Session 7 Network Ports & Services (WellKnown Ports)

1.What is a Port?

A port is like a “door” through which data enters and exits a computer over a network.
It helps identify which service/application should handle the traffic.
Ports range from 0 – 65535.

Classification:

1. WellKnown Ports (0 – 1023) : Standard services (HTTP, HTTPS, FTP, DNS, etc.) assigned by IANA.
2. Registered Ports (1024 – 49151) : Used by software vendors for applications.
3. Dynamic Ports (49152 – 65535) : Temporary ports chosen by OS for client connections.

2. Important WellKnown Ports & Services

Port	Protocol/Service	Description
20/21	FTP	File Transfer Protocol (20 = Data, 21 = Control)
22	SSH	Secure remote login, encrypted communication
23	Telnet	Remote login, unencrypted
25	SMTP	Sending emails
53	DNS	Domain Name System (domain ↔ IP resolution)
67/68	DHCP	Automatic IP assignment (67 = server, 68 = client)
69	TFTP	Trivial FTP, no authentication
80	HTTP	Web traffic (unencrypted)
110	POP3	Retrieving emails
123	NTP	Time synchronization
143	IMAP	Advanced email retrieval
161/162	SNMP	Network device monitoring
389	LDAP	Directory services (authentication, AD)
443	HTTPS	Secure web traffic (SSL/TLS)
445	SMB	Windows file sharing
514	Syslog	System logging
3306	MySQL	Database service
3389	RDP	Remote Desktop Protocol

3. Why Are Ports Important in Cybersecurity?

Attack Surface: Open ports can be exploited if unnecessary services are running.
Reconnaissance: Hackers scan ports (e.g., with Nmap) to discover services.
Defense: Security teams close unused ports and apply firewall rules.

Examples:

Port 22 (SSH) → brute force login attacks.
Port 445 (SMB) → exploited by WannaCry ransomware.
Port 3306 (MySQL) → weak DB credentials = data theft.