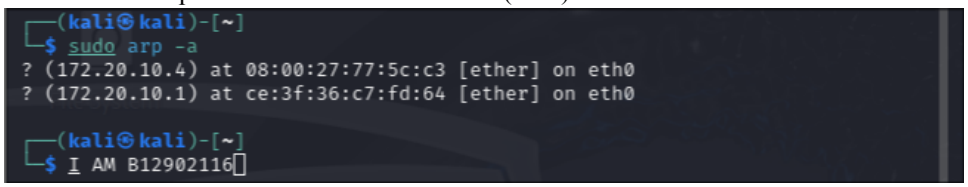
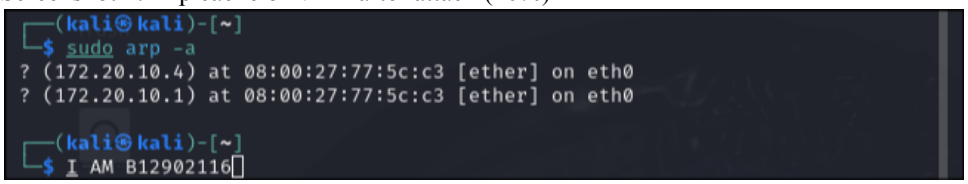
Lab Report

1. Name: 林靖昀 Command prompt ID: Student ID: B12902116

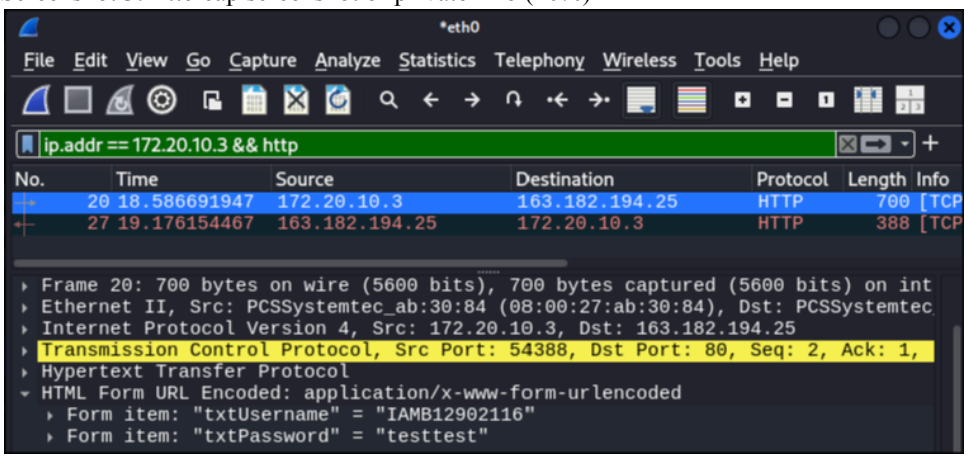
2. Proof of your lab work
   a. Screenshot 1: Arp cache of VM2 before attack (10%)



   b. Screenshot 2: Arp cache of VM2 after attack (10%)



   c. Screenshot 3: Ettercap screenshot of private info (10%)



3. Please specify two methods to protect ARP spoofing and briefly explain how it works. (20%)
   1. Setting static ARP tables manually. Since static ARP tables are not changed by received ARP responses, ARP spoofing can be prevented.
   2. If our hardware supports it, we can enable Dynamic ARP Inspection (DAI). DAI verifies the ARP request and responses against a trusted database, and only allows valid ARP packets through, thus preventing ARP spoofing.

4. Complete following packet challenge:
   - Open AWESOME.pcapng with Wireshark and Answer the following questions :
     i. Who or what is “awesome”? (10%)
        Teja, Tejaisawesome is the hostname of a machine that sent DHCP discovery messages.
     ii. What is the IP address of the DHCP Relay Agent? (10%)
        172.19.134.2
     iii. How many TCP FIN packets are marked as spurious retransmissions? (10%)
        1
     iv. What manufacturer’s products are looking for 169.254.255.255? (10%)
        Apple
     v. How many IP hosts advertise a window scaling factor of 128? (10%)
        88