Practical – 3

Understand packet capturing tool Wireshark or Ethercap and analysis of those packets.

Man in The Middle Attack (MITM)

A man-in-the-middle (MiTM) attack is a type of cyber attack in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other. The attack is a type of eavesdropping in which the attacker intercepts and then controls the entire conversation.

MiTM cyber attacks pose a serious threat to online security because they give the attacker the ability to capture and manipulate sensitive personal information -- such as login credentials, account details or credit card numbers -- in real time.

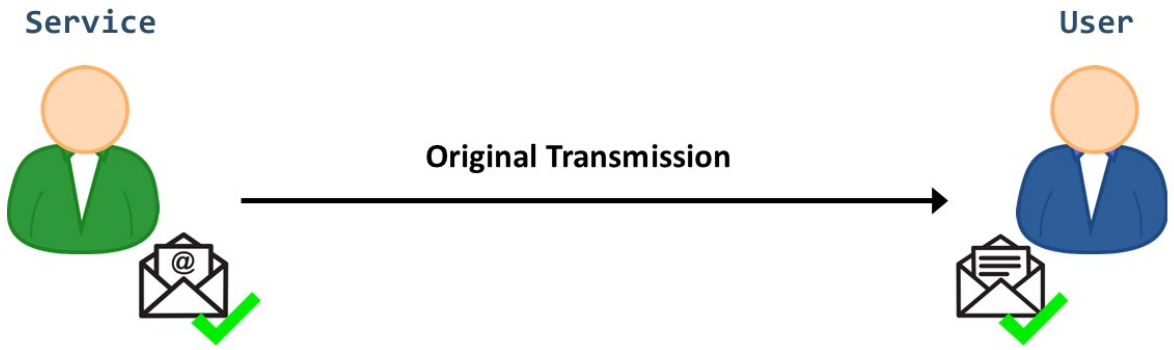
Arp Poisoning

ARP Poisoning (also known as ARP Spoofing) is a type of cyber attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table. ARP Protocol translates IP addresses into MAC addresses. Because the ARP protocol was designed purely for efficiency and not for security, ARP Poisoning attacks are extremely easy to carry out as long as the attacker has control of a machine within the target LAN or is directly connected to it.

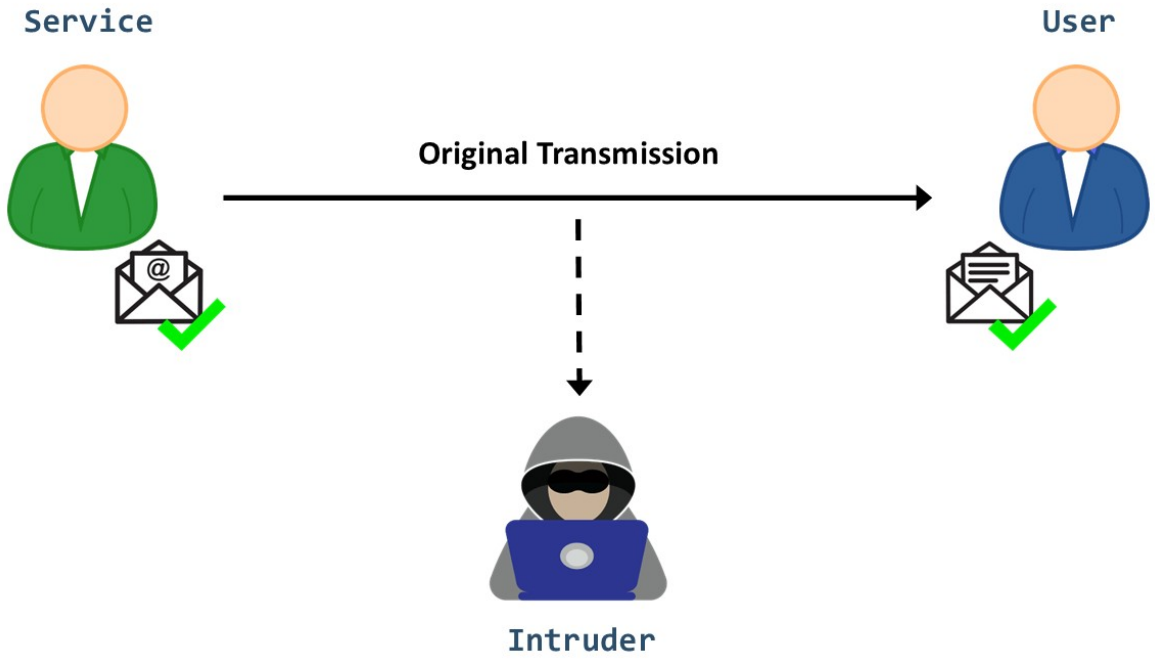
The attack itself consists of an attacker sending a false ARP reply message to the default network gateway, informing it that his or her MAC address should be associated with his or her target's IP address (and vice-versa, so his or her target's MAC is now associated with the attacker's IP address). Once the default gateway has received this message and broadcasts its changes to all other devices on the network, all of the target's traffic to any other device on the network travels through the attacker's computer, allowing the attacker to inspect or modify it before forwarding it to its real destination. Because ARP Poisoning attacks occur on such a low level, users targeted by ARP Poisoning rarely realize that their traffic is being inspected or modified. Besides Man-in-the-Middle Attacks, ARP Poisoning can be used to cause a denial-of-service condition over a LAN by simply intercepting or dropping and not forwarding the target's packets.

Interception

Usually, data communication occurs when two connected entities exchange a message over the Internet:



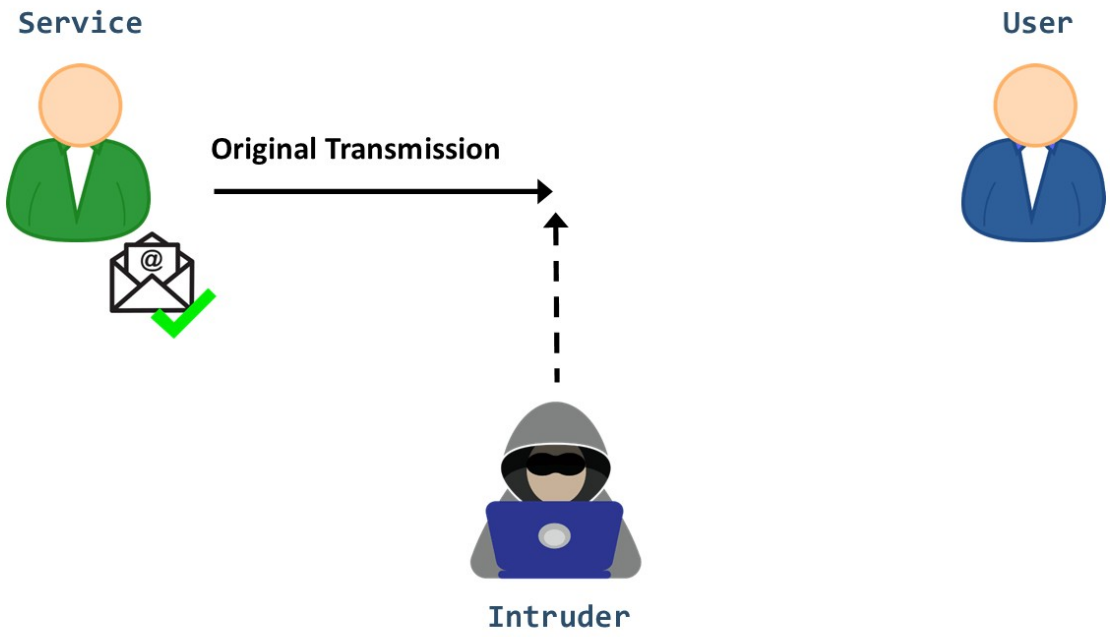
In the case of an interception attack, a malicious actor can access private or confidential information with no legitimate authorization. Eavesdropping attacks are a typical example of this category of attack. Namely, an intruder can refer to several techniques, such as packet sniffing and man-in-the-middle (MITM).



Generally, he aims to obtain critical information such as passwords and credit card numbers or to disturb data exchanges on the network. When effectively executed, it can be very hard to identify traces of the attack: This category of attacks is mainly a threat to data confidentiality. We can mitigate it by encrypting communications, avoiding untrusted Wi-Fi networks, and regularly updating our software.

Interruption

This form of attack manifests when a network service or a system asset is disrupted or destroyed:



As a result, legitimate users can no longer reach it, either permanently or temporarily.

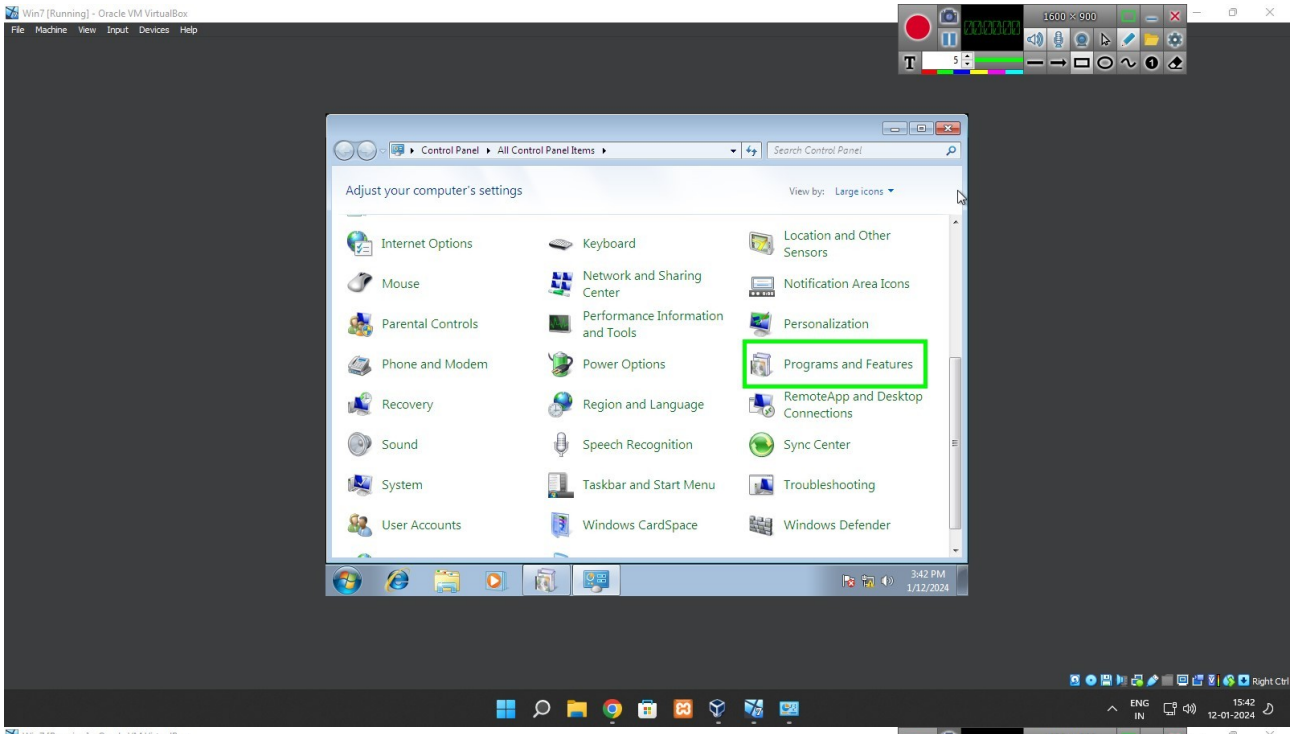
For example, an attacker may steal or damage a hardware/software component. He can also overwhelm a server host with requests so that it can't respond, causing a DoS attack. Another example is using malware, such as viruses or trojans, to delete data or disable a system's functioning.

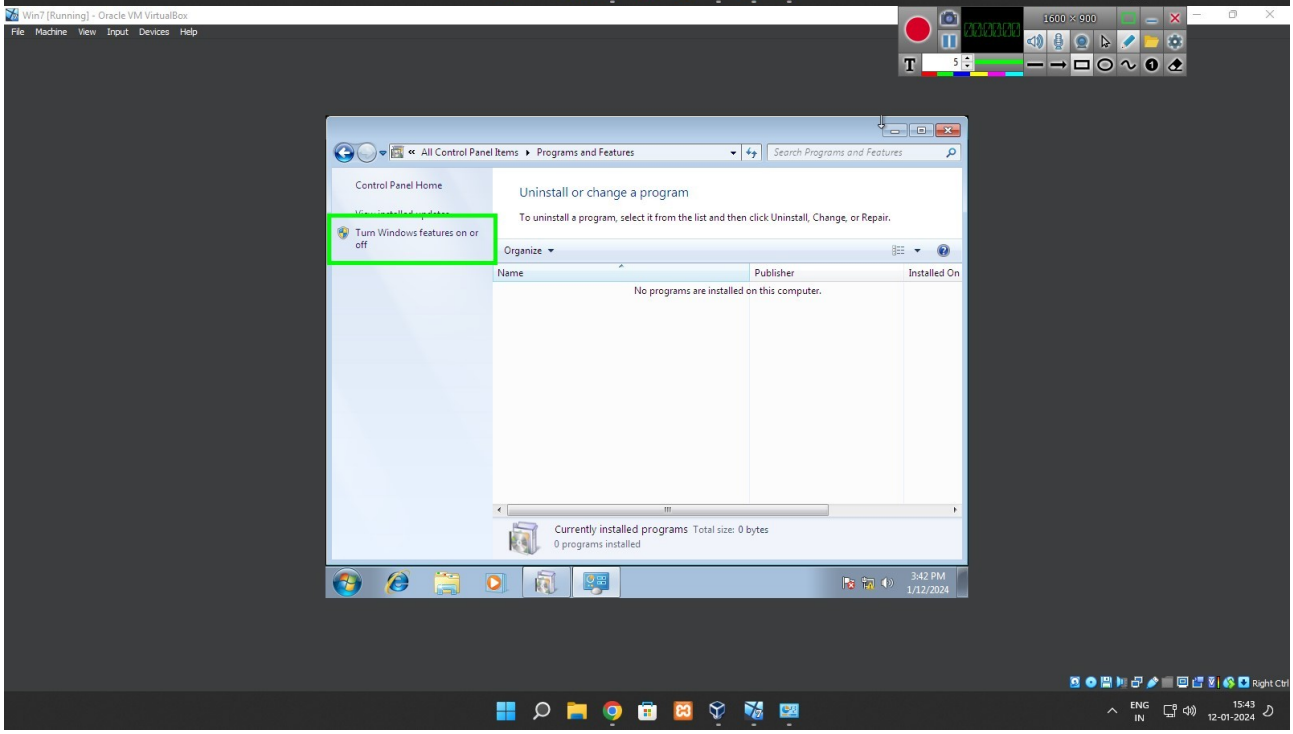
This type of attack is a threat to data availability.

