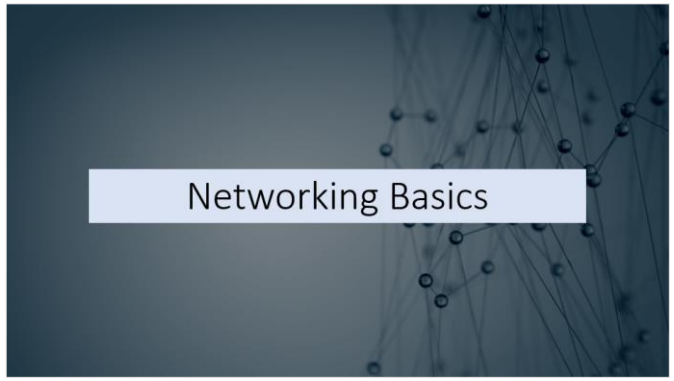
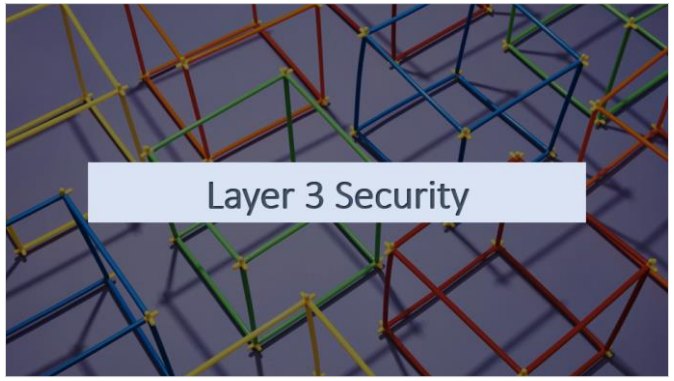
# Network Security and Penetration Testing

