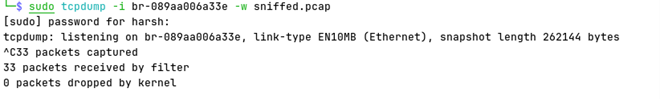
**Lab Practical #7:**

**Study sniffing and MIM attack using ettercap, Bettercap and TCPdump tools**

**1. MIM using TCPdump**

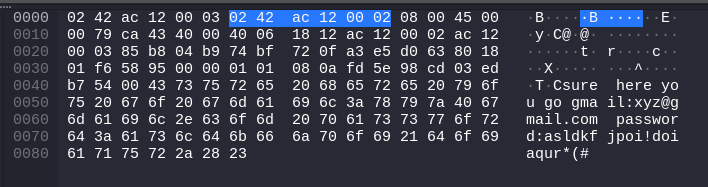
• TCPdump prints out a description of the contents of packets on a network interface that match the Boolean expression the description is preceded by a time stamp, printed, by default, as hours, minutes, seconds, and fractions of a second since midnight. It can also be run with the -w flag, which causes it to save the packet data to a file for later analysis, and/or with the -r flag, which causes it to read from a saved packet file rather than to read packets from a network interface.



• The above command needs to be run as sudo (super user do) privileges

• -i flag specifies the interface we are working with here we are using a virtual interface.

• -w flag specifies where to store the packets which are captured here we are storing them in sniffed.pcap file which is located in current directory.



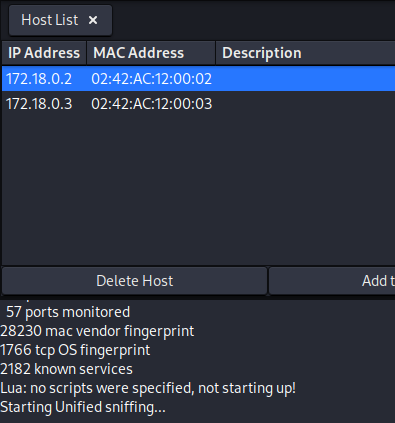
• In above image you can see a packet which was sniffed in sniffed.pcap which contains some credentials which were transferred from a user to another user.

• Below is a more readable version of the text in the above image.



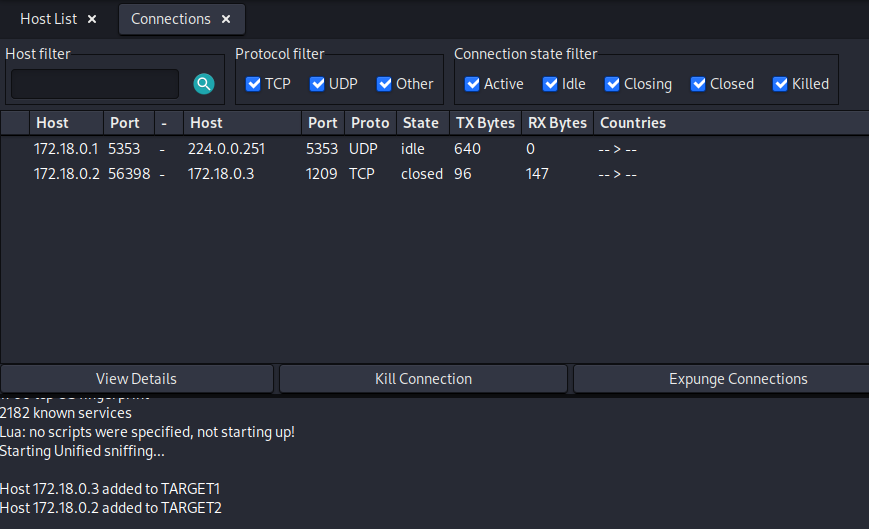
**2. MIM using Ettercap**

• Ettercap was born as a sniffer for switched LAN, but during the development process it has gained more and more features that have changed it to a powerful and flexible tool for Man-in-the-Middle attacks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.



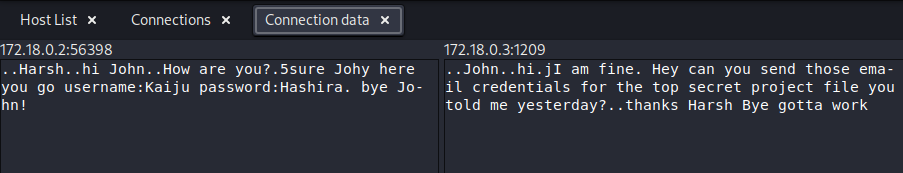
• Here in above image we can see that Ettercap has found two hosts in our network and (We are using a virtual network for this process)

• Add both the addresses as Target1 and Target2 by right clicking each of them.



• From the top right corner we can open Connections tab from the View menu.

• Here we can see all the connections made in network, we can see we have two connections one UDP and other TCP.



• By double clicking on the connection you can see the data which was transferred through the

connection.

**3. MIM using Bettercap**

• It is a upgraded version of ettercap as the name says “better”.

Command : sudo bettercap -iface virbr0 -eval “https-ui on”

• In above command we can see a few flags which are explained below

◦ -iface: it specifies on which interface we are going to run bettercap

◦ -eval: it is used to execute a command of bettercap from the terminal for our purpose we are just launching bettercap ui version which can be seen through browser.



**•** In above command we are starting probing on local network by running “net.probe on” command, we can see that we found a potential target in the network.



**•** we will set the target using “set arp.spoof.target <ipaddress>” command which can be used to set one or more targets.



**•** now we are setting “net.sniff.local true” which means that we are going to sniff all the incoming and outgoing packets from the target/ to the target machiene(s).



• now we are starting the actual attak by running “arp.spoof on”.



• Turning on the actual sniffer so we can see the incoming and outgoing traffic in the bettercap terminal interface.



• In above image we are seeing a sniffed packet which contains username and password of some vulnerable website where the target logged in.

**4. (Active) MIM Using Bettercap**

• Here we are performing a Active man in the middle attack

• In a Active MIM attack we are not only reading the data but we are also altering the data/content of the request or response from/ to the target.



• Here we are starting “net.probe on” to probe the network.

• In above image we have discovered a potential target “192.168.122.144”



• Here we are setting the target to “192.168.122.144”



• Starting the actual ARP(Address Resolution Protocol) attack.



• Here we are spoofing the domain “darshanums.in” for the target machiene. i.e., when ever the target searches for “darshanums.in” there is a DNS query for “darshanums.in” instead of the DNS server we are going to respond to the query instead of the DNS server with a different address rather than the actual address of “darshanums.in”.



• Now we are starting the dns spoofing attack on which shows us that the query for “darshanums.in” is

replaced by “192.168.122.1” which is the IP address of the spoofed website.

• Here we can see that on the target machine when we search for “darshanums.in” on the target machine we are actually redirected to other website which is “DVWA” login page.



* In our Bettercap CLI(Command Line Interface) we can see that there was a request for “darshanums.in” in target machine and the request was responded by our spoofed DNS response