FIT5037 Network Security Final Assessment
Total Marks 100
Due on Aug 22nd, Friday, 11:55 PM (AEST) - 9:55 PM Beijing Time

1 Overview

The learning objective of this assignment is for you to gain a first-hand experience on designing, implementing, testing and ethically using an enterprise network.
This is an **individual** assignment and **you are not allowed to discuss any aspect of it with others** (excluding teaching team members). Failing this requirement (e.g. helping other students, discussing solutions towards answering assignment questions in any platform) will result in penalties in accordance with the University's Academic Integrity guidelines:
`https://www.monash.edu/students/academic/policies/academic-integrity`

2 Submission Policy

You need to submit video, report and GNS3 files (under multiple Moodle submission links) as described below. Name your files in the format: **[Your Name]-[Student ID]-FIT5037-FA** (followed by file extension such as pdf, mp4, etc).:

- **Main submission:** Under the 'Final Assessment' Moodle submission link, submit
  - One PDF file to describe what you have done and what you have observed with screenshots whenever necessary, and
  - One video file to demonstrate certain tasks.
- **Project Hash:** Create a hash of your GNS project following the below instructions and include it in your report.
  - Compress your GNS3 project directory and create a SHA1 hash of the compressed file using the following three commands (one by one):
    - For Intel CPU VMs

      ```
      cd /home/netadmin/GNS3/projects/
      tar -czvf <ProjectName>.tar.gz <ProjectName>
      sha1sum <ProjectName>.tar.gz
      ```

    - For Apple Silicon VMs

      ```
      cd /opt/gns3/projects/
      tar -czvf <ProjectName>.tar.gz <ProjectName>
      sha1sum <ProjectName>.tar.gz
      ```

    The <ProjectName> phrase above should be replaced by your GNS3 project name. **The hash output must be included in the first page of your report.**
  - Do not delete the <ProjectName>.tar.gz file from your VM as the teaching team may request for this file if a validation of your work is required.

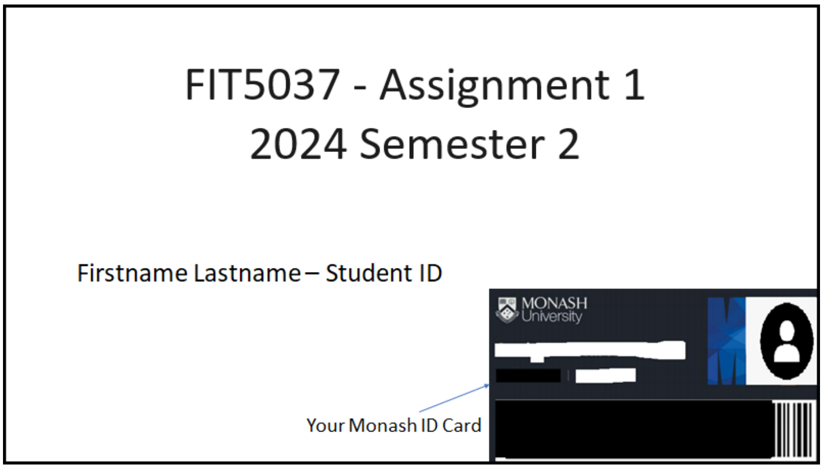
All of your video recordings should be merged into a single video file. For each of the tasks demonstrated in the video, clearly display which question is being solved. For example, when you demonstrate, say, Q1, have a slide before starting the task that contains a statement of the form 'Q1 - <Topic>'. Then, before moving onto Q2, have a slide stating 'Q2 - <Topic>', and so on.

Important notes and penalties

- It is the student's responsibility that the submitted video file can be opened on a standard Windows computer (without requiring specialised software), and that the images, texts and audio included in the video are clearly visible/understandable/readable (in English). If the video file cannot be opened, you will receive zero mark. After making a **draft** submission (**before** finalising it), we recommend you to download your uploaded files and check that they open and run properly. Once you finalise your submission, you will **not** be able to revise it. Note that your video file (together with the report) cannot exceed 500 MB.

- Note that draft files are **NOT** accepted and will not be marked. You must finalise your submission (with status shown as "submitted for grading") for your assignment to be considered as valid. Otherwise, standard late submission penalty will apply.

- At the beginning of your recording, you must clearly show your face and have your photo ID (preferably your Monash ID with photo) presented in the first slide as shown below (please update the slide contents as appropriate). Make sure the ID card details are clearly readable/visible.