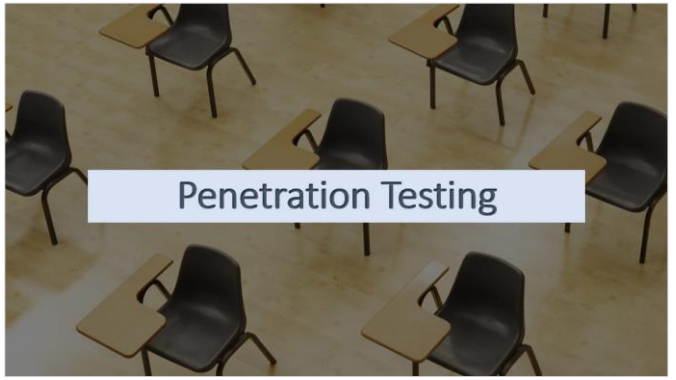
ITSM Session 9

# Session Overview





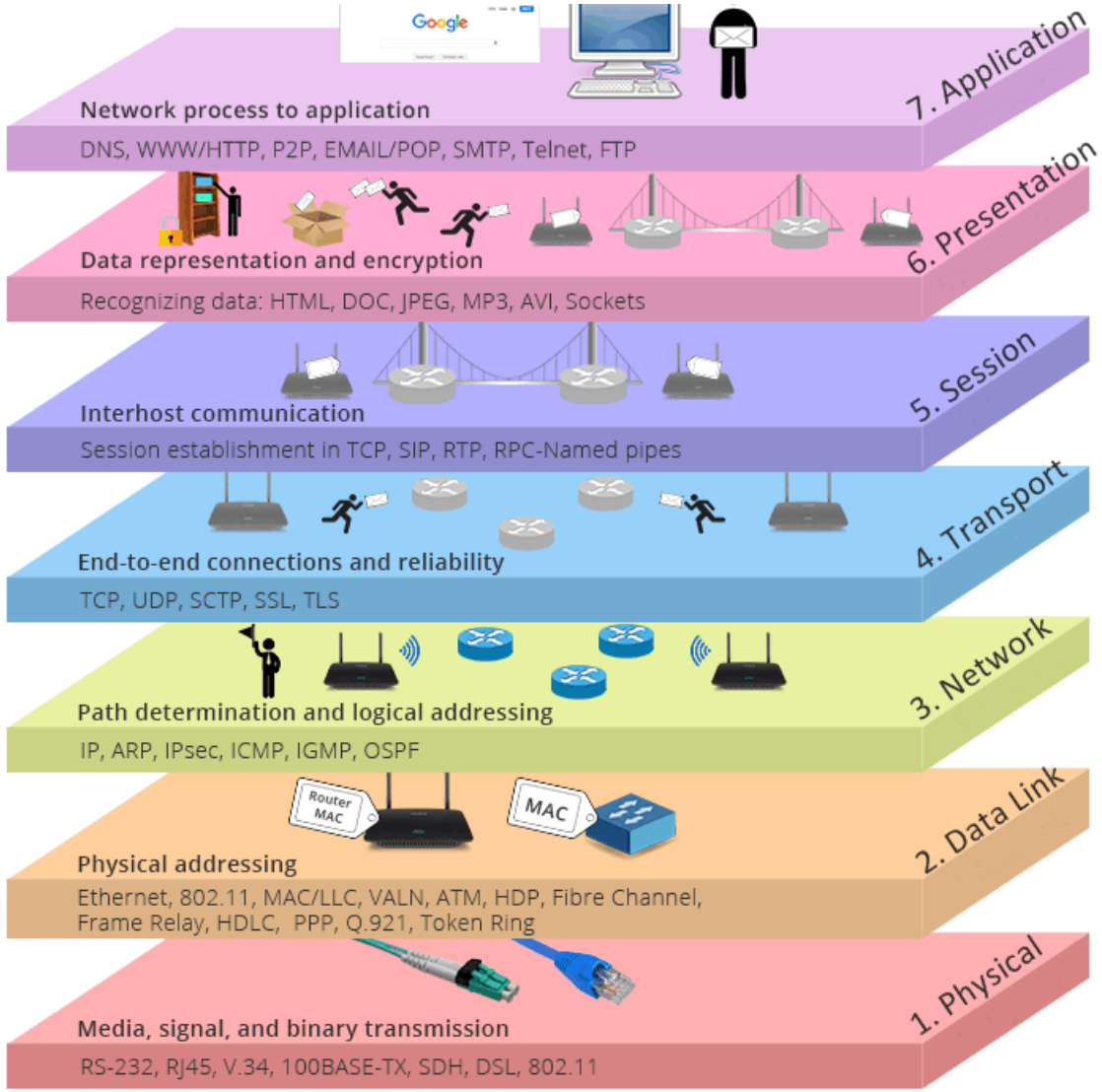



# Networking Basics


# Networking Devices

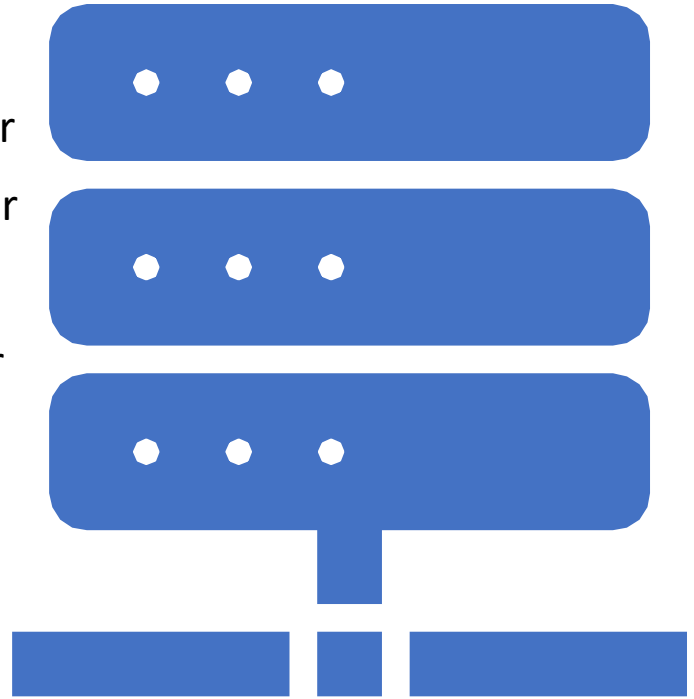
# Terminology

- **OSI:**
  OSI stands for **Open Systems Interconnection**. It is a reference model that specifies standards for communications protocols and also the functionalities of each layer.
- **Protocol:**
  A protocol is the set of rules or algorithms which define the way how two entities can communicate across the network and there exists different protocol defined at each layer of the OSI model. Few of such protocols are TCP, IP, UDP, ARP, DHCP, FTP and so on.