> To protect against interruption attacks, we need appropriate precautions such as firewalls and system backups. Moreover, we can use cloud-based solutions and Content Delivery Networks (CDN) to boost security against these attacks and keep our system and network operable.

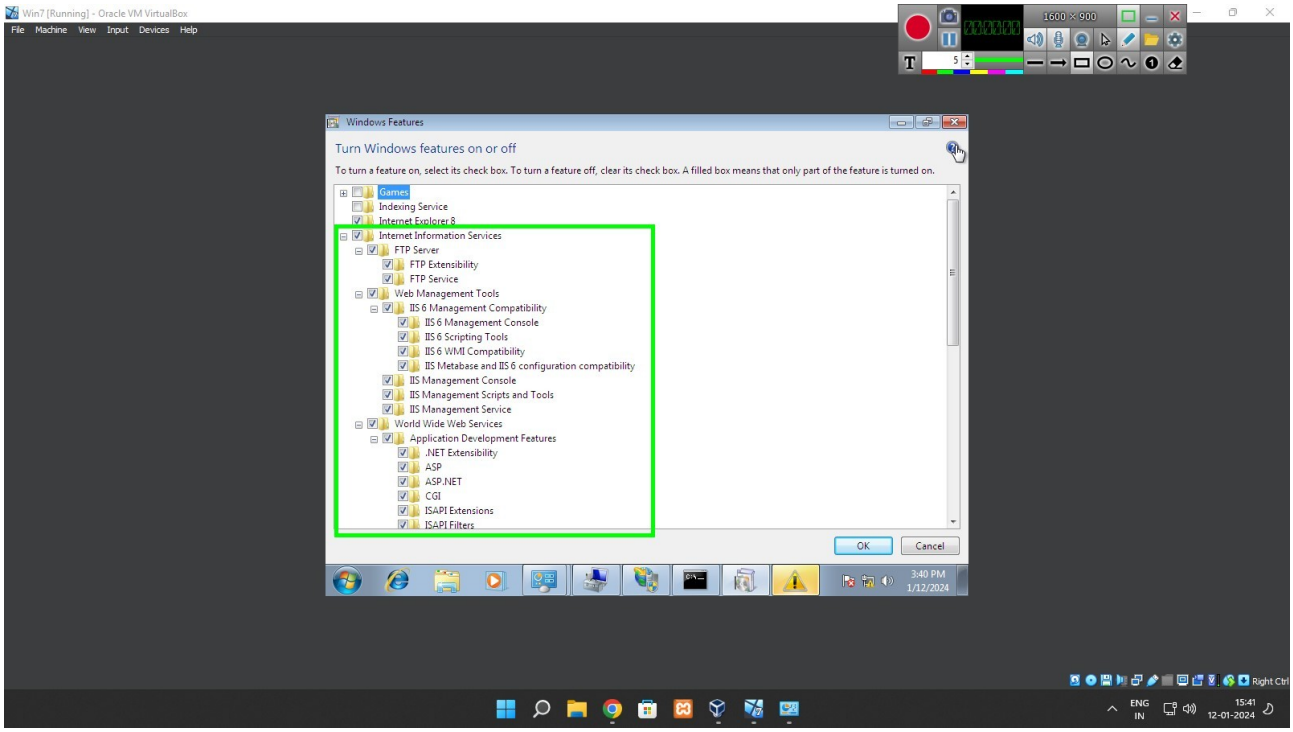
1) Creating FTP server

- Go to Control Panel\All Control Panel Items\Programs and Features then click Turn Windows features on or off.





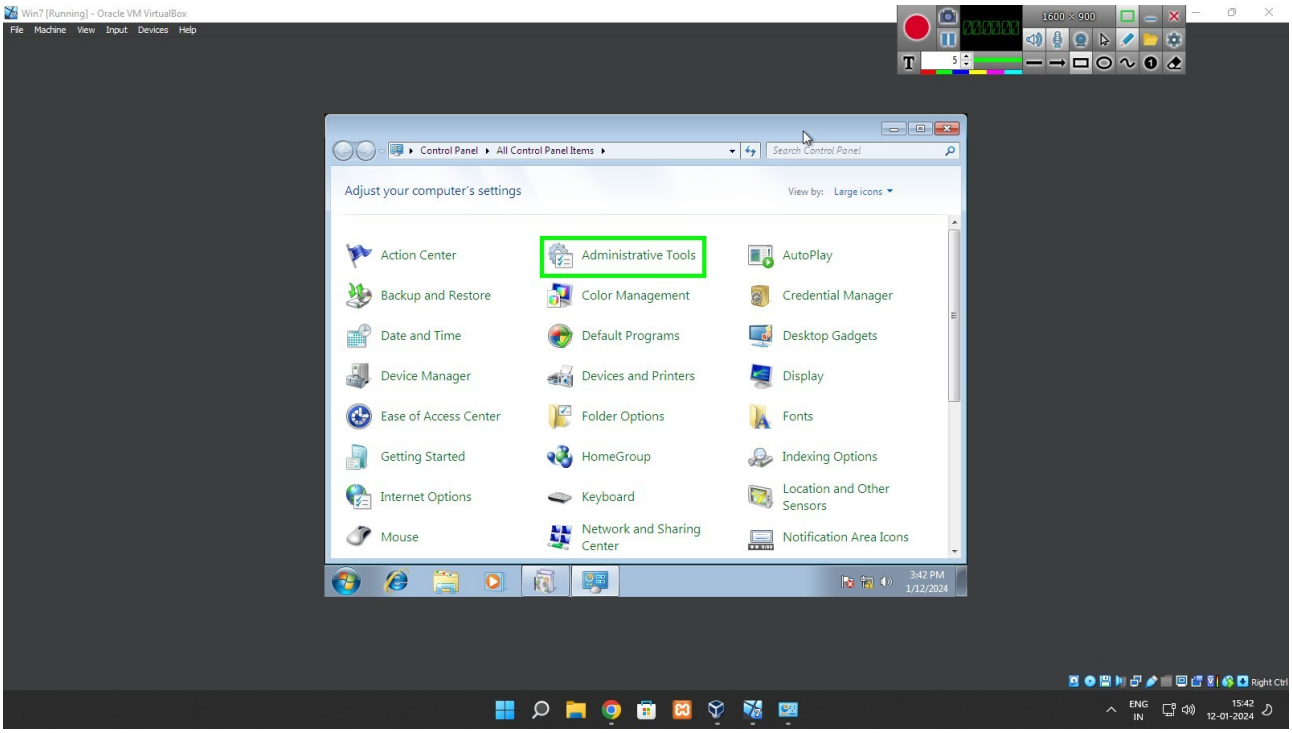
- Select Internet Information Services(IIS) , Internet Information Services Hostable Web Core and TFTP client

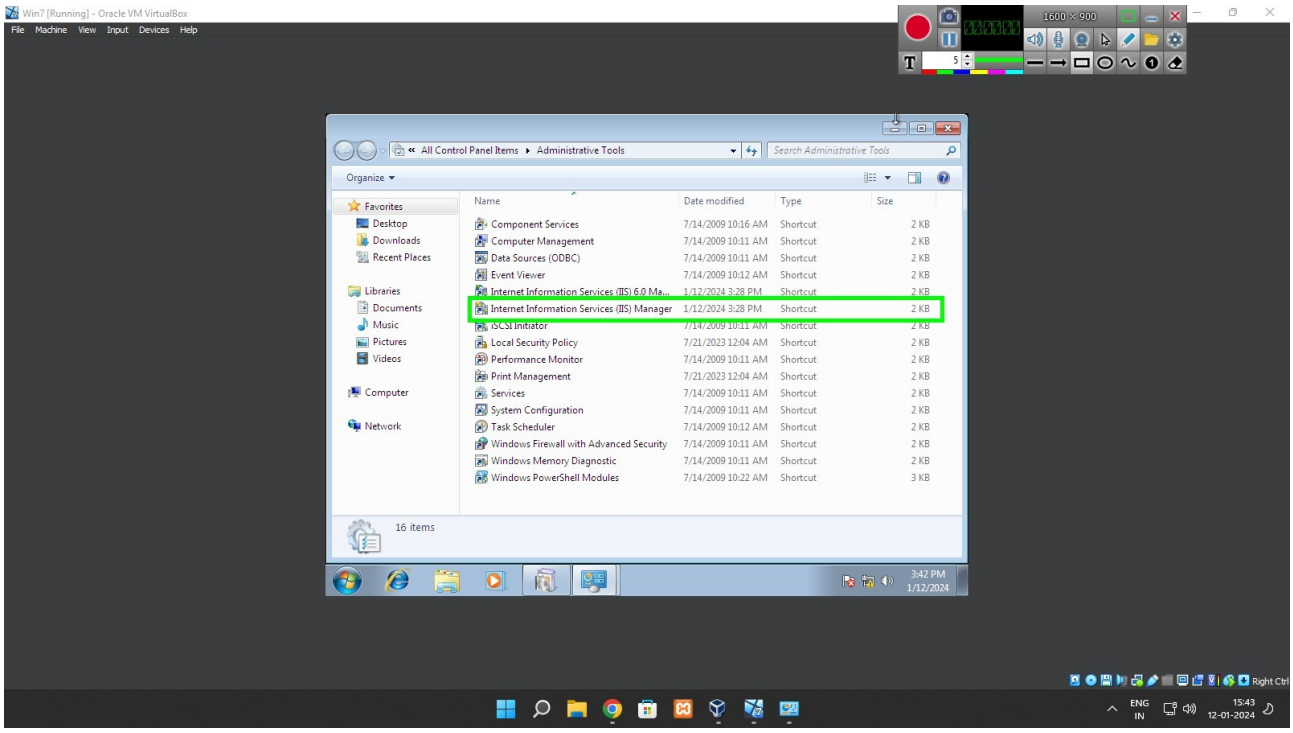


- Then click ok
- Wait for process to complete
- After process is complete we can create out ftp server

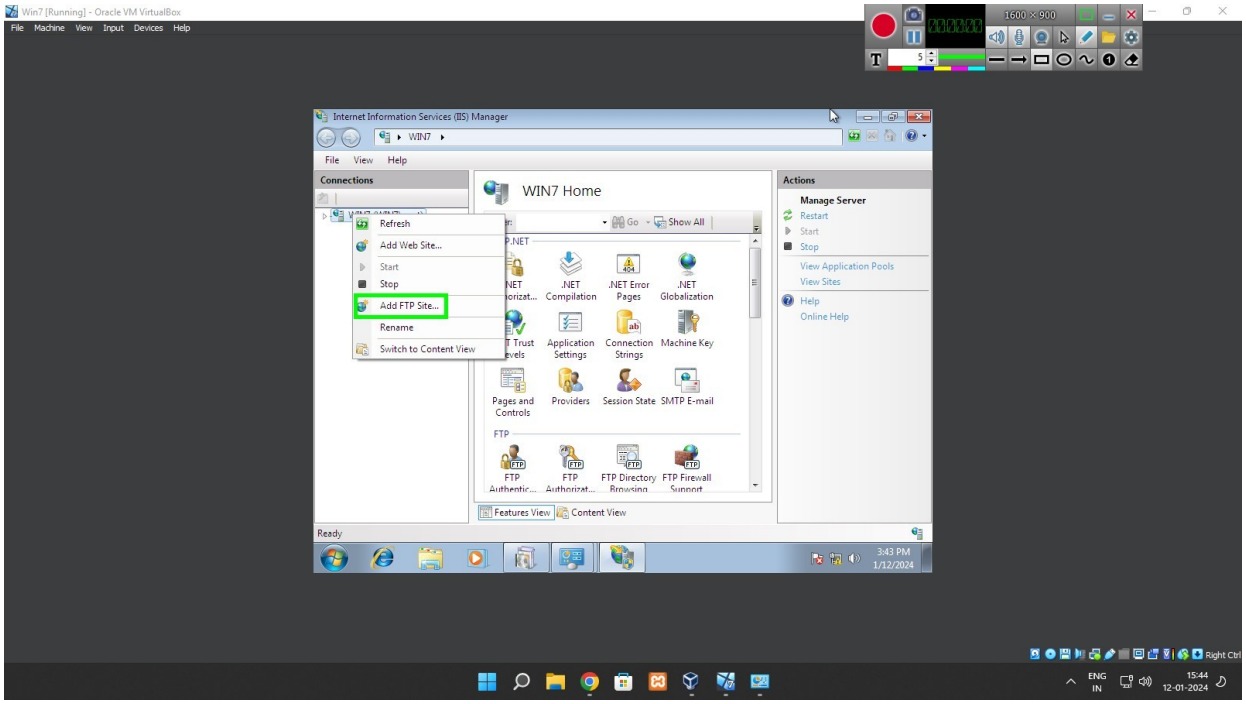
Note :- Any system can only create one ftp server

