INTERNSHIP ON CYBER SECURITY

Introduction:

My name is Mohammad sheik Sauban. Currently pursuing Bachelors of Engineering from Mangalore Institute of Technology and Engineering, Moodabidri.

About DLithe:

DLithe Consultancy Services Pvt Ltd is an EdTech company established in 2018. It is based in Bengaluru and offers various services such as Data Analytics, Data Science, Machine Learning, Artificial Intelligence, Cyber Security and Bigdata solutions to clients in different industries. The company's goal is to provide quality services to its clients by leveraging advanced technologies and methodologies.

Summary of the Internship:

It was a one-month internship program i.e., from 06/02/2023 to 06/03/2023 from the expert professionals. The first 15 days we learnt about the networking. The next 15 days was all about working with real-world live projects. The projects like Brute-force attack, Malware Attack, Exploiting Metasploit, Password Creation etc... The technology used in this internship were Kali-Linux, OWASP, Meta and Cisco Packet Tracker.

TECHNICAL TASKS PERFORMED

Group 1:

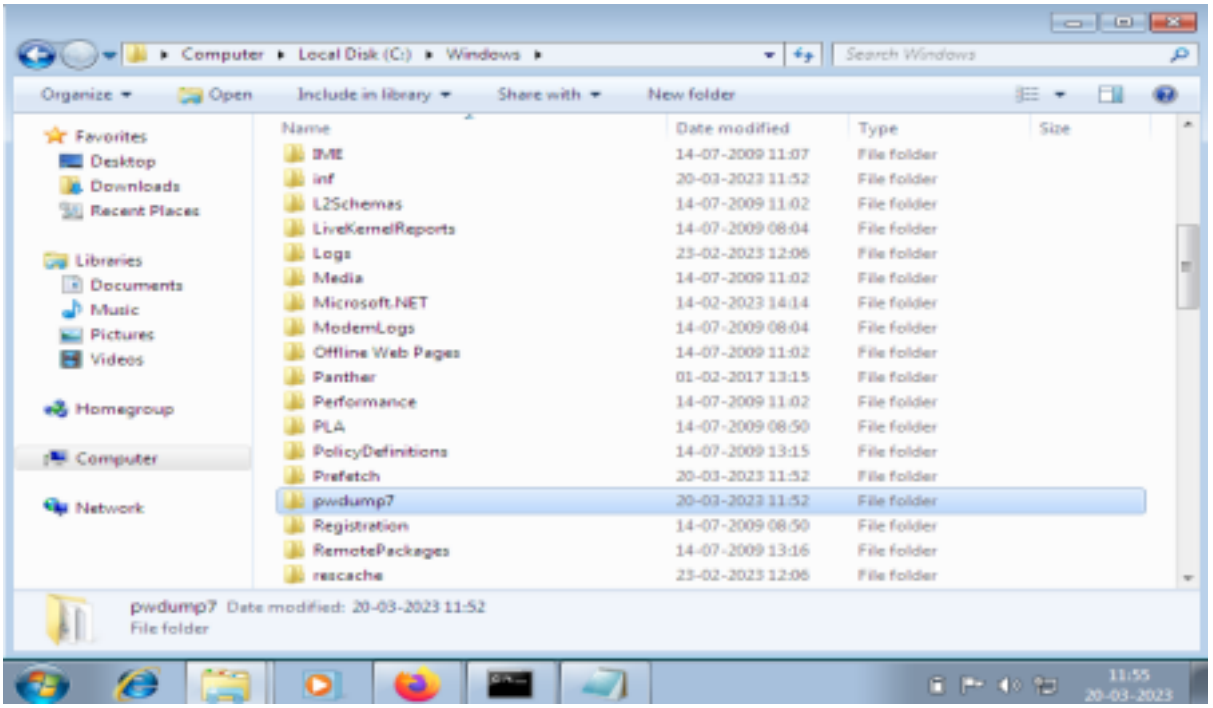
2a) PASSWORD CRACKING OF WINDOWS 7

Here, we are cracking the password of windows7 using **John the Ripper** tool.

It is a popular password cracking tool that can be used to perform brute-force attacks using different encryption technologies and helpful wordlists. John the Ripper is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force) passwords.

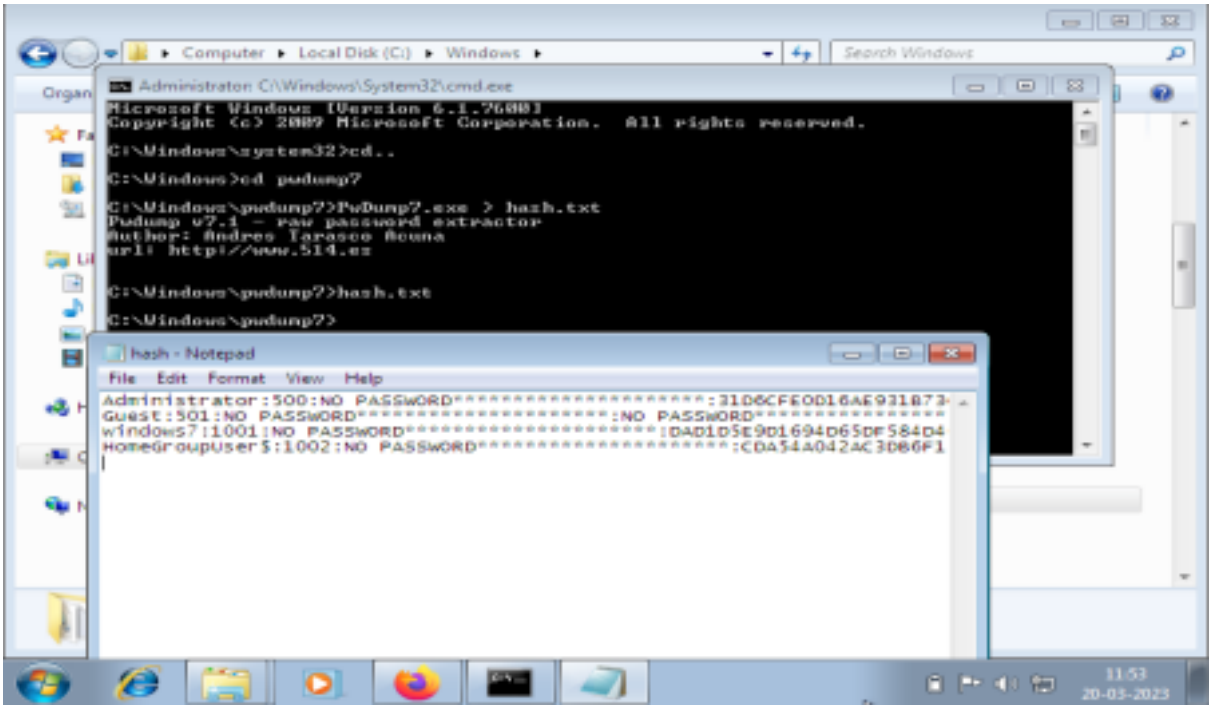
Step 1: Go to windows7 and download pwdmp7 and unzip it.

Step 2: After unzipping the file and extract it in the C-drive of my computer and add it inside windows.

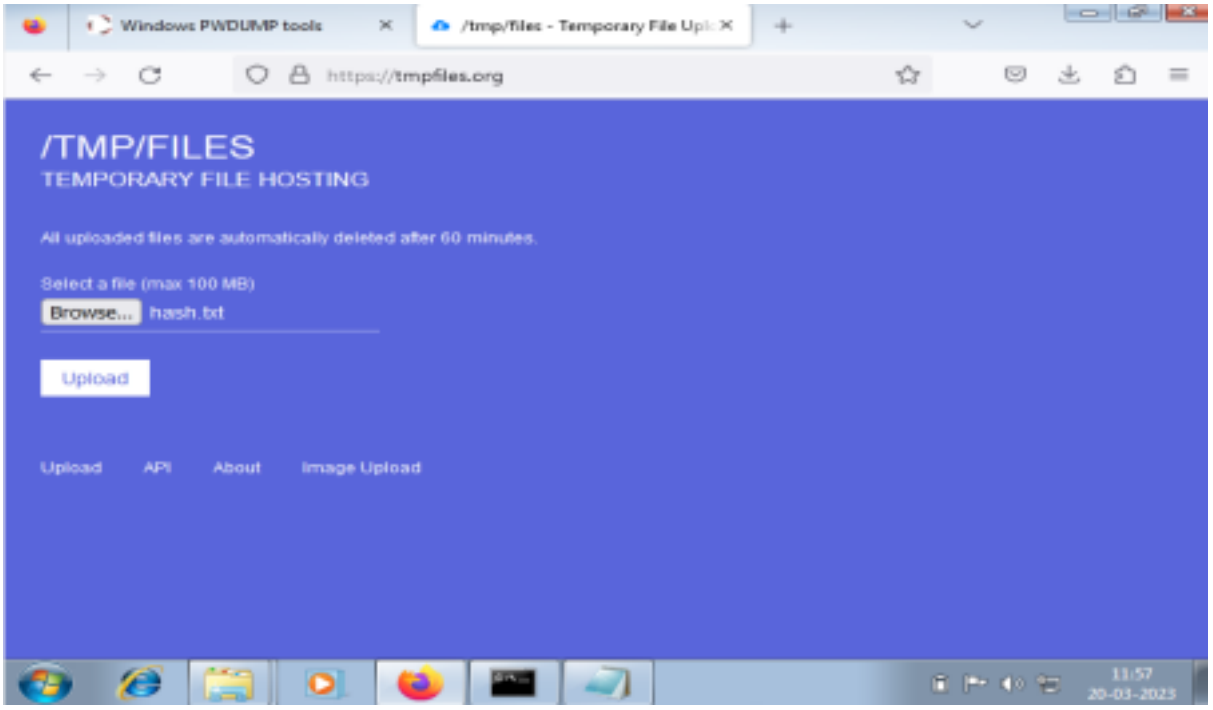


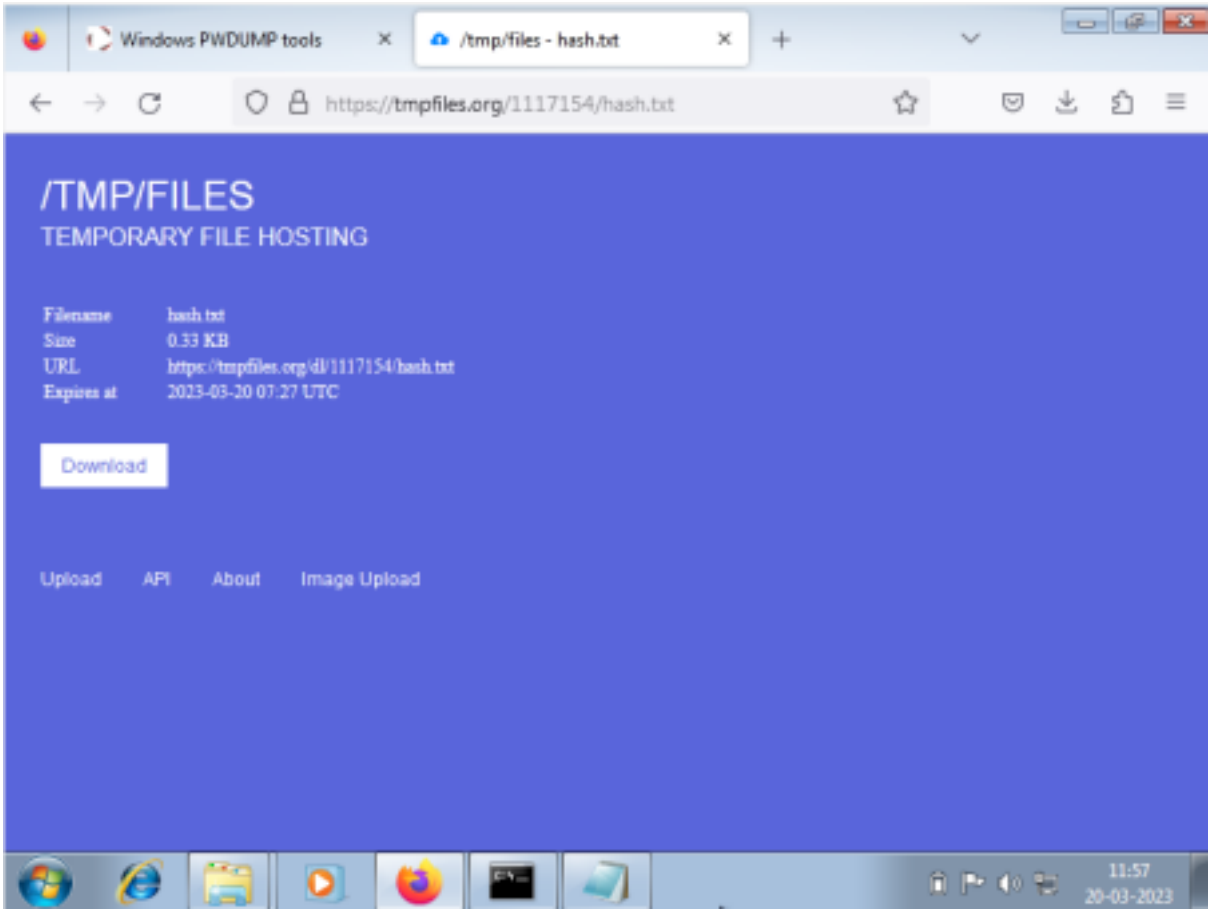
Step 3: Run cmd as administrator and perform these steps

- cd..
- cd pwdump7
- PwDump7.exe > hash.txt
- hash.txt (to view the file)

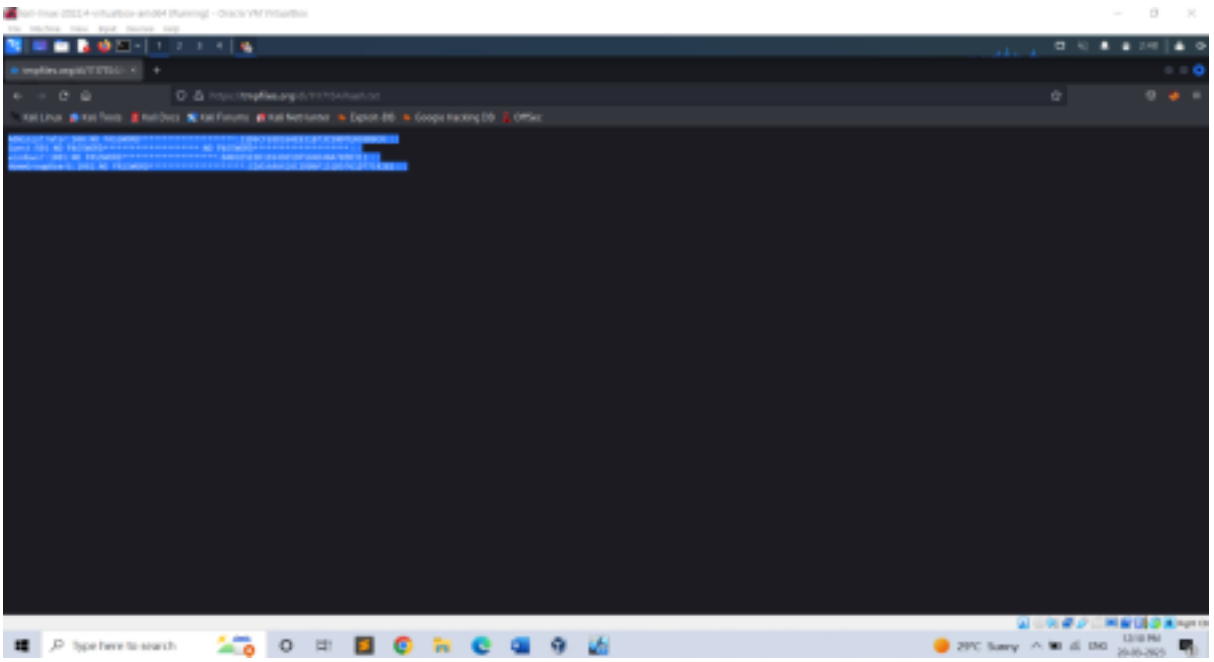


Step 4: Now send the hash.txt file to kali. So, upload the file in **tmpfile.org**





Step 5: In the Kali in order to access the tmpfile copy and paste the link in the Kali Firefox and hit enter. You can see the file in the browser then copy it.

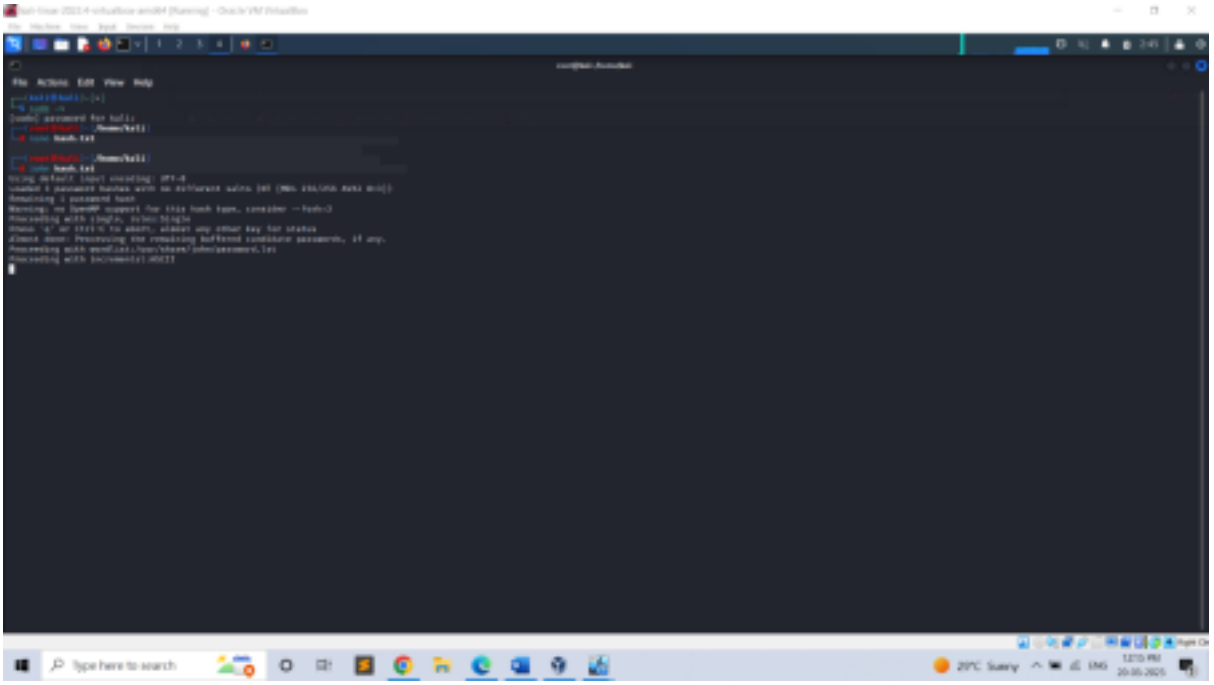


Step 6: Run the cmd and become the super user using sudo –su.
Create a new file using **nano** (file name) and paste the file. Save it and exit.
In order to crack use **John** command.

i.e.-> nano hash.txt

(paste) Ctrl+S and Ctrl+X

John hash.txt



2b) PASSWORD CRACKING OF METASPLOIT MACHINE USING HYDRA (BRUTE-FORCE ATTACK)

A brute force attack is a method of trying to crack a password or encryption key by systematically guessing every possible combination until the correct one is found. It is a common type of attack used by hackers to gain unauthorized access to systems, networks, or accounts.

