Introductory Networking writeup

This write up will cover tryhackme’s introductory networking room. We look at the OSI, TCP/IP models and some basic networking tools. They have us start with the 7 layers of the OSI model as a stander for networking communications. Layer 7 the application layer will pass data from applications running on a computer and start to prep that data to be passed onto the next layer of the OSI. Layer 6 the presentation layer here data received from the application layer is translated into a standardized format the receiving machine can understand as well as any encryptions compression or other transformations that would be done on the data before being sent through the network next data is passed to layer 5 the session layer when correctly formatted data is received this layer will establish a connection to another system on the network via the same OSI layer of the system when a connection is established the data is sent to layer 4. The Transport layer will do several things first it will choose a protocol TCP or UDP over which data will be sent. Think of TCP as using a garden hose to fill a bucket verses UDP where you using the rain to fill the bucket you catching water your just not catching all of the water all the time this is why streaming comes in grainy sometimes not all the water is getting into the bucket. With a protocol chosen the data is broke down into bite size pieces and sent to layer 3. The networking layer is responsible for locating the destination and the path to get to that destination using a IPV4 formatted logical address once the path is set. Layer 2 the data link layer establishes MAC addresses via NIC’s in both machines basically verifying who’s on each side of the conversation and makes sure there’s no information corrupted during transmission. Finally it will present the data in a format suitable for transmission (1’s and 0’s) to layer 1 the physical layer. The hardware that sends and receives those 1’s and 0’s as electrical pulses or signals that can be sent and received over a network and converted back into binary for the next peace of hardware. The TCP/IP model is vary similar to the OSI model it just lumps some of the OSI layers together. The application, presentation, and session layers in the OSI model are lumped into TCP/IP application layer. OSI network layer turns into TCP/IP internet layer. Last OSI data link and physical layers are combined to form TCP/IP network interface layer. We cover how TCP is a three way hand shake using synchronies and acknowledgment. Clients will syn with server. Server will syn/ack the client. Client will ack. The tools we cover in this lab are ping, tracrout, whois and dig. Ping is used to find information on your endpoint using ping <target>. Tracrout shows information on the path to that endpoint using traceroute <destination>. Whois will help you determine who or what owns that endpoint with whois <domain>. Dig will help you manually connect from a dns server to the end domain using dig <domain> @<dns-server-ip>.