Comprehensive Guide to Network Ports and Protocols for SOC Analysts

Abstract

For Security Operations Center (SOC) analysts, a strong understanding of network ports and their associated protocols is essential for effective monitoring, detection, and response. This guide provides an overview of common network ports, explaining their purpose and relevance within security operations.

Contents

1 Introduction **2**

2 Network Ports and Protocols **2**

2.1 Apple Filing Protocol (AFP) . . . 2
2.2 Dynamic Host Configuration Protocol (DHCP) . . . 2
2.3 Domain Name System (DNS) . . . 2
2.4 File Transfer Protocol (FTP) . . . 2
2.5 Hypertext Transfer Protocol (HTTP) . . . 2
2.6 Hypertext Transfer Protocol Secure (HTTPS) . . . 2
2.7 Secure Shell (SSH) . . . 3
2.8 Remote Desktop Protocol (RDP) . . . 3
2.9 Simple Mail Transfer Protocol (SMTP) . . . 3
2.10 Internet Message Access Protocol (IMAP) . . . 3
2.11 Post Office Protocol (POP3) . . . 3
2.12 Lightweight Directory Access Protocol (LDAP) . . . 3
2.13 Syslog . . . 3
2.14 Network Time Protocol (NTP) . . . 3
2.15 Simple Network Management Protocol (SNMP) . . . 4
2.16 Telnet . . . 4
2.17 Database Ports (MySQL, MSSQL, Oracle) . . . 4
2.18 Kerberos . . . 4
2.19 Windows File Sharing (SMB) . . . 4
2.20 Virtual Private Network (VPN) . . . 4

3 Additional Ports for SOC Monitoring **4**

3.1 Secure Real-Time Transport Protocol (SRTP) . . . 4
3.2 Hypertext Transfer Protocol Proxy (HTTP Proxy) . . . 5
3.3 Elasticsearch . . . 5

1 Introduction

This document details essential network ports and protocols relevant for SOC analysts. These ports are commonly monitored in security operations and help detect unusual activity, possible threats, and unauthorized access attempts. Each section includes a description of the port's usage and security considerations.

2 Network Ports and Protocols

2.1 Apple Filing Protocol (AFP)

Port: 548
AFP is primarily used on macOS systems for file sharing, allowing networked macOS devices to share files and resources securely.

2.2 Dynamic Host Configuration Protocol (DHCP)

Ports: 67, 68
DHCP automatically assigns IP addresses to devices on a network, simplifying network configuration. Monitoring DHCP is important for tracking network devices and detecting rogue devices.

2.3 Domain Name System (DNS)

Port: 53
DNS resolves domain names into IP addresses, enabling access to websites and services. Malicious DNS requests can indicate phishing or exfiltration attempts.

2.4 File Transfer Protocol (FTP)

Ports: 20, 21
FTP facilitates file transfers but lacks encryption, making it susceptible to interception. Monitoring FTP is essential in detecting unauthorized file movements.

2.5 Hypertext Transfer Protocol (HTTP)

Port: 80
HTTP is the primary protocol for web traffic. Analyzing HTTP traffic helps identify potential threats, such as malicious websites or C2 communications.

2.6 Hypertext Transfer Protocol Secure (HTTPS)

Port: 443
HTTPS encrypts HTTP traffic using SSL/TLS. Though secure, HTTPS can mask malicious traffic, so SOC analysts often monitor HTTPS for encrypted threats.

2.7 Secure Shell (SSH)

Port: 22
SSH provides secure remote access to servers. SOC analysts monitor SSH to detect unauthorized access or brute-force attempts.

2.8 Remote Desktop Protocol (RDP)

Port: 3389
RDP enables remote access to Windows desktops. Due to its frequent targeting by attackers, RDP traffic is crucial to monitor for unusual login patterns.

2.9 Simple Mail Transfer Protocol (SMTP)

Ports: 25, 587
SMTP is used for sending emails. Unusual SMTP traffic can signify phishing, spamming, or data exfiltration attempts.

2.10 Internet Message Access Protocol (IMAP)

Port: 143
IMAP retrieves email from mail servers. Monitoring this port can help detect unauthorized access to email accounts.

2.11 Post Office Protocol (POP3)

Port: 110
POP3 is another email retrieval protocol. Any abnormal POP3 activity may suggest compromised accounts.

2.12 Lightweight Directory Access Protocol (LDAP)

Port: 389
LDAP is used in directory services for user and device authentication. Analyzing LDAP traffic helps detect unauthorized directory access.

2.13 Syslog

Port: 514
Syslog is used for logging events from network devices, providing centralized event tracking crucial for incident detection and investigation.

2.14 Network Time Protocol (NTP)

Port: 123
NTP synchronizes device clocks, ensuring accurate timestamps for events. NTP spikes may indicate NTP reflection attacks.

2.15 Simple Network Management Protocol (SNMP)

Ports: 161, 162
SNMP manages and monitors network devices. Unexpected SNMP requests might signify reconnaissance attempts.

2.16 Telnet

Port: 23
Telnet provides remote access but lacks encryption, making it a target for exploitation. SOC analysts flag any Telnet activity as suspicious in secure environments.

2.17 Database Ports (MySQL, MSSQL, Oracle)

Ports: 3306 (MySQL), 1433, 1434 (MSSQL), 1521 (Oracle)
Databases are commonly targeted by attackers for unauthorized access. Monitoring these ports can help detect anomalous database activity.

2.18 Kerberos

Port: 88
Kerberos is a secure authentication protocol used in Windows AD environments. Abnormal Kerberos activity may indicate credential attacks.

2.19 Windows File Sharing (SMB)

Ports: 445, 139
SMB facilitates file sharing on Windows. SMB is a target for lateral movement and ransomware, making it a critical port for SOC monitoring.

2.20 Virtual Private Network (VPN)

Ports: 1194 (OpenVPN), 1701 (L2TP), 4500 (IPSec)
VPN ports secure remote network access. Unusual VPN activity may indicate unauthorized access or brute-force attempts.

3 Additional Ports for SOC Monitoring

In addition to the above, SOC analysts may also monitor these ports:

3.1 Secure Real-Time Transport Protocol (SRTP)

Port: 5004
SRTP encrypts media streams, commonly used in VoIP applications.

3.2 Hypertext Transfer Protocol Proxy (HTTP Proxy)

Port: 8080
HTTP Proxies manage web traffic. Abnormal activity on this port could indicate proxy abuse.

3.3 Elasticsearch

Port: 9200
Elasticsearch is used in data analytics and search functions. Unauthorized access on this port could indicate a data breach.

Connect with Me

For more insights and professional discussions on SOC analysis, feel free to connect with me on LinkedIn: Meer Hamza K.