



# TAHA BORAN KOTAN



# CYBER SECURITY

C F S S   I N T E R N S H I P   P R O G R A M

T A H A   B O R A N   K O T A N  
P R O J E C T 1 : M E T A S P L O I T A B L E 2  
I N S T A L L A T I O N   P R O C E S S



# 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.

02

INSTALLATION =>



# 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

A screenshot of a Google search results page. The search bar at the top contains the query "metasploitable 2 download". Below the search bar, there are several search filters: Tümü (selected), Videolar, Görüşler, Haberler, Web, Kitaplar, Uçuş Arama, Daha fazla, and Araçlar. The main content area displays four search results:

- SourceForge** <https://sourceforge.net/files> · Bu sayfanın çevirisini yap ...  
**Metasploitable - Browse /Metasploitable2 at SourceForge.net**  
13 Haz 2012 — Download Latest Version metasploitable-linux-2.0.0.zip (865.1 MB) ... 11,632.  
This is **Metasploitable2** (Linux) Metasploitable is an intentionally ...
- Rapid7** <https://docs.rapid7.com/m...> · Bu sayfanın çevirisini yap ...  
**Metasploitable 2**  
Downloading and Setting Up **Metasploitable 2** ... The easiest way to get a target machine is to use **Metasploitable 2**, which is an intentionally vulnerable Ubuntu ...
- VulnHub** <https://www.vulnhub.com/m...> · Bu sayfanın çevirisini yap ...  
**Metasploitable: 2**  
**Metasploitable: 2**, made by Metasploit. Download & walkthrough links are available.
- SourceForge** <https://sourceforge.net/m...> · Bu sayfanın çevirisini yap ...  
**Metasploitable2 download**  
8 Nis 2023 — Download **Metasploitable2** for free. None.

A red arrow points from the text "Write 'metasploitable 2 download'" in the list above to the first search result on the page.



## 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

The screenshot shows the SourceForge website for the Metasploitable project. The top navigation bar includes links for Open Source Software, Business Software, and Resources. Below the navigation is a breadcrumb trail: Home / Browse Open Source / Security / Metasploitable / Files. The main content area features a logo for Metasploitable and a brief description: "Metasploitable is an intentionally vulnerable Linux virtual machine. Brought to you by: rapid7User". There are tabs for Summary, Files (which is selected), Reviews, and Support. A prominent green button labeled "Download Latest Version" with the file name "metasploitable-linux-2.0.0.zip (865.1 MB)" is visible. A red arrow points to this button. Below the button is a table listing files: "metasploitable-linux-2.0.0.zip" (modified 2019-08-19, size 865.1 MB, downloads 11,503), "README.txt" (modified 2012-06-13, size 569 Bytes, downloads 129). The table footer shows "Totals: 2 Items" and "865.1 MB" for downloads. Below the table, text states: "This is Metasploitable2 (Linux)", "Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.", "The default login and password is msfadmin:msfadmin.", and "Never expose this VM to an untrusted network (use NAT or Host-only mode if you have any questions what that means.)." At the bottom, it says "To contact the developers, please send email to msfdev@metasploit.com".



# STEP 3

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



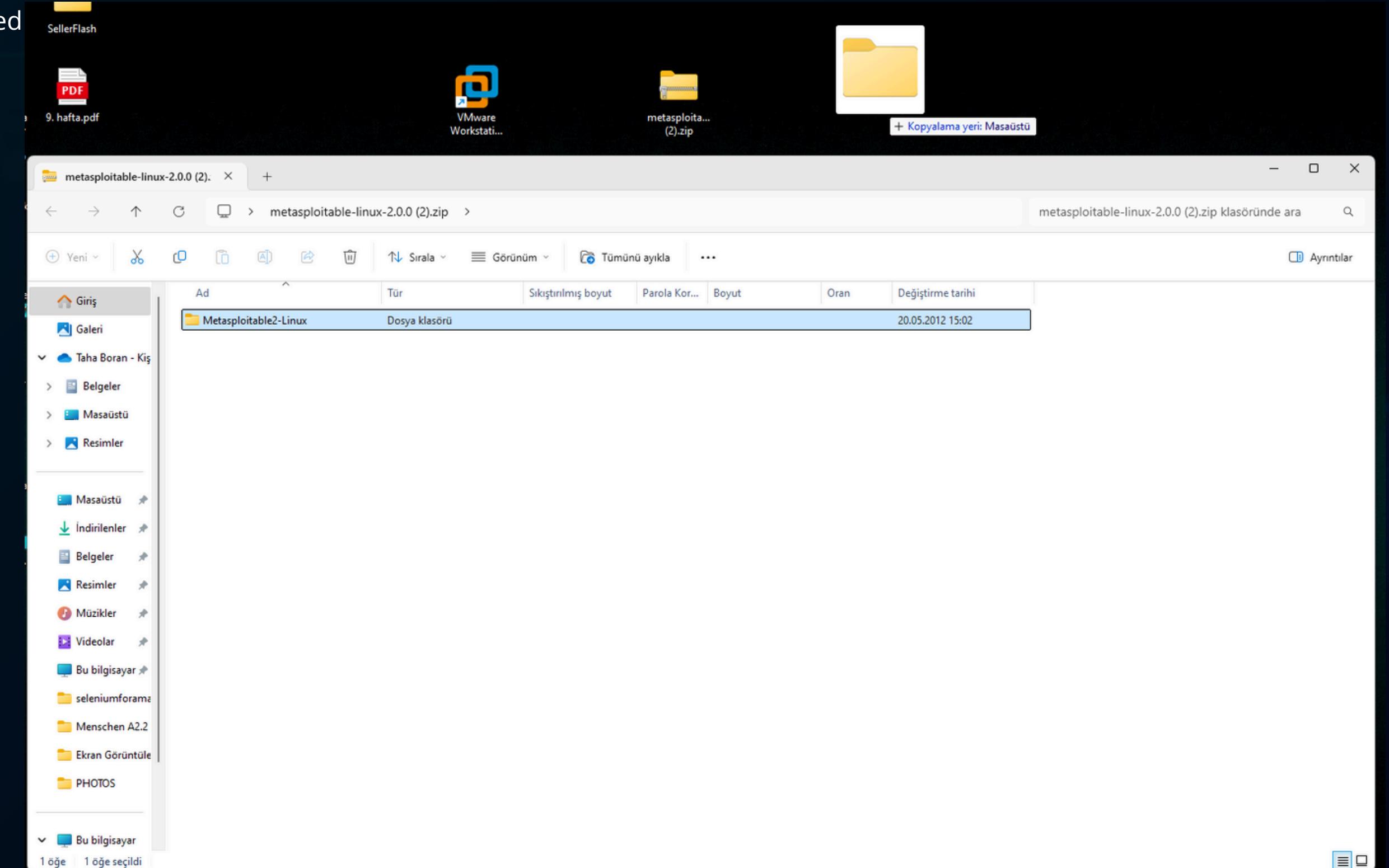
- For unzip this folder, firstly we should click and open the zip folder, then we should drag this file to desktop or where we want.



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



- After unzipping process, Open the folder.





## 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.

The screenshot shows the VMware Workstation interface. On the left, a file explorer window displays several files related to the Metasploitable2-Linux VM, including "Metasploitable.vmx" which is highlighted with a red box and has a red arrow pointing to it. The main window shows the "Metasploitable2-Linux" configuration screen with details about the virtual machine's hardware and description.

