### Me, In Cyber Security as an Ethical Hacker.

#### Life of a Ethical hacker as a Beginner

#### Hello viewers, I am ****SRIVISHNU C S**** a computer science student doing post graduation in Computer Application. I am more passionate about ethical hacking and networking.

As a child, i was very curious about how the people are able to login or accessing the personal device without knowing their detail. This made to look over the cyber security domain and to explore more about hacking devices and securing my own device. So, to explore more on this domain, i joined **Dlithe Consultancy Service Pvt Ltd.** as a intern in Cyber Security and Ethical hacking.

This Blog is going to be straight, long and is updated everyday about new techniques involving online and offline attacks and different hacking techniques.

#### ETHICS OF ETHICAL HACKING:

* As a professional ethical hacker he/she should not perform hacking for personal benifits or to showoff in front of your friends and family.
* Hacking someone’s machine or device to steal data is offensive.
* An ethical hacker should always uses his/her skills and technique to protect ourself and others from any type of frauds.

As a intern, today(02–03–2022) is the first day. I am going to describe my story of learing ethical hacking from my mentor in straight and simple way.

**What is hacking?**

An hacking is a process of exploring methods for breaching defencses and exploiting weakness in a computer system or a network.To perform hacking there are two team involved.

* Red Team
* Blue Team

Red Team:- This is a team who involve in using offensive approach to identify vulrenabilities for targeted machines.

Blue Team:- This is a team who involve in using defensive approach to stop hackers from stealing information from a system.

TOOLS AND HARDWARE SPECIFICATION OF HOST SYSTEM

* Virtual Machine Software.
* Kali linux or any other Hacking OS.
* MetasploitTable.
* Windows 7 OS(for Victim hacking)
* 8GB RAM(Minimum)
* Stable network connection.

Build your own hack lab form your machine. add all the tools to virtual machine if you don’t use Linux or other Hacking OS as root OS.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

TOPICS:

* Phases of hacking.
* why hacking is equals to robbery?
* Ports and services.
* Vulnerability Scanning.

**PHASES OF HACKING**

In the real world, there are five phases of hacking. They are as follows:

* Information gathering.
* Exploitation.
* Privilege escalation.
* Creating a backdoor.
* Clearing the tracks.

1. **INFORMATION GATHERING:**

It means gathering different kinds of information about the target. There are two types of information gathering, they are as follows.

a. Active: collecting information directly from the target. It has high accuracy for information but, the risk of getting caught is very high.

b. Passive: collecting information through third party. It has low accuracy for the information but, the risk of getting caught is very low.

**2. EXPLOITATION:**

Exploitation is the act of selfishly taking advantage of someone or a group of people in order to profit from them or otherwise benefit oneself.

**3. PRIVILEGE ESCALATION:**

Privilege escalation is a type of network attack used to gain unauthorized access to systems within a security perimeter. Attackers start by finding weak points in an organization’s defenses and gaining access to a system.

**4. CREATING BACKDOOR:**

A backdoor is a malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.

**5. CLEARING THE TRACKS:**

This involves modifying or corrupting or deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.

**WHY HACKING IS EQUALS TO ROBBERY?**

In the world of cyber security, the term hacking is referred to accessing someone’s system without their knowledge. But, for a true ethical hacker, hacking is the skill which he/she uses to protect/educate/build awareness about not getting into any losses.

Most of the skilled hackers use their knowledge for their own benefits like getting into someone’s account and stealing their money. there are many online frauds happening every second, hence hackers are termed as robbers in the modern world.

for example,

Hacker=Robber

Computer/server=bank

data=Money

**PORTS AND SERVICES**

Ports : Are the doors of a computer through which the data enters and exit. each computer has 65535 ports per NIC

Services: A network task that is running on a computer

Process / Protocol: set of rules (Services)  
Actual medium where the content / data is passed is Ports:

Service + Ports : Communication from Server to client.

address for the packet to send / receive . Socket = IP : Port number

ex: [192.168.1.10:8080](http://192.168.1.10:8080/)

Port Scanning: Identifying the ports of the target computer to fetch information about the target computer.

Information can be gained using Port scanning:-  
Ports Open.  
Services running.  
Target Operating system.  
Some information which is being leaked.

**VULNERABILITY SCANNING**

Vulnerability scanning is the process of identifying security weaknesses and flaws in systems and software running on them. This is an integral component of a vulnerability management program, which has one overarching goal to protect the organization from breaches and the exposure of sensitive data.

To learn this part more effectively please go through the below links:

how to find vulnerabilities? PART-1

<https://www.youtube.com/watch?v=keer2qQxWRQ&list=PLXvO0GafEUZJ9a1qtxyWUI3VYRfZRgiYY&index=2&t=223s>

Setting up the hacking lab

how to find vulnerabilities? PART-2

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

BASIC LINUX COMMANDS:

**$pwd:** print work directory.  
**$mkdir <directory name>:** creating directory.  
**$cd <path>:** change directory.  
**$cp <src\_path> <destination\_path>:** copies the source file to some other destination file.  
**$mv <src\_path> <destination\_path>:** copy and replace, can also be used for renaming file.  
**$rm <filename.extension>:** delete the file if it is present in the same directory. else, to specify the path.  
**$touch <filename>:** creates a text file with the given filename.  
**$ls <file\_path>:**lists the files inside the directory.  
**$ls -la:** lists the files with its attributes.  
**$ifconfig:** shows all interfaces and its information, including IP and Mac address.  
**$cat <filename.extension>:** displays the content of the text file.  
**$head <filename.extension>:** displays the starting n lines of the text file.  
**$tail <filename.extension>:** displays the ending n lines of the text file.  
**$file <filename.extension>:** shows what type of the file specified.  
**$id:** displays the current user’s id and permissions.  
**$whoami:** show as which user you have been logged in.  
**$uname -a :** shows the kernel info.

**NMAP**

Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection.

Using nmap, we can scan some of the ports available in destination system. This process is called as port scanning.

The following things can be achieved from the port scanning.

* opened Ports.
* Service running.
* Target OS.
* Some Information which has been leaked.

To achieve the above above steps using nmap, there are several steps which are as below.

**STEP-1:** first identify the victim/destination machine’s IP address. To get the destination IP address, there are several way such as,

* sending links through image or video or by other documents.
* By using victims machine itself we can able to find out the IP address. The risk of getting caught is very high.
* by joining the same network of which victim connected.

NOTE: This is only for education purpose. If anyone wants to do live demonstration of working of port scanning, please do it through the own lab setup. PUBLIC PORT SCANNING is a offensive crime under section 43(a) of the IT Act, 2000.

**STEP-2:** After identify the IP address of destination machine, there are several commands through which we can process the above things. The commands are:

* #nmap <Ip\_address>: used to check the open ports of destination machine.
* #nmap -P <specify\_port\_range> <IP\_address>: used for getting all the #ports available within the range specified.
* #nmap -sV <IP\_address>: used for service version scan.
* #nmap -O <IP\_address>: used to find target OS type.
* #nmap -sC <IP\_address>: used to trigger the target.
* #nmap -T4 -A <IP\_address>: used to do all thee operation at once.

STEP-3: The results will be available on the screen of open ports visible from target machine.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**What is a vulnerability in a system?**

the quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally. In general, these are the loopholes of target/any system through which an attacker can able enter and make any once system under their control.

