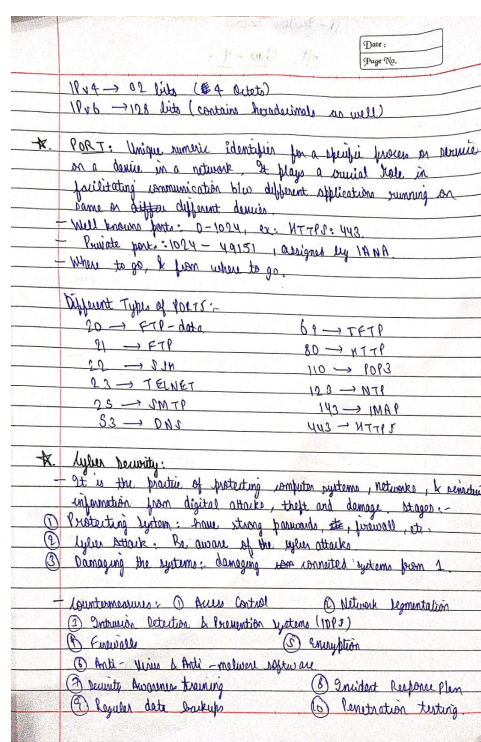
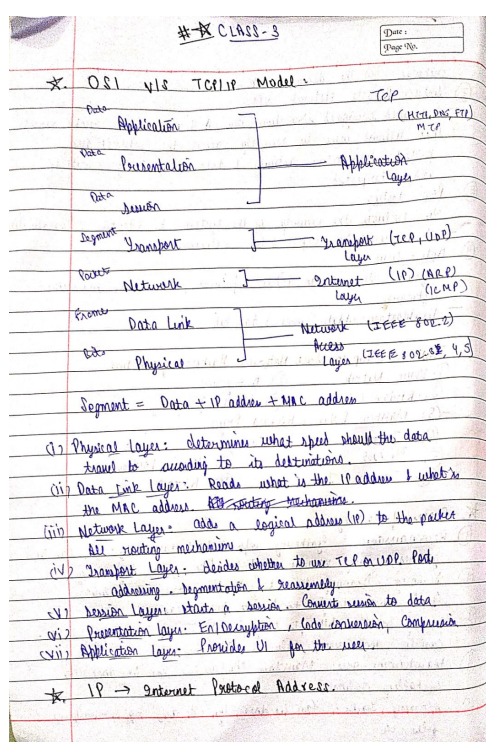


Class 3 - 24/08/2023

In this class, we studied about the OSI and TCP model, then we saw what IP addresses are: IPv4 and IPv6, then we learnt about what ports are and what types of ports there are along with their vulnerabilities and then at the end we learnt about the fundamentals of cyber security.

Instead of writing short lines about the topics, i am attaching my short notes here:



Task - Port and Vulnerabilities

Port number	Protocol	Vulnerabilities	Protocol used
-------------	----------	-----------------	---------------

Port number	Protocol	Vulnerabilities	Protocol used
20	FTP data	Data exfiltration, denial-of-service (DoS) attacks, and remote code execution (RCE) attacks	TCP
21	FTP control	Data exfiltration, denial-of-service (DoS) attacks, and remote code execution (RCE) attacks	TCP
22	SSH	Brute-force attacks, man-in-the-middle attacks, and other attacks	TCP
23	Telnet	Password guessing, session hijacking, and data exfiltration	TCP
25	SMTP	Spam attacks, phishing attacks, and other attacks	TCP
53	DNS	DNS poisoning attacks, which can redirect users to malicious websites	TCP & UDP
69	TFTP	File exfiltration attacks and DoS attacks	UDP
80	HTTP	Cross-site scripting (XSS) attacks, SQL injection attacks, and other attacks	TCP & UDP
110	POP3	Password guessing attacks and session hijacking attacks	TCP

Port number	Protocol	Vulnerabilities	Protocol used
123	NTP	NTP spoofing attacks, which can be used to inject false time stamps into network traffic	TCP
143	IMAP	Password guessing attacks and session hijacking attacks	TCP
443	HTTPS	Man-in-the-middle attacks, if the encryption is not properly configured	TCP