|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CONSIDERED SECURE - are designed to provide confidentiality, integrity, and availability.** | | | | | |
| **CONSIDERED INSECURE - do not provide these guarantees.** | | | | | |
| **PROTOCOL** | **PORT** | **TCP/UDP port** | **OSI LAYER** | **DESCRIPTION** | **ATTACKS/ VULNERABILITES** |
| **IEEE 802.11** | - | - | Physical | Specifies MAC & physical layer protocols for implementing WLAN Wi-Fi. | DoS by MAC address spoofing |
| **PPTP** (Point- to-Point Tunneling Protocol) | 1723 | Both | Data Link | Implements VPN; Uses TCP control channel and Generic Routing Encapsulation(GRE) | MitM; Bit flipping |
| **L2TP** (Layer 2 Tunneling Protocol) | 1701 | Both | Data Link | Extension of PPP; Uses UDP to avoid TCP meltdown problem. | DoS |
| **PPP (**Point to Point Protocol) | - | - | Data Link | Provides communication b/w 2 routers directly without any host or networking; Provides connection authentication, transmission encryption & compression. | Format string attack |
| **ARP** (Address Resolution Protocol) | - | - | Layer 2.5 | Discovers the MAC address; Creates a communication in internal N/W. | ARP cache poisoning |
| **RARP** (Reverse Address Resolution Protocol) | - | - | Layer 2.5 | Resolves MAC address to an IP address. | ARP Poisoning |
| **ICMP** (Internet Control Message Protocol) | - | - | Network | Used by ping & traceroute utility to report info. about network connectivity; Uses a data packet with 8- byte header; Each packet has a Type & Code; No port used as N/W software itself interprets all ICMP messages. | Ping sweep; Ping flood; ICMP tunneling; Forged ICMP redirects |
| **IGMP** (Internet Group Management Protocol) | - | - | Network | Used by TCP/IP suite to achieve dynamic multicasting; Class D IP addresses are used. | DoS |
| **OSPF** (Open Shortest Path First) | - | - | Network | Routing protocol for IP networks; Uses link state routing algorithm; Part of interior gateway protocols (IGPs). | DoS; Local authentication bypass |
| **NAT** (Network Address Translation) | - | - | Network | Maps one IP address space to another; Modifies network address in IP header of packets; Helps to conserve global address space. | DoS; Interception of internal & external traffic due to improper configuration. |
| **PAT** (Port Address Translation) | - | - | Network | Aka NAT overloading; Permits multiple devices on a LAN to be mapped to a single public IP address; Provides many-to-one relationship. | Discovery of intranet IP addresses. |
| **IP** (Internet Protocol) | - | - | Network | Provides the functions necessary to deliver a datagram from a source to a destination over an interconnected system of networks; No reliability, flow control & sequencing. | IP Spoofing |
| **RIP** (Routing Information Protocol) | 520 | UDP | Network | Dynamic routing protocol; Uses hop count to find the best path b/w source & destination. | DDoS reflection attacks. |
| **IPSEC** (IP Security) | 1293 | Both | Network | Provides data authentication, integrity, and confidentiality; 3 components: Encapsulating Security Payload, Authentication Header & Internet Key Exchange. | Bleichenbacher attack |
| **TCP** (Transmission Control Protocol) | 0-65535 | TCP | Transport | Connection oriented; Error checks & reporting; Acknowledgement; 20 byte header. | SYN flooding; TCP Reset; TCP Session hijacking |
| **UDP** (User Datagram Protocol) | 0-65535 | UDP | Transport | Connectionless; Error checks but no reporting; No acknowledgement; 8 byte header. | UDP flood attack. |
| **NETBIOS** (N/W Basic Input Output System) | 137,138 | Both | Session | Allows applications on separate computers to communicate over a local area network; Relies on API. | Information disclosure; Connection using null sessions |
| **RPC** (Remote Procedure Call) | 530 | Both | Session | Used for interprocess communication in client- server based applications. | XML-RPC attacks. |
| **SMB** (Server Message Block) | 139,445 | Both | Session | Enables user to access file on a server, or other application; CIFS was its early version. | Eternal Blue attack; Gives remote access; WannaCry & Petya. |
| **SOCKS** (Socket Secure) | 1080 | Both | Session | Exchanges network packets between a client and server through a proxy server; No compatibility issues unlike HTTP proxy. | Arbitrary command execution; DoS |
| **RTP** (Real- time Transport Protocol) | 16384-32767 | Both | Session | VoIP protocol; Delivers audio & video over IP networks. | RTP flooding attack; RTP bleed |
| **SRTP** (Secure Real-time Transport Protocol) | 16384-32767 | Both | Transport | Protect the privacy and integrity of real-time multimedia communications, such as voice and video, over IP networks. | Cryptographic attacks; Replay attacks; DoS; Man-in-the-middle |
| **SSL** (Secure Sockets Layer) | - | - | Presentation | Establishes encrypted communication b/w client & server. | BEAST; SSL Renegotiation |
| **TLS** (Transport Layer Security) | - | - | Presentation | Establishes encrypted communication b/w client & server. | DROWN; ROBOT; POODLE; Heartbleed |
| **Kerberos** | 88 | Both | Presentation | Provides security & authentication, Uses symmetric key distribution using symmetric encryption to access file server; Helps nodes to prove their identity to one another. | DoS; Arbitrary code execution; Buffer Overflow. |