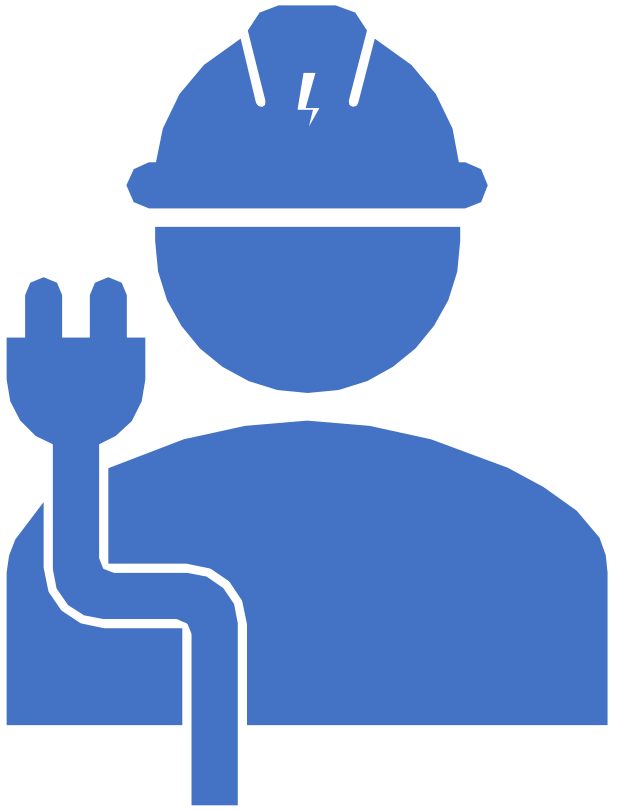
# UNIQUE IDENTIFIERS OF NETWORK

- Hostname -- Application Layer
- Port number -- Transport Layer
- IP Address -- Network Layer
- MAC Address -- Datalink Layer



