Cyberkraft

Security+ 601 Ports and Protocols Reference Sheet

Layer 7 Application	Port Number	Use
File Transfer Protocol (FTP)	20/21	Port 21 is the control port while port 20 is used to transfer files.
Secure Shell (SSH)	22	Designed to transmit data through a remote connection.
SSH File Transfer Protocol	22	A completely separate protocol from FTP (it is not compliant with FTP servers) that uses SSH to encrypt file transfers.
TACACS+	49	Cisco proprietary protocol used for authentication, authorization, and accounting (AAA) services
Domain Name System (DNS)	53	Used to associate IP addresses with domain names
Dynamic Host Configuration Protocol (DHCP)	67/68	This network management protocol is used to assign local IP addresses to devices on a network. It is used to create multiple private IP addresses from one public IPv4 address.
Hypertext Transfer Protocol (HTTP)	80	Protocol used for websites and most internet traffic.
Kerberos	88	Network authentication protocol that allows for communication over a non-secure network.
Post Office Protocol (POP)	110	E-mail protocol that allows e-mail clients to communicate with e-mail servers. POP provides only one-way communication.

Internet Message Access Protocol (IMAP)	143, 993	E-mail protocol used by e-mail clients to communicate with e-mail servers. Provides two way communication unlike POP.
Simple Network Management Protocol (SNMP)	161/162	Protocol used to monitor and manage network devices on IP networks.
Lightweight Directory Access Protocol (LDAP)	389	Used to manage and communicate with directories.
Hypertext Transfer Protocol Secure (HTTPS)	443	Secure version of HTTP that used TLS for encryption. Most websites use HTTPS instead of HTTP.
Lightweight Directory Access Protocol Secure (LDAPS)	636	Secure version of LDAP that uses TLS for encryption.
File Transfer Protocol Secure (FTPS)	989/990	FTPS uses TLS for encryption. It can run on ports 20/21 but is sometimes allocated to ports 989/990.
Internet Message Access Protocol Secure (IMAPS)	993	Secure version of IMAP that uses TLS for encryption.
Post Office Protocol 3 Secure (POP3S)	995	Secure version of POP that uses TLS for encryption.
Remote Authentication Dial-In User Service (RADIUS)	1812, 1813	Used to provide AAA for network services
Diameter	3868	Developed as an upgrade to Radius
Secure Real Time Protocol (SRTP)	5004	SRTP replaced RTP and is a protocol used to stream audio and video communication using UDP.

Layer 5 Session Layer	Port Number	Use
Layer 2 Tunneling Protocol (L2TP)	1701	Used to create point to point connections, like VPNs over a UDP connection. Needs IPSec for encryption. Designed as an extension to PPTP. Operates at the data link layer but encapsulates packets at the session layer.
Layer 4 Transport	Port Number	Use
Transmission Control Protocol (TCP)	N/A	One of two main protocols of the Internet Protocol (IP) suite used to transmit data over an IP network. TCP provides error checking to ensure packets are not lost in transit.
User Datagram Protocol (UDP)	N/A	The second main protocol in the IP suite that transmits datagrams in a best effort method. UDP does not include error checking.
Point to Point Tunneling Protocol (PPTP)	1723	Based on PPP. Deprecated protocol for VPNs.
Remote Desktop Protocol	3389	Windows proprietary protocol that provides a remote connection between two computers.

Layer 2 Data Link Layer	Port Number	Use
Point to Point Tunneling Protocol	1723	Based on PPP. Deprecated protocol for VPNs.