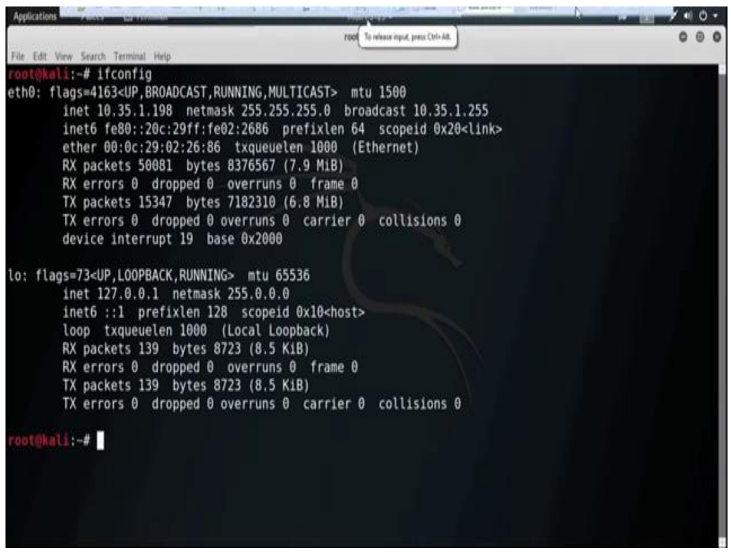
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 25
MITM

Today's session we will discuss about man-in-the-middle attack using the concept of sniffing via ARP poisoning.

(Refer Slide Time: 00:25)



Address resolution protocol that means ARP is a stateless protocol used for resolving IP addresses to machine MAC addresses. All network device that need to communicate on the network broadcast ARP queries in the system to find out other machines MAC address. ARP poisoning is also sometimes known as ARP spoofing.

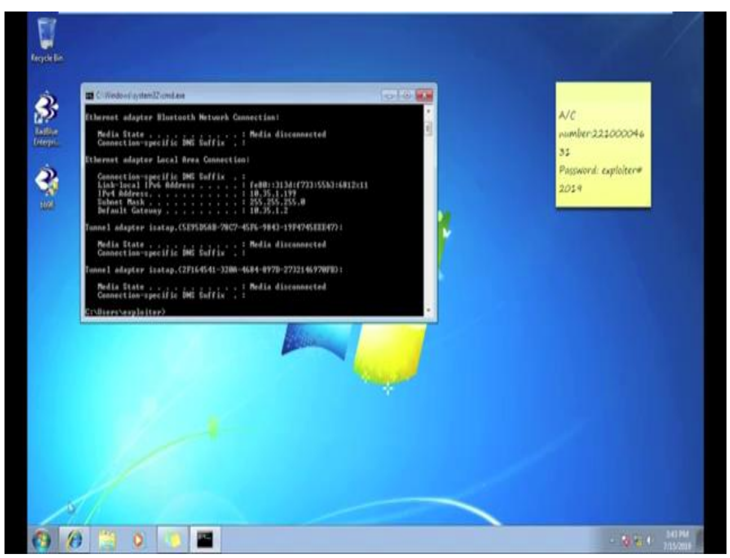
Now, the question is that how ARP works? When one machine needs to communicate with another it looks up its ARP table. If the MAC address is not found in the table, the ARP request is broadcasted over the network. All the machines on the network will compare this IP addresses to MAC addresses. If one of the machines in the network identifies this address, then it will respond to the ARP request with its IP and MAC address. The requesting computer will store the address pair in its ARP table and communication will take place.

Now, the question is that what is ARP spoofing? ARP packets can be forced to send data to the attacker's machine. ARP spoofing constructs a large number of forced ARP request and reply packet to overload the switch. The switch is set in forwarding mode and after the ARP table is flooded with spoofed ARP response the attackers can sniff all the network packets.

Attackers flood a target computer ARP catching with first entries which is also known as poisoning. ARP poisoning uses man-in-the-middle access to poison the network. So, the man-in-the-middle attack implies an active attack where the attacker creating a connection between the victim and send message between them in or may capture all the data packet from the victim. In this case, the victims think that they are communicating with each other, but in reality the malicious attacker controls the communication. A third person exists to control and monitor the traffic of communication between two parties that is client and server. Some protocol such as SSL, serve to prevent this type of attack by encrypting the data.

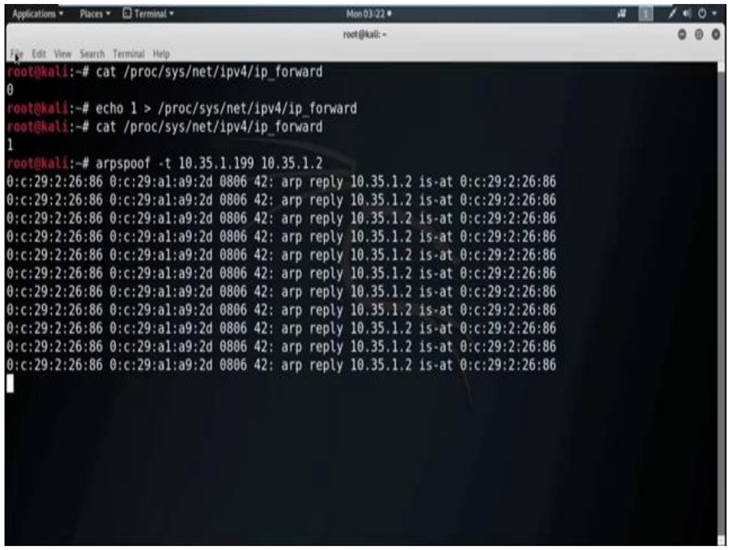
Now, we will show you a demo how to perform man-in-the-middle attack. So, now, for our scenario we will consider that this is our attacker machine with the IP address 10.35.1.198.

(Refer Slide Time: 04:23)



And, this is our victim with the IP address 10.35.1.199 and the default gateway 10.35.1.2.

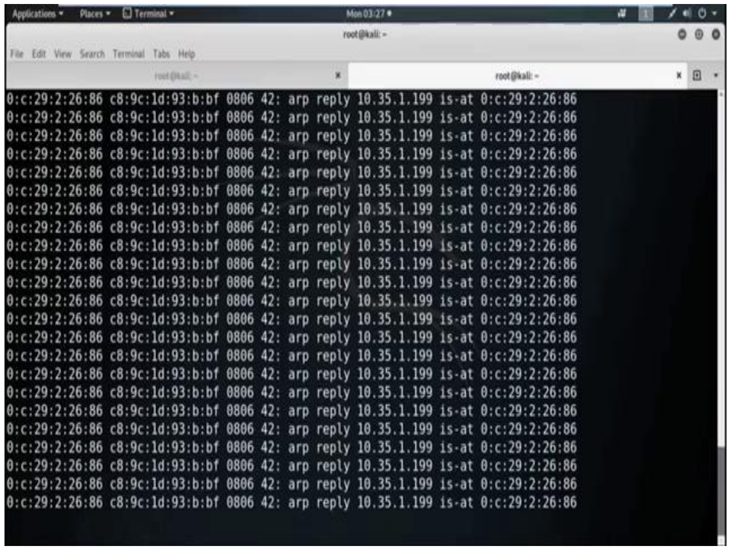
(Refer Slide Time: 04:37)



Now, from the attacker machine first we need to start port forward. To check the port forward is enabled or not, we need to check the $ip\_forward$ file and the location of $ip\_forward$ file is under $/proc/net/ipv4$ directories. So, to check that particular file $ip\_forward$ we use the command cat. cat is the command to see the content of a text file or to content of a file. cat then the location is $/proc/net/ipv4$, then the file name is $ip\_forward$. So, it written as 0; that means, it is disabled. So, to enable it we need to write it as 1. So, by using the $echo$ command we can write in a file.

So, our next command is $echo$ then 1 then the location is $/proc/net/ipv4$ then the filename $ip\_forward$. Now, check the content of the file. Now, see it is become 1; that means, it enable port forward. Now, our next task is to perform the ARP poisoning. So, to perform the ARP poisoning we use the command $arpspoof$. $arpspoof$ then $-t$ specify the IP address of the target machine. So, now, our target machine IP addresses is 10.35.1.199. Then we need to provide the IP address of the default gateway that is 10.35.1.2. Now, for the reverse connection we also need to perform the same thing, but this time we interchange the target and the destination.

