TAHA BORAN KOTAN

CYBER SECURITY

CFSS INTERNSHIP PROGRAM

TAHA BORAN KOTAN
PROJECT 1: METASPLOITABLE 2
INSTALLATION PROCESS

TAHA BORAN KOTAN

ABOUT THE PROJECT 1

IN THIS PROJECT, I WILL PRESENT TO YOU HOW TO INSTALL METASPLOITABLE 2 ON YOUR VIRTUAL MACHINE.

WHAT IS THE METASPLOITABLE 2

METASPLOITABLE2 IS A TEST ENVIRONMENT CREATED FOR USE IN HANDS-ON PENETRATION TESTING TRAINING AND SECURITY RESEARCH.

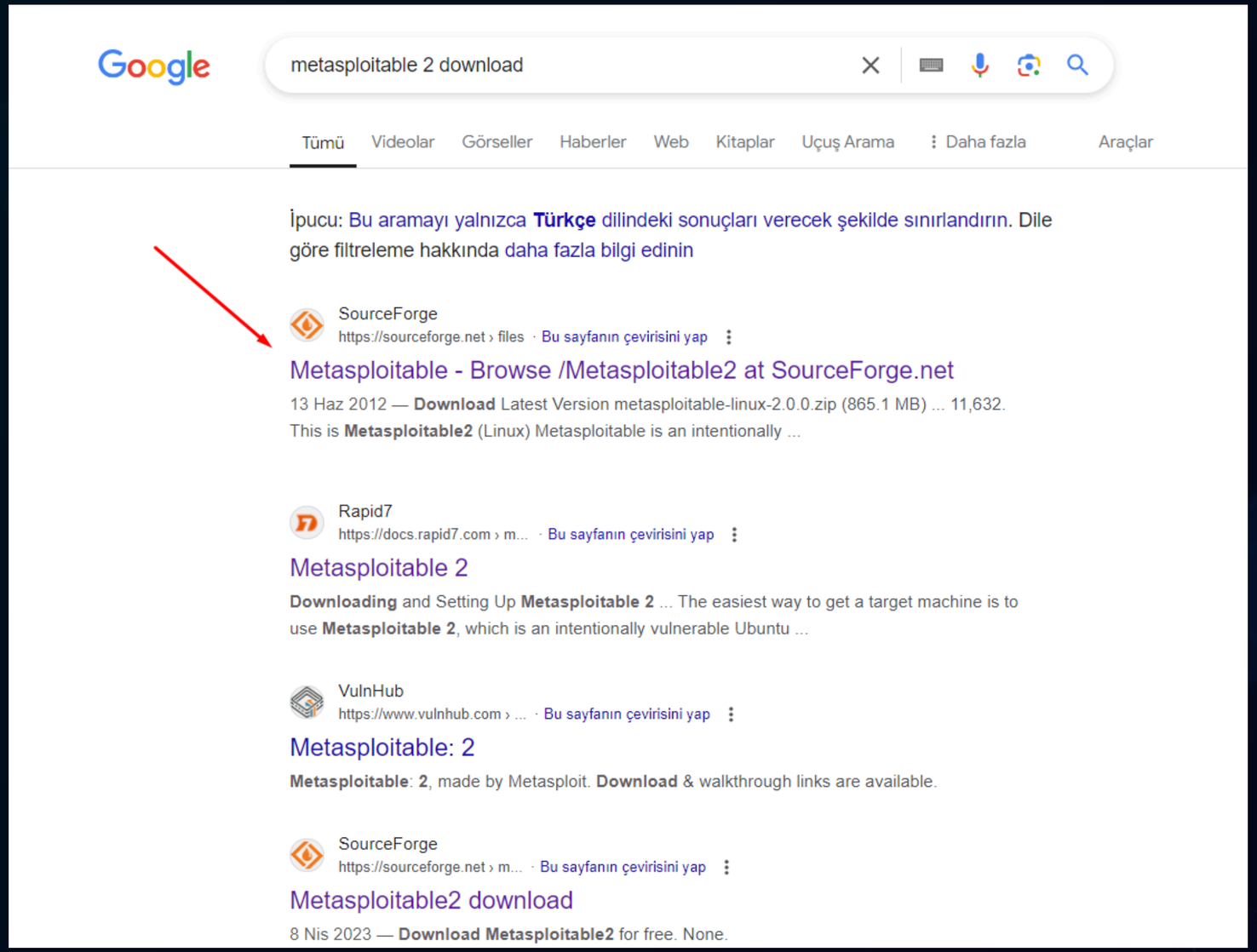
INSTALLATION =>

TAHA BORAN KOTAN

STEP 1

- In first step, we should download the Metasploitable 2 files on the Internet. You can use any search engine for reach to the downloading site.

- Write “metasploitable 2 download” and click the “SourceForge” result. Then you will might achieve this url: https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

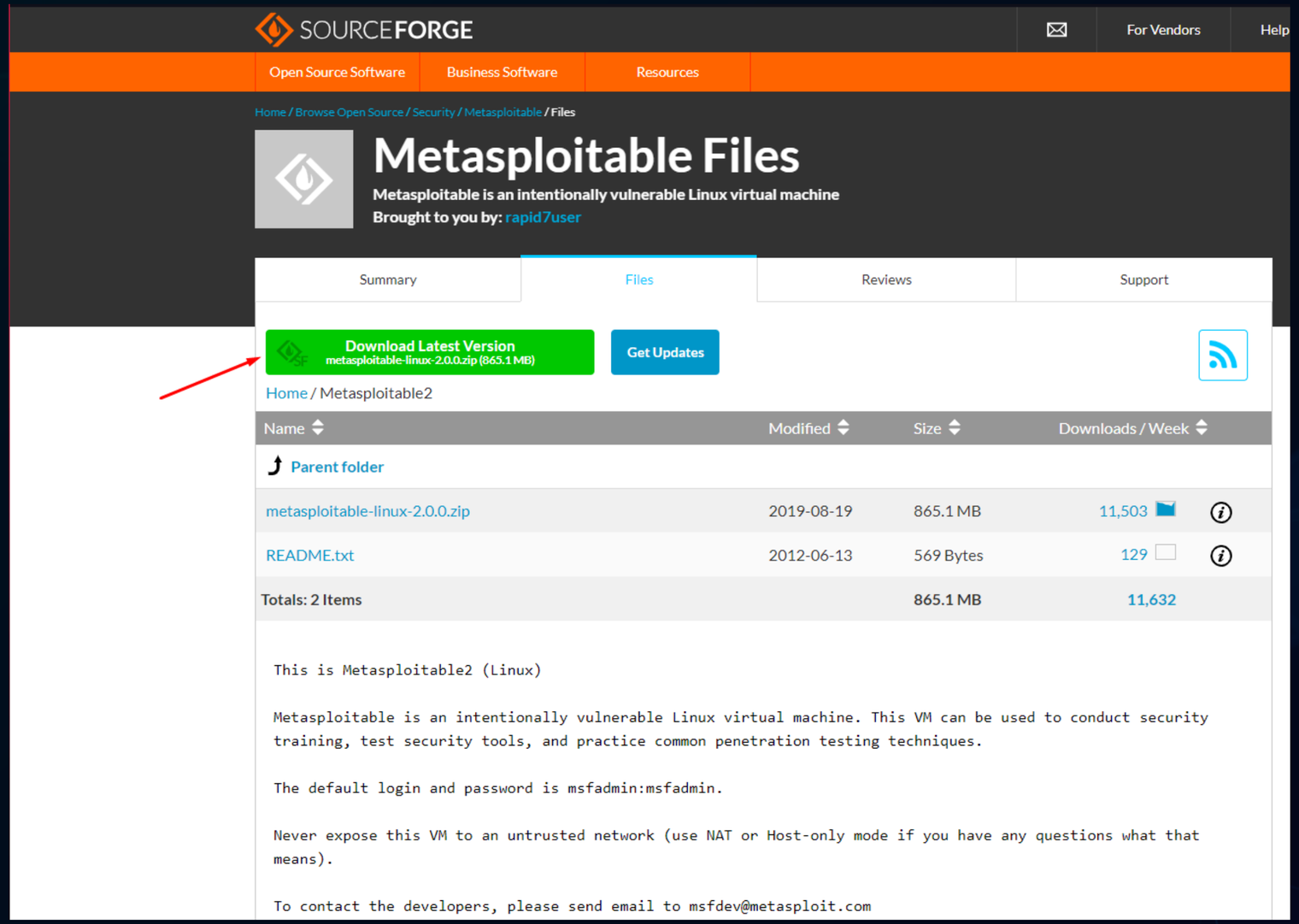


TAHA BORAN KOTAN

STEP 2

- After that, the page will look the same with the picture.

- Click the -green- “Download Latest Version” button, then the downloading will be started.



TAHA BORAN KOTAN

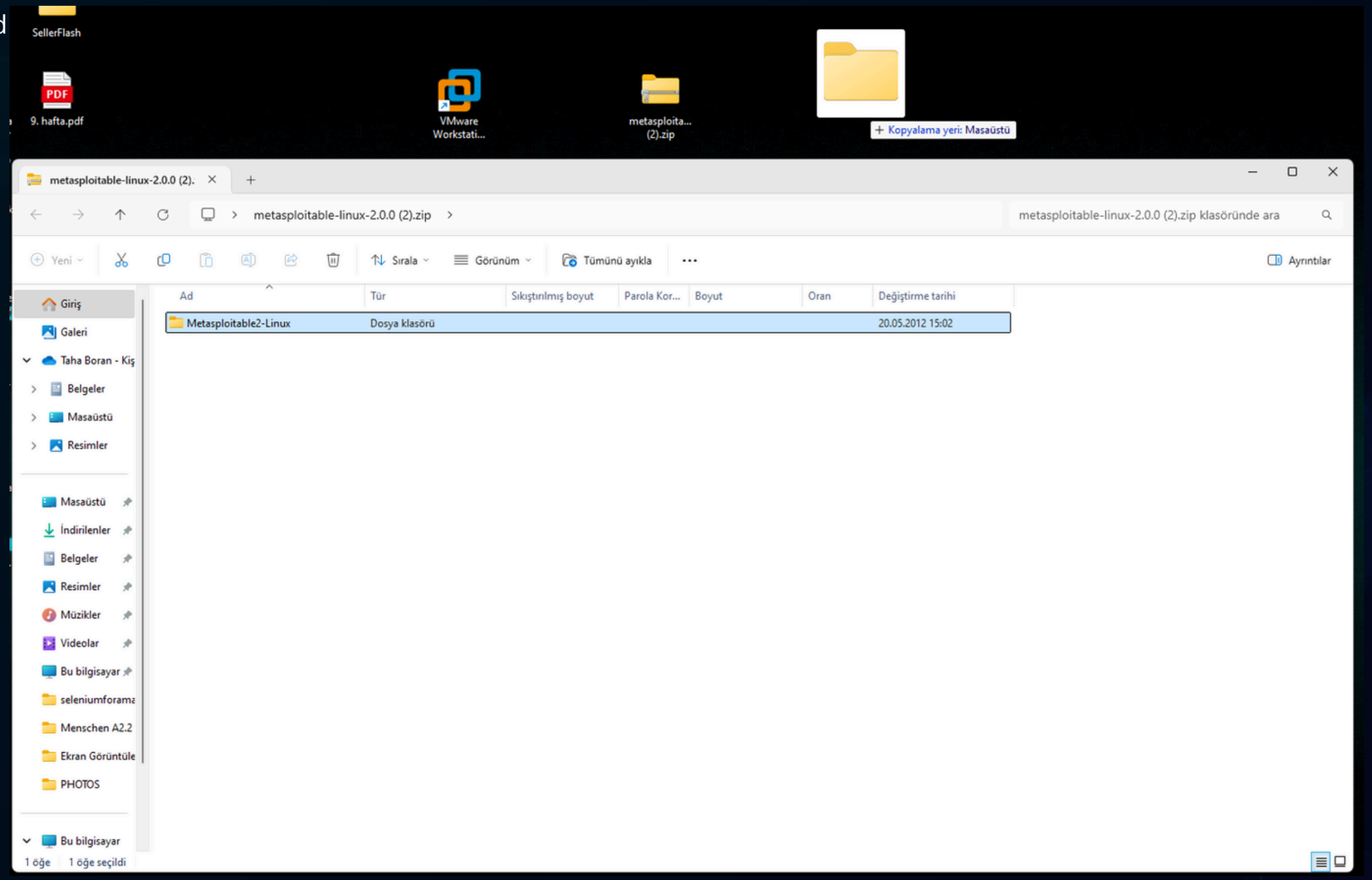
STEP 3

- After the downloading, we will had downloaded a zip folder. So, we should unzip this folder.

- For unzip this folder, firstly we should click and open the zip folder, then we should drag this file to desktop or where we want.

- We will do the eaisest way ant drag this folder to desktop. After unzipping process, Open the folder.

