MONASH University

FACULTY OF INFORMATION TECHNOLOGY

FIT1047 Introduction to computer systems, networks and security – S2 2024

Assignment 4 – Cybersecurity

Purpose	For the first part (Part 2a), students will use a specific generative AI tool to analyse and discuss a recent vulnerability or a cybersecurity attack. This demonstrates an understanding of related cybersecurity topics and the ability to research information on cybersecurity incidents. For the second part (Part 2b), students need to show how a given set of security controls are used in a medium-sized enterprise scenario. This demonstrates an understanding of the different security controls and the ability to assess and explain their use. The assignment relates to Unit Learning Outcomes 5, 6, and 7.
Your task	Part 1: Your weekly reflection (week 10, 11 and 12) Part 2a: You need to choose one article from your allocated category, then use a specific generative AI tool to analyse and discuss this recent vulnerability or cybersecurity attack. You also need to use your judgement to justify whether the generative AI gives the correct and accurate analysis, and identify the gap that is missing from the analysis. You need to prepare a report and a video presentation with slides to explain your justification. Part 2b: You need to prepare a video presentation with slides that shows how a given set of security controls are used in a medium-sized enterprise scenario. The instructions below contain concrete questions you should answer in your report and presentation. All files have to be submitted via Moodle.
Value	**30%** of your total marks for the unit Parts 2a and 2b are 15% of the total marks for the unit each.
Word Limit	Part 1: ● At least 100 words per week Part 2a: ● A report with at least 1000 words ● A presentation video (max 7 minutes) along with slides (max 15 slides) Part 2b: ● A presentation video (max 7 minutes) along with slides (max 15 slides)

Due Date	**Monday, October 28, 11:55 PM**
Submission	• Via Moodle Assignment Submission. **Part 1:** 1. One pdf file for your weekly reflection **Part 2a:** 2. One pdf file for your report 3. One pdf file for your slides 4. One video file for your presentation **Part 2b:** 5. One pdf file for your slides 6. One video file for your presentation **Total: 4 pdf files and 2 video files.** You should clearly indicate the part that the file refers to, e.g. using appropriate file names such as `Part2a_Report.pdf`, `Part2a_Slides.pdf` etc. • Turnitin will be used for similarity checking of all submissions. • ***Generative AI tools are not restricted for this assessment task (except Part 1 in which Generative AI tools cannot be used)*** *In this assessment, you can use generative artificial intelligence (AI) to assist you in any way. Any use of generative AI* ***MUST be appropriately acknowledged****.*
Assessment Criteria	See rubric in Moodle Assessment submission page
Late Penalties	• 5% deduction per calendar day or part thereof for up to one week • Submissions more than 7 calendar days after the due date will receive a mark of zero (0) and no assessment feedback will be provided.
Support Resources	See Moodle Assessment page
Feedback	Feedback will be provided on student work via: general cohort performance specific student feedback ten working days post submission

INSTRUCTIONS

Part 1: Reflection (Hurdle - you MUST submit it in order to pass this assignment!)

Complete your reflection activities in **Week 10 to Week 12** Ed Lesson and copy/paste them into a pdf file. **Each week the reflection must have at least 100 words** (relevant and meaningful to the specific week).

Failure to submit all relevant week's reflections (missing all submissions or incomplete submissions) will result in your assignment 1 having a maximum mark of 49% only. For example, if the overall combined mark is 61/100, it will be scaled to 49/100. If the overall combined mark is 44/100 then it will remain as 44/100.

You may use this template: https://docs.google.com/document/d/18UIEJQeyarYW1pl8oDEaf--ubCdJ5LDf-9_jSLbGxrE/edit?usp=sharing to write down your reflection.

Submit your reflection for this part (Part 1) as a PDF file in Moodle.

Part 2a - Analyse a cybersecurity vulnerability or incident (upload 2 pdf files and 1 video file to Moodle) [30 marks]

Information on security problems, weaknesses and attacks can be found in many places (blogs, newsletters, experts' pages, etc.). Your task is to pick **one item only** from your allocation group, read the news item, look up and read the referenced sources, and finally **write a report** and **record a video presentation** on the findings.