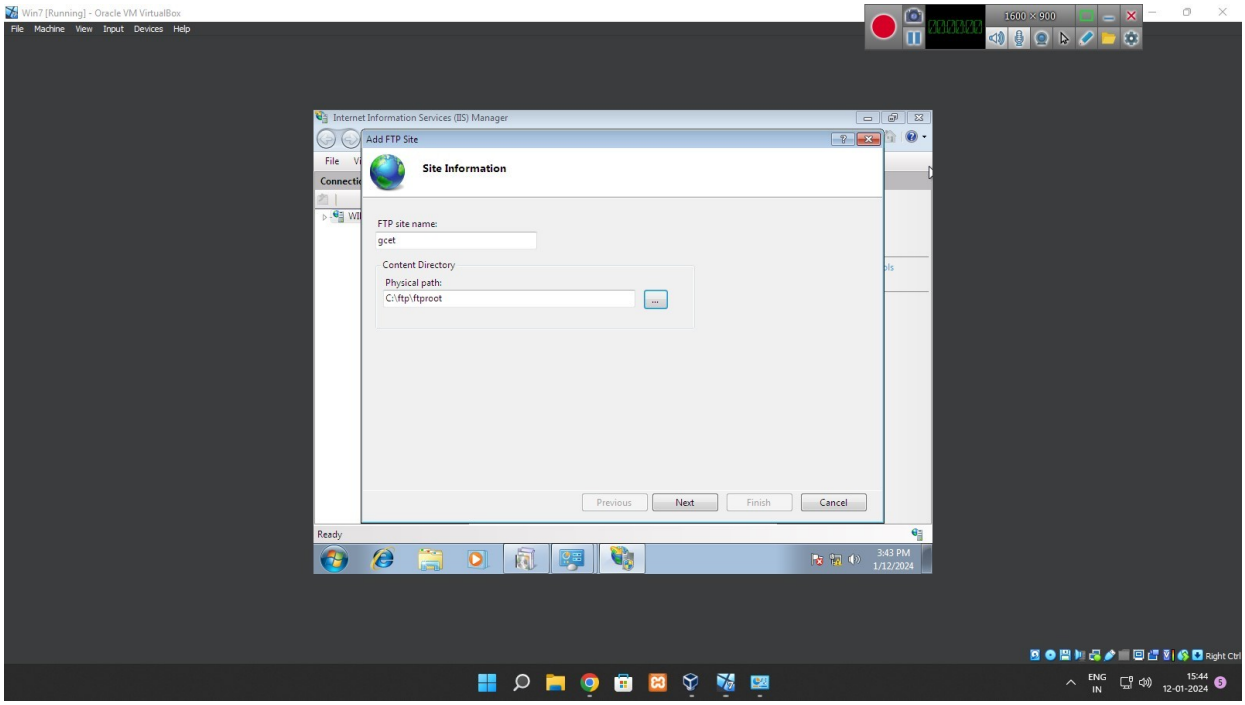
- After process is done Go to Control Panel\All Control Panel Items\Administrative Tools and select simple IIS manager and click on it





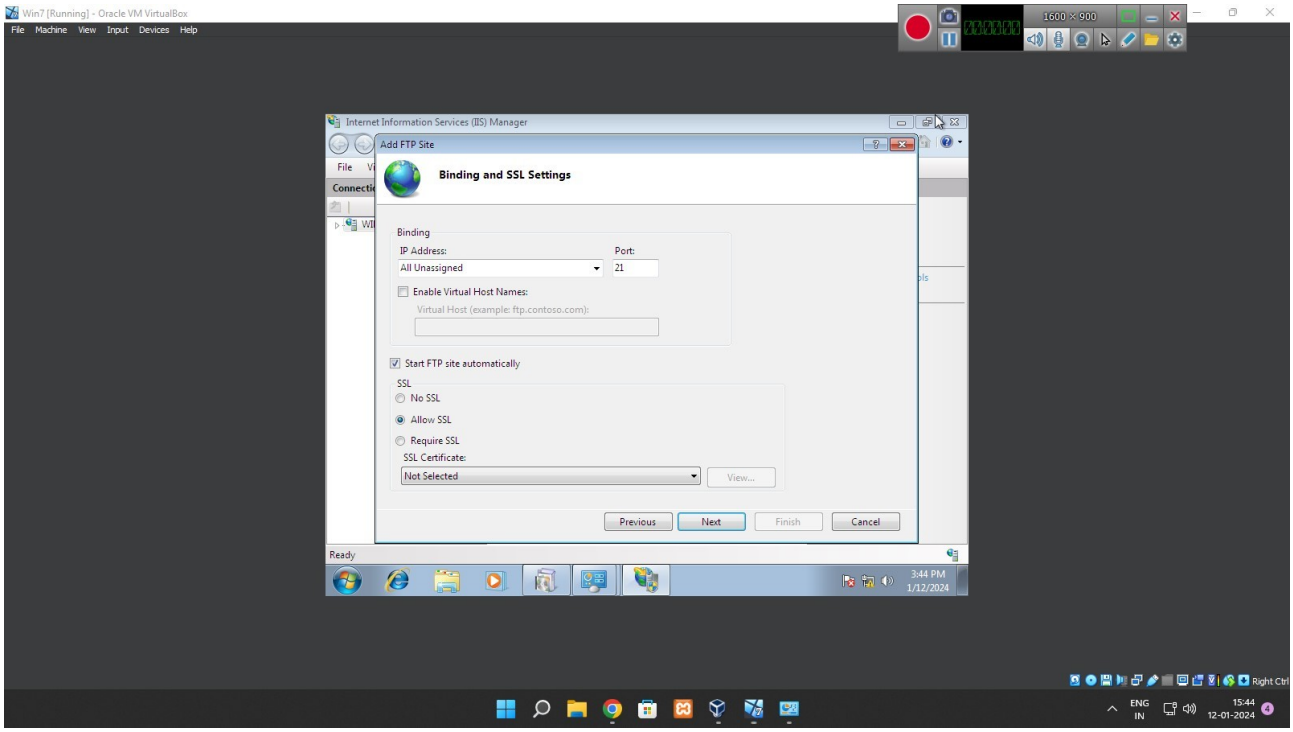
- Add ftp site and name it in following way :

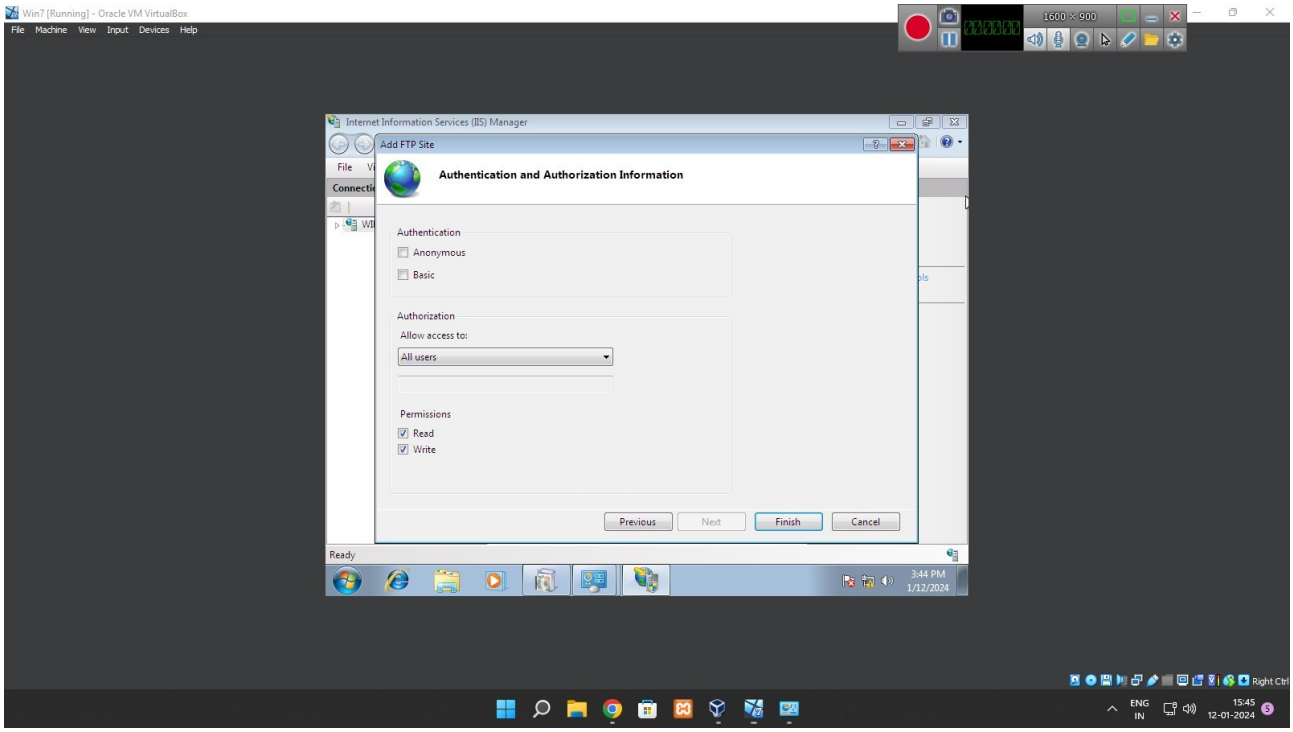




- Now click on next

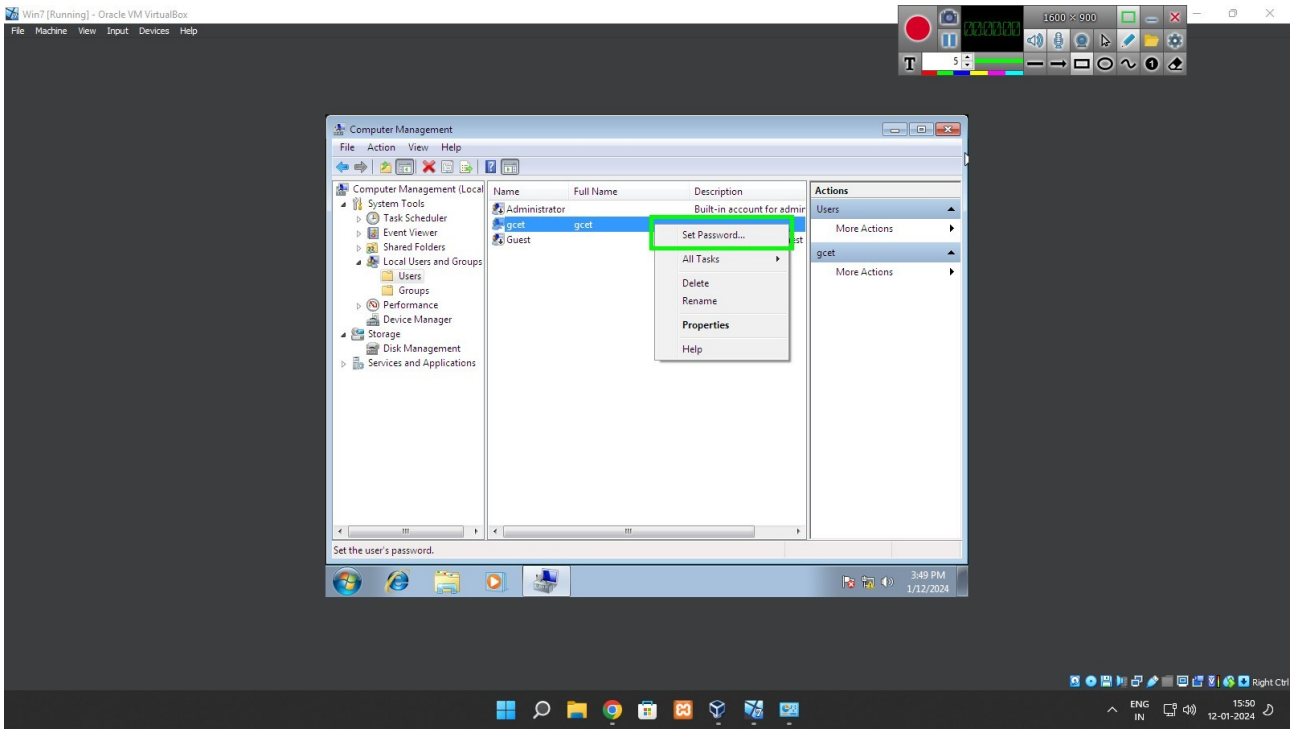
- Allow ssl certificate click next and if you want you may allow authentication when starting server for other user and click finish