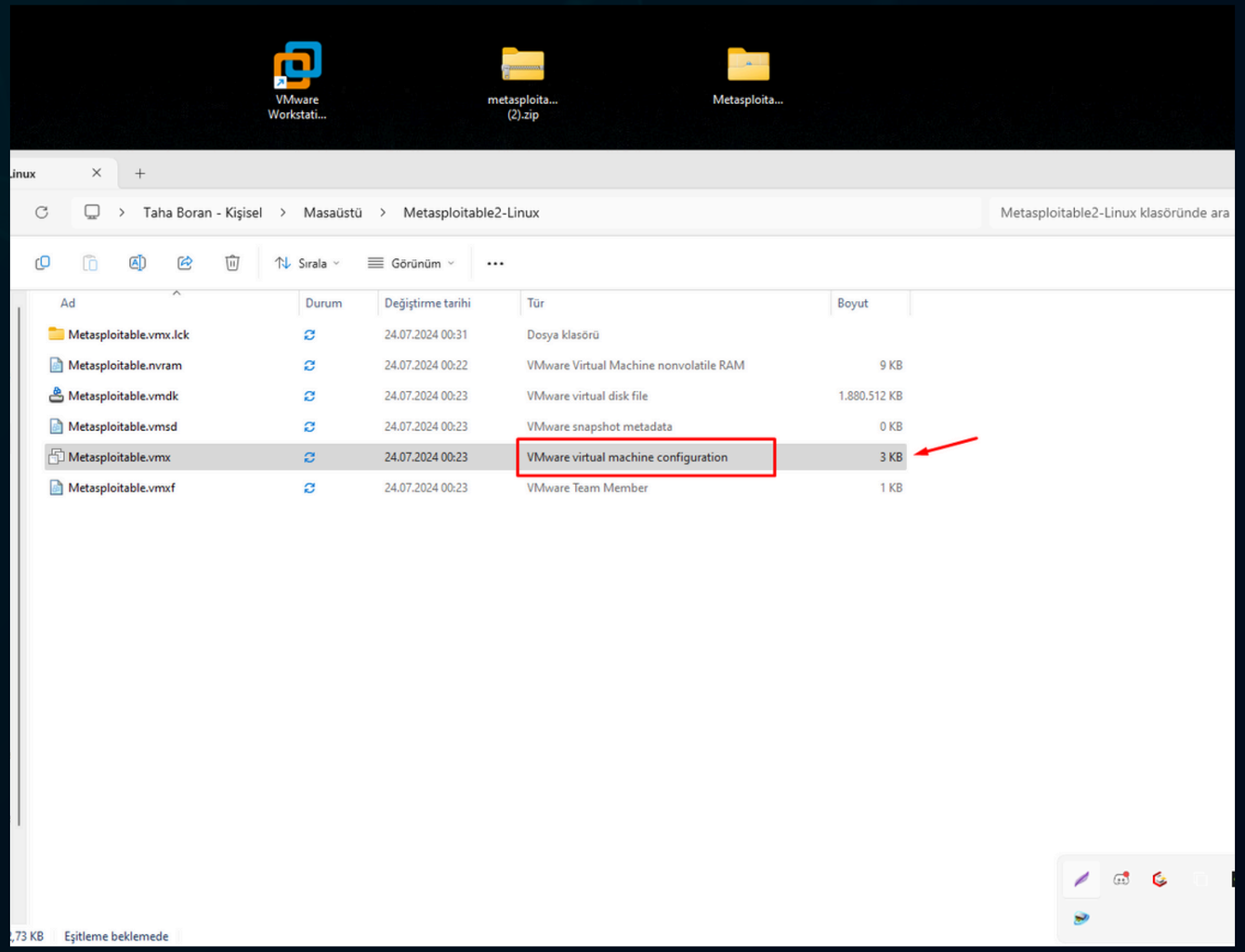
- After unzipping process, Open the folder.



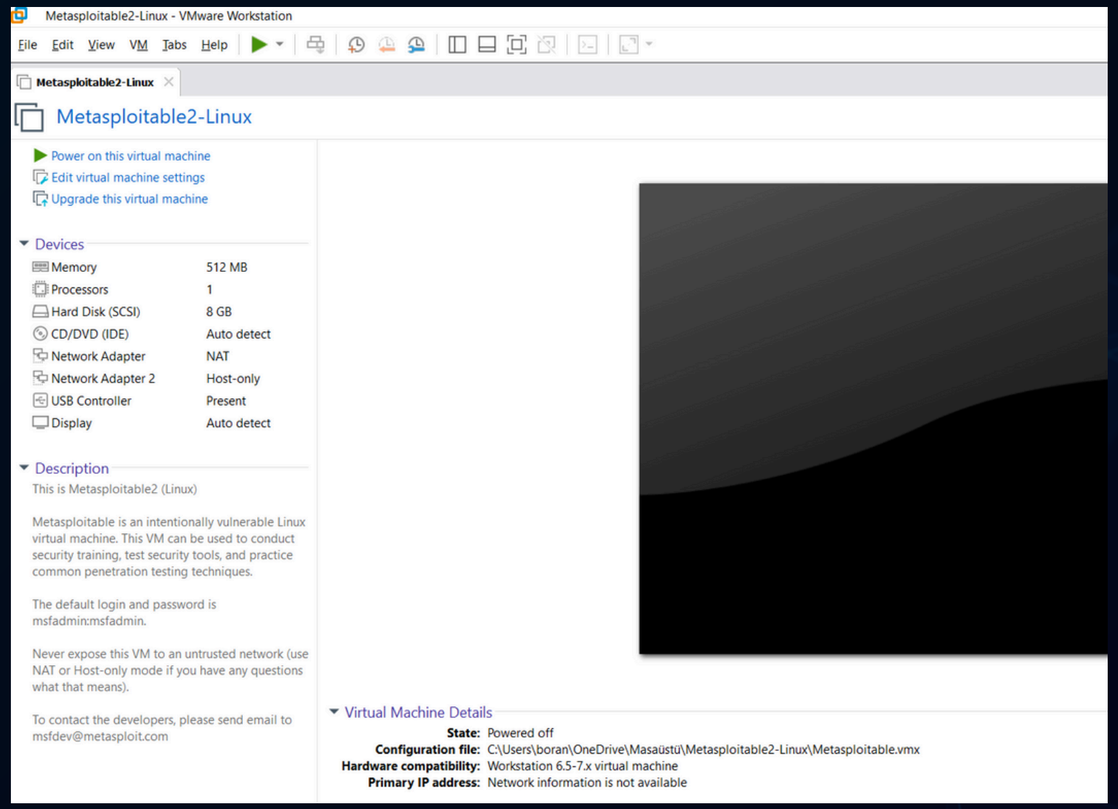
TAHA BORAN KOTAN

STEP 4

- We have been installing the Metasploitable 2 for using on our virtual machines. So, I suppose you already have a virtual environment. In this case I have a VMware Workstation Virtual Environment.



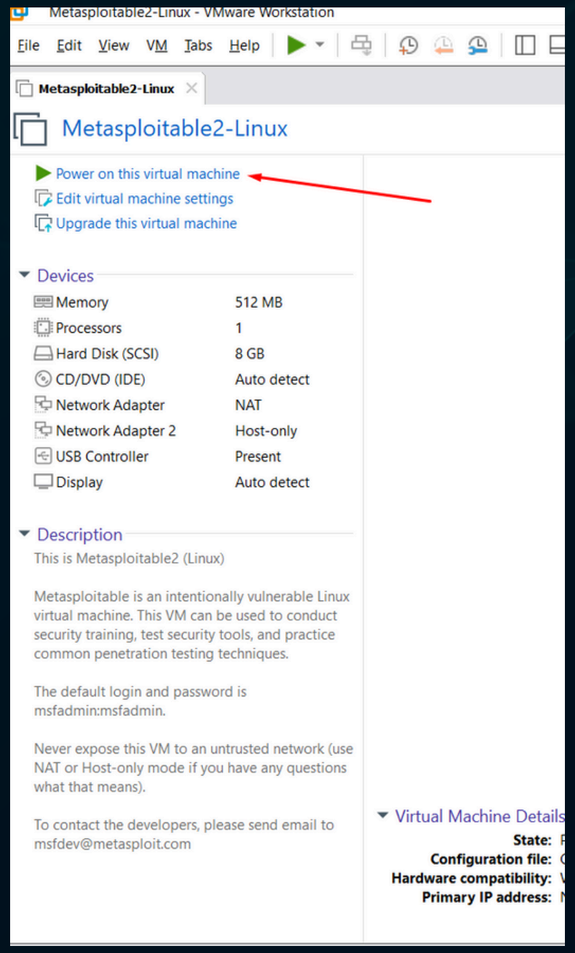
- After the opening folder, click “Metasploitable.vmx” file. As you can see, it is a configuration file. After clicking, Metasploitable 2 will automatically opens in your Virtual Environment.



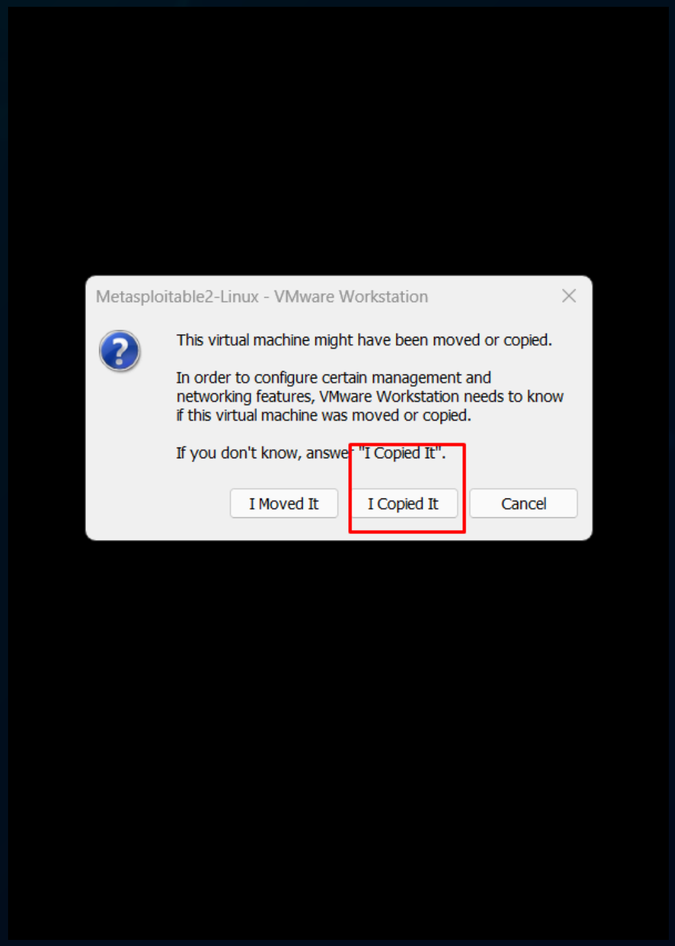
TAHA BORAN KOTAN

STEP 5

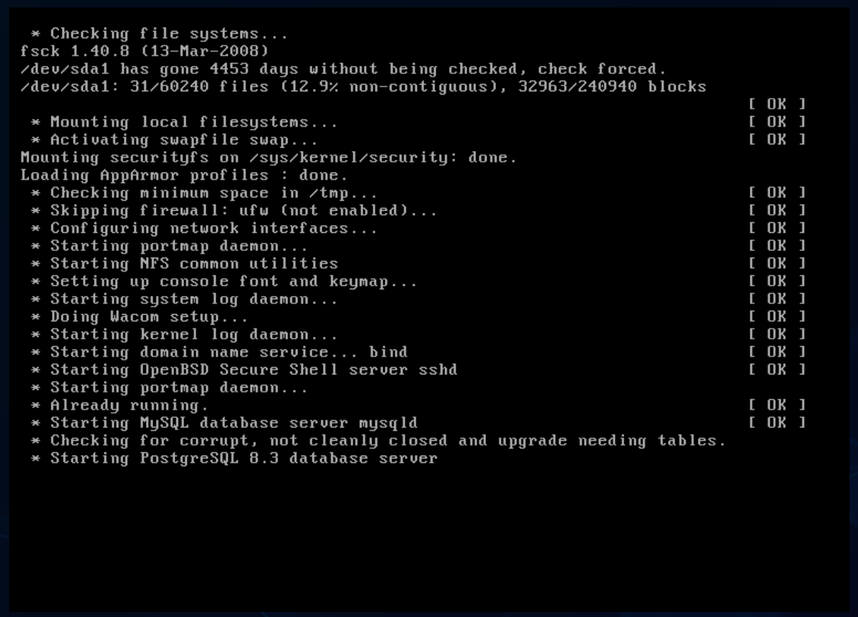
- Click: “Power on this virtual machine”.



- Click: “I Copied It”.



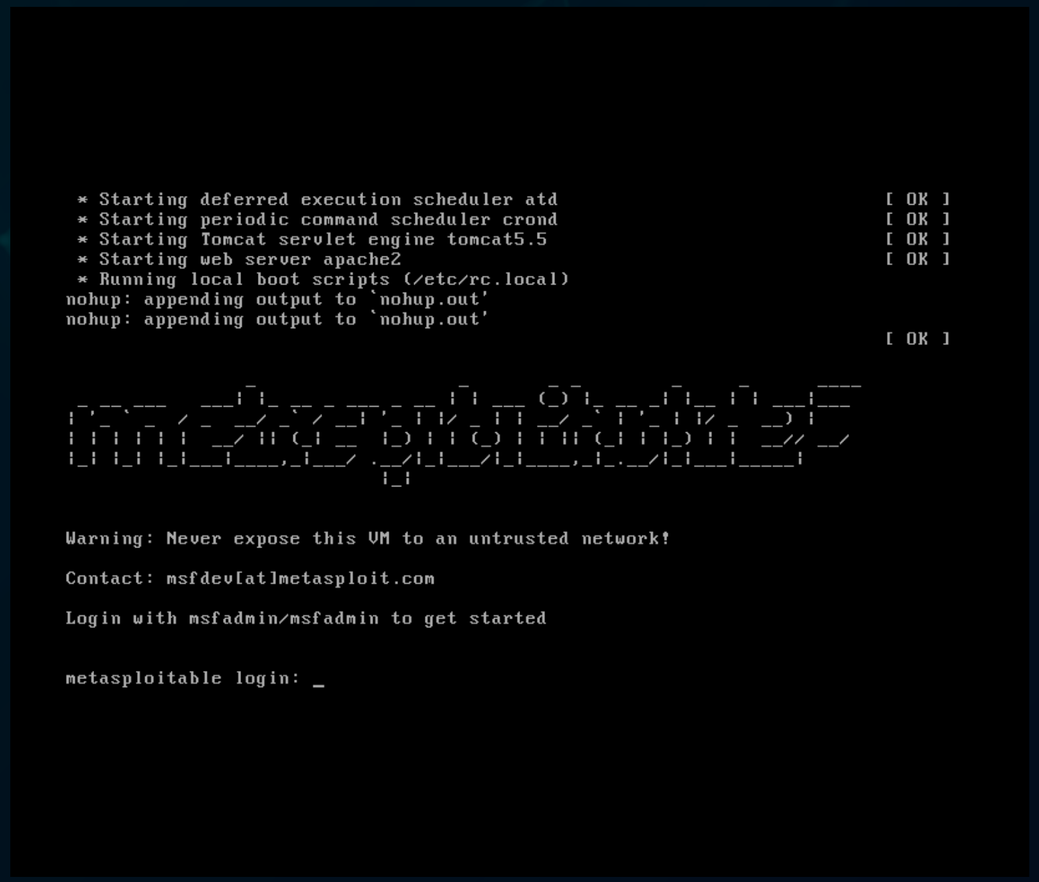
- Installation starts…

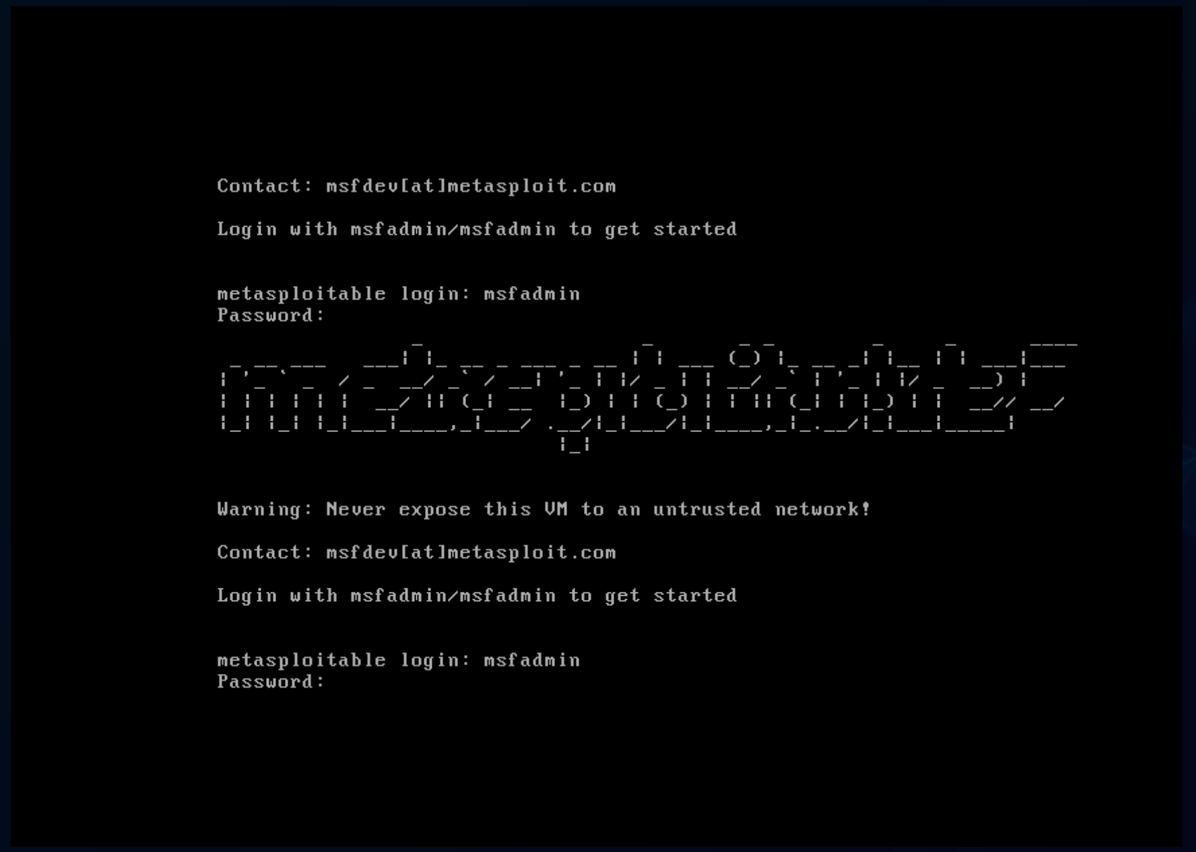


TAHA BORAN KOTAN

STEP 6

- Installation ended.





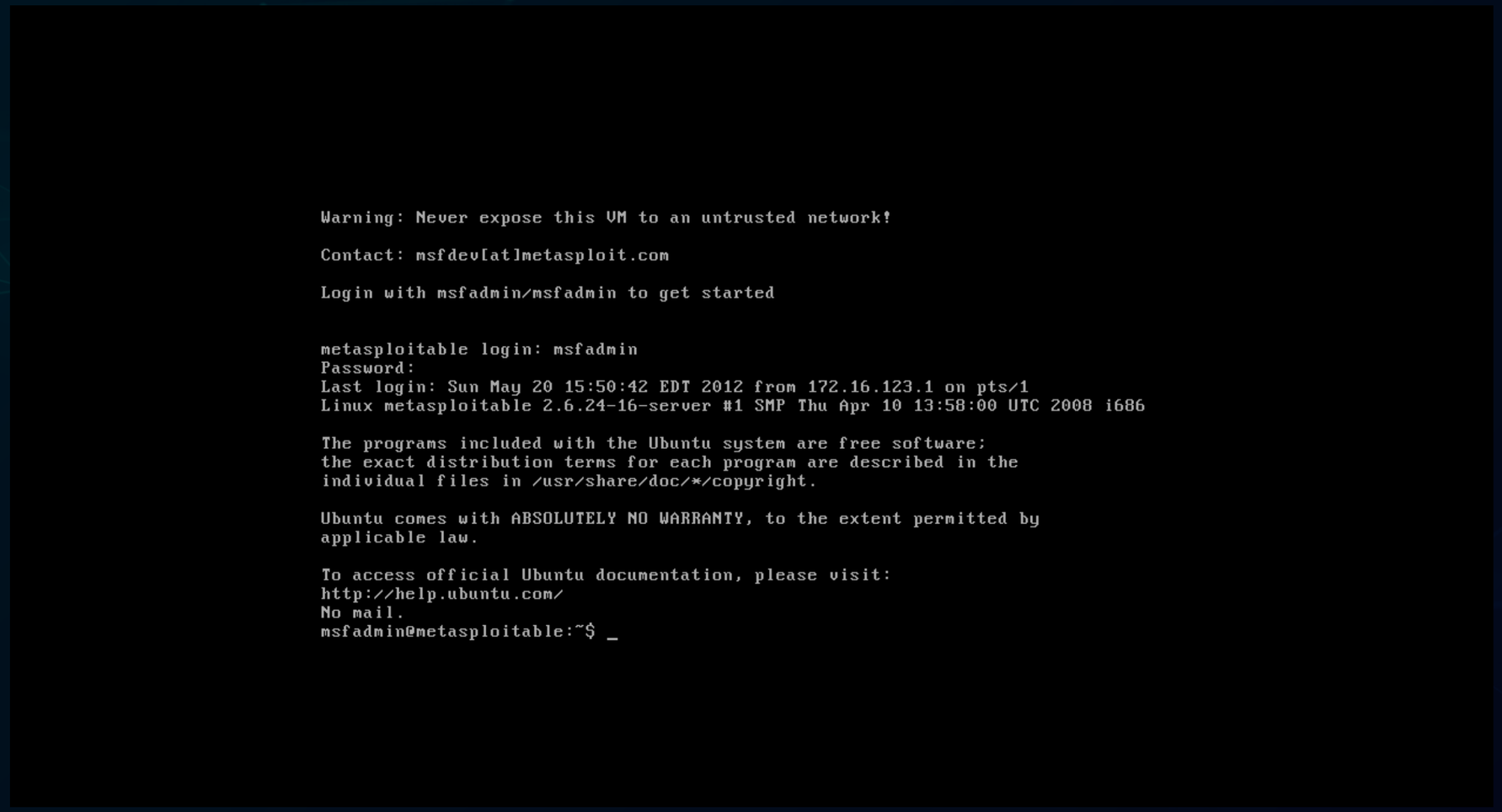
- username: msfadmin
- password: msfadmin

While you are writing the password, it won't being shown.

TAHA BORAN KOTAN

CONGRATULATIONS!

- If you see this page, you successfully installed the Metasploitable!



- So, you are in the machine now. You can try “ifconfig”,”whoami” etc. commands.

TAHA BORAN KOTAN

CYBER SECURITY

CFSS INTERNSHIP PROGRAM

TAHA BORAN KOTAN
PROJECT 2: GETTING LOGIN PAGE CREDENTIALS WITH BURP SUITE

TAHA BORAN KOTAN

ABOUT THE PROJECT 1

IN THIS PROJECT, I WILL PRESENT TO YOU HOW TO GET LOGIN CREDENTIALS USING WITH BURP SUITE.

WHAT IS THE BURP SUITE?

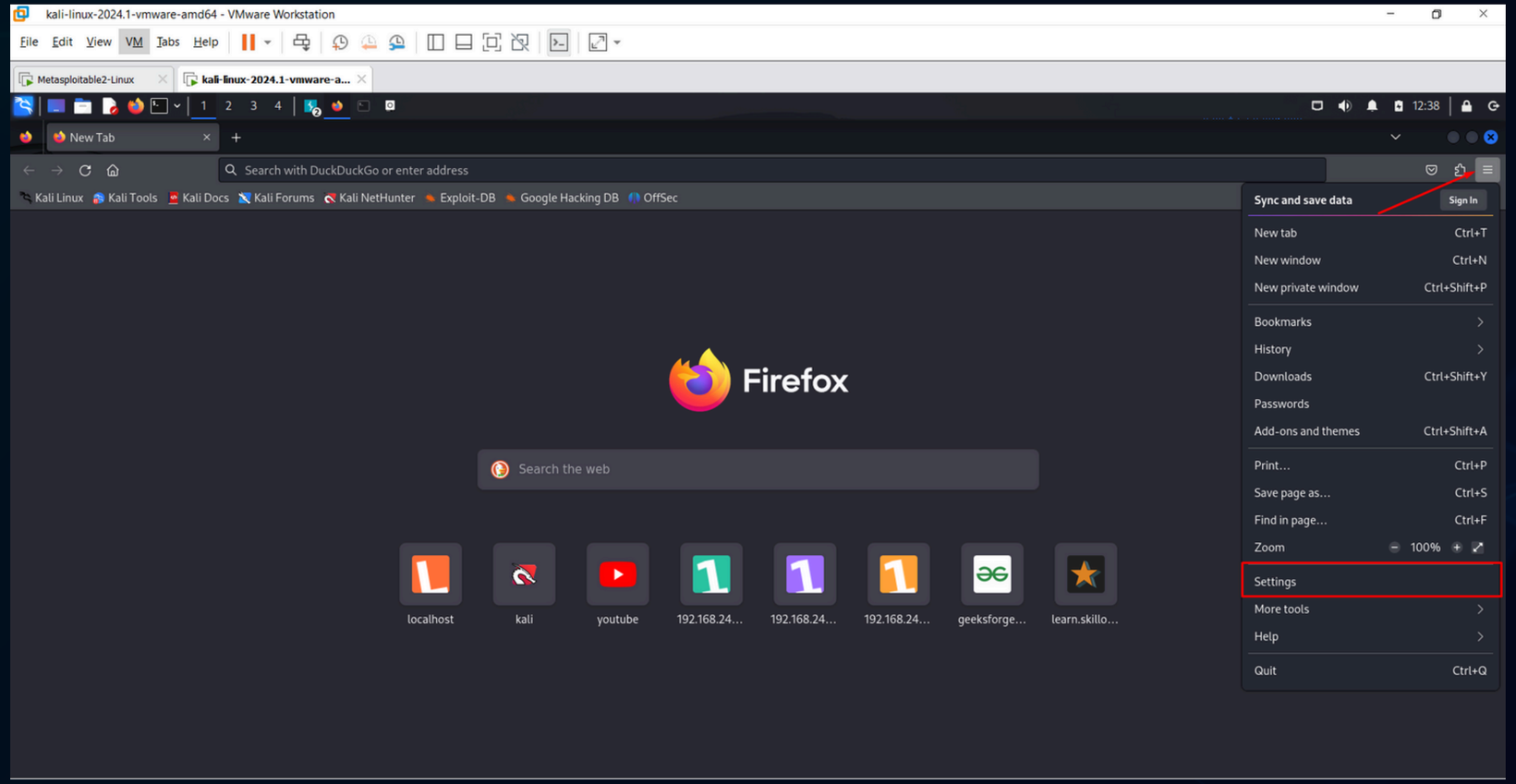
THE SUITE INCLUDES FEATURES LIKE A WEB VULNERABILITY SCANNER, AN INTERCEPTING PROXY, AND TOOLS FOR ANALYZING AND MANIPULATING WEB TRAFFIC.