- **Students with student number ending with "1" and "6": Data Breach**

1) Bank of America (updated 13/02/2024): https://www.americanbanker.com/news/data-breach-affects-57-000-bank-of-america-accounts
2) Giant Tiger (updated 13/04/2024): https://www.bleepingcomputer.com/news/security/hacker-claims-giant-tiger-data-breach-leaks-28m-records-online/
3) Dropbox (updated 01/05/2024): https://sign.dropbox.com/blog/a-recent-security-incident-involving-dropbox-sign

- **Students with student number ending with “2” and “7”: Software Security**

4) Github (updated 24/04/2024): https://www.bitdefender.com.au/blog/hotforsecurity/github-flaw-could-allow-threat-actors-to-distribute-malware-on-gitlab/
5) Palo Alto Networks (updated 13/04/2024): https://thehackernews.com/2024/04/hackers-deploy-python-backdoor-in-palo.html
6) Xiaomi Android Devices (update 06/05/2024): https://cybersecuritynews.com/multiple-xiaomi-android-devices-flaw/

- **Students with student number ending with “3” and 8”: Network Security**

7) CISCO VPN (update 24/04/2024) https://www.cyber.gc.ca/en/news-events/cyber-activity-impacting-cisco-asa-vpns
8) Railway (update 31/01/2024) https://blog.railway.app/p/2024-01-31-incident-report
9) New Mexico Highlands University (updated 11/04/2024) https://therecord.media/ransomware-new-mexico-highlands-east-central-oklahoma-universities

- **Students with student number ending with “4” and “9”: Human Behaviour Security**

10) Romance Scams (update 13/02/2024) https://www.commbank.com.au/articles/newsroom/2024/02/romance-scams-around-valentines-day.html
11) Deepfake (update 04/02/2024) https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
12) MGM Resort (update 14/03/2024) https://specopssoft.com/blog/mgm-resorts-service-desk-hack/?utm_source=thehackernews.com&utm_medium=referral&utm_campaign=na_thehackernews&utm_content=guest-post

- **Students with student number ending with “5” and “0”: AI Security**

13) Microsoft AI Security Flaw (update 28/06/2024) https://www.pymnts.com/artificial-intelligence-2/2024/microsoft-reveals-ai-security-flaw-that-threatens-ecommerce-and-financial-services/
14) SAP AI Core Vulnerabilities (update 18/07/2024) https://thehackernews.com/2024/07/sap-ai-core-vulnerabilities-expose.html
15) NVIDIA AI Toolkit Vulnerability (update 27/09/2024) https://www.trendmicro.com/en_au/research/24/i/nvidia-ai-container-toolkit-vulnerability-fix.html

Follow the steps to write your report:

1. Choose **<u>one of the 3 news items</u>** in your allocated group above, read the text.
2. Look up and read the articles and information referenced in the news item.

Use ChatGPT (refer to the Appendix on how to use ChatGPT) to generate a report, containing the following information:

- A short abstract of the news item (***less than*** 200 words).
- Identify which software, hardware or system is affected. The identification should be as precise as possible. Include exact product names, distribution of the product, version numbers, etc. (around 100 words)
- Describe how the problem was discovered and how it was initially published. Try to find this information in the referenced articles. The problem might have been found by researchers at a university, by a professional security company, by some hacker, published in a scientific conference/journal, in a newspaper on a blog, etc. Was it the result of targeted research, found by chance, were any tools used, etc? (around 200 words)
- Discuss how serious the issue/weakness/attack is, describe what is necessary to exploit the weakness, evaluate what the consequences might be if it is exploited, and what reactions or mitigations you think are necessary/useful on (i) a technical level, (ii) in terms of human behaviour, and (iii) on a policy level (around 500 words).

