**DAY-2**

🡪Protocols used to communicate the devices are TCP and UDP

🡪TCP is Transmission Control Protocol

🡪UDP is User Datagram Protocol

Transmission Control Protocol

1. Connection process between devices to transfer data

TCP flags:

🡪SYN: Synchronize

🡪ACK: Acknowledgement

🡪FIN: Finish

🡪RST: Reset

🡪URG: Urgent

🡪PSH: Push

SYN flag is used to request a connection

ACK flag is used to acknowledge received data or give feedback

FIN flag is used to end connection after data transfer

RST = abort a connection

URG = process data immediately

PSH = send data from buffer immediately

2. 3-way handshake connection (to enable connection)



Host B

Host A

**SYN**

**SYN+ACK**

**ACK**

----CONNECTION SUCCESS­----

4-way handshake

Host B

Host A

**FIN**

**ACK**

**FIN**

****

**ACK**

----CONNECTION ENDED----

TCP examples:

Text messages, files upload

UDP examples:

Video calls, games

**Introduction to Ethical Hacking and Cybersecurity**

Some terminologies:

1. Hack value

🡪The interest hacker has over the target

2. Vulnerability

🡪A weak point or a loophole in a software

3. Exploit

🡪Code to take advantage of vulnerability

4. Payload

🡪Actual message transferred between devices or the portion of malware

5. Zero-day vulnerability

🡪Vulnerability found by the external individual rather than the developer

6. Zero-day attack

🡪Attack performed using zero-day vulnerability before the first patch is given to the vulnerability

7. Doxing

🡪Gathering private and publicly available information of an individual or government and posting in internet

8. Attack

🡪 Attack = Goal + Methods + Vulnerability

9. Patch

🡪A fix or an update given to the vulnerability

Elements of Information Security / Cyber Security:

**Confidentiality**

**Integrity**

**Availability**

**Authenticity**

**Non-repudiation**

Restriction or feature which is used to make the sender and receiver to not deny the data sent or received (Ex. Email delivery report)

Information security threat challenges:

1. Network threats

🡪Information gathering

🡪Sniffing and eavesdropping (used yepme.com)

🡪Password based attacks

🡪Denial of service

2. Host threats

🡪Malware attacks

🡪Unauthorized access

🡪Backdoor attacks

🡪Physical security threats

3. Application threats

🡪Improper data/input validation

🡪Information disclosure

🡪Security misconfiguration

🡪Buffer overflow attack