Day 12 - PORTS AND PROTOCOLS

What is a Port?

- A communication endpoint on a device.
- Ports are numbered from **0 to 65535**.
- Used by applications and services to send and receive data.

Port Ranges:

Range	Description
0–1023	Well-known ports (HTTP, FTP, SSH, etc.)
1024–49151	Registered ports
49152–65535	Dynamic/private ports

Common Ports and Their Services:

Service	Port	Protocol
HTTP	80	TCP
HTTPS	443	TCP
FTP	21	TCP
SSH	22	TCP
DNS	53	UDP/TCP
SMTP	25	TCP

What is a Protocol?

- Set of rules that define communication between devices.
- Examples:

  - **TCP** (Transmission Control Protocol) — reliable communication.
  - **UDP** (User Datagram Protocol) — faster but less reliable.
  - **HTTP**, **HTTPS**, **FTP**, **SSH** — higher-level application protocols.

Practical Task: Checking Open Ports

Command to list active connections:

```
bash
CopyEdit
netstat -an
```

Command to check a specific port (e.g., port 80):

```
bash
CopyEdit
netstat -an | findstr :80
```

Key Takeaways:

- Ports and protocols are **critical for understanding cybersecurity attacks and defenses**.
- Services run on specific ports, which can be **protected or exploited**.
- Knowing open ports is the **first step toward securing a system**.