Common Ports and Protocols

What is a Port?

A **port** is like a doorway for data. You can open or close these doorways, and you can set them up to allow specific types of data to go through.

What is a Protocol?

A **protocol** is a set of rules that govern how data is communicated between devices. It ensures that devices understand each other when sending or receiving data.

Secure vs Insecure Ports and Protocols

- **Ports**: Think of open ports as doorways without locks, and secure ports as doorways that are locked for protection.
- **Protocols**: A regular protocol is like a simple language you can easily understand, while a secure protocol is like a language that is encrypted and requires a key to understand.

Some of the Most Common Protocols

- **IP (Internet Protocol)**: This protocol is used to get the address of where to send data. It's like the "address system" of the internet, helping data find its way to the right destination.
- **TCP (Transmission Control Protocol)**: This protocol ensures that data sent between devices arrives correctly and in the right order. It's reliable and guarantees the delivery of data.
- **UDP (User Datagram Protocol)**: This protocol sends data quickly without checking if it arrives correctly. It's often used for real-time applications like video streaming, where speed matters more than perfect delivery.

Generally Non-Secure vs Generally Secure Ports and Protocols

Some ports and protocols are not secure unless they add encryption.

Non-Secure Port/Protocol	Secure Port/Protocol
21 - **FTP (File Transfer Protocol)**: Used for transferring files over a network, but without encryption.	22* - **SFTP (Secure File Transfer Protocol)**: A secure version of FTP that uses SSH to encrypt the file transfer.
23 - **Telnet (Protocol)**: Allows remote login to another computer, but without encryption, making it insecure.	22* - **SSH (Secure Shell)**: A secure method of accessing and managing devices remotely, with encrypted communication.
25 - **SMTP (Simple Mail Transfer Protocol)**: Used for sending emails to a mail server, usually unencrypted.	587 - **SMTP (Used by email clients like Gmail or Outlook)**: Encrypts communication between email clients and servers to ensure security when sending emails.

Non-Secure Port/Protocol	Secure Port/Protocol
143 - **IMAP (Internet Mail Access Protocol)**: Used to retrieve emails from a server, typically without encryption.	993 - **IMAP (Encrypted)**: IMAP with added encryption (via SSL or TLS) to protect your email data while it's being retrieved.
37 - **Time (Time Protocol)**: A protocol used to synchronize the time on computers, but it does not include any security features.	123 - **NTP (Network Time Protocol)**: A protocol that synchronizes time across devices on a network, typically with more security than the Time Protocol.
53 - **DNS (Domain Name System)**: Helps translate human-readable website names (like google.com) into machine-readable IP addresses.	853 - **DoT (DNS over TLS)**: Encrypts DNS queries, adding a layer of security to prevent eavesdropping on domain lookups.
80 - **HTTP (HyperText Transfer Protocol)**: Used for transmitting web pages but without encryption, meaning data can be intercepted.	443 - **HTTPS (Secure HTTP)**: A secure version of HTTP that encrypts the data exchanged between your browser and the website, protecting your privacy.
161/162 - **SNMP (Simple Network Management Protocol)**: Used for managing devices like routers and switches on a network, typically without encryption.	161/162 - **SNMP v3**: A secure version of SNMP that adds authentication and encryption for better security when managing network devices.
389 - **LDAP (Lightweight Directory Access Protocol)**: Used for accessing and maintaining directory services, like user info, but without encryption.	636 - **LDAPS (Secure LDAP)**: A secure version of LDAP that uses encryption (SSL/TLS) to protect directory service data.

FTPS and SFTP (Extended)

Some protocols that handle communication can also use protocols for security:

- **FTPS (File Transfer Protocol Secure)**: This version of FTP adds SSL (Secure Sockets Layer) encryption to ensure that the file transfer is secure and private.
- **SFTP (Secure File Transfer Protocol)**: A more secure version of FTP that uses SSH (Secure Shell) for encryption and secure file transfer. It’s considered more secure than FTPS.

What is a Shell?

A **Shell** is a program that lets you control a computer using text commands instead of a graphical interface (like what you see in Windows or macOS). It's often used by system administrators and developers for managing systems.

SSH (Secure Shell)

SSH is a cryptographic protocol that allows secure access to a device over an unsecured network. It’s used to manage remote servers securely by encrypting data during the communication. SSH is widely used for remote command-line access and file transfers.

When hackers try to access a server, one way they might do it is by stealing SSH login details. That’s why it’s very important to keep SSH credentials safe and only let trusted admins use them.

Web Shell

A **Web Shell** is a malicious script that hackers use to remotely control a web server. They can upload the shell to a server they’ve compromised, allowing them to execute commands and take control of the server without needing physical access.