To find the vulnerability of the system, there are may tools available over the internet. Some of the vulnerability scanner tools are,

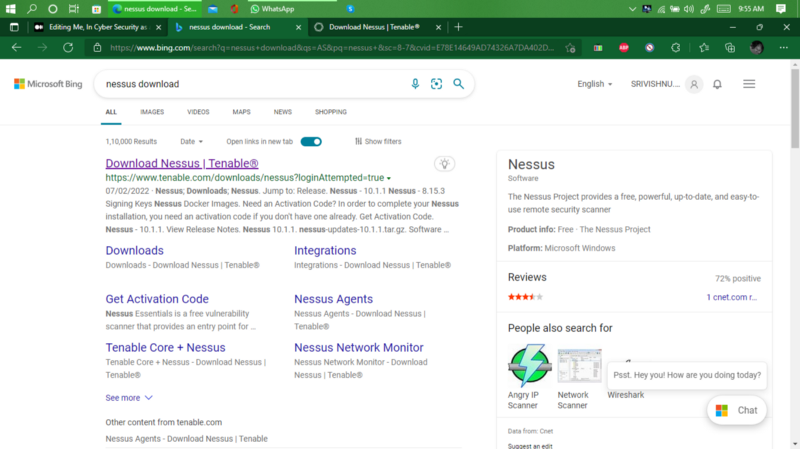
* OpenVAS.
* Nikto.
* Aircrack-ng.
* Nessus.
* Tripwire IP360 and many more.

In particular, I am going to use the NESSUS vulnerability scanner for scanning target IP address.

Step to Install a NESSUS tools in windows/kali Linux.

STEP-1: browse the name to the tool “NESSUS DOWNLOAD” in the search bar.

STEP-2: click on to the fist link.



after clicking the first link there will be several options of software for different OS. In that select .msi file extension for the windows and .deb file for kali.

STEP-3: Accept all the terms and conditions and press download option.

When download is complete, follow the procedure for both windows and kali OS.

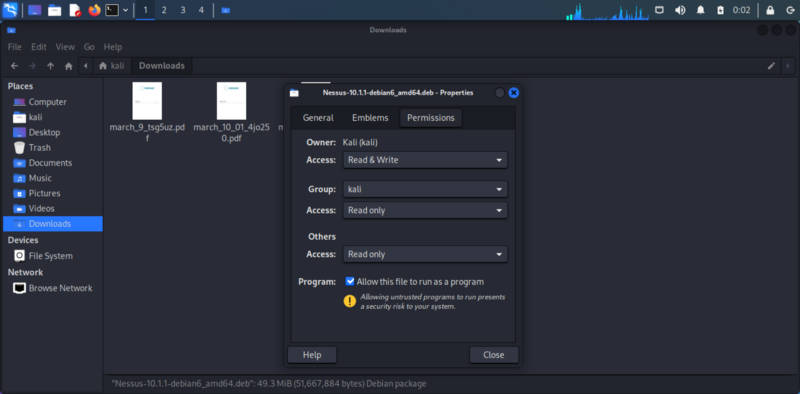
For Windows,

* Double click the downloaded file.
* Accept all the T&C’s from the company.
* Wait until all the plugins are Initialized and installed(it may take 1hr to complete the process).
* Now, you will be able to see the form where username, G-mail will be asked to send you the activation key. fill it and submit it.
* Check in mail for the activation key and copy the activation key and paste it.
* After doing that procedure you will be asked to create username and password. make sure you note it in book as Nessus has no privilege's to change user id or password.
* After successful login now you can use NESSUS in windows.
* To start NESSUS you need to start it in browser just by typing “ <https://localhost:8834/> ” and you will see the login page.

For Kali Linux,

* Right click the Downloaded file in your OS.

Go to Properties->permission->click the tick button which is showing Allow this file to run as a program as shown is below image.



Now, run the program.

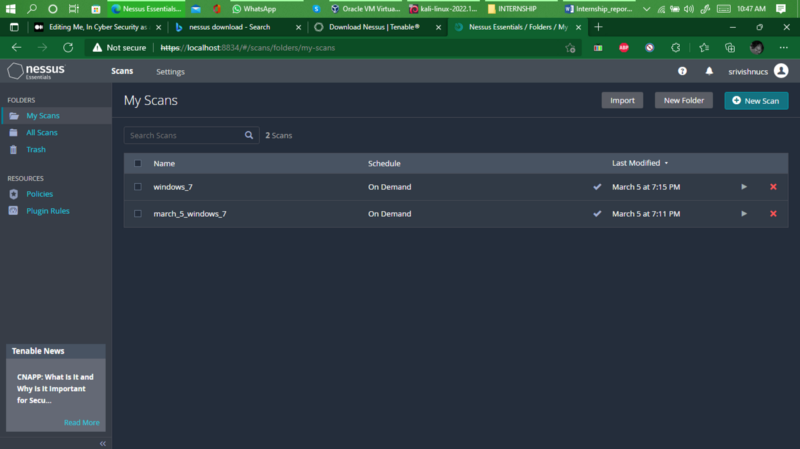
* Double click the downloaded file.
* Accept all the T&C’s from the company.
* Wait until all the plugins are Initialized and installed(it may take 1hr to complete the process).
* Now, you will be able to see the form where username, G-mail will be asked to send you the activation key. fill it and submit it.
* Check in mail for the activation key and copy the activation key and paste it.
* After doing that procedure you will be asked to create username and password. make sure you note it in book as Nessus has no privilege’s to change user id or password.
* After successful login now you can use NESSUS in Kali.
* To start the Nessus in kali every time first you need to open terminal as root. and type the following commands.
* #sudo service nessusd start //it start nessus in kali.
* Now, open browser and type [https://kali:8834/#](https://kali:8834/#?)/ to open Nessus.
* to stop Nessus, again go to terminal and type #sudo service nessusd stop

**How to scan vulnerability in Nessus?**

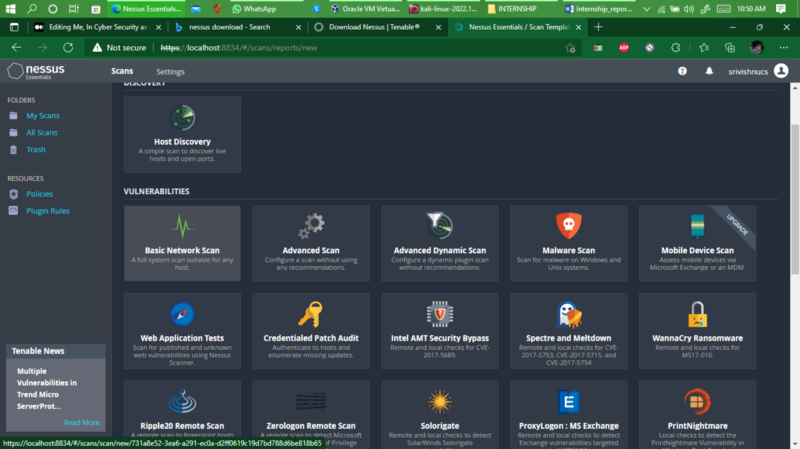
For that, you need the IP address of target machine. Ip address can be collected through many ways as i told in the beginning of this story.

After getting the Target machine IP address, OPEN Nessus.

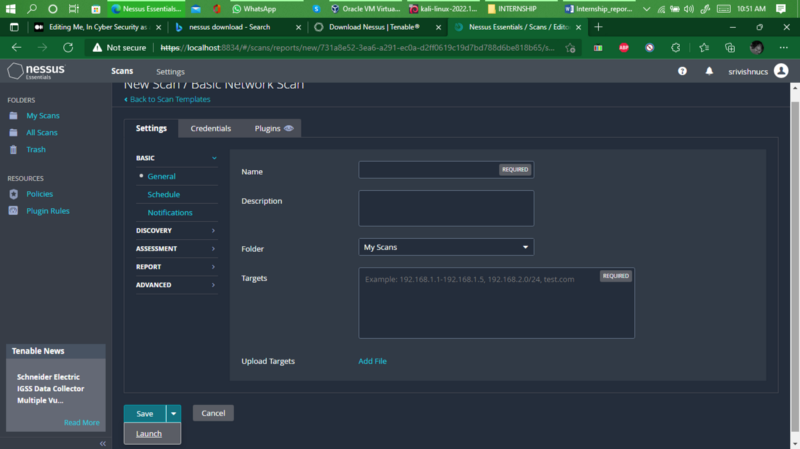
Now, you will be able to see the the NEW SCAN option at the top right corner of the window.



