Sri Lanka Institute of Information Technology

Specialized in Cyber Security

Year 2, Semester 2

Weekend Group

Physical and Logical Security Vulnerabilities of SLIIT

IE2052 - Advanced Networking Technologies

Assignment 1 - Individual

IT21170720– K.D.S.P. Jayawikrama

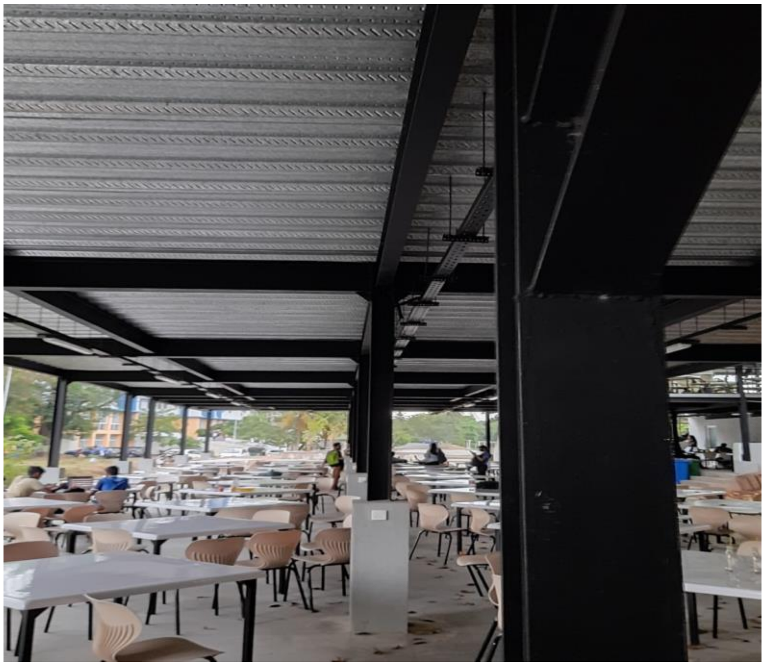
Table of Contents

Physical Vulnerabilities of SLIIT

Fire situation:

One of the most frequent physical weaknesses is fire. Implementing fire detection and suppression systems, such as fire alarms and fire extinguishers, can help ensure that any fire can be immediately put out. There are no fire prevention actions in the SLIIT study region for bird nests.

According to the following photo, we can see there are not any fire prevention actions.



Natural Disasters:

Infrastructure can sustain serious harm from natural catastrophes including hurricanes, earthquakes, and floods. The institute needs to take precautions to defend its infrastructure against catastrophic catastrophes, such building with reinforced foundations and setting up backup power. As there are no nearby rivers, there won't be any flooding in the SLIIT, although there could be earthquakes and hurricanes. Thus, we need to take precautions against them.

Theft:

Installing surveillance cameras and motion detectors will stop theft of pricey equipment. There are no CCTV cameras in the research area for bird nests. This makes it easy for any student to steal another's laptop, phone, or other valuables. We can see there are not any CCTV operations in the in the bird nest study area.

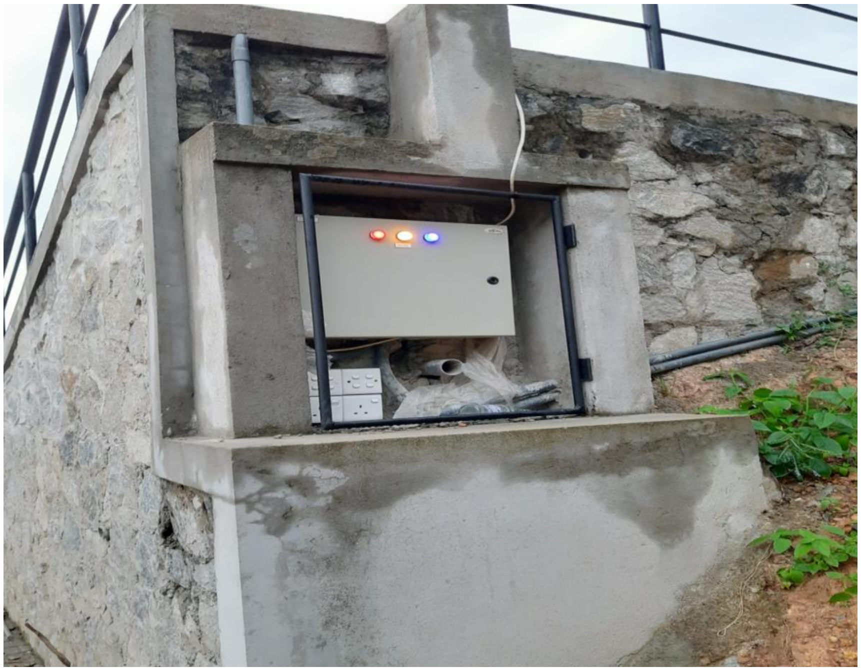
Insecure Perimeter:

Insufficient barriers or poorly maintained fencing may make it simple to enter the property. The main gate is opened in the morning and evening for all lecturers arriving at and departing from SLIIT. Several students might enter the SLIIT campus at that time without going through security checks at the main gate. because any student could bring drugs or other dangerous items onto the campus of SLIIT.

Poorly maintained infrastructure:

Security problems and poor performance might result from an obsolete or neglected infrastructure. Students may use tables and other equipment inadvertently because SLIIT's cafeteria area and bird nest study space do not operate any CCTV cameras.

we can see below picture. It is transformer unit of current system. It has not any coverage. Water and other harmful thins can enter to it and after can be happened fire.



Solutions for physical Vulnerabilities of SLIIT

Solutions for fire Vulnerability:

1. Conduct routine audits and checks of physical security to find and fix any potential weaknesses.

2. Create a fire protection strategy for the property that includes both suppression and suppression response measures.

3. Ensure that all areas of the building have smoke and fire detectors.

4. Put in place fire safety measures including fire drills and training for fire extinguishers.

5. Ensure that everyone on staff is familiar with the fire safety plan and evacuation routes.

6. Put in fire doors to stop the spread of the fire.

7. Keep any ignition sources and combustible materials apart.

8. Establish and routinely test a plan for responding to emergencies.

9. To safeguard the computer system from future fires, use firewalls, antivirus software, and other security measures.

10. Regularly check the area for any signs of fire.

Solutions for natural disaster vulnerabilities:

1. Create a risk management plan:

   The first thing that needs to be done is to create a plan that covers recovery tactics, evacuation protocols, and emergency procedures. The specific risks unique to the area should be considered, and the plan should be revised and tested frequently.

2. Invest in Structural Upgrades:

   Upgrades to existing infrastructure, including buildings, can help lessen the effects of natural disasters. Making ensuring that roofs are securely fastened, strengthening walls, and putting up storm shutters are a few examples of what this might entail.

3. Enhance Land Use Planning:

   By placing buildings and other structures in places with lower risks of flooding, landslides, and other hazards, land use planning can help lower the risk of natural disasters.

4. Teach the pupils:

Teaching students about the dangers of natural disasters and how to be prepared is a crucial step in lowering vulnerability. Giving information on emergency shelters, evacuation strategies, and other resources is one example of this.

5. Create Early Warning Systems:

Early warning systems can help people prepare for and evacuate during catