Sri Lanka Institute of Information Technology

IT21299902 (Zakey M.S.M.A)

ANT assignment 01.

Advance Networking Technology – IE2052

B.Sc. (Hons) in Information Technology Specialization in cyber security.

Assignment Cover Sheet

Declaration:

- I hereby certify that no part of this assignment has been copied from any other work or any other source. No part of this assignment has been written/produced for me by another person.

- I hold a copy of this assignment that I can produce if the original is lost or damaged.

Case Study	Identify logical and physical vulnerabilities of SLIIT.
Date Of submission	25/02/2023

Project Details:

Student registration Details:

	Student registration number	**Student name**	**Signature**
1	IT21299902	ZAKEY.M.S.M. A	

Table of contents.

Introduction.

With the increment of cyber attacks day to day it is compulsory to take the necessary actions to prevent from cyber-attacks. To prevent a company or by any institution can take many actions like using perfect malware guards, good security policies, maintaining the security systems and managing logs to each and every system also need to educate the staff of the premises to well over come from the cyber-attacks.

When we are looking at universities, they have huge networks that interconnect their branches and systems that provide 24/7 service to the student as well as for the lecturer also to the other staff. To successfully overcome those cyber-attacks, we need to first identify vulnerabilities.

As per the need of this assignment I have identified logical and physical vulnerabilities of SLIIT that can be used by intruders to exploit them and attack the systems and network to gain advantages like information theft. Also mentioned the solution that can be taken to identify vulnerabilities.

1.Physical vulnerabilities of SLIIT.

As we are looking at vulnerabilities there can be physical and logical vulnerabilities. What does physical vulnerabilities mean is it can cause harm to people or can cause any injuries to the person who uses it [1]. Somehow physical vulnerabilities must be mitigated to an acceptable level that no can be harmful to people. Specially in a university it a key point to be considered. If ignored those physical vulnerabilities it may end up in disaster [2].

There are many physical vulnerabilities can be identified in SLIIT premises. Some of them can't mitigate. Must accept it. By addressing the physical vulnerabilities in universities can help ensure the security of their facilities, sensitive information, and critical systems. Some of most important physical vulnerabilities mentioned below.

1. **Lack of surveillance.**
    - There are not enough CCTV cameras around the university premises. It will be very hard to monitor the suspicious movement around the university also things that belong to student or to university can be stollen very easily.

    Evidence – I have noticed that areas like Bird nest, outdoor study areas don't have CCTV monitoring systems. So those are the places where the students spend a lot of time very much. Not having cctv in that areas will lead to risks like losing the assets belong to student or they can damage the university assets without any hesitation.

2. **Lack of security personals.**
    - There are not enough security guards to protect the entrances to the SLIIT premises. Because of lack of the security personals, it will be very easy to steal items from SLIIT and take away.

    Evidence – I every time enter SLIIT using the back gate. There are 2 guards to check the student ID's. I have noticed that some of the senior students don't scan their ID in the scanner, because they get to know the guards very well and being friendly with them. So, the guard allowed them to SLIIT premises without checking their ID's.

3. **Poor maintenance of security systems.**
    - This is the key system of an any institute or in a company. If the security system has vulnerabilities it will lead to big problems like possible data loss, DOS attack, information theft etc.

    Evidence – I have personally experienced a situation where I must scan my student ID to enter the SLIIT. When I scanned my card, instead of showing my name and profile

picture in system screen it showed me another unknown person's details. On the same day lots of my friends faced this issue the same as me.

4. **Lack of lighting issues.**
    - Lighting is none of the key elements in universities. Students usually spend their time on university premises and if there is not enough lighting around the university premises it's hard to do the studies on campus overnight.

Evidence – I have personally stayed on campus until 8 or 10 in order to finish my daily study routine. Usually there is power cut going around the country and most of student those who are in hostel stay in campus to do studies. If there is too much rush inside the university, we need to find another place that is available to do our studies. Due to the unavailability of clear lighting it's hard to find a better place to do our study than study areas.