Now, Click on to the NEW SCAN and you will see the new window showing different types of scanning tools. In that Select BASIC SCAN NETWORK.



After selecting that fill the following details in next window.



NAME: “Give any name to initialize the scan”

DESCRIPTION: “can be any or empty”

TAGGET: “targets IP address”

Press launch button.

The scan will be completed and you will be able to see the Vulnerability of Target system.

STEPS TO GET CONTROL OVER VICTIM/TARGET MACHINE UNDER SAME NETWORK.

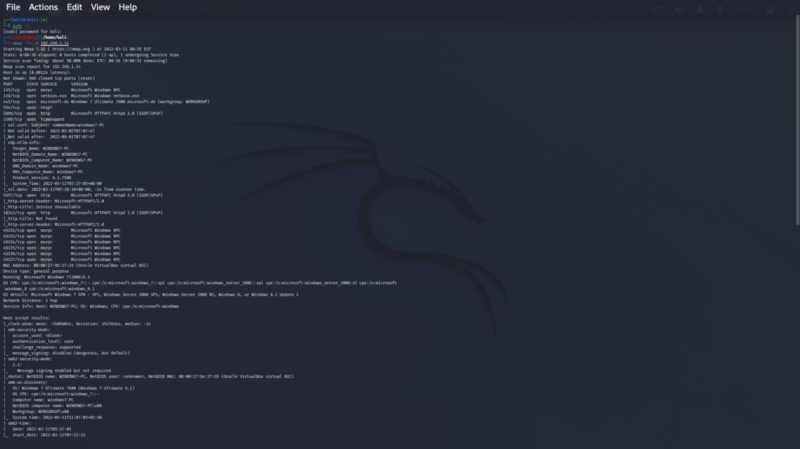
To do so, We need the IP address of the Target machine connected to network. For that use command **arp -a** in command prompt to see all connected network devices.

After getting the IP address, Scan for Open ports using Nmap. In my case My target IP address is 192.168.1.14.

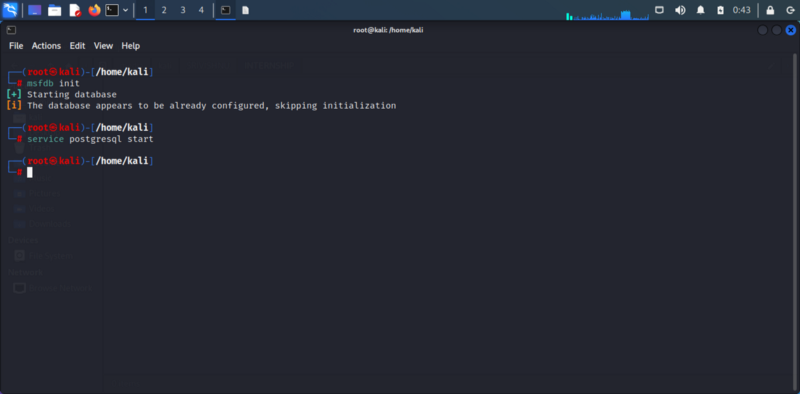
To check the communication between attacker and Target machine you can use PING command.

STEP-1: Scanning for open ports.

Below image shows you all open port present in target system and you can use any port to take control over it.



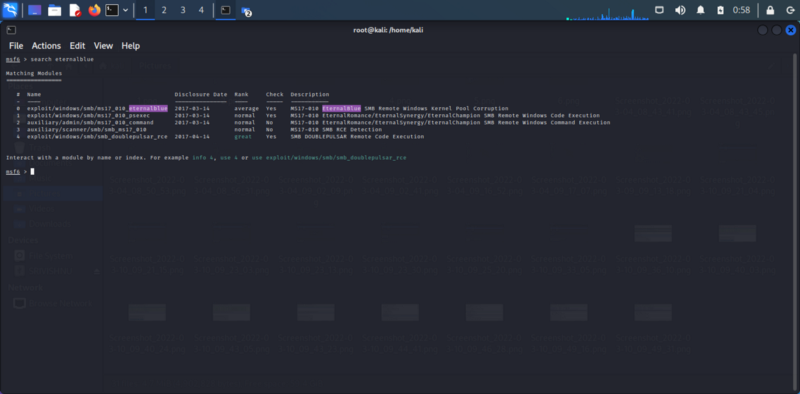
STEP-2: Turning on MSFConsole



STEP-2: now, find all the properties of port and for which it is used.

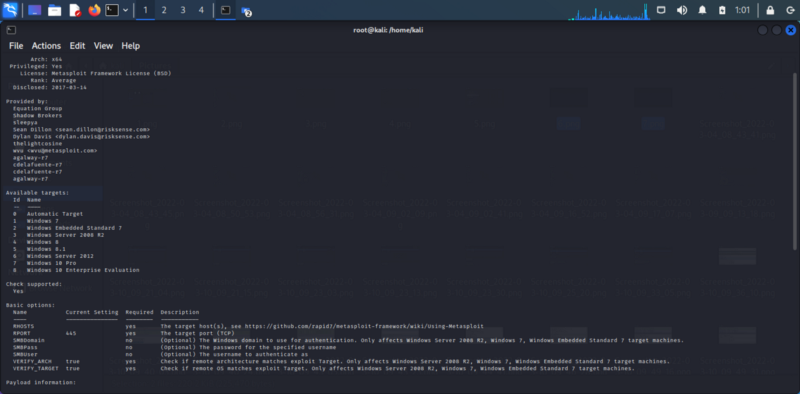
command is #show all. // it finds all port with path that can be used for getting control over target system.

STEP-3: In that, I am selecting PORT which has eternalblue vulnaralable.



STEP-4: check the detail of that port. whether it can be used for windows 7(victim machine) or not. for that use command.

#info <full path of the port>



In the image you can see the targets foe which this works and it indicates that we can use it for getting control over target machine.

STEP-5: set RHOSTS to your target IP address Machine

#set RHOSTS <IP\_ADDRESS>



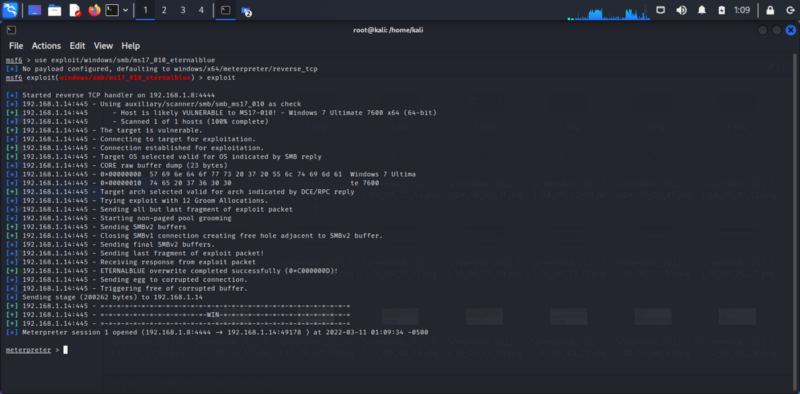
To check whether RHOSTS is set or not use INFO command.

STEP-6: Use that file path.