(Refer Slide Time: 07:47)



Open a new terminal and again use the command $arpspoof$. Now, this time target will be the default gateway that is 10.35.1.2, then the IP address of the victim machine 10.35.1.199. This way we forward the both way traffic which is coming from the default gateway to target machine and which is going to the default gateway from target machine. Now, we are able to place the attacker machine between the gateway and the target machine successfully.

Now, our aim is to capture the data packet which is sometimes known as sniffing technique. Sniffing is the process of monitoring and capturing all the packet passing through a given network using sniffing tool. It is a form of a tapping internet wire or maybe phone wire and get to know about the conversation or all the data. There is so much possibility that if a set of enterprise switch port is open, then one of their employee can sniff the whole traffic of the network. Anyone in the same physical location can plug into the network using Ethernet cable or connect wirelessly to that network and sniff the total traffic.

In other words, sniffing always allow you to see all sort of traffic both protected and unprotected. In the right condition and with the right protocol in place and attacking party may be able to gather information what can be used for further attack or to cause other issues for the network or system owner. One can sniff the sensitive information from the network via e-mail traffic, FTP password, web traffic, telnet password, router configuration, chat session, DNS traffic etc. A sniffer normally turns the NIC, that means, Network Interface Card of the system to the promiscuous mode so that it listen to all the data transmitted on it segment.

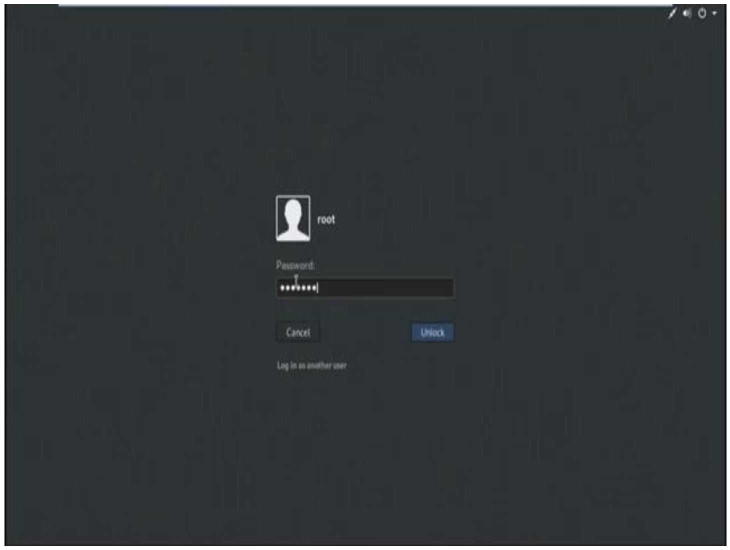
Promiscuous mode refers to the unique way of Ethernet hardware in particular network interface card that allows an NIC all to receive all traffic on the network even if it is not address to this NIC. By default NIC ignore all the traffic that is not addressed to it which is done by comparing the destination addresses of the Ethernet packet with the hardware address that is the MAC address of the device while this make perfect sense for networking. Non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issue or traffic accounting.

A sniffer can continuously monitor all the traffic to a computer through the NIC by decoding the information encapsulated in the data packet. There are two types of sniffing are there; one is active and another one is passive. In passive sniffing the traffic is locked, but it is not altered in any way. Passive sniffing allows listening only. It works with hub device. On a hub device the traffic is sent to all the ports in a network that uses hub to connect systems. All host on the network can see the traffic. Therefore, it can easily captured traffic going through.

The good news is that now hubs are almost absolute nowadays. Most modern network use switches. So, passive sniffing is no more effective. So, now, it is all about active sniffing. In active sniffing the network traffic is not only locked and monitor, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch based network. It involves injecting address resolution packet that is ARP packet into a target network to flood on the switch Content Addressable Memory table that is CAM table. CAM keeps track of which host is connected to which port.