Brute force attacks can be successful if the password or key is weak, short, or has been reused across multiple accounts. To prevent brute force attacks, it is important to use strong and unique passwords or passphrases that are difficult to guess or crack.

'nbtscan' is a command-line tool used to scan networks for NetBIOS name information. It can be used to identify Windows machines on a network, as well as gather information such as hostnames, MAC addresses, and workgroups.

Nano is a command-line text editor that is available in Kali Linux, Nano is a lightweight text editor that is designed to be easy to use and has a user-friendly interface. It provides basic text editing features such as cut, copy, and paste, as well as search and replace, spell checking, and syntax highlighting for various programming languages.
To open a file using nano in Kali Linux, you can use the command **nano <filename>** in the terminal. Once you have made your edits, you can save the changes and exit the editor by pressing **Ctrl+X**, and then confirming the save changes prompt.

1st create a file named 'user' and add the user's name. Then create another file named 'pass' and add the user's password in to that file. To save the file press Ctrl+S and exit it by Ctrl+X.

The command **hydra -L user -P pass ftp://192.168.56.101** is a sample command for using the Hydra password cracking tool to perform a brute force attack on an FTP server running on the IP address **192.168.56.101**.

- **hydra**: This is the command to invoke the Hydra password cracking tool.
- **-L user**: This option specifies the path to the file containing a list of usernames to use during the attack. In this case, the word "user" is being used as a placeholder for the actual file name or path.
- **-P pass**: This option specifies the path to the file containing a list of passwords to use during the attack. Similarly, the word "pass" is being used as a placeholder for the actual file name or path.
- **ftp://192.168.56.101**: This is the protocol and IP address of the target FTP server.

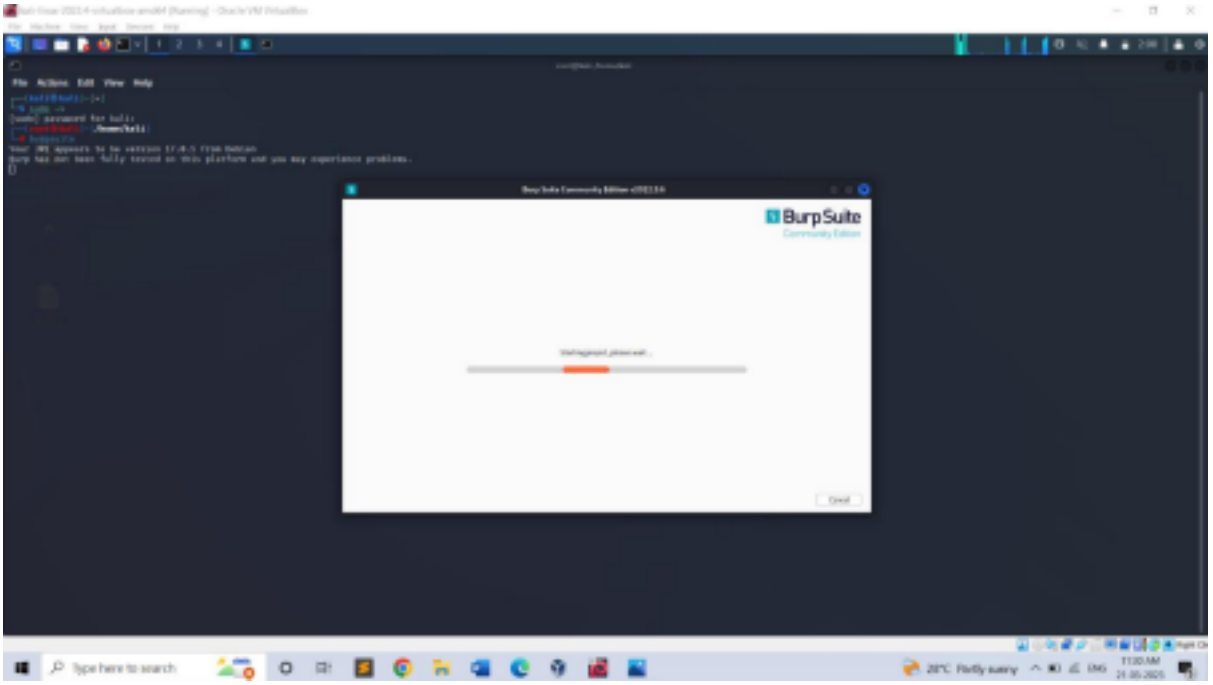
By this we can perform brute-force attack. At the end we get the username and password of the user.

3) PERFORM PASSWORD CRACKING OF ONLINE VULNERABLE WEBSITE(TESTFIRE.NET) USING BURPSUITE

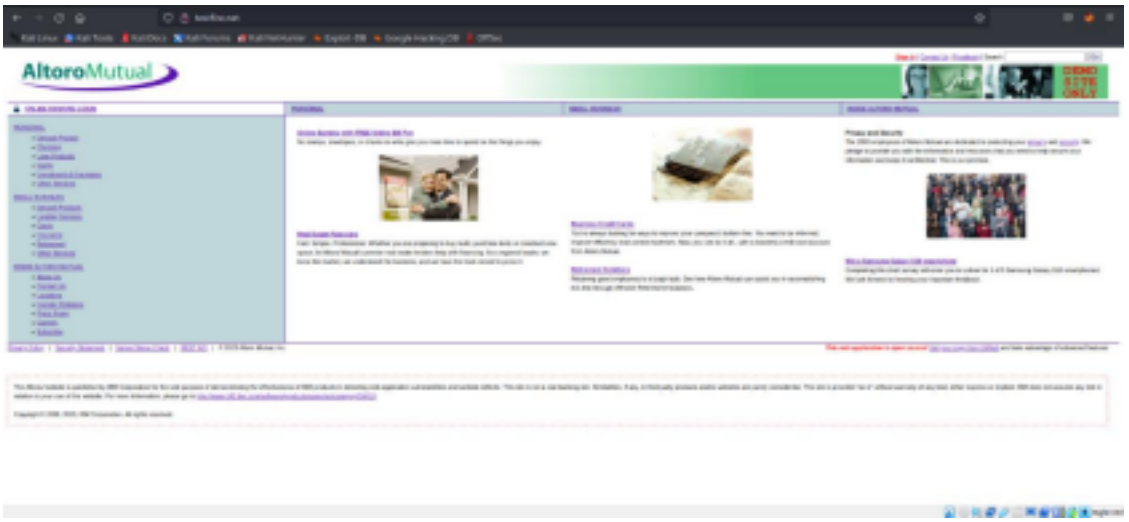
 Initially enter the command burpsuite. It will be redirecting to another page. Next step is to turn on the intercept. Next login in to the website testfire.net and then turn on the burp.

 As soon as you login your login details will be come under intercept. The code which is available in the proxy of the intercept just copy and send it to the intruder.

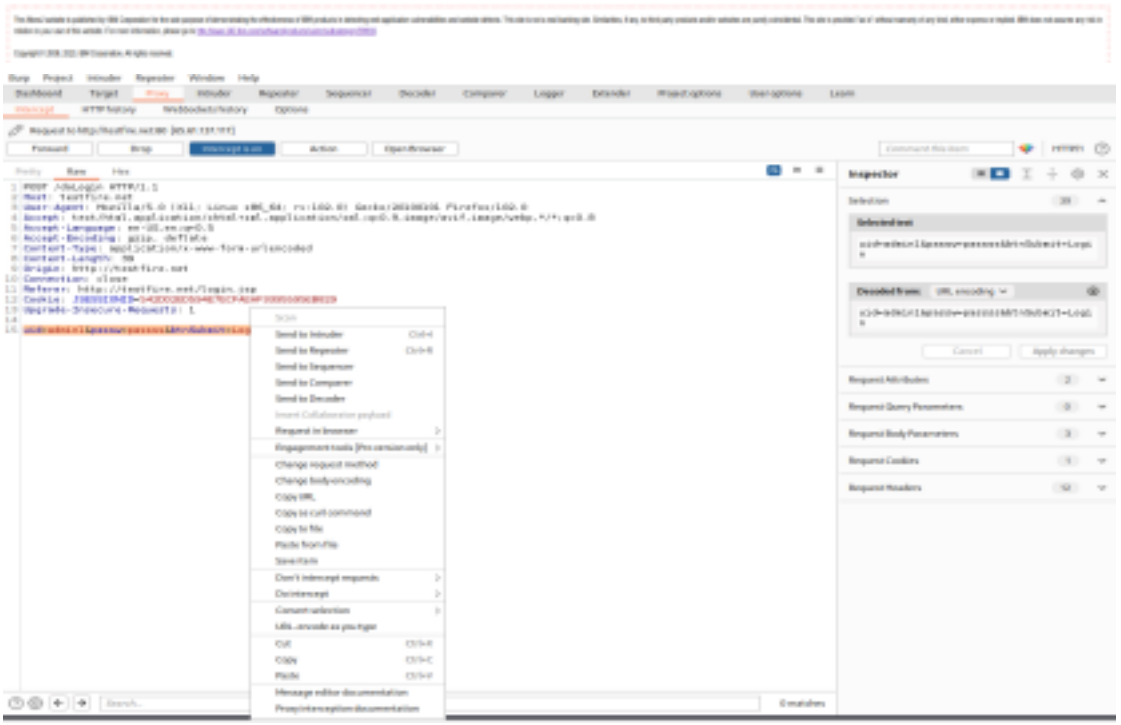
 There just copy the username and password the click on add button. Then select the attack type Cluster bomb set the payloads and start the attack.

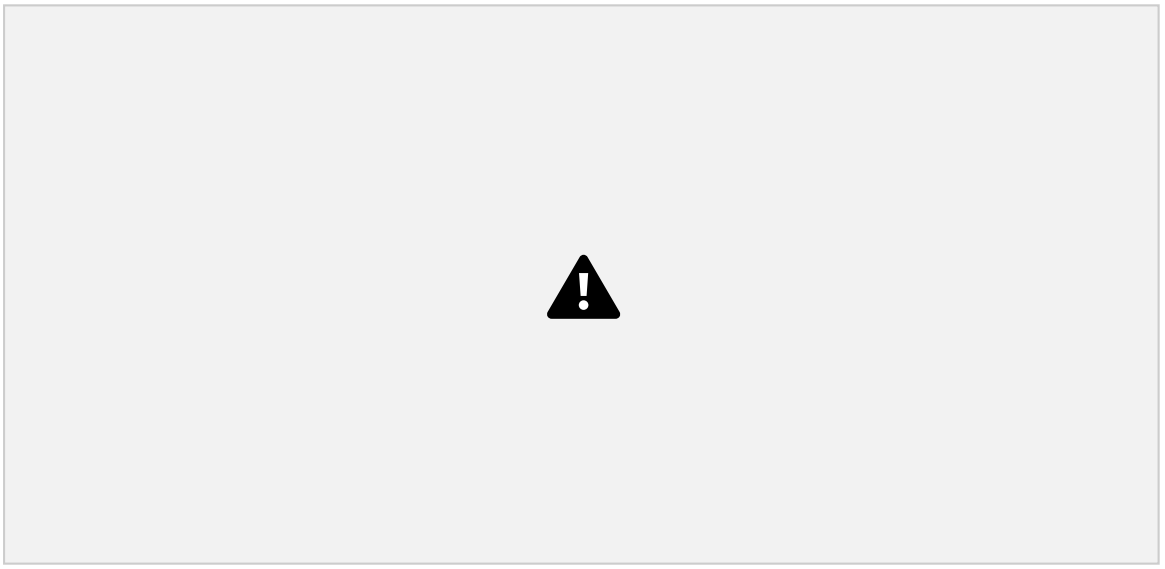

BurpSuite
Community Edition


Intercept is on


AltoroMutual


AltoroMutual
DEMO SITE ONLY
Online Banking Login





4a) Exploiting Metasploit using FTP

Step 1: Getting super access using the command $ sudo -s

Step 2: Enter the command nmap -sV followed by the target IP, nmap is a utility for network exploration security auditing and -sV for the system versions. nmap -sV 192.168.56.101

Step 3: Enter msfconsole, it is used to provide a command line interface to access and work with the Metasploit framework

Step 4: Enter the command search vsftpd

Step 5: Enter the command exploit/unix/ftp/vsftpd_234_backdoor which is available from step 4 use exploit/unix/ftp/vsftpd_234_backdoor

Step 6: Payload is not configured. Just enter show options

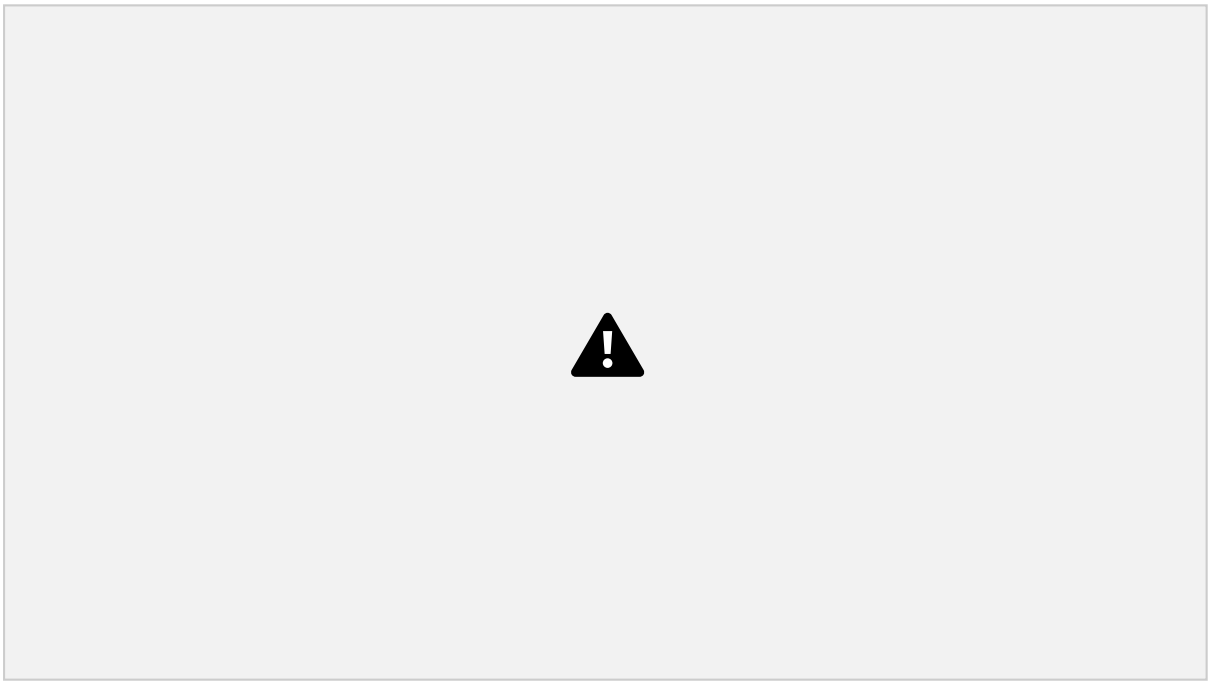
Step 7: In the option we must set the value for RHOSTS so enter the command set RHOSTS followed by the IP of the target, set RHOSTS 192.168.56.101

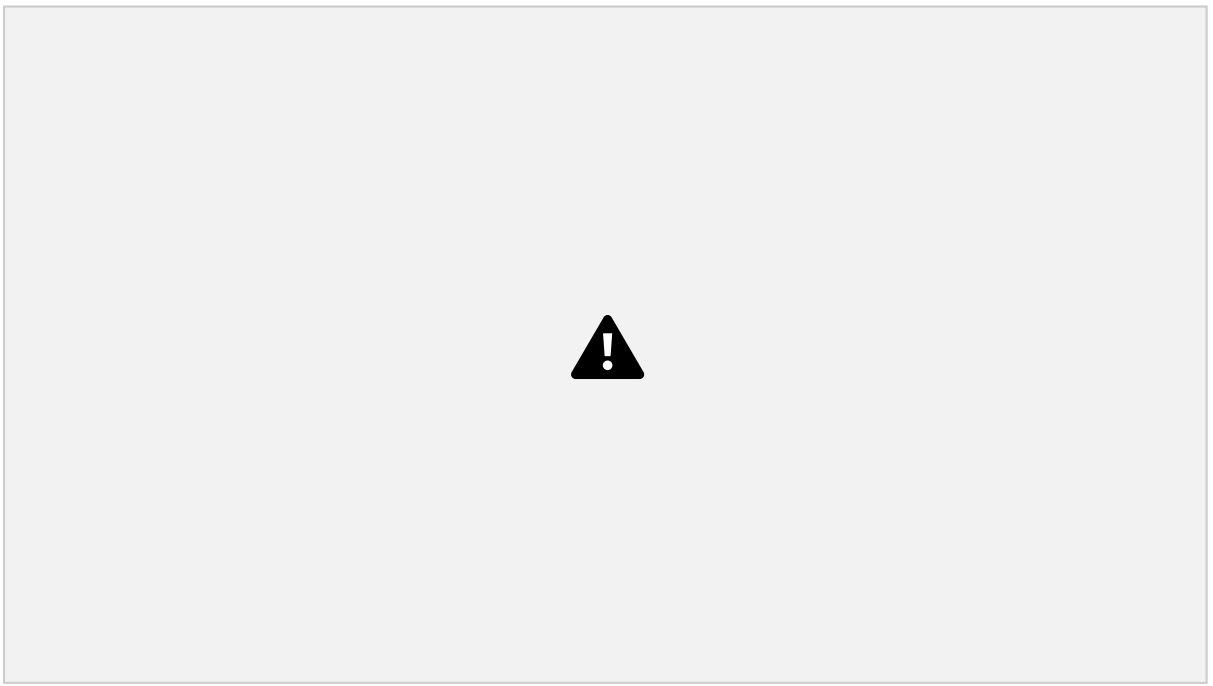
Step 8: We use show options in-order to check whether the RHOSTS has been updated or not.