#use <full path of the port>

After this command the curser will go into the file path which indicates that the port is being used.

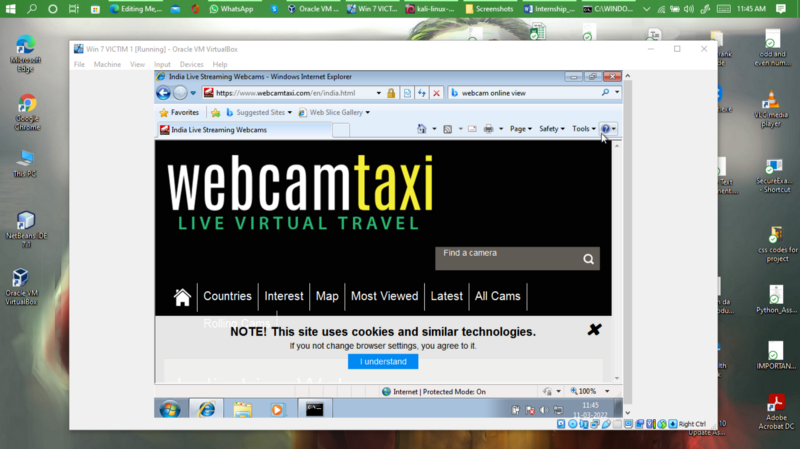
Then use command #exploit to start control.



STEP-7: When You see the meterpreter line in the terminal that means you have successfully entered the target machine and it is under your control now.

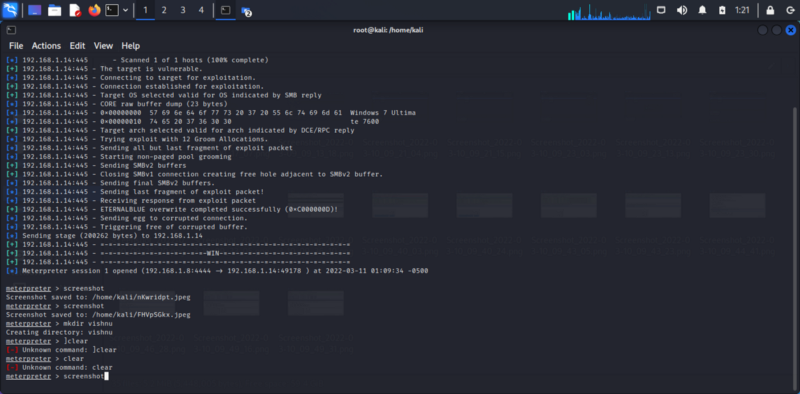
To varify that the target machine is under my control, I am going to take the screenshot from my kali Machine.

THE BELOW IMAGE IS THE SCREENSHOT OF THE WINDOWS-7 VIRTUAL MACHINE(target machine).



Now, I will take the screenshot in the kali Linux machine. It will be saved in my Kali Machine.

RESULT:

COMMAND OF TAKING SCREENSHOT AND THE RESULT

NOW, you can exit. To check the working, Try yourself with your own lab setup.

Attack towards Linux based Machine.

**NEEDS:**

**Attacker Machine:** Kali Linux.

**Target machine:** Metasploitable OS(IP:192.168.1.8).

The procedure is same as I did before for Windows-7. Instead I will use manual way to find Vulnerability,

In simple from the steps involved in the attack is,

* find the IP address of target machine and make a note.
* start the nmap port scanning to find the open ports.
* now, use web browser to find the vulnerability with the version name which is visible when the port scanning is made.
* Collect the results from famous websites like rapid7.com, exploit-db.com, packetsteram.com,etc.
* Now, same procedure as the above attack.
* find the vulnerability with the name SAMBA
* after finding it SET LHOST with victim IP address

commands in flow are:-

#msfdb init

#service postgresql start

#msfconsole

#search

#info

#use

#exploit

After exploiting use command #session -l and use basic Linux command for the result.

Sniffing Attacks

What is sniffing?

Sniffing is a process of monitoring and capturing all data packets passing through given network. Sniffers are used by network/system administrator to monitor and troubleshoot network traffic. Attackers use sniffers to capture data packets containing sensitive information such as password, account information etc.

Tools required:

* Ettercap
* Wireshark

Specify which one should be the attacker and victim. collect target machine IP address and gateway physical address.

Attacker: Kali Linux(192.168.1.8).

Target: Windows-7(192.168.1.14).

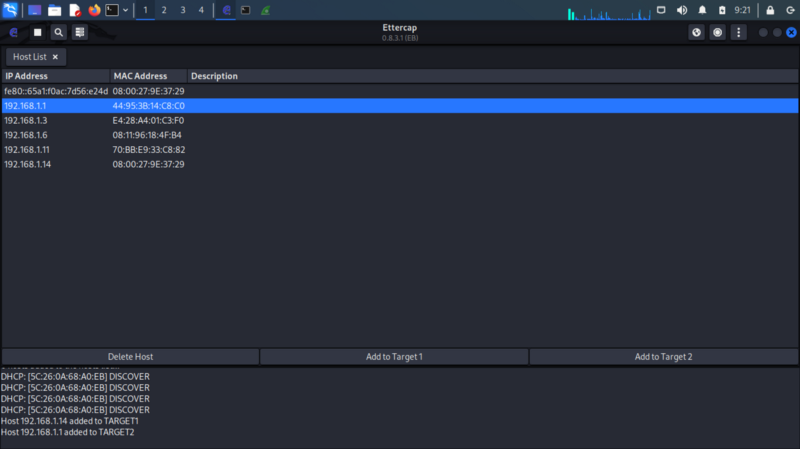
Gateway: 192.168.1.1

PROCEDURES TO BE FOLLOWD TO MAKE THE ATTACK SUCCESS FULL

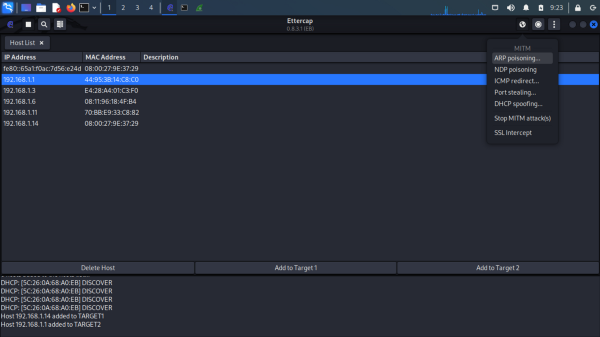
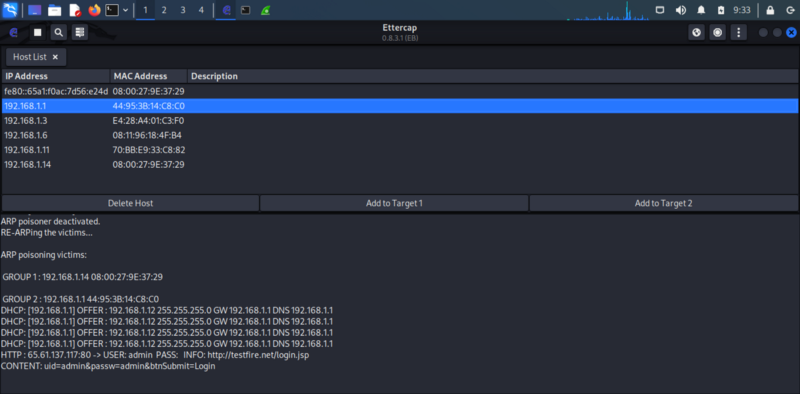
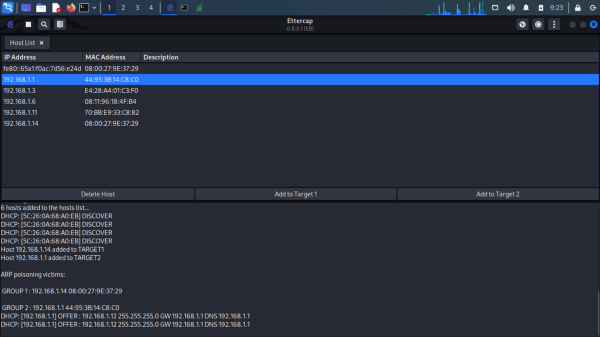
This attack is used to perform attack over target machine without modifying any data. It is also called as MIMA(man in the middle attack).

