PORTS AND PROTOCOLS

SOC L1 INVESTIGATION

PREPARED BY
SHUBHAM SONI

1. What Are Ports?

A **port** is a **logical endpoint** in networking that helps identify different services running on a device. Each port is assigned a **number** ranging from **0 to 65535** and is used with an IP address to form a unique connection.

- **Well-Known Ports (0-1023):** Reserved for common services (e.g., HTTP, HTTPS, FTP).
- **Registered Ports (1024-49151):** Used by software vendors (e.g., database services).
- **Dynamic/Ephemeral Ports (49152-65535):** Used for temporary connections.

2. What Are Protocols?

A **protocol** is a set of rules that governs how data is transmitted between devices in a network. They define how data is structured, sent, received, and acknowledged.

Protocols operate at different layers of the **OSI Model** and **TCP/IP Model**.

3. Important Ports and Protocols for SOC L1

(1) HTTP (HyperText Transfer Protocol)

- **Port:** 80
- **Protocol Type:** TCP
- **Purpose:** Used for web browsing (unencrypted).
- **SOC L1 Investigation:**
    - Check for unauthorized access to websites.
    - Look for **HTTP-based attacks** (e.g., **XSS, SQL Injection**).
    - Analyze **GET and POST requests** in logs.
    - Use **Wireshark** or **Splunk** to inspect traffic.

(2) HTTPS (HyperText Transfer Protocol Secure)

- **Port:** 443
- **Protocol Type:** TCP
- **Purpose:** Secure web browsing with encryption (TLS/SSL).
- **SOC L1 Investigation:**
    - Look for **SSL/TLS handshake failures** in logs.
    - Monitor **HTTPS-based phishing or MITM attacks**.
    - Use **SSL/TLS logs** for decryption in SOC tools.

(3) FTP (File Transfer Protocol)

- **Ports:** 20 (Data), 21 (Control)
- **Protocol Type:** TCP

- **Purpose:** Transfers files over the network.
- **SOC L1 Investigation:**
    - Check logs for **unauthorized file transfers**.
    - Monitor for **brute-force login attempts**.
    - Look for **anonymous FTP access vulnerabilities**.

(4) SFTP (Secure File Transfer Protocol)

- **Port:** 22
- **Protocol Type:** TCP (uses SSH)
- **Purpose:** Secure file transfer.
- **SOC L1 Investigation:**
    - Monitor **unauthorized file uploads/downloads**.
    - Analyze SSH authentication logs.
    - Detect **excessive login attempts (brute-force attacks).**

(5) SSH (Secure Shell)

- **Port:** 22
- **Protocol Type:** TCP
- **Purpose:** Secure remote access to servers.
- **SOC L1 Investigation:**
    - Look for **multiple failed SSH login attempts**.
    - Monitor for **suspicious remote connections**.
    - Check **session hijacking** attempts in logs.

(6) Telnet

- **Port:** 23
- **Protocol Type:** TCP
- **Purpose:** Unencrypted remote login.
- **SOC L1 Investigation:**
    - Identify **unauthorized remote access**.
    - Look for **credentials sent in plaintext** (dangerous!).
    - Disable Telnet and recommend using SSH.

(7) DNS (Domain Name System)

- **Port:** 53
- **Protocol Type:** TCP/UDP
- **Purpose:** Resolves domain names to IP addresses.
- **SOC L1 Investigation:**
    - Monitor for **DNS spoofing and poisoning attacks**.
    - Check for **unusual DNS queries to malicious domains**.
    - Look for **excessive DNS requests** (DDoS attack signs).

(8) SMTP (Simple Mail Transfer Protocol)

- **Port:** 25 (unencrypted), 587 (secure), 465 (SSL)
- **Protocol Type:** TCP
- **Purpose:** Sending emails.
- **SOC L1 Investigation:**
    - Check email headers for **phishing attacks**.
    - Look for **mass email sending behavior** (spam or malware).
    - Monitor for **unauthorized SMTP relay abuse**.

(9) POP3 (Post Office Protocol)

- **Port:** 110 (unencrypted), 995 (SSL)
- **Protocol Type:** TCP
- **Purpose:** Receiving emails (downloads emails locally).
- **SOC L1 Investigation:**
    - Monitor for **unauthorized email access**.
    - Check logs for **failed authentication attempts**.
    - Analyze phishing emails and attachments.

(10) IMAP (Internet Message Access Protocol)

- **Port:** 143 (unencrypted), 993 (SSL)
- **Protocol Type:** TCP
- **Purpose:** Email retrieval without downloading.
- **SOC L1 Investigation:**
    - Look for **suspicious logins from different locations**.
    - Detect **email account hijacking attempts**.
    - Monitor for **email forwarding rule abuse**.

(11) RDP (Remote Desktop Protocol)

- **Port:** 3389
- **Protocol Type:** TCP/UDP
- **Purpose:** Remote desktop access.
- **SOC L1 Investigation:**
    - Look for **unauthorized remote login attempts**.
    - Detect **brute-force attacks on RDP**.
    - Monitor for **RDP session hijacking or lateral movement**.

(12) SNMP (Simple Network Management Protocol)

- **Port:** 161 (Queries), 162 (Traps)
- **Protocol Type:** UDP
- **Purpose:** Monitors network devices.
- **SOC L1 Investigation:**

- Check for **SNMP brute-force attacks**.
- Look for **unauthorized network scanning**.
- Monitor SNMP logs for suspicious activity.

(13) NTP (Network Time Protocol)

- **Port:** 123
- **Protocol Type:** UDP
- **Purpose:** Synchronizes time across devices.
- **SOC L1 Investigation:**
  - Look for **NTP reflection/amplification attacks (DDoS).**
  - Monitor for **incorrect timestamps** in logs.
  - Ensure **secure NTP server configurations**.

(14) LDAP (Lightweight Directory Access Protocol)

- **Port:** 389 (unencrypted), 636 (SSL)
- **Protocol Type:** TCP/UDP
- **Purpose:** Directory services authentication (Active Directory).
- **SOC L1 Investigation:**
  - Monitor for **unauthorized AD access attempts**.
  - Look for **LDAP brute-force login attempts**.
  - Detect **LDAP injection attacks**.

(15) MySQL

- **Port:** 3306
- **Protocol Type:** TCP
- **Purpose:** Database management system.
- **SOC L1 Investigation:**
  - Monitor for **SQL injection attempts**.
  - Check for **unauthorized database access**.
  - Look for **large database queries (data exfiltration).**

(16) SMB (Server Message Block)

- **Port:** 445
- **Protocol Type:** TCP
- **Purpose:** File sharing between systems.
- **SOC L1 Investigation:**
  - Detect **ransomware attacks using SMB (e.g., WannaCry).**
  - Monitor for **suspicious file transfers.**
  - Look for **SMB brute-force attacks.**