FIT5037 - Assignment 1
2024 Semester 2

Firstname Lastname – Student ID

Your Monash ID Card

MONASH University
[redacted]

Figure 1: Sample opening slide. Update it to state 'Final Assessment' instead of 'Assignment 1'.

- A part of the submitted video (at a corner) must clearly show your face at all times. Otherwise, your submission will be deemed invalid and receive zero mark.

- Late submissions incur a 5-point deduction per day. For example, if you submit 2 days and 1 hour late, that incurs 15-point deduction. Submissions more than 7 days late will receive a zero mark.

- If you require **extension or special consideration**, refer to `https://www.monash.edu/students/admin/assessments/extensions-special-consideration`. No teaching team member is allowed to give you extension or special consideration, so please do not reach out to a teaching team member about this. Follow the guidelines in the aforementioned link.

- **The maximum allowed duration for the recorded video is 20 mins.** Therefore, only the first 20:00 mins of your submitted video will be marked. Any exceeding video components will be ignored. Speeding up the video recording (e.g. using a software) is not allowed and such submissions will receive a zero mark.

- If your device does not have a camera (or for whatever reason you can't use your device), you can borrow a device from Monash Connect or Library. It's your responsibility to plan ahead for this. Monash Connect or Library not having available devices for loan at a particular point in time is not a valid excuse.

- You can create multiple video parts at different times, and combine and submit a single video at the end. Make sure that all parts of the final video is clear and understandable.

- All tasks must be live demonstrated instead of explaining an already completed task. You are **not** allowed to add voice-over later on. You are also **not** allowed to read from prepared scripts. At the beginning of each task, please clearly mention what task is being carried out in the video.
- If any task requires installing new software, you are allowed to do that in advance of recording your video. You do not need to demonstrate software installation in the video.
- You can do (online) research in advance, take notes and make use of them during your video recording. You may also prepare Python codes in advance. But you cannot simply copy-paste commands to carry out the tasks without any explanations. Explanations (of what the code does) while completing the tasks are particularly important.
- Zero tolerance on plagiarism and academic integrity violations: If you are found cheating, penalties will apply, e.g., a zero grade for the unit. The demonstration video is also used to detect/avoid plagiarism. University policies can be found at `https://www.monash.edu/students/academic/policies/academic-integrity`.

3 Scenario for the Assignment

You have been hired to design and implement a secure network – containing several servers, firewalls, routers, clients etc. - for Monash University. The network spreads across three campuses: Caulfield, Clayton, and Peninsula. The location of the primary data-center (`Primary DC`) depends on your student ID as follows. StudentID is your Monash student ID number.

StudentID mod 3	Primary DC
0	Caulfield
1	Clayton
2	Peninsula

You will be asked to carry out different tasks depending on the location of the `Primary DC`. **If you solve a question based on an incorrect `Primary DC` value (or any other value computed based on your student ID), you will receive a zero mark (regardless of the correctness of your answer based on a different `Primary DC`).**

4 Secure Network Design and Implementation [12 Marks]

This task entails designing and executing a network that spans across the three Monash campuses, utilizing GNS3. The network's architecture should prioritize security considerations. Your design should establish inter-connectivity between the three campuses leveraging the perimeter firewalls or routers present. While an illustrative example of a topology configuration file has been provided, it remains incomplete. You can use your own network topology if you would like. Mikrotik documentation can be found here: `https://help.mikrotik.com/docs/`. Please use the following command to download the example configuration file:

```
gdown 1RrVCevGYfvSNGwAv75ng_7ylsnQ1dBAD ; sudo bash ./install_Monash.sh
```

Or for Apple Silicon VM, run the following command in GNS3 VM Shell. Instructions on how to access the shell is given in the appendix section of the Apple Silicon lab setup document:

```
gdown 1oGUUx-QfQHDK4-w7mJZ1rCyvA2HPwIMY ; sudo bash ./install_Monash_arm.sh
```

Additionally, there are supplementary network prerequisites that must be addressed.

- All campuses must have at least one perimeter firewall/router.
- All campuses must have a Client LAN, each LAN should contain at least one client container.

