CprE 489
Lab 2 Report
Matt Rose
2/11/16

In this lab, we learned how to analyze network traffic using tcpdump, tcptrace, and wireshark, a packet sniffing tool. With these tools, we can glean valuable information on how our traffic is routed, and if we're so inclined, we can learn secrets about user's private information, such as usernames, passwords, sensitive material, etc. Of course, we would never use these tools for such means, but they can be helpful in analyzing possible security weaknesses, viewing traffic as network admin, and debugging network applications.

(Performed lab at home between my two Linux machines)
1. IP address of laptop pinging desktop: 192.168.1.104
2. The -X flag will print the packet in ASCII and hex.
3. The -P flag can filter packets based on direction (send/receive). This can help alleviate noise in output.
4. IAState:
   a) Source IP: 192.168.1.105: 60433; Destination: 129.186.97.220: 443
   b) Duration: 30 seconds (homepage, then Academics tab)
   c) 4 packets sent from my machine, 4 packets received.
   d) send: avg owin: 17 bytes, wavg owin: 0 bytes
      receive: avg owin: 17 bytes, wavg owin: 33 bytes
Huawei (Assuming jh-in-f188.1e100.net is Huawei – can't find host in tcpdump):
   a) Source IP: 192.168.1.105: 60654, Destination: 74.125.225.7: 443
   b) 37 seconds
   c) 32 total: 15 out, 17 in.
   d) send: avg owin: 311 bytes, wavg owin: 39 bytes
      receive: avg owin: 81 bytes, wavg owin: 1 byte
5. RTT avg: mrose → iastate: 12.9 ms
   RTT avg: mrose → Huawei: 25.6 ms
6. a) Each ICMP packet contains 98 bytes
   b) The hex pattern is very similar, with a variable header based on request/reply and the same payload for both request and reply.
   c) A new ICMP request is sent roughly 1 s after the last reply is received.
   d) We can tell if a superuser is running ping if the inter-arrival time is less than 0.2 seconds.
7. a) Other than TCP, we caught UDP, TLSv1.2, DNS, and ARP
   b) UDP IP header: User Datagram Protocol, Src Port: https (443), Dst Port: 49257 (49257)
      TCP IP header: Transmission Control Protocol, Src Port: 37273 (37273), Dst Port: https (443), Seq: 204, Ack: 4200, Len: 0
      The difference in the headers is that UDP only contains the port numbers where TCP includes the IP numbers, port numbers, and length of message.
   c) The two most common ranges of packet lengths are 1280-2559 (9875/22510) and 80-159 (5964/22510)
8. a) It appears that traceroute uses MDNS packets
   b) Tcptraceroute, on the other hand, uses ICMP packets.
9. It looks like all of the application data transmitted is encrypted, and can't be sniffed. However, I could clearly read the response in HTML in my command prompt.