MONASH University

FACULTY OF INFORMATION TECHNOLOGY

FIT1047 Introduction to computer systems, networks and security – S2 2022

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 not longer than 5 minutes
Due Date	**Friday, November 4, 11:55 pm**
Submission	• Via Moodle Assignment Submission. • Turnitin will be used for similarity checking of all submissions.
Assessment Criteria	See rubric
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
Feedback	Feedback will be provided on student work via: general cohort performance specific student feedback ten working days post submission

MONASH University

FACULTY OF INFORMATION TECHNOLOGY

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.theverge.com/2022/8/12/23303411/zoom-defcon-root-access-privilege-escalation-hack-patrick-wardle
- https://www.zdnet.com/article/this-thermal-attack-can-read-your-password-from-the-heat-your-fingertips-leave-behind/
- https://www.theverge.com/23308394/usb-rubber-ducky-review-hack5-defcon-duckyscript
- https://www.theregister.com/2022/08/17/software_developer_cracks_hyundai_encryption/
- https://www.zdnet.com/article/this-sneaky-ransomware-attack-tries-to-switch-off-your-security-software/
- https://arstechnica.com/information-technology/2022/07/microsoft-details-phishing-campaign-that-can-hijack-mfa-protected-accounts/
- https://www.wired.com/story/biggest-hacker-rickroll-high-school-prank/
- https://krebsonsecurity.com/2022/08/paypal-phishing-scam-uses-invoices-sent-via-paypal/
- https://www.zdnet.com/article/fortinet-warns-that-critical-authentication-bypass-flaw-has-been-exploited/
- https://www.zdnet.com/article/this-new-windows-features-makes-password-hacking-attacks-much-harder/
- 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 11 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 50 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 50-100 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 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).
7. Create a pdf file and upload it to Moodle

Part 2 - Security controls in a medium sized company scenario (upload 1 pdf file with the slides and 1 video with your presentation to Moodle)

This task is about security controls in a medium sized scenario. The company has several departments, but we focus on a customer-facing management department and a research and development department. For this part you take on the role of a *security architect* (as defined in the NIST NICE workforce framework) for this medium sized company. 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:

- Employee PCs for the customer-facing management department used in the office
- Employee laptops for the sales staff used from home or while travelling
- Company customer databases also used by sales staff (a physical server)
- Employee PCs for research and development for work on future products
- Printer and scanner for general use
- WiFi access point for guests in the office
- Router
- Switch

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

- Firewalls (provide port numbers to be open for traffic from the outside)
- VPN gateway
- VPN clients
- TLS (provide information between which computers TLS is used)
- Authentication server
- Secure seeded storage of passwords
- Disk encryption
- WPA2 encryption

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
4. Create slides for the diagrams and the explanation for security controls. Prepare a maximum of 10 presentation slides, excluding the title page, references, and Appendix. 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 and the video to Moodle.