INSTALLATION =>

TAHA BORAN KOTAN

STEP 1

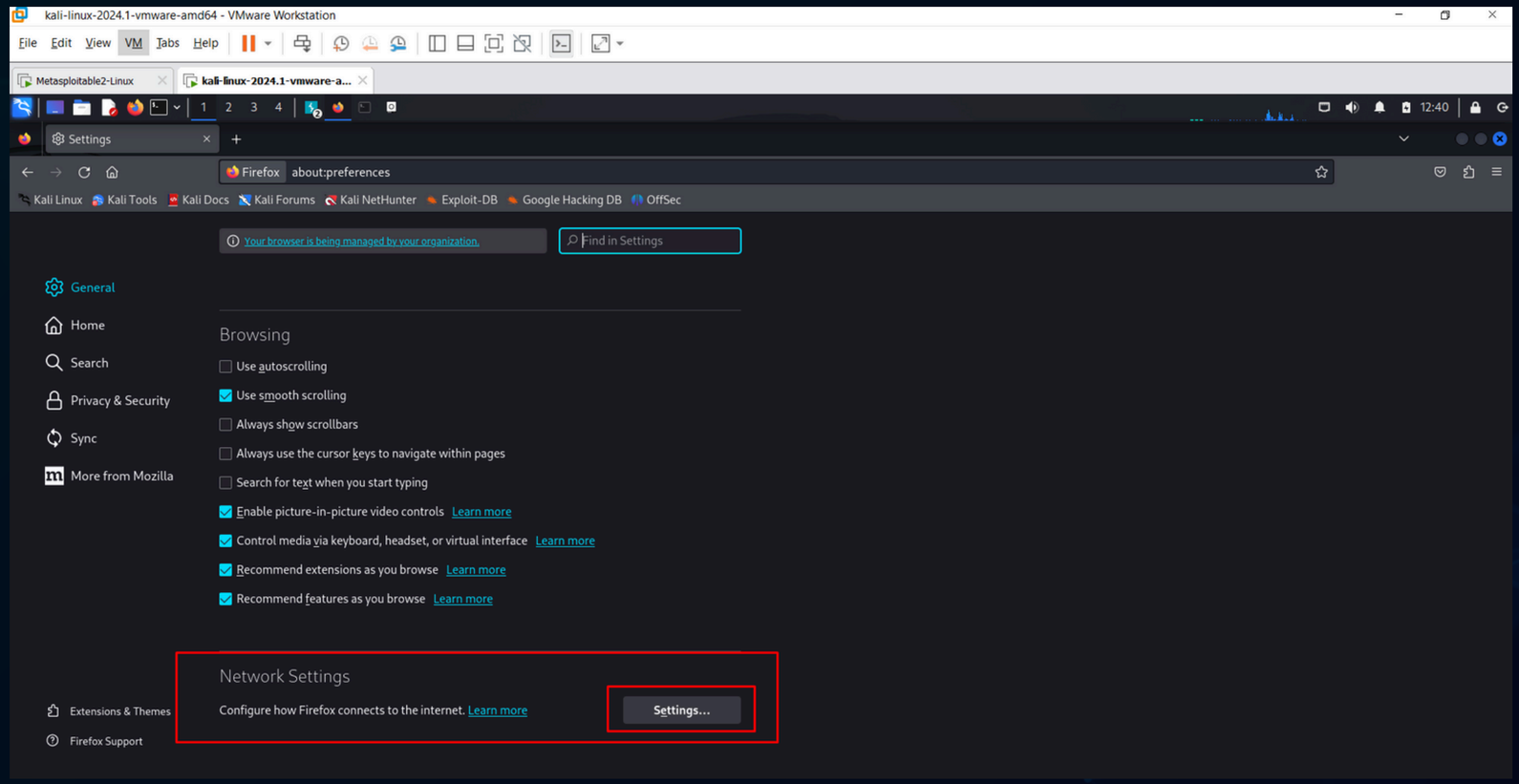
- In first step, we configure our web browser proxy for capture credentials.
- Open your Kali Linux virtual machine. Then, open your Firefox Web Browser.
- On Firefox, follow the image and open “Settings”.



TAHA BORAN KOTAN

STEP 1

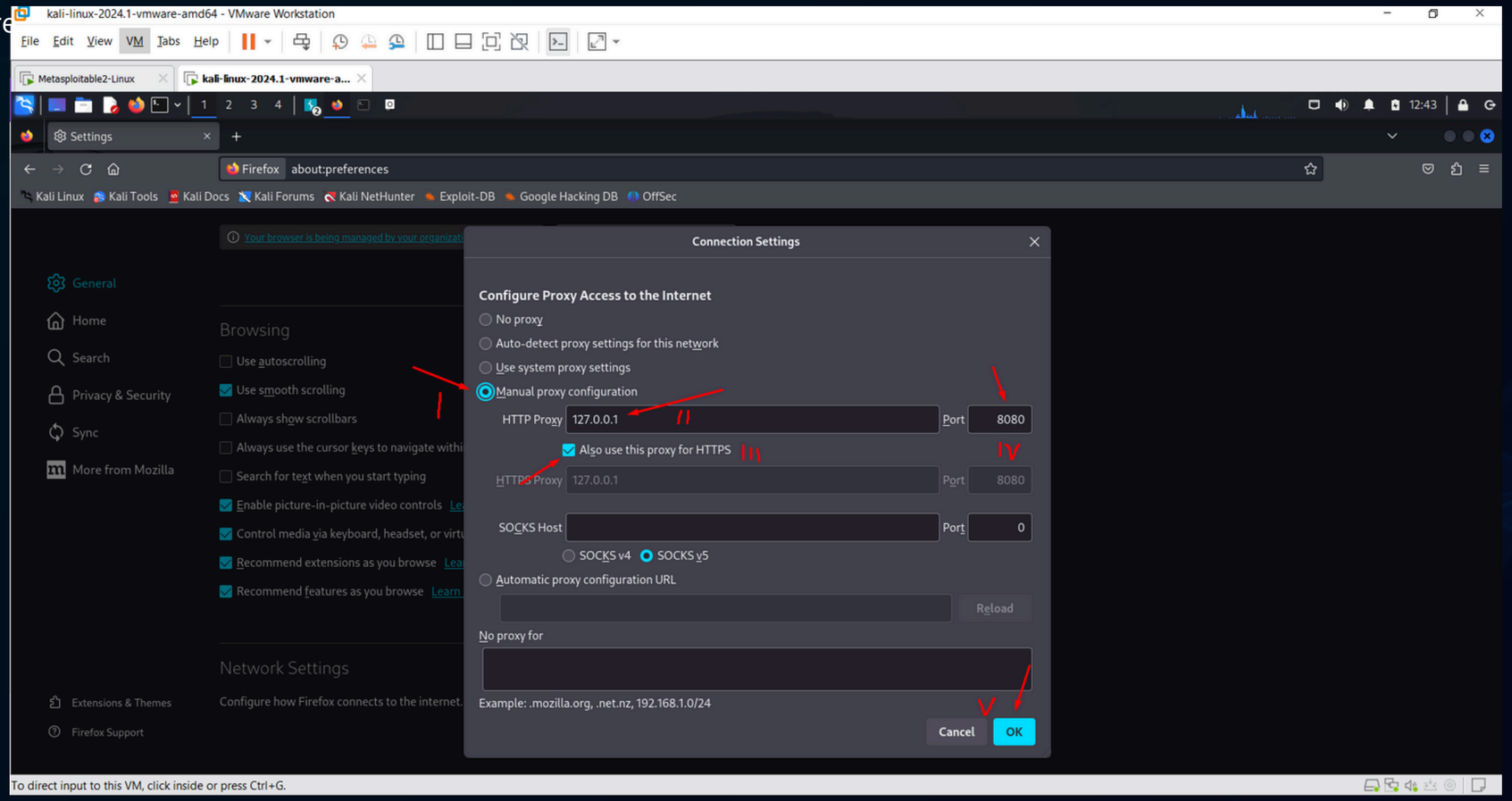
- Scroll down on this page and find “Network Settings”.
- Click “Settings”.



TAHA BORAN KOTAN

STEP 1

- Follow the steps like on the image and configure your web browser proxy settings.
- Then, close your web browser for now.



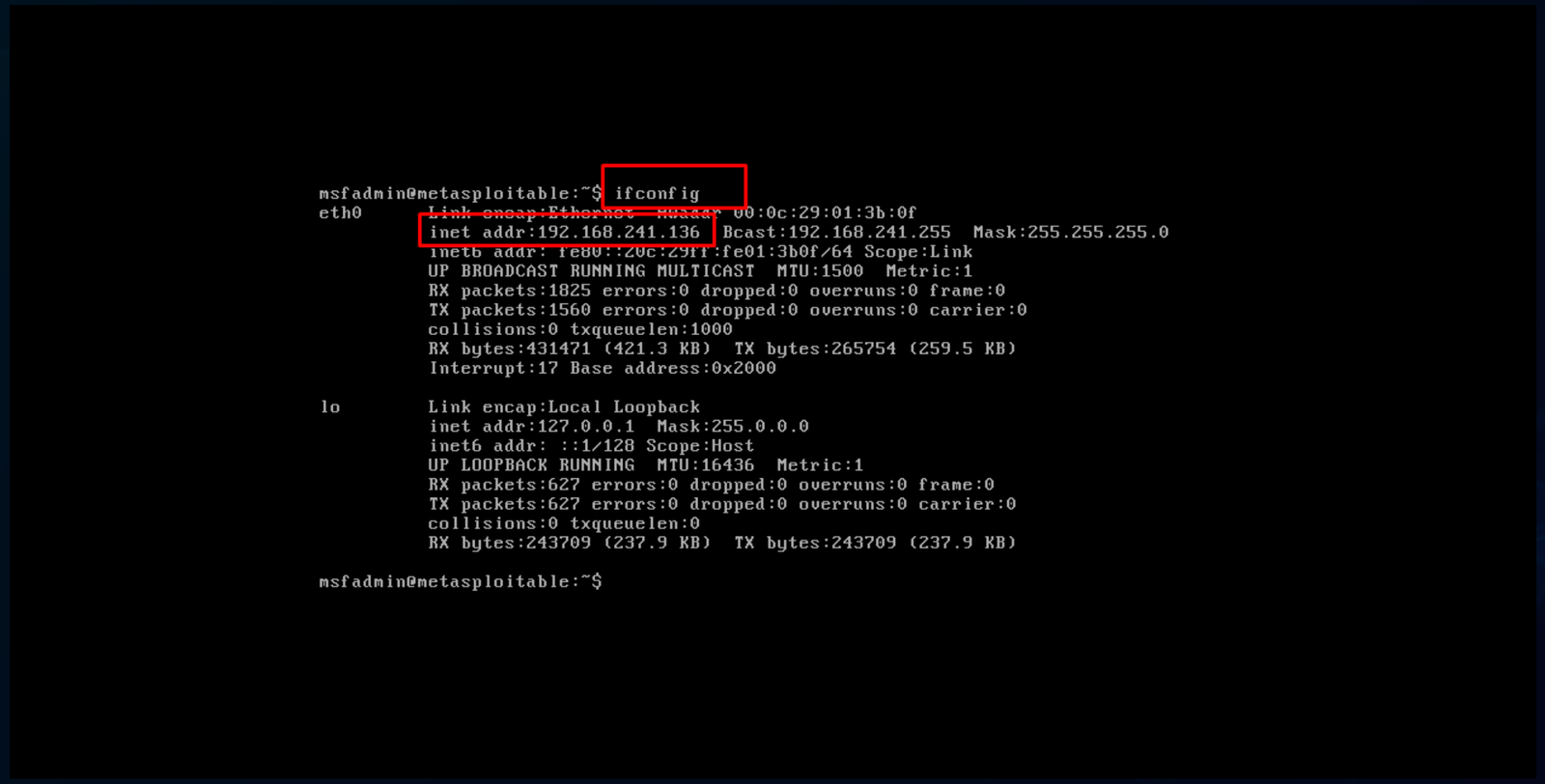
TAHA BORAN KOTAN

STEP 2

- Open your Metasploitable 2 virtual machine which we have just installed.

- Type: “ifconfig” and learn your IPv4 adress.

- We will use this IPv4 adress to reach Metasploitable 2 machine’s web server.

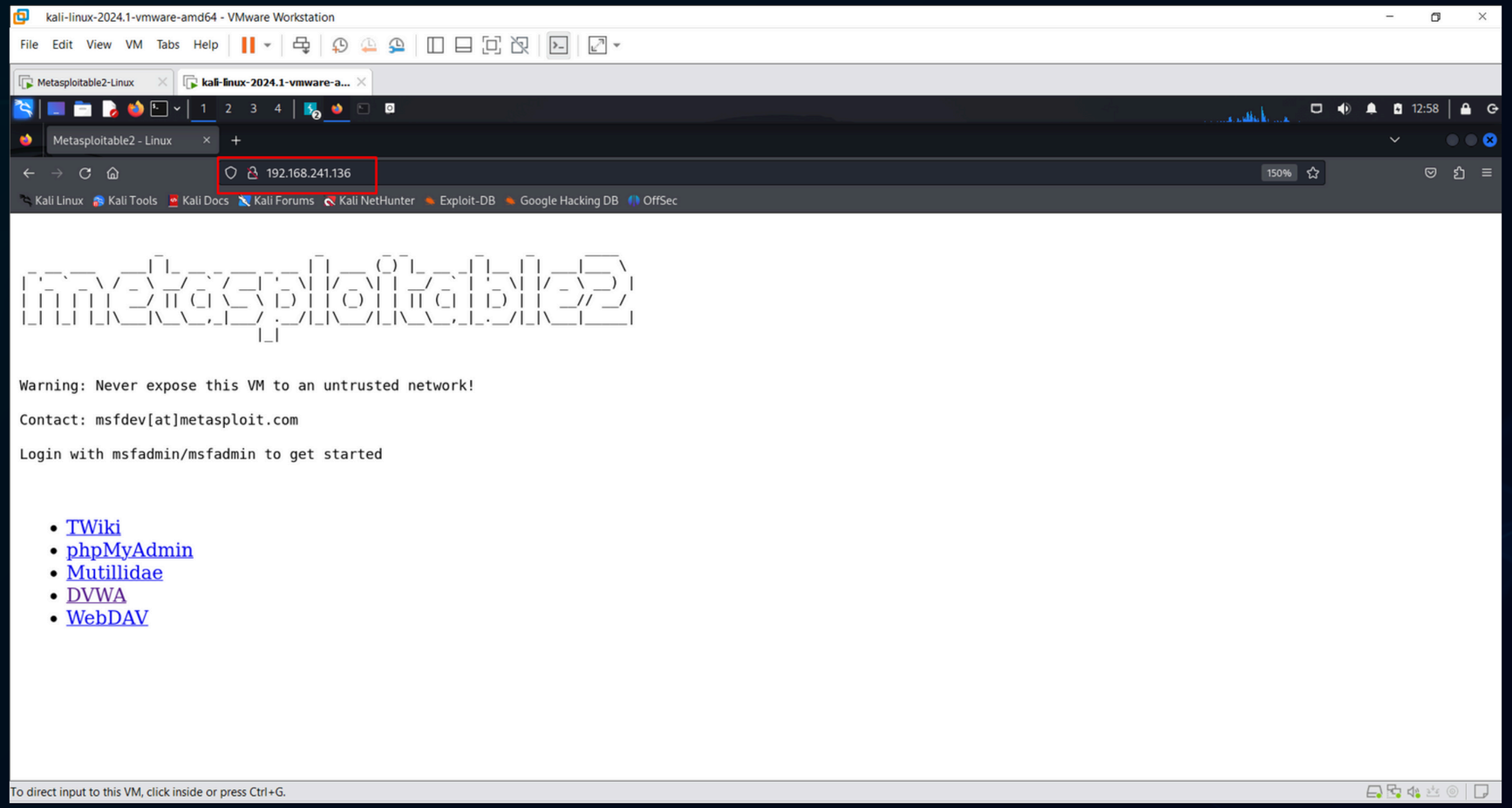


TAHA BORAN KOTAN

STEP 3

- Open your web browser and type this IPv4 adress to url part.

