VICTORIA UNIVERSITY OF WELLINGTON
TE HERENGA WAKA

CYBR371: System and Network Security

2024–T1: Arman Khouzani, Mohammad Nekooei

Assignment 2 (15%): Network Security

Submission Deadline: ***23:59:00 (NZST) on Sunday, 02 June 2024***

- There are two parts for a total of 150 points. Since this assignment has 15% contribution, think of each 10 points contributing 1% to your overall grade.
- you should upload **a single PDF file** (12 pages max in total, excluding references) containing your answers to questions in the order they appear on this document.
- The answer to each question must start on a new page, properly marked showing which question. If you decide to skip a question, you must still label it on your document and leave the answer blank. **Do not include the question statement in your report.**
- For screenshots, do not use a phone to snap a shot, use **`PrintScreen`**!
- Since **`NetLab`** does not allow saving, and is time-limited, it is recommended that you run a Linux VM on your own machine. Just beware: if you are using the lab machines, move your image file to **`/local/scratch/[yourname]`** directory, which saves it to that local machine. This is because you have a limited disk quota on your home directory, and also your VM would run faster.
- Recall that you can ask for help from tutors during lab times. However, never, under any circumstances, share your answers. **There is zero tolerance toward plagiarism.** If you are in doubt what constitutes plagiarism, ask me!

Question:	1	2	3	4	5	6	7	Total
Points:	10	15	15	15	30	15	50	150
Score:								

Part A: Network Attacks and Vulnerabilities

Q.1 [10 points] Write a Scapy script which monitors ICMP requests and replies back with packets simulating a Windows host.

Q.2 [15 points] Write a Scapy script which illustrates the ICMP Teardrop attack. The attack must use 8 packets with overlapping offsets. Include the script in your submission document, explain the code and the fragmented and overlapping bits. You must also illustrate the attack on the receiving end (i.e. target host) using any packet capturing, analysis or detection tools.

Q.3 [15 points] Explain the Xmas Tree attack and write a Scapy script to deploy this attack on a target host.

Q.4 [15 points] (a) Explain the term "Backscatter traffic" and why it is generated by some but not all types of Distributed Denial of Service (DDoS) attacks.

(b) Explain how backscatter traffic can be used to secure a network.

Q.5 [30 points] Demonstrate the DoS amplification attack through two different methods. In partcular, for each method:

(a) Provide a Scapy code that can launch the attack.

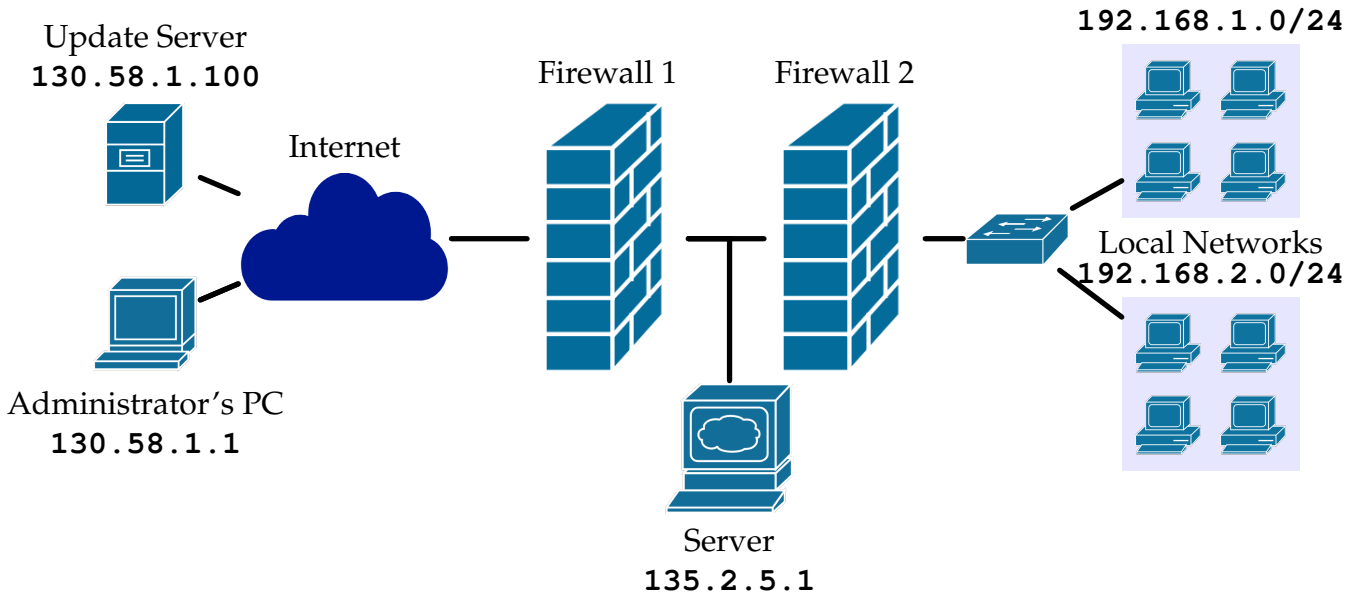
(b) Demonstrate its working by showing what is sent by the attacker and what is received at the target.

(c) Compute the amplification ratio in your practical example.

Firewalls and Intrusion Detection Systems

Q.6 [15 points] Explain the capability and the process (i.e. procedure/steps) by which some firewalls, intrusion prevention systems and honeypots can use the TCP protocol properties such as Window Size and Maximum Segment Size to slow down (NOT stop) the propagation of worms across the networks.