Step 9: Enter the command show payloads

Step 10: We must set the payload as set payloads 192.168.56.101

Step 11: Enter the command exploit





4b) Exploiting Metasploit using SMTP

Step 1: Getting super access using the command $ sudo -s

Step 2: Check the IP address of the target (Metasploitable)

Step 3: Enter the command nbtscan, it is a program for scanning IP networks for NetBIOS name

information. nbtscan 192.168.56.0/24

Step 4: Enter the command nmap -sV followed by the target IP, nmap is a utility for network exploration

security auditing and -sV for the system versions. nmap -sV 192.168.56.101

Step 5: Enter msfconsole, it is used to provide a command line interface to access and work with the

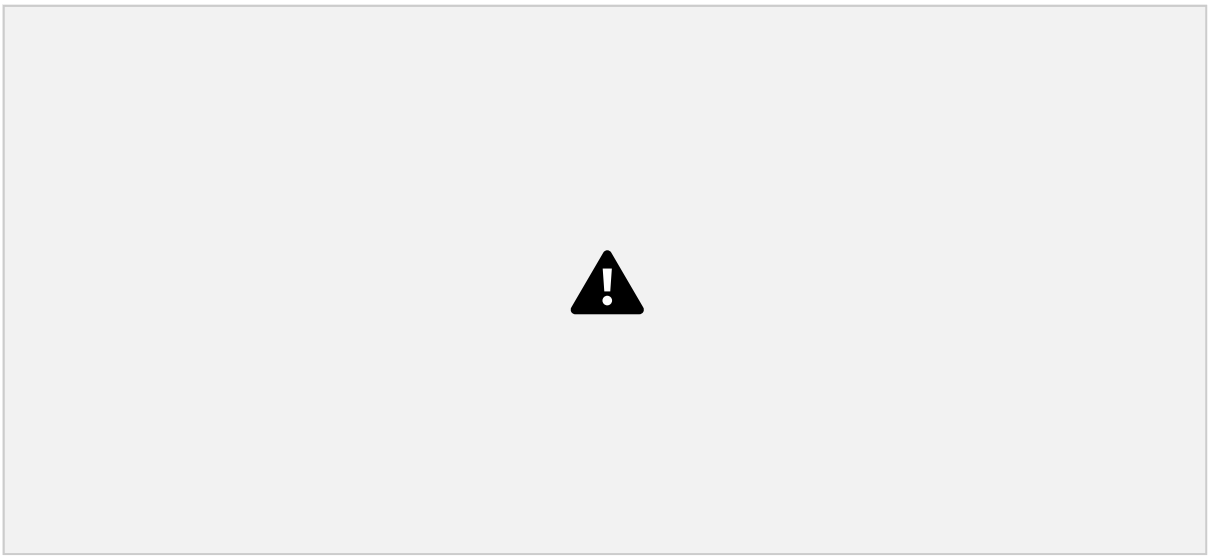
Metasploit framework

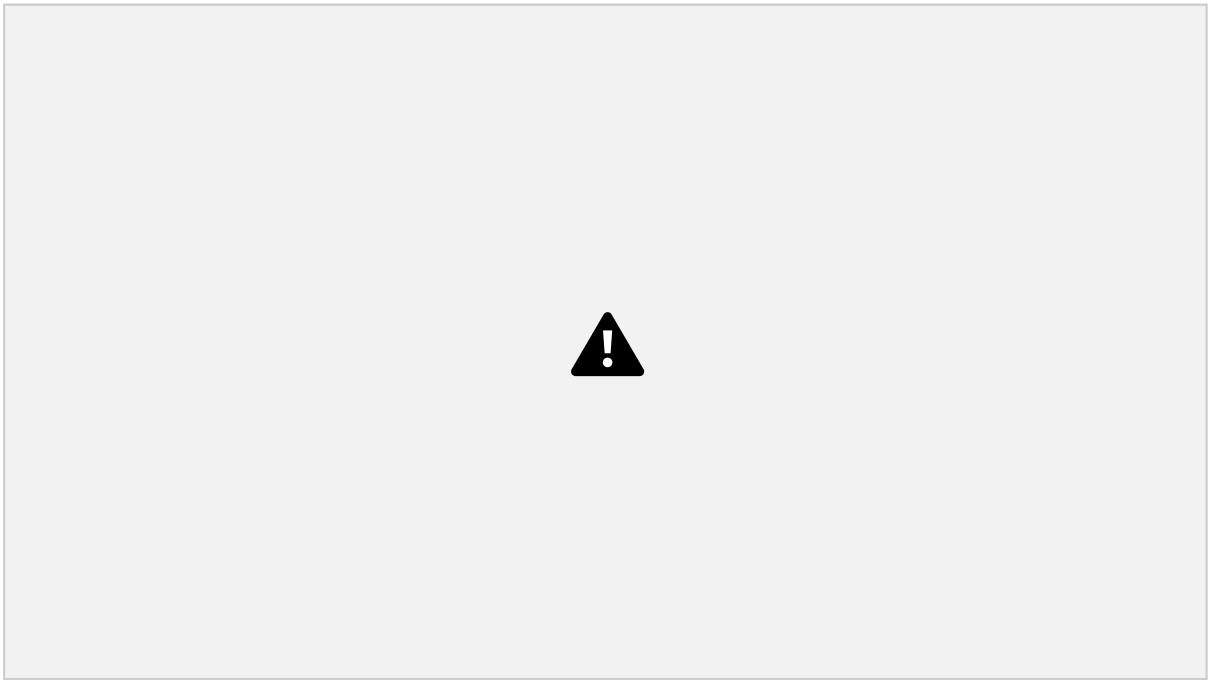
Step 6: In the msfconsole itself give the command use auxiliary/scanner/smtp/smtp_enum

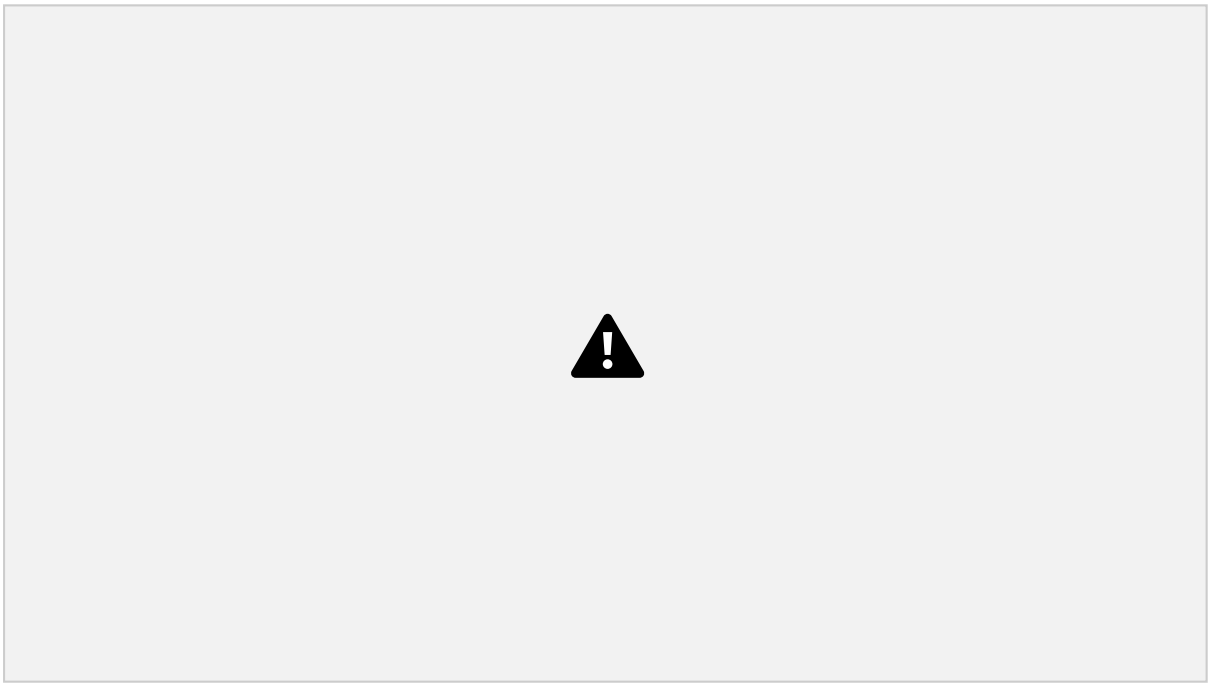
Step 7: Enter the command the show options.

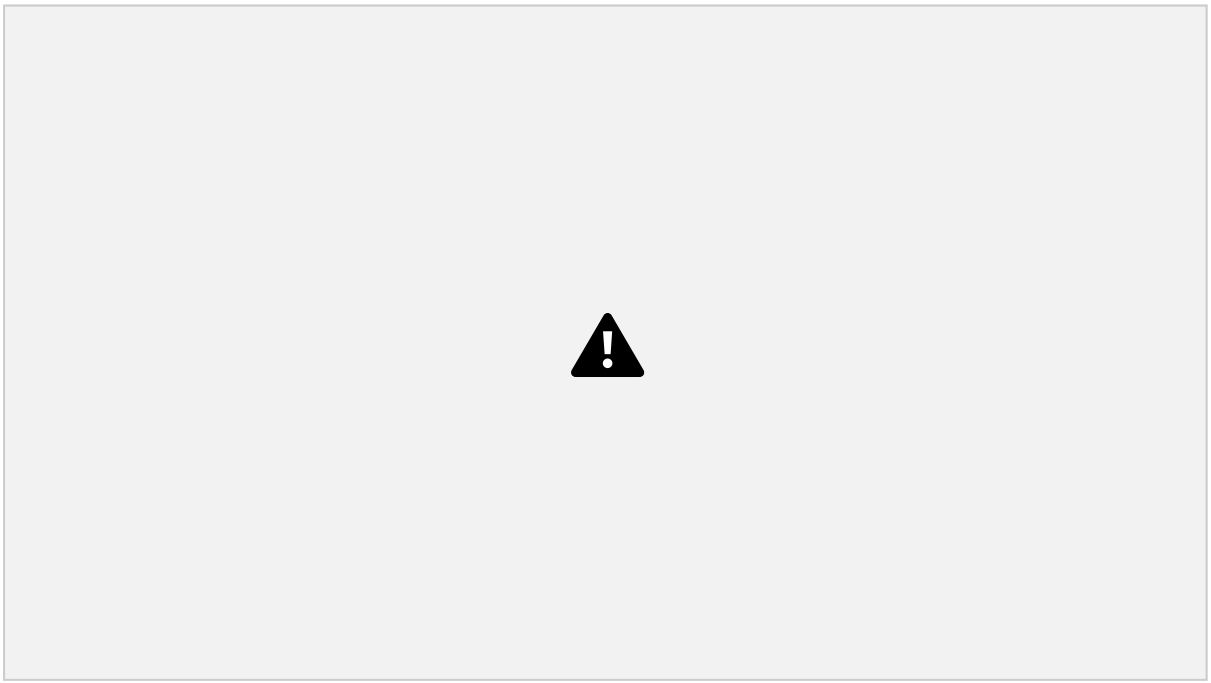
Step 8: Next we must set the rhosts so enter the command as set rhosts 192.168.56.101

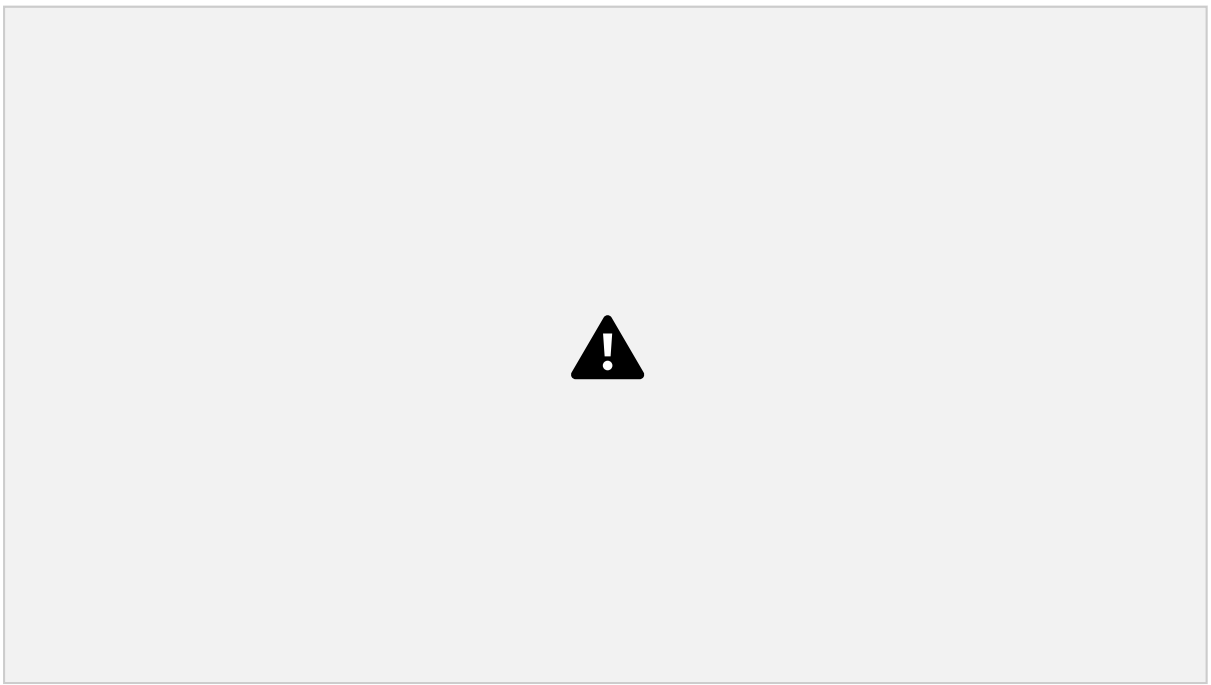
Step 9: Enter the command exploit



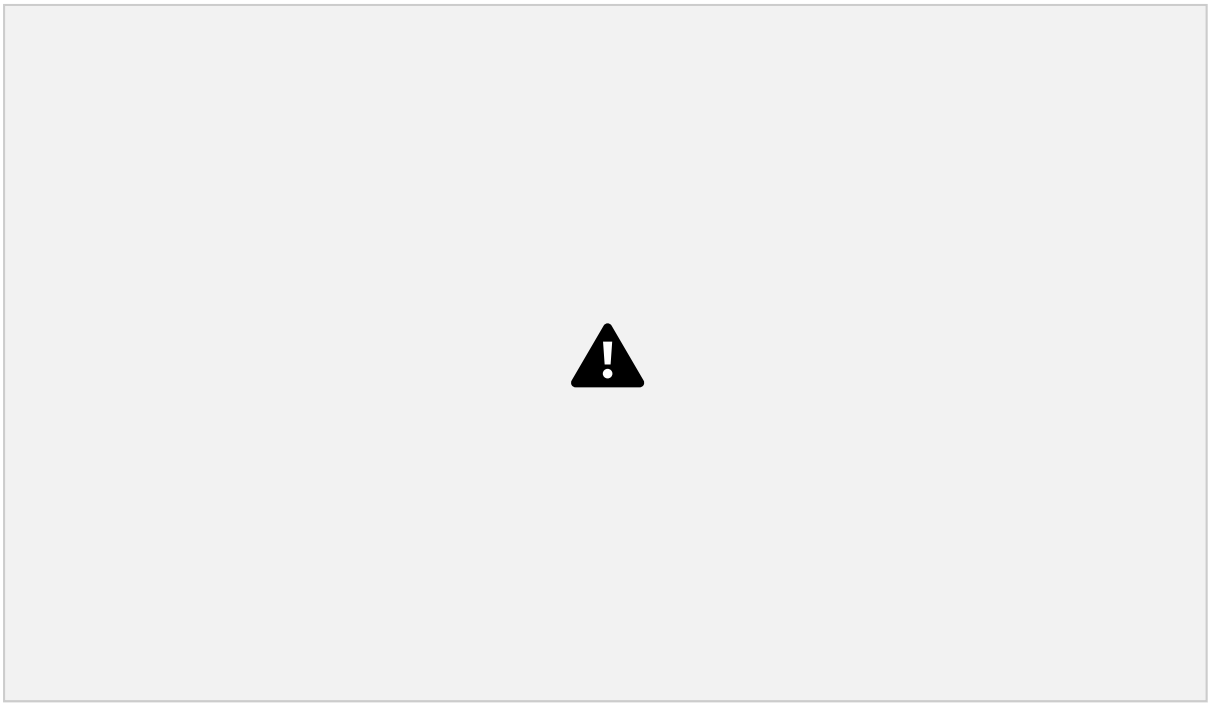








4c) Exploiting Metasploit using Bind shell



‘ifconfig’ is used to find the IP address of the machine.