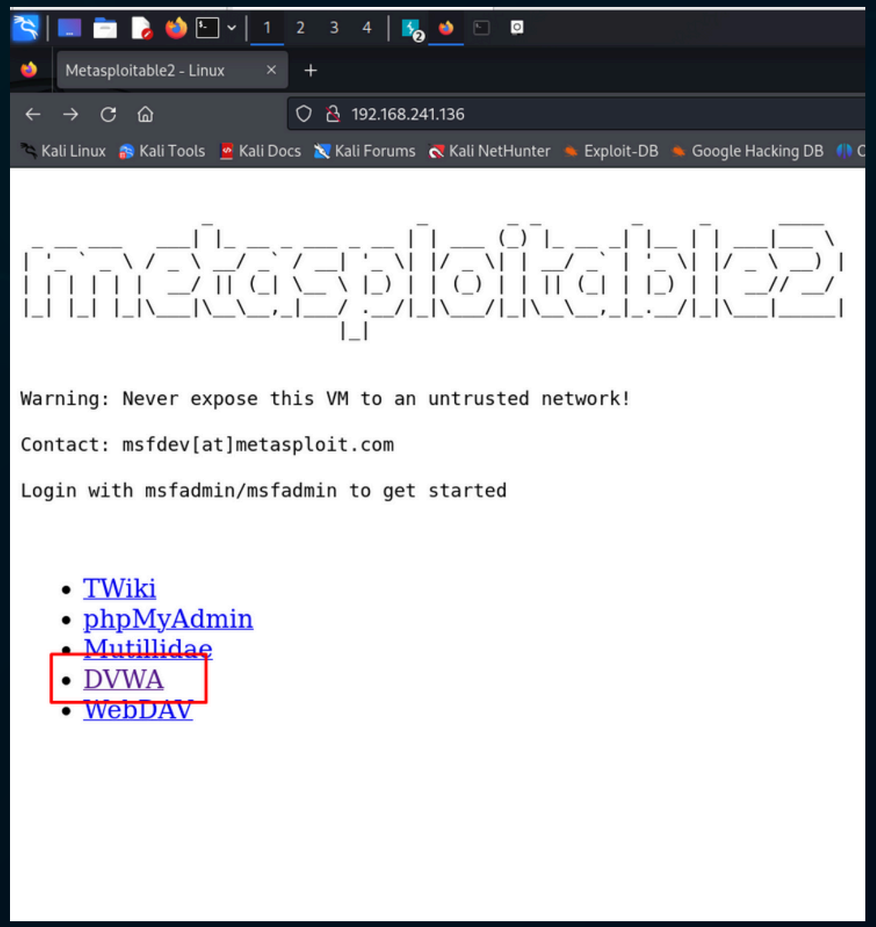
- Then type “Enter” to reach web server.



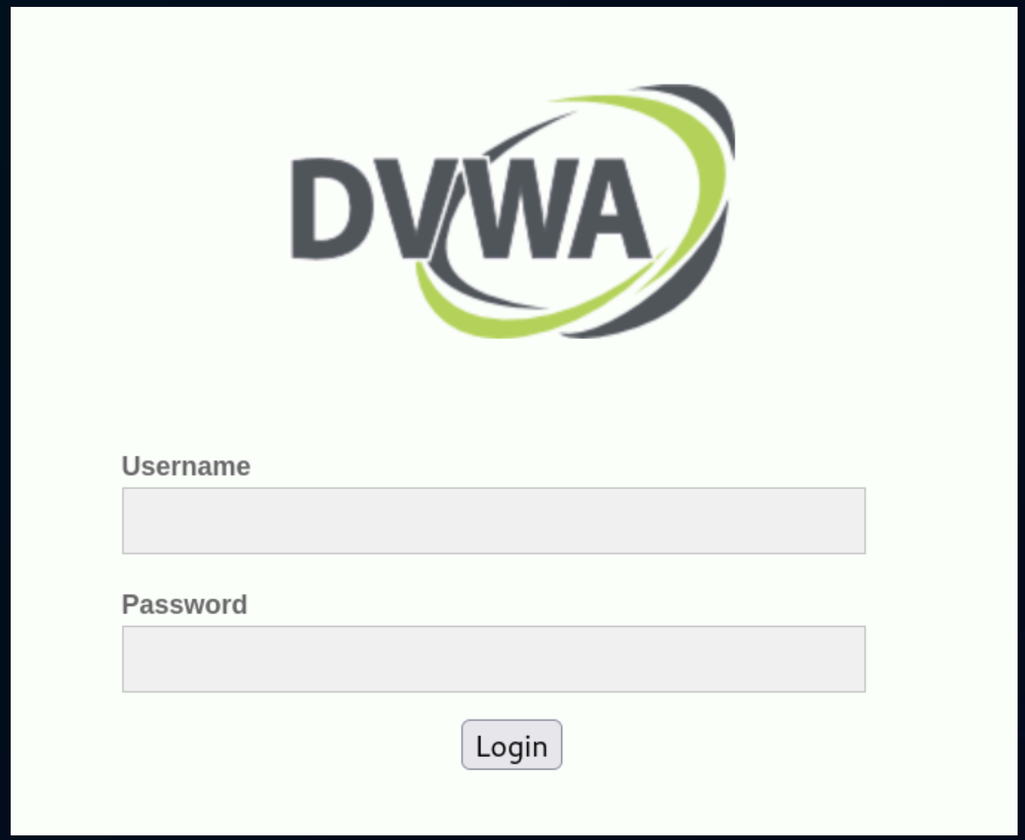
TAHA BORAN KOTAN

STEP 3

- Click “DVWA” to reach login page.

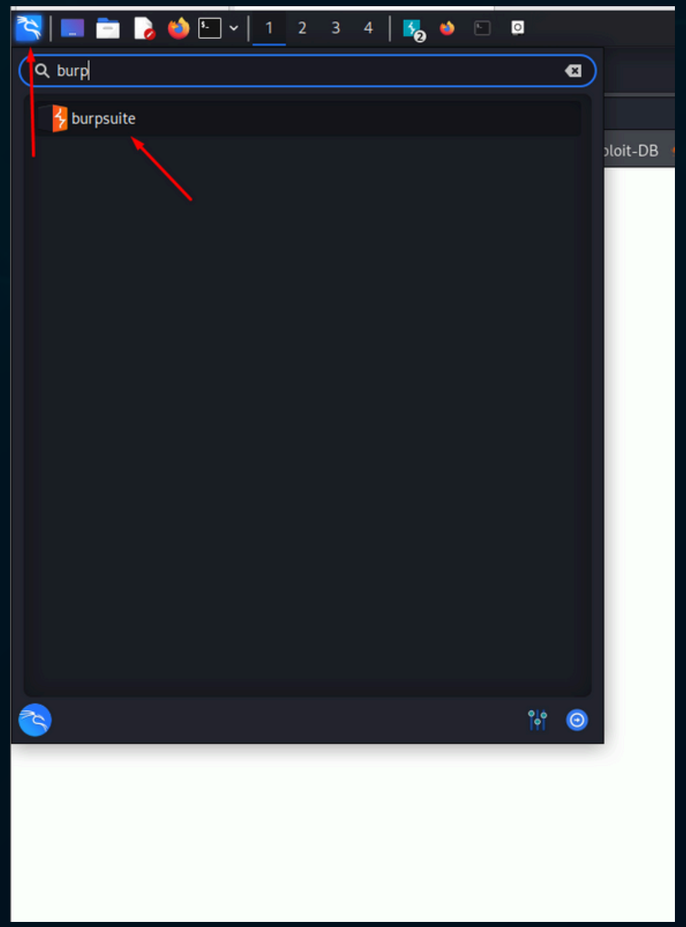


- Then the login page looks like that:

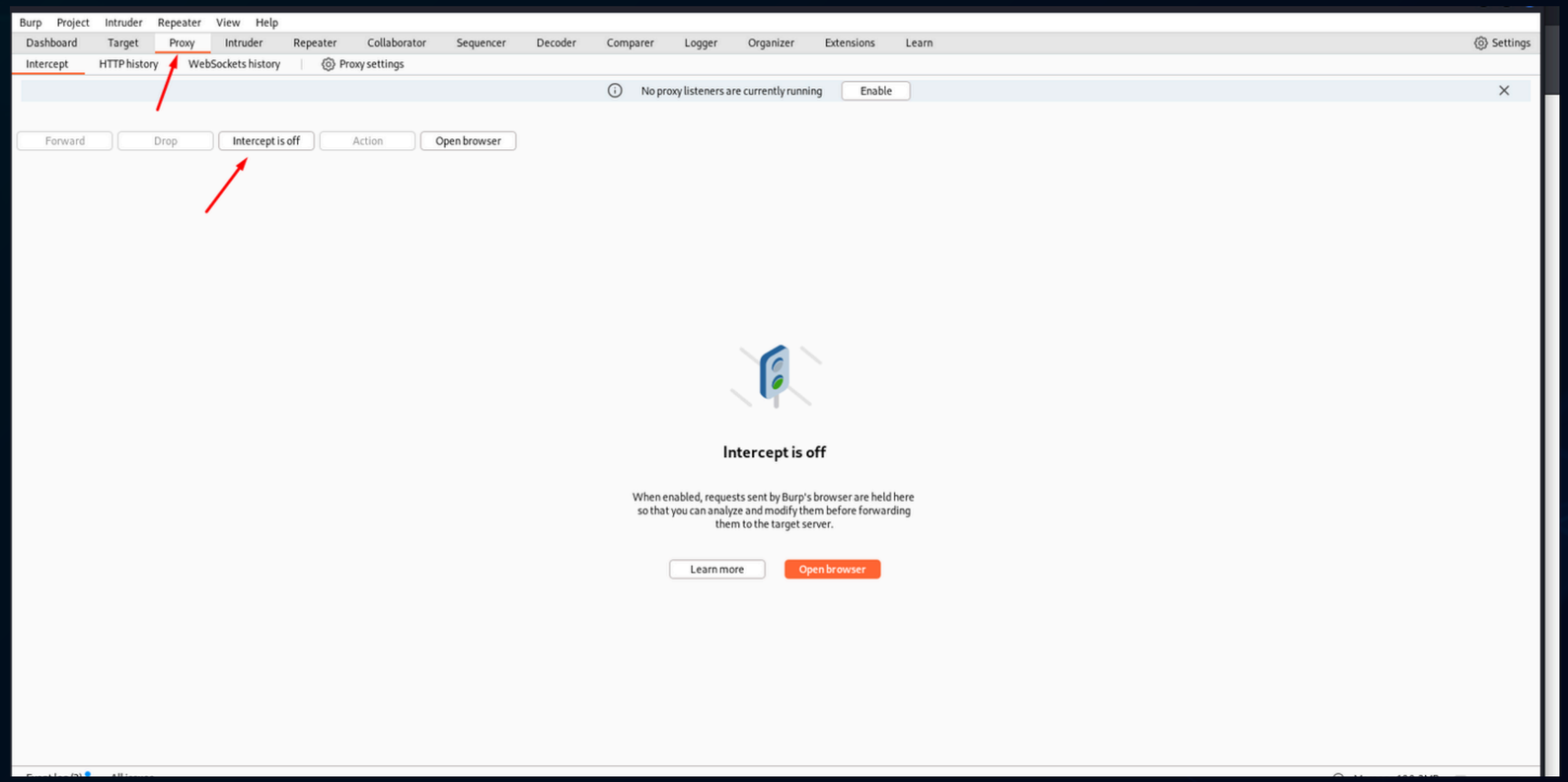


STEP 4

- Open the Burp Suite.



- Click “Proxy” then “Intercept is off” buttons.

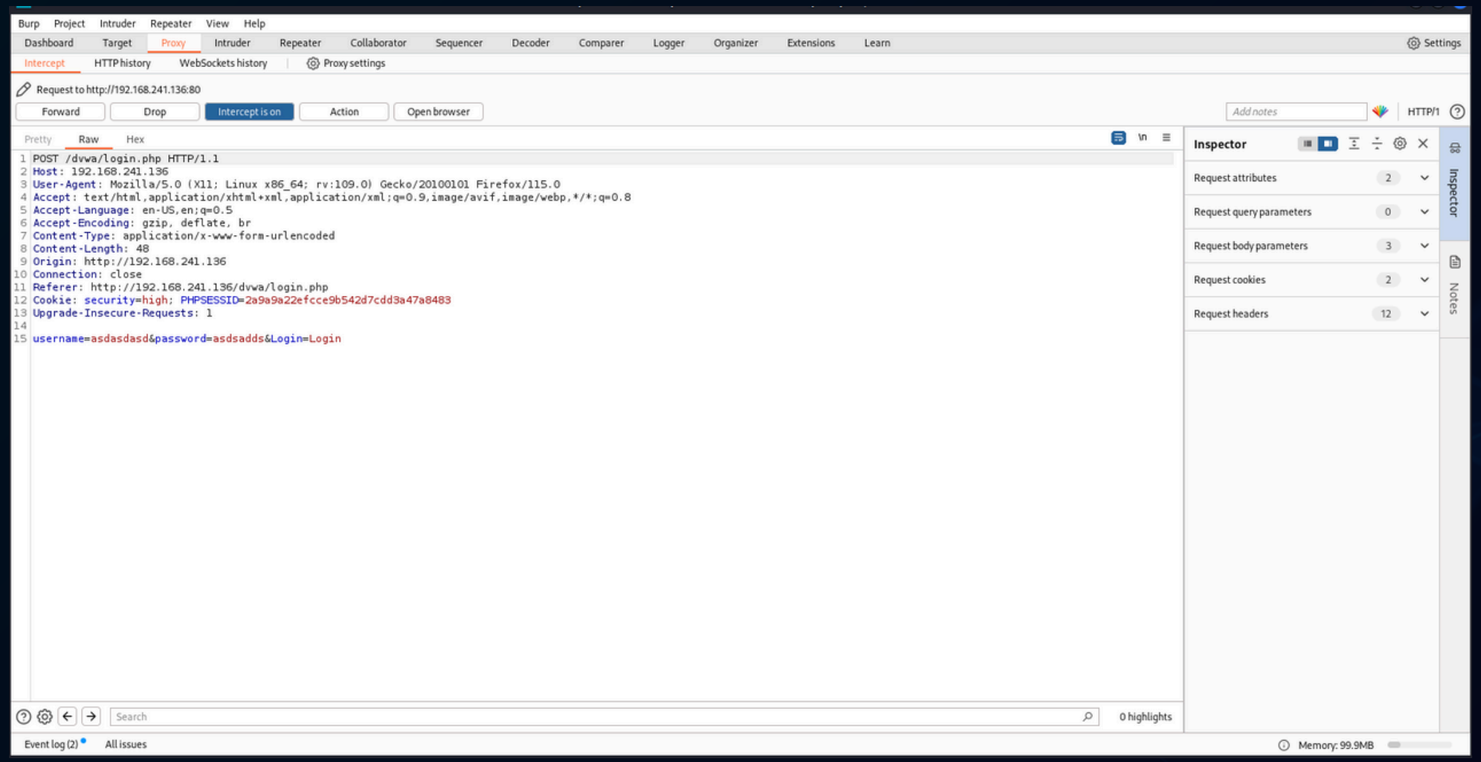


TAHA BORAN KOTAN

STEP 4

- Return to login page and type anything in username and password areas.
- Then click “Login”

- Then, Burp Suite automatically pop ups the login credentials.