**VMware Workstation File Explorer:**

Ad	Durum	Değiştirme tarihi	Tür	Boyut
Metasploitable.vmx.lck		24.07.2024 00:31	Dosya klasörü	
Metasploitable.nvram		24.07.2024 00:22	VMware Virtual Machine nonvolatile RAM	9 KB
Metasploitable.vmdk		24.07.2024 00:23	VMware virtual disk file	1.880.512 KB
Metasploitable.vmsd		24.07.2024 00:23	VMware snapshot metadata	0 KB
<b>Metasploitable.vmx</b>		24.07.2024 00:23	VMware virtual machine configuration	3 KB
Metasploitable.vmxsf		24.07.2024 00:23	VMware Team Member	1 KB

**Metasploitable2-Linux - VMware Workstation Configuration:**

- Power on this virtual machine
- Edit virtual machine settings
- Upgrade this virtual machine

**Devices:**

Device	Setting
Memory	512 MB
Processors	1
Hard Disk (SCSI)	8 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
Network Adapter 2	Host-only
USB Controller	Present
Display	Auto detect

**Description:**  
This is Metasploitable2 (Linux)  
Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.  
The default login and password is msfadmin:msfadmin.  
Never expose this VM to an untrusted network (use NAT or Host-only mode if you have any questions what that means).  
To contact the developers, please send email to msfdev@metasploit.com

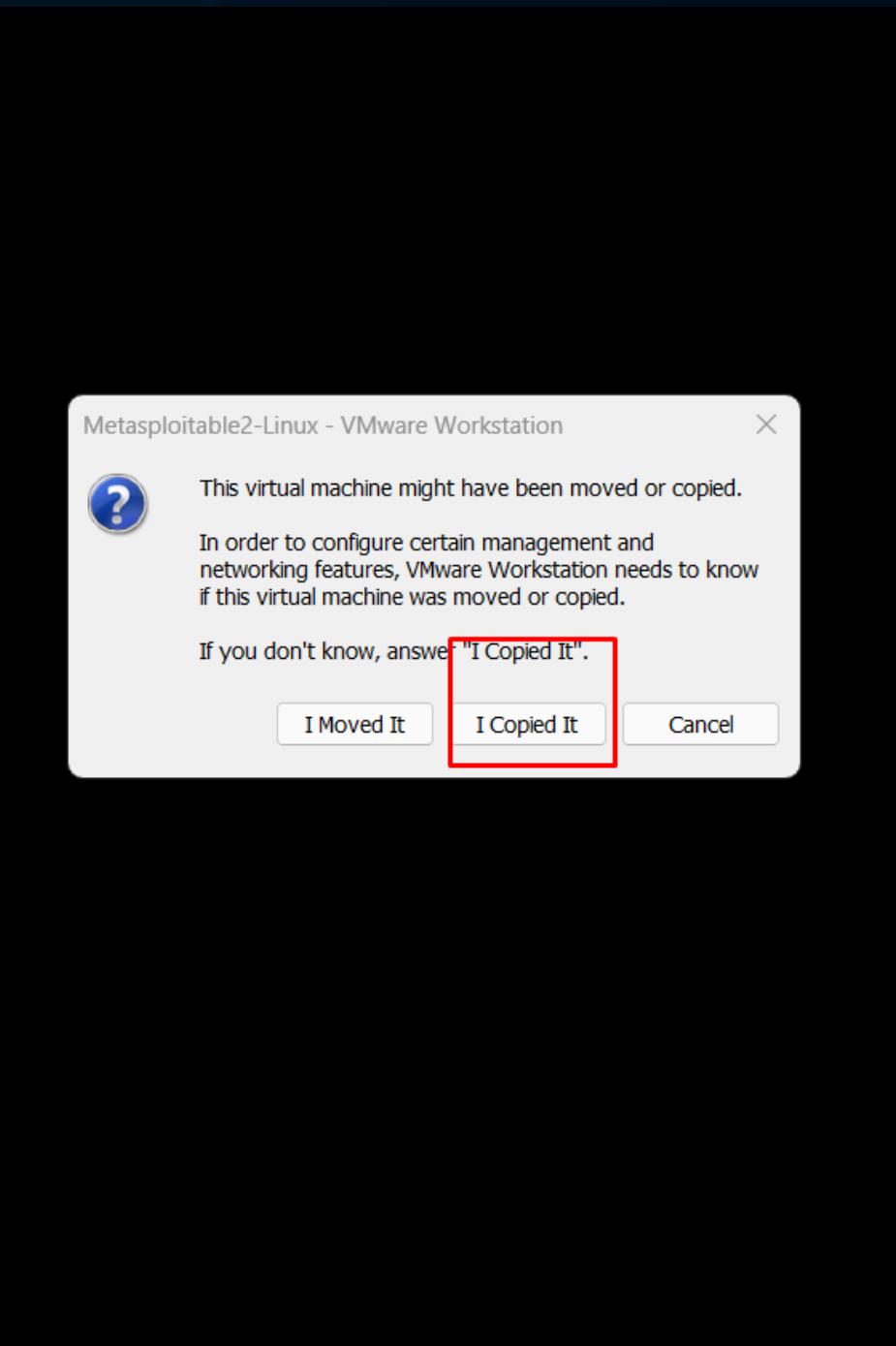
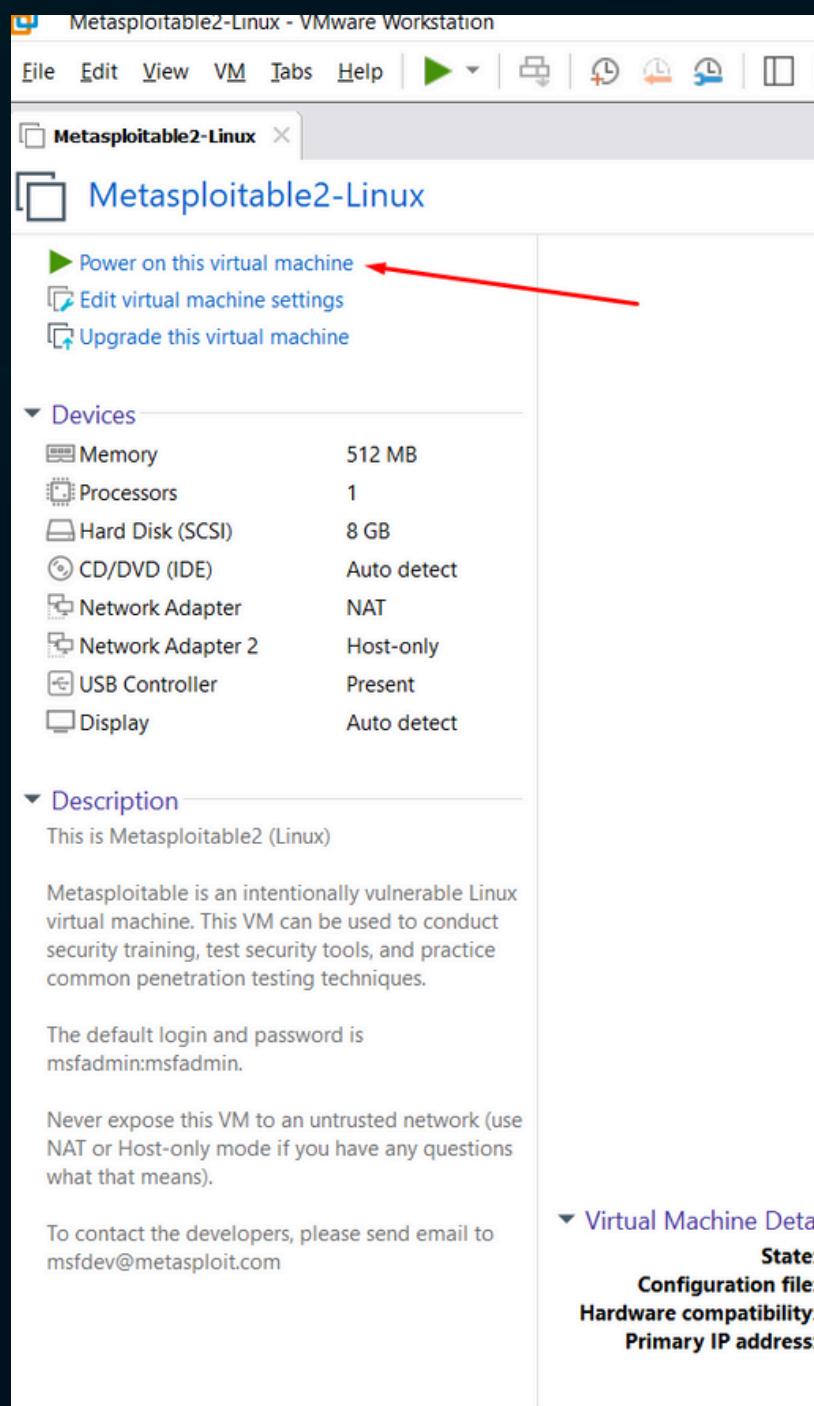
**Virtual Machine Details:**  
State: Powered off  
Configuration file: C:\Users\boran\OneDrive\Masaüstü\Metasploitable2-Linux\Metasploitable.vmx  
Hardware compatibility: Workstation 6.5-7.x virtual machine  
Primary IP address: Network information is not available



