Module 14
(A Little Networking)

• In this module, we briefly introduce the OSI 7-layer network model. You will become aware of the different layers of the model and will start to understand the structure of packets used in layers 3 and 4 of an IP network.
 OSI Model

- Open Systems Interconnection (Model) ISO/IEC 7498-1
- Messages to be sent flow from top to bottom, the SDU (service data units) from the upper layers are encapsulated in PDUs (protocol data units) as the messages go from one layer to the next.

- Received messages flow from bottom to top, unwrapping the SDUs at each layer.

Picture source: about.com
What OSI Layers do Penetration Testers Deal With?

• Possibly all layers. If any kind of tap is installed in a physical network, we're working at layer 1. If any application communication is intercepted, we're working at layer 7.

• Two layers that will be foreign to some of you but are of great importance are layers 3 (network) and 4 (transport).

• We'll look at the IP Network Layer protocol.

• We'll also briefly look at Transport Layer protocols ICMP, TCP, and UDP.
IPv4

- Connectionless protocol used on packet-switching networks.
- No guarantee of delivery or sequence of packets.
- Addresses: 32-bits
- TTL Field (decremented upon forwarding) guarantees packets don't live forever.
ICMP

- ICMP is the Internet Control Message Protocol.
- ICMP Packets embedded in IP with protocol = 1.
- These messages are used for control or diagnostic purposes or are generated in response to errors associated with IP operations.

<table>
<thead>
<tr>
<th>ICMP packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit 0 - 7</td>
</tr>
<tr>
<td>Version/IHL</td>
</tr>
<tr>
<td>Identification</td>
</tr>
<tr>
<td>Time To Live (TTL)</td>
</tr>
<tr>
<td>Source IP address</td>
</tr>
<tr>
<td>ICMP Payload (8+ bytes)</td>
</tr>
<tr>
<td>Quench</td>
</tr>
</tbody>
</table>
TCP and UDP
What are They, Really?

- TCP is a communication protocol that provides reliable ordered streams of octets between programs.

- UDP is a communication protocol that provides communication of *datagrams* or packets of octets.

  TCP communicates streams as ordered sequences of packets. UDP packets are not guaranteed to be received in the same order in which they were sent. (This really happens!)

- TCP is useful for communications where it is critical to know what order the data are received in. Example would be file transmission.

- UDP is useful for real-time communication where speed of transmission is more important than reliability or order of receipt. Example: On-line First-Person-Shooter (FPS) game screen updates. One is more willing to live with small glitches than the slower interface TCP would require.
TCP

- TCP Packet Structure will be covered in more detail the next module.
UDP

- UDP Packet Structure will be covered in more detail in a higher-numbered module.