Assignment Two [Total Marks:40] (30% of the final grade)

Submission due date: 18/9/2023, 12:00 noon.

Weight: 30% of the final grade
Submission: ECS Submission System

What to submit:

1. Please submit a document (preferably a **pdf** file) containing answers to the tasks in the assignment in order they appear in this document. The document file must be named **Student-Fullname.pdf**
2. The report **must not be less than 6 and exceed 15 pages** (excluding appendix).
3. Diagrams (if any) can be included in the appendix to save space.
4. In the context of this assignment, please pay attention to the following keywords and answer accordingly. Please refer to the marking criteria for more information.
    a. **List**: a simple list of answers with minimum explanations.
    b. **Briefly**: Provide the answer in minimum 2 to 3 summarized lines (can be longer if you need).
    c. "**Explain**", "**Describe**", "**Discuss**", "**Explain in detail**": Provide the answer in minimum 2 paragraphs (can be longer). You may also include diagrams or figures for better clarification.
    d. **Demonstrate**: "Explain", "Describe", "Discuss", "Explain in detail" using a combination of steps, figures, diagrams and screenshots.

Notes:

- Use the submission system on the course website to submit it before the due date.
- Please make sure to start this assignment early and submit on time. Managing time and workload is the responsibility of the student.
- Extensions are only provided in valid circumstances with official relevant documents.
- Please refer to the course outline for extension information.
- Plagiarism will be dealt with under the University policies. Answers containing copied and not properly referenced materials will receive significantly lower grades than one you have written in your own words.

Ministry of Social Development Security Breach Review

The Ministry of Social Development is New Zealand's largest government department providing services to more than 1.1 million clients. It receives in excess of 230,000 calls a week, and approximately 40,000 online applications a month. Like many organisations in the public and private sectors, the Ministry sought to improve its service delivery. One of these initiatives was the implementation of self-service "kiosks", completed in October 2011. In the Ministry environment, the "kiosks" were essentially ordinary computers that were readily accessible to the Ministry's clients in its Work and Income service centers. These kiosks provided valuable information and tools, with a particular focus on supporting job seekers.

However, the Ministry's information security was breached. In one instance, a breach allowed a client to download 7000 documents from the Ministry's network, via kiosks set up for job-seekers in two offices. These documents included invoices detailing the medical conditions of children in state care, the names of people being investigated for benefit fraud, and pay rates for individual Ministry contractors [1].

Tasks [40 Total Marks]

Make sure you read the attached Deloitte report thoroughly and provide a document detailing the following tasks. **Writing and presentation of the report is quite important** and contributes to the grade for each task.

1. **[5 Marks]** Provide a network diagram figure highlighting the architecture of the Kiosk network and services. The figure **must include the network topology, software and services** running on the kiosk systems and servers, **potential** configurations **and, the type of current security controls in place**.

2. **[5 Marks] List and briefly** explain the containment strategy, Incident Response (IR) and Disaster Recovery (DR) actions taken by the Ministry in response to the incidence. This should include actions taken by all incident handlers on this incident.

3. **[30 Marks]** Citing NIST SP.800-61, NIST SP.800-53 and NZISM [2] and/or other relevant NIST documents, **discuss in details** how the vulnerabilities **in the physical and logical design and architecture of kiosk** can be mitigated or minimized **by application of physical and technical controls**:
    a. Deterrent, detective and Preventive controls (e.g. Banners, locks, CCTV, access control, encryption, packet filtering, HIDPS, NIDPS, audits and logs etc.)
    b. Responsive and corrective controls (e.g. Removal of malicious files by an antivirus, backups etc.)

Avoid using controls without proper detailed justification. Unjustified and/or improper suggested controls **will result in partial reduction of marks for this task** as each proposed control will require additional resources (e.g. systems, tools, cost, time, expertise) to implement and maintain.

Additional Notes:

You do not have to rely on the recommendations of the report to suggest adequate controls or improvements and must also use your own domain knowledge of the controls (i.e. What you know, e.g. controls from CYBR171, CYBR271, CYBR371 courses). You may also refer to the course book for an overview of some of the controls. The recommended controls must be detailed and, specify, include and explain the following:

  - The type and description of the control
  - Description on how a physical and technical control should be applied to the kiosk system, its architecture, processes and/or procedures and, the physical and logical location of the control
  - The type of threats/vulnerabilities those controls will protect the kiosk information system components from
  - How your recommended controls would mitigate or minimize the risks (i.e. impact or likelihood) introduced by the identified vulnerabilities and associated threats

- All controls and recommendations must be referenced using appropriate sections in the NIST or NZISM documents, highlighted by the document name and section number (e.g. NIST SP.800.14 Section CP-13)
- Some of the relevant standards and guidelines have been attached as reference.
- NIST SP-800 series standards and guidelines can be obtained from: https://csrc.nist.gov/publications/sp
- You may use other sources to gather information about the incident or the architecture of the kiosk or kiosk services and reference them with proper citation. Use any numbering references (e.g. [1], [2,3])
- Avoid direct copying and plagiarism at any cost. Direct quote should be within "*double quotations*" and "*Italic*". **Minimal number of direct quotations must be given in the main report**. Attach direct quotations from the standard documents as appendix at the end of the report. An example of recommended controls and referencing to the guidelines can be as following (**examples only**):

"A two-factor authentication system [3] should have been installed to authenticate the kiosk admin account on the server."