3. Edit the above report generated by ChatGPT to
    a. modify the part(s) that you think ChatGPT is not correct, not accurate or not adequate. You can use your own judgement or knowledge learnt from this unit to make this modification.
    b. add at least 4 more references excluding the original article reference, (e.g. other related articles or news, or academic papers published by researchers) as a comparable analysis or discussion. You can easily Google to find more references. You **MUST** use APA 7th referencing style. Don't forget to add the reference of the original article (the one that you have chosen). For example, you can use the following sentence at the beginning of the report. "The following report is based on the article given in (XXX, 2024)." So altogether, there should be at least 5 references in your report.
4. Create a pdf file as your report. In the report, you **MUST** acknowledge the use of ChatGPT. The Monash guideline is given here: https://www.monash.edu/student-academic-success/build-digital-capabilities/create-online/acknowledging-the-use-of-generative-artificial-intelligence
   You **MUST** also provide the link to show your interaction with ChatGPT (refer to the Appendix).

Note 1: We will not strictly enforce the word count, except that the **Abstract should be *<u>less than</u>* 200 words**, and the **overall report should be *<u>at least</u>* 1000 words** excluding the reference and acknowledgement parts.

Note 2: Your report should contain a suitable title (do NOT write something like “FIT1047 Assignment 4 Part 2a Report” but think of a title that can describe the content of your report). Your report should also contain sub-headers to differentiate different parts or paragraphs. Add appropriate references to support the claim of your report. These references can be those within the articles, or you can use Google to find more related articles (that can be referred to the same incident described in the article, or related but not the same incident.) Marks will be deducted if the format of the report is not correct.

Note 3: Do not include the original ChatGPT generated wordings into your report, but just include the link (the URL) that shows the interaction between you and ChatGPT into your report. Your report should only contain the final version: the one that you have modified from the original one generated by ChatGPT, including all the references.

Note 4: You cannot use other generative AI tools other than ChatGPT (such as Gemini) to complete this task, due to marking consistency and functionality differences.

Follow the steps to prepare your video:

1. Create a maximum of 15 presentation slides, excluding the title page, references, and Appendices (if any). Any page beyond the page limit will not be marked. The slides should include the following:
    - The summary of your report
    - Your justification on whether the ChatGPT’s generated parts are correct or accurate (If YES, the reason for that. If NO, what are missing or what are not correct / accurate.)
2. Record a video presentation (using Panopto, Zoom, Teams or any software of your choice) showing the slides and you talking to the slides (length maximum 7 minutes excluding self introduction)
3. At the start of the video, introduce yourself (you **MUST** turn on your camera!) and show your ID (Monash or others) while introducing yourself. ***Without turning on your camera is regarded as a breach of academic integrity (as we cannot verify if your presentation is done by another person). If you have technical difficulties on turning on your camera, you may seek support from the Monash eSolution team.***
4. The video needs to be in a common format (AVI, MOV, MP4, M4V, etc) and should be of high enough quality to be clearly understood and viewed. The video should be no more than 500MB in size.
5. Don’t forget to add references into your presentation. Use APA 7th referencing style.

Submit your work for this part (Part 2a) as 3 different files:

1. **One pdf file for your report**
2. **Another pdf file for your slides**
3. **One video file for your presentation**

Part 2b - Security controls in an IT network of a medium sized company with automated production of vacuum cleaners (upload 1 pdf file with the slides and 1 video file to Moodle) [30 marks]

For this task you take on the role of a *security architect* (as defined in the NIST NICE workforce framework[1]) You are responsible for a re-design of a company network (using best practices - refer to NSA Network Infrastructure Security Guide[2]), including placing security controls in the right places of the network. As security always costs money, you need to prepare a presentation that explains to the management of the company why each security control is required at that particular part of the company network.

The company has several departments, but the focus is on three network areas:

- Production with automated machines controlled from PCs connected to the network. Production runs 24/7 and outages would be very expensive for the company. The company is very modern and customers can design their own colour combinations and specifications for their vacuum cleaner. Thus, data needs to frequently (every 6 hours) be transferred to the PCs controlling the machines.
- Outward facing servers including a web server that is used for marketing and online sales and the company's mail server.
- Administration with PCs and laptops, a server running administration software and databases, wireless printers and Wifi for meeting rooms and general office areas. Employees also travel with their laptops and need to access the administrative network, but not the production area.

