

# Ethical Hacking and Penetration Testing

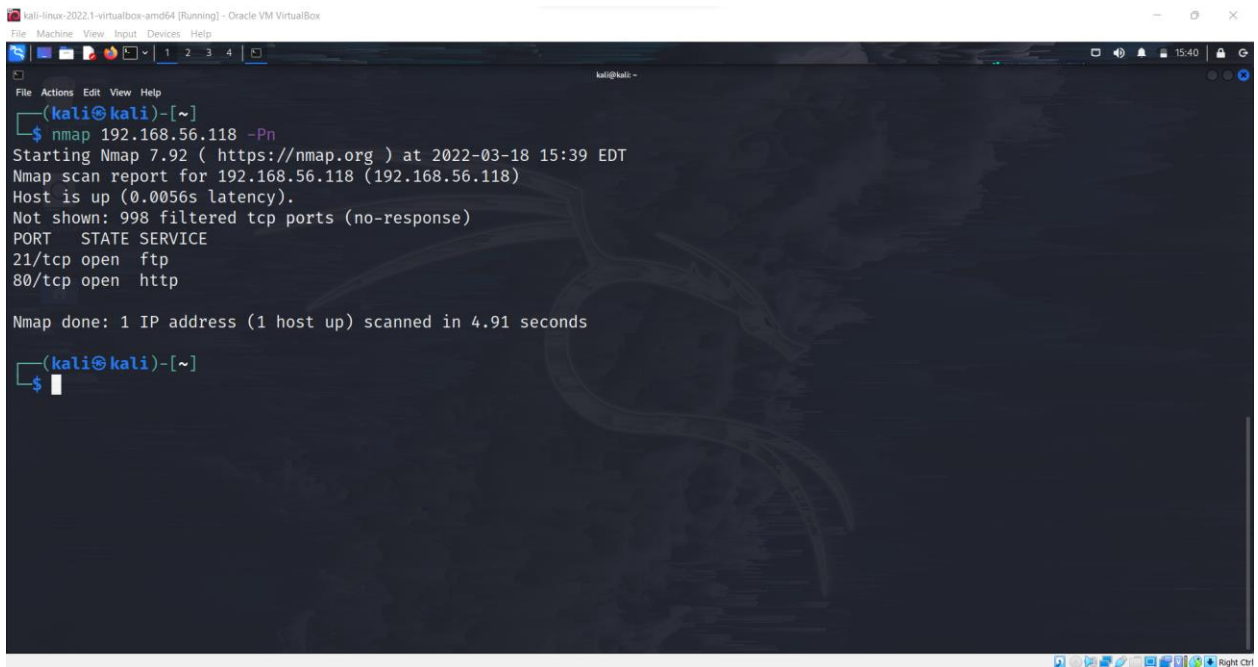
## Assignment 2

### Scanning and Enumerating to login to Jangow VM

Name: John Ehab

ID: 100-2096

1- Search for the open ports in the given IP address using nmap, we'll notice that port 80 is open, this means that it uses http.