| **WPA** (Wi-Fi Protected Access) | - | - | Presentation | Security standard that provides better encryption & authentication than WPA. | KRACK |
| **MIME** (Multipurpose Internet Mail Extensions) | - | - | Presentation | Supports text in multiple character sets; as well as attachments of audio, video, apps & images. | XSS using MIME Sniffing |
| **ECHO** | 7 | Both | Application | Used for testing & measurement of round trip timings in IP networks; Server sends back identical copy of the data it received. | DoS |
| **DHCP** (Dynamic Host Configuration Protocol) | 67 | UDP | Application | A network management protocol used to automate the process of configuring devices on IP networks. | Remote code execution; Bogus DHCP client & server |
| **BOOTP** (Bootstrap Protocol) | 67,68 | Both | Application | Older version of DHCP; Automatically assigns IP address to network devices from a configuration server. | BootpD; BOOTP server impersonation |
| **HTTP (Hyper Text Transfer Protocol)** | 80 | Both | Application | Used for communication over World Wide Web. | MitM attack |
| **HTTPS (Hyper Text Transfer Protocol Secure)** | 443 | Both | Application | HTTPS with SSL for security. | SSL Stripping; DROWN attack |
| **FTP (File Transfer Protocol)** | 20,21 | Both | Application | File transfer, Uses TCP, hence file delivery is guaranteed. | Brute force attack; Packet capture; Anonymous authentication; Directory traversal attack |
| **FTPS (FTP with SSL)** | 989,990 | Both | Application | Uses command channel & opens new connections for data transfer; Requires a certificate. | MitM |
| **SFTP (SSH File Transfer Protocol)** | 22 | Both | Application | Uses encrypted credentials to authenticate; SSH keys can also be used to authenticate. | Brute force attack |
| **POP3 (Post Office Protocol)** | 110,995 | Both | Application | Store-and-forward client/server protocol; Deletes mail on server as soon as user has downloaded it. | Buffer overflow in POP3 servers can cause DoS. |
| **SSH (Secure Shell)** | 22 | Both | Application | Cryptographic network protocol for operating network services securely over an unsecured network. | Static SSH keys; Embedded SSH keys can provide backdoor. |
| **Telnet (TELecommun ication NETwork)** | 23 | Both | Application | Allows to connect to remote computers over a TCP/IP network. | Brute force; Stealing credentials by sniffing; SSH and SMTP banner grabbing. |
| **NTP (Network Time Protocol)** | 123 | Both | Application | Synchronizes clock among devices. | NTP Amplification DDoS attack. |
| **IMAP/S (Internet Message Access Protocol)** | 143; 993 | Both | Application | Allows user to create folders & assign messages to folders; User can obtain just the message header (useful in low-bandwidth connection). | Password spraying attacks. |
| **DNS (Domain Name System)** | 53 | Both | Application | Resolute names in TCP/IP network. | Typosquatting; DNS Poisoning. |
| **SOAP (Simple Object Access Protocol)** | 80 | Both | Application | XML based messaging protocol to exchange info; Characteristics: extensibility, neutrality & independence. | SOAP injection; Unauthenticated romote access |
| **SNMP/S (Simple Network Management Protocol)** | 161; 162 | Both | Application | Allows network manager to monitor networking equipment & remotely modify settings & configuration. | Sniffing of plain text password; Modification of packet header. |
| **SMTP (Simple Mail Transfer Protocol)** | 25; 465 | Both; TCP | Application | Transfers mail from sender’s mail server to recipient’s mail server. | Account enumeration; E-mail header disclosures; Helps find internal IPs. |
| **SMTP/S (Simple Mail Transfer Protocol Secured)** | 465, 587 | TCP | Application | Secure version of SMTP, and it provides encryption and authentication mechanisms to protect the confidentiality and integrity of email messages. | Man-in-the-middle; Spoofing; DoS; Brute-force |
| **SNTP (Simple Network Time Protocol)** | 123 | - | Application | Used when full implementation of NTP is not needed; Synchronizes a computer's system time with a server that has already been synchronized by a source such as a radio, satellite receiver or modem; Supports unicast, multicast and anycast operating modes. | DoS via a crafted NTP packet. |
| **RFB (Remote Frame Buffer)** | 5900 | Both | Application | Used by VNC (Virtual N/W computing) [only TCP port used]; Graphical desktop sharing system; Used in technical support. | Stack buffer overflow; Information disclosure. |
| **RDP (Remote Desktop Protocol)** | 3389 | Both | Application | Provides GUI to connect to another computer. | Reverse RDP attack; Sabotage sandboxes. |
| **TFTP (Trivial File Transfer Protocol)** | 69 | Both | Application | A lockstep FTP; Allows a client to get a file from or put a file onto a remote host. | No encryption & authentication; TFTP server spoofing. |
| **NFS (Network File System)** | 2049 | Both | Application | Allows a user to access files over a computer network much like local storage is accessed. | Elevation of privilege; Arbitrary code execution. |
| **SIP/S (Session Initiation Protocol)** | 5060; 5061 | Both; TCP | Application | Used for initiating, maintaining & terminating real-time sessions; VoIP protocol. | Registration hijacking; Message tampering. |
| **LDAP/S (Lightweight Directory Access Protocol)** | 389; 636 | Both | Application | An open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an IP network. | LDAP injection; DoS; NULL Base querying |