Module 16
(VM Networks, UDP, ICMP, Traceroute and a tiny bit about Wireshark)

- In this module, we find out a little bit about how virtual machines can be networked to each other and the outside world. We also see a little more about the structure of UDP and ICMP packets. We identify some important ICMP packet types and discuss how traceroute works. We then look at running Wireshark to see what happens when we're running traceroute.
VM Networks

- Virtual Machine Applications maintain a virtual network inside the host machine. It serves as a gateway for the virtual machines.
- Three network options for the virtual machines are usually available:
  - Host only (VMs cannot communicate outside the virtual network)
  - Bridged (VM packets are routed directly to the external network on which the host is attached)
  - NAT (Network Address Translation) or Shared (communicating VM ports are assigned host ports and the source address is overwritten with the host address. Replies to the host port are sent back to the VM.)
# UDP Packet Structure

- Like TCP Packets, have a source and destination.
- Aside from this, they contain length, checksum and application data.
- These are quite primitive!

<table>
<thead>
<tr>
<th>Source Port Number (16 bits)</th>
<th>Destination Port Number (16 bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length (UDP Header + Data) 16 bits</td>
<td>UDP Checksum (16 bits)</td>
</tr>
</tbody>
</table>

Application Data (Message)
ICMP Packet Structure

- Message Type - 8 bits
- Code (subtype of message) - 8 bits
- Checksum (of header + data excluding checksum) - 16 bits
- Other header data (labeled Quench here) – 32 bits
- Data – rest of packet

<table>
<thead>
<tr>
<th>Type of message</th>
<th>Code</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quench</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data (optional)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Common ICMP Packet Types

- 0 – Echo reply (response to a ping)
- 3 – Destination Unreachable
- 5 – Redirect (use another route to your destination)
- 8 – Echo request (aka ping)
- 11 – Time Exceeded (TTL became 0)
How Does Traceroute Work?

- Traceroute tries to find all hosts on the network between your local host and some destination host.
- It does this by sending packets with TTLs increasing from 1 up to 30.
- For each TTL, 3 packets are sent.
- As each packet expires, it should receive an ICMP Time Exceeded reply from the host at which it arrived.
- Traceroute waits 5 seconds for each expiration.
  - If 5 seconds is exceeded, a * is printed.
  - Otherwise, the IP address and name of each host responding with the Time Expired message along with the TTL value are printed.
Wireshark and Traceroute

• Wireshark is a packet sniffing and analysis tool.
• It is extremely useful.
• You can find Wireshark in kali at Applications-> Kali Linux-> Information Gathering-> Traffic Analysis-> wireshark
• Once it starts up, you can start to sniff packets by selecting Capture->Interfaces
• And choosing a network interface to sniff.
• It will show you the packets that it captures on that interface.
Demonstration

• I run Wireshark and do a traceroute on my Mac
• I show you what happens and how to look at the packets to see traceroute's behavior (3 pings), 3 responses, recording of the ICMP Time Exceeded response.
• I then do the same thing in a NATed kali VM and we see that almost all the responses are *s.
• Let's talk about that.