- The network must have the following servers: DNS, CA (Certificate Authority), SSH and SMTP.
- DNS and CA are internal servers and WEB, SMTP and SSH are externally accessible servers. **All external servers must be placed in your `Primary DC`**. Internal servers can be placed in any appropriate location.
- Add an Ubuntu container directly to the ISP switch and name it as External-Attacker.
- Assign different subnets to campuses and configure perimeter firewalls/routers.
- For SSH server, open OpenSSH on a regular Ubuntu container.
- For the DNS, WEB and SMTP servers, any open-source server can be installed. Using lab material is also fine. CA can just be a regular container with OpenSSL. Web server should host a web page designed by you **where your student ID is displayed**. DNS can be a forwarding DNS server to Google DNS.
- WEB and SMTP servers should use TLS with certificates issued by the CA. Use your student ID as domain name for both WEB and SMTP servers. E.g., for student ID 111222333, use `111222333.com` as domain name.
- At this stage all devices should be able to reach each other and all services should be active.

Note: If you use the provided GNS3 project most of the above network configurations are already done. However, you may need to add more LANs in your network. Instructions are provided in appendix section on steps to add a new LAN.

Note: It's recommended to go through the Firewall and IDS questions before completing this task.

4.1 Submission Requirement

Video: Video should demonstrate access to DNS, WEB, SMTP and SSH services from a different campus from which the server is hosted. You can use any client side tool to access the services (E.g: Lynx, OpenSSL SClient, dig etc.). Use Wireshark to show that all secure services are encrypted (WEB, SMTP and SSH).

Report: Report should include a screenshot of the network topology (GNS3), IP subnets of any new subnets, IP addresses of all nodes, name of your `Primary DC`. You can mention all these in the GNS3 topology itself and capture them in the screenshot.

5 BGP [10 Marks]

Configure the perimeter firewalls in each campus with BGP routing. Each campus should be a separate BGP AS and all directly connected networks to each firewall should be advertised on BGP. If you are using the provided GNS3 topology, this is already configured. Perform the following tasks on the firewalls:

- Perform a BGP prefix-hijacking attack from any of the firewalls **other than your `Primary DC` firewall**, to redirect the traffic going to the `Primary DC`. Demonstrate the live attack and the live re-direction of the traffic in your video. **(5 marks)**
- Apply a countermeasure to temporally fight back from the victim firewall. Live demonstrate the configurations and the change of the direction of traffic using Wireshark. **(5 marks)**

Note: You have to perform this task before attempting the other tasks to avoid the complications with VPNs and firewall rules. Revert back all changes before proceeding to the next tasks.

5.1 Submission Requirement

Video: Recording of the demonstration of the attack and the fight back.

Report: N/A.

6 VPN [15 Marks]

For this task, your objective is to establish VPN tunnels using IPSec with ESP between the three campuses, forming a mesh network topology. The primary goal is to ensure that all inter-campus traffic is securely protected by these VPN tunnels.

6.1 Submission Requirement

Video: Record a video showing ESP traffic using Wireshark capture on all three paths. You will have to generate some traffic between the campuses to demonstrate this. **(3 marks for each)**

Report: Provide the result of the command "`/ip ipsec installed-sa print`" from all three firewalls in the report. **(2 marks per router for the command result)**

7 Firewall Configuration [18 Marks]

In this task, you will configure firewalls to make the network secure and control access. Here are general requirements **(8 marks)**:

- DNS server should only be accessible from clients from the 3 campuses.
- WEB server should be accessible from all internal and external clients.
- Clients at each site should be able to ping their default gateway (local firewall's IP address).

Additionally, configure the firewall according to one of the options below.

Compute the result of your student ID modulo 4 - e.g., if your student ID is 111222333, then student ID mod 4 = 1. Configure the firewall according to the following options **(8 marks)**:

- If student ID $\bmod 4 = 0$:
  - Restrict access to the SSH server to clients located exclusively within the Caulfield campus and all external clients.
  - Restrict access to the MAIL server to clients located exclusively within the Clayton campus.
- If student ID $\bmod 4 = 1$:
  - Restrict access to the SSH server to clients located exclusively within the Caulfield campus and all external clients.
  - Restrict access to the MAIL server to clients located exclusively within the Peninsula campus.
- If student ID $\bmod 4 = 2$:
  - Restrict access to the SSH server to clients located exclusively within the Peninsula campus and all external clients.
  - Restrict access to the MAIL server to clients located exclusively within the Caulfield campus.
- If student ID $\bmod 4 = 3$:
  - Restrict access to the SSH server to clients located exclusively within the Clayton campus and all external clients.
  - Restrict access to the MAIL server to clients located exclusively within the Peninsula campus.