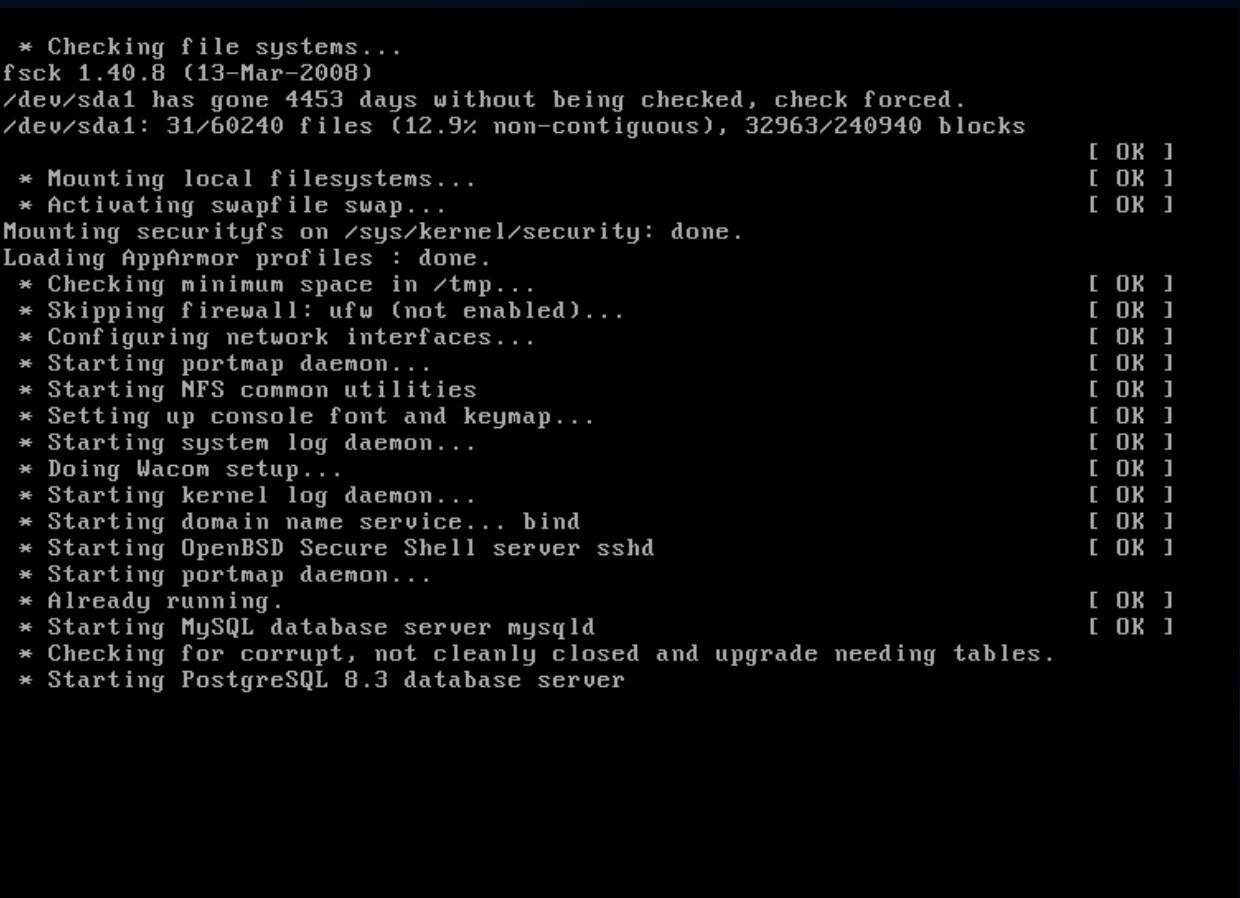
# STEP 5

# TAHA BORAN KOTAN

- Click: "Power on this virtual machine".



- Installation starts...





# STEP 6

# TAHA BORAN KOTAN

- Installation ended.

A white curved arrow pointing from the 'REVIEW' section to the 'ANSWER' section.

- 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!

```
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _
```

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



# TAHA BORAN KOTAN



# CYBER SECURITY

C F S S   I N T E R N S H I P   P R O G R A M

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.

