VICTORIA UNIVERSITY OF WELLINGTON
TE HERENGA WAKA

CYBR371: System and Network Security
2024– T1

Arman Khouzani, Mohammad Nekooei

Lab 2 (4%): Sniffing, Spoofing, and ARP Poisoning

Submission Deadline: ***23:59:00 (NZST) on Sunday, 31 March 2024***

Instructions: Skim through this document quickly (to get an idea what the questions are about). Carry out the following labs on netlab through nuku (under modules):

- Lab: Investigating ARP poisoning
- Lab: Capturing Network Traffic
- Lab: Packet Crafting with Scapy

Answer the questions in the order they appear in this document. Submit your answer document as a single pdf using the ecs submission link (https://apps.ecs.vuw.ac.nz/submit/CYBR371) for Lab2.

1 ARP Poisoning & Network Traffic Capturing

Complete the following labs on netlab (access via Nuku/Modules):

- Lab: Investigating ARP poisoning
- Lab: Capturing Network Traffic

Q 1.1 [18 points] Explain the utility of the following settings/commands used in these labs. Provide clear, concise answers with one example scenario highlighting their significance (60 words max per each answer.) [3 points each]

(a) Promiscuous mode

(b) IP forward field

(c) **`arpwatch`**

(d) **`urlsnarf`**

(e) **`tcpdump`**

(f) **`netstat`**

2 Packet Crafting with Scapy

Go to Nuku of the module and under Modules, complete the following lab:

- Lab: Packet Crafting with Scapy

Then answer the following questions.

Q 2.1 [6 points] Explain the utility of the following settings/commands used in this lab concisely – 100 words max per each entry (3 points per each).

(a) TTL

(b) the `/` Operator (Provide an example)

Q 2.2 [16 points] Write the commands in Scapy for the following. Please make sure your Scapy code matches the requirements in each task. Partially correct answers are not accepted. (4 points each):

(a) Create and send a TCP packet with the payload "CYBER" with source port of 1234 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) Create and send an "ICMP echo" 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 (i.e. capture) ARP traffic on all the interfaces on the host machine (i.e. Kali). Provide a snippet of the screenshot of its output showing it runs as expected.

(d) Create and send a spoofed TCP/IP packet (with forged source IP address) from the host (Kali) to the destination machine, OWASP BWA with forged source IP address of **`3.1.7.0`**. Take a screenshot of the **`tcpdump`** capture on the destination proving your message was delivered. Briefly explain why the message was not dropped in transmission even though the source IP address does not exist.