Assignment 1 – IT Forensics 2023

Submission instructions

Deadline: Friday, 18 August 2023 (11:55pm)

Submission format: One PDF file of your report and only one drawio file. You can use any freely available PDF converter to make a PDF file from an editable one. Your report should not exceed 1,000 words excluding tables, figures, and references. Exceeding this limit may incur penalty. Write your report like if you want to present to the CEO of the company in the assignment specification.

Referencing format: APA 6th is the recommended style in the Faculty of Information Technology. Please see:
https://www.monash.edu/it/current-students/resources-and-support/style-guide/referencing

Submission platform: There are two links to submit your assignment. Upload your report (pdf file) via Turnitin assignment link on Moodle. There is a separate link to upload your network design (drawio file) as well. It is your primary responsibility to ensure you have submitted your files correctly. The submitted files should be markable by tutors, if not, you may lose upto 50% your marks depending on when your tutors would notice this. Not markable files include PDF file which cannot be opened/read by your tutor or empty drawio file.

Late submissions:

- via special consideration request
- or, without a special consideration request, you lose 10% of your mark per day that you submit late. Submissions will not be accepted more than 5 days late.

Plagiarism: It is an academic requirement that your submitted work be original.

Zero marks will be awarded for the whole submission if there is any evidence of copying, collaboration, pasting from websites, or copying from textbooks. The faculty's Plagiarism Policy applies to all assessments:
http://intranet.monash.edu.au/infotech/resources/students/assignments/polic ies.html

When you are asked to use Internet resources to answer a question, this does not mean copy-pasting text from websites. Write answers in your own words with proper referencing to the original source such that your understanding of the answer is evident.

Covered Learning Outcomes:

- explain the motivations and landscape of forensic investigations in an IT context;
- explain the relevant legal definitions and frameworks that apply to digital forensic investigations;

Marks:

- This assignment is worth **10% of your unit marks**.
- The assignment is marked out of **100 nominal marks**.

Network Layout: An empty network layout is accessible at:
https://drive.google.com/file/d/1w1LHGBGlvYQVDfiOMUCEkGxjj7o463Cr/view?usp=sharing

You have to only use https://app.diagrams.net/ and make changes using the available legends in the above empty layout.

ENTERPRISE FORENSIC READINESS

The CEO of a consulting IT company has asked you to design the company's network. She has asked you to be prepared as much as possible for the next 10 years in terms of IT equipments and being prepared for forensic investigations and cyber attacks. The company's infrastructure is to stay like what you have designed for the next 10 years. The company has one headquarter and it has X-1 branch offices in different cities, some national and some international ones. The number X that is representing the total number of branches (including headquarters) depends on your student ID. The main office and each branch has exactly 40 employees. Each employee is exactly equipped with one single workstation. You may also have a working from home (WFH) option for employees in your diagram (based on your student ID).

How to choose X: Calculate your student ID modulo 6 plus 1, the result is X. Example student ID: 1234567 and

$X = (1234567 \bmod 6) + 1 = 1 + 1 = 2.$

The student with ID 1234567 should work with a company network that consists of X=2 branches, that is one headquarter and X-1=1 branches[1]. Each of these X branches can accommodate exactly 40 workstations each of which is allocated to exactly one employee.

How to see if the CEO has allowed WFH or not: If your student ID is an even number, the CEO would not allow WFH. If your student ID is an odd number, she has allowed WFH.

You have to use the empty layout given to you and add more branches to it and integrate by yourself. The following servers of the company are to be located in a proper place.

1. Database server (inaccessible to public)
2. Application/web server (public)
3. File server (inaccessible to public)
4. Email server (inaccessible to public)

Based on your specific X you have to design a network diagram by using only various options given in the legend of the empty diagram and answer questions 1-4 below.

In all the below steps, when you are deciding about your choices and justifying them,

- Consider the size of your network. A network is small if it has less than 50 workstations and it is considered large if it has more than 50 workstations.
- Discuss how you would implement forensic readiness into the mentioned mechanisms. You can refer to ISO/IEC 27043:2015. Please refer to Moodle Week 3 for a copy of this document.

[1] If X=1, no branch but you still have headquarter.

1) Server Farm Location, WAN connections, and Internet connection (3 options)

You have to decide where to put the server farm. First, decide about the location of the company's server farm. You have four different options: in the main office, on the cloud, in the data center, or a hybrid choice (data center + cloud). You can use the icons in the legend to put the servers in the desired location. Second, decide about the WAN connection and draw the connections in your diagram (including the routers) between the headquarter, branches, and the location of the server farm (based on the legend, you have two choices for WAN connections, MPLS or Internet). Finally, decide about the Internet connection to your company/server farm, which has been shown as a red cloud in the empty diagram. Justify your choices in all these steps according to your network size and forensic readiness.

Note: The difference between "Cloud" and "Data Center" for us is that a cloud is public but a data centre is owned by the company and can act as a private cloud. In fact, A public cloud for a company is a cloud that is not owned by the company itself. It is owned by a third party. In contrast, a private cloud (a data centre) is something that the company can build for itself, own and manage forever.

((2+4)*2=12 marks)

2) AAA server location, SIEM server location, VPN, SSL Terminator, and Firewall (3 options)

Now, you have a complete diagram with all connections and the company's servers' location specified. First, decide about the location of AAA (authentication, authorization, and accounting) Server and SIEM (Security information and event management) Server. Second, use Firewall, VPN, and SSL terminator, if needed, to provide security. Justify all your 5 choices based on your network size and forensic readiness. For the tools that need a start and endpoint like VPN, use the tool for the start and endpoint, and determine these by numbers, e.g., one VPN connection has a start point of VPN**1** and endpoint of VPN**1'**.

((2+4)*5=30 marks)

3) Enterprise Defence System (6 options)

Develop a more detailed cyber system defence mechanism for the enterprise considering all 6 tools: Web Application Firewall (WAF), Web filtering, Malware filtering, SSL inspection, IDS/IPS, and Email security.

Their icons have been given in the legend. Use the icons to complete your diagram, some of them can be enabled on the firewall, mention each of them you use by using the icon. Based on your design, you may not use all the tools listed in the legend of your network, though. If you decide to use any of these, specify its location and justify your choice according to the size of your network and forensic readiness. If you decide not to use any of these, explain why you have not used it.

((2+5)*6=42 marks)

4) Cost Estimation and Justification

Based on your design, estimate the cost to implement the defence system and maintain the system for 10 years. Break down the tasks and put references whenever necessary if you are referring to any specific product or service. Your cost estimates should be proportionate to the size of your network.

(10 marks)

5) Structure, Look, and Referencing

5 marks are allocated to the report structure (2 marks), look (2 marks) and proper referencing (1 mark). Keep in mind you are preparing the report for your CEO not the teaching team.

(5 marks)