‘nbtscan’ is a command-line tool used to scan networks for NetBIOS name information. It can be used to identify Windows machines on a network, as well as gather information such as hostnames, MAC addresses, and workgroups.

The **‘nmap -sV 192.168.56.101’** command is an example of using the Nmap security scanner tool to perform a version detection scan on the IP address **192.168.56.101**.

- **nmap**: This is the command to invoke the Nmap security scanner.
- **-sV**: This option instructs Nmap to perform version detection on any open ports found on the target system.
- **192.168.56.101**: This is the IP address of the target system that Nmap will scan.

When you run this command, Nmap will attempt to discover any open ports on the target system and identify the services running on those ports by performing a version detection scan.

The **nmap -p 1524 192.168.56.101** command is an example of using the Nmap security scanner tool to perform a port scan on the IP address **192.168.56.101**, specifically checking for the presence of an open port with port number 1524.

- **nmap**: This is the command to invoke the Nmap security scanner.
- **-p 1524**: This option instructs Nmap to scan only port 1524 on the target system.
- **192.168.56.101**: This is the IP address of the target system that Nmap will scan.

When you run this command, Nmap will attempt to discover whether the port number 1524 is open on the target system. If the port is open, Nmap will report it as an open

port, along with any additional information about the service running on that port. This type of scan is useful for determining which ports are open on a system and can help in identifying potential vulnerabilities or weaknesses that may exist.

- **nc**: This is the command to invoke the **nc** (short for netcat) tool.
- **192.168.56.101**: This is the IP address of the target system to which you want to connect.

When you run this command, **nc** will attempt to establish a connection to the target system. If the connection is successful, **nc** will open a command-line interface where you can send and receive data to and from the remote system.

- **uname**: This is the command to invoke the **uname** tool.
- **-a**: This option instructs **uname** to display all available information about the system

When you run this command, uname will output a series of system information, including:

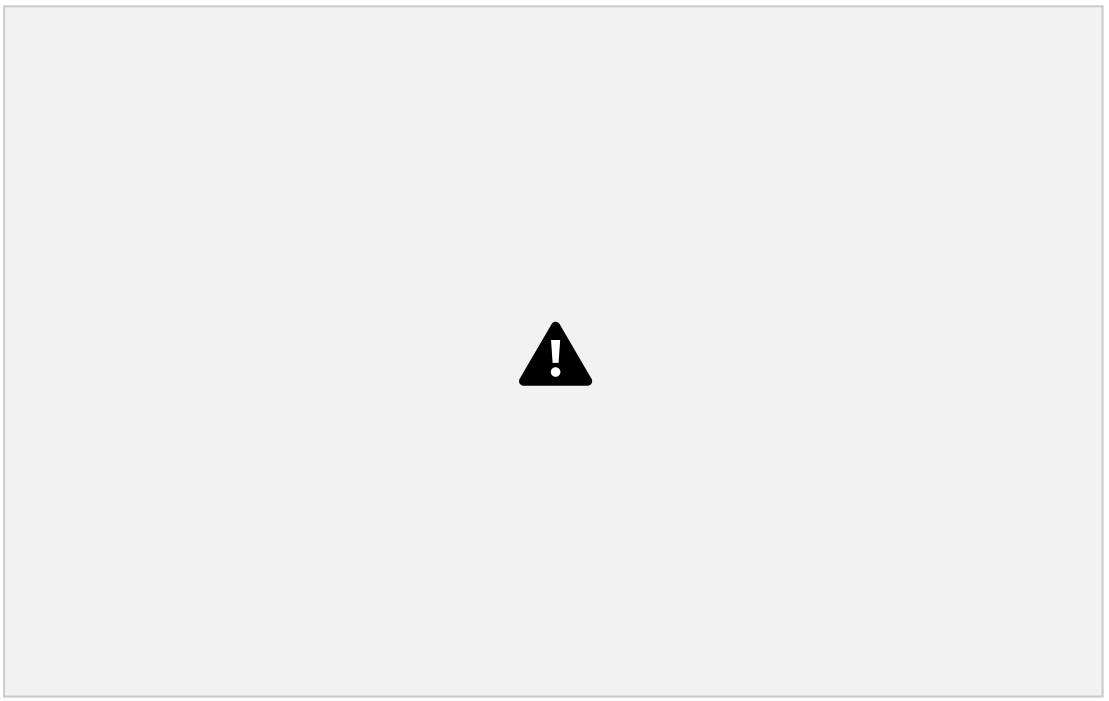
- Linux: This is the kernel name of the system.
- hostname: This is the name of the system.
- x86_64: This is the machine hardware name.
- GNU/Linux: This is the operating system name.

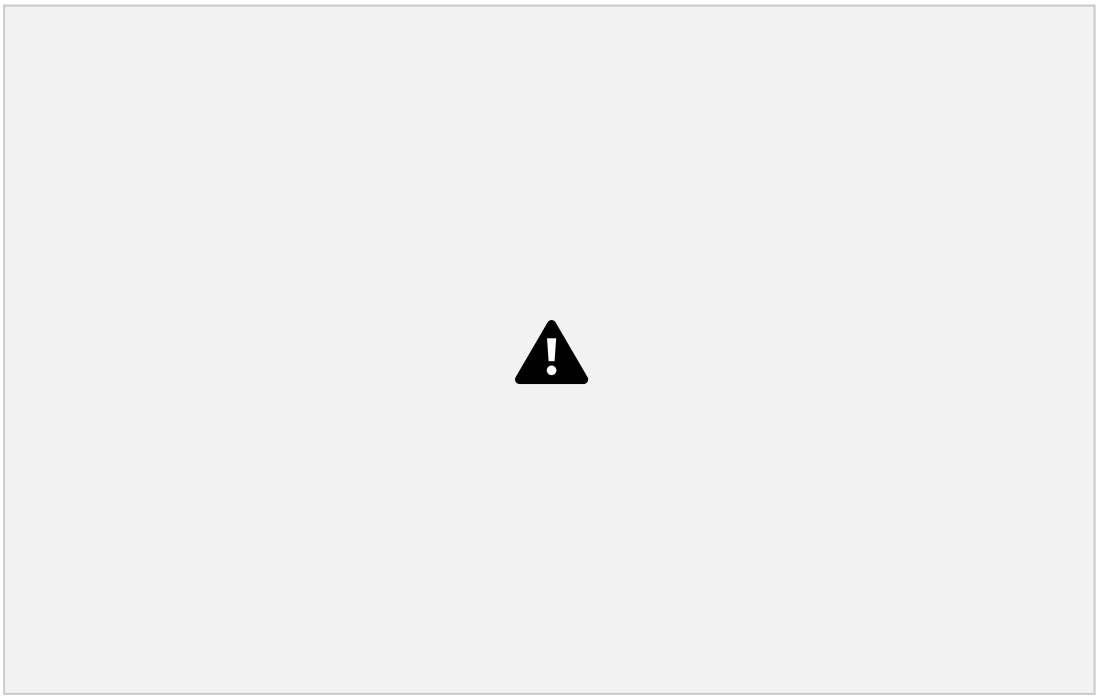
uname -a provides a quick way to obtain detailed information about the system's kernel and operating system, which can be useful for system administration and troubleshooting purposes.

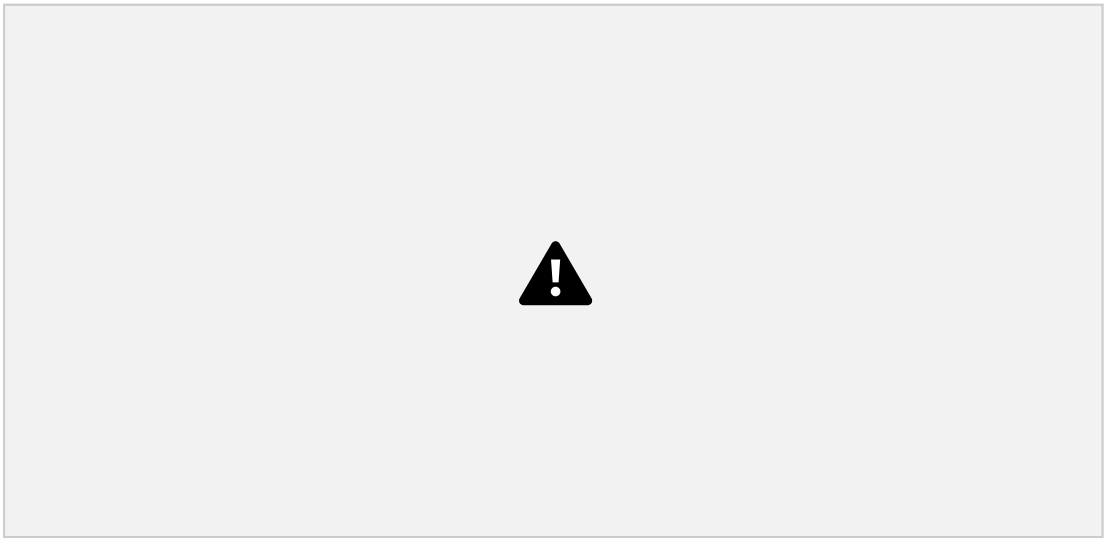
the '**whoami'** command is a simple command that is used to print the username of the current user who is logged in to the current terminal session.

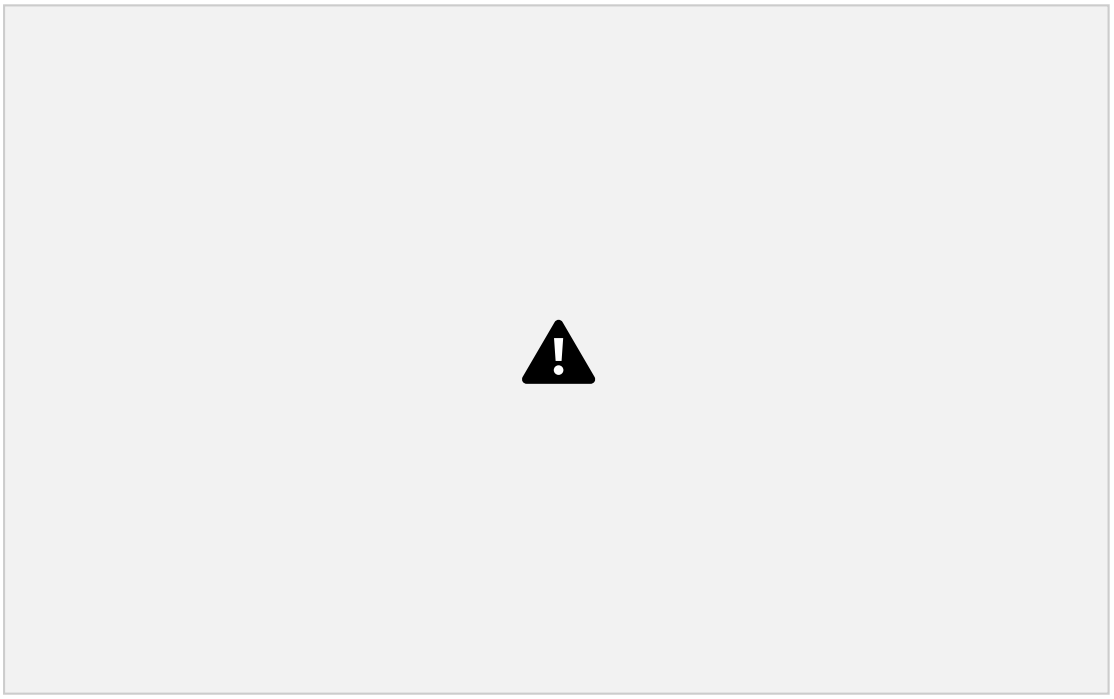
4c) Exploiting Metasploit using HTTP

First check the IP of the metasploitable, then enter the command nmap -sV 192.168.56.102 to check the port which is open. Then check for http, set the rhosts, payloads, show options and at last hit run or exploit.

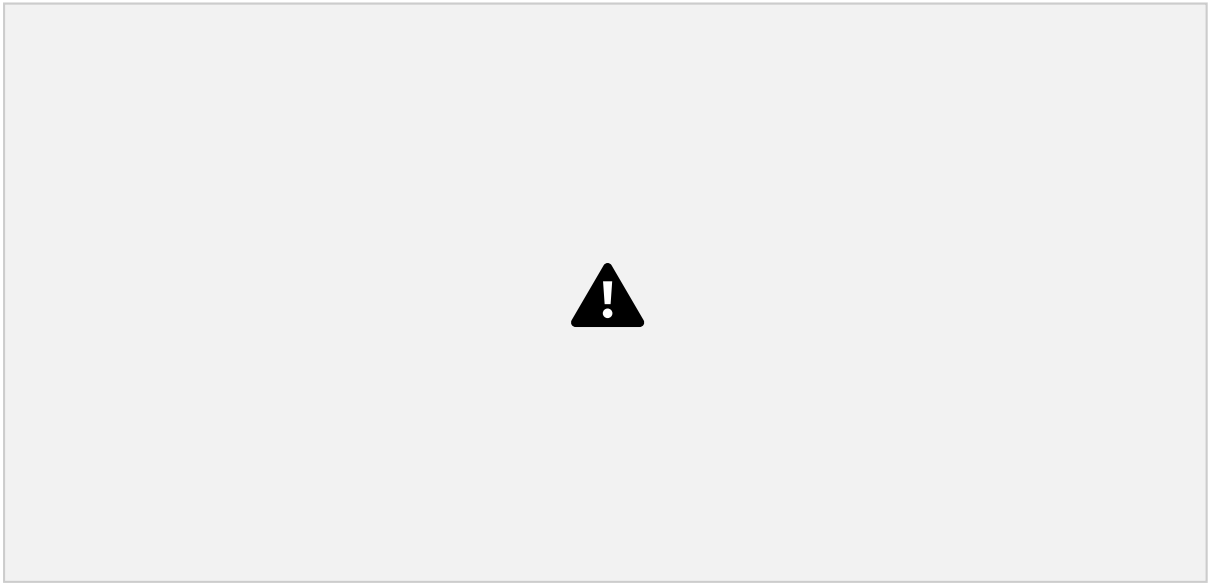


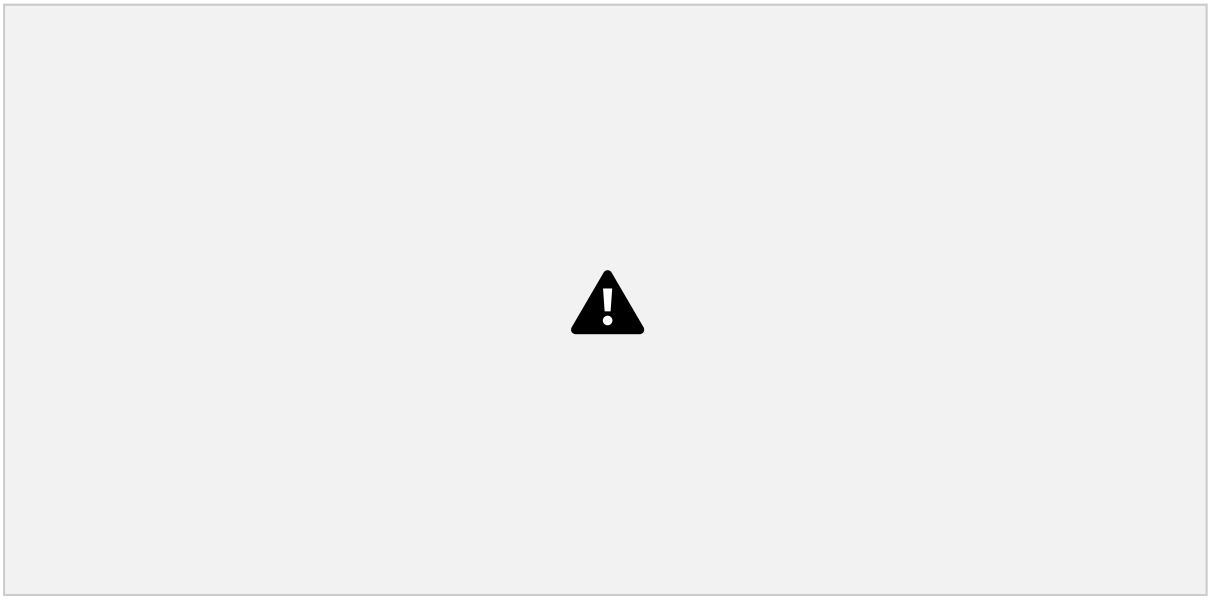






5) Network scanning using following nmap commands:





nbtscan is a network scanning tool used to identify NetBIOS names and gather information about Windows-based systems on a network. The command "nbtscan 192.168.56.0/24" instructs nbtscan to scan the network range from 192.168.56.1 to 192.168.56.254 (which is the /24 subnet mask) for NetBIOS names and related

information.