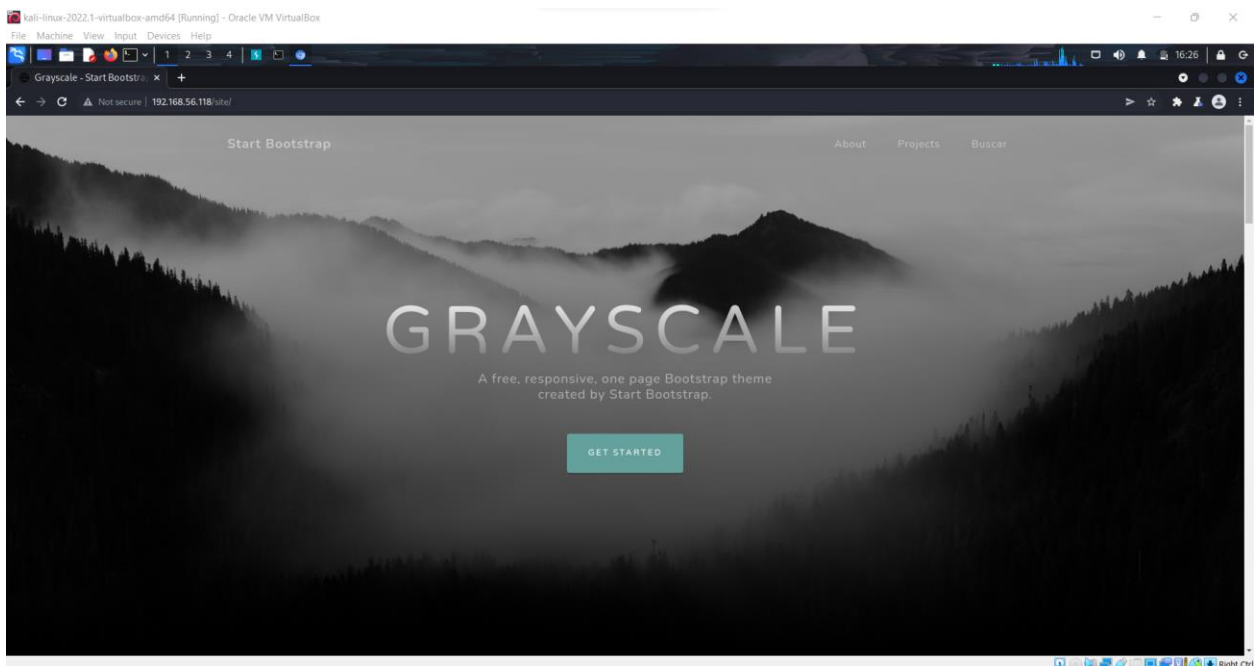


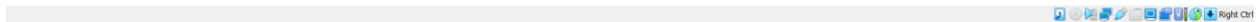
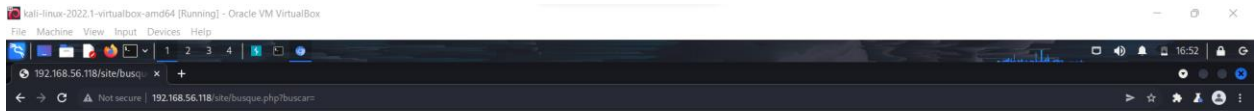
```
kali@kali:~$ nmap 192.168.56.118 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-18 15:39 EDT
Nmap scan report for 192.168.56.118 (192.168.56.118)
Host is up (0.0056s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 4.91 seconds

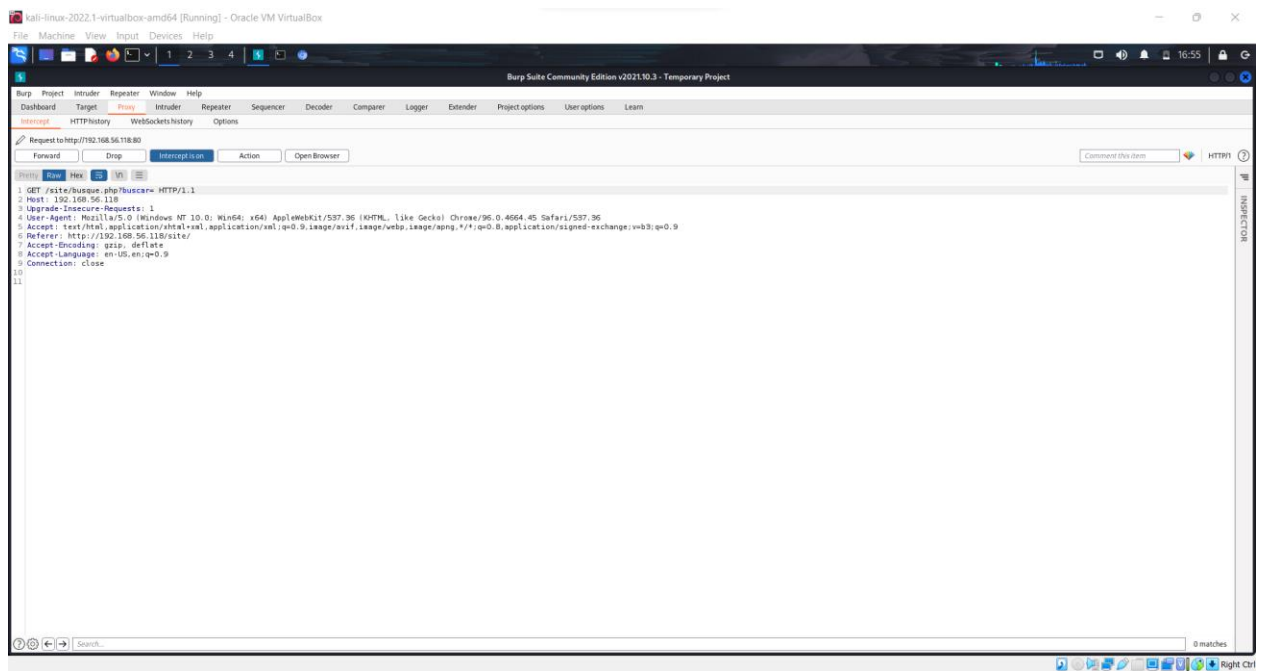
kali@kali:~$
```

2- Then I started navigating the different webpages of the website, and I found out that buscar webpage is passing a parameter in its url, it might not be secured.



