FIT9137 Assignment 3 Specification

Submission Guidelines details: -

- **Deadline**: Semester-1 Week-14 Friday 2023, [9th June 2023 11:55pm]
- **Marks**: The assignment is marked out of **100** marks and is worth **30%** of your unit marks.
- A report (a PDF file including your screenshots with file name format as FirstName_STUDENT_ID.pdf)
- Your network configuration (the CORE file name format as FirstName_STUDENT_ID.imn) file containing the required changes to complete the assignment tasks.

Brief Description:

Assignment will include the material covered in Weeks 7-10. In particular, the assignment will consist of questions related to network and transport layers, structures and functions of local area, backbone and wide area networks, and network security. The format of the student submission will be a written report and a network configuration. This is an individual assignment. By completing this Assignment, you will understand the learning outcomes 3, 4, & 5.

Notes: Do not submit a compression of multiple files. Such submissions may risk losing partial or complete assignment marks. A handwritten document is **not** acceptable and will **not** be marked even if converted and submitted electronically.

Submission Details:

- Electronic submission via Moodle for the report, and core configuration file. **Two Submission links.**
- Submit a special consideration through available link on Moodle under assessment section to formally request a late submission.
- Without an approved special consideration request, a late submission penalty of **10%** per day deduction will apply. Submissions that are more than **5 days late** will not be accepted, unless special case (SC) consideration is approved.

Plagiarism: This is an individual assignment and group work is prohibited. It is an academic requirement that your submitted work be original. Penalty will be applied to the whole submission if there is any evidence of copying, collaboration, pasting from websites, or copying from textbooks. When asked to use Internet, books, or other academic resources to answer a question, it does not mean to copy the text verbatim from the source. You must write the answers in your own words such that your understanding of the answer is evident. You must always cite your references within the text and list them at the end of the report. Plagiarism policy applies to all assessments, and FIT Integrity committee applies the rules.

Warning: - When you submit the assignment in Moodle, please make sure the submission is not left in the **draft** mode. Before the expiry of the deadline make sure, the submission is made final. If the submission is left in draft mode, it will be deemed as NOT submitted. Also, important Submission check for every student, It is student's responsibility to check if his/her submitted work is markable by our teaching team. It is recommended that every student immediately download your own submitted work (e.g., PDF/imn file, etc) and check if the submission would be downloadable/readable/markable by a tutor. If the teaching team is unable to mark your submission, you may end up losing up to **50% or more** of your marks.

Network Configuration and Security

Introduction

For this assignment you will use the core network emulator to complete a series of tasks on an individual core configuration file that is generated for you. To download your individual core configuration file, open the subject's Moodle page then navigate to the Assessments section and follow the provided instructions for the Assignment 2. The downloaded ***.imn*** file will be in **zip** format, please **unzip** the file to use it.

You must write a report to explain the changes you make and the configuration you add to achieve the goals of each task and your reasons for each change/configuration as well as the tests you perform to check the task is accomplished. Your submitted core file will be marked by running the configuration and testing that the tasks are completed. The report will serve as a reference and maybe checked during marking. However, if a test fails when running your submitted core file, you will receive no mark for that failed test (i.e., part of a task) regardless of your explanations in the report. If tasks are similar, you only need to explain your reasons once, and then just report the changes you make to individual services on each node.

Network Structure

The provided network is Comprised of two organisations labelled **Talos** and **Delos**, a router named **`Internet`** playing the role of the Internet, and a global DNS server named **`clio`**. The internal subnets of Talos are labelled **`Internal`**, and the public servers of the Talos network are placed in a separate subnet named **`DMZ`**. The Internet facing router of the Talos organisation, **`R3`**, is also its network firewall. The Delos network is divided into two subnets: (i) a subnet for the organisation clients and private servers and (ii) a subnet for its public servers. The public servers of Delos are named **`apollo`**, **`artemis`**, and **`demeter`** providing web, domain name, and mail services respectively.

DNS Setup

The core file is configured to resolve the domain names between the two organisations, **`talos.edu`** and **`delos.edu`**. This is achieved through a global DNS server named **`clio`**. The server only resolves the names for the two domains in the configuration (**`talos.edu`** and **`delos.edu`**) by sending the request to the corresponding nameserver for each domain and send back the response to the requesting client. Each DNS server in aforementioned networks must have access to UDP port 53 of the server **`clio`** as the organisation DNS servers resolve the names on behalf of their respective clients. You do not need to make any changes to DNS servers; this section only explains the DNS setup.

