MONASH University

FACULTY OF INFORMATION TECHNOLOGY

FIT1047 Introduction to computer systems, networks and security – S1 2023

Assignment 4 – Cybersecurity

Purpose	In Part 1 of this assignment, students will analyse and discuss a recent vulnerability or cybersecurity attack. The report will demonstrate an understanding of related cybersecurity topics and demonstrate the ability to research information on cybersecurity incidents. For part 2, students prepare a video presentation with slides that shows 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	You need to choose one option and submit a report with your findings regarding the analysis tasks for Part 1. For Part 2, you need to prepare a video presentation. The instructions below contain concrete questions you should answer in your report and presentation. All files (one pdf file for Part 1 and for Part 2 two files, a video file plus a pdf file with the slides) have to be submitted via Moodle.
Value	**30%** of your total marks for the unit Parts 1 and 2 are 15% of the total marks for the unit each.
Word Limit	Part 1: A report with between 500 and 700 words Part 2: A presentation video (max 5 minutes) along with slides (max 15 slides)
Due Date	**Friday, June 9, 11:55 PM**
Submission	• Via Moodle Assignment Submission. • Turnitin will be used for similarity checking of all submissions. • In this assessment, you must **not** use generative artificial intelligence (AI) to generate any materials or content in relation to the assessment task.
Assessment Criteria	See rubric in Moodle Assessment submission page
Late Penalties	• 10% 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

MONASH University

FACULTY OF INFORMATION TECHNOLOGY

Feedback	Feedback will be provided on student work via: general cohort performance specific student feedback ten working days post submission

INSTRUCTIONS

PART 1 - Analyse a cybersecurity vulnerability or incident (upload 1 pdf file with the report to Moodle)

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 the following list (additional other sources can be added, but need to cover the same vulnerability/incident), read the news item, look up and read the referenced sources, and finally write a report on the findings.

- https://www.bleepingcomputer.com/news/microsoft/windows-11-snipping-tool-privacy-bug-exposes-cropped-image-content/
- https://arstechnica.com/information-technology/2023/04/crooks-are-stealing-cars-using-previously-unknown-keyless-can-injection-attacks/
- https://theintercept.com/2023/02/14/whistleblower-image-crop-document/
- https://arstechnica.com/information-technology/2023/03/malware-infecting-widely-used-security-appliance-survives-firmware-updates/
- https://techcrunch.com/2023/03/22/fortra-goanywhere-xansomware-attack/
- https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/
- https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/
- https://arstechnica.com/information-technology/2022/12/critical-windows-code-execution-vulnerability-went-undetected-until-now/
- https://techcrunch.com/2022/12/13/apple-zero-day-webkit-iphone/
- https://arstechnica.com/information-technology/2023/02/until-further-notice-think-twice-before-using-google-to-download-software/
- https://arstechnica.com/information-technology/2023/01/a-fifth-of-passwords-used-by-federal-agency-cracked-in-security-audit/
- https://arstechnica.com/gadgets/2022/12/samsungs-android-app-signing-key-has-leaked-is-being-used-to-sign-malware/
- https://www.thedrive.com/news/hacker-uncovers-how-to-turn-traffic-lights-green-with-flipper-zero
- https://www.zdnet.com/article/this-sneaky-fraud-attack-looks-like-an-email-forwarded-by-your-boss/

Follow the following steps to write your report

1. Choose **one of the 14 news items** above, read the text.
2. Look up and read the articles and information referenced in the news item.
3. Write a short summary of the news item in your own words (max 200 words).
4. Identify which software, hardware or system is affected (max 100 words). The identification should be as precise as possible. Include exact product names, distribution of the product, version numbers, etc.
5. 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? (write 100-150 words)

6. 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 you think
7. are necessary/useful on (i) a technical level, (ii) in terms of human behaviour, and (iii) on a policy level (between 200 and 350 words).
8. Create a pdf file and upload it to Moodle.

Part 2 - 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 with your presentation to Moodle)

For this task you take on the role of a *security architect* (as defined in the NIST NICE workforce framework) You are responsible for a re-design of a company network, 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 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
- Webserver
- Mailserver
- 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
4. Create slides for the diagrams 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 5 minutes)
6. At the start of the video, introduce yourself and show your ID (Monash or others) while introducing yourself.
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. Upload the slides in pdf format and the video to Moodle.