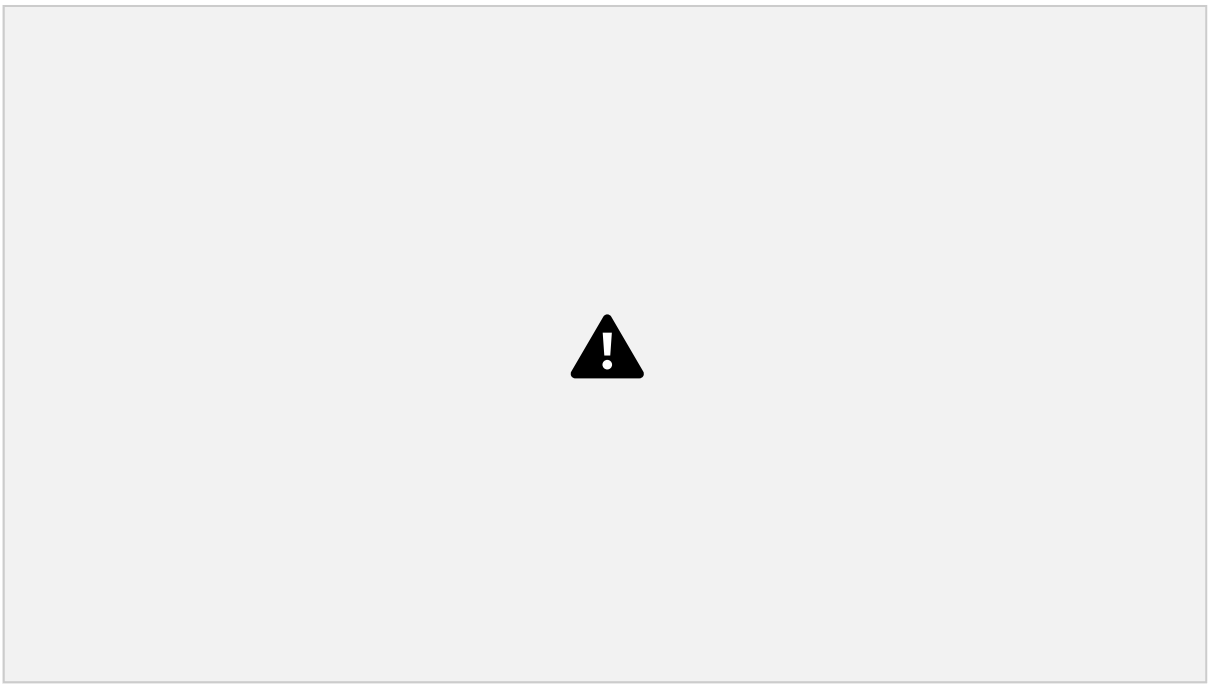
nmap is a network scanning tool used to identify hosts and services on a network, as well as gather information about them. The command "nmap 192.168.56.0/24" instructs nmap to scan the network range from 192.168.56.1 to 192.168.56.254 (which is the /24 subnet mask) for open ports and services running on hosts.

a) nmap -p

The command "nmap -p 21,22,23 192.168.56.101" instructs nmap to scan the host with IP address 192.168.56.101 for open ports 21, 22, and 23. Ports 21, 22, and 23 correspond to the FTP (File Transfer Protocol), SSH (Secure Shell), and Telnet protocols respectively. By scanning for open ports on a target host, nmap can identify which services are running and potentially vulnerable to attacks.

b) nmap -sV

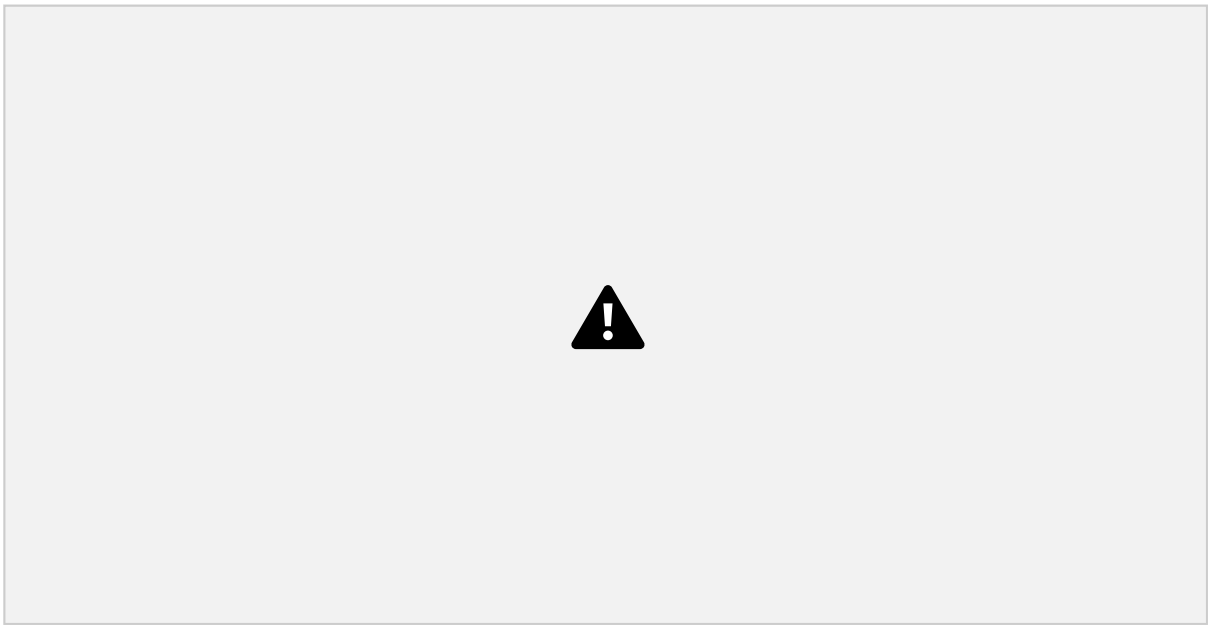
The command "nmap -sV 192.168.56.101" is a command-line tool used for network exploration and security auditing.



c) nmap -sT

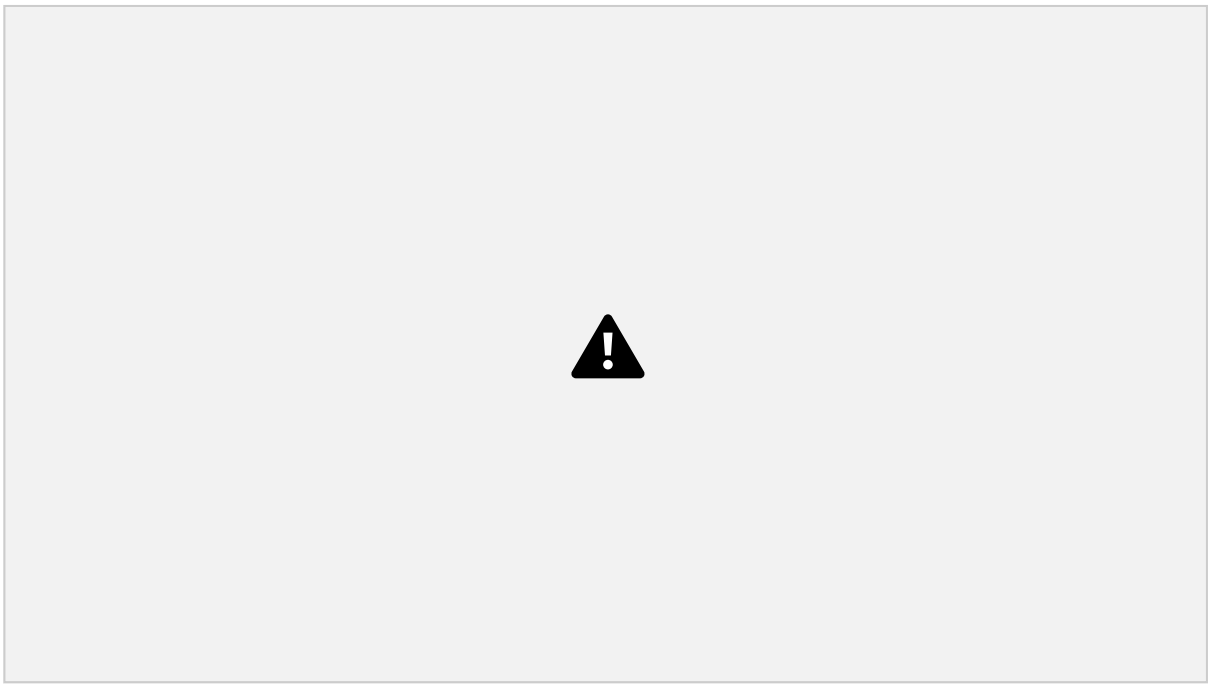
The command "nmap -sT 192.168.56.101" instructs nmap to perform a TCP connect scan on the host with IP address 192.168.56.101.

The **"-sT"** flag is used to specify that nmap should use a TCP connect scan technique.



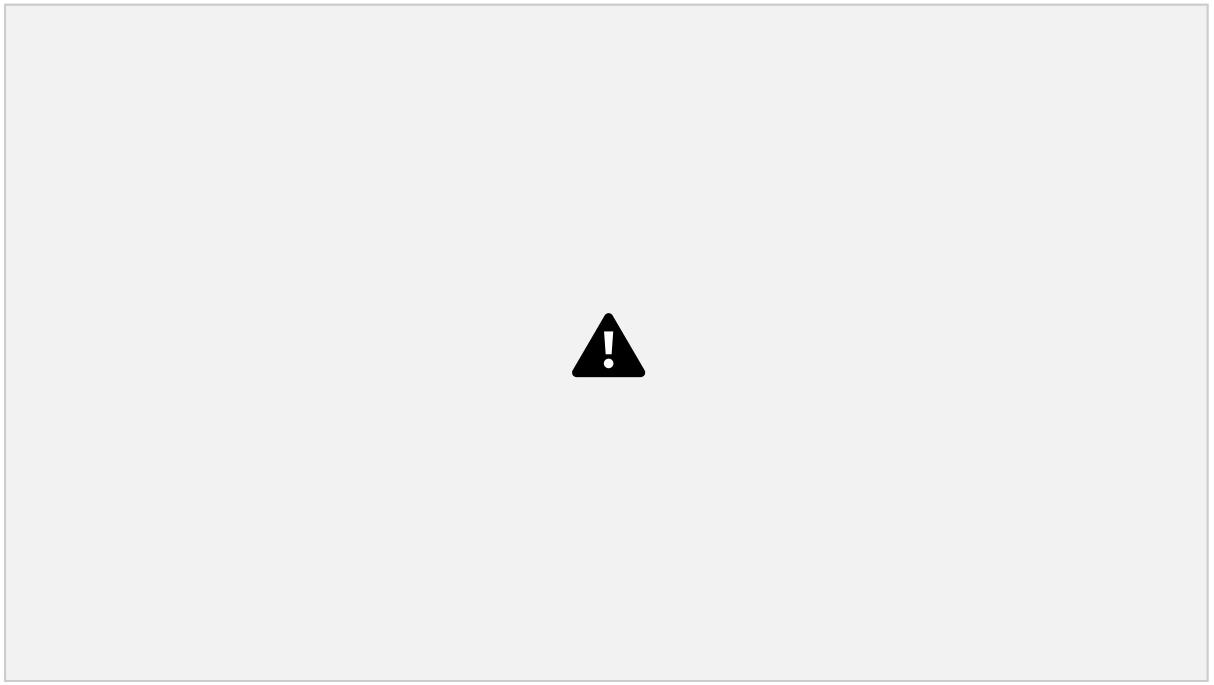
d) nmap -O

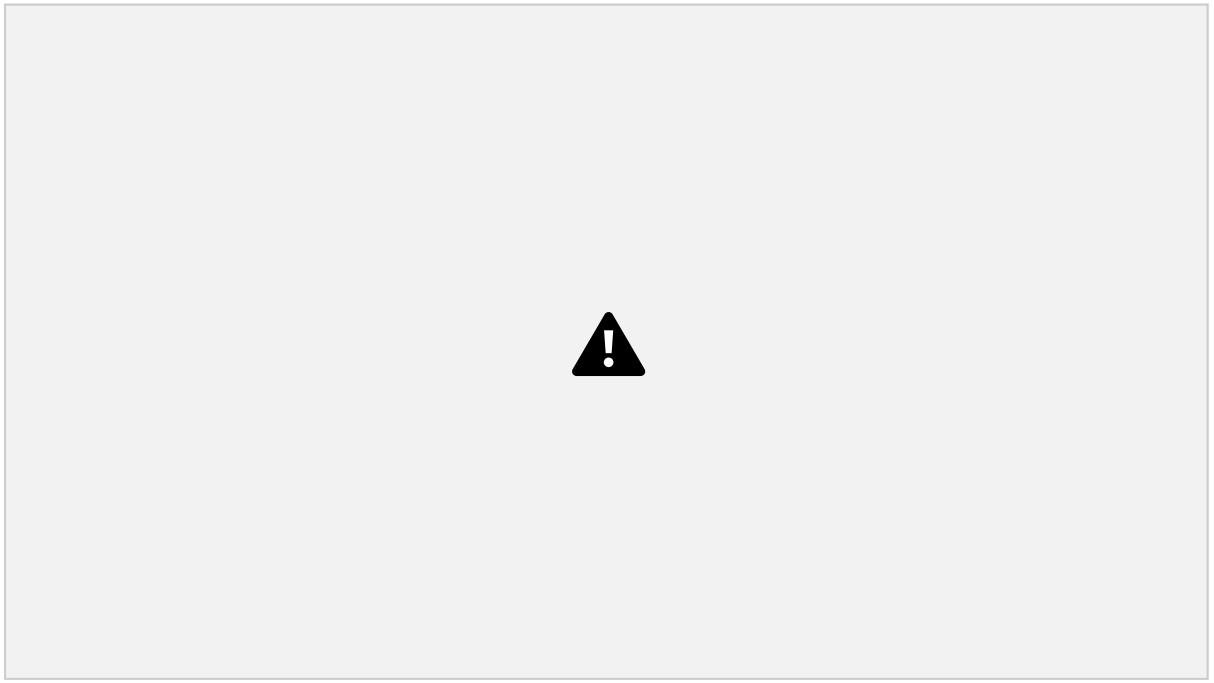
The command "nmap -O 192.168.56.101" instructs nmap to perform an operating system detection scan on the host with IP address 192.168.56.101. The "-O" flag is used to specify that nmap should perform an operating system detection scan.



e) nmap -A

The command "nmap -A 192.168.56.101" instructs nmap to perform an aggressive scan on the host with IP address 192.168.56.101.
The "-A" flag is used to specify that nmap should perform an aggressive scan.





Fire extinguisher using cisco packet tracer

Fire Extinguisher project is done using the cisco packet tracer. Cisco packet tracer is a network simulation tool. This project is used to control the fire and to activate the filter when there is smoke detected beyond the range specified. To implement this, we required mainly 4 components they are the server, water sprinkler, smoke detector, and 3 cars that emits the smoke.

Steps:

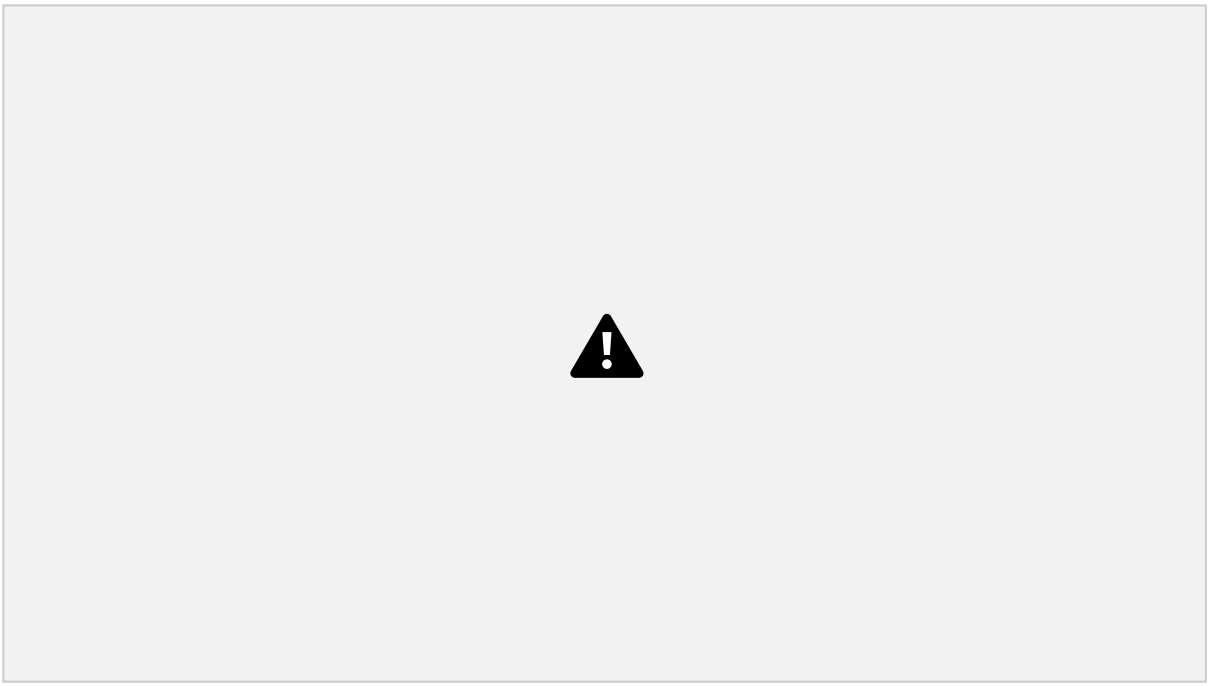
- Drag and Drop Server pt, Access point, Smoke detector, lawn sprinkler, old car3.
- • Rename Server pt as "Registration Server" and Rename lawn sprinkler as

"lawn sprinkler IOT-0".

