Common Ports and Protocols

What is a Port?

A **port** is like a doorway. You can open and close ports, and you can designate certain ports to be open for only certain things to go through them.

What is a Protocol?

A **protocol** is a set of rules for communication. It has an established set of rules that must be followed for network communication to work. Each protocol has its own purpose.

Secure vs Insecure Ports and Protocols

- **Ports**: Gateways without locks vs gateways with locks.
- **Protocols**: Languages you can easily understand vs languages that are encrypted and need a key to crack.

Some of the Most Common Protocols

- **IP (Internet Protocol)**: About getting the address to which to send data.
- **TCP (Transmission Control Protocol)**: Enables application programs and computing devices to exchange messages.
- **UDP (User Datagram Protocol)**: Enables communication for low latency and loss tolerance. Think broadcast. No acknowledgment needed for transmission. Low overhead. Used for streaming.

Generally Non-Secure vs Generally Secure Ports and Protocols

Some of these can be either secure or non-secure, depending on whether encryption has been added.

Non-Secure Port/Protocol	Secure Port/Protocol
21 - FTP (File Transfer Protocol)	22* - SFTP (Secure File Transfer Protocol)
23 - Telnet (Protocol used to login into another computer on the same network)	22* - SSH (Secure version of Telnet)
25 - SMTP (Simple Mail Transfer Protocol: Focuses on sending email to the email server. Typically, only used between email servers for relaying messages)	587 - SMTP (Used by an email client like Gmail or Outlook to submit messages to the server)
143 - IMAP (Internet Mail Access Protocol: Associated with retrieving or accessing email)	993 - IMAP (encrypted with TLS and SSL encryption)
37 - Time (Time Protocol)	123 - NTP (Network Time Protocol)

Non-Secure Port/Protocol	Secure Port/Protocol
53 - DNS (Domain Name System: Helps internet users discover websites and internet-based devices using human-readable names like google.com)	853 - DoT (DNS over TLS)
80 - HTTP	443 - HTTPS (Associated with how you're able to see multi types of files on the internet)
161/162 - SNMP (Simple Network Management Protocol: Manages how devices on the same network share information with each other. It helps identify devices on the network and monitors and networks performance. Keeps track of changes on the network)	161/162 - SNMP v3
389 - LDAP (Lightweight Directory Access Protocol: Use a directory to find a person's name and contact information)	636 - LDAPS (Lightweight Directory Access Protocol Secure)

FTPS and SFTP (Extended)

A protocol that handles communication may be used along with a protocol that handles security.

- **FTPS**: File transfer is done with SSL (Secure Sockets Layer) encryption added to it.
- **SFTP**: File transfer is done with SSH (Secure Shell), which provides a secure channel for the file transfer to take place.

What is a Shell?

A **Shell** is a computer program that allows you to control a computer from a command-line interface (CLI). This is where you don't have a graphical user interface, but just a command prompt, where you type in the commands to control what's happening on the computer.

SSH (Secure Shell)

A **Secure Shell** is a cryptographic network protocol for operating network services securely over an unsecured network. Its most notable applications are remote login and command-line execution.

When a hacker wants to get access to a server on a network and control it, a major accomplishment would be for the hacker to obtain SSH credentials for that server. So, it's extremely important to protect those credentials, which should only be accessible to authorized administrators.

Web Shell

A **Web Shell** is a script that a hacker will use to access and control a web server remotely.