Important Notes

- It is recommended to use **tcpdump** if you wish to capture traffic and to observe whether the packets reach their intended destination when trying to accomplish the tasks. To use tcpdump, you can right click on a node and move the mouse to select tcpdump in the provided list and then select the intended interface. You can also run tcpdump from the command line using the command `tcpdump -l - i eth0` to print the summary of the captured packets from `eth0` interface in the terminal. To write the captured packets to a file use the command with `w` option followed by a filename. For instance, running the command `tcpdump -w /home/muni/R3 eth3.pcap - i eth3` on the node `R3` will capture the traffic on its `eth3` interface and store the frames in a file named `R3 eth3.pcap` under `/home/muni` directory. You can then stop the capture with Control+C and use Wireshark to analyse the captured packets.
- Any changes you make to the nodes when the emulation is running will be lost when you stop the emulation. You can test the changes you want to make when the emulation is running and once you have the correct commands then add them through the GUI in the proper service. For example, to add static routes to a router that persist and will be stored with the configuration file, you need to add `ip route add` commands to the `StaticRoute` service of that router.
- If you make changes to a core configuration file and then close the core window without saving the changes, you will not be warned and the changes will be lost, hence if you wish to keep the changes you have made, you must save before closing the core window.
- Make sure to keep a backup of your core file in the shared folder in case you encounter issues with your VM and you need to replace the VM so that you would not lose the work you have done. It is your responsibility to back up your work.
- You must not change the name of any node in the given configuration file.

Tasks

Task A: Routing

[35 +10 = 45 Marks]

The routing tables of the routers in the provided network are not configured. The correct configuration of this task allows any host from any network to reach any other host in the entire network. You must
satisfy the following requirements while completing this task:

1. All hosts inside `talos.edu` network must be reachable from any other host within that network through an *optimal path*. You need to add static routes to routers `R1`, `R2`, `R3`, and `R4` to accomplish

this goal. You must explain your reasons for choosing a path in the report. The notation ***us*** for links represents the propagation delay in ***microseconds***. You can assume that the processing delay is negligible.

2. The router **R3** must be the default gateway of the **talos.edu** network. The router **Internet** must be the default gateway of **R3** and **minerva** (the only router of Delos). You will lose marks if you create routing loops.

Task B: DHCP Server

[8 + 2 = 10 Marks]

The clients of **delos** are configured with static IP addresses. Your task is to:

1. Configure DHCP server on the node **minerva** to assign dynamic IP addresses and other required settings to the client machines in the client's subnet. You can use the DHCP server configuration on **R1** as a reference to follow.
2. Enable DHCP client service on clients of **delos**.

Note: The node **leto** is a private local server in the client's subnet and must have a static IP address as assigned for the given configuration.

Task C: Firewall

[45 Marks]

The node **R3** is the firewall for **talos** network. Configure the Firewall service on this node to satisfy the following requirements:

1. Allow traffic from anywhere to DMZ for the provided service by each server. This must be limited to only the public service that a server provides: **dns** only DNS, **web** only HTTP, **mail** only SMTP.
2. Allow servers in DMZ to initiate a communication if it is required by the service the server provides and only for that service (stateful inspection: DMZ → External).
3. Allow internal hosts to access all services provided by servers in the DMZ (stateful inspection: Internal → DMZ). This includes all services that DMZ servers provide. You can be more permissive here and use address ranges and all IP traffic. All servers in DMZ run SSH service which you can use to test your rules for the internal subnets.
4. Allow internal hosts to reach other internal hosts (if the traffic passes through R3). All traffic is allowed if it is internal to internal.
5. Allow internal nodes to access external servers however packets from external to internal are only allowed if they are responses to communications that were initiated from inside (stateful inspection: Internal → External).

6. Allow the nodes in clients subnet of `talos` to ssh to node `R3` (any host connected to the `R1.eth0` subnet).
7. Allow the node `R3` to send and receive ICMP echo messages to internal nodes and DMZ servers.
8. All other traffic must be dropped (see Notes below).

Important Notes for Task C:

- If the **requirement 8 is not satisfied** you will receive a **zero mark for the firewall task** regardless of any other correct rule you add as it would expose the entire network. You will lose partial marks if your rules are too permissive allowing more traffic than specified to reach the destination for each requirement.
- You only receive marks if the test for each requirement succeeds. No partial marks will be given if only part of a rule is correct. When two rules are required for the incoming and outgoing traffic, no partial marks will be given if one of the rules is correct.
- For stateful inspection the traffic is allowed if it is initiated from the more trusted side of the firewall to the less trusted side. The traffic in the opposite direction, from the less trusted interface to the more trusted interface, is only allowed if the packets are the responses to an initiated communication from the more trusted side. The trust level in the requirements is indicated as **Higher→ Lower** for each stateful inspection, meaning the connection initiation is allowed from the higher level to the lower level and only the responses for the initiated connections are allowed from the lower level to the higher level.
- If you have reachability issues in task A, that is a host is not reachable from another host, you may lose marks in firewall tests as well when the traffic must be allowed. You will not lose any marks for firewall rules if a host is reachable but through a sub-optimal path and the firewall rules are correct.
- You must submit the core file with Firewall service enabled on node `R3`. The service is enabled in the individual files without any rules hence all traffic is allowed.

Reference Notes

Please acknowledge any reference appropriately and also the use of ChatGPT

Generative AI tools are not restricted for this assessment task, ChatGPT use and referencing:

In this assessment, you can use generative artificial intelligence (AI) to assist you in any way. Acknowledging the use of generative artificial intelligence, If you use ChatGPT, then you need to acknowledge the use of ChatGPT (https://chat.openai.com/) to generate materials that may have been used in some form or the other and included within this assessment in a modified form (see Learn HQ)