- Double click on Access point and select config then select port1 and write "SSIO" in place of CISCO.
- Double click on server and select desktop then select IP config then select "static" & also write IPv4 as "1.0.0.1"
- Double click on Smoke detector and select config then select wireless0 and write "SSIO" in place of CISCO & also select IP config as "static" and IPV4 as "1.0.0.2".
- Double click on Sprinkler and select config then select wireless0 and write "SSIO" in place of CISCO & also select IP config as "static" and IPV4 as "1.0.0.3"
- Now connect access point to registration server using symbol

▪

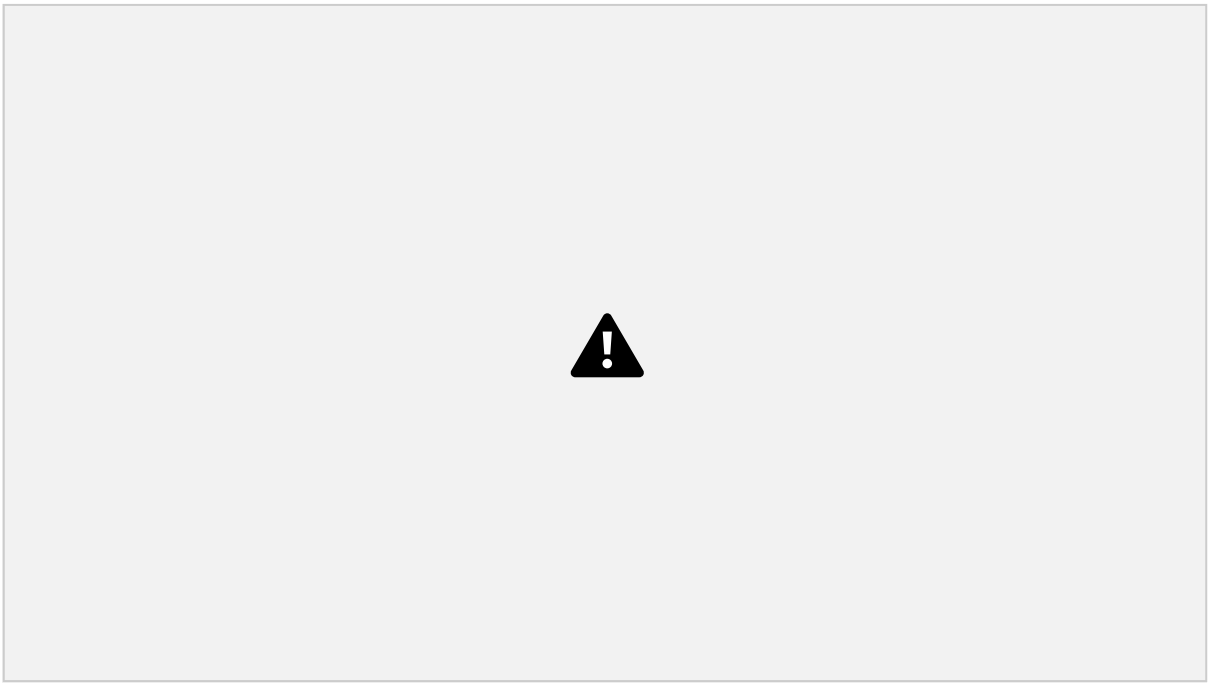
- Double click on Sprinkler and select settings and then Remote Server and write server address as "1.0.0.1", username:"admin" & password:"admin" and press connect.
- Double click on Smoke detector and select config and then select settings and then select Remote Server and write server address as "1.0.0.1", username:"admin" & password:"admin" and press connect.
- Add IP address for Registration Server as "1.0.0.1", Smoke detector as "1.0.0.2" & Lawn sprinkler IOT-0 as"1.0.0.3".
- Now double click on Registration server and select services and select IOT and select "on".
- Now double click on Registration server and select Desktop and select web browser and in URL type as "1.0.0.1" and press go.
- Now select "signup" and type username & password as "admin" then press create.
- Select "conditions" and select add and type name as "smoke on" and then set the level as ">=0.4" and select sprinkler status "true" and then press ok. Select "conditions" and select add and type name as "smoke off" and then set the level as "<=0.4" and select sprinkler status "false" and then press ok. •To obtain the smoke press ALT+ car.



Perform exploiting DVWA

a) Perform SQL injection on DVWA
b) Perform Cross-site scripting on DVWA
c) Perform File upload DVWA

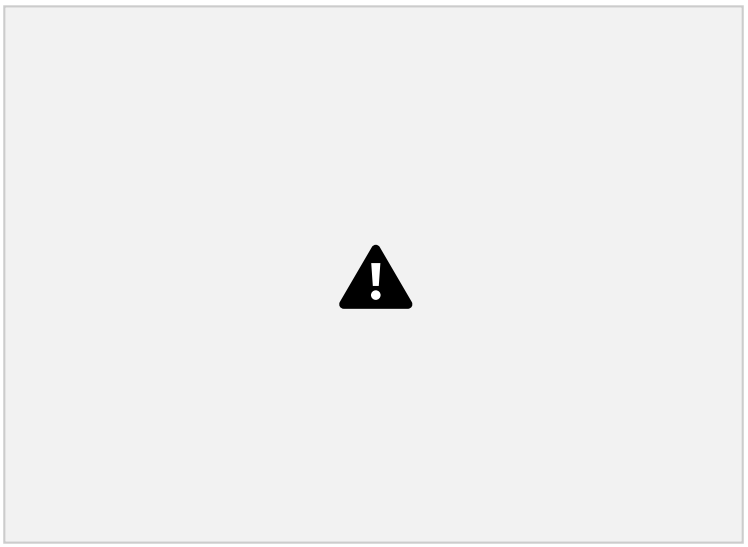
Step 1: Find the IP address of the pc using- ifconfig. Then find IP of Metasploit using - nbtscan.

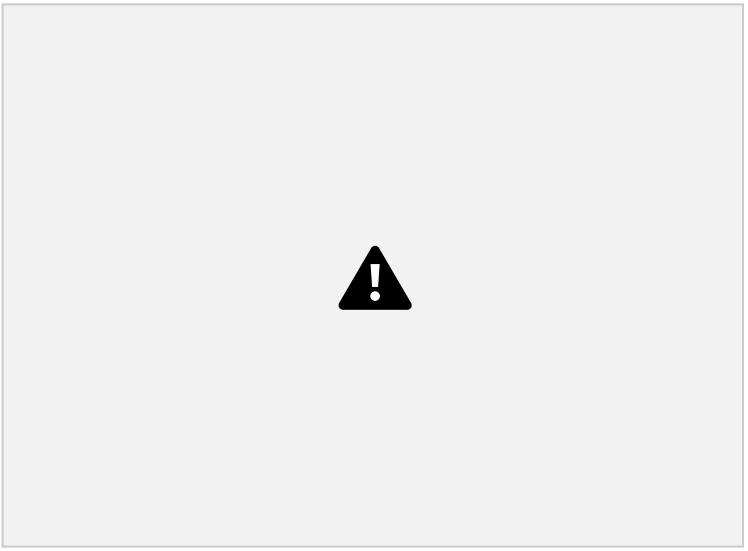


Step 2: Copy the IP of Metasploit and paste it in Firefox. Choose the DVWA in order to find the vulnerabilities.

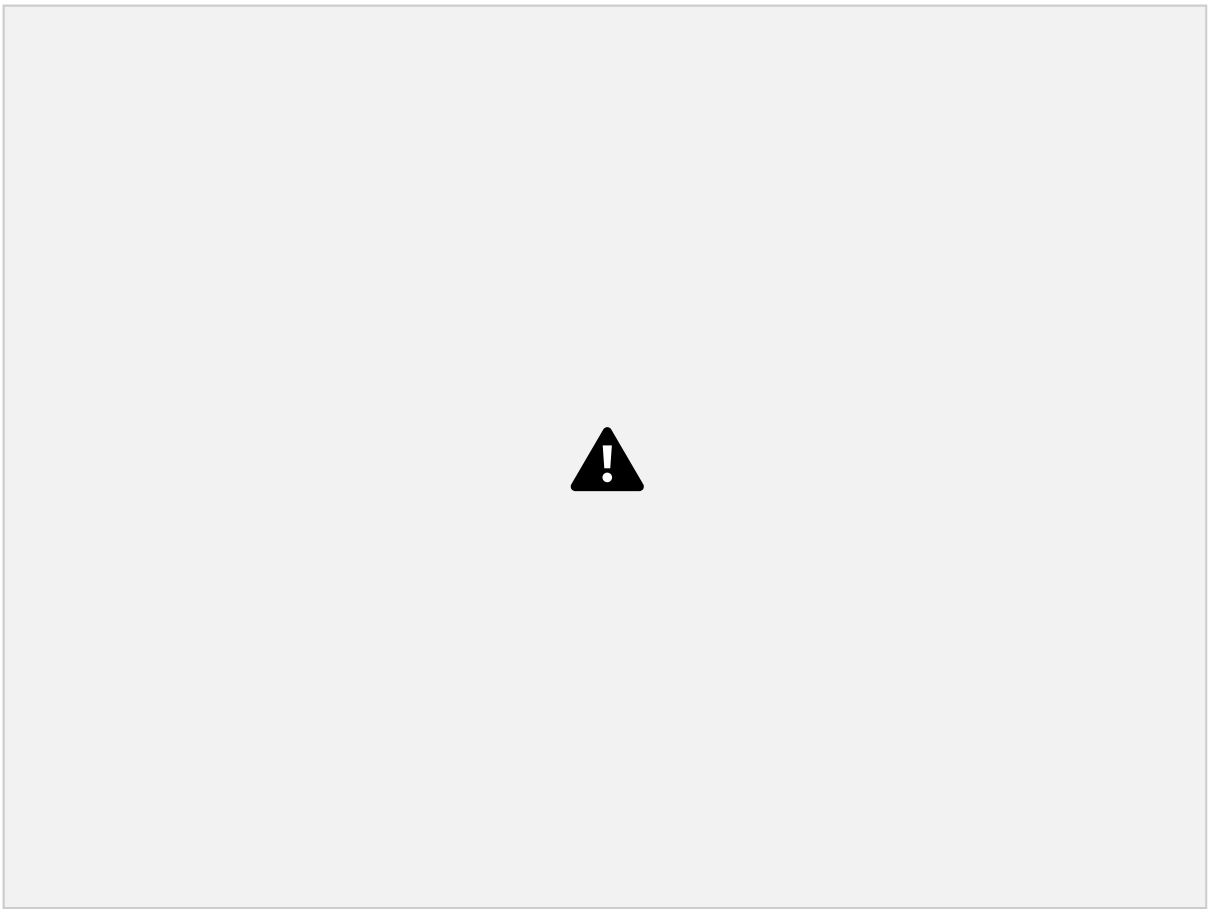
Enter the username and password –

(ie. username: admin, password: password)

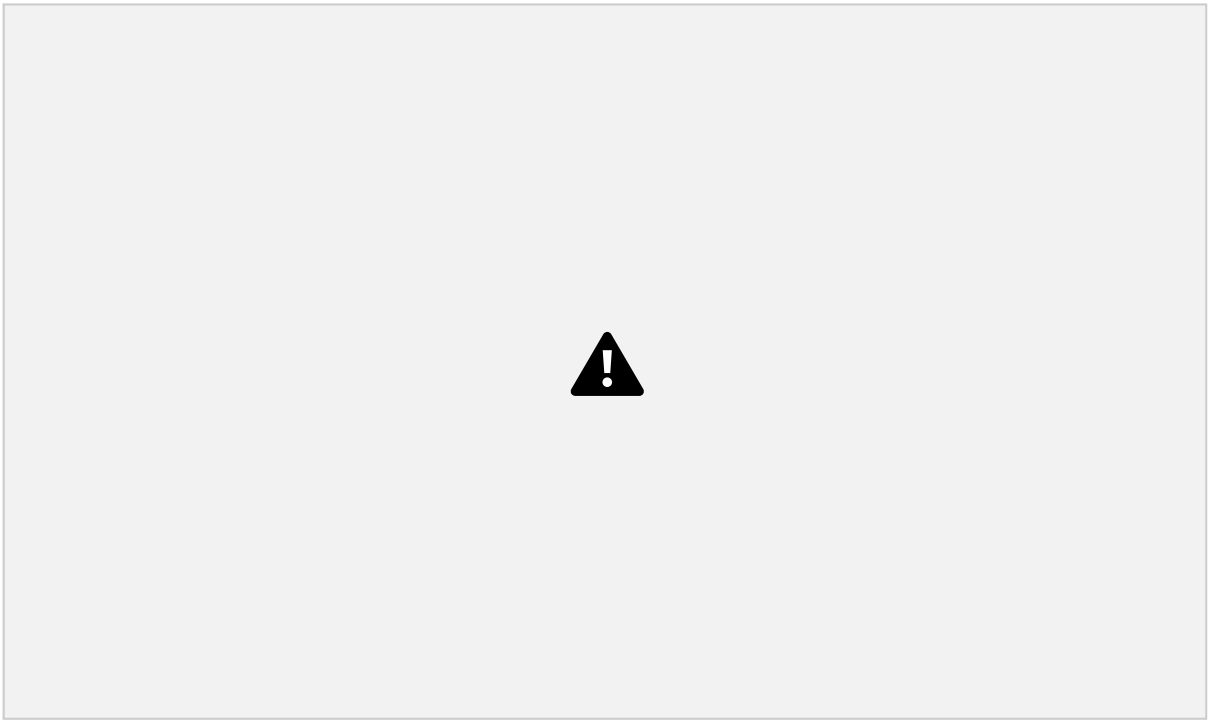




Step 3: Set the DVWA security to low.

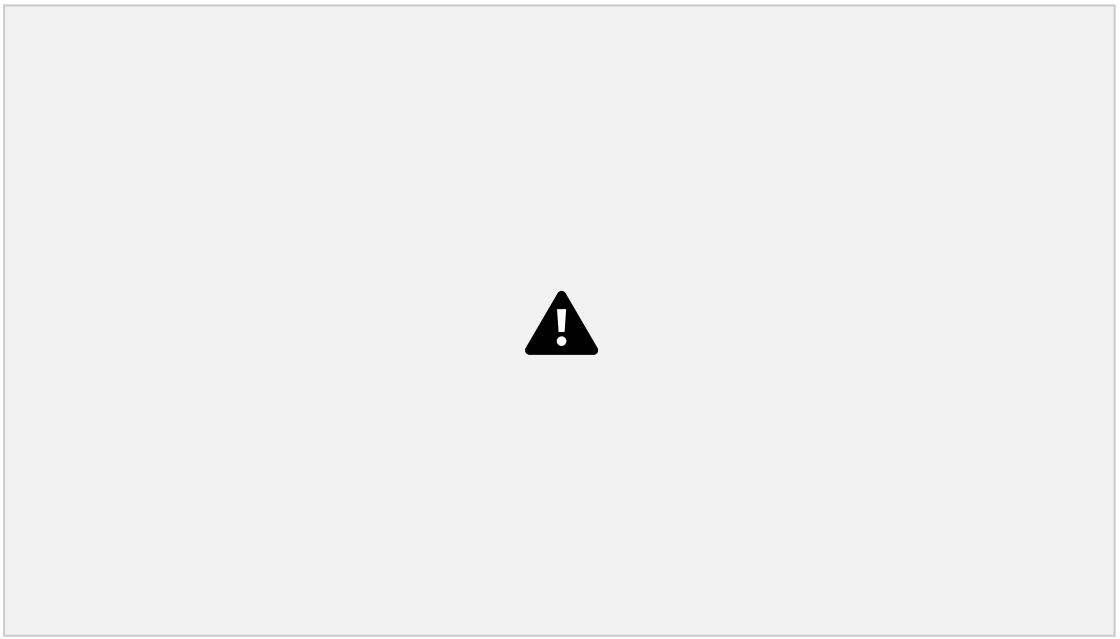


Step 4: SQL Injection – Process by passing the queries, so that we can get unauthorized access.



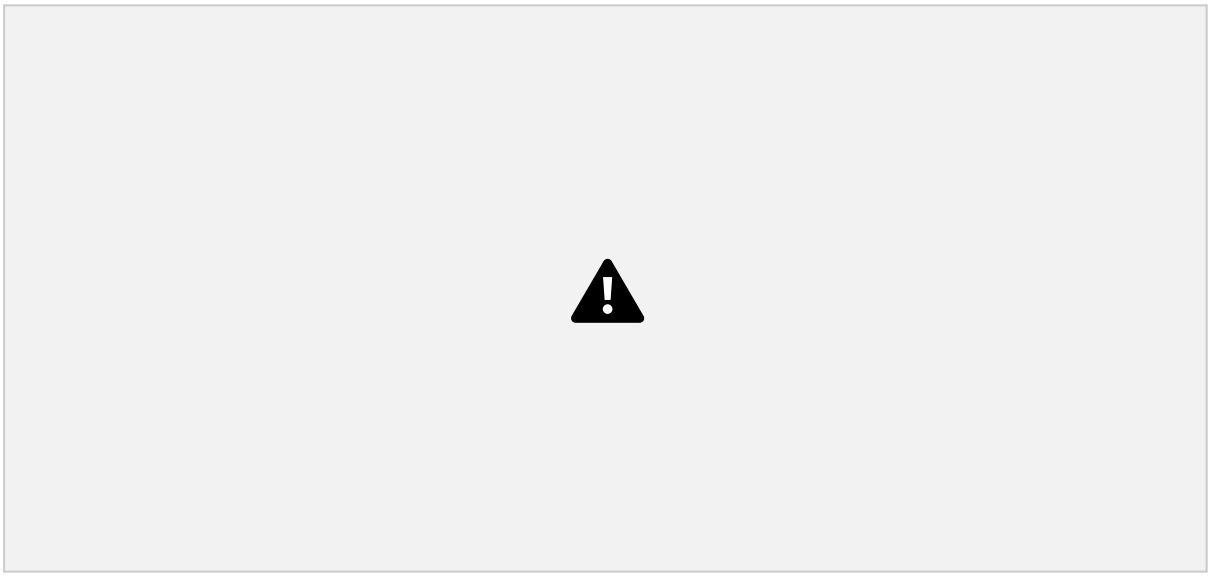
Step 5: SQL Injection (Blind)- also a kind of SQL injection used to attack data- driven applications using SQL statements.

SQL statements are inserted into an entry field for execution.