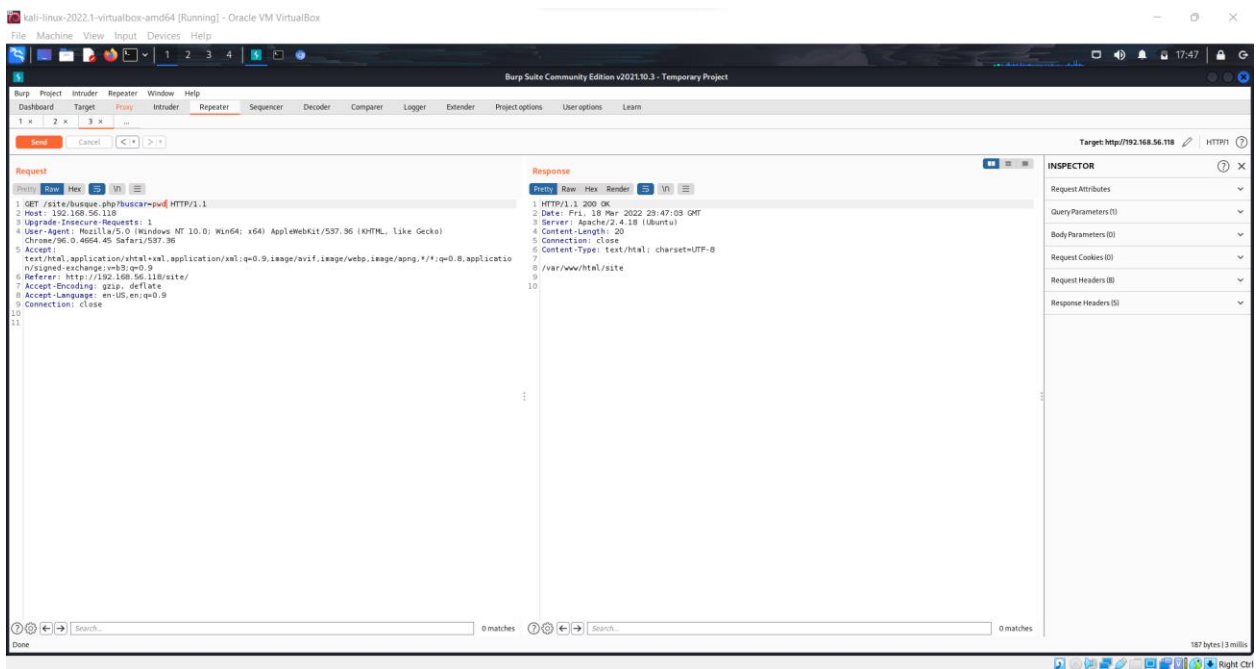


3- I used burpsuite proxy to intercept the packet.