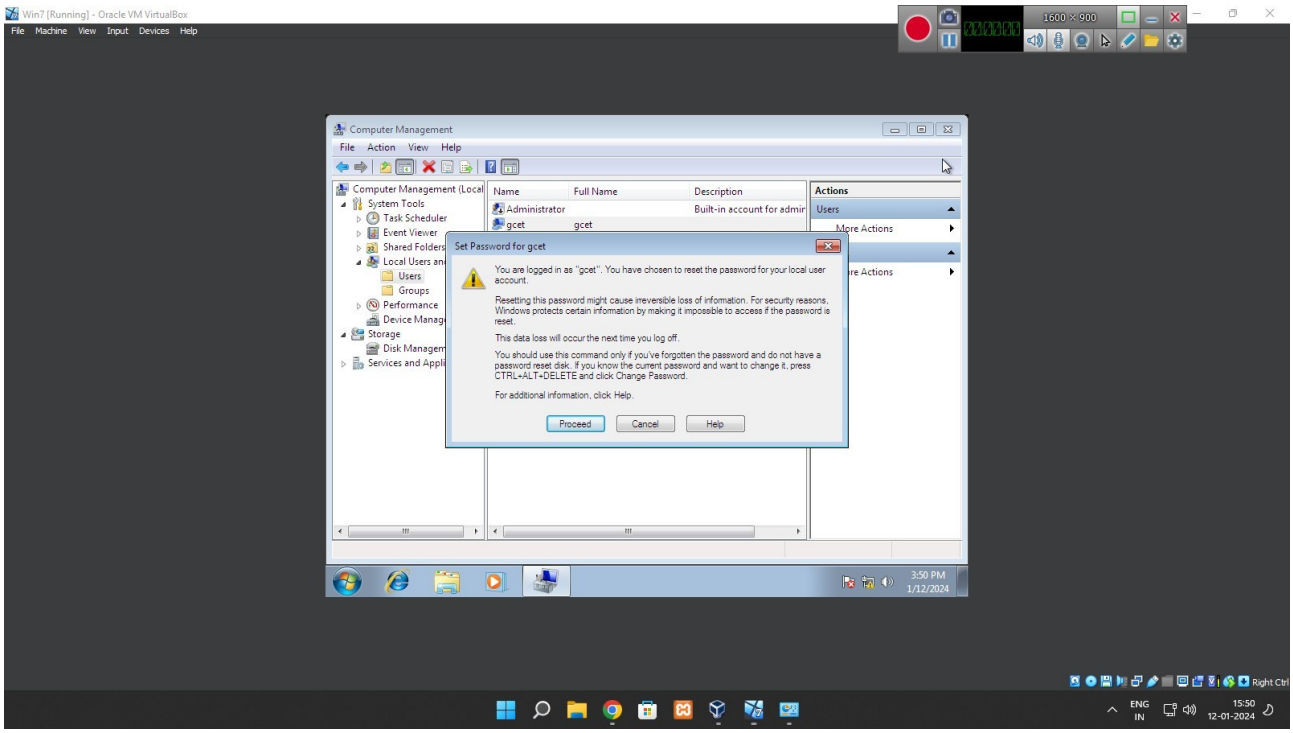


- Now we can set its password

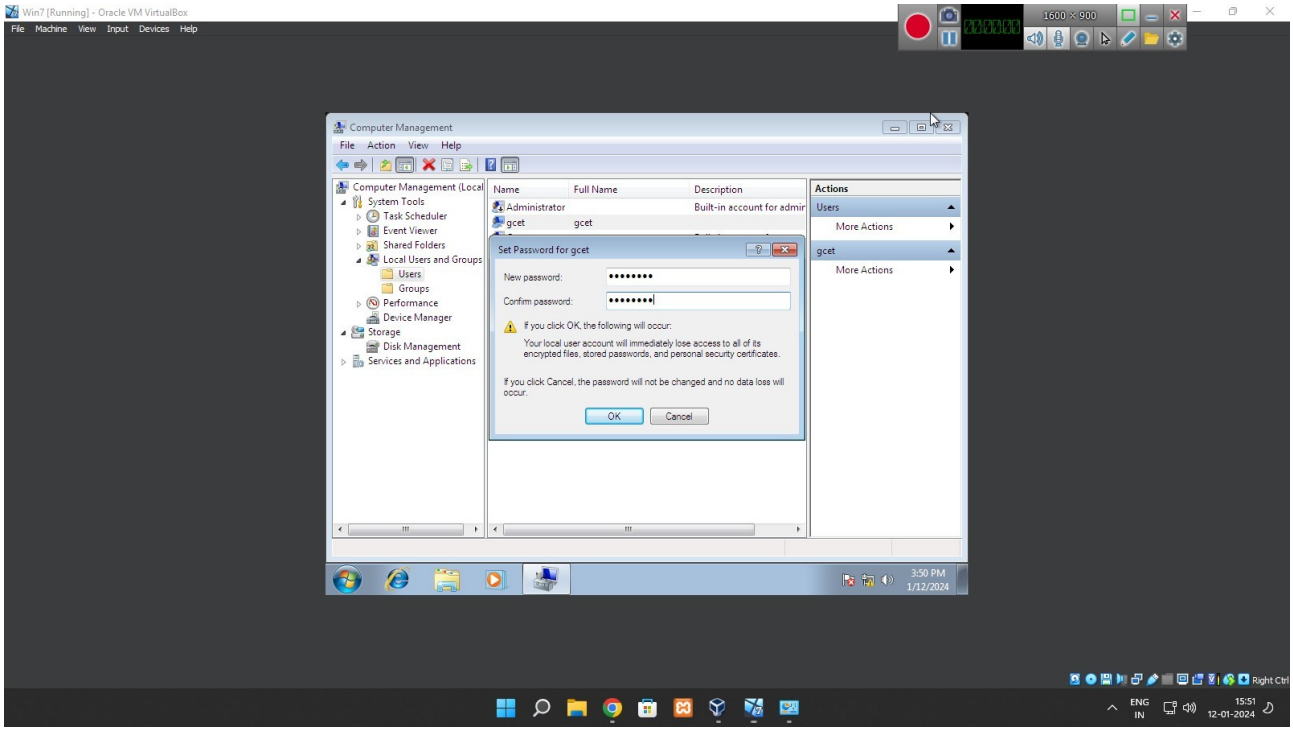
- For password setting setting go to
  Computer management > Local users and Groups > Users
  Hear you can see our ftp server name right click on it and select Set Password option



- Click Proceed

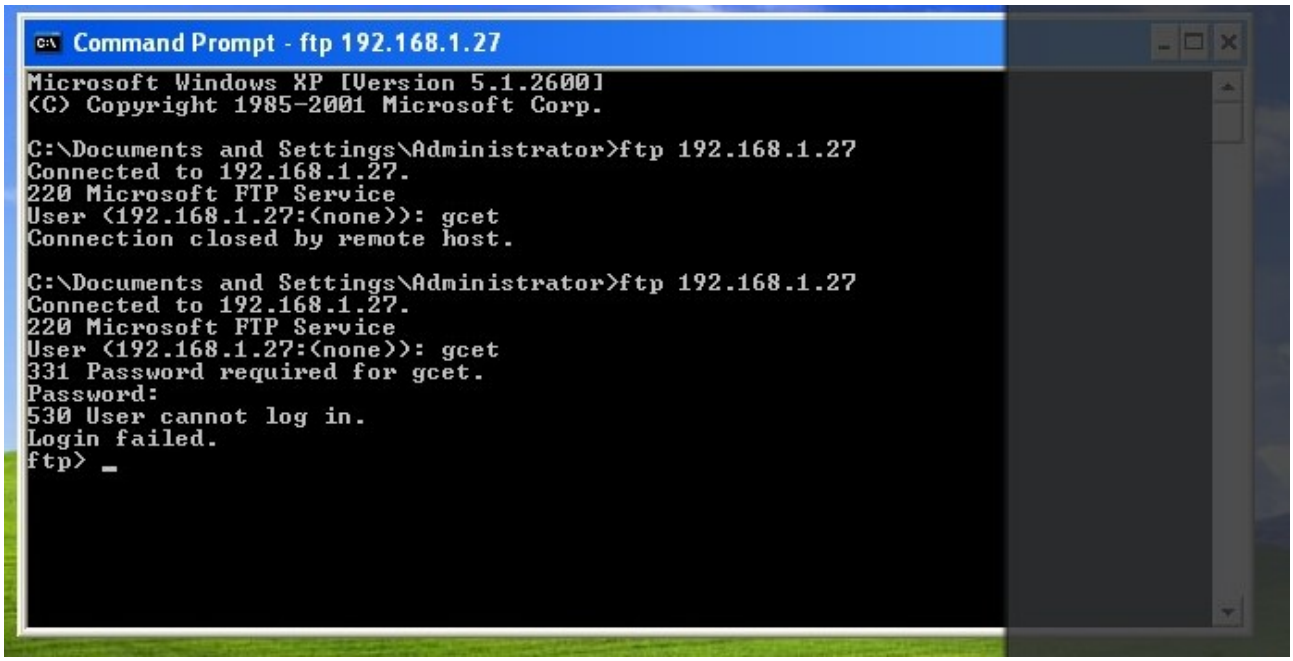


- Enter your password & click Ok



- You can access FTP server from client machine by running following in CMD
  > ftp 192.168.1.27

  192.168.1.27 is IP of server



Hence our ftp server setting is completed

Ettercap

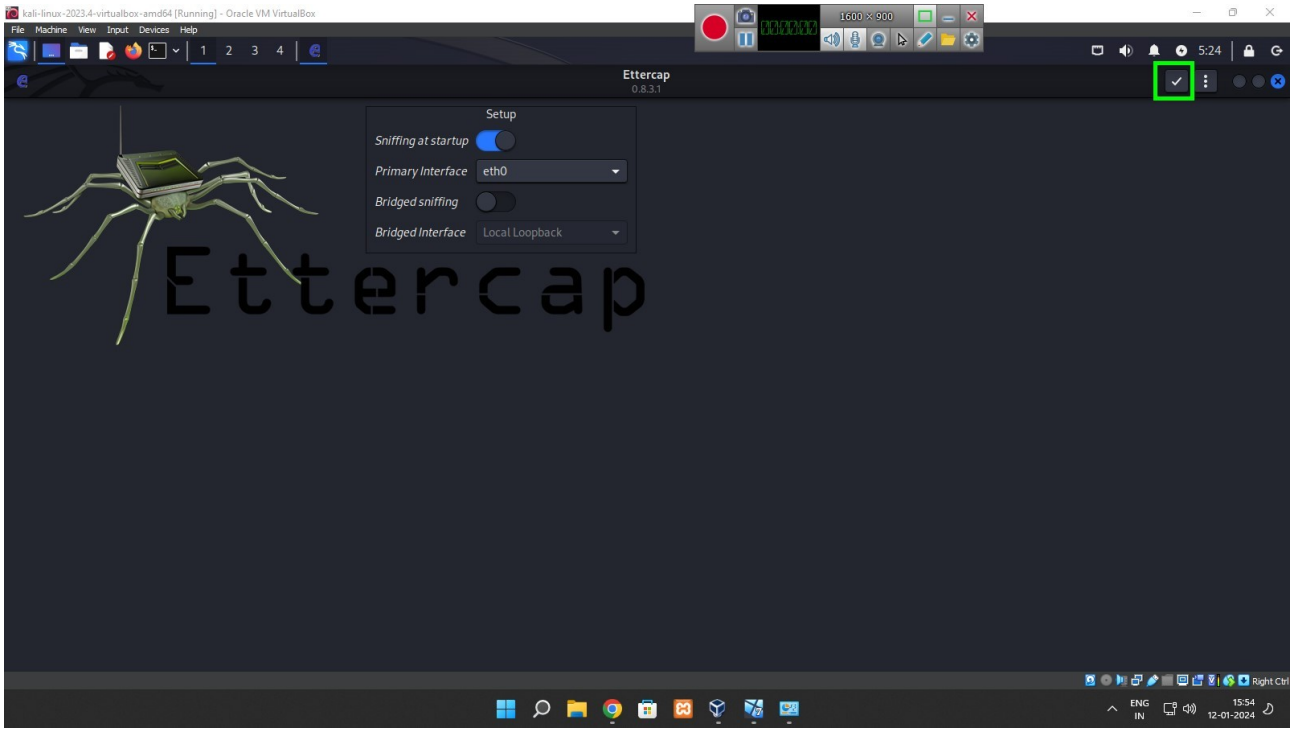
- Ettercap is a comprehensive suite for man in the middle attacks.
-
- Ettercap supports active and passive dissection of many protocols (even encrypted ones) and includes many feature for network and host analysis.
- Data injection in an established connection and filtering (substitute or drop a packet) on the fly is also possible, keeping the connection synchronized.
- Many sniffing modes are implemented, for a powerful and complete sniffing suite. It is possible to sniff in four modes: IP Based, MAC Based, ARP Based (full-duplex) and PublicARP Based (half-duplex).
- Ettercap also has the ability to detect a switched LAN, and to use OS fingerprints (active or passive) to find the geometry of the LAN.

➔ Ettercap enables us to place ourselves in the middle between two machines and then;

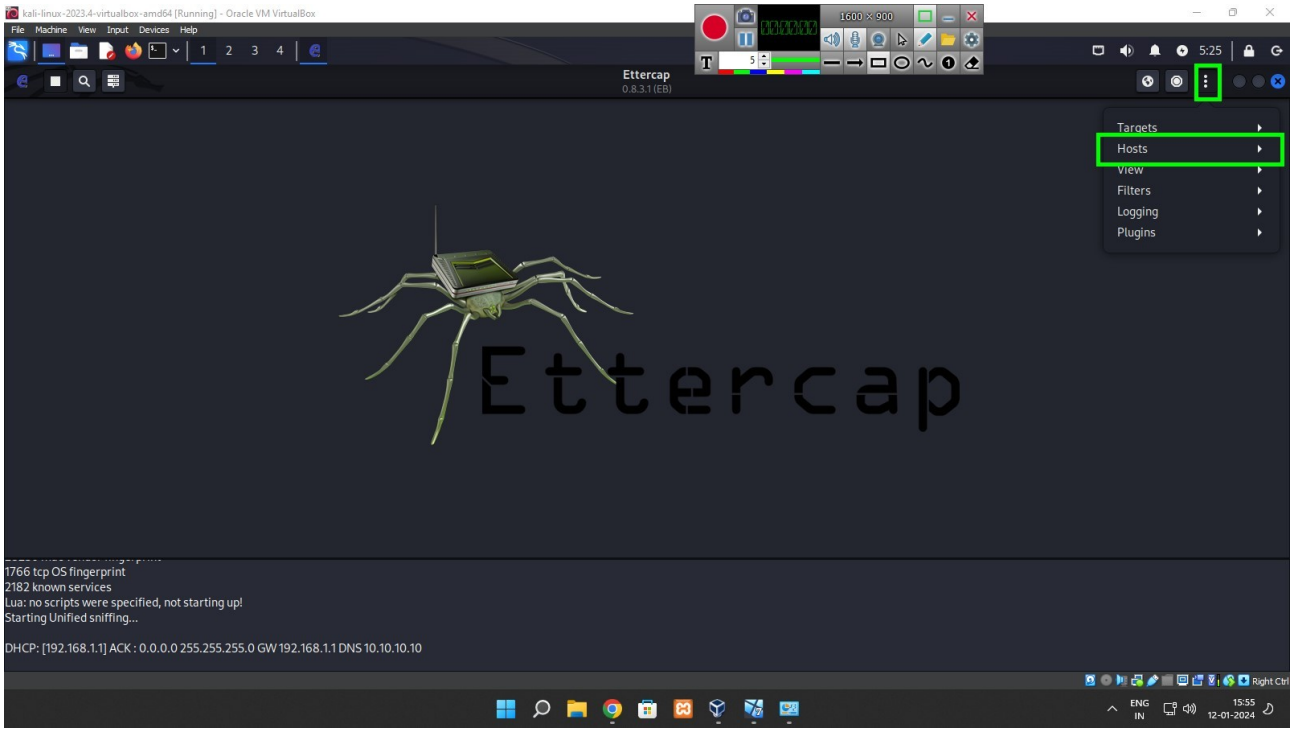
- infect the traffic with malware
- delete traffic
- sniff passwords
- provide fake certificates for HTTPS
- DNS spoof

Doing arp poisoning attack using Ettercap to steal ftp server Password

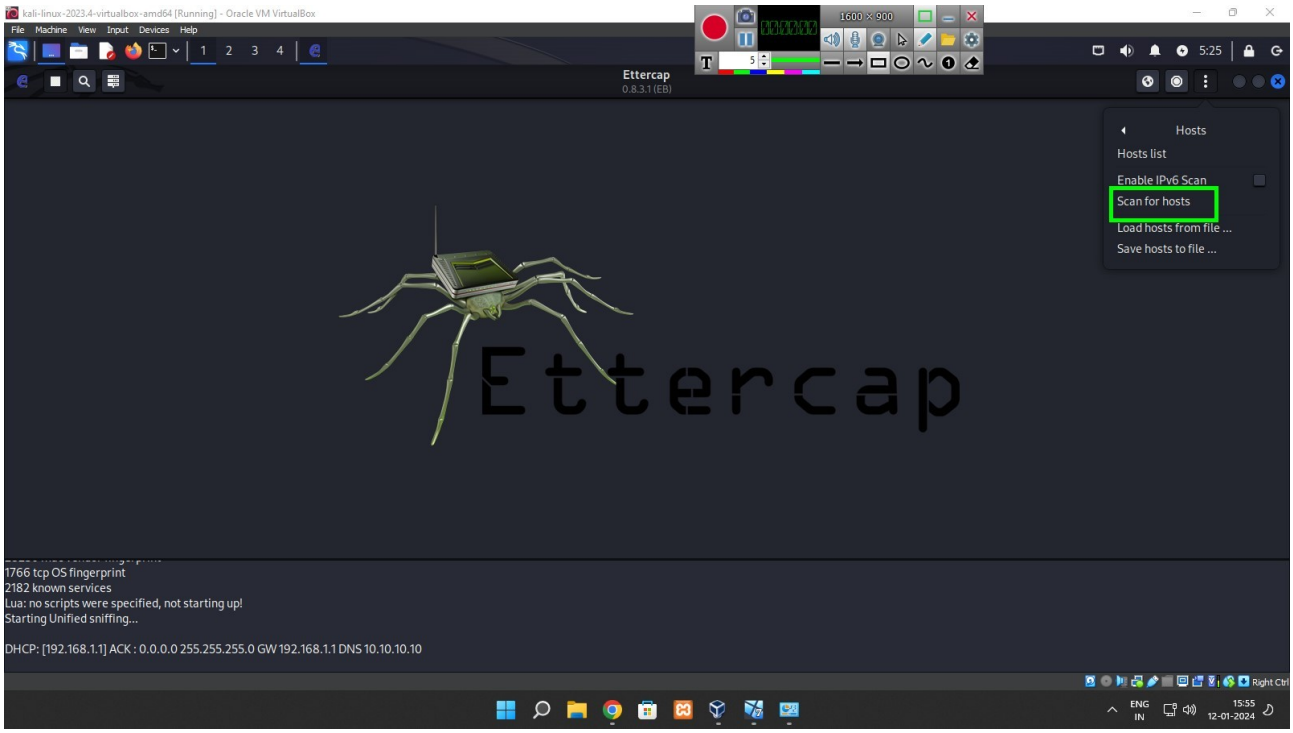
➔ Start Ettercap & click on the right tick symbol



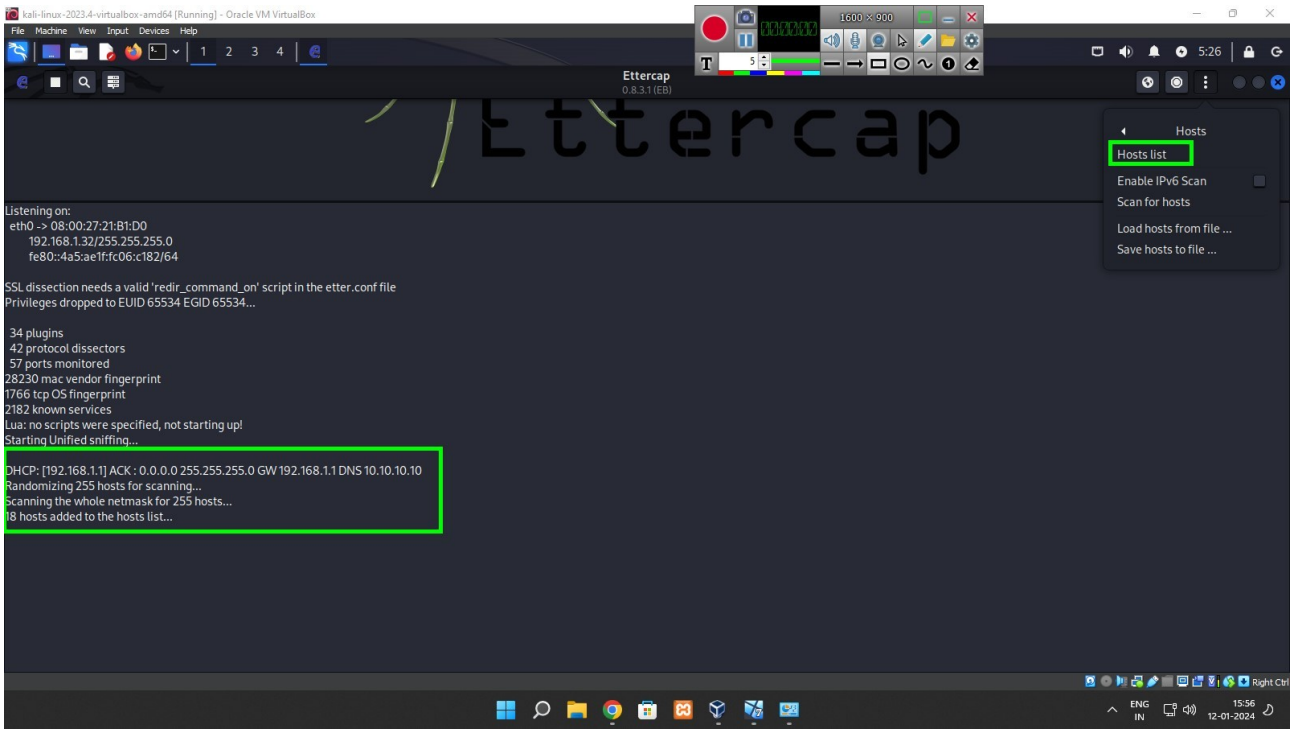
➔ After starting ettercap click on the three dots and select host option



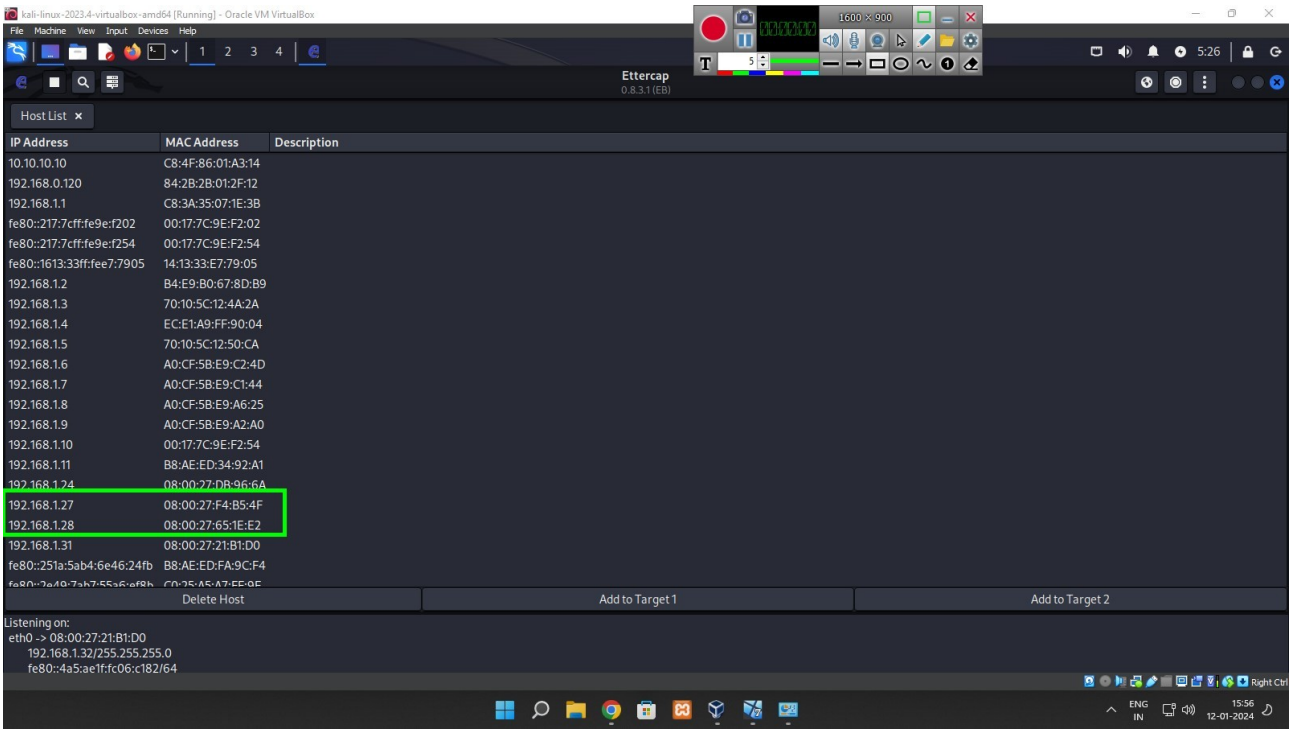
➔ After selecting host option scan for hosts



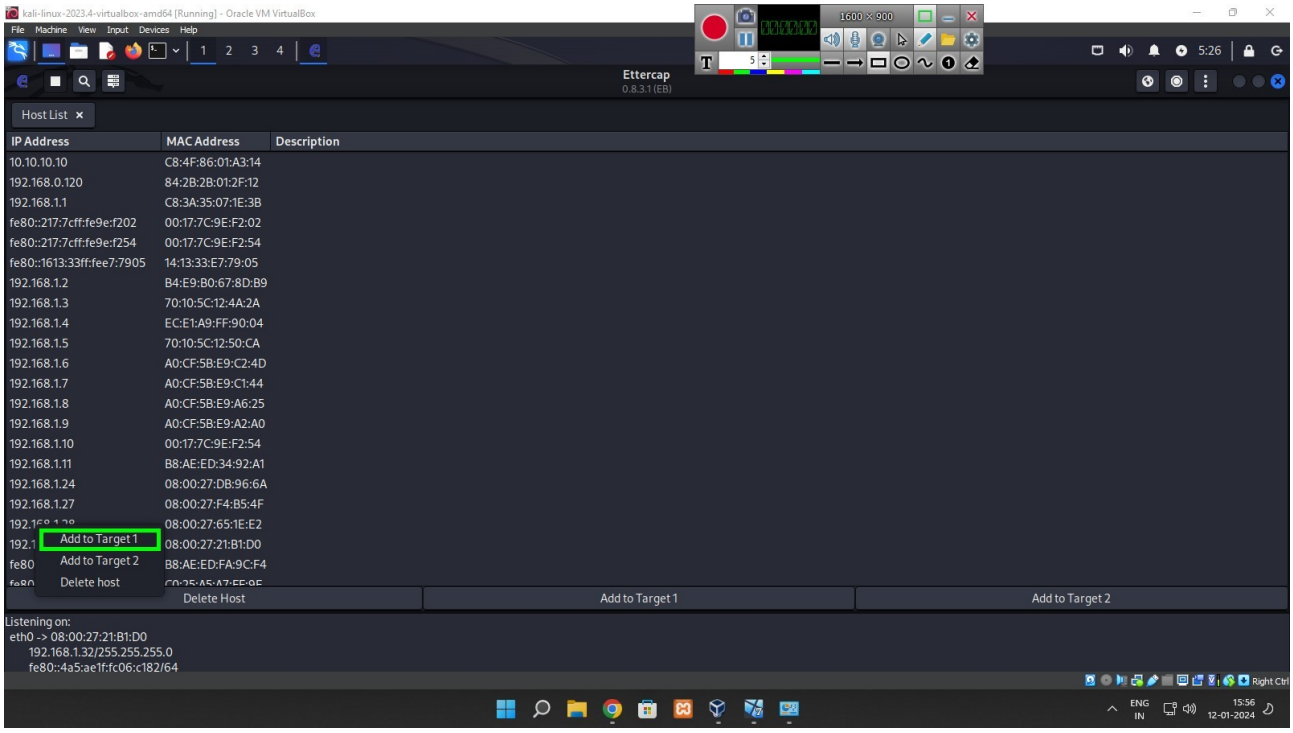
➔ After scanning for hosts go to host list in Hosts option



