confidence: 100%
[+] http://192.168.1.110/wordpress/wp-cron.php
Found By: Direct Access (Aggressive Detection)
Confidence: 60%
References:
- https://www.iplocation.net/defend-wordpress-from-ddos
- https://github.com/wpscanteam/wpscan/issues/1299
[+] WordPress version 4.8.7 identified (Insecure, released on 2018-07-05).
Found By: Emoji Settings (Passive Detection)
- http://192.168.1.110/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=4.8.7'
Confirmed By: Meta Generator (Passive Detection)
- http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.7'
[i] The main theme could not be detected.
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:01 <==========> (10 / 10) 100.00% Time: 0
[i] User(s) Identified:
[+] steven
Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
Confirmed By: Login Error Messages (Aggressive Detection)
[+] michael

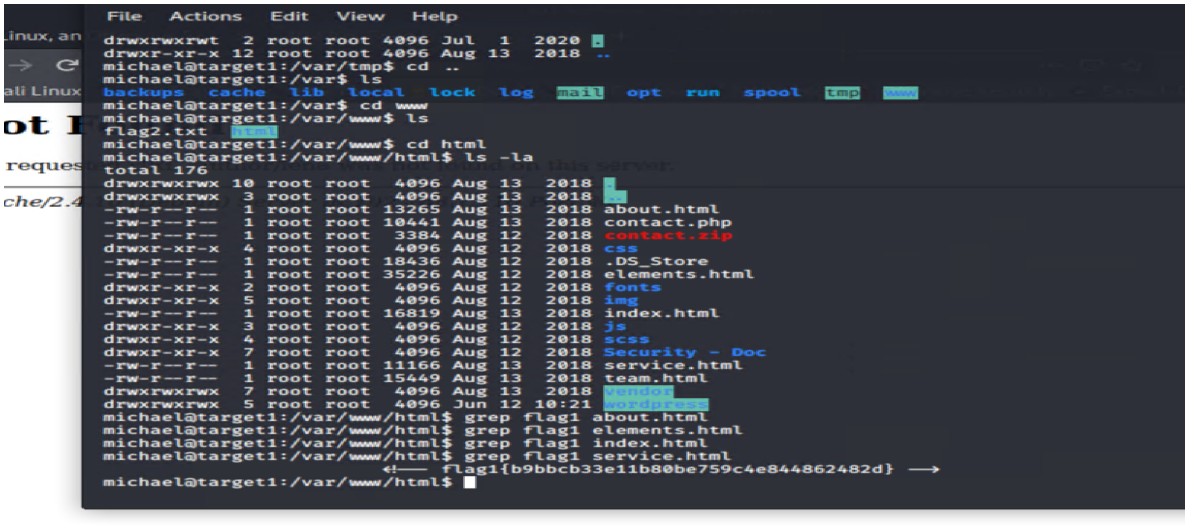

Shell No. 1
File Actions Edit View Help
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 (https://nmap.org) at 2022-06-11 10:01 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00064s latency).
Not shown: 995 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 6.7p1 Debian 5+deb8u4 (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 12.23 seconds

Exploitation

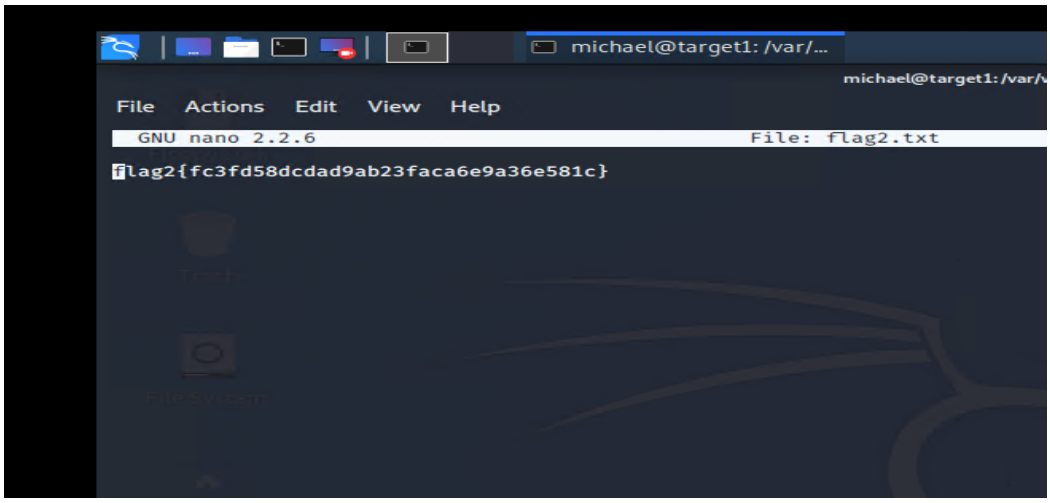
The Red Team was able to penetrate `Target 1` and retrieve the following confidential data:
- Target 1
  - `flag1.txt`:



  - **Exploit Used**



  - `flag2.txt`:



- **Exploit Used**

```
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$ cd html
michael@target1:/var/www/html$ ls -l
total 148
-rw-r--r-- 1 root root 13265 Aug 13  2018 about.html
-rw-r--r-- 1 root root 10441 Aug 13  2018 contact.php
-rw-r--r-- 1 root root  3384 Aug 12  2018 contact.zip
drwxr-xr-x 4 root root  4096 Aug 12  2018 css
-rw-r--r-- 1 root root 35226 Aug 12  2018 elements.html
drwxr-xr-x 2 root root  4096 Aug 12  2018 fonts
drwxr-xr-x 5 root root  4096 Aug 12  2018 img
-rw-r--r-- 1 root root 16819 Aug 13  2018 index.html
drwxr-xr-x 3 root root  4096 Aug 12  2018 js
drwxr-xr-x 4 root root  4096 Aug 12  2018 scss
drwxr-xr-x 7 root root  4096 Aug 12  2018 Security - Doc
-rw-r--r-- 1 root root 11166 Aug 13  2018 service.html
-rw-r--r-- 1 root root 15449 Aug 13  2018 team.html
drwxrwxrwx 7 root root  4096 Aug 13  2018 vendor
drwxrwxrwx 5 root root  4096 Jun 12 10:21 wordpress
michael@target1:/var/www/html$ cd ../
michael@target1:/var/www$ ls -l
total 8
-rw-r--r--  1 root root   40 Aug 13  2018 flag2.txt
drwxrwxrwx 10 root root 4096 Aug 13  2018 html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```