Common Ports and Protocols 01

SSH (22)

- Secure Shell (SSH) is a cryptographic protocol that is used to remotely administer Linux servers and network equipment through a text console.
- The SSH protocol uses public-key cryptology to authenticate and encrypt network access from the remote computer.
- The SSH protocol listens for incoming requests on TCP port 22.

DNS (53)

- Domain Name System (DNS) is a distributed directory of domain resource records.
- Primarily used in translating fully qualified domain names (FQDNs) to IP addresses.
- DNS can also be used for other lookups, such as IP addresses to FQDNs (called reverse DNS lookups)
- "DNS resolvers operate on UDP port 53 for simple lookups. DNS servers also use TCP port 53 (called the zone transfer) for data replication.

SMTP (25)

- Simple Mail Transport Protocol (SMTP) is a protocol used by mail transfer agents (MTAs) to deliver emails to a destination email server.
- The protocol is used only in the process of delivering the email to the email server.
- SMTP operates on TCP port 25.
- SMTP TLS (587)
  - The Simple Mail Transport Protocol (SMTP) can operate over Transport Layer Security (TLS).
  - Uses TCP port 587.

FTP (20, 21)

- File Transfer Protocol (FTP) is a legacy file sharing protocol that is still commonly used on the Internet.
- FTP is slowly being replaced with SFTP because SFTP offers encryption and doesn' t have the firewall issues FTP has.
- Control channel operates on port 21 while the data channel operates on port 20.
- SFTP (22)
  - Secure File Transfer Protocol (SFTP) is a file transfer protocol that uses the SSH inner workings.
  - Since SFTP is used with the SSH protocol, the server awaits an incoming connection on TCP port 22.
- TFTP (69)
  - Trivial File Transfer Protocol (TFTP) is a handy protocol because it provides no security and is simplistic in its operation.
  - TFTP is used to boot computers over the network with the Preboot Execution Environment (PXE). It is also used to transfer software images for network devices such as routers and switches during software upgrades.
  - Network devices also use TFTP to back up and restore configurations.
  - The TFTP server listens for requests on UDP port 69.

Telnet (23)

- Telnet is another legacy protocol slowly being replaced by the SSH protocol.
- The Telnet protocol allows remote administration of network devices through a text-based console.
- No encryption which is why it's being replaced by SSH.
- A Telnet server or device will await connection on TCP port 23.

DHCP (67)

- Dynamic Host Configuration Protocol (DHCP) is a protocol that provides automatic configuration of IP addresses, subnet masks, and options such as Domain Name System (DNS) servers and the remote gateway to network devices.
- DHCP operates in a connectionless state because during the process the client does not yet have an established IP address.
- During the configuration process, the DHCP server waits for a request from clients on UDP port 67.
- Clients will send the initial request from UDP port 68. When the server responds it responds to UDP port 68 from UDP port 67.

HTTP (80)

- Hypertext Transfer Protocol (HTTP) is an application protocol for web data communications.
- The server listens for incoming requests on TCP port 80.
- HTTPS [Transport Layer Security (TLS)]
  - Basically HTTP over secure channel (SSL)
  - SSL is a cryptographic suite of protocols that uses Public Key Infrastructure (PKI).
  - The web server listens for requests on TCP port 443.
  - A private key must be imported into the web server from a mutually trusted source to allow SSL to properly work.

RDP (3389)

- Remote Desktop Protocol (RDP) is a Microsoft protocol used for connecting to another Microsoft computer or server for remote administration
- The RDP client built into the Microsoft operating system is mstsc.exe (the Microsoft Terminal Services Client).
- The operating system listens for requests on TCP port 3389.

POP (110)

- The Post Office Protocol (POP), also known as POP3, is a legacy protocol, but it' s still used on the Internet today.
- POP is slowly being replaced with IMAP.
- POP allows email clients, also called mail user agents (MUAs), to log in and retrieve email.
- POP listens for requests to the server on TCP port 110.
- POP3 over SSL (995)
  - Although POP3 is a legacy protocol, it is still used for legacy applications and transmits information in clear text. Therefore, POP3 over SSL can be employed to encrypt any data in transit

IMAP (143)

- Internet Message Access Protocol (IMAP) is used to allow email clients to retrieve and read email on the email server.
- IMAP allows for multiple email clients to access the same email box simultaneously.
- IMAP also uses flags on the messages so that email clients can keep track of which emails are read and unread.
- IMAP listens for incoming connections on the email server from email clients on TCP port 143.
- IMAP over SSL (993)
  - IMAP can also operate over SSL.
  - When encryption is used, all data transmitted is encrypted on TCP port 993.