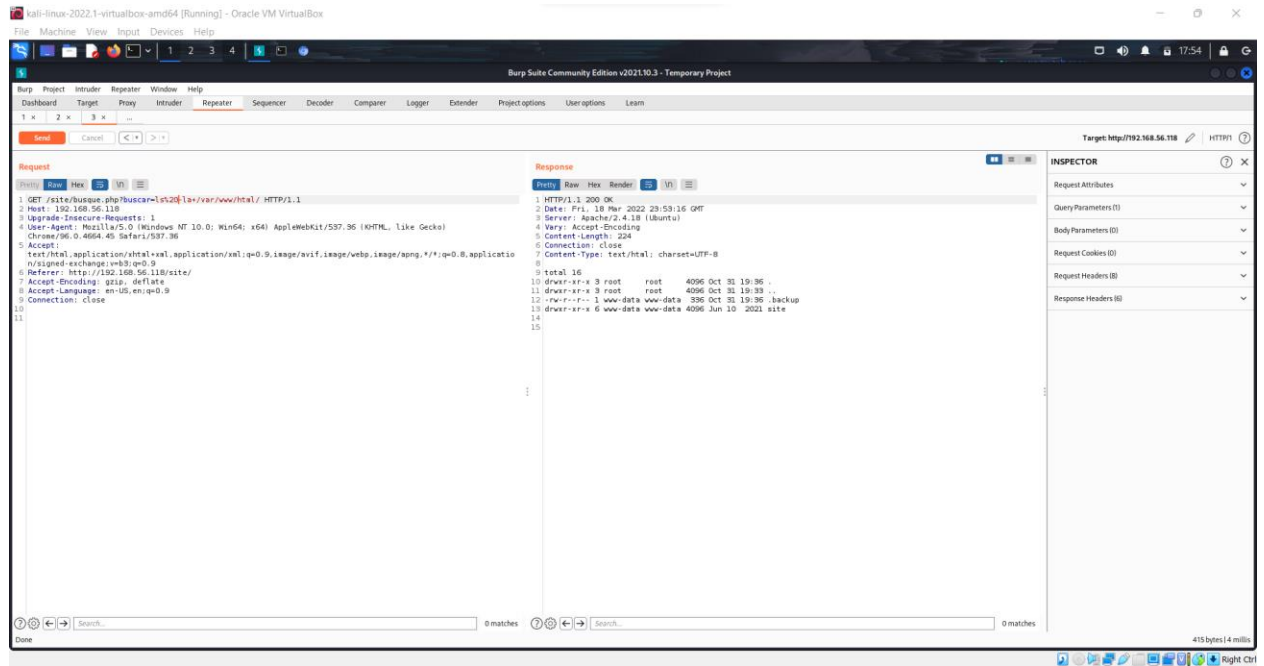


4- Then I sent it to the burpsuite repeater to be able to play with the buscar parameter in that get request and I found out that it has an OS command injection vulnerability as it allows me to write any command in the url and it executes it on the server without filtering or validating it. This will allow me to access files from the server, so I just need to start searching for the file that contains the username and password.

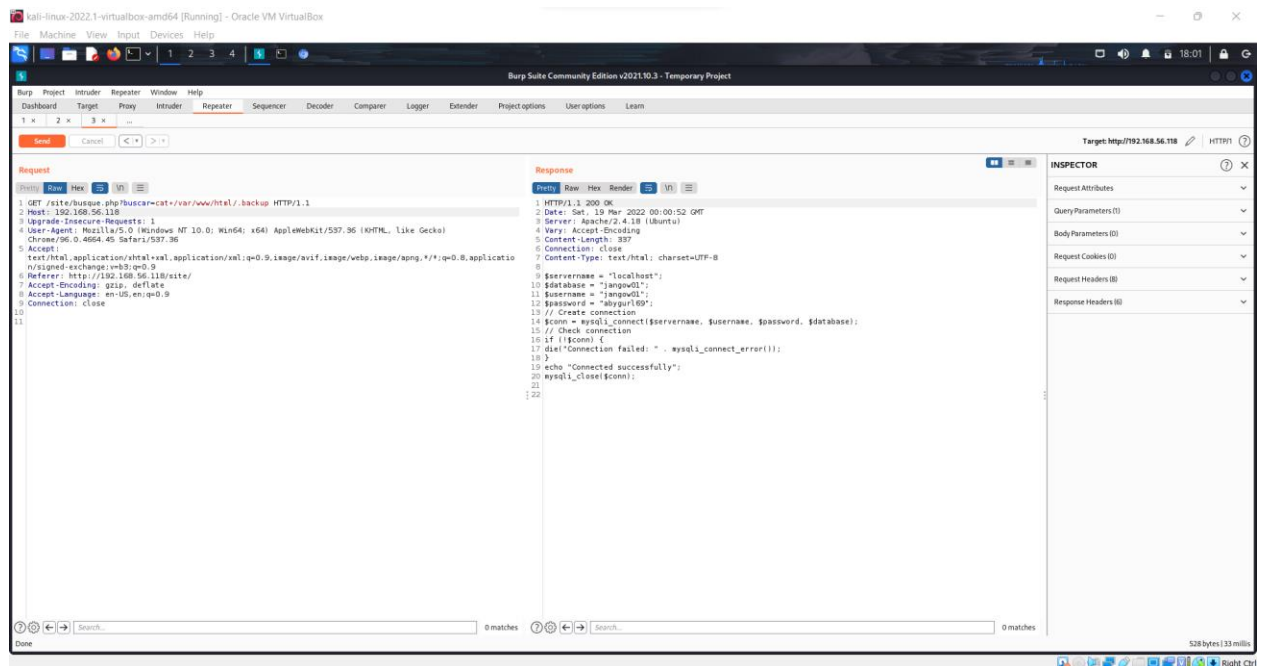
5- pwd to see in which directory we are.



6- ls in the upper folder to see the list of files and directories.



7- cat to open the backup file, use the username and password shown to login to the machine.



8- Finally, a screenshot after successfully logging in to the machine using the username “jangow01” and the password “abygurl69”.

