Week 2 – Networking & System Basics

Task 1. Networking Basics

Networking is the foundation of cybersecurity. It explains how devices communicate, share data, and access services over a network such as the internet or a local network.

TCP/IP

TCP/IP (Transmission Control Protocol / Internet Protocol) is the **core communication model of the internet**.

> **IP (Internet Protocol)** is responsible for **addressing and routing** data to the correct destination.
>
> **TCP (Transmission Control Protocol)** ensures **reliable communication** by breaking data into packets, sending them, and reassembling them correctly.
>
> TCP checks for errors and resends lost packets.
>
> Without TCP/IP, devices would not be able to communicate over networks.

DNS (Domain Name System)

DNS is like the **phonebook of the internet**.

> It converts **human-readable domain names** (e.g. google.com) into **IP addresses** (e.g. 142.250.185.46).
>
> Users remember names, but computers communicate using IP addresses.
>
> DNS plays a major role in cybersecurity because attackers can exploit it for phishing or redirection attacks.

IP Address

An **IP address** is a unique identifier assigned to a device on a network.

Types of IP addresses:

> **IPv4:** 192.168.1.1
>
> **IPv6:** 2001:0db8:85a3::8a2e:0370:7334

Public vs Private IPs:

> Public IP: Accessible over the internet
>
> Private IP: Used within internal networks

Why it matters in cybersecurity: IP addresses are used for logging, access control, and detecting malicious activity.

Ports

Ports are **communication endpoints** that allow multiple services to run on a single device.

Each port is associated with a specific service.

Common examples:

Port 80 – HTTP

Port 443 – HTTPS

Port 22 – SSH

Port 21 – FTP

In cybersecurity, open ports can be **entry points for attacks** if not properly secured.

Firewalls

A firewall is a **security control** that monitors and filters network traffic.

It allows or blocks traffic based on predefined rules.

Firewalls can be:

Network-based (protect entire networks)

Host-based (protect individual systems)

Firewalls help prevent unauthorized access and reduce attack surfaces.

Routing

Routing is the process of **directing network traffic** from one network to another.

Routers determine A **best path** for data to travel.

Routing ensures data reaches its destination efficiently.

Poor routing configuration can lead to security risks such as traffic interception or data leakage.