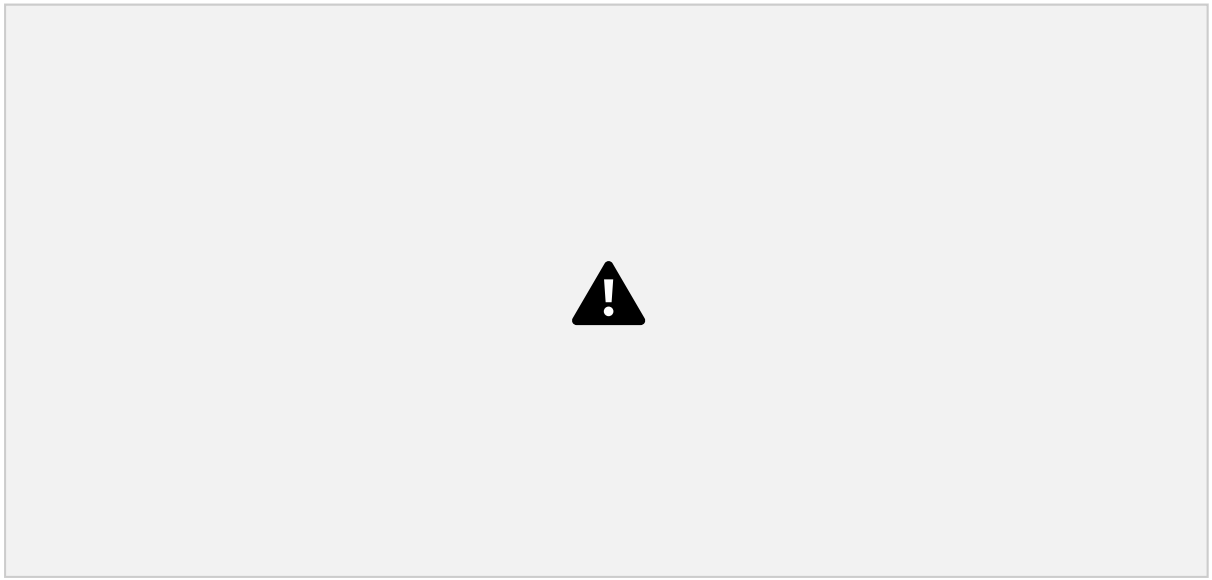
Step 6: XSS reflected-Used to add the script
<script>alert(“hacked”) </script>

This change will be for temporary period of time.
Step 7: XSS stored -Used to add the script but the effect here is permanent.



Step 8: To check the vulnerability in the upload. We can upload any files that cause damage or hacking.

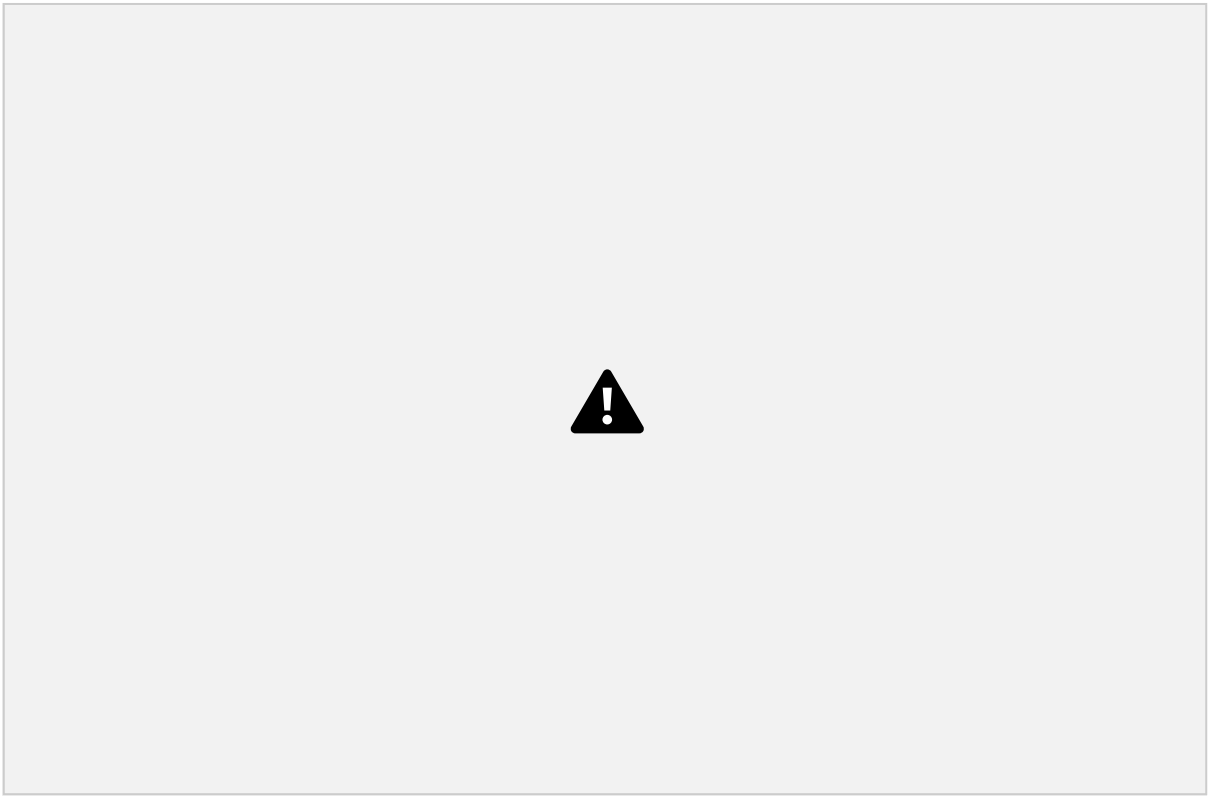
i.e. If the website or any form doesn't specify the document type we can easily add any scripts or txt format in order to hack.



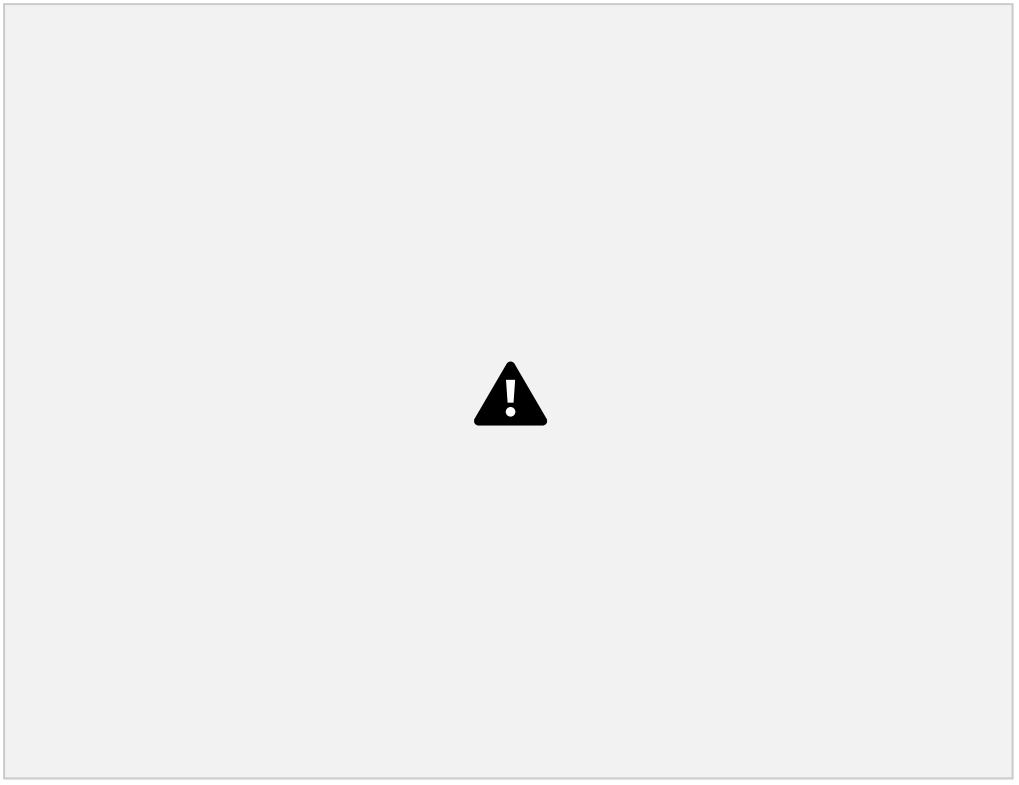
Perform Sniffing using Wireshark in Kali Linux

Wireshark is a popular network protocol analyser that allows you to capture, view, and analyse network traffic in real-time. It is an open-source software tool that can be used to troubleshoot network issues, identify security vulnerabilities, and analyse network performance.

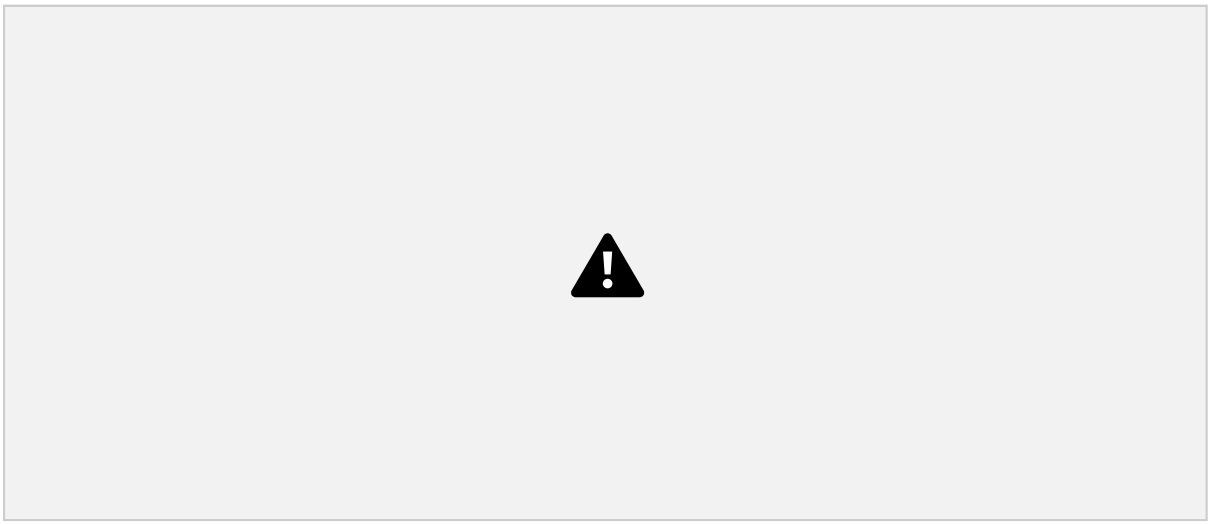
Step 1: Login to kali as root user and type Wireshark.



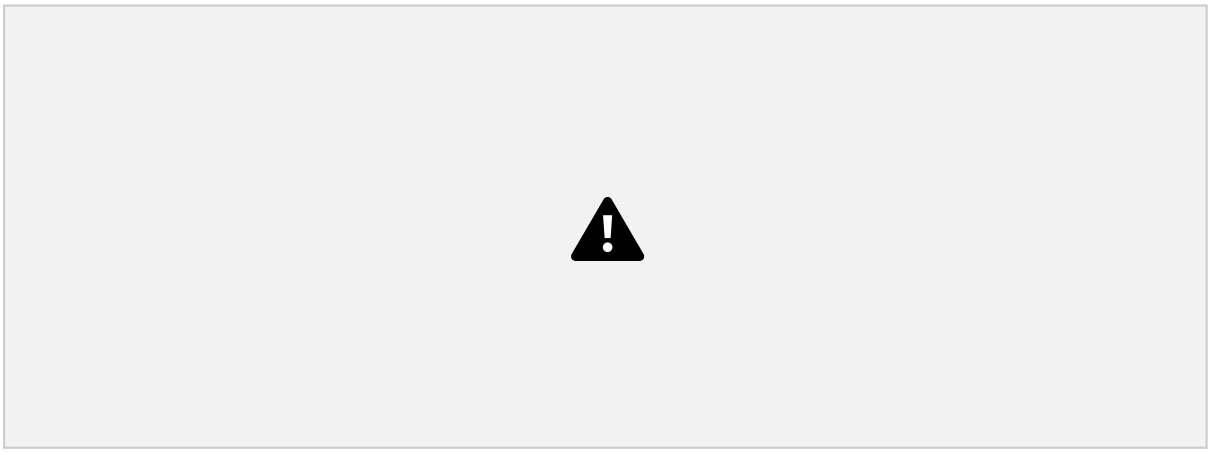
Step 2: Wireshark Network Analyzer will be opened and double click on eth0 (1st option).

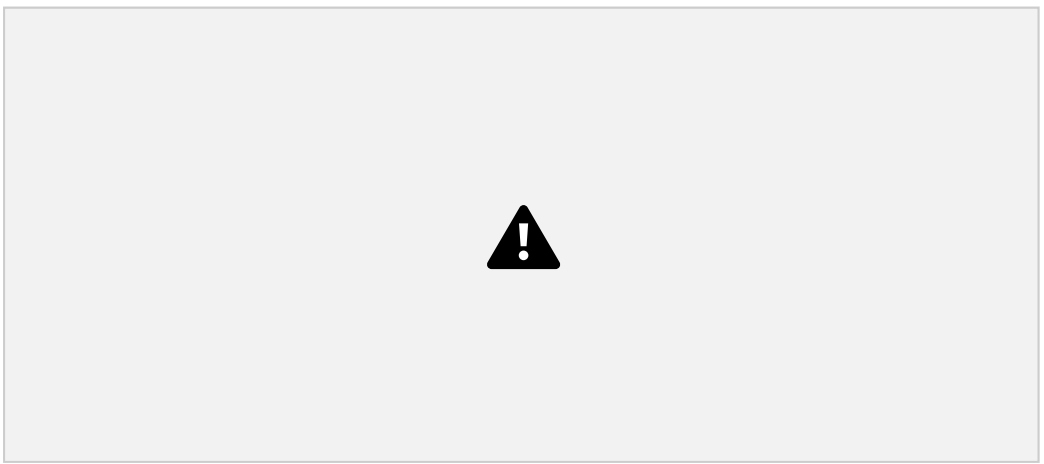


Step 3: Go to Firefox and search **testfire.net**

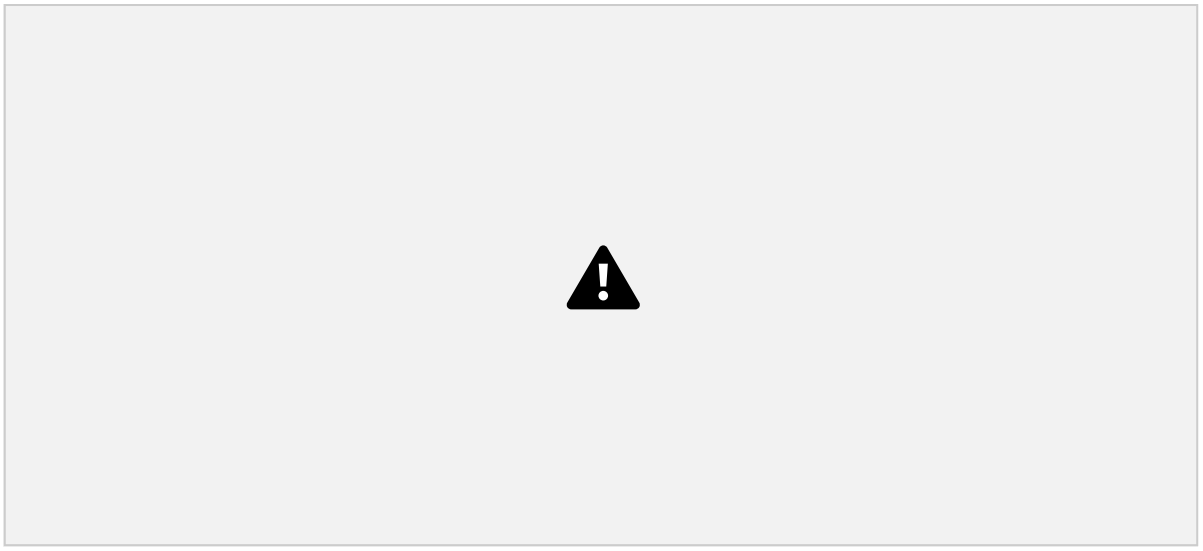


Username: **admin** Password: **admin**





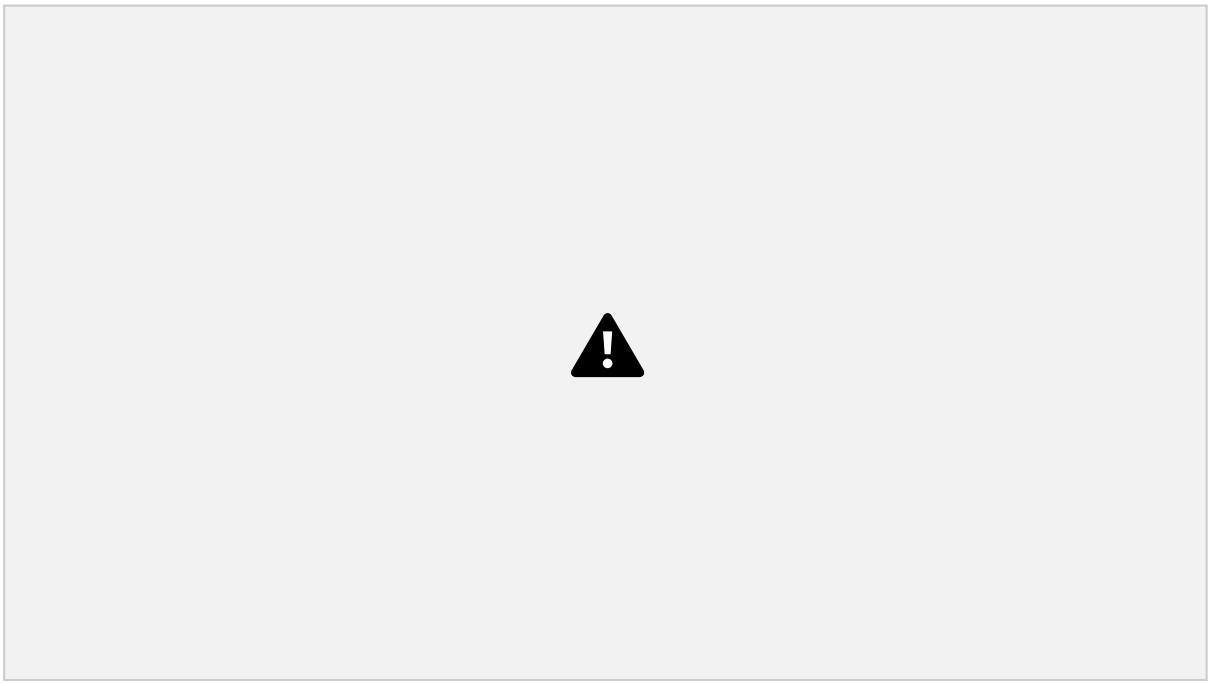
Step 4: Go to wire shark and in search bar filter http -post. By clicking last option, you will get the password and username we able to crack it.