Note: All firewalls must have implicit deny rules at the bottom of the input, output, and forward chains. Failure to include these will result in your attempt being invalid, leading to zero marks for this section. If any additional firewall rules are needed to ensure the previously configured network infrastructure is functioning properly, they should be added.

Note: When enabling inter-site traffic, firewall rules must be configured on both sites' firewalls, as shown in the example entry in the firewall rule template.

Note: Only the respective service port(s) should be allowed in all firewall rules. E.g: TCP 443/80 for WEB, UDP 53 for DNS etc. All firewall rules should be restricted with source IP, destination IP, destination port, source interface, destination interface.

7.1 Submission Requirement

Video: Record a video demonstrating that the firewall rules are functioning as expected. Begin by attempting to connect to the service from a node where access is allowed, followed by a connection attempt from a node where access is restricted. Briefly showcase all relevant firewall rules during the demonstration. Ensure the firewall rules align with the screenshots and the rule table included in the report.

Report: Provide a screenshot of the firewall rules of each firewall. You can use the command "`/ip firewall filter print`". Document all firewall rules in the provided rule template and add it to the report. **(2 marks)**

8 Security Analysis [12 Marks]

Perform a security analysis of the network that you configured in the previous tasks. More specifically, discuss the following in the report (no actual configuration is required for these questions, please limit your answer to under 400 words):

- Can the firewall configuration be bypassed? **(6 Marks)**
  - If so, explain how it can be bypassed and how to counter it?
  - If not, explain what rules are in effect to prevent bypassing?
- Discuss how the security of the network (including the servers) you have constructed be further improved. Your discussion can also include removing/adding servers and network devices. Y **(6 Marks)**

Note: No video demonstration is required for this task.

9 IDS [15 Marks]

In this task, you are required to exploit an internal server as an external attacker and configure IDS to detect and alert on these intrusion attempts. Perform the following tasks:

- Configure a Snort IDS node to the same network where your public servers (WEB, SSH and SMTP) are connected. Configure the switch to send all traffic in/out from the public servers to the IDS, similar to our approach in the IDS lab. **(4 Marks)**
- Perform TCP port scan on the SSH server from a external attacker node which is outside Monash network. You can use any type of scan here. The External Attacker can be connected to the ISP switch. Create custom rules in the IDS to generate alerts in response to the above attempts. **(5 Marks)**
- Perform a Denial of Service (DoS) attack on the Web server from a external attacker node which is outside Monash network. You can use any type of attack here (ex: SYN flooding). Create custom rules in the IDS to generate alerts in response to the above attempts **(5 Marks)**

Note: Configurations without demonstration are not sufficient to receive any marks.

Note: IDS rules must be customized to detect only the specific attack/scan while ignoring legitimate traffic.

9.1 Submission Requirement

Video: Demonstrate in the video a live exploitation of the scan and the attack and the IDS detection alerts. Briefly explain the logic behind the IDS rules, emphasizing how it alerts only for malicious traffic while ignoring legitimate traffic.

Report: Provide the IDS rule configuration in the report. **(1 Mark)**

10 Ethical Conduct [8 Marks]

With all suggested security improvements from Task 8, identify unethical activities a network user (staff or a student) can perform in the above network. Develop an Ethical Network Usage policy with a list of guidelines to Monash staff and students regarding appropriate network conduct, prohibited activities, and behaviors classified as unethical. List a minimum of 4 policy directives. Ensure your response falls within the 150 to 300 word limit. All directives must be related to the specified network, and failure to comply will result in significant penalties. For this task, you are allowed to conduct some research, and appropriately cite and acknowledge the resources you have consulted.

11 Quality of Presentation [10 Marks]

The remaining 10 marks are allocated to the quality and clarity of presentation in the report (5 marks) and the video (5 marks).

Appendix

A Steps to add additional LAN to a campus

- Add a switch and connect it to a vacant port in the campus router/firewall.
- Decide the IP subnet for the new network. If you are using the provided GNS3 project, only increment the third octet of the corp LAN IP. E.g: New subnet for Clayton campus could be 10.200.20.0/24, 10.200.30.0/24 etc. For Peninsula campus it could be 10.201.20.0/24, 10.201.30.0/24 etc.
- Login to the firewall and assign an IP address to the firewall port connected to the new switch. This will the default gateway IP for your clients in this LAN. E.g:

  ```
  /ip address add address=10.200.20.1/24 network=10.200.20.0 interface=ether3
  ```

- In the firewall configure a DHCP server for the new subnet. If you are using statically assigned IP for your clients, this step is optional.