BRUTE FORCE ATTACK ON METASPLOITABLE 2 =>

TAHA BORAN KOTAN

CYBER SECURITY

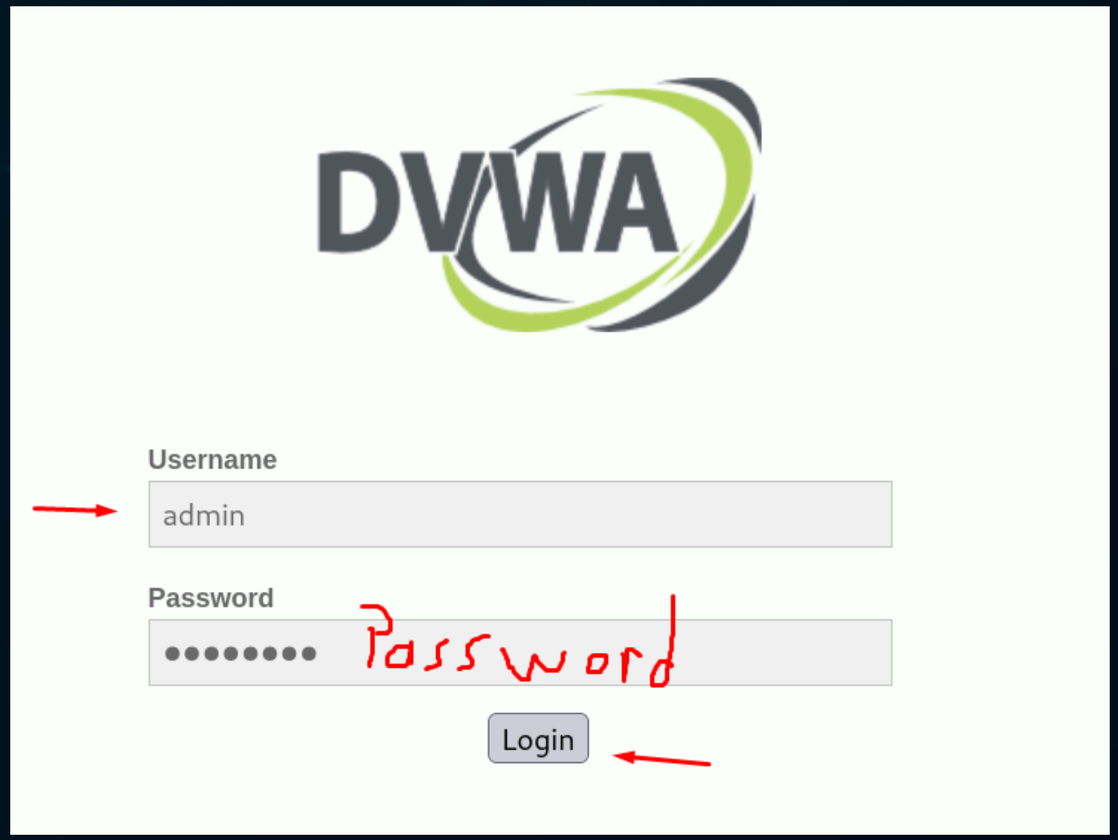
CFSS INTERNSHIP PROGRAM

TAHA BORAN KOTAN
PROJECT 4: BRUTE FORCE
ATTACK ON METASPLOITABLE 2

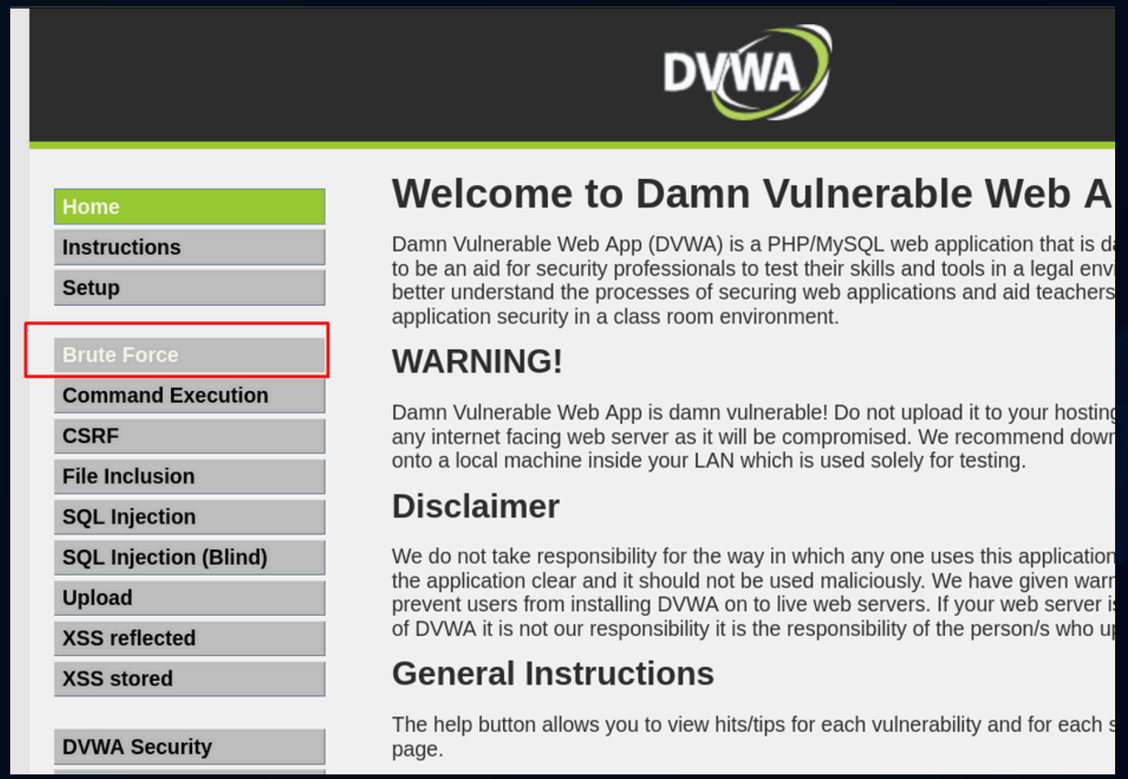
TAHA BORAN KOTAN

STEP 1

- Firstly, we should join the server and reach the brute force test area.
- Username: admin
- Password: password



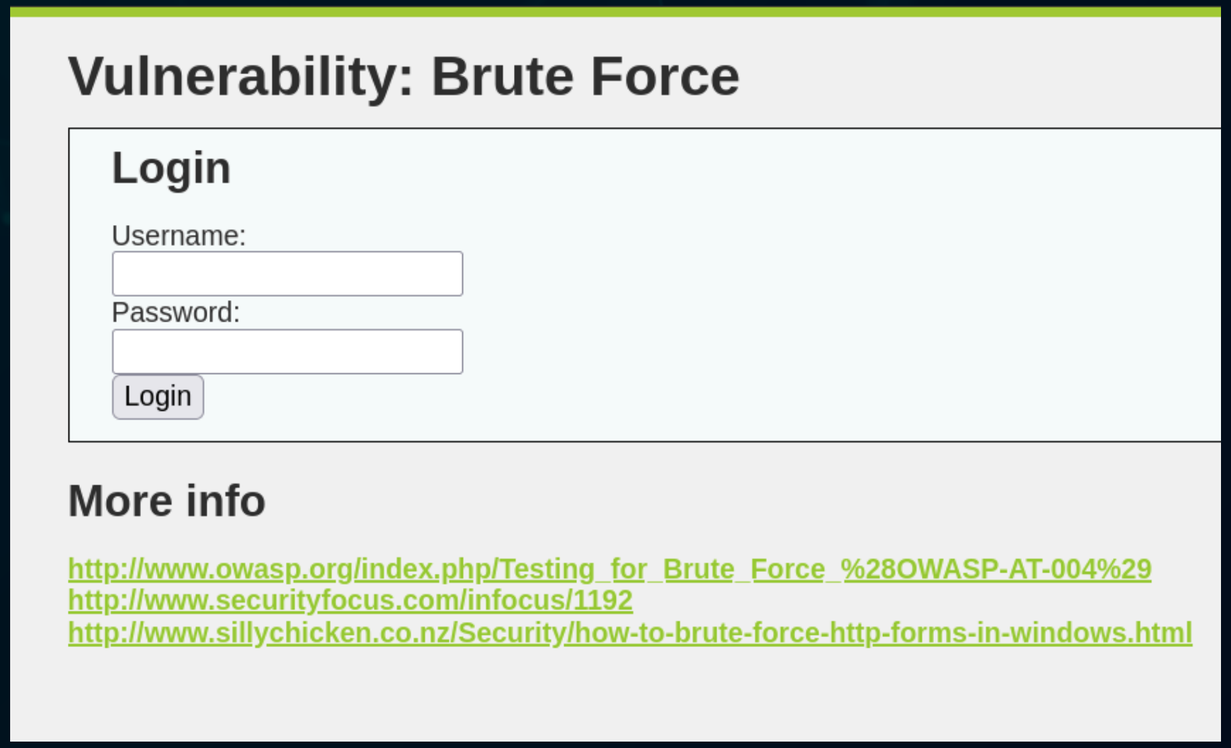
- Click “Brute Force” button.



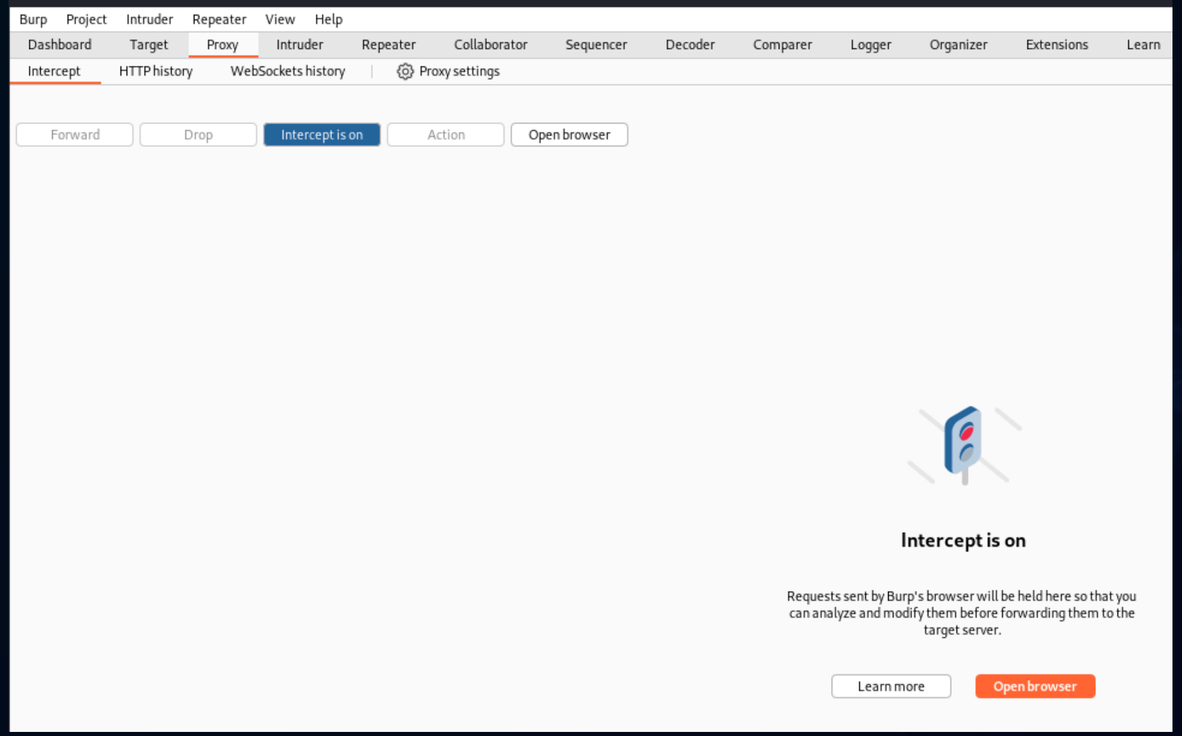
TAHA BORAN KOTAN

STEP 1

- Now, you can see another login page where we will do brute force attack.



