Common Ports and Protocols 02

SQLnet (1521)

- SQLnet is a proprietary networking software developed by Oracle.
- It enables communication between Oracle databases, so information can be exchanged for queries.
- The SQLnet protocol operates on TCP port 1521.

MySQL (3306)

- MySQL is an open-source relational database system, similar to Microsoft SQL Server.
- TCP port 3306, is associated with MySQL.

SQL (1433)

- Structured Query Language (SQL) is a generic term for the language a SQL server talks, and it does not specify a particular implementation.
- However, the term SQL server is synonymous with Microsoft SQL Server. The key take-away is that when you see TCP port 1433, you associate it with Microsoft SQL Server traffic.

Syslog (514)

- A syslog server sits and waits for a syslog message: it sounds simple and it really is.
- Syslog awaits messages on UDP port 514.

H.323 (1720)

- The H.323 protocol is similar to the SIP protocol but different in the respect that it encompasses all of the communications technologies used by VoIP and videoconferencing.
- The H.323 protocol performs call setup on TCP port 1720.
- 4 Main functionalities
  - Terminal control, which provides endpoint signaling such as the VoIP phone itself
  - Gateway services that provide transcoding functionality as well as communications with circuit-switched and packet-switched networks
  - Gatekeeper services that provide admission control (authentication and authorization), bandwidth control, and management of endpoints (also known as zone management)
  - The multipoint control unit (MCU), which provides conference call capabilities and call control of data, voice, and video for future in-call conferencing.

LDAP (389)

- Lightweight Directory Access Protocol (LDAP) is an application protocol that can search a directory service for objects.
- An LDAP client communicates to LDAP servers on TCP port 389; it can also use UDP port 389.
- LDAPS (636)
  - Lightweight Directory Access Protocol over SSL (LDAPS) is the application protocol of LDAP when SSL is configured.
  - LDAPS operates on TCP port 636 and can also use UDP port 636.

SNMP (161/162)

- Simple Network Management Protocol (SNMP) is a protocol used for the management of servers and network devices.
- SNMP can be used to collect data from servers and network devices such as memory, CPU, and bandwidth.
  - When used in this way, the data is read from a centralized network management station (NMS).
  - The NMS is then responsible for arranging the data into an acceptable display such as a graph; this allows an administrator to create a baseline of performance.
- SNMP can also be used in a trap configuration.
  - If a certain variable such as CPU usage crosses a threshold the administrator has set, the SNMP agent can send a trap message to the NMS.
  - Traps are sent to UDP port 162.
- SNMP can also be used in a writable mode.
  - This is often done with network equipment because SNMP requests can be sent to reconfigure the equipment.
  - SNMP agents and servers listen for requests on UDP port 161.

NTP (123)

- Network Time Protocol (NTP) is a network protocol that is optimized for synchronizing clocks between computers over the Internet.
- NTP listens for requests on UDP port 123. The requesting host will send requests from UDP port 123 as well.

SIP (5060, 5061)

- Session Initiation Protocol (SIP) is a communication protocol for the setup and signaling of Voice over IP (VoIP) calls.
- SIP does not transport the media stream—it only assists in setting up the media stream for the communication session.
- The SIP protocol operates on UDP port 5060, although it can operate on TCP as well.
- SIP can also use encryption via Transport Layer Security (TLS) on UDP port 5061 and can be changed to TCP if needed.

SMB (445)

- The Server Message Block (SMB) protocol is a common network file and printer sharing protocol that is used with Microsoft products.
- Linux also has an SMB filer called Samba that is compatible with the SMB file protocol for file and printer sharing.
- The SMB protocol is enabled on every server and client in a Microsoft network.
- The SMB protocol waits for a connection on TCP port 445.