FIT3031 Network Security Final Assessment
Total Marks 100
Due on Nov 7th, Friday, 11:55 PM

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 the video and the report (under the Moodle submission link) as described below. Name your files in the format: **[Your Name]-[Student ID]-FIT3031-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):

```
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 virtual machine until the final grades are released, as the teaching team may request this file for validation of your work.

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, you can include a slide or add text directly to the video that contains a statement in the form of 'Q1 - <Topic>'.

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.

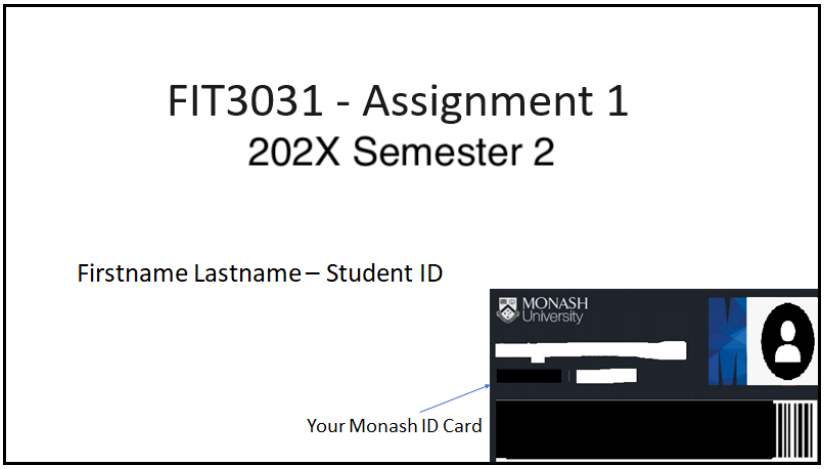

Figure 1: Sample opening slide. Update it to state 'Final Assessment' instead of 'Assignment 1'.

- 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 will incur a **5-point** deduction per day. For example, submitting **2 days and 1 hour** late will result in a **15-point** deduction. Submissions more than **7 days** late will receive a zero mark. The late submission penalty is applied automatically. For more details, please refer to this link.
- Make sure to allow enough time for exporting and uploading your video before the deadline. Long export or upload times cannot be accepted as a reason for waiving a late submission penalty.
- If you require **extension or special consideration**, refer to this link. 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.
- Make sure that your video is clear and fully markable. Blurry, unreadable, or inaudible videos will receive zero marks, as assessors must be able to evaluate your work properly.
- The maximum video file size allowed for upload on Moodle is 500 MB. If your video exceeds this limit, you can use a free video compression tool to reduce its size (ex: ffmpeg). After compression, make sure the video retains its full length and that the visual quality is not blurred.

- 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

Assume you are a network security engineer, and 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. Divide your student ID by 3 and use the remainder (0, 1, or 2) to identify your assigned data center.

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 [18 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 run the following command to download the example configuration file. To log in to the firewalls, use the username **admin** and leave the password field blank (no password):

```
gdown 1b3obWVb1L9kcOztDuAe-CjG_Csmt1Sx7 ; sudo bash ./install_Monash.sh
```

Alternatively, you can use the link below to download the same project. However, if you are connected to the **Monash Wi-Fi**, this method may not work. In that case, please use a mobile hotspot. (single command)

```
wget https://sniffnrun.com/install_Monash.sh --no-check-certificate ; \
sudo bash ./install_Monash.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, Web and SMTP.
- DNS and CA are internal servers and WEB and SMTP are externally accessible servers. SSH server is only accessible for the Remote Access VPN users. **All external servers must be placed in your `Primary DC`**. Other servers can be placed in any appropriate location.
- Add two Ubuntu-24.04-plus-essentials containers directly to the ISP switch and name them as External-Attacker and External-Client.
- 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 server 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.
- SMTP server should be enforcing encryption for both Client-to-Server and Server-to-Server communications with either STARTTLS/SMTP or SMTPS.
- 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.

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/script 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). You are also allowed to use any scripts used in the labs.

Report: Report should include a screenshot of the network topology (GNS3), IP subnets (network address and the subnet mask) 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 [22 Marks]

6.1 Site-to-Site VPNs

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.

6.2 Remote Access VPNs

For this task, create a Remote Access IPsec VPN on the Primary DC so remote workers can securely access internal services. Configure the external client to route all traffic destined for the Primary DC's internal subnet through the VPN, and ensure all other traffic bypasses the VPN. (i.e., enable split tunneling so only Primary-DC–bound traffic uses the remote VPN).

6.3 Submission Requirement

Video: Record a video showing ESP traffic using Wireshark capture on **all three site-to-site tunnels**. You will have to generate some traffic between the campuses to demonstrate this. **(4 marks for each)**
Video: Record a video that demonstrates ESP traffic in Wireshark while accessing an internal service on the Primary DC over the Remote Access VPN. Also show that traffic not destined for the Primary DC is not routed through the VPN (i.e., remains outside the tunnel). **(8 marks)**

Report: Provide the result of the command "`/ip ipsec installed-sa print`" from all three firewalls in the report. **(0.5 marks per router for the command result)**
Report: Show the External-Client's VPN configurations on the report. **(0.5 marks)**

7 Firewall Configuration [18 Marks]

In this task, you will configure firewalls to make the network secure and control access. Here are general requirements **(12 marks)**:

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

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

Compute the result of your student ID modulo 3 - e.g., if your student ID is 111222333, then student ID mod $3 = 0$. Configure the firewall according to the following options **(3 marks)**:

- If student ID $\bmod 3 = 0$:
  - The SMTP server must be accessible to users on the Clayton campus and to the external users. SMTP should not be accessible via the remote access VPN.
- If student ID $\bmod 3 = 1$:
  - The SMTP server must be accessible to users on the Peninsula campus and to the external users. SMTP should not be accessible via the remote access VPN.

- If student ID $\bmod 3 = 2$:
  - The SMTP server must be accessible to users on the Caulfield campus and to the external users. SMTP should not be accessible via the remote access VPN.

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.

Note: If any additional firewall rules are needed to ensure the previously configured network infrastructure is functioning properly, they should be added (ex: VPN tunnels, Remote Access VPN etc.). Failure to comply will result in a penalty of up to **8 marks**.

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. **(3 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 1000 words):

- Can the firewall configuration be bypassed? **(4 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 its servers) you have built can be further improved. You may propose new security devices, services and security controls beyond those taught in the unit. For each suggestion, explain clearly and specifically: what the control is, where and how it would be integrated into your network topology, and exactly how it strengthens the infrastructure. General answers not related to your network will be considered invalid. **(8 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 an 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. You may use any already available tool or write a custom Python script to perform the attack. **(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 Quality of Presentation [5 Marks]

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

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.