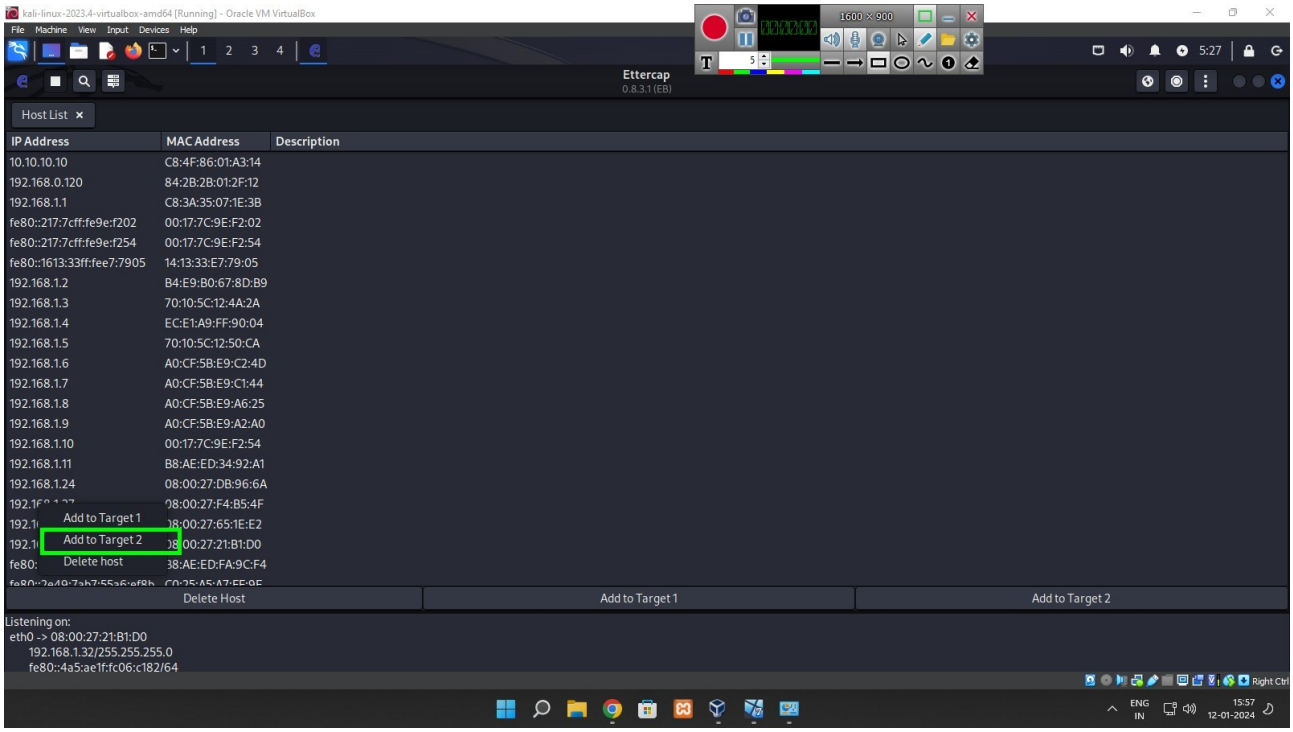
➔ Now we can view all hosts connected in LAN and also our targets



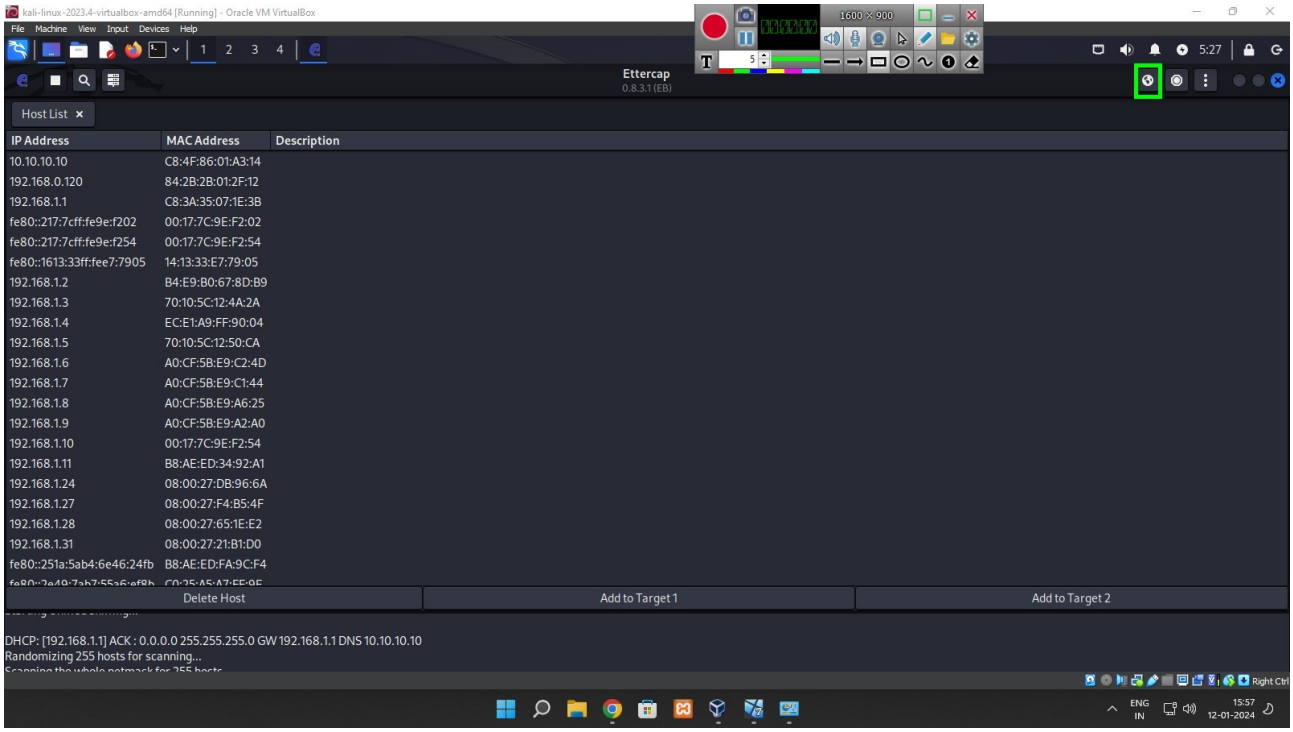
➔ Select client as target 1 by right clicking on it



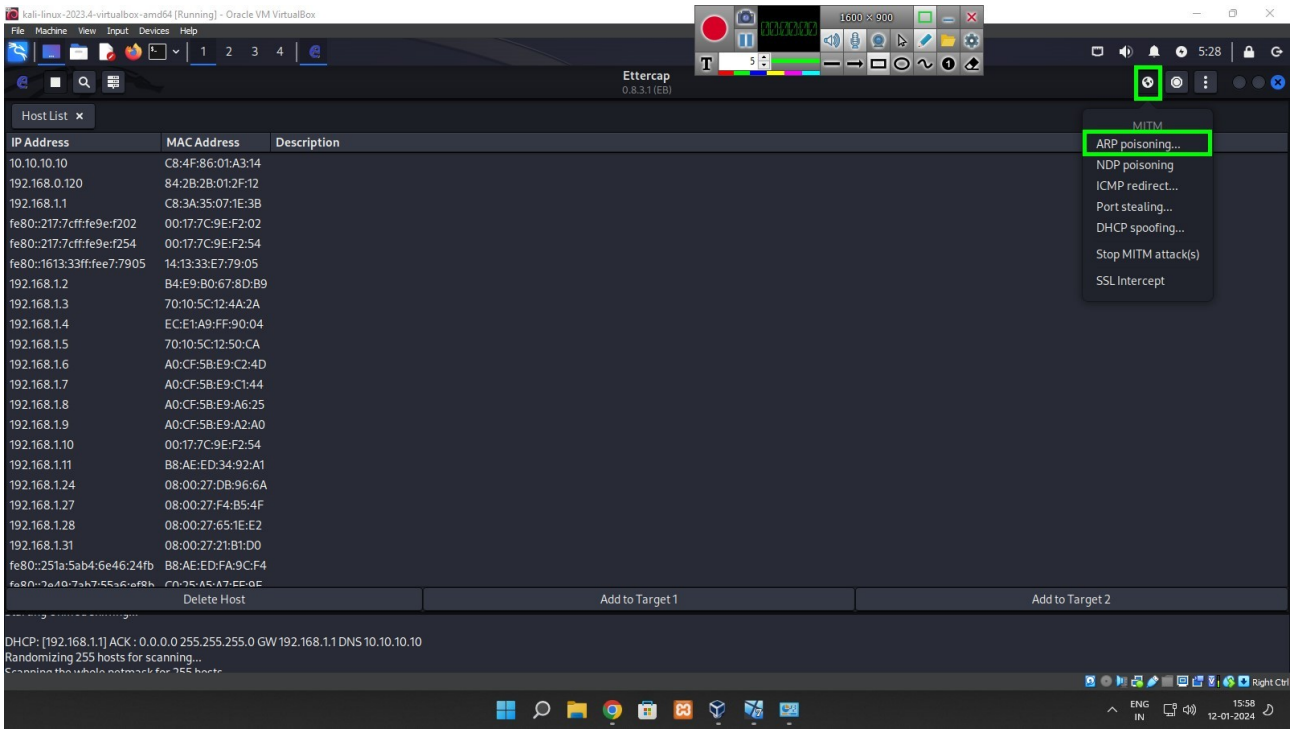
➔ Select server as target 2



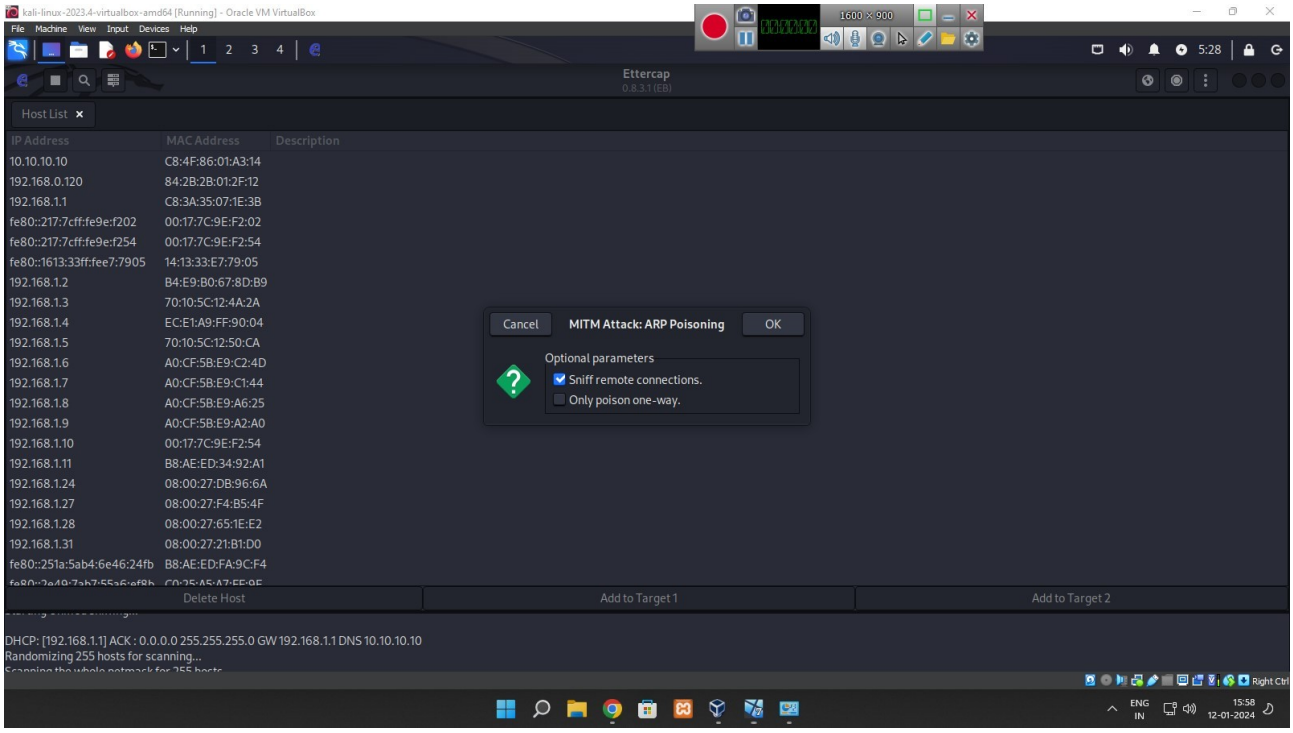
➔ Select symbol of globe on top right corner