STEPS ARE,

* Open Ettercap and click the 3-dot option above the right corner.
* Select the host and click.

IP ADDRESS

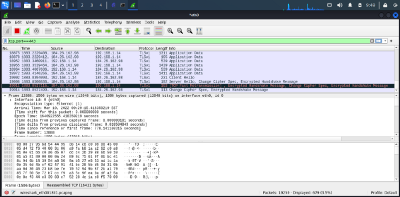
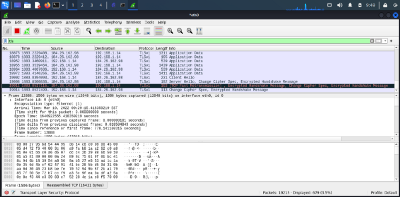
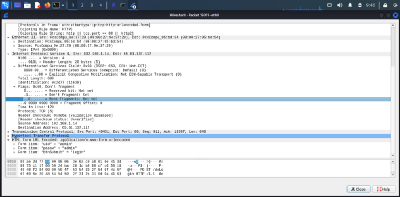
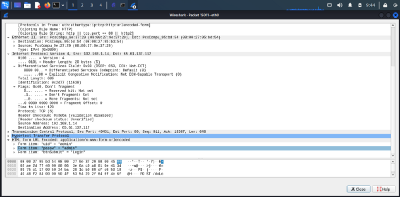
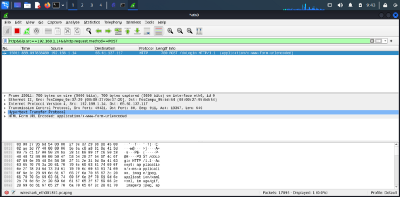
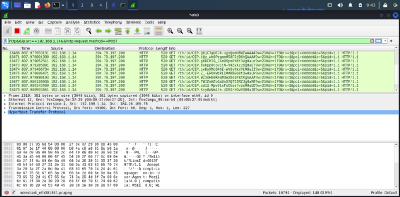
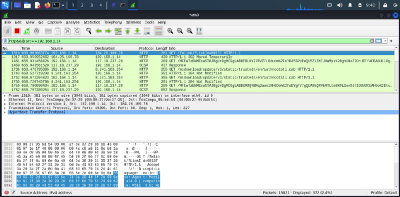
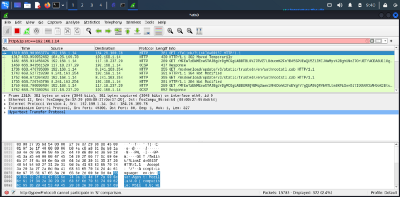
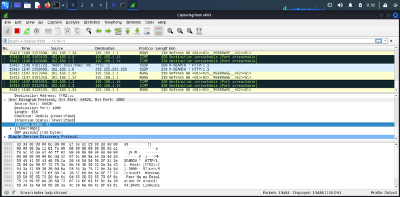
* Specify and add target-1 as windows-7 IP address.
* for Target-2 add windows-7 Gateway physical address. and press the button saying MIMA start.
* always select ARP poisoning.
* After starting attack and open the browser and use http source.
* for testing purpose I have used testfire.com to see the result.
* Once I logged in to the website ettercap will capture the login credentials and it displays it.

left-1 right-2left-3 right-4

* As you can see the result of User name and password is shown.

Wire shark is used to check the data packed touched the network and it can be used for several filter to check whether the packets are being sent and received.

Some of the filters used in Wireshark are:



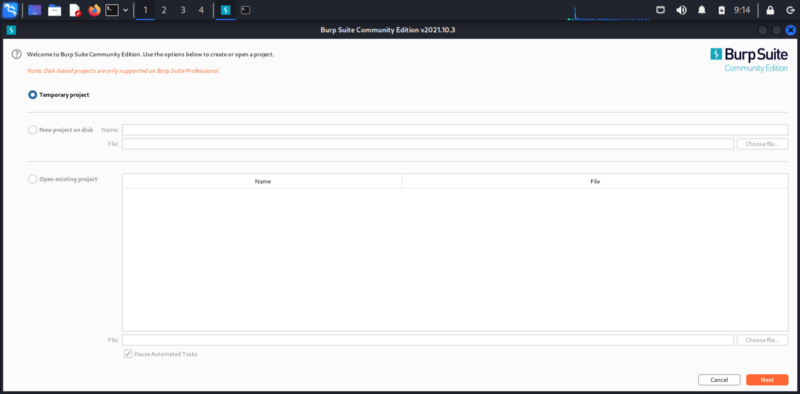
Web Application Penetration Testing

The required tool for web this testing is BURPSUITE and OWASPBWA Os.

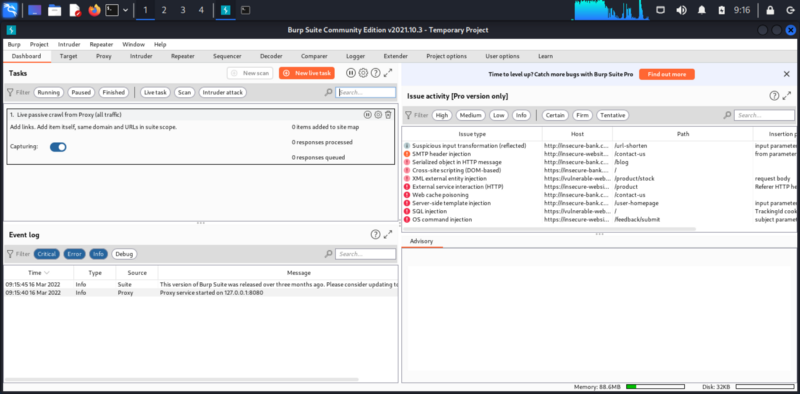
As a beginner, first lesson to be learnt is to configure the Burpsuite.

STEPS INVOLVED IN CONFIGURING BURP SUITE IS:

* Go to application menu->select Web Application Analysis-> click on to Web application Proxies-> click Burpsuite
* Then, agree the T&C’s and press enter.

After configuration the above image will be shown.

* click on to temporary Project and click next.
* You will be redirected to the dashboard.

DASHBOARD OF BURPSUITE

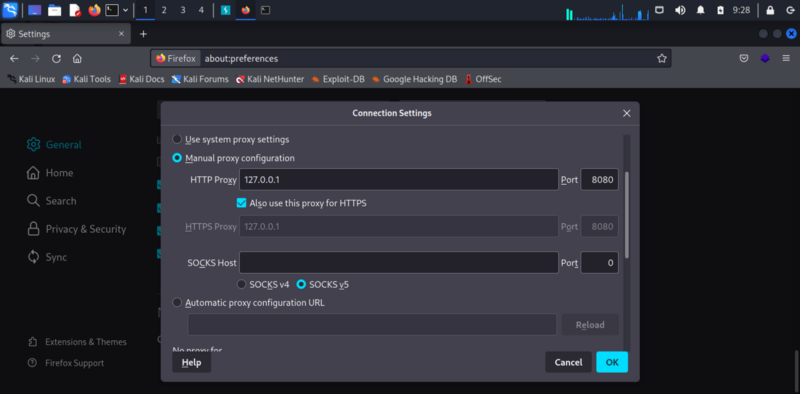
Most Commenly Used Tabs of Burpsuite:

* Target.
* Proxy.
* Intruder.
* Repeater.
* Decoder.