5. **Unsecured buildings.**
    - As the main faculty of SLIIT is computing the computer labs must be protected enough. Only having CCTV cameras is not enough to protect the computer laboratory equipment. If there is no any security systems to laboratories might lead to easily steal the assets that belong to SLIIT.

Evidence – Personally I get to know that a student stole a mouse that attached to the computer and got escaped. Because there is no security mechanism like face recognition or biometric authentication when entering the laboratory, it is very easy to steal assets.

1.1 Solutions to detect & correct physical vulnerabilities.

1. **Lack of surveillance.**
    - As a solution to this problem need to **install sufficient cameras** around the university premises. Especially in high-risk areas like libraries, laboratories, and parking lots. Above that needs to be installed in areas where the students mostly move around to avoid any damage to the properties of SLIIT and to the students [3].

2. **Lack of security personals.**
    - As a solution to this problem university can hire more security personals. If it's hard to afford that much security personals, they can simply use a system like **automatic intruder detection system** to ensure that there is no un-authorized person inside the university premises [4].
    - By installing such a system, they can detect the person and if there is an unauthorized person inside, they can use the available security personnel and inquire about the person using security personnel.

3. **Poor maintenance of security systems.**
    - As a solution to this problem, universities can **keep documentation and record of the system**. By that they can keep all the details records of all security systems, maintenance history and security patches. By referring to those record can identify the issues and can apply the perfect solutions to them.
    - Also, can do **security audits** to keep the security systems up to date and at its max performance to avoid possible exploitation.

4. **Lack of lighting issues.**
    - As a solution to this problem, can **upgrade the lighting system** like installing additional lighting around the university to reduce the risk of accidents. This is a must need in areas like parking lots, walkways, and staircases.
    - If adding additional lighting costly they can simply move to LED lighting systems. By using **LED lighting** systems, they can reduce the cost and can improve the quality of lighting [5].

5. **Unsecured buildings.**
    - As a solution to this problem, universities can use **access control systems** like card readers and biometric systems to enter and exit from the lecture halls and from the laboratories [6].

- By using such a system, they can greatly mitigate the vulnerability detecting and correcting the issue. If they used a system like that unauthorized students can no longer enter the lecture hall at inappropriate time and steal assets that belong to university.

2. Logical vulnerabilities of SLIIT.

Previously discussed about physical vulnerabilities of SLIIT and acceptable solutions for them. As we know there are another type of vulnerabilities as well. Those are called logical vulnerabilities. Logical vulnerabilities can be referred to as technical vulnerabilities. Those can happen due to technical issues, bad implementation or from incorrect usage [7].

When we are looking at technical vulnerabilities there are a ton of them. but in SLIIT notice some important technical vulnerabilities that can bring some damage to the systems, or it may lead to data loss.

1. **Poor password management.**
    - Passwords are the verification method of a specific user. If someone is using the same password across multiple platforms its very easy to figure out the password by the attackers doing social engineering.

` **Evidence –** So far until year 2 of academic year I have used the same account that provided to me by the university to access course web and endoscope. Finally I have managed to change account passwords. But most of the students still using the same account credentials to login to those platforms.

2. **Insufficient access controls.**
    - Access control is a must when came to the laboratories and equipment's. If there is no access control mechanism used in those there will be a huge problem, or we can say threat to the system and network.

   Evidence – personally I have seen we can get access to accessibility tools like task manager, control manager, and firewall etc. if the user of that system has the great knowledge on what they do and how to use them he/she might take that advantage to do harm to the system.

3. **Unsecured BYOD devices.**
    - Usually, universities allow bringing BYOD devices to laboratories in order to reduce the demand to use the computers that provided by SLIIT. Allowing uncontrolled BYOD devices is a very sicky decision. They can do different things by connecting to a network.

   Evidence – personally one of my friend connected to the SLIIT network and tried to download a torrent file. But initially torrent sites are blocked by proxy. But he managed to use a technique and he was able to download the torrent files easily.

4. **Malware infections.**
    - Malware can be different types. But the basic intention of malware is to harm the computer system or to steal information from the system. If doesn't use perfect mechanisms to prevent infecting malware to the system, it can lead to a data breach that may cause a service down time until fix it.

