**Lab 2 – Sniffing, Spoofing and ARP Poisoning (Total: 4 Marks)**

**Due Date – 05/04/2022**

• Follow the instructions in this document.

• Write the answers to the questions in the order they appear in a separate document file

(studentid.docx/.pdf)

• Submit the file using the ECS submission system (i.e., lab2). <https://apps.ecs.vuw.ac.nz/submit/CYBR371>

**Part 1 (1.5 Marks Total)**

Sign in into the NETLAB (https://netlab.ecs.vuw.ac.nz/) with the provided credentials and complete the following labs:

• **Lab: Investigating ARP poisoning**

• **Lab: Capturing Network Traffic**

3. Explain the utility of the following settings/commands used in these labs. Provide clear, concise answers with one example scenario highlighting their significance (0.25 Mark each).

1. Promiscuous mode
2. IP forward field
3. arpwatch
4. urlsnarf
5. tcpdump
6. netstat

**Part 2 (2.5 Marks Total)**

Sign in into the NETLAB (https://netlab.ecs.vuw.ac.nz/) with the provided credentials and complete the following lab:

• **Lab: Packet Crafting with Scapy**

1. Explain the utility of the following settings/commands used in this lab (0.25 Mark each).

a. TTL

b. / Operator (Provide an example)

2. Write the commands in Scapy for the following (0.5 Mark each):

a. Create and send a UDP packet with the payload “CYBR371” with source port of 9000 from the Kali host, and to OWASP BWA host on destination port of 9090. Take a screenshot of the tcpdump capture on the destination, confirming your packet was delivered.

b. Send an ICMP packet from the host (Kali) to the destination (OWASP BWA). Take a screenshot of the tcpdump capture on the destination confirming your ICMP packet was delivered.

c. Sniff UDP traffic on all the interfaces on the host machine (i.e., Kali)

d. Send a spoofed IP packet (with forged source IP address) from the host (Kali) to the destination machine (OWASP BWA) with forged source IP address of 4.3.2.1 . Take a screenshot of the tcpdump capture on the destination proving your message was delivered. Why was the message not dropped in transmission even though the source IP address does not exist?