Assignment 1

Due 11:59 PM, Feb 2, 2017

Download the ***network_traffic.pcapng*** file, which was captured on one Kali box in the class infrastructure. Based on the network knowledge that you learned from this class so far, analyze the network traffic using Wireshark, and write a one-page report. From the packet capture, what activities can you infer about the users on the class network when the packets were captured? Please explain your answers with evidence you gather from the pcap file. Don't include screen shots. If you need to refer to packets, use the packet number you can observe from Wireshark. Please note that you will see many RDP related traffic which is not interesting, and you do not need to report anything regarding this traffic.

Hint:

1. You can use command such as ***whois*** to figure out who an IP address belongs to
2. Use the sample pcap file available on canvas for practice
3. Using Wireshark's display filtering functions will help you quickly get useful information (Reference to https://www.wireshark.org/docs/wsug_html_chunked/ for details)

   Filter syntax examples:

   ```
   eth.addr == 00:11:11:00:11:15
   ip.addr == 192.168.0.5
   !(ip.addr == 192.168.0.5)
   tcp
   udp
   icmp
   arp
   !(tcp.port == 53)
   tcp.port == 80 || udp.port == 80
   http
   not arp and not (udp.port == 53)
   not (tcp.port == 80) and not (tcp.port == 25) and ip.addr == 192.168.0.5
   ```