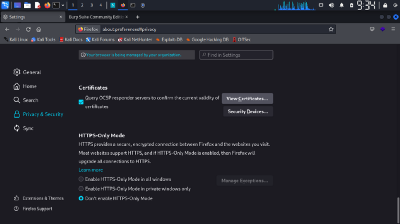
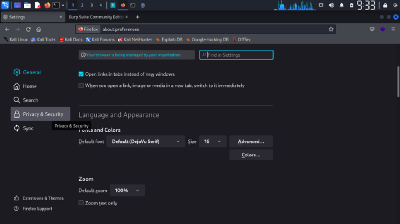
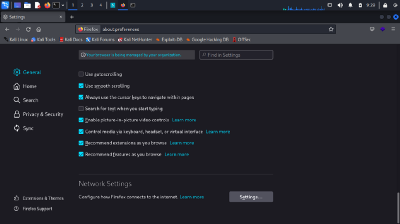
Now, it is time to configure the browser,

STEPS INVOLVED:

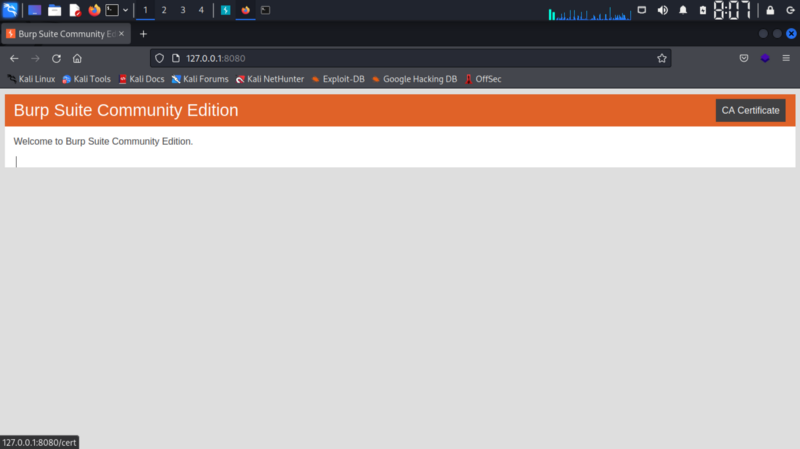
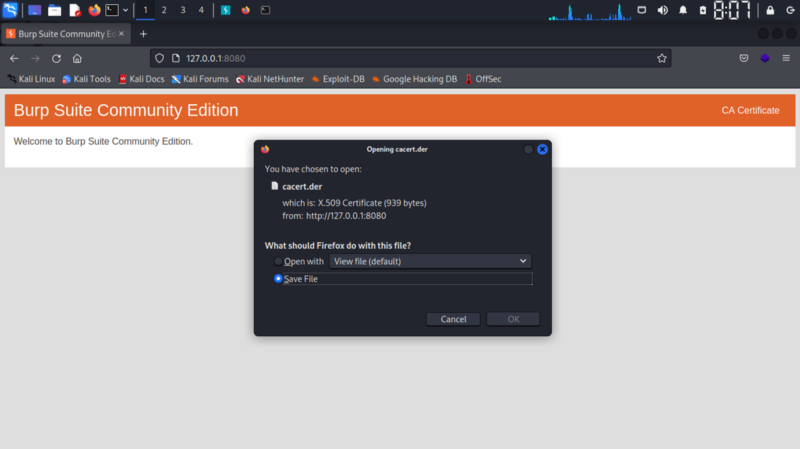
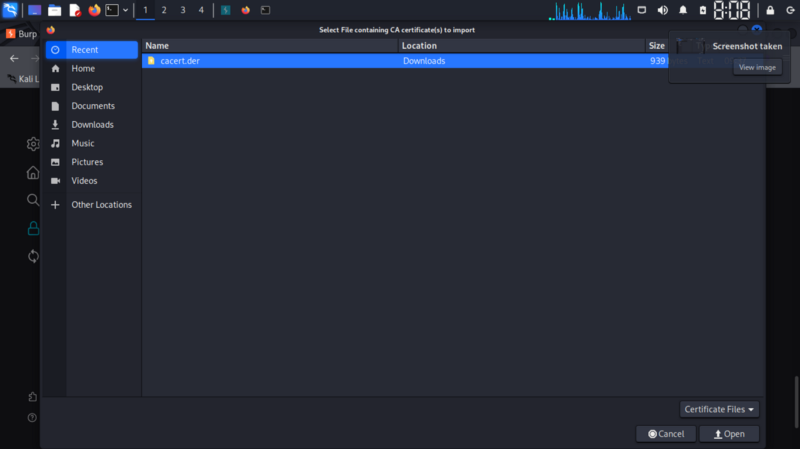
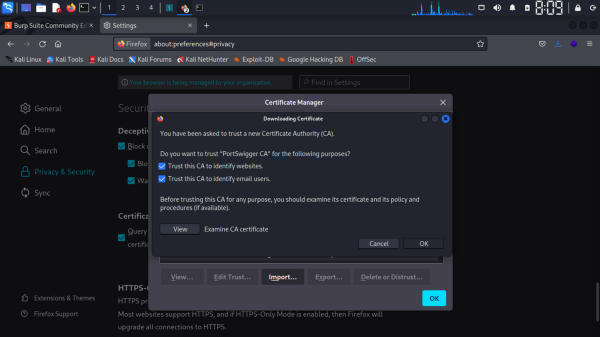
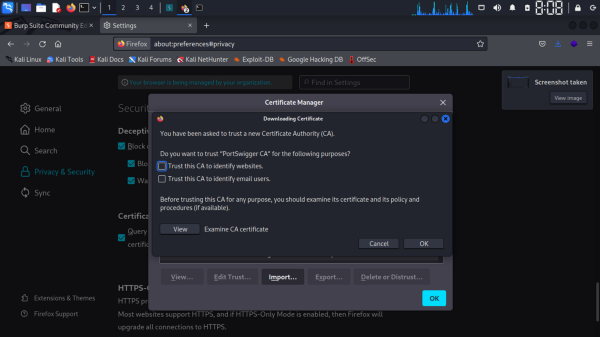
* Open browser->application menu->settings->Connection settings
* In the connection setting select Manual proxy settings and assign 127.0.0.1 for HTTP PROXY with PORT:8080.(implies same to HTTPS).

Proxy configuration and port allocation

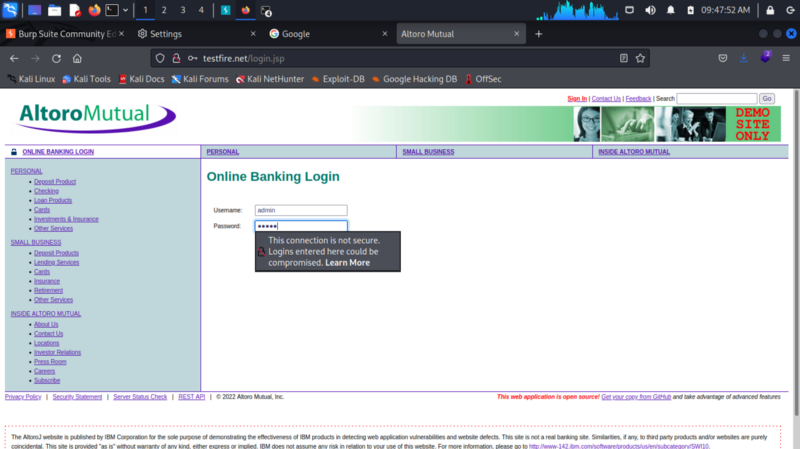
* Again in the settings, goto Privacy and Security
* Click on to the Certificates and add cacert.der file downloaded using browser.



