Cyberkraft

Security+ 701 Ports and Protocols Reference Sheet

Layer 7 Application	Port	TCP/ UDP	Use
File Transfer Protocol (FTP)	20/21	TCP	Port 21 is the control port while port 20 is used to transfer files.
Secure Shell (SSH)	22	TCP	Designed to transmit data through a remote connection.
SSH File Transfer Protocol	22	TCP	A completely separate protocol from FTP (it is not compliant with FTP servers) that uses SSH to encrypt file transfers.
Simple Mail Transfer Protocol (SMTP)	25	TCP	Internet mail protocol used to send outgoing mail from email clients to mail servers.
TACACS+	49	TCP	Cisco proprietary protocol used for authentication, authorization, and accounting (AAA) services
Domain Name System (DNS)	53	UDP	Used to associate IP addresses with domain names
Dynamic Host Configuration Protocol (DHCP)	67/68	UDP	This network management protocol is used to assign multiple local private IP addresses from one public IPv4 address.
Hypertext Transfer Protocol (HTTP)	80	TCP	Protocol used for websites and most internet traffic.
Kerberos	88	TCP/ UDP	Network authentication protocol that allows for communication over a non-secure network. Primarily uses UDP but can use TCP.
Post Office Protocol (POP)	110	TCP	E-mail protocol that allows e-mail clients to communicate with e-mail servers. POP provides only one-way communication.
Network Time Protocol	123	UDP	Low latency protocol used to synchronize timekeeping across a network.
Server Message Block (SMB)	139	UDP	Windows proprietary protocol built on NetBIOS. Allows users to remotely access servers. Originally used port 139 over UDP.

Cyberkraft

Internet Message Access Protocol (IMAP)	143, 993	TCP	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	UDP	Protocol used to monitor and manage network devices on IP networks.
Lightweight Directory Access Protocol (LDAP)	389	UDP	Used to manage and communicate with directories.
Hypertext Transfer Protocol Secure (HTTPS)	443	TCP	Secure version of HTTP that used TLS for encryption. Most websites use HTTPS instead of HTTP.
Secure Socket Tunneling Protocol (SSTP)	443	TCP	Microsoft developed SSTP technology to replace the more insecure PPTP or L2TP/IPSec options available in Windows. SSTP uses TLS
Server Message Block (SMB)	445	TCP	Windows proprietary protocol built on NetBIOS. Allows users to remotely access servers. Modern versions use port 445 and TCP.
Internet Protocol Security (IPSec) using ISAKMP	500	UDP	Internet Protocol security achieved through the use of ISAKMP – Internet Security Association and Key Management Protocol
Simple Mail Transfer Protocol Secure (SMTPS)	587	TCP	The secure version of SMTP. Uses TLS for encryption.
Lightweight Directory Access Protocol Secure (LDAPS)	636	TCP	Secure version of LDAP that uses TLS for encryption.
File Transfer Protocol Secure (FTPS)	989/ 990	TCP	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	TCP	Secure version of IMAP that uses TLS for encryption.
Post Office Protocol 3 Secure (POP3S)	995	TCP	Secure version of POP that uses TLS for encryption
Remote Authentication Dial-In User Service (RADIUS)	1812, 1813	UDP	Used to provide AAA for network services

Remote Desktop Protocol (RDP)	3389	TCP	This Windows proprietary protocol that enables remote connections to other computers
Diameter	3868	TCP	Developed as an upgrade to Radius
Secure Real Time Protocol (SRTP)	5004	UDP	SRTP replaced RTP and is a protocol used to stream audio and video communication using UDP.
Layer 4 Transport	Port	TCP/ UDP	Use
Transmission Control Protocol (TCP)	N/A	TCP	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	UDP	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	TCP	Based on PPP. Deprecated protocol for VPNs.
Layer 2 Data Link	Port	TCP/ UDP	Use
Layer 2 Tunneling Protocol (L2TP)	1701	UDP	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.
Point to Point Tunneling Protocol (PPTP)	1723	UDP	Based on PPP. Deprecated protocol for VPNs.