# Command Line tools

- ping
- tracert
- netstat
- nslookup
- whois



# Wifi Security

# Terminology

Access point

Gateway

QoS

Bandwidth

Firewall

VPN

Port forwarding

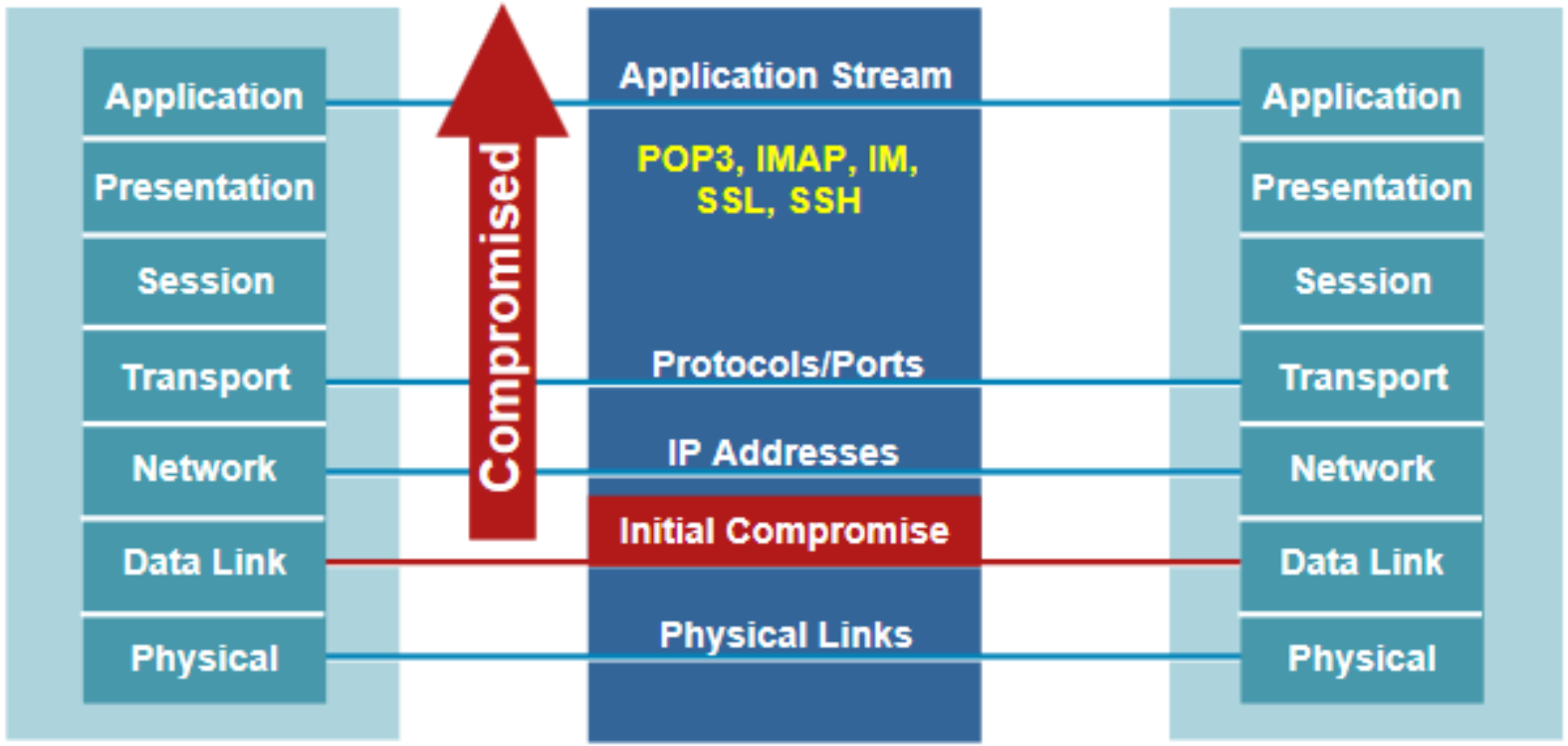
# Protect Your WiFi Network

- While WPA2 offers more protection than WPA and therefore provides even more protection than WEP, the security of your router heavily depends on the password you set. WPA and WPA2 let you use passwords of up to 63 characters.
- Use as many various characters in your WiFi network password as possible. Hackers are interested in easier targets, if they can't break your password in several minutes, they will most likely move on to look for more vulnerable networks.
- Remember :
  - WPA2 is the enhanced version of WPA;
  - WPA only supports TKIP encryption while WPA2 supports AES;
  - Theoretically, WPA2 is not hackable while WPA is;
  - WPA2 needs more processing power than WPA;

# Layer 2 Security

# Lower Levels Affect Higher Levels

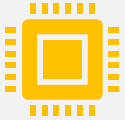
- Unfortunately this means if one layer is hacked, communications are compromised without the other layers being aware of the problem
- Security is only as strong as the weakest link
- When it comes to networking, layer 2 can be a very weak link



