6.1.8 Enumerate Ports and Services Facts

Enumeration requires the ethical hacker to understand protocols, ports, and services. Although these items are a prerequisite for this course, we're going to identify the ones that are used for enumeration. The following table lists common ports:

Port	Description
TCP 21 FTP	Port 21 is used for the File Transfer Protocol (FTP). FTP is used by all operating systems to transfer files between client and server machines.
TCP 23 Telnet	Port 23 is used for the Telnet protocol/software. Telnet is used to connect to and run services on remote systems. Because of security concerns, Telnet is not used as frequently as it once was.
TCP 25 SMTP	Port 25 is used for the Simple Mail Transfer Protocol (SMTP). SMTP is used to send emails between client and server and between server and server.
TCP 53 DNS	Port 53 is used for DNS zone transfers. DNS zone transfer is the process of transferring a copy of the DNS zone file from the primary DNS server to a secondary DNS server. Zone transfers are designed to provide updated network and access information to the DNS servers.
UDP 53 DNS	Port 53 is used for UDP queries about IP-to-name and name-to-IP mappings.
TCP 80 HTTP	Port 80 is used for Hypertext Transport Protocol. HTTP is used by all web browsers and most web applications.
TCP 135 RPC	Port 135 is used by the Remote Procedure Call service in Windows for client-server communications.
TCP 137 NetBIOS	Port 137 is used by the NetBIOS Name Server (NBNS.) NBNS is used to associate names and IP addresses of systems and services.
TCP 139 NetBIOS	Port 139 is used by the NetBIOS Session Service (SMB over NetBIOS.) SMB over NetBIOS allows you to manage connection between NetBIOS clients and applications.
TCP 445 SMB over TCP	Port 445 is used by SMB over TCP. SMB over TCP also known as Direct Host is a service used to improve network access. This service is available in Windows 2000 and newer.
UDP 161 and 162 SNMP	Ports 161 and 162 are used by the Simple Network Management Protocol (SNMP.) SNMP is a standard method of managing devices and software from most manufacturers.
TCP/UDP 389 LDAP	Port 389 is used by the Lightweight Directory Access Protocol (LDAP.) LDAP is an internet protocol for accessing distributed directory service. If this port is open, it indicates that Active Directory or Exchange may be in use.
TCP/UDP 3268 Global Catalog Service	Port 3268 is used by the Global Catalog Service. The Global Catalog Service is used by Windows 2000 and later systems to locate information in Active Directory.