02

INSTALLATION =>

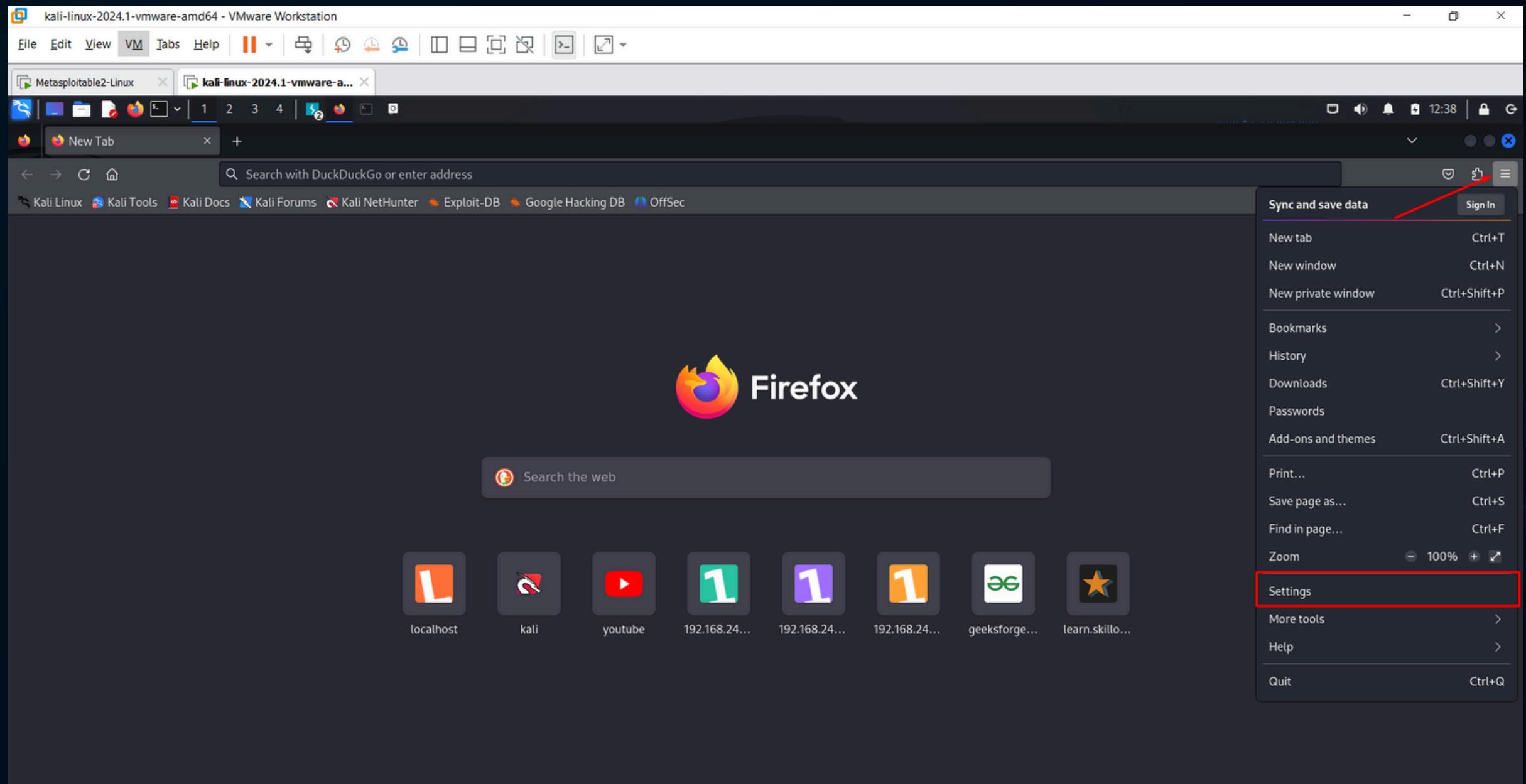


# STEP 1

- In first step, we configure our web browser proxy for capture credentials.
- Open your Kali Linux virtual machine. Then, open your Firefox Web Browser.



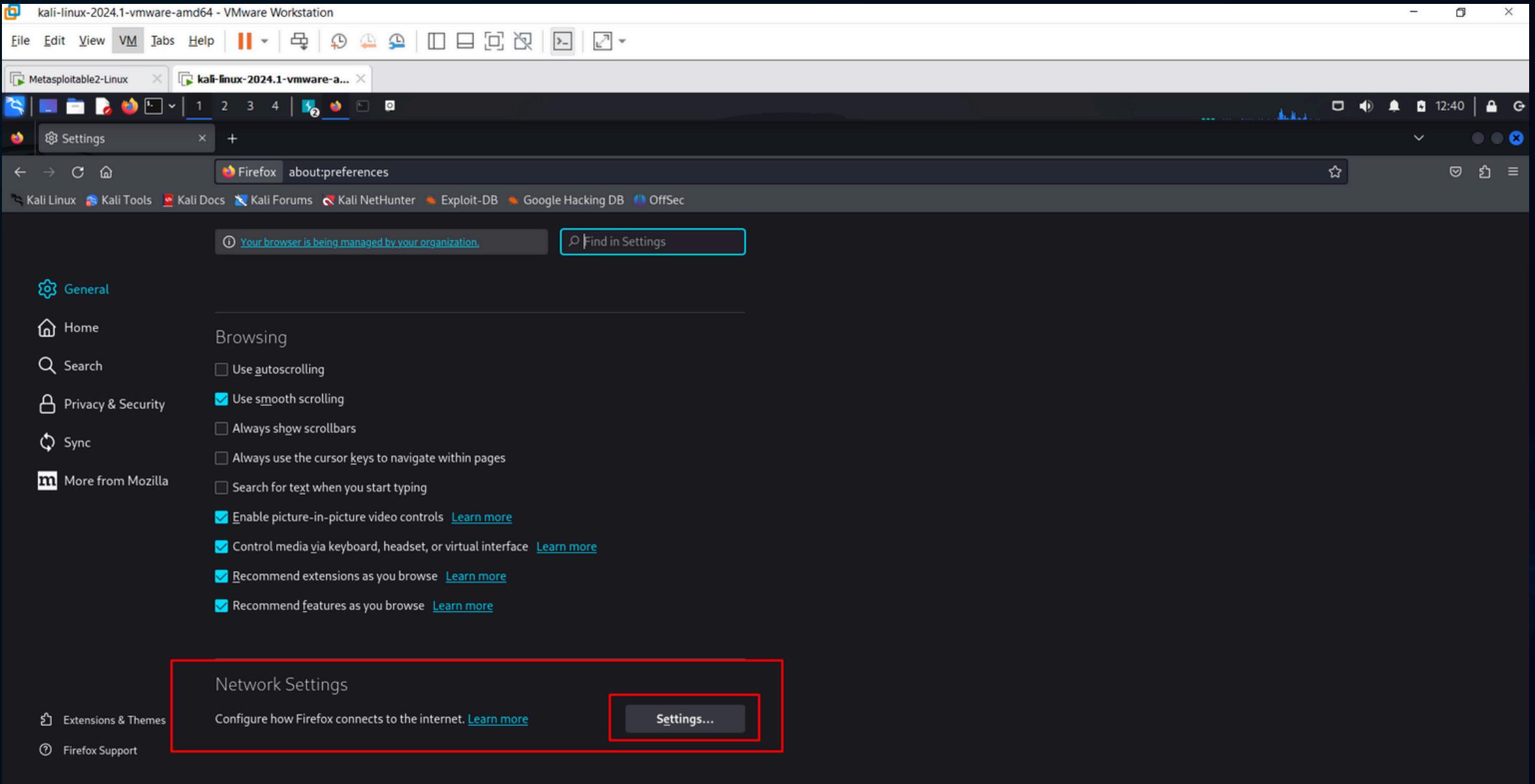
- On Firefox, follow the image and open “Settings”.