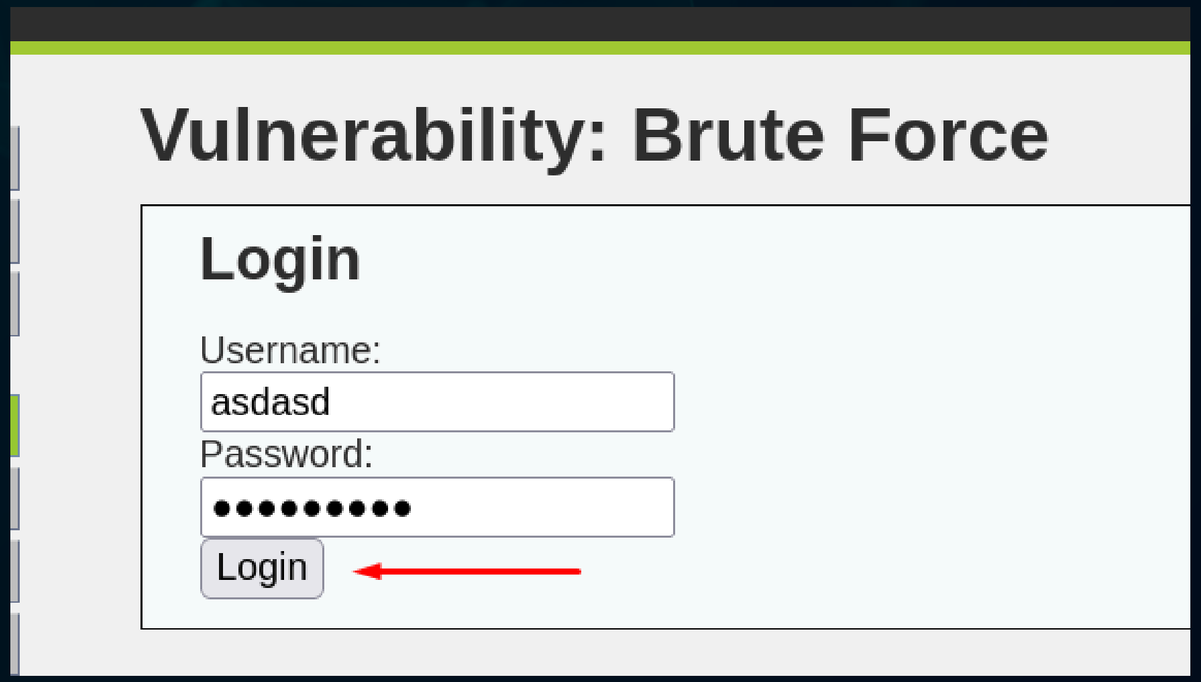
- Turn your Burp Suite and make sure the button: “Intercept is on” is on.



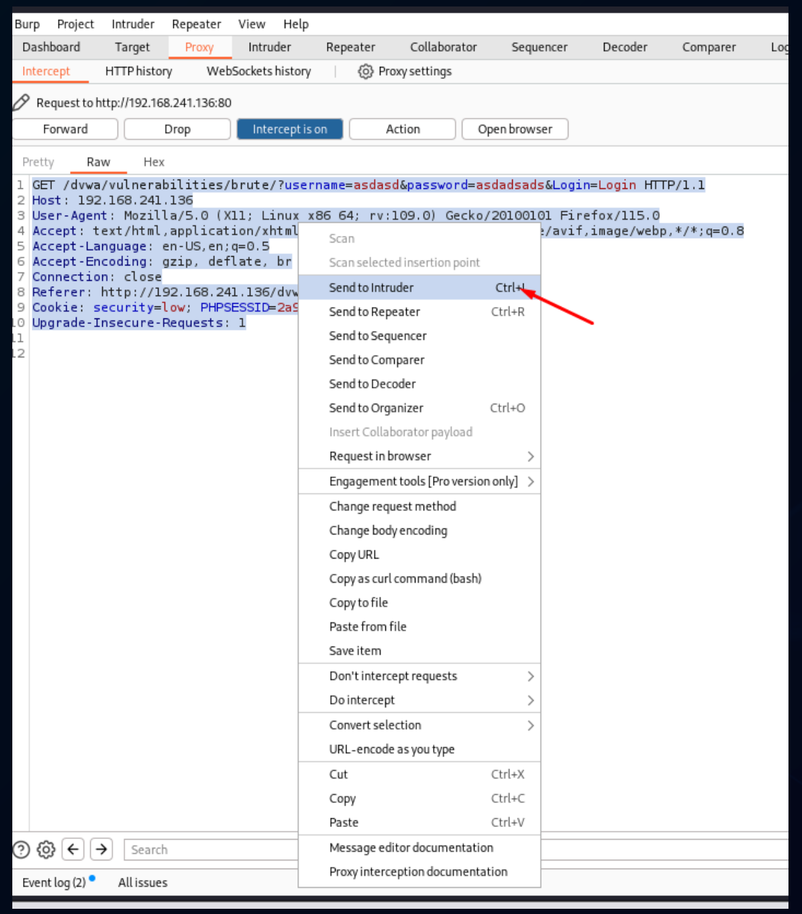
TAHA BORAN KOTAN

STEP 1

- Return to the web server and fill wrong id and password for capture credentials on burp suite, and click “Login”.



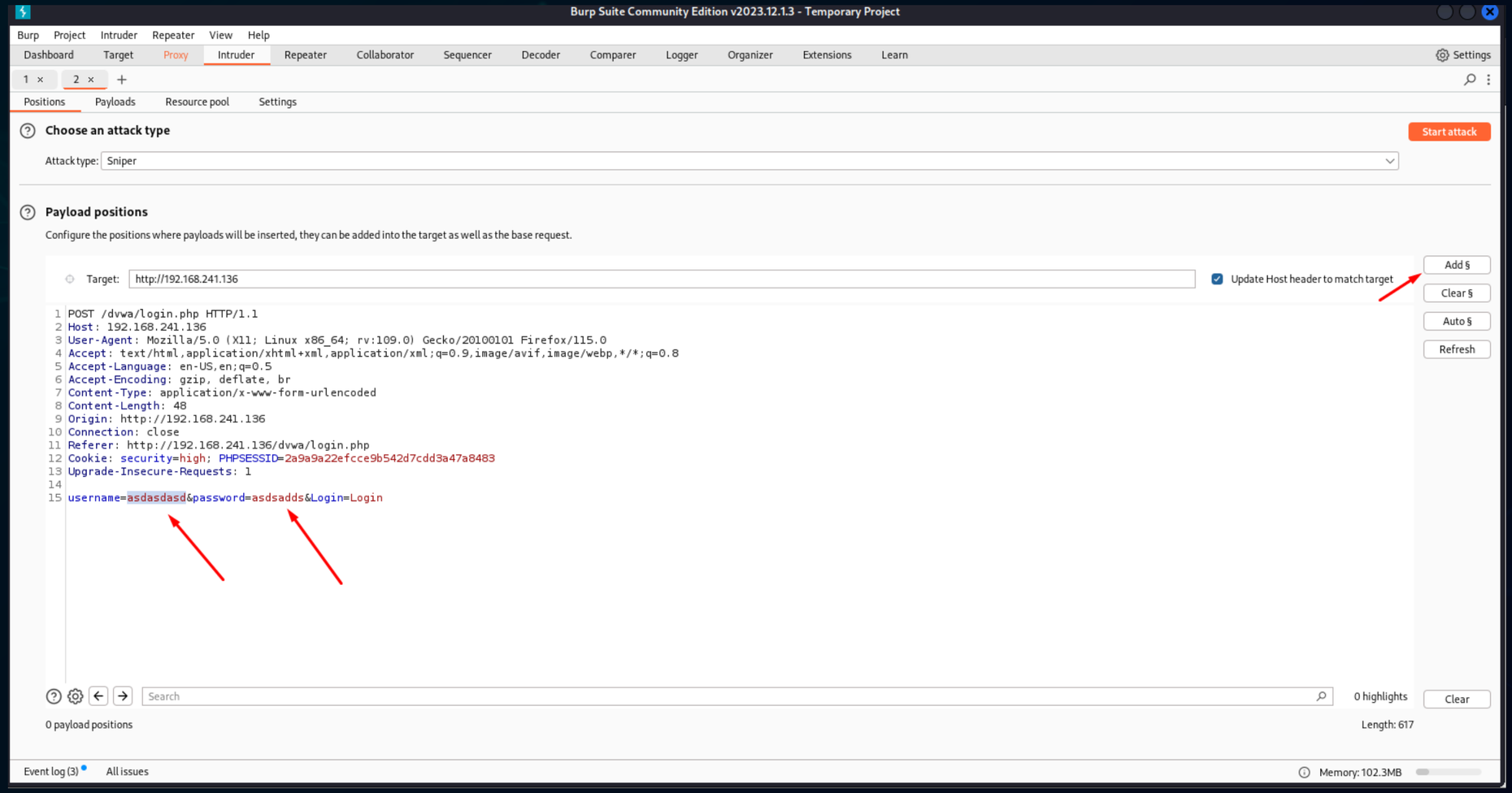
- Now, we have captured another request. We will follow the same steps which we followed on previous project.



TAHA BORAN KOTAN

STEP 2

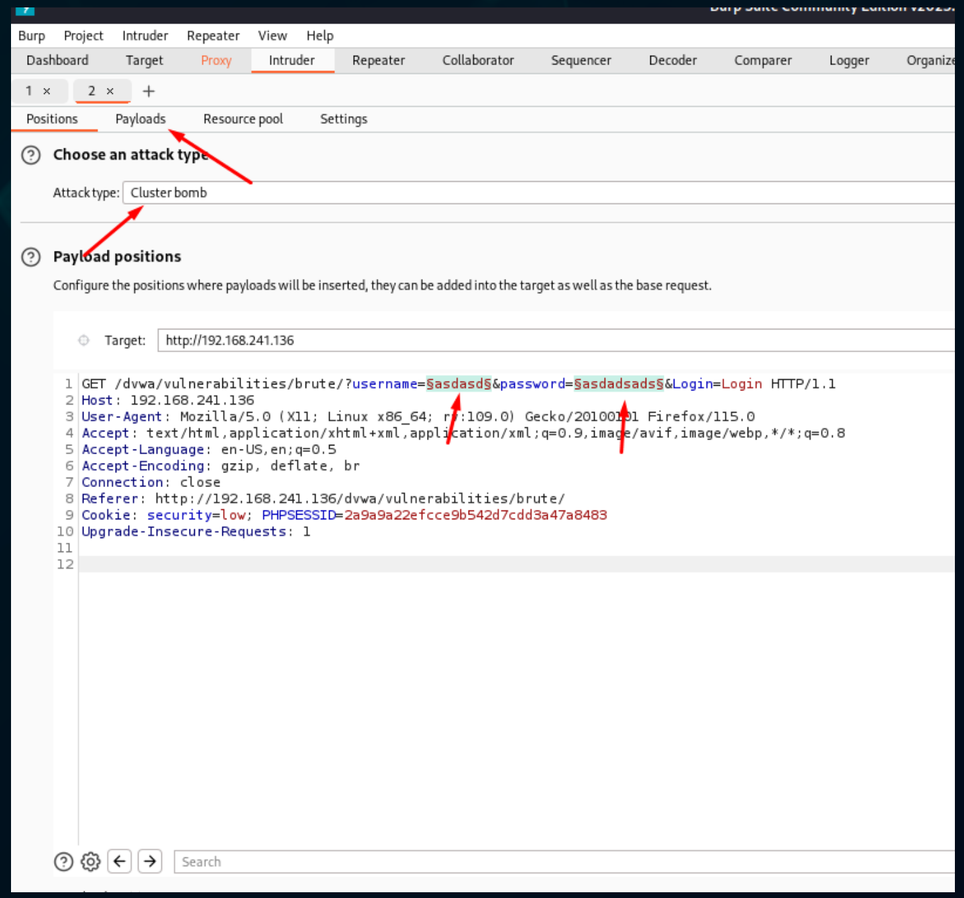
- Select username and password which you filled before seperately and click “Add” button. We add this symbol to these place because we will mark the places for attacks.



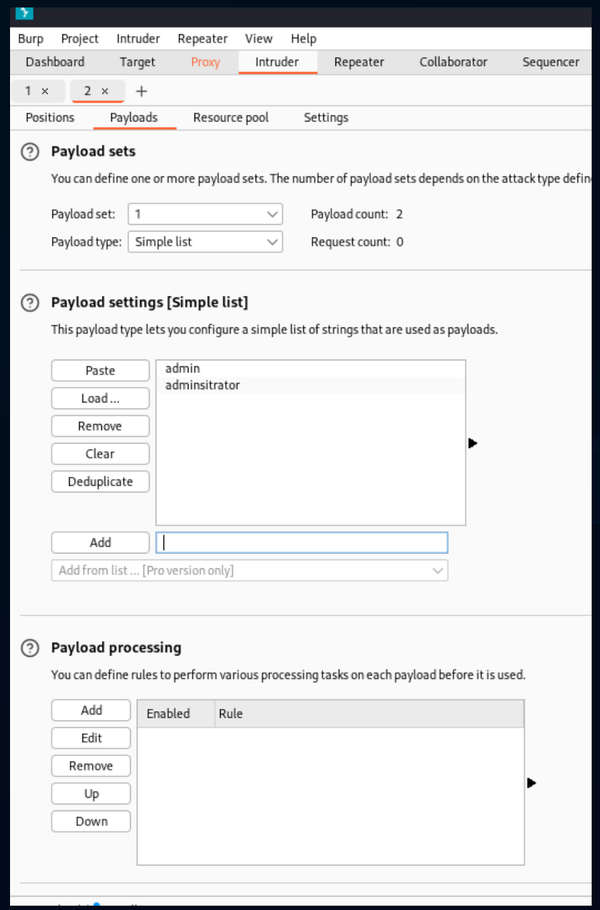
TAHA BORAN KOTAN

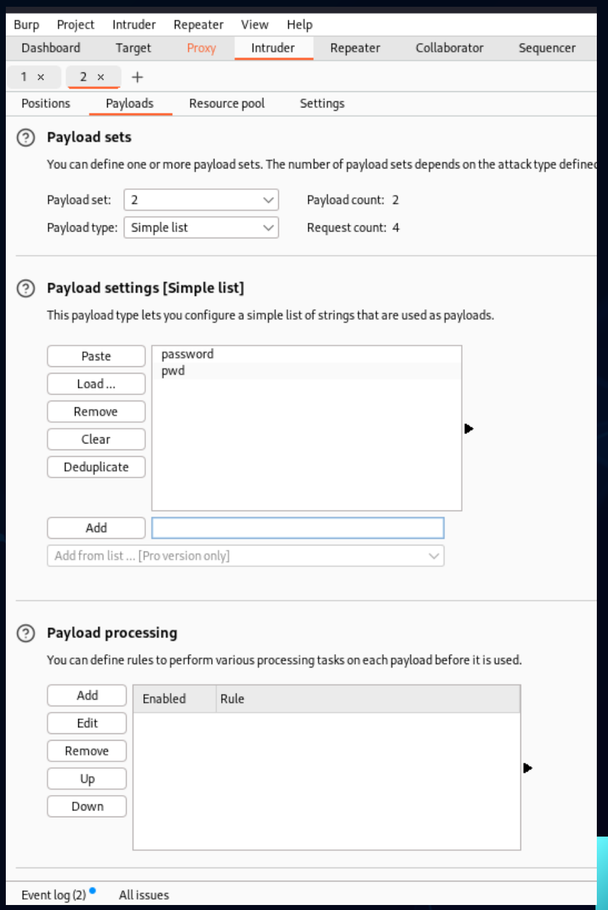
STEP 2

- Make sure you added the symbols and make attack type “Cluster Bomb”. Then click “Payloads”.