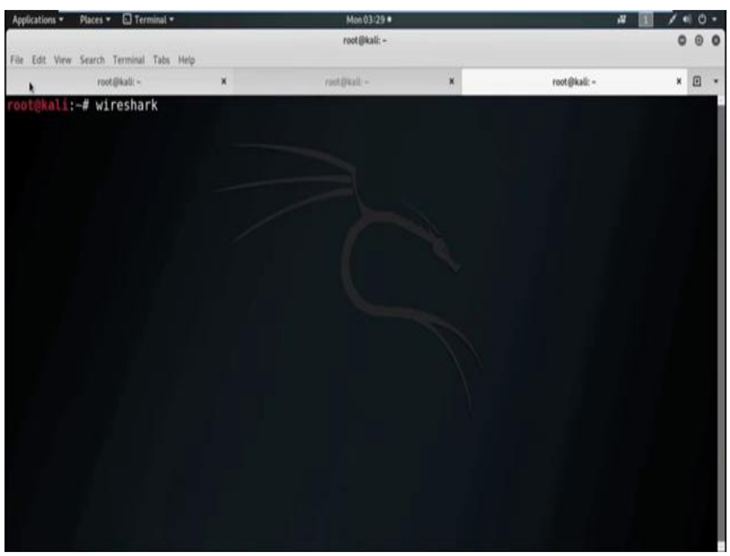
Now, by active sniffing technique, now for active sniffing technique MAC flooding, DHCP attacks, DNS poisoning, spoofing attack, ARP poisoning are there.

(Refer Slide Time: 13:51)

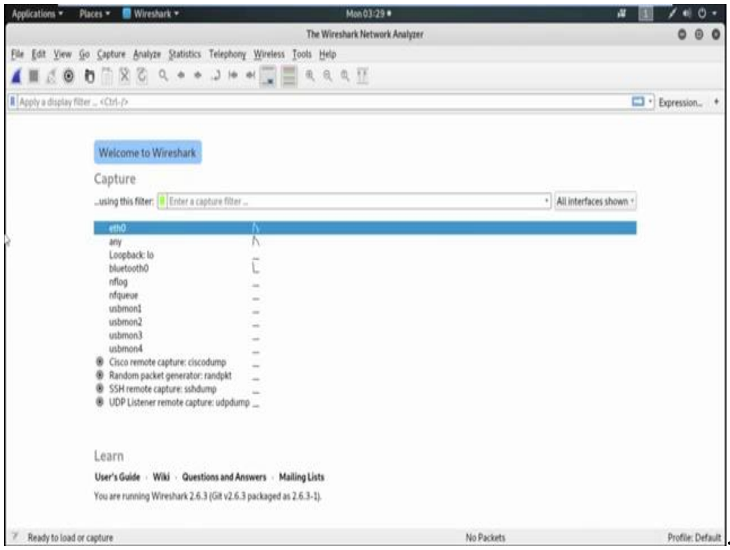


Now, we are demonstrated ARP poisoning. Now, we are in the middle of the ARP poisoning. Now, our aim is to open a sniffing tool. The best sniffing tool I ever used that is $wireshark$; now to open the tool $wireshark$ to capture all the data packet.

(Refer Slide Time: 14:05)

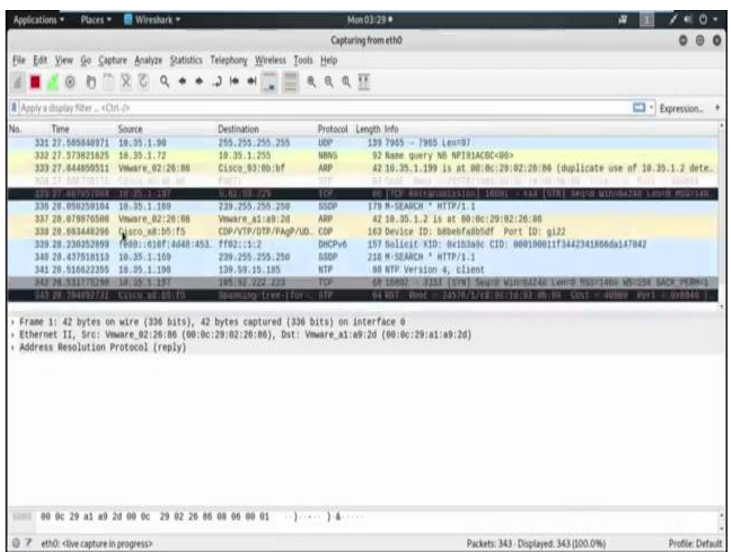


(Refer Slide Time: 14:15)



