FIT5037 Network Security Final Assignment
Total Marks 100
Due on Oct 27th, 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 a corporate network.

2 Submission Policy

Create a detailed PDF document with task descriptions and relevant screenshots. Upload the GNS3 configuration file to Google Drive and link it in the PDF. Additionally, embed video links in the PDF document. **Your final submission should include a well-organized PDF with project details, screenshots, GNS3 configuration file link, and video references for a comprehensive overview.** Name your file in the format: **[Your Name]-[Student ID]-FIT5037-Assignment**.

If a demonstration video is required, you should record your screen demonstration with your voice explanation and upload the video to your Monash Google Drive. **For video demonstration, please keep it to maximum of 20 minutes in total duration; you are required to say your name and student ID at the start of recording, showing face is mandatory.** The shared URL of the video should be mentioned in your report wherever required. You can use any tool you would like to record videos, for example panopto (`https://monash-panopto.aarnet.edu.au/`) and Zoom.

Late submission penalty: 10-point deduction per day. If you require a special consideration, the application should be submitted and notified at least three days in advance. Zero tolerance on plagiarism: If you are found cheating, penalties will be applied, i.e., a zero grade for the unit. The demonstration video is also used to detect/avoid plagiarism. University polices 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.

4 Secure Network Design and Implementation [20 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 interconnectivity 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 toplogy 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:

```
curl -s https://cloudstor.aarnet.edu.au/plus/s/izZw6ZlAsEMfPoL/download | sudo bash
```

Additionally, there are supplementary network prerequisites that must be addressed **(10 marks for completing the following topology)**:

- 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), FTP, SSH, WEB, MAIL and VPN (this is for external clients connecting to Monash VPN). Servers can be placed in any campus(es). It's assumed that the network is connected to the internet (can be shown using cloud in GNS3).

- Assign different subnets to campuses and configure perimeter firewalls/routers.
- For the DNS, FTP, SSH, WEB and MAIL servers, any open-source servers can be installed. Using lab material is also fine. CA can just be a normal container. Installation/Configuration of VPN server is not required, a normal container can be used for this as well, you can assume that it's a SSL VPN (port 443).
- WEB and MAIL servers should use TLS with certificates issued by the CA. Use your student ID as domain name for both WEB and MAIL servers. E.g., for student ID 111222333, use 111222333.com as domain name. MAIL server should have at least two email recipients configured. It's assumed that the client containers have CA's certificate installed.
- At this stage all devices should be able to reach each other. All services (DNS, SSH etc.) should be active, e.g., doing nslookup 111222333.com from a client container should return the IP address of the web server; and visiting https://111222333.com from a client container should show the test web page designed by you.

Record a video showing the network and explaining the design. The video must show the following **(10 marks for testing)**:

- Perform a ping test from one campus to the other, e.g., ping from the client in the Clayton to the Peninsula, and from Peninsula to the Caulfield campus.
- For FTP, SSH, WEB and MAIL services, connect the service from one of the clients and show the connectivity.
- For TLS connection, show Wireshark capture.
- For the DNS server, perform a nslookup to the domain created in above steps from one of the clients.

Provide the screenshot of the network topology (GNS3) and routing table of the routers/firewalls in the report.

5 VPN [15 Marks]

For this task, your objective is to establish VPN tunnels using IPSec with ESP between the campuses. This is site-to-site VPN, each perimeter router will have two tunnels. For example, Caulfield perimeter router will have a VPN tunnel with Peninsula router and a tunnel with Clayton campus router. The primary goal is to ensure that all inter-campus traffic is securely protected by these VPN tunnels. **(Note: this setup is not related withe VPN server which is just a container)**

Record a video showing ESP traffic using Wireshark capture on all paths. **(3 marks for each capture)**

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)**

6 Firewall Configuration [18 Marks]

In this task you will configure firewalls to make the network secure and control access. Here are general requirements **(2 marks each rule)**:

- WEB, MAIL, and VPN servers should be accessible to everyone, including the clients on the internet.
- WEB and VPN servers cannot initiate a connection to the internal network, they can only reply to the connection requests from the clients.
- The DNS server should only be accessible to all internal clients (no external/internet clients)

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

Perform student ID modulo 4 - e.g., if your student ID is 111222333, 111222333mod4=1. Configure the firewall according to the following options **(4 marks each rule)**:

- If studentIDmod4=0:

  - Restrict access to the FTP server to clients located exclusively within the Clayton campus.
  - Restrict access to the SSH server to clients located exclusively within the Caulfield campus.
  - Restrict access to the MAIL server to clients located exclusively within the Peninsula campus.

- If studentIDmod4=1:
  - Restrict access to the MAIL server to clients located exclusively within the Clayton campus.
  - Restrict access to the SSH server to clients located exclusively within the Caulfield campus.
  - Restrict access to the FTP server to clients located exclusively within the Peninsula campus.

- If studentIDmod4=2:
  - Restrict access to the MAIL server to clients located exclusively within the Clayton campus.
  - Restrict access to the FTP server to clients located exclusively within the Caulfield campus.
  - Restrict access to the SSH server to clients located exclusively within the Peninsula campus.

- If studentIDmod4=3:
  - Restrict access to the SSH server to clients located exclusively within the Clayton campus.
  - Restrict access to the MAIL server to clients located exclusively within the Caulfield campus.
  - Restrict access to the FTP server to clients located exclusively within the Peninsula campus.

Record a video proving that the firewall rules work. First try connecting the service from a node where it was permissible and then from a node where it was not allowed. Provide the firewall rules, from each firewall, in the report.

7 Security Analysis [12 Marks]

Perform a security analysis of the network and firewall configuration you have performed in the previous task. More specifically, discuss the following (no actual configuration is required for these questions, please limit your answer to under 100 words):

- Can the firewall configuration be bypassed? If so, how do we counter it? Provide new firewall rules if the rules need to be changed. **(4 Marks)**
- Does this network, or individual servers, need other security solutions? If so, which ones and where/how do we implement them? **(4 Marks)**
- Any general security recommendations? It can also include removing/adding servers or network devices. **(4 Marks)**

8 IDS [15 Marks]

Employ the Metasploitable Docker environment, similar to our approach in the IDS lab, to set up and incorporate the Snort IDS (or an alternative IDS of your preference). Perform the following two tasks:

- Exploit a vulnerability in Metasploitable Docker using Metasploit, capture the traffic in Wireshark and discuss how an IDS rule can be made to detect the usage of Metasploit tool. **(5 Marks)**
- Configure this IDS to generate alerts in response to any attempts by attackers to exploit vulnerabilities within the Metasploitable Docker. Specifically, the IDS configuration should encompass the detection of the exploitation tool Metasploit. Perform exploitation on two of the services in Metasploitable Docker and show the IDS detection. **(10 Marks)**

Provide the IDS rule configuration in the report. Demonstrate in the video a live exploitation of the vulnerabilities in Metasploitable and the IDS results.

9 Ethical Conduct [10 Marks]

Developing an Ethical Network Usage Policy is essential. Your task is to communicate guidelines to Monash staff and students regarding appropriate network conduct, prohibited activities, and behaviors classified as unethical. List a minimum of five policy directives. Kindly ensure your response falls within the 150 to 500 word limit.