# STEP 1

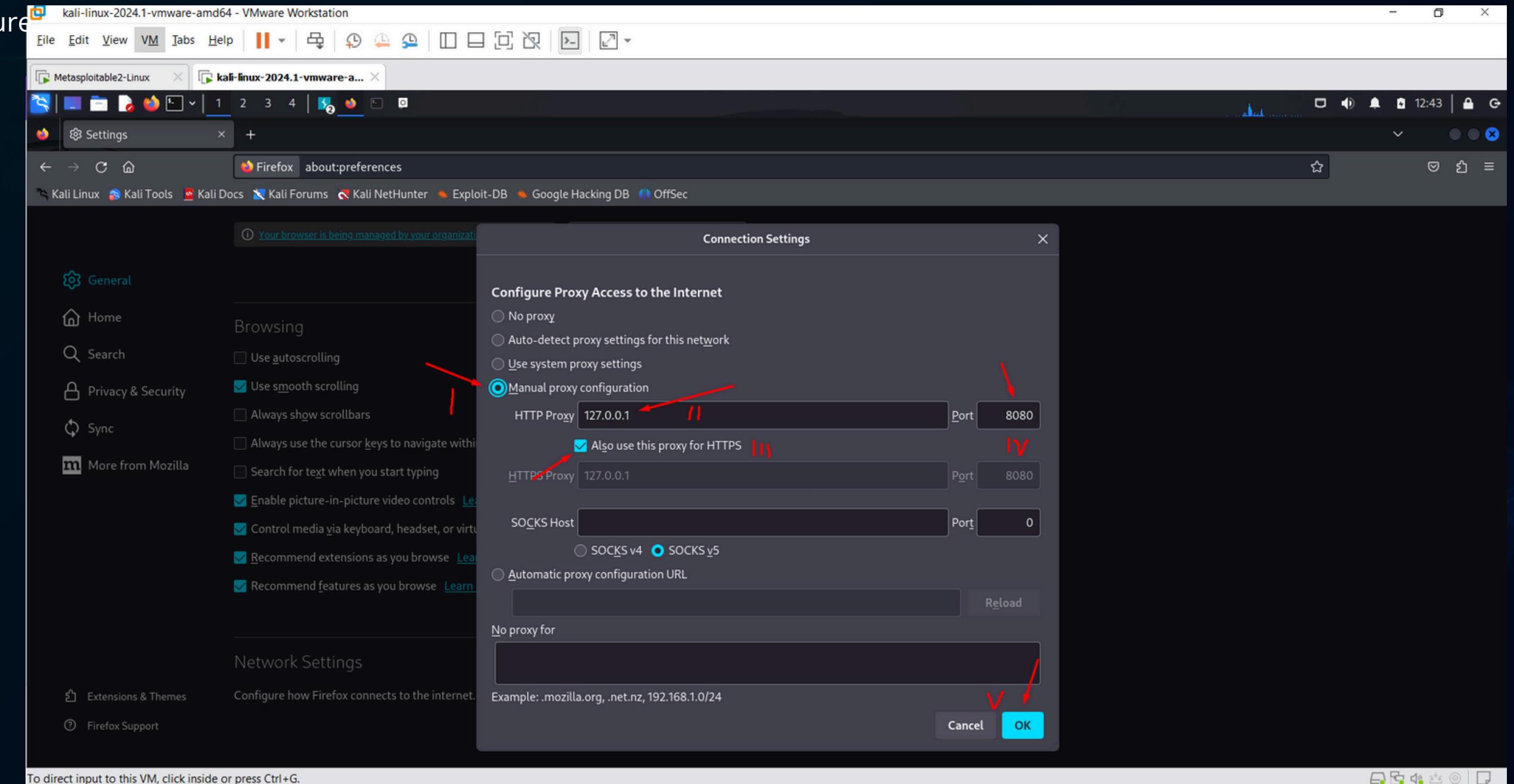
- Scroll down on this page and find “Network Settings”.
- Click “Settings”.





# STEP 1

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





## STEP 2

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



- Type: "ifconfig" and learn your IPv4 address.



- We will use this IPv4 address to reach Metasploitable 2 machine's web server.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:01:3b:0f
          inet  addr:192.168.241.136  Bcast:192.168.241.255  Mask:255.255.255.0
                  inetb  addr: fe80::20c:29ff:fe01:3b0f/64  Scope:Link
                      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                      RX packets:1825 errors:0 dropped:0 overruns:0 frame:0
                      TX packets:1560 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:1000
                      RX bytes:431471 (421.3 KB)  TX bytes:265754 (259.5 KB)
                      Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet  addr:127.0.0.1  Mask:255.0.0.0
          inet6  addr: ::1/128  Scope:Host
                  UP LOOPBACK RUNNING  MTU:16436  Metric:1
                  RX packets:627 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:627 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:243709 (237.9 KB)  TX bytes:243709 (237.9 KB)

