**Tracy Robinson**

**Wireshark File Analysis Lab.**

TASK: -Analyzing a network traffic- Our security system recorded a connection attempt to our Linux server. You’ve been tasked to analyze this captured traffic and send the answers for the following questions. Please analyze this file and answer the questions.

1)Which Layer3, Layer-4 and Layer-7 protocols have been recorded?

**Layer 2** (ARP) **Layer 3** (ICMPv6) **Layer 4** (TCP) **Layer 7** (Telnet, DNS, SSDP, NTP)

2)What is the number of the packet that 3-way handshake process has been started?

It appears **Packet 5** is when the third ACK message was established by the user after sending request to the target.

3)Which remote connection protocol has been used to make a connection to server? **TELNET**

4)Which TCP port number does this protocol use? **Port 23**

5) What is the disadvantage of this protocol? **Transmits remotes sessions in plaintext and should any unauthorized access or traffic within the network is able to sniff any packets, that data will be easily readable and interpreted.**

\*\*Find the packet that 3-way handshake starts, right click on it, then click on “Follow→ TCP Stream” and answer the following questions.

6)Did the user be able to login this server? **YES**

7)if yes, what is the valid username-password combination? **mmssffaaddmmiinn & msfadmin**

8)Which Linux shell commands did the user run? **Ifconfig, cat etc/passwd, cat etc/shadow, ls --aa**

9)What would you recommend to the administrator of this server? **I would suggest closing Port 23 and only permitting SSH remote sessions that require local login procedures upon a remote request.**

10)What is the IP address of this server? **192.168.146.137**

11)What is the IP address of the user(client)? **192.168.146.130**