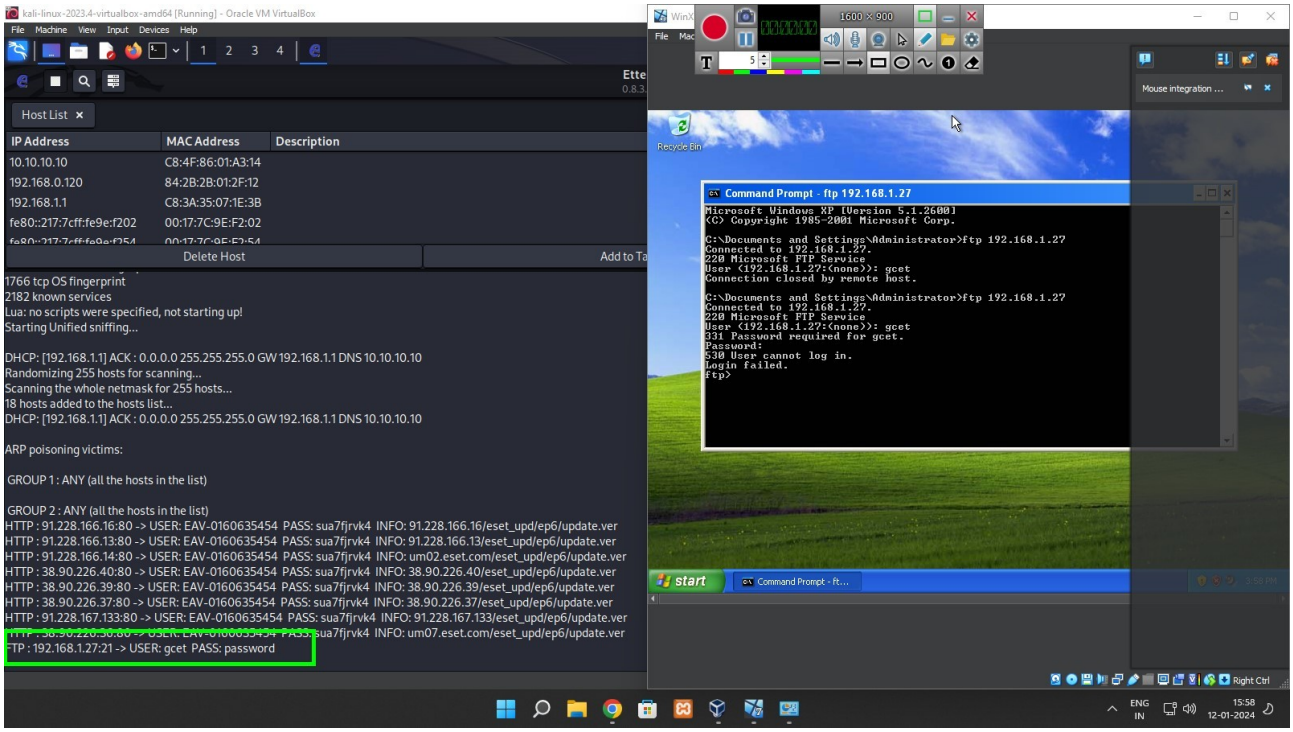
➔ Select ARP poisoning option



➔ Start Sniffing



➔ As client tries to connect to ftp server we can see it's password



Hence Password Cracking Is Successful.

Wireshark

Wireshark is a network “sniffer” - a tool that captures and analyzes packets off the wire. Wireshark can decode too many protocols .

Wireshark is a widely used, open source network analyzer that can capture and display real-time details of network traffic. It is particularly useful for troubleshooting network issues, analyzing network protocols and ensuring network security.

Networks must be monitored to ensure smooth operations and security. Popular with academic institutions, government agencies, corporations and nonprofits, Wireshark is one such tool that can offer an in-depth view into network activities, diagnose network performance issues or identify potential security threats.

Key features of Wireshark

Wireshark seeks to simplify and enhance the process of network traffic analysis. Each function is designed to offer unique insights and control over network activities. Here are some of its core features:

- *Packet capture (PCAP).* Converts network traffic into a human-readable format, making it easier to understand and diagnose concerns.
- *Real-time analysis.* Provides a live view of network traffic, offering immediate insights into ongoing network activities.
- *Filtering capabilities.* Enables users to focus on specific types of network traffic, making analysis more efficient and targeted.
- *Graphical user interface (GUI).* Designed for ease of use, ensures that both beginners and experts can navigate and analyze data effectively.

Common uses for Wireshark

Wireshark can be used to examine the details of traffic at a variety of levels, ranging from connection-level information to the bits constituting a single packet.

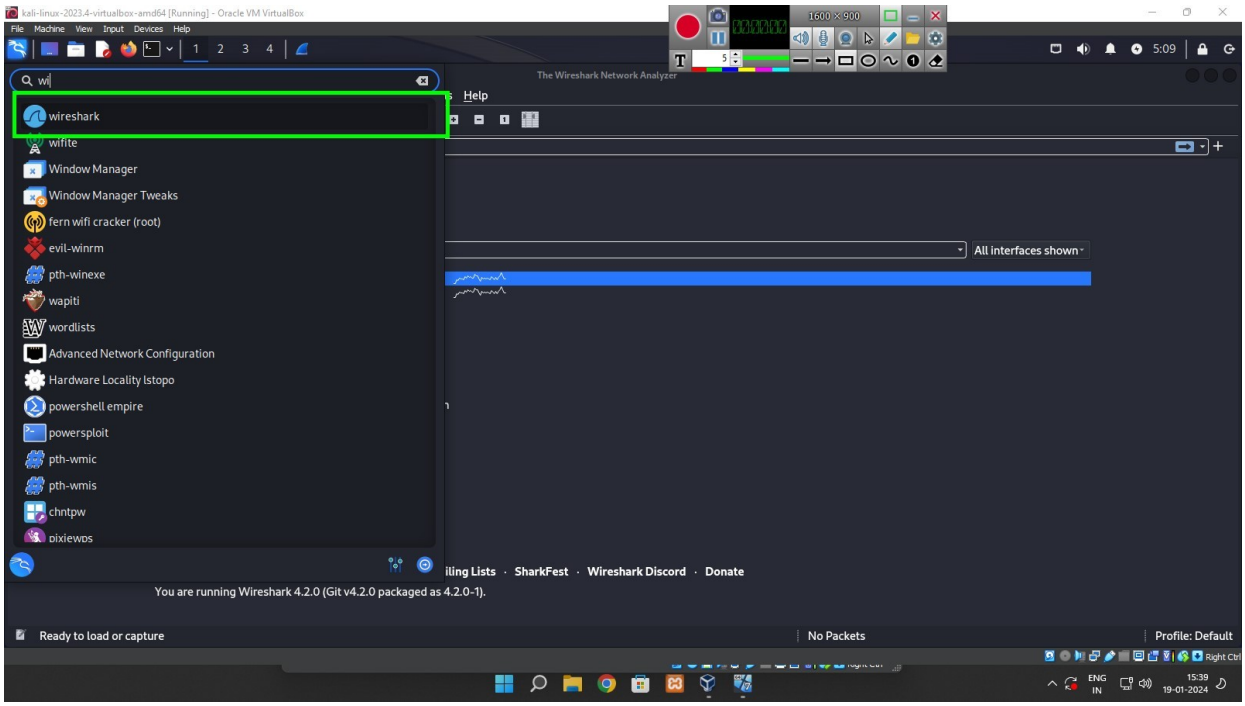
PCAP can provide a network administrator with information about individual packets, including transmit time, source, destination, protocol type and header data. This information can be useful for evaluating security events and troubleshooting network security device issues.

Wireshark's capabilities extend beyond just monitoring to address other network administration tasks:

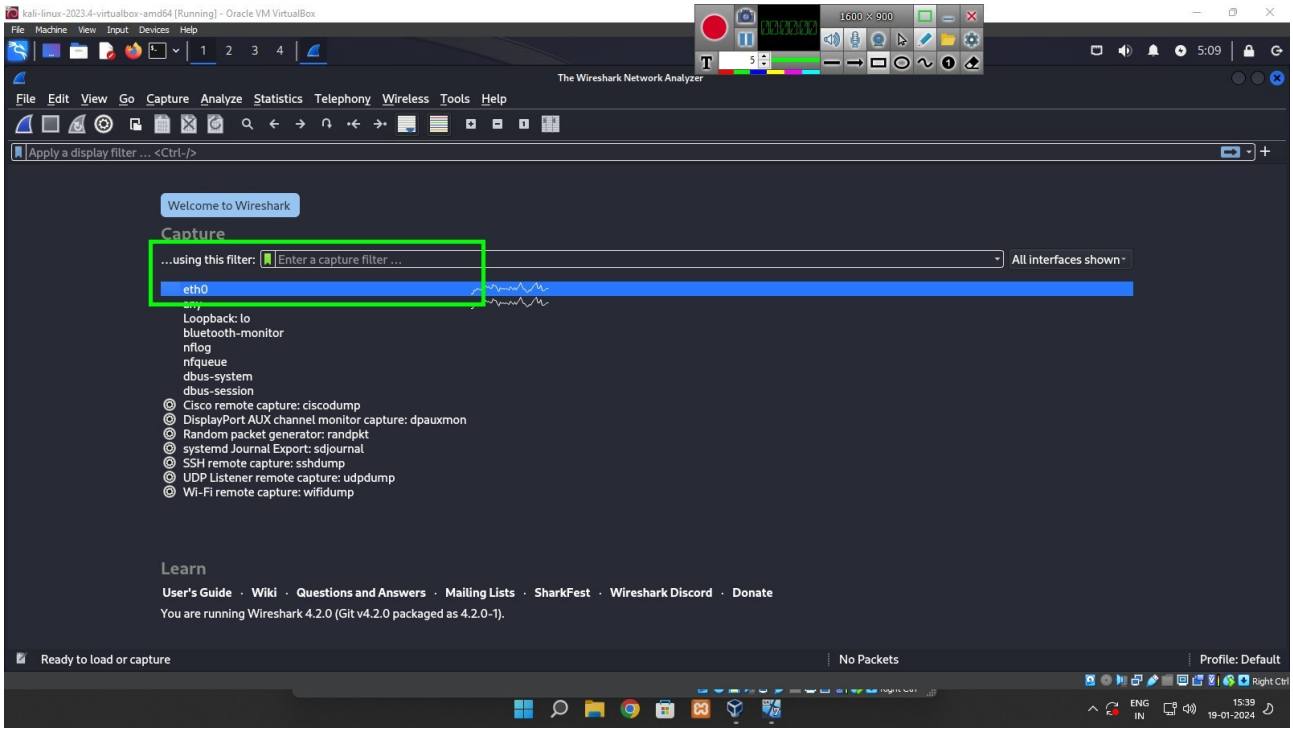
- *Network troubleshooting.* Pinpoints and resolves network issues with the comprehensive data Wireshark provides.
- *Security analysis.* Detects and analyzes potential security threats in the network.
- *Performance analysis.* Monitors and optimizes network performance to ensure smooth operations.
- *Protocol analysis.* Gains insights into the behavior of individual protocols within the network.

Cracking password of FTP using Wireshark

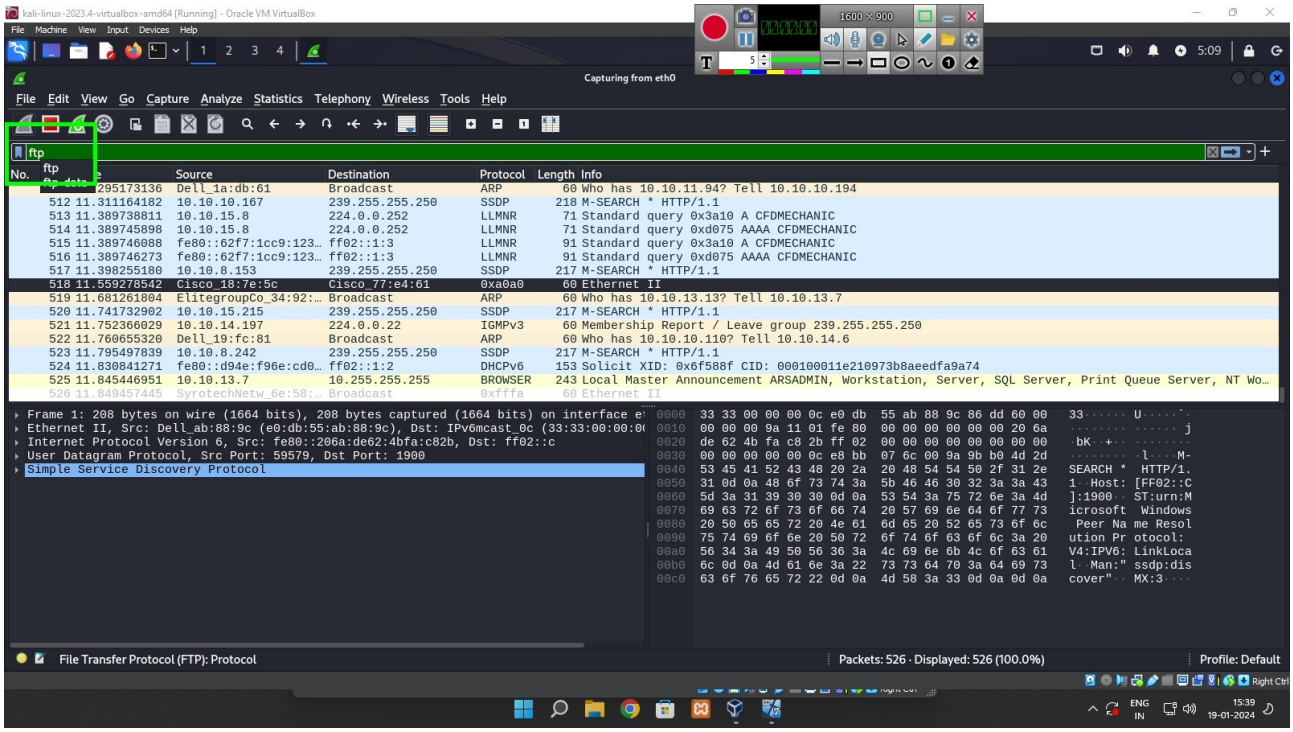
- Open Wireshark software in kali & make sure your computer is in same LAN as targets