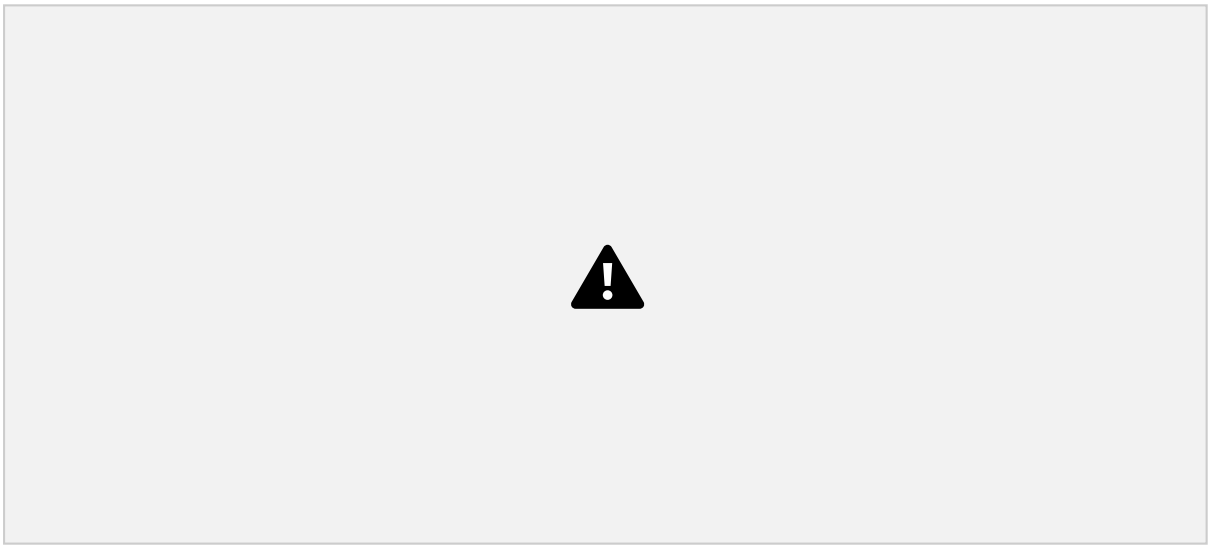
Perform Sniffing using Ettercap in Kali Linux

Ettercap is an open-source tool that can be used **to support man-in-the-middle attacks on networks**. Ettercap can capture packets and then write them back onto the network. Ettercap enables the diversion and alteration of data virtually in real-time.

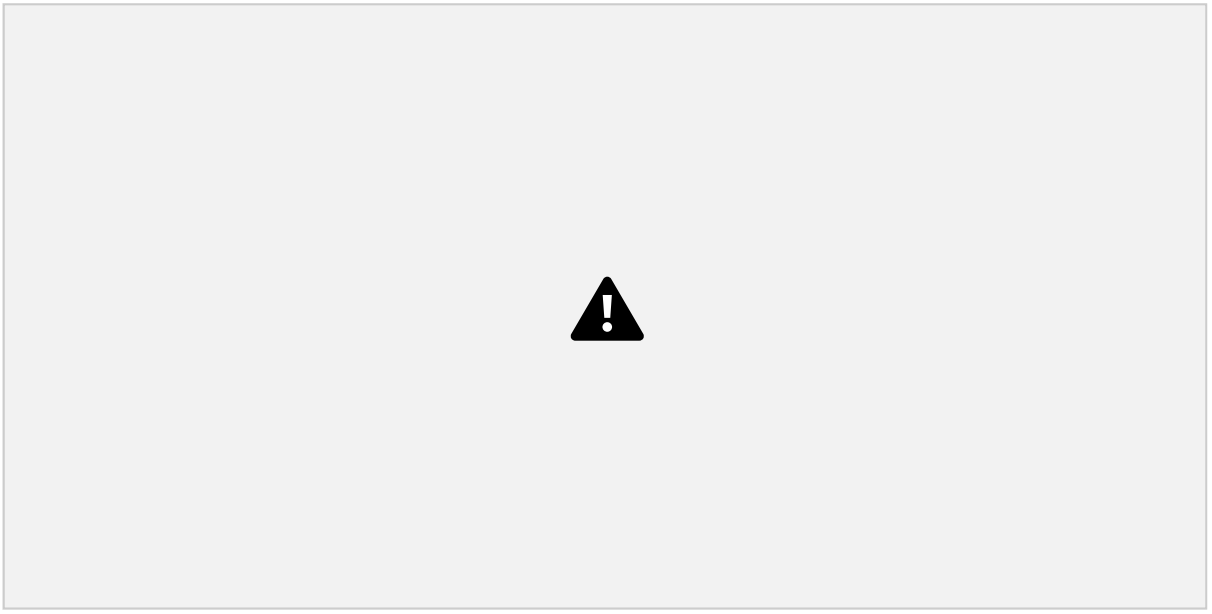
Step 1: To perform **Ettercap** turn on Meta, Windows7 and Kali-Linux.



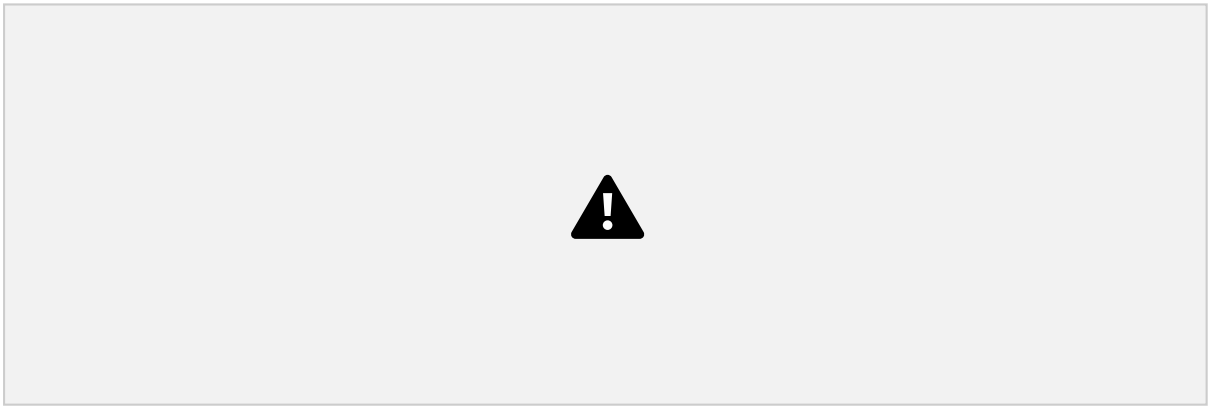
A pop-up window appears on the screen and now click the ☐ mark.



Step 3: Select three dots in the top right corner then select hosts -> scan for the hosts from the page displayed below.



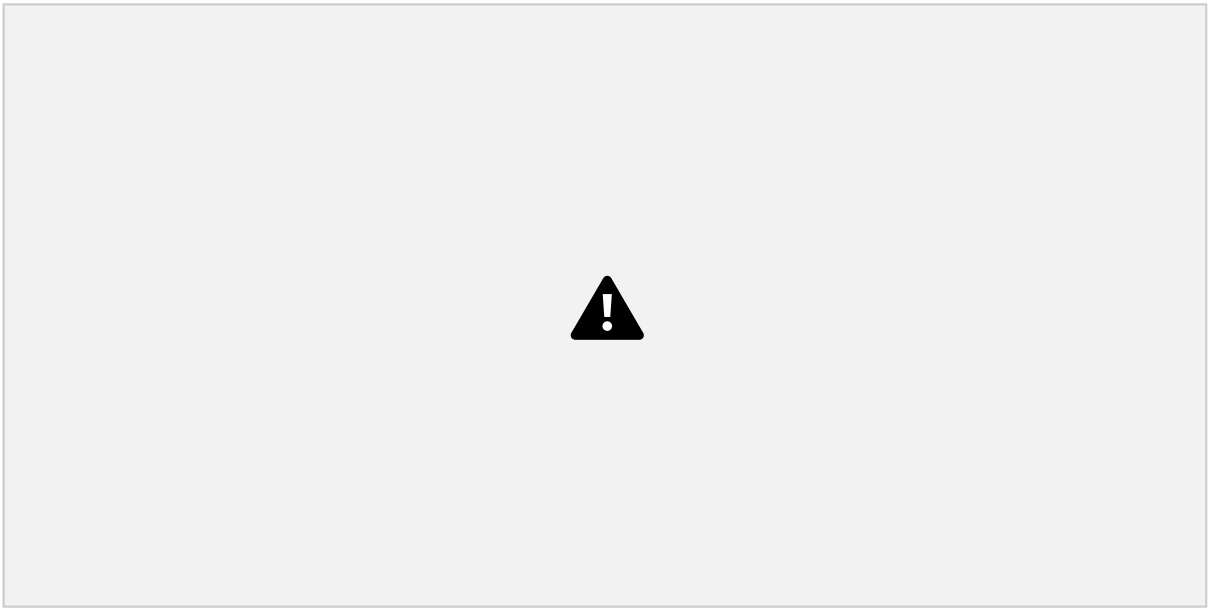
Then again select 3 dots -> hosts -> host lists and the below window will display



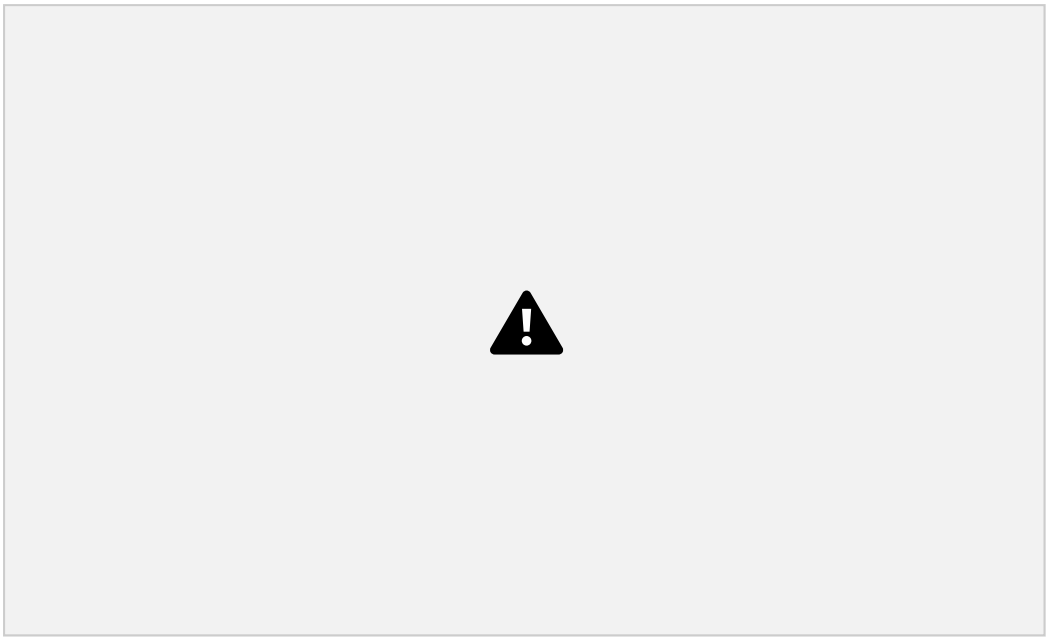
Select the IP of windows7 [192.168.56.103] and add to target1 and select IP network of Metasploitable [192.168.56.101] and add to target2.

Step 4: Select ARP poisoning from the drop-down menu on clicking globe icon. In ARP poisoning attacker sends falsified ARP messages over a LAN to link an attacker's MAC address with the IP address of a legitimate computer or

server on the network.

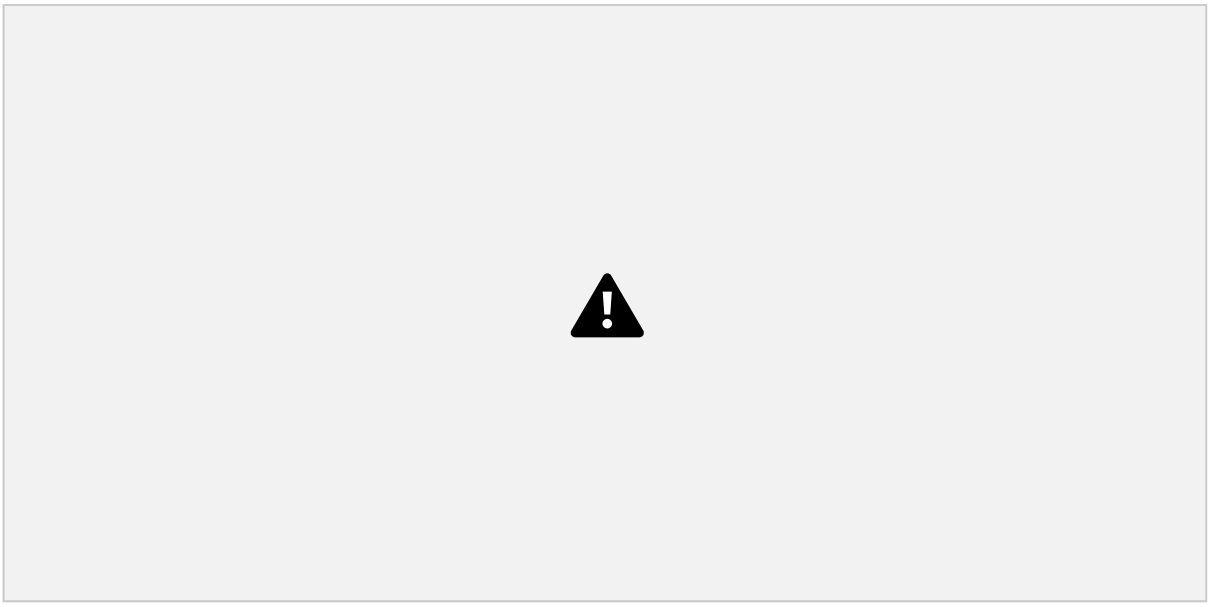


Step 5: Open Firefox in the windows 7 and browse the IP address of metasploitable machine and select DVWA option and enter the username and password to login.

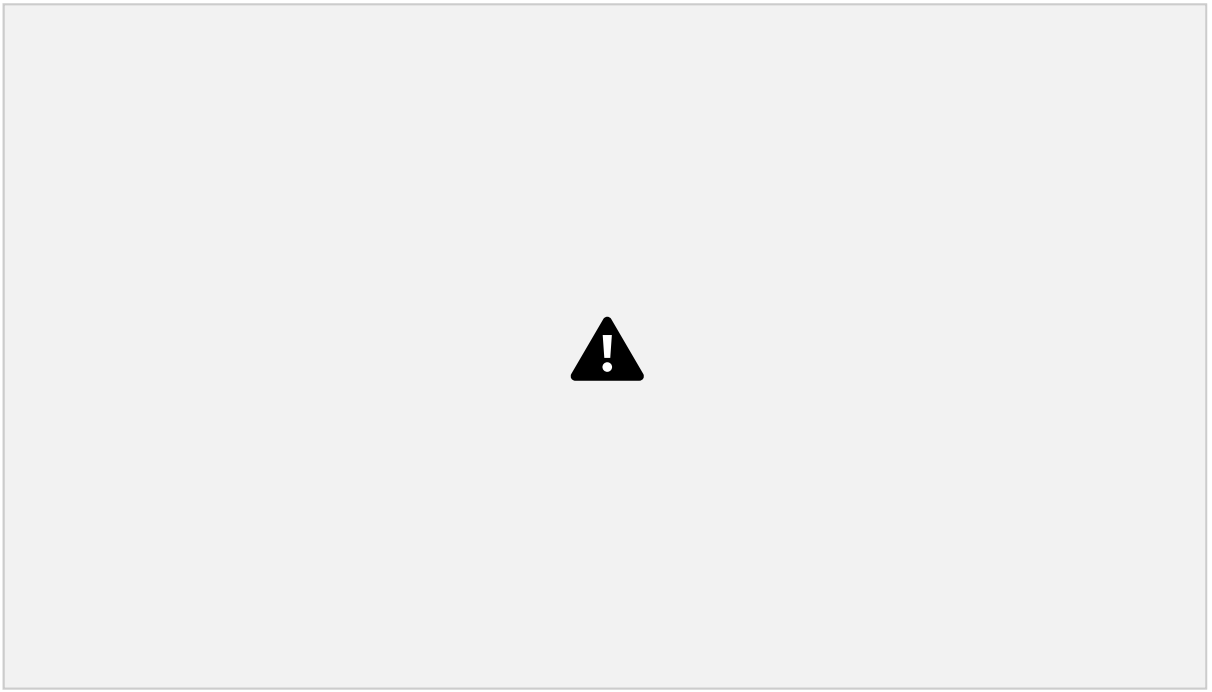


Step 6: Transfer packets from metasploitable machine to windows

7. [command: ping windowsIP]



Step 7: The entered username and password in Windows 7 will be now visible at Kali-Linux. By this successful sniffing between Windows7 and Metasploitable machines done using **Ettercap** tool.



CONCLUSION

This is my report after I completed my internship at DLithe. It was a great experience for me to learn beyond my academics. It was fabulous opportunity for me to learn and gain knowledge before I enter my professional life. When I started my internship, I was asked to learn or become familiar with Linux. Later, the team did and was affected with the project through.

It was my first experience in the internship where I got set of protocols, about the communication with other people, being professional talking skills.