Evidence – when we using computers that has in the laboratories we are using pen drives to copy the work done on that system to copy to our devices or for later refereeing. But when connecting external storage devices that are not totally safe at all can contain viruses or any harmful payloads infected to that drive earlier.

5. **Lack of employment training.**
    - If the computer laboratory instructors don't have the perfect knowledge on how to fix things if something happen to a system or to help out system errors that can happen in runtime it will be a useless of having a lab assistant. because they can't fix the issue temporarily and make the system back on live.

Evidence – I have noticed when something going wrong with the computers in laboratory the instructor currently allocated to us couldn't fix it he/she calling an technical expert to help out he/she or they might say try to any other computer that available in that laboratory instead of trying to fix it immediately or without giving a try to fix it.

2.1 Solutions to detect & correct logical vulnerabilities.

1. **Poor password management.**
    - As a solution to this problem, universities can use **automated password management systems** to store and manage passwords. By using such a system, they can store passwords in a more encrypted manner than entering a single password at a time to the system [8].
    - Also, they can establish **password policies** to ensure that students have created more complex passwords by following those password policies [9].

2. **Insufficient access controls.**
    - As a solution to this problem, SLIIT can use a mechanism like **Role-Based access control (RBAC)** to ensure only students can access resources that given access. Also same to lecturer and to devs [10].
    - By that can greatly manage the system resources and data integrity.

3. **Unsecured BYOD devices.**
    - As a solution to this problem, SLIIT can use **mobile device management (MDM) policies** to regulate the use of BYOD devices on the university network. So that users that connected to the SLIIT network only can-do limited work on their BYOD device. Such as the sites that permission granted by SLIIT only can be access though the SLIIT network [11].
    - By that SLIIT can assure the security of the network.

4. **Malware infections.**
    - As a solution to this problem, universities can use well configured **firewalls** to prevent the campus network being infected by malwares. Firewalls can block unauthorized access to the university network [12].

5. **Lack of employment training.**
    - As a solution to this problem, university can do **tailer training** based on employee's role and responsibilities. By that can ensure that they have the specific knowledge and skills they need to perform their job functions securely.

References

[1] P. jullion, "study buff," [Online]. Available: https://studybuff.com/what-is-a-physical-vulnerability/#:~:text=What%20is%20a%20physical%20vulnerability%3F%20Physical%20vulnerability%20describes,value%20of%20physical%20assets%20in%20the%20hazardous%20zone.. [Accessed 16 02 2023].

[2] Elsevier, "Science direct," [Online]. Available: https://www.sciencedirect.com/topics/computer-science/physical-vulnerability. [Accessed 16 02 2023].

[3] "Vmukti," [Online]. Available: https://www.vmukti.com/9-advanced-cctv-camera-surveillance-solutions-to-protect-people/. [Accessed 16 02 2023].

[4] [Online]. Available: https://www.infosecurity-magazine.com/news/lack-of-skilled-personnel-biggest/. [Accessed 2023].

[5] Nosbaum, "smart energy," [Online]. Available: https://www.smart-energy.com/industry-sectors/smart-meters/street-lighting-problems-and-solutions/. [Accessed 16 02 2023].

[6] "nedap," [Online]. Available: https://www.nedapsecurity.com/insight/what-is-access-control/. [Accessed 16 02 2023].

[7] "Acunetix," [Online]. Available: https://www.acunetix.com/blog/web-security-zone/logical-and-technical-vulnerabilities/. [Accessed 16 02 2023].

[8] "Spiceworks," [Online]. Available: https://www.spiceworks.com/it-security/identity-access-management/articles/what-is-password-management/. [Accessed 16 02 2023].

[9] "MUO," [Online]. Available: https://www.makeuseof.com/what-is-a-password-policy/. [Accessed 16 02 2023].

[10] "Up guard," [Online]. Available: https://www.upguard.com/blog/rbac. [Accessed 16 02 2023].

[11] "power DMS," [Online]. Available: https://www.powerdms.com/policy-learning-center/mobile-device-management-mdm-policy-best-practices. [Accessed 16 02 2023].

[12] "cisco," [Online]. Available: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html. [Accessed 16 02 2023].