Q.7 As a system/network engineer you have been asked to create a firewall ruleset for a DMZ. The DMZ topology is depicted below:



The server offers the following services and characteristics:

- Operating system: Ubuntu 22.04 LTS
- Server's IP address: **`135.2.5.1/24`**
- Services: **`ICMP`**, **`SSH`**, **`Apache`**, and **`PureFTPd`**

Other Information:

- Clients' networks: **`192.168.1.0/24`**, **`192.168.2.0/24`**
- Update server: **`130.58.1.100`**, Port **`4119`**

Requirements:

A. Provide service for HTTP and HTTPS requests for all clients within the internal and external networks. Drop inbound traffic to port 80 (http) from source ports less than 1024.

B. Protect the server against ICMP ping flooding from external network.

C. Protect the server against UDP Fraggle attacks from anywhere.

D. Provide remote SSH service for administrator from the remote system with an IP address of **`130.58.1.1`**.

E. Protect the server against SSH dictionary attack from anywhere.

F. Protect the server against Xmas Tree attack from external network.

G. Drop all incoming (i.e. inbound) packets from reserved ports **`135`** and **`139`** from anywhere as well as all outbound traffic to these ports.

H. Redirect all the DNS requests from your internal network to Google's **`8.8.4.4`** IP address and associated port.

I. The server is not allowed to create any new outgoing connections to any networks, except to download security updates from the Update Server.

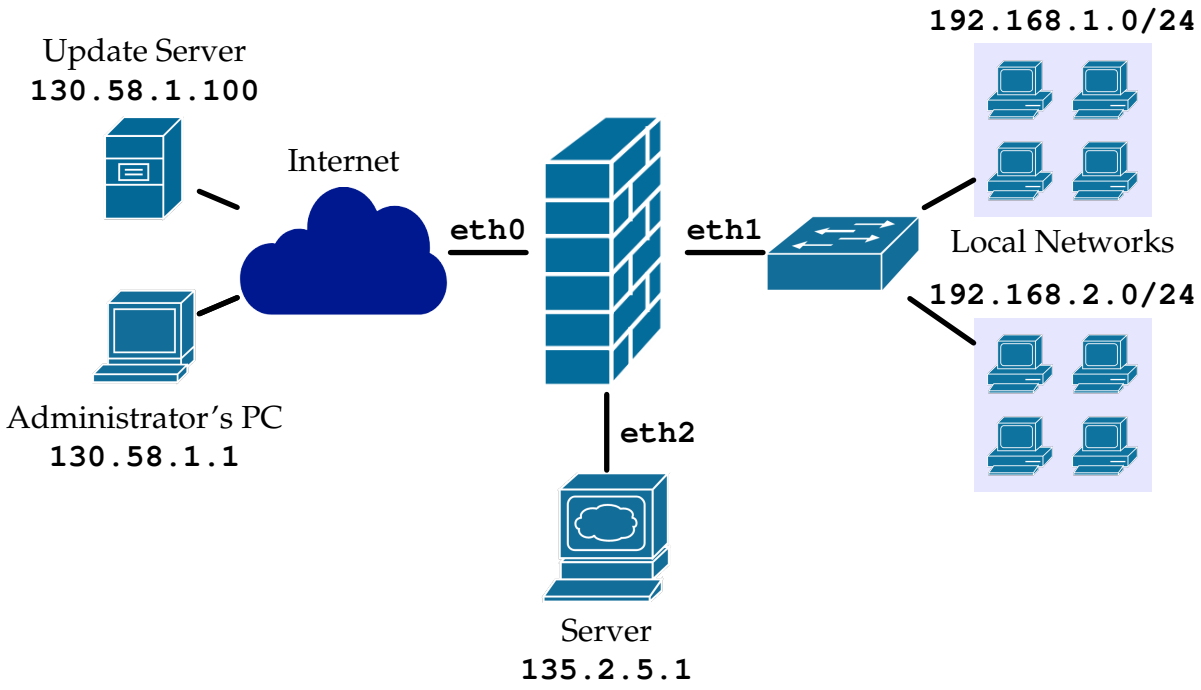
J. There is a new worm outbreak! The worm targets the TCP 8080 or UDP port 4040 and contains the signature "AC 1D 1C C0 FF EE" (hex) follow by "PASS : CYBR371" (ascii) within the first 40 bytes. The worm is coming from external network targeting the server.

(a) [20 points] Create firewall policy tables for "Firewall 1" and "Firewall 2" with the given information. Use the template below (example only). The policies must be complete, specific and, take into account the bidirectional nature of the connections. The rules must filter the traffic accurately, must not cause denial of service to legitimate hosts and must be immune to evasion by attackers. Incomplete policies will not be assigned any marks.

Number	Transport Proto.	Direction	Src. IP/Network	Dest. IP/Network	Src. Port	Dest. Port	Action
1	TCP	OUT	192.168.1.0/24 192.168.2.0/24	135.2.5.1	any	23 (Telnet)	Allow New, Established
	TCP	IN	135.2.5.1	192.168.1.0/24 192.168.2.0/24	23 (Telnet)	any	Allow Established
2							

(b) [15 points] Write the appropriate set of iptables (netfilter) rules to fulfil the requirements for each firewall. The iptables rules must be complete, specific and, take into account the bidirectional nature of the connections. The rules must filter the traffic accurately, must not cause denial of service to legitimate hosts and must be immune to evasion by attackers. The iptables rules must match the order of the policy table rules. Incomplete rules will not be assigned any marks.

(c) [15 points] Suppose instead of two separate firewalls, we use the following (3-legged) DMZ topology instead:



Write the appropriate set of iptables rules that fulfil the same requirements as before.