

Top 50 Well-Known Ports for SOC Analysts

| Port Number | Use | Cyber Risk |
|-------------|---|--|
| 20, 21 | FTP (File Transfer Protocol) | Unencrypted, susceptible to sniffing, spoofing, and brute force attacks. |
| 22 | SSH (Secure Shell) | Target for brute force attacks; vulnerable if weak credentials are used. |
| 23 | Telnet | Unencrypted, prone to eavesdropping, hijacking, and credential theft. |
| 25 | SMTP (Simple Mail Transfer Protocol) | Can be exploited for spamming and relay attacks. |
| 53 | DNS (Domain Name System) | Vulnerable to DNS spoofing and DDoS attacks. |
| 80 | HTTP (Hypertext Transfer Protocol) | Unencrypted, susceptible to interception and manipulation. |
| 110 | POP3 (Post Office Protocol version 3) | Unencrypted, vulnerable to eavesdropping if not secured. |
| 119 | NNTP (Network News Transfer Protocol) | Can be exploited in distributing malicious content. |
| 123 | NTP (Network Time Protocol) | Can be misused for DDoS attacks. |
| 137-139 | NetBIOS | Vulnerable to unauthorized access and spreading malware. |
| 143 | IMAP (Internet Message Access Protocol) | Unencrypted, potential for credential theft. |
| 161, 162 | SNMP (Simple Network Management Protocol) | Vulnerable to unauthorized access and information disclosure. |
| 443 | HTTPS (HTTP Secure) | Can be targeted by SSL stripping or MiTM attacks, though less risky than HTTP. |
| 445 | SMB (Server Message Block) | Known for vulnerabilities like EternalBlue, used in ransomware attacks like WannaCry. |
| 993 | IMAPS (Internet Message Access Protocol over SSL) | While encrypted, it can be a vector for targeted attacks if credentials are compromised. |
| 135 | Microsoft RPC | Can be exploited for unauthorized remote procedure calls. |
| 139 | NetBIOS Session Service | Vulnerable to unauthorized access and attacks on Windows networks. |
| 143 | IMAP (Internet Message Access Protocol) | Susceptible to interception, especially if unencrypted. |
| 389 | LDAP (Lightweight Directory Access Protocol) | Can be exploited in injection attacks and unauthorized access. |
| 443 | HTTPS (Hypertext Transfer Protocol Secure) | Potential for SSL/TLS vulnerabilities, MiTM attacks. |
| 445 | Microsoft-DS (Active Directory, Windows shares) | Known for SMB vulnerabilities, like EternalBlue. |
| 465 | SMTPS (Secure SMTP) | Can be targeted for spam and phishing attacks, even though encrypted. |
| 587 | SMTP with TLS/SSL | Secure, but can be targeted in mail-based attacks. |
| 636 | LDAPS (LDAP over SSL) | Encrypted, but vulnerable to specific SSL/TLS attacks. |
| 993 | IMAPS (IMAP over SSL) | Encrypted, but susceptible to targeted email attacks. |

| | | |
|------------|---|---|
| 995 | POP3S (POP3 over SSL) | Encrypted, but vulnerable to targeted email attacks. |
| 1723 | PPTP (Point-to-Point Tunneling Protocol) | Known vulnerabilities in VPN connections. |
| 3306 | MySQL Database Service | Vulnerable to SQL injection and unauthorized access. |
| 3389 | RDP (Remote Desktop Protocol) | Target for brute force and credential stuffing attacks. |
| 5900 | VNC (Virtual Network Computing) | Vulnerable to eavesdropping and remote control if unsecured. |
| 69 | TFTP (Trivial File Transfer Protocol) | Unsecured, vulnerable to interception and unauthorized access. |
| 88 | Kerberos | Can be targeted for authentication attacks. |
| 109 | POP2 (Post Office Protocol version 2) | Unencrypted, susceptible to eavesdropping. |
| 156 | SQL Service | Vulnerable to SQL injection and unauthorized access. |
| 194 | IRC (Internet Relay Chat) | Can be used for communication in botnets, susceptible to eavesdropping. |
| 220 | IMAP3 (Internet Message Access Protocol version 3) | Prone to the same risks as IMAP. |
| 389 | LDAP (Lightweight Directory Access Protocol) | Susceptible to directory traversal and unauthorized access. |
| 427 | SLP (Service Location Protocol) | Vulnerable to spoofing and DoS attacks. |
| 546, 547 | DHCPv6 (Dynamic Host Configuration Protocol for IPv6) | Vulnerable to unauthorized DHCP servers and MITM attacks. |
| 554 | RTSP (Real Time Streaming Protocol) | Can be exploited in streaming and DoS attacks. |
| 631 | IPP (Internet Printing Protocol) | Vulnerable to interception and unauthorized printing/access. |
| 989, 990 | FTPS (FTP over SSL) | More secure than FTP, but still can be targeted for data interception. |
| 1194 | OpenVPN | Can be targeted in VPN bypass and DoS attacks. |
| 1433, 1434 | Microsoft SQL Server | Vulnerable to SQL injection and unauthorized access. |
| 1701 | L2TP (Layer 2 Tunneling Protocol) | Vulnerable in unencrypted implementations. |
| 1812, 1813 | RADIUS (Remote Authentication Dial-In User Service) | Vulnerable to credential theft and replay attacks. |
| 2049 | NFS (Network File System) | Vulnerable to unauthorized file access and interception. |
| 2082, 2083 | cPanel | Can be targeted for web hosting control panel attacks. |
| 2483, 2484 | Oracle Database | Vulnerable to SQL injection and unauthorized access. |
| 5060, 5061 | SIP (Session Initiation Protocol) | Vulnerable to VoIP spam, eavesdropping, and hijacking. |