Insecure Port	Description	Secure Port	Description
21 (FTP)	File Transfer Protocol (FTP) sends username and password in plaintext.	**22 (SFTP)**	Uses encryption to protect user credentials and transferred data.
23 (Telnet)	Sends all information in plaintext, making it vulnerable to interception.	**22 (SSH)**	Encrypts the data for secure communication between the host and terminal.
25 (SMTP)	Used for sending emails; data is unencrypted and susceptible to sniffing.	**587 (SMTP)**	Adds TLS encryption to secure the data between the email client and server.
37 (TIME)	Used by legacy systems for time synchronization; insecure.	**123 (NTP)**	Network Time Protocol (NTP) on port 123 provides secure and efficient time synchronization.
53 (DNS)	Widely used for domain name resolution but lacks encryption.	**853 (DoT)**	DNS over TLS (DoT) encrypts DNS traffic, preventing tampering in transit.
80 (HTTP)	Sends information in plaintext, making it susceptible to sniffing.	**443 (HTTPS)**	Uses TLS encryption to secure data between the server and browser.
143 (IMAP)	Retrieves emails without encryption, making it vulnerable to sniffing.	**993 (IMAP)**	Adds SSL/TLS encryption for secure email retrieval.
445 (SMB)	Used for accessing network files without encryption.	**2049 (NFS)**	Network File System (NFS) can be used securely but is recommended to be allowed only through firewalls.
389 (LDAP)	Transfers directory information without encryption, leaving it vulnerable to sniffing and attacks.	**636 (LDAPS)**	Adds SSL/TLS encryption to secure directory information during transit.