msfadmin@metasploitable:~$
```



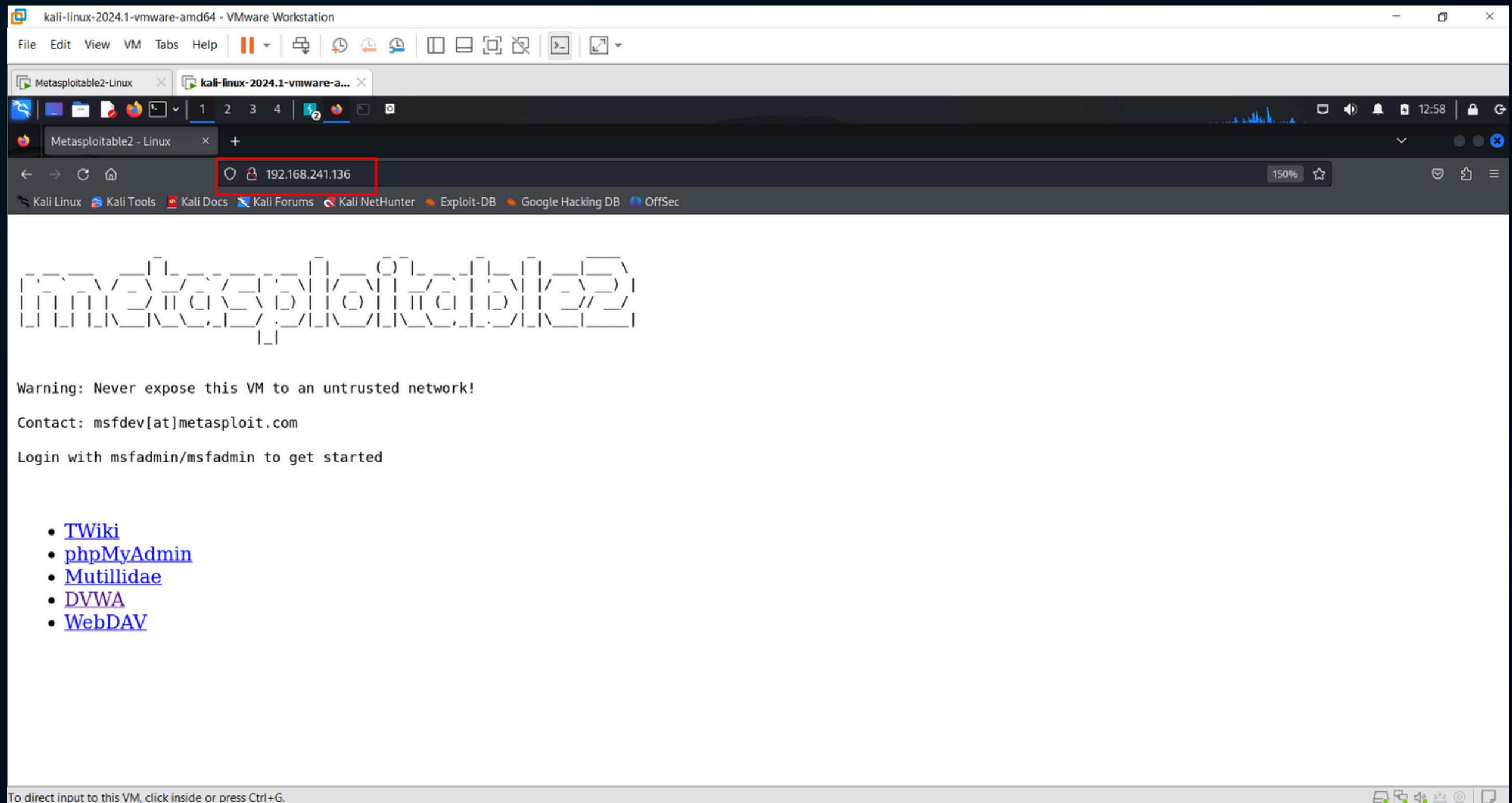
# STEP 3

# TAHA BORAN KOTAN

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



- Then type “Enter” to reach web server.





# STEP 3

- Click “DVWA” to reach login page.

The screenshot shows a Kali Linux desktop with a Metasploitable2-Linux VM running in a Firefox browser. The address bar displays the IP address 192.168.241.136. The VM's interface includes a warning message: "Warning: Never expose this VM to an untrusted network!", contact information: "Contact: msfdev[at]metasploit.com", and a login prompt: "Login with msfadmin/msfadmin to get started". A list of links at the bottom includes TWiki, phpMyAdmin, Mutillidae, DVWA (which is highlighted with a red box), and WebDAV.

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- **DVWA**
- [WebDAV](#)

# TAHA BORAN KOTAN

- Then the login page looks like that:

The screenshot shows the DVWA login page. It features a large DVWA logo at the top. Below it are two input fields: "Username" and "Password", both currently empty. A "Login" button is positioned below the password field. The background of the page is white.

Username

Password

Login

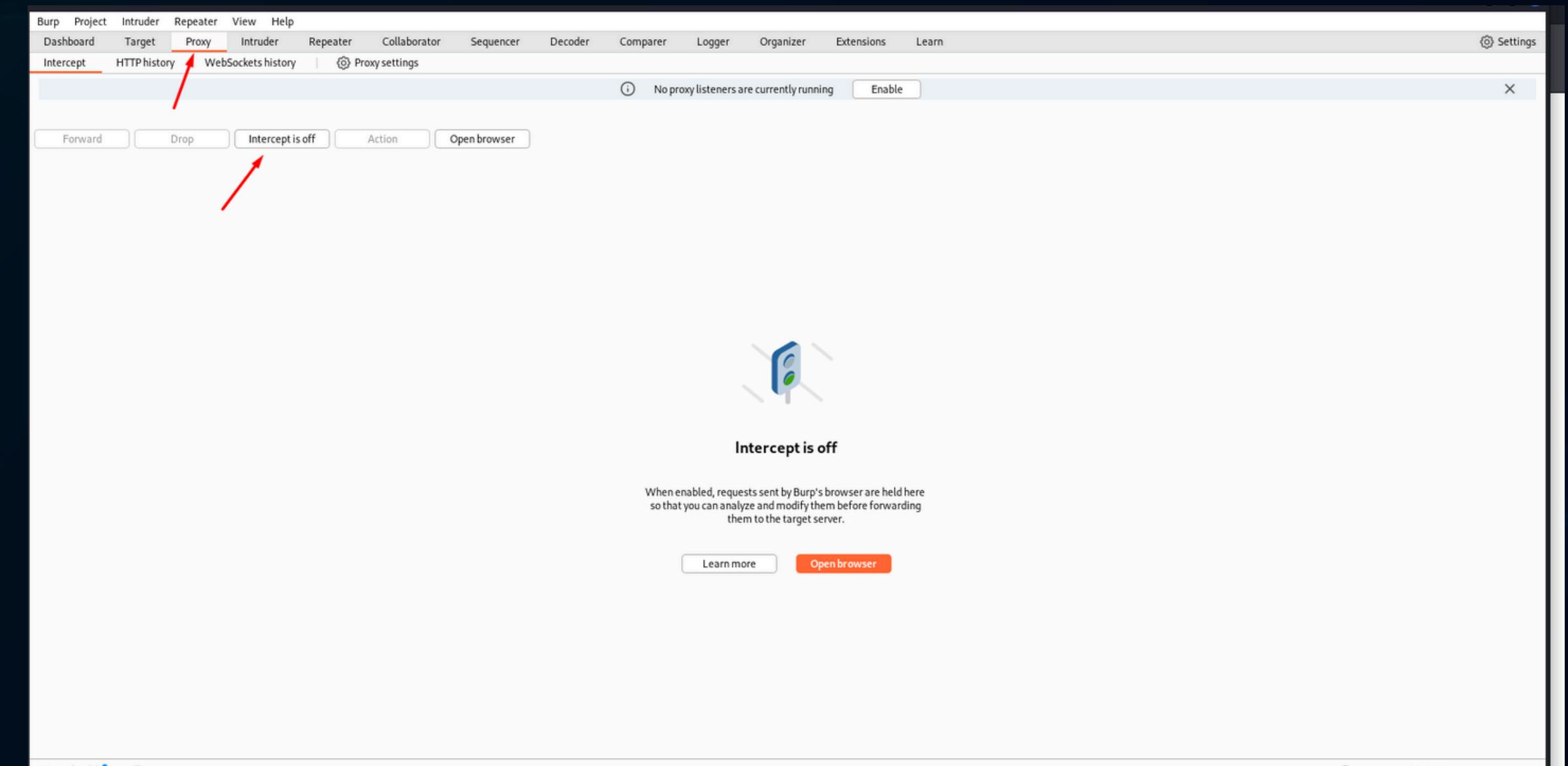
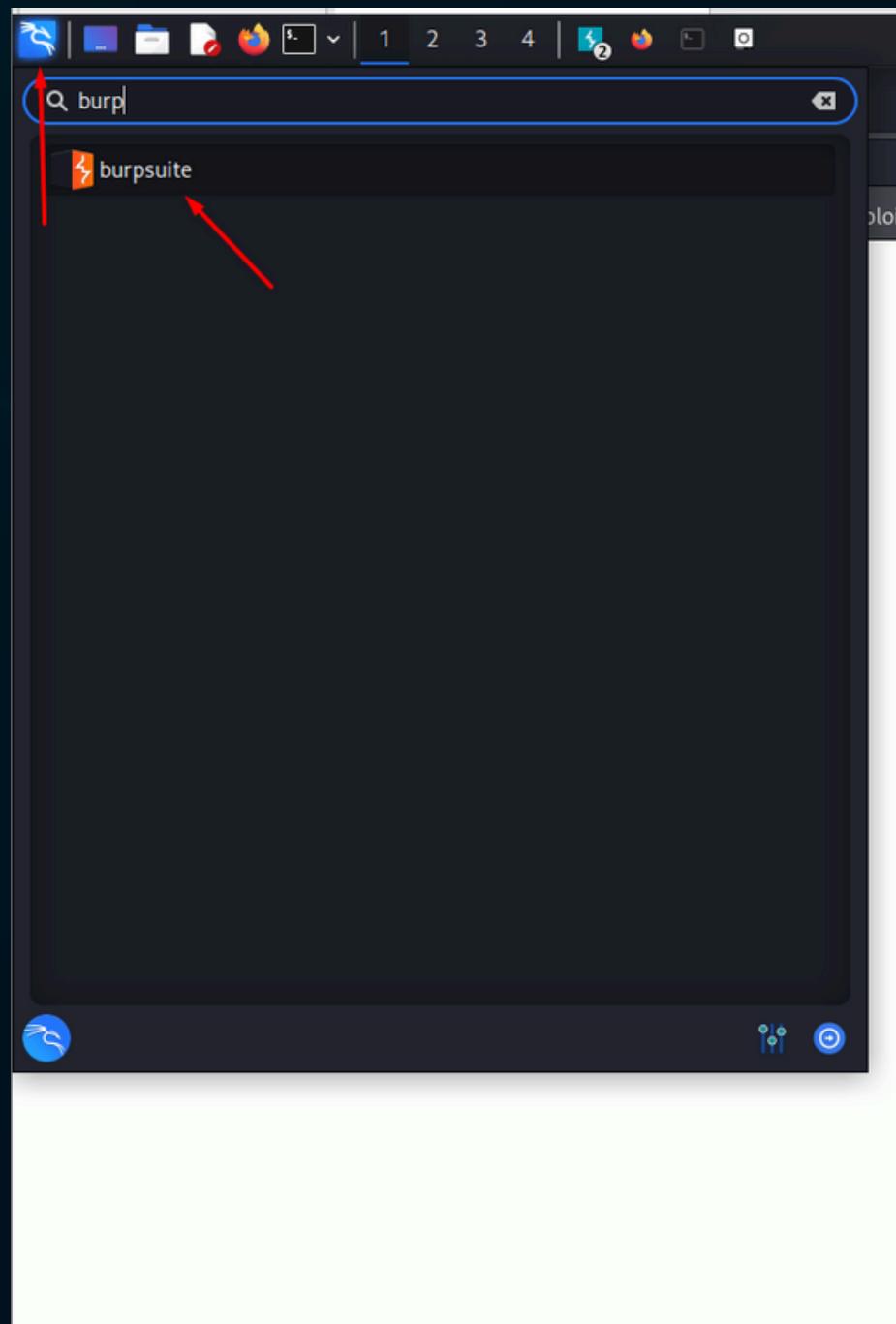


# STEP 4

- Open the Burp Suite.

# TAHA BORAN KOTAN

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





# 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.

DVWA

Username: asdasdasd

Password: ••••••••

Login

Burp Suite Intercept screen showing the captured POST request:

```
POST /dvwa/login.php HTTP/1.1
Host: 192.168.241.136
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 48
Origin: http://192.168.241.136
Connection: close
Referer: http://192.168.241.136/dvwa/login.php
Cookie: security=high; PHPSESSID=2a9a9a22efcce9b542d7cdd3a47a8483
Upgrade-Insecure-Requests: 1
username=asdasdasd&password=asdsadds&Login=Login
```

BRUTE FORCE ATTACK ON METASPLOITABLE 2 =>



# TAHA BORAN KOTAN



# CYBER SECURITY

C F S S   I N T E R N S H I P   P R O G R A M

T A H A   B O R A N   K O T A N  
P R O J E C T   4 :   B R U T E   F O R C E  
A T T A C K   O N   M E T A S P L O I T A B L E   2



# STEP 1

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

Username  
admin

Password  
..... *password*

Login

# TAHA BORAN KOTAN

- Click "Brute Force" button.

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

**Welcome to Damn Vulnerable Web App**

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is designed to be an aid for security professionals to test their skills and tools in a legal environment. It allows them to better understand the processes of securing web applications and aid teachers in teaching application security in a class room environment.

**WARNING!**

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting or any internet facing web server as it will be compromised. We recommend downloading onto a local machine inside your LAN which is used solely for testing.

**Disclaimer**

We do not take responsibility for the way in which any one uses this application. It is clear and it should not be used maliciously. We have given warnings to prevent users from installing DVWA on to live web servers. If your web server is hacked because of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded it.

**General Instructions**

The help button allows you to view hits/tips for each vulnerability and for each section of the application.



# TAHA BORAN KOTAN

## STEP 1

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

### Vulnerability: Brute Force

**Login**

Username:

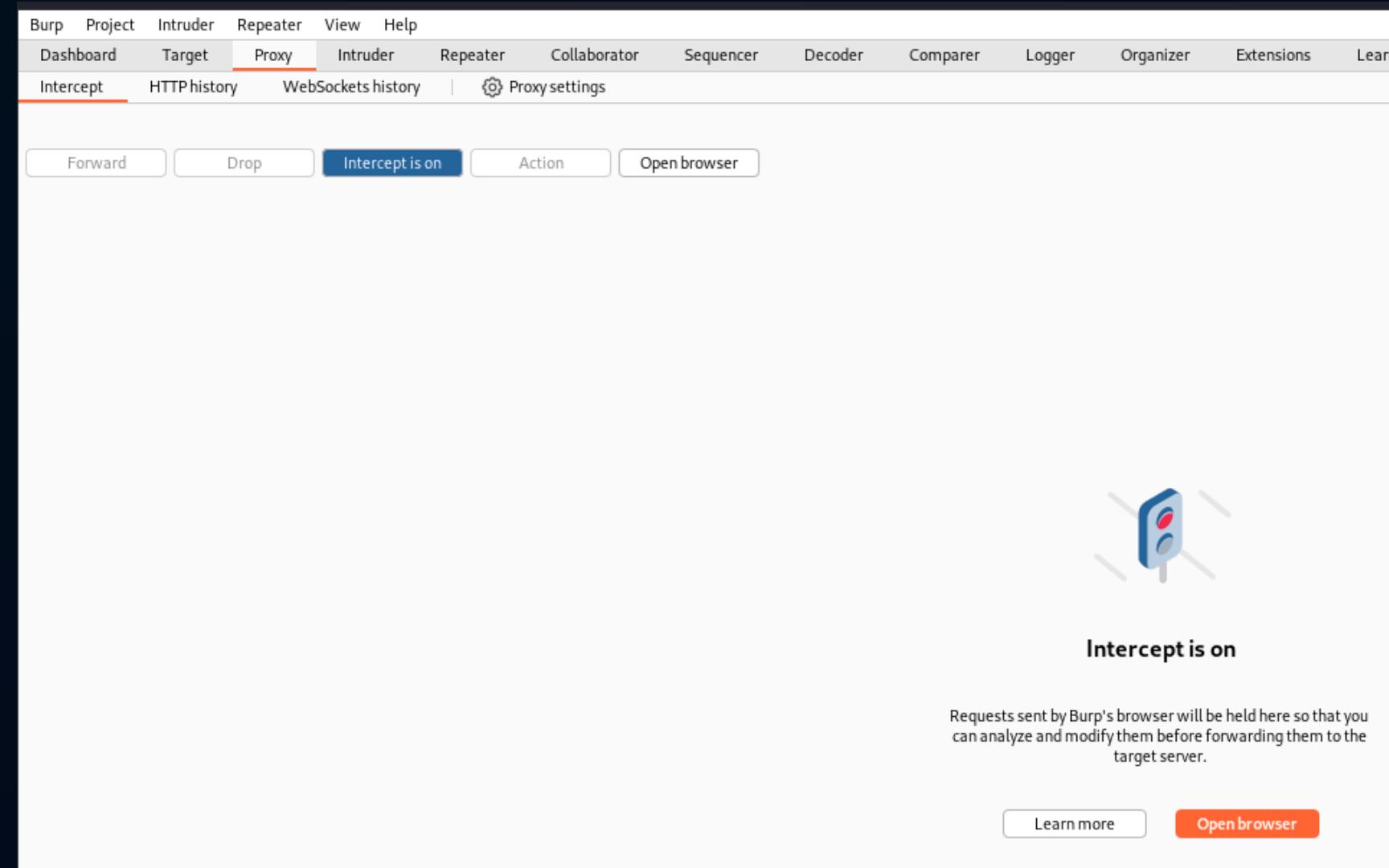
Password:

**Login**

**More info**

[http://www.owasp.org/index.php/Testing\\_for\\_Brute\\_Force\\_%28OWASP-AT-004%29](http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29)  
<http://www.securityfocus.com/infocus/1192>  
<http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>

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



The screenshot shows the Burp Suite interface. The top navigation bar includes Burp, Project, Intruder, Repeater, View, Help, Dashboard, Target, Proxy (which is selected and highlighted in red), Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. Below the navigation is a sub-menu with Intercept (selected and highlighted in red), HTTP history, WebSockets history, and Proxy settings. At the bottom of the interface are several buttons: Forward, Drop, Intercept is on (highlighted in blue), Action, and Open browser. To the right of the interface is a small icon of a blue and red traffic light with the text "Intercept is on" next to it. Below the icon is a descriptive text: "Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server." At the very bottom are two more buttons: Learn more and Open browser.



# 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.

### Vulnerability: Brute Force

**Login**

Username:

Password:

**Login** ←

The screenshot shows the Burp Suite interface with the "Proxy" tab selected. A context menu is open over the captured request, with the "Send to Intruder" option highlighted by a red arrow. The request details are as follows:

```
1 GET /dvwa/vulnerabilities/brute/?username=asdasd&password=asdadsads&Login=Login HTTP/1.1
2 Host: 192.168.241.136
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Referer: http://192.168.241.136/dvwa/vulnerabilities/brute/
9 Cookie: security=low; PHPSESSID=2as9
10 Upgrade-Insecure-Requests: 1
```



# STEP 2

# TAHA BORAN KOTAN

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

Burp Suite Community Edition v2023.12.1.3 - Temporary Project

Attack type: Sniper

Target: http://192.168.241.136

1 POST /dvwa/login.php HTTP/1.1  
2 Host: 192.168.241.136  
3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate, br  
7 Content-Type: application/x-www-form-urlencoded  
8 Content-Length: 48  
9 Origin: http://192.168.241.136  
10 Connection: close  
11 Referer: http://192.168.241.136/dvwa/login.php  
12 Cookie: security=high; PHPSESSID=2a9a9a22efcce9b542d7cdd3a47a8483  
13 Upgrade-Insecure-Requests: 1  
14  
15 username=**asdasdasd**&password=**asdsadds**&Login=Login

Add \$ Clear \$ Auto \$ Refresh

Update Host header to match target

0 payload positions 0 highlights 0 issues 0 memory 102.3MB

Event log (3) All issues Memory: 102.3MB

03



# STEP 2

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

Burp Suite Community Edition v2023.1

Choose an attack type

Attack type: Cluster bomb

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://192.168.241.136

```
1 GET /dvwa/vulnerabilities/brute/?username=$asdasd$&password=$asdasdads$&Login=Login HTTP/1.1
2 Host: 192.168.241.136
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Referer: http://192.168.241.136/dvwa/vulnerabilities/brute/
9 Cookie: security=low; PHPSESSID=2a9a9a22efcce9b542d7cdd3a47a8483
10 Upgrade-Insecure-Requests: 1
11
12
```

② Choose an attack type

② Payload positions

Burp Suite Community Edition v2023.1

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined.

Payload set: 1 Payload count: 2

Payload type: Simple list Request count: 0

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	admin
Load ...	administrator
Remove	
Clear	
Deduplicate	

Add |

Add from list ... [Pro version only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

Burp Suite Community Edition v2023.1

Proxy Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer

1 x 2 x +

Positions Payloads Resource pool Settings

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined.

Payload set: 2 Payload count: 2

Payload type: Simple list Request count: 4

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	password
Load ...	pwd
Remove	
Clear	
Deduplicate	

Add |

Add from list ... [Pro version only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

Event log (2) All issues



# 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 received some answers and in one attempt answer length seems so different.

The screenshot shows the Burp Suite interface with the "Intruder" tab selected. In the main pane, there is a table for configuring payloads. A single payload row is selected, containing the value "password". Below the table are buttons for Paste, Load..., Remove, Clear, and Deduplicate. At the bottom are Add, Enter a new item, and Add from list... buttons.

The screenshot shows the "Results" tab of the Burp Suite Intruder attack interface. It displays a table of attack results for the URL <http://192.168.241.136>. The table includes columns for Request ID, Payload 1, Payload 2, Status code, Error, Timeout, Length, and Comment. The "Length" column shows varying lengths for each response. A red arrow points to the length of the fourth response, which is 4919, highlighting a potential security vulnerability.

Req...	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0			200	<input type="checkbox"/>	<input type="checkbox"/>	4920	
1	admin	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4985	→
2	adminsitrator	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4920	
3	admin	pwd	200	<input type="checkbox"/>	<input type="checkbox"/>	4919	
4	adminsitrator	pwd	200	<input type="checkbox"/>	<input type="checkbox"/>	4920	



# STEP 3

# TAHA BORAN KOTAN

- 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.

2. Intruder attack of http://192.168.241.136

Req...	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0			200	<input type="checkbox"/>	<input type="checkbox"/>	4920	
1	admin	password	200	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4985	
2	administrator	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4920	
3	admin	pwd	200	<input type="checkbox"/>	<input type="checkbox"/>	4919	
4	administrator	pwd	200	<input type="checkbox"/>	<input type="checkbox"/>	4920	

Request Response

Pretty Raw Hex

```
1 GET /dvwa/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
2 Host: 192.168.241.136
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Referer: http://192.168.241.136/dvwa/vulnerabilities/brute/
9 Cookie: security=low; PHPSESSID=2a9a9a22efcce9b542d7cdd3a47a8483
10 Upgrade-Insecure-Requests: 1
11
12
```

Attack Save Columns

2. Intruder attack of http://192.168.241.136

Req...	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0			200	<input type="checkbox"/>	<input type="checkbox"/>	4920	
1	admin	password	200	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4985	
2	administrator	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4920	
3	admin	pwd	200	<input type="checkbox"/>	<input type="checkbox"/>	4919	
4	administrator	pwd	200	<input type="checkbox"/>	<input type="checkbox"/>	4920	

Request Response

Pretty Raw Hex Render

DVWA

Vulnerability: Brute Force

Home Instructions Setup Brute Force Command Execution CSRF File Inclusion SQL Injection

Login

Welcome to the password protected area admin

03



# TAHA BORAN KOTAN

## CONTACT ME



+90-0535-085-26-33



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



borantaha@gmail.com



ISTANBUL, TURKEY



# TAHA BORAN KOTAN

# THANK YOU

TAHA BORAN KOTAN