* Now, In the browser when you seart <http://127.0.0.1:8080/> somethin called Welcome to Burp Suite Community Edition will be Displayed.

Welcome pageDownloading CertificateCertificate fileconfiguration and import of certificate

* Now, turn on the intercept in proxy tab of burpsuite and start browsing.
* To check the working of this method lets go to testfire.net website and try tp login.

login Credentials….. uname:admin password:admin

* afer logging in the brup suite must track this credential and should be shown.
* To verify that, lets go to burpsuite and see the targeted machine work.

RESULT

* As you can see the requested result in the above image.

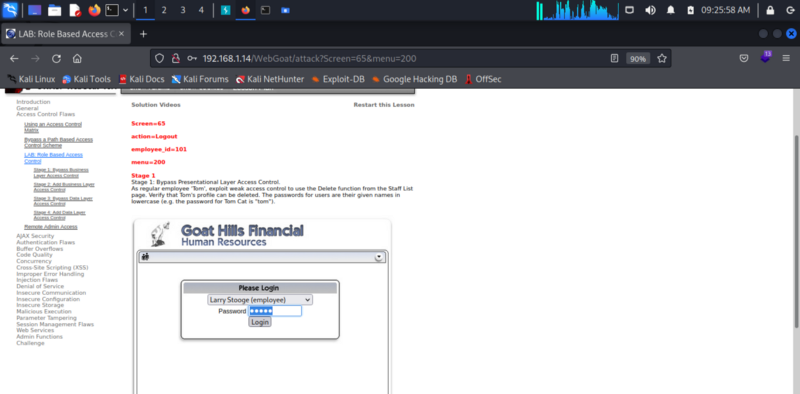
INDIRECT OBJECT REFERENCE & LOCAL FILE INCLUSION

IDOR and LFI can be achieved using the webgoat.

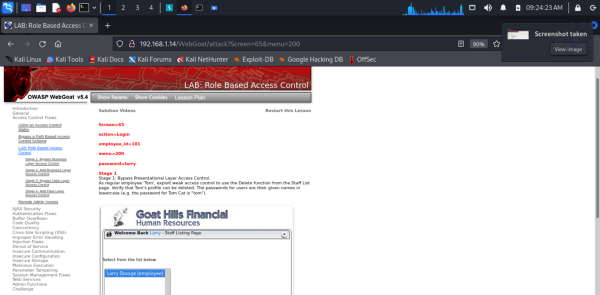
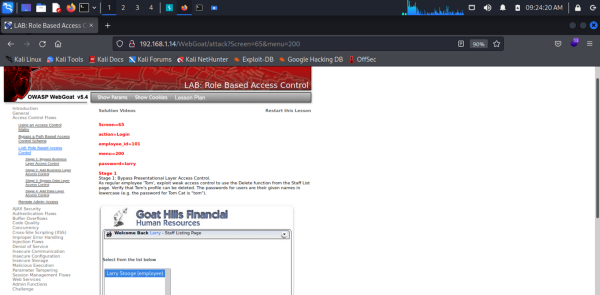
To open the webgoat, in the browser, use the IP address of OWASPBWA’s IP Address and paste it in the URL.

To Achieve IDOR lets use the role based access control methods.

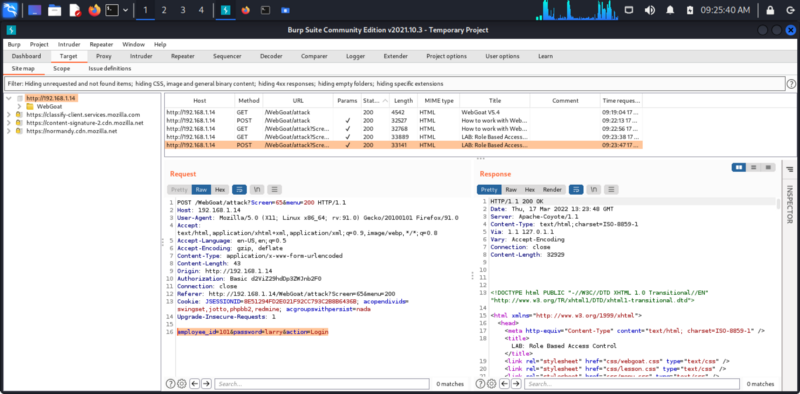
* turn on Burpsuite Intercept.
* go to role based access control and login as employee.
* the employe’s first name is the password of the login.
* The goal is the view the detail of other employee using one employee ID.



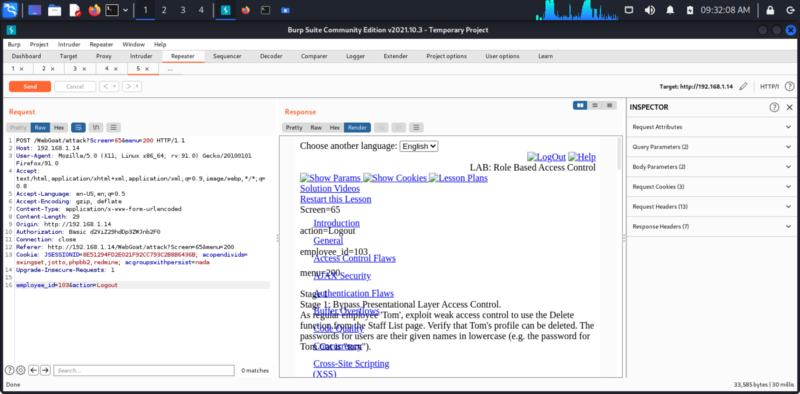
* then, Burp suite will record the activity and will be book marked.



* go to the burp suite and check for the latest activityin the target.



* you can see the login details has been tracked by burpsuite.
* Now, send it to the repeater and modify the employee if which is 101 to 103 and check result.
* If you are able to see the detail of the employee with ID 103 from ID 101 then you have successfully viewed the other employee information using one Employee ID.

RESULT IS SUCCESSFULL

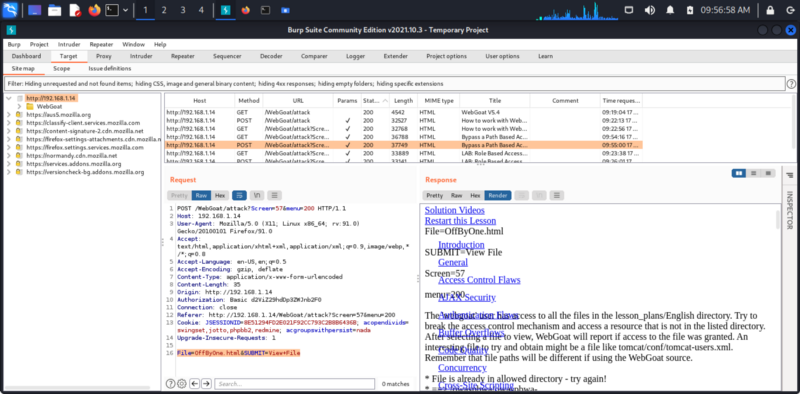
LFI

Local file inclusion involves the accessing the target machine file though viewing file.