# Layer 2 attacks

MAC address flooding

DHCP server spoofing



"Man-in-the-middle" attacks using gratuitous ARP

IP host spoofing

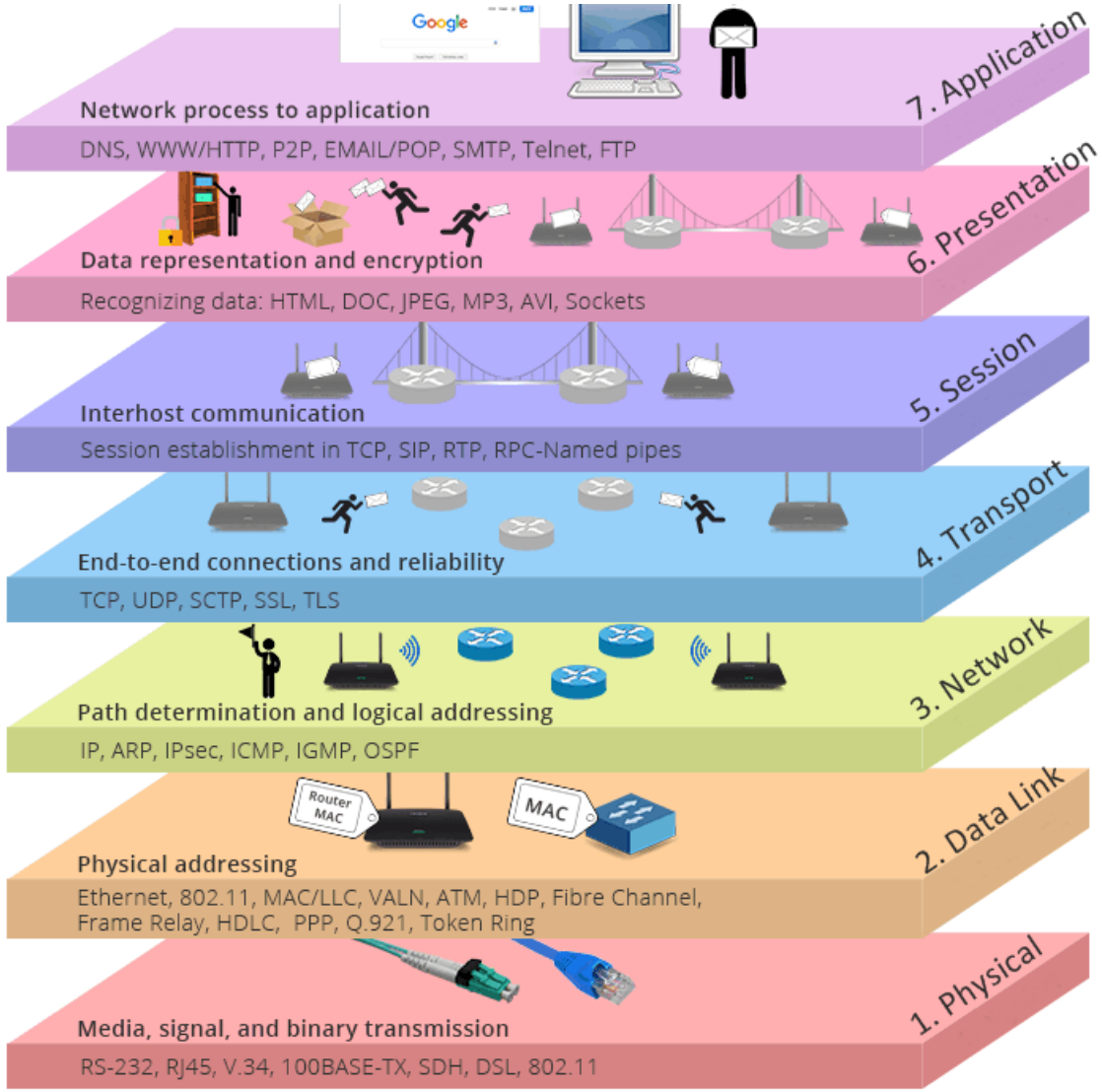
# Best Practices

- Manage the switches in a secure manner. For example, use SSH, authentication mechanism, access list, and set privilege levels.
- Restrict management access to the switch so that untrusted networks are not able to exploit management interfaces and protocols such as SNMP.
- Always use a dedicated VLAN ID for all trunk ports.
- Deploy the Port Security feature to prevent unauthorized access from switching ports.
- Use the Private VLAN feature where applicable to segregate network traffic at Layer 2.
- Use MD5 authentication where applicable.
- Prevent denial-of-service attacks and other exploitation by disabling unused services and protocols.
- Shut down or disable all unused ports on the switch, and put them in a VLAN that is not used for normal operations.
- Use port security mechanisms to provide protection against a MAC flooding attack.
- Use port-level security features such as DHCP Snooping, IP Source Guard, and ARP security where applicable.