- Give most common username and passwords for cracking. In this time you can add “admin, administrator” and “password, pwd” instead of wordlists.

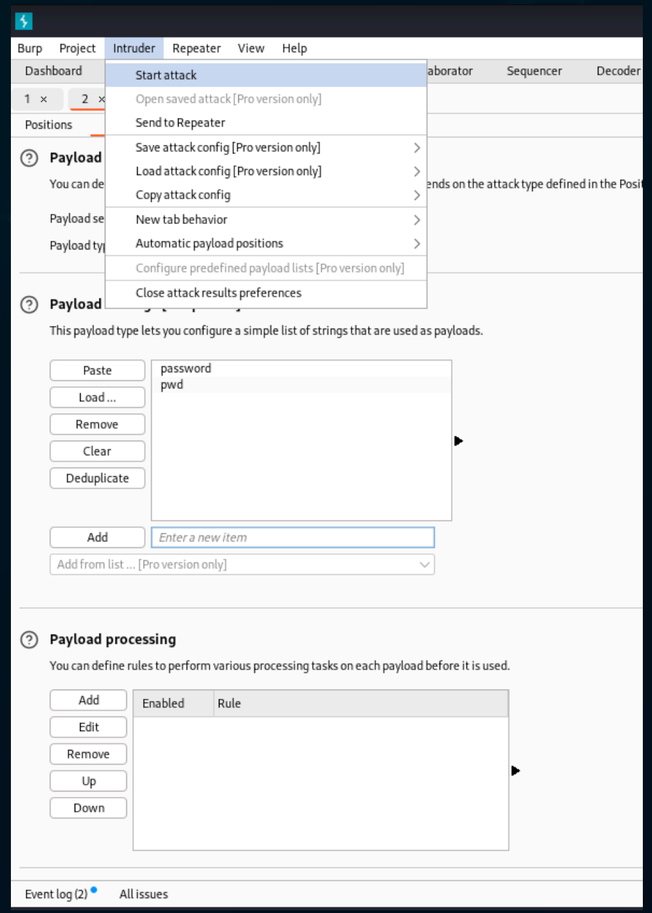




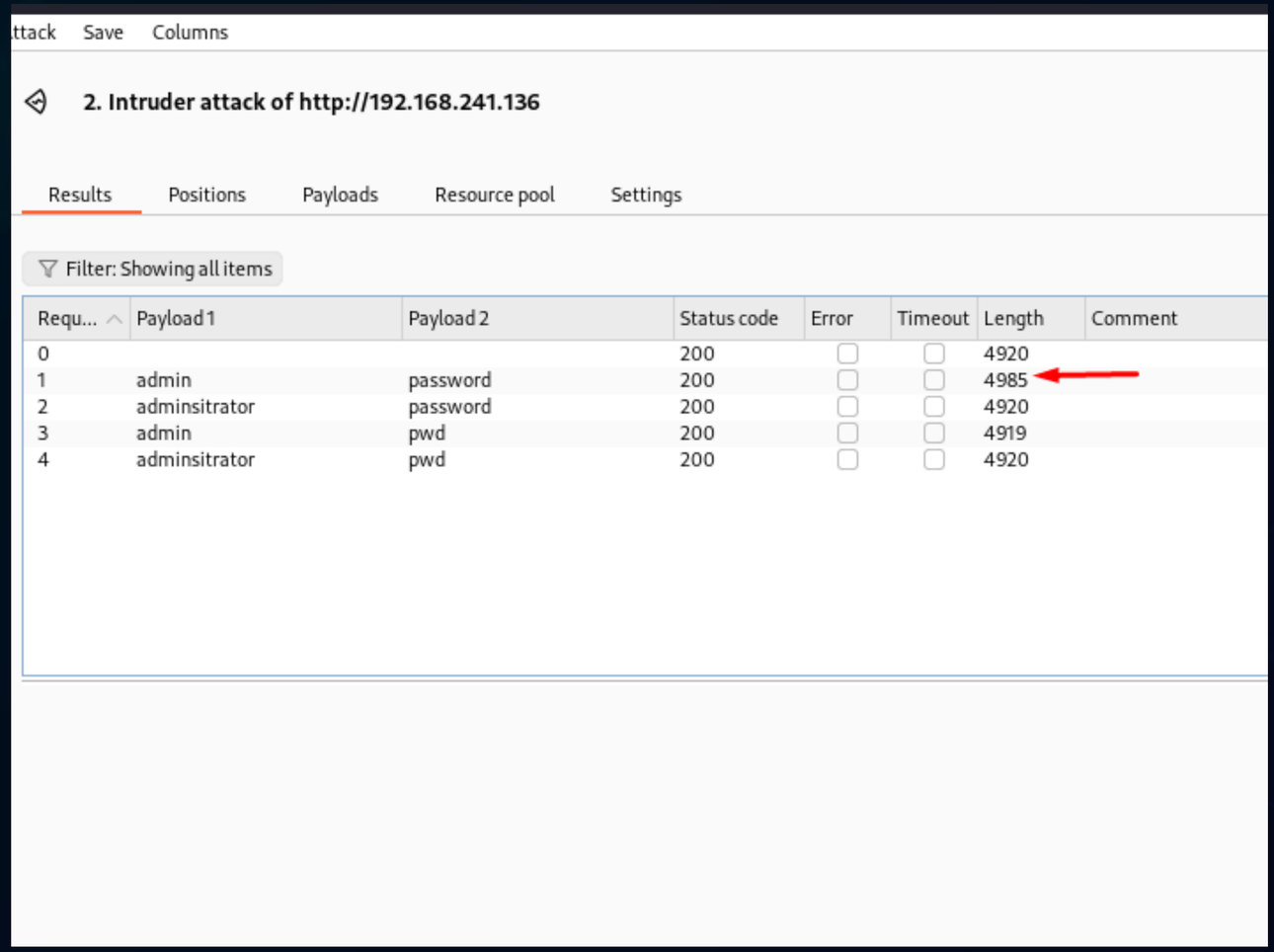
STEP 3

TAHA BORAN KOTAN

- Now, click “Intruder” and “Start Attack”.



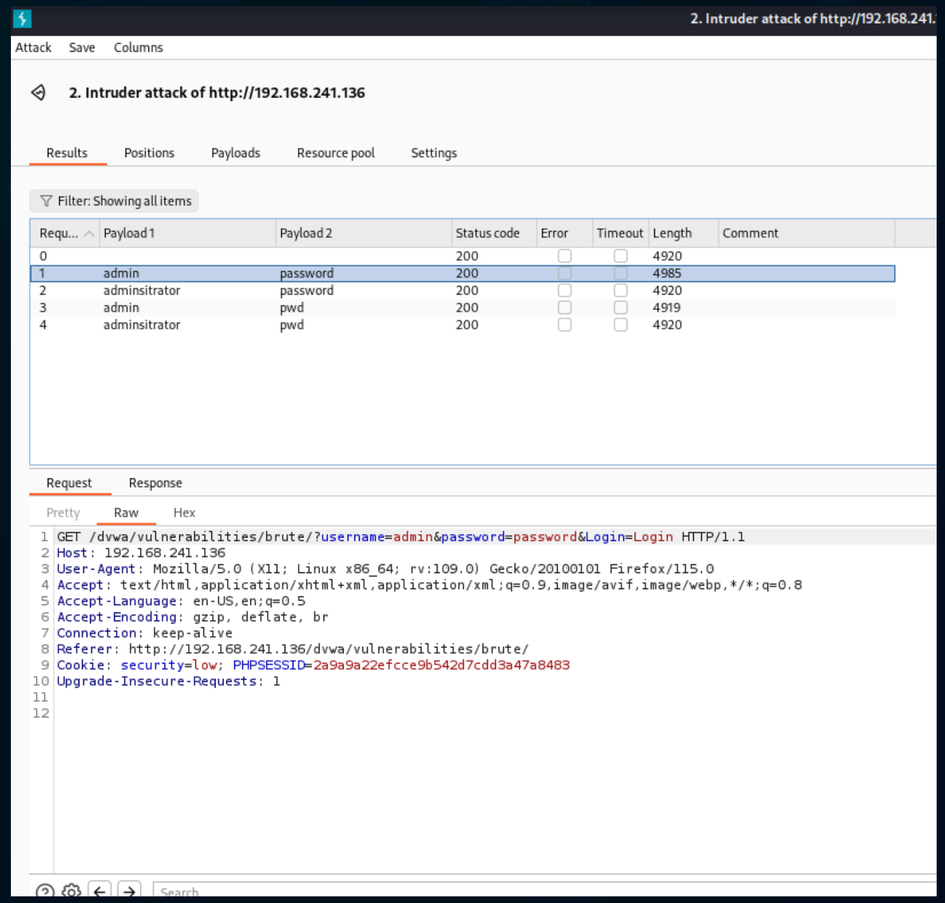
- Brute force attack has just ended and we should analyze the result. As you can see, after the request we recieved some answers and in one attempt answer length seems so different.



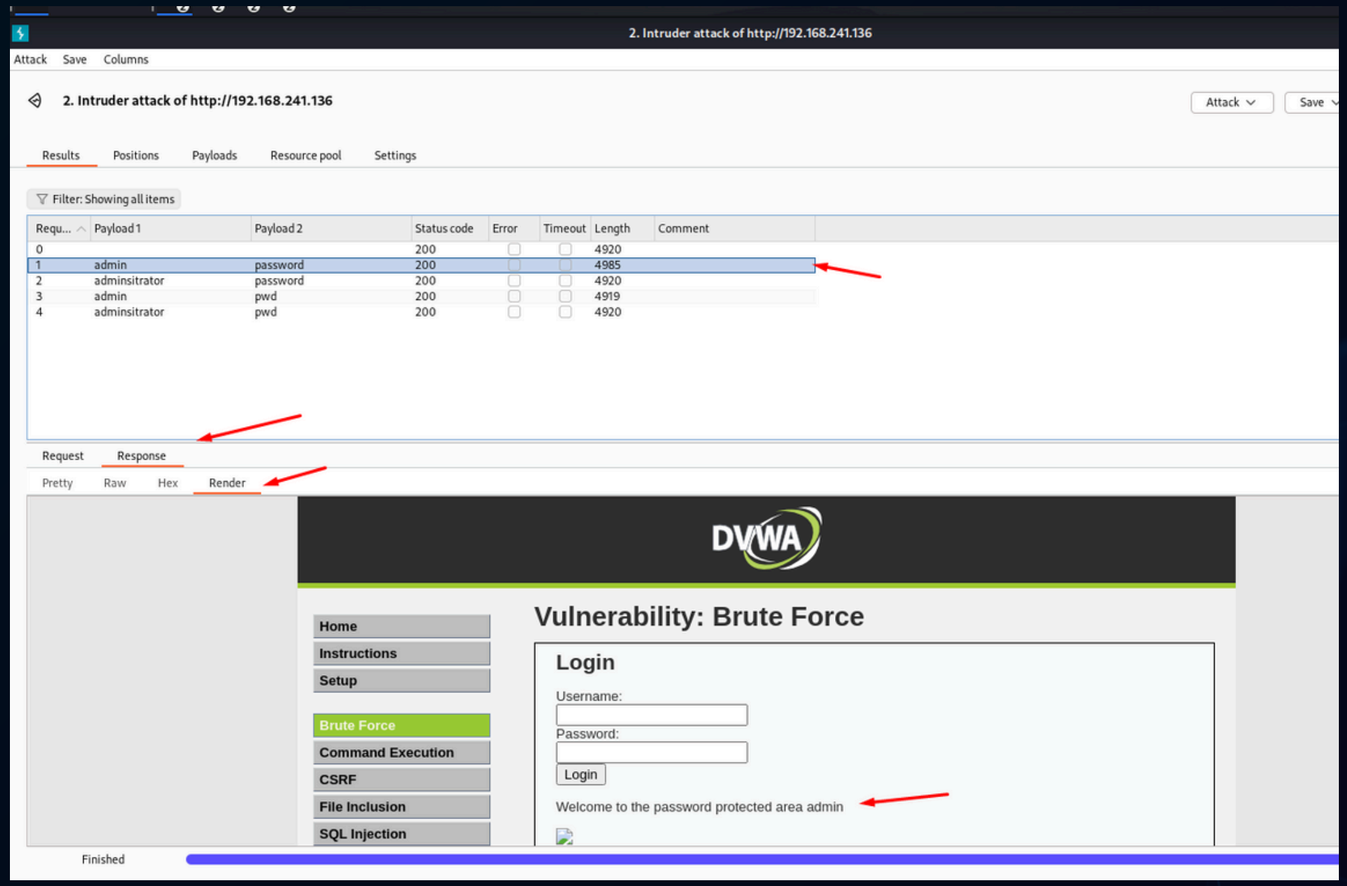
TAHA BORAN KOTAN

STEP 3

- Click on the result which has different length.



- Click “Response” and “Render”. As you can see on the snapshot, in this attempt server allowed the login credentials.



TAHA BORAN KOTAN

CONTACT ME

+90-0535-085-26-33

https://www.linkedin.com/in/taha-boran-kotan/

borantaha@gmail.com

ISTANBUL, TURKEY

THANK YOU

T A H A B O R A N K O T A N