- Two-factor authentication (2FA), also called two-step verification is a security mechanism in which users authenticating with a system will have to provide two different authentication factors to verify themselves. Two-factor authentication systems generally rely on a user providing a password, "what you know" (i.e. password) as the first factor and a second, different factor such as "what you have" (i.e. pin on mobile phone) or what you are (e.g. biometrics). This ensures the authentication does not only rely on one single mechanism for verification.
- In the case of Kiosk system, a combination of password and pin number sent to a verified admin mobile number/email would be a feasible choice. Alternatively, login through Microsoft Authenticator app which is freely available, can be enabled on the account which would send the pin number to a registered mobile device owned by the administrator.
- According to the guidelines provided in the SP800-14 section 14-3 (Please see Appendices 3.A - **you may copy the relevant rule to the appendix),** application of 2FA authentication would have provided an additional layer of authentication for privileged admin account and would have mitigated the likelihood of an unauthorized local access as well as remote brute-force and dictionary attacks from the internal and external networks against the privileged admin account on the server. All authentication attempts without the specified pin number are automatically rejected and information associated with the attempt is logged.
- 2FA authentication systems also impose a time on the validity of the pin. This ensures the pin is only valid for a certain period of time before it expires and new pin number needs to be issued. This reduces the likelihood of a successful brute-force and dictionary attack which may attempt to try a large number of password and pin combinations over a long period of time.

References:

[1] - Bennett 'mortified' at MSD security breach, Radio NZ, October 2015
[2] - New Zealand Information Security Manual available at: https://www.nzism.gcsb.govt.nz/ism-document/
[3] - Implementing Multi-Factor Authentication, Australian Cyber Security Centre (ACSC), January 2019, available at: https://www.cyber.gov.au/sites/default/files/2019-03/Multi_Factor_Authentication.pdf
[4] - Haseeb J, Mansoori M, Hirose Y, Al-Sahaf H, Welch I, "Autoencoder-based feature construction for IoT attacks clustering", 1 Feb 2022, Future Generation Computer Systems 127:487-502 (***Journal publication referencing example***)

[5] - Haseeb J, Mansoori M, Welch I, "A Measurement Study of IoT-Based Attacks Using IoT Kill Chain" 2020, IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 557-567 (***Conference publication referencing example***)

Marking Criteria

The criteria for grading are:

- **Completeness** – Did you complete all the tasks and how comprehensively? Did you Provide explanation where necessary.
- **Accuracy** - How well did you complete the tasks?
- **Presentation** - Did you use the right terminology? Did you reference the correct relevant document? Please check for readability! We mark a lot of these and well-structured and well-written report will receive higher grades.

Letter grades

A-range:

- Complete, accurate, and well presented. Shows good knowledge and good understanding of methods. Well-argued. Where required, contains good original input from the student.
- Shows understanding of the technical issues from different perspectives; understands the limitations of answers and potential for further investigation.
- No spelling errors, no discernible flaws in punctuation, grammar and sentence construction.

B-range:

- Mostly complete, mostly accurate, and well presented. Shows a good knowledge and fairly good understanding of the methods but either fails to complete some parts of the tasks or is unclear or is poorly argued.
- Shows fairly good comprehension of technical issues but limited understanding of limitations or room for improvement.
- Very few spelling errors, correct punctuation, grammatically correct, complete sentences.

C-range:

- Satisfactory performance although some errors in accuracy and/or problems with presentation. Shows only some basic knowledge of the material or fails to understand some important parts of it, or does not provide solutions to a significant portion of the tasks.
- Exhibits a basic grasp of the technical issues form the most important perspective, without considering others. No real considerations of the limitations of the answers.
- Lapses in spelling, punctuation and grammar, but not enough to seriously distract the reader.

D-range:

Poor performance overall, some evidence of learning but very problematic in all aspects mentioned above.

Incomplete understanding of technical issues involved. Overall analysis or evaluation is limited and may contain minor errors or deficiencies. Some evidence of reasoning. A cut and paste answer would fit here.

E-range:

- Well below the required standard. Made some attempt but tasks were not completed correctly or only addressed a small number of points required.
- Little or no evidence of analysis, evaluation or the formation of judgements.
- Difficult to understand what is being conveyed to the reader.