# Layer 3 Security

# Network Layer (Layer 3)

- This deals with the routing of packets between networks, connecting different broadcasting domains.
- The addressing model used at this level is that of IP addresses, and the mechanism that centralizes traffic management is the router.
- Activating the various security characteristics included in this equipment is important for preventing unauthorized control of it.
- Use of strong passwords and correct configuration of management protocols through encrypted connections are some of the measures that can be taken to protect this

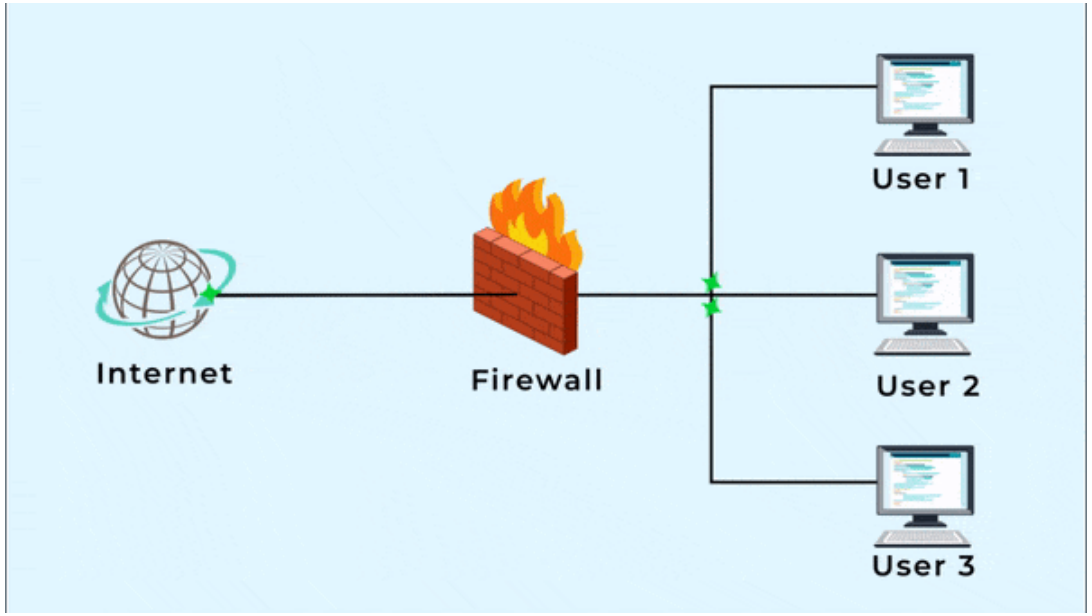


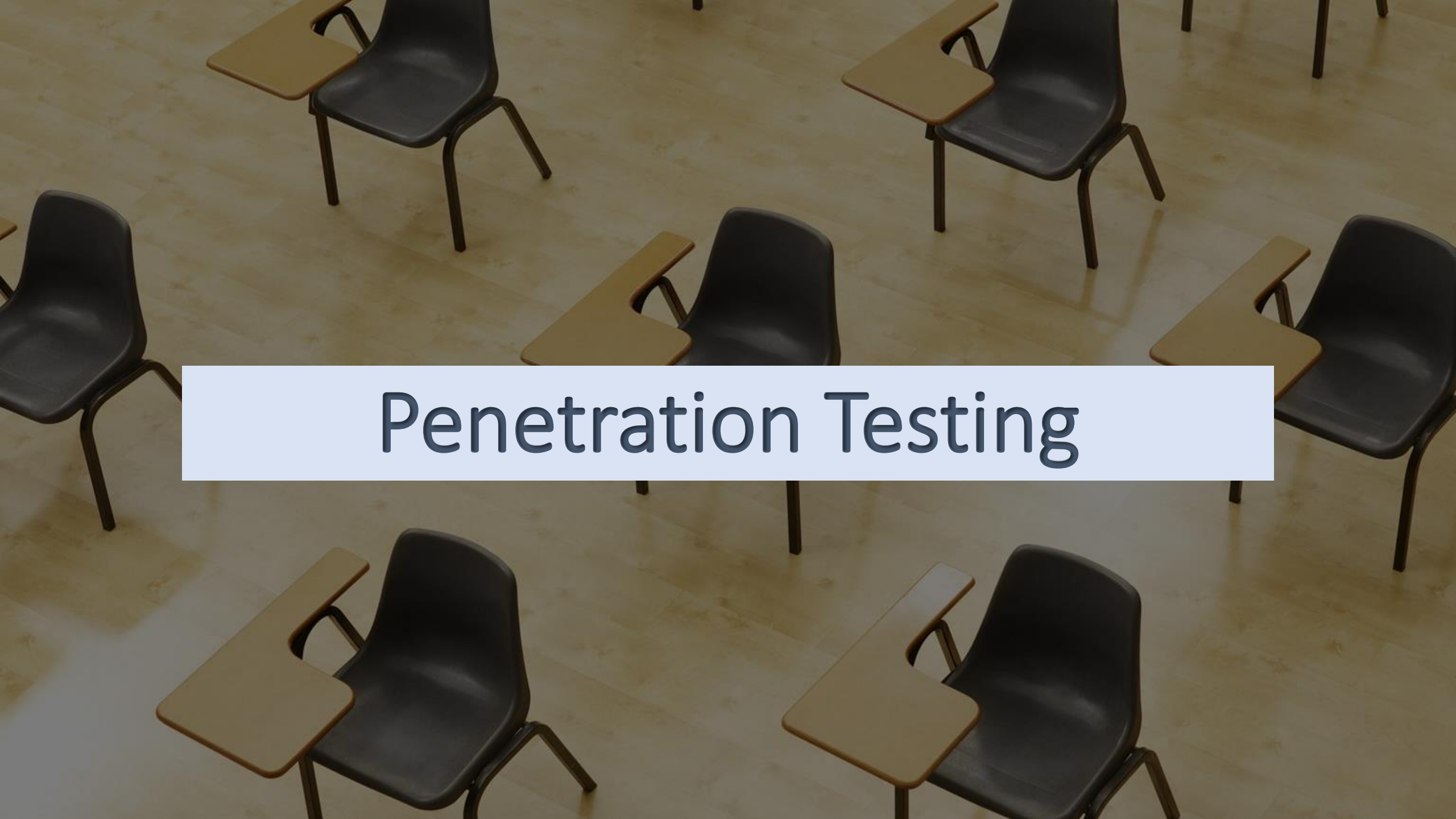
# IP spoofing

- The possibility of an attacker trying to send data from equipment with a certain IP address when in reality they are doing so from another address—a process called IP spoofing.
- One way to minimize such attacks is to include authentication processes in the application layer, together with data encryption mechanisms.

# Firewalls

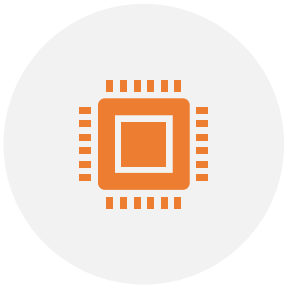
- Firewalls on the network layer can reduce such attacks
- A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.





# Penetration Testing

# Penetration Testing



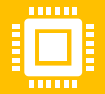
The testing that examines the security of an organisation prior to an attack on the network by a hacker is known as penetration testing.

Special tools are used to simulate real-world attack scenarios to identify security gaps that may lead to stealing of records, compromising with user credentials and various other details.

# Exploit Vulnerabilities

Penetration testing tools or a third party

Identify vulnerable systems or accounts



Scanning is done for every system on the network for open ports and services running on them

Use testing tools to avoid situations of vulnerability so that there is no unwelcome access over the network.

Not only target the systems but also the users available over the network with the help of phishing emails, pretext calling, or onsite social engineering.

# Test the User Risk to the IT Security Chain

The attack over the network because of human error or incorrect user credentials

The penetration tester tries the brute-force password guessing for identified user accounts in order to seek access to the systems and applications

Simulated phishing attacks as a common mechanism to test the security of network users

# Issues that can be manged by Penetration Testing

- Vulnerable security areas prior to a hacker attack
- Loopholes in information security compliance
- Response time taken by the IT team to detect a security breach and  minimise the impact of breach
- Possible adverse effects of the breaching of information or the cyber attack

# Thank you