

DAY 5/30

(Part of my 30-Day SOC Analyst Learning Challenge)

20 ESSENTIAL PROTOCOLS FOR SOC ANALYSTS

BY HARSH KADU

Understanding network protocols is essential for identifying suspicious behavior, investigating alerts, and building better detections.

Here's a breakdown of the **20 most common protocols** a SOC analyst should be familiar with.

1. HTTP (Port 80)

What is it?

Used for unencrypted communication between web clients and servers.

What attackers can do:

- Deliver malicious payloads via websites
- Redirect victims to phishing pages

SOC Analyst Focus:

- Unusual URLs
 - Suspicious user-agents
 - Large POST requests from unknown IPs
-

2. HTTPS (Port 443)

What is it?

Encrypted version of HTTP using TLS/SSL.

What attackers can do:

- Hide malicious traffic (malware C2, exfiltration)
- Phishing with HTTPS to appear legitimate

SOC Analyst Focus:

- Certificate anomalies
 - Unknown domains with short lifespans
 - Traffic to known bad IPs/domains
-

3. DNS (Port 53)

What is it?

Resolves domain names to IP addresses.

What attackers can do:

- Use DNS tunneling for data exfiltration
- Connect to C2 servers using DGA domains

SOC Analyst Focus:

- Excessive DNS requests
 - Queries for uncommon domains
 - Suspicious TXT-type DNS records
-

4. FTP (Port 21)

What is it?

Used to transfer files over the internet.

What attackers can do:

- Upload/download malware
- Exfiltrate data

SOC Analyst Focus:

- Anonymous or failed login attempts
 - Large outbound transfers
 - Use of non-standard FTP tools
-

5. SMB (Port 445)

What is it?

Allows file sharing on Windows systems.

What attackers can do:

- Lateral movement
- Exploit EternalBlue (WannaCry)

- Spread malware over internal networks

SOC Analyst Focus:

- Unauthorized file access
 - Connections to high-risk shares
 - Internal SMB scanning
-

6. RDP (Port 3389)**What is it?**

Used for remote desktop access.

What attackers can do:

- Brute-force credentials
- Access internal systems remotely

SOC Analyst Focus:

- RDP from external IPs
 - Unusual login times
 - Geographically distant logins
-

7. SSH (Port 22)**What is it?**

Secure remote login for administration.

What attackers can do:

- Brute-force SSH logins
- Tunnels for C2 or data exfiltration

SOC Analyst Focus:

- Brute-force attempts
 - Logins from new/untrusted IPs
 - Long-lived SSH sessions
-

8. Telnet (Port 23)

What is it?

Unencrypted remote login protocol.

What attackers can do:

- Intercept credentials
- Gain access to legacy devices

SOC Analyst Focus:

- Use of Telnet (should be deprecated)
 - Cleartext credentials
-

9. ICMP

What is it?

Used for diagnostics (ping, traceroute).

What attackers can do:

- Reconnaissance
- ICMP tunneling
- DDoS (ICMP flood)

SOC Analyst Focus:

- Unusual ICMP volume
 - ICMP echo requests to internal hosts
-

10. LDAP (Port 389 / LDAPS 636)

What is it?

Used for directory services like Active Directory.

What attackers can do:

- User enumeration
- Query user/groups info

SOC Analyst Focus:

- Excessive LDAP queries
 - Anonymous binds
 - Privileged account enumeration
-

11. NetBIOS (Ports 137-139)**What is it?**

Legacy protocol for file/printer sharing.

What attackers can do:

- Enumerate shares and users
- Exploit legacy Windows vulnerabilities

SOC Analyst Focus:

- High NetBIOS traffic
 - Traffic from unexpected devices
-

12. SNMP (Port 161/162)**What is it?**

Used to monitor and manage network devices.

What attackers can do:

- Access sensitive config info
- Exploit default credentials

SOC Analyst Focus:

- SNMP v1/v2 (insecure) in use
 - Unknown devices sending SNMP traps
-

13. NTP (Port 123)

What is it?

Used for clock synchronization.

What attackers can do:

- Amplification DDoS attacks
- Timestamp manipulation

SOC Analyst Focus:

- NTP traffic from/to unusual IPs
 - NTP reflection/amplification signs
-

14. TFTP (Port 69)

What is it?

Lightweight, unauthenticated file transfer protocol.

What attackers can do:

- Transfer malicious firmware/configs
- Upload/download scripts

SOC Analyst Focus:

- TFTP traffic should be rare
 - Log all file names transferred
-

15. Kerberos (Port 88)

What is it?

Authentication protocol used in Active Directory.

What attackers can do:

- Kerberoasting
- Ticket manipulation

SOC Analyst Focus:

- Ticket requests for high-privilege users
 - Repeated TGT/Service ticket anomalies
-

16. IMAP (Port 143/993)**What is it?**

Used to retrieve emails.

What attackers can do:

- Steal email data
- Brute-force credentials

SOC Analyst Focus:

- Unusual IPs accessing mailboxes
 - Multiple login failures
-

17. SMTP (Port 25/587)**What is it?**

Used to send emails.

What attackers can do:

- Spam/phishing campaigns
- Exfiltration via email

SOC Analyst Focus:

- Mass outbound emails
 - Spoofed "From" addresses
-

18. POP3 (Port 110/995)

What is it?

Another protocol to retrieve emails.

What attackers can do:

- Read stored email
- Account hijacking

SOC Analyst Focus:

- Abnormal download activity
 - Multiple access from unknown locations
-

19. Syslog (Port 514)

What is it?

Used for centralized logging from devices.

What attackers can do:

- Hide logs
- Flood logs to hide real activity

SOC Analyst Focus:

- Log manipulation
 - Gaps in expected logs
 - Large log bursts
-

20. HTTPS over VPN (OpenVPN, IKEv2, etc.)

What is it?

Encrypted remote access via VPN protocols.

What attackers can do:

- Hide command and control
- Gain secure remote access

SOC Analyst Focus:

- VPN logins from unusual geolocations
- Session hijacking attempts
- Overuse of bandwidth

Stay tuned for my next post ...