You have a list of security controls to be used and a number of entities that need to be connected in the internal network. Depending on the role of the entity, you need to decide how they need to be protected from internal and external adversaries.

Entities to be connected:

- PCs to control production machines
- Production machines themselves
- Employee PCs and laptops for administration
- Server for administration and internal databases
- Wireless printer and scanner for administration use
- Authentication server
- DNS server
- Web Server
- Mailserver

[1] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

[2] https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF

- WiFi access points
- Routers
- Switches

Security controls and appliances (can be used in several places)

- Firewalls (provide port numbers to be open for traffic from the outside of the respective network segment)
- VPN gateway
- VPN clients
- TLS (provide information between which computers TLS is used)
- Authentication server
- Secure seeded storage of passwords
- Disk encryption
- WPA3 encryption
- Air gaps
- Intrusion detection system

To prepare for your presentation video, follow these steps:

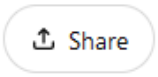
1. Create a diagram of your network (using any diagram creation tool such as LucidChart or similar) with all entities.
2. Place security controls on the diagram.
3. For each security control explain what it is used for and why it is needed in this particular scenario.
4. Create slides for the diagrams (of your full/partial network without and with security controls) and the explanation for security controls. Prepare a maximum of 15 presentation slides, excluding the title page, potential references, and Appendices. Any page beyond the page limit will not be marked.
5. Record a video presentation (using Panopto, Zoom, Teams or any software of your choice) showing the slides and you talking to the slides (length maximum 7 minutes excluding self introduction)
6. At the start of the video, introduce yourself (you **MUST** turn on your camera) and show your ID (Monash or others) while introducing yourself. ***Without turning on your camera is regarded as a breach of academic integrity (as we cannot verify if your presentation is done by another person). If you have technical difficulties on turning on your camera, you may seek support from the Monash eSolution team.***
7. The video needs to be in a common format (AVI, MOV, MP4, M4V, etc) and should be of high enough quality to be clearly understood and viewed. The video should be no more than 500MB in size
8. Don't forget to add references into your presentation. Use APA 7th referencing style.

Submit your work for this part (Part 2b) as 2 different files:

1. **One pdf file for your slides**
2. **One video file for your presentation**

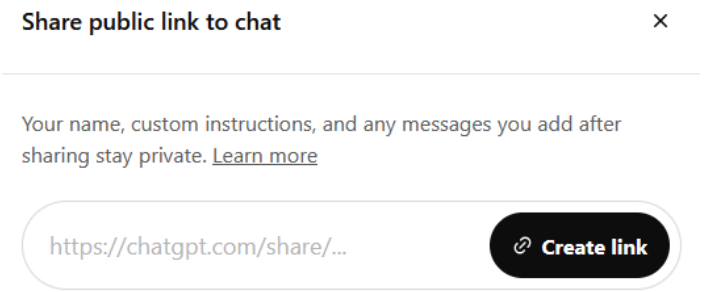
Appendix: How to use ChatGPT

1. Go to chatgpt.com
2. Sign up (if you don't have an account yet) or Login (if you have an account). We recommend you to use your Monash account to sign up.
3. If you are using the free version (ChatGPT Free tier), you can only type your questions in free text (no word or no pdf file as input). You have to copy and paste the content of the articles as free text into the input space.
4. If you are using the paid version (ChatGPT Plus), you can simply upload a word document or pdf file. You can save the article as a pdf and upload to ChatGPT Plus. [For this assignment, ChatGPT Free tier should be good enough.]
5. After generating the text from ChatGPT, copy and paste into your report.
6. Copy the link of your interaction with ChatGPT (click the button on top right corner) into your report



← **This button**
(you will only see it if you have logged in)

and click "Create link"



7. You can ask ChatGPT to refine the answer or re-generate the text, if you are not satisfied with the answer given by ChatGPT (in an interactive way), until you are happy with the answer.