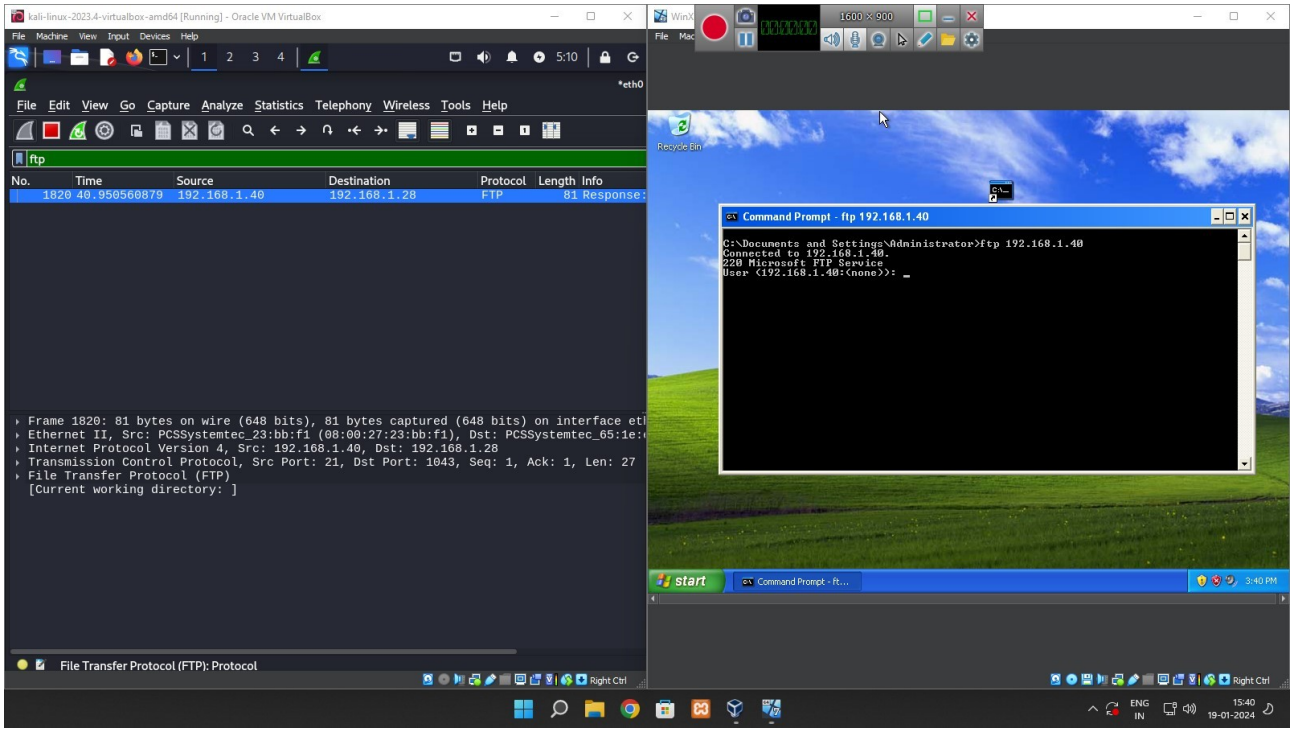
- Select eth0 as preference



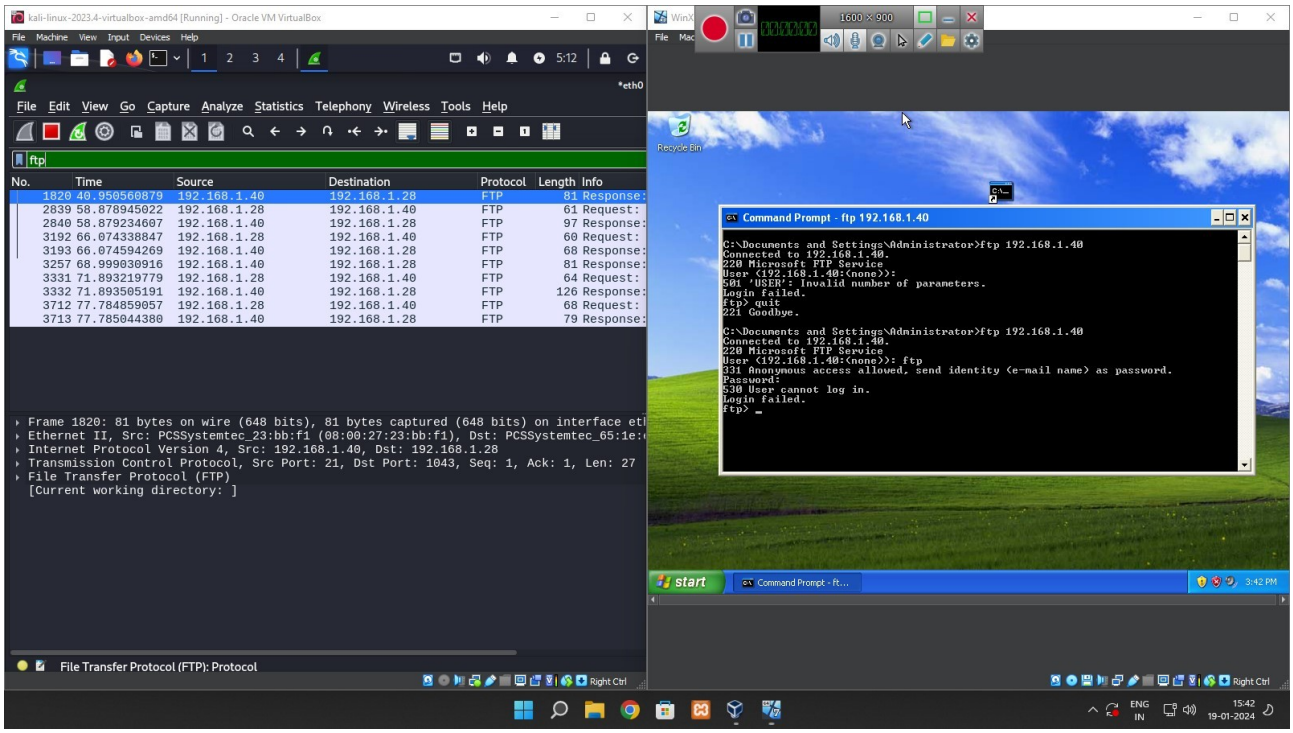
- Search for FTP protocol in search bar



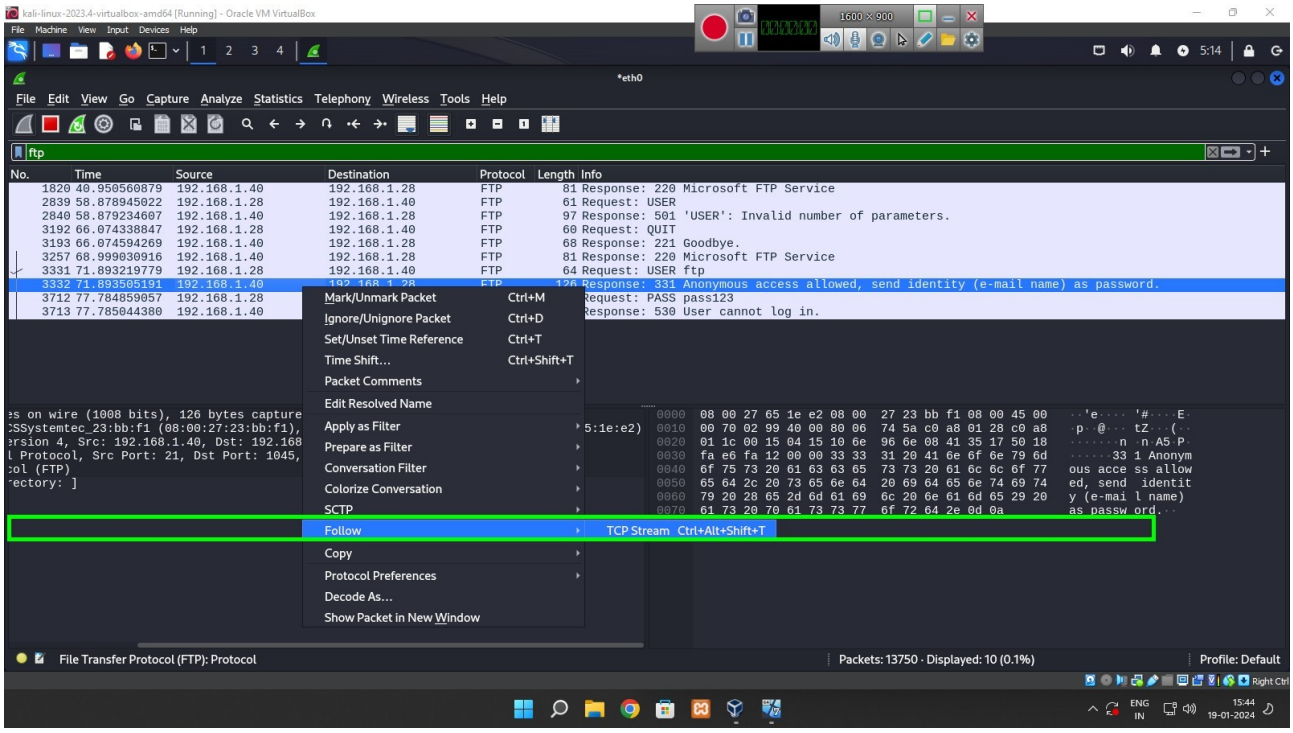
- Now let the client connect to server



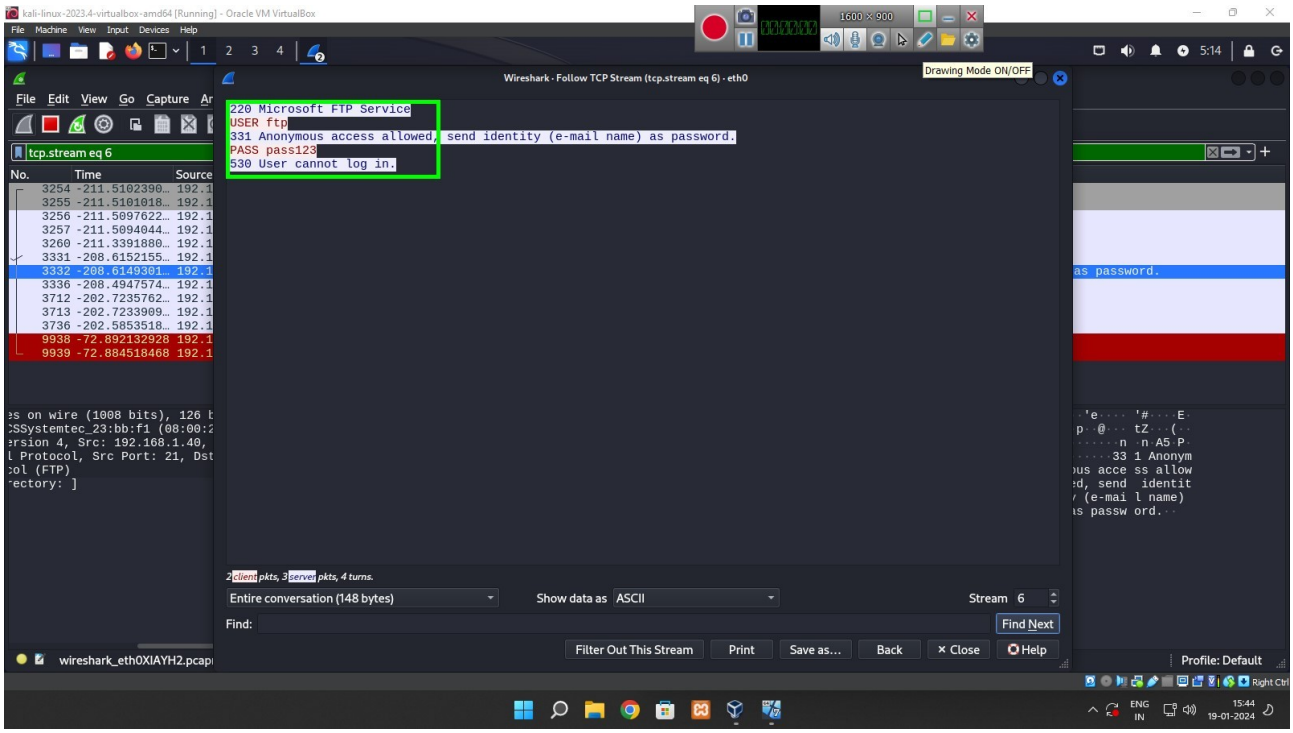
- Now we can see in wireshark that all the conversations between client and server are listed



- Right click on any one conversation select Follow > TCP Stream



- Now we can see whole conversation in human readable form in that we can see User name & Password



Hence our password cracking is successful