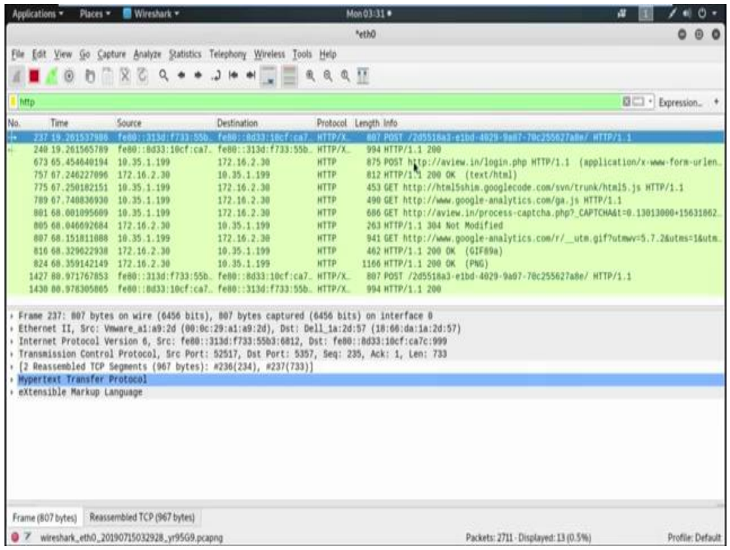
Now, select the interface eth0.

(Refer Slide Time: 14:25)



Now, my kali machine; that means, the attacker machine successfully placed between the default gateway and the attacker machine with the IP address 10.35.1.199. Now, I send some traffic from the victim machine and try to capture all that data packet from the attacker machine. Now, see this is my victim machine.

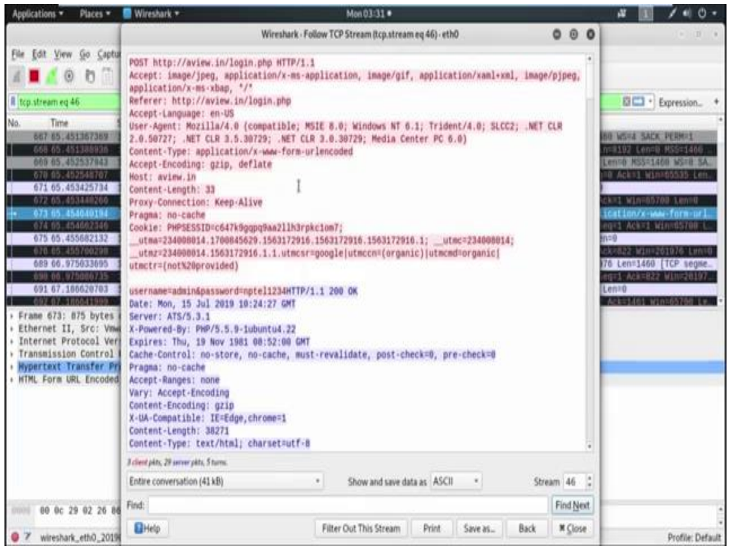
(Refer Slide Time: 15:05)



And, from the victim machine I try to login into a web application $aview.in$. Now, in the login credential I put some login credential like username admin and I am giving some password and try to sign in. Now, I am trying to capture all these data packets which is sent from the victim machine, from my attacker machine and go to the tool $wireshark$ and filter those that data packet which have sent through http protocol.

Now, see, these are the data packet which have sent through http protocol. These way we can also filter the data packet. Now, see here is the data packet which sent to $aview.in$ login page. Now, try to open the details of this data packet, right click on this data stream and follow TCP stream for the detail data.

(Refer Slide Time: 16:45)



Now, see, wow great, here is the username and password as I give in nptel1234. This way by ARP poisoning and via sniffing technique we can perform man-in-the-middle attack and can capture all the data packet which is coming to the victim machine and which is going from the victim machine.