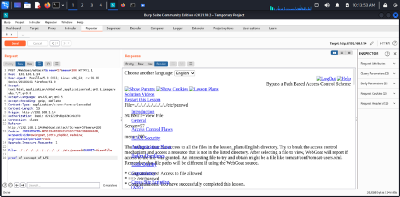
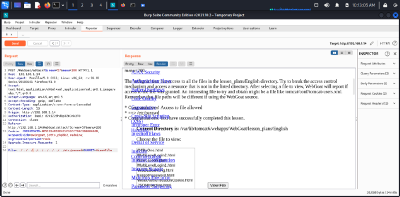
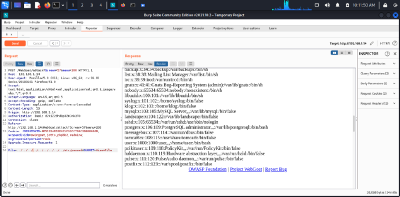
* for that, lets view a file using Webgoat.
* In webgoat, use BYPASS A PATH BASED ACCESS CONTROL SCHEME.
* view a file you see in that column.

BYPASS A PATH BASED ACCESS CONTROL SCHEME.

* When you view a file the burp suite will record the activites and you will be able to view it in the target tab of burp suite.

file view

* Move it to the repeater and change the file name with local system file.
* To include local file in the above file lets use /etc/passwd/ folder.
* When you include the file in the repeater and send, it will view that file.
* the results are,

Results

Modifying the other Employee detail from One employe:

to achieve that we need two employee

User1: Curly

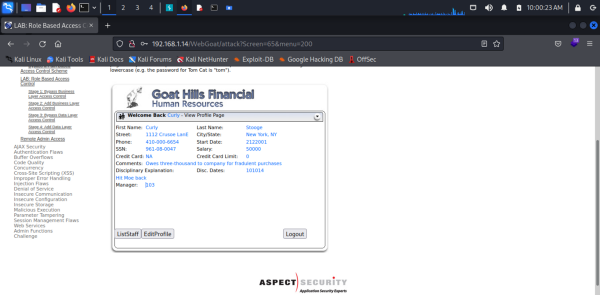
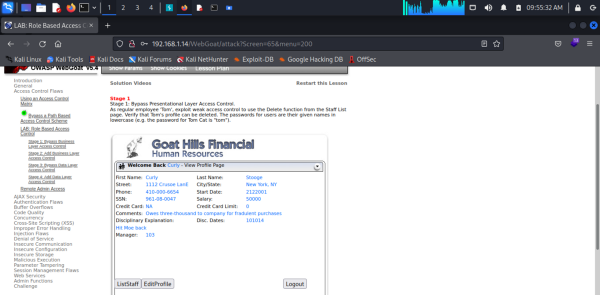
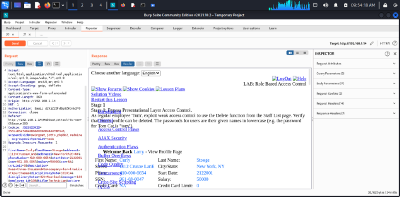
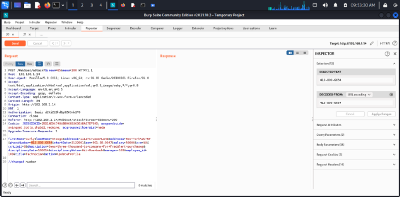
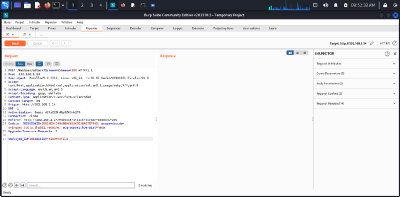
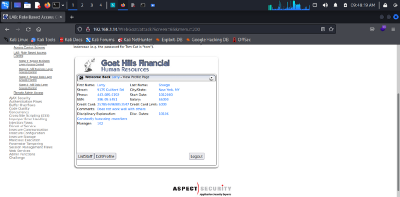
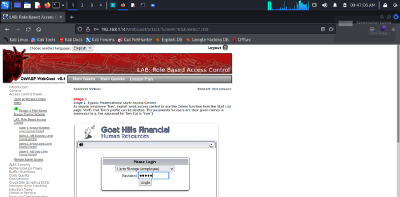
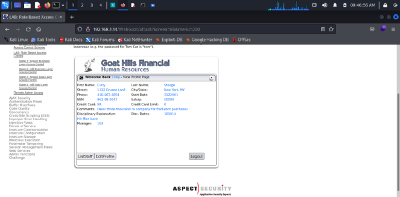
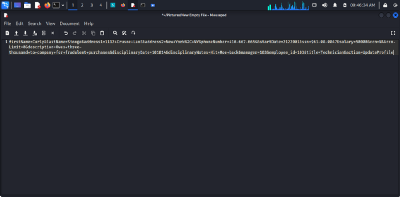
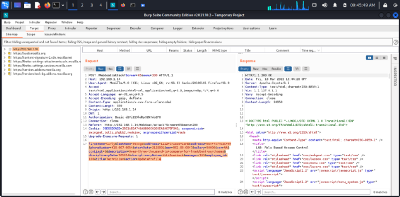
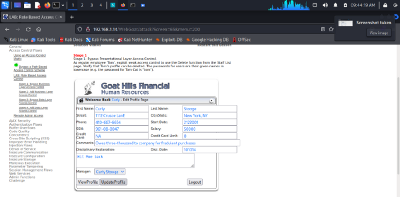
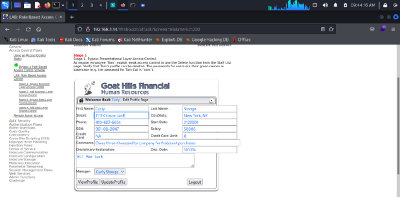
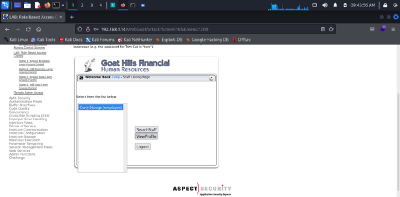
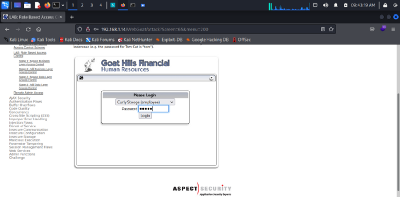
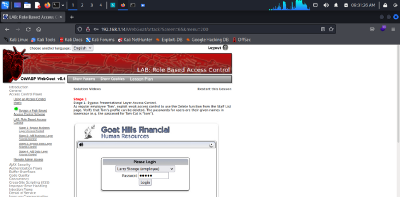
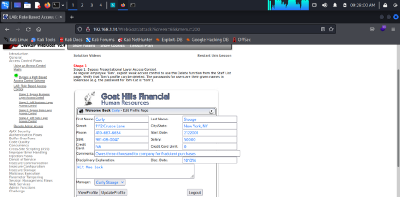
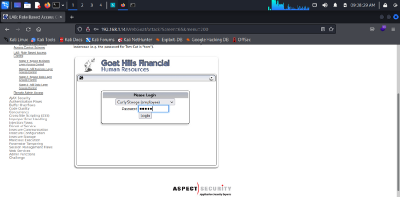
User2: Larry

Its an attack where one user is able to steal/modify/delete data of another user

User is able to edit / access data of a similar role user  
Guest : Guest / User : User : Administrator : Administrator

User is able to edit / access data of a higher role user  
Guest : Standard User / Root | User : Administrator

Steps to perform Privilege Escalation:-  
1. Login as , perform an unique operation for that profile  
2. Record that request body and keep a backup  
3. Logout from  
4. Login as ,  
5. Create a dummy request of User 2  
6. Replay the recorded request body by pasting the recorded data  
7. Cross verify if the changes have been made  
Login to and check if the changes have been made



The above screenshots are the procedure to conduct the attack

THANK YOU