IS 430 Virtual Lab Requirements

Purpose: The purpose of the Virtual Lab Assignment is to provide the students with basic information security reconnaissance, monitor and detection techniques that the hacker may employ to utilize to gain access into the network.

1. Pinging
2. IP Address- IP Address, MAC Address, Source, Destination, Time Stamp e.g. ipconfig 10.0.2.15
3. PCAP
4. SSH
5. Trace router –
   1. Tool for displaying the route (path) and measuring transit delays of packets across an IP.
   2. Traceroute is a utility that records the route through the Internet between your computer and a specified destination computer.
   3. It calculates and displays the amount of time each hop took.
6. Launch Wireshark
   1. Captures packets in real time and display them in human-readable format.
   2. You can use Wireshark to inspect a suspicious program’s network traffic, analyze the traffic flow on your network, or troubleshoot network problems.
   3. Wireshark uses colors to help you identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue if UDP traffic, and black identifies packets with errors – for example, they could have been delivered out of order.
7. Host, Kernel and Switch –e.g. h1, h2
8. ICMP Ping
9. TCP (TCP Dump), TCP Ports
10. UDP Characterization
11. SSL. TLS
12. Rootkit Characterization

Delivery: Please provide screen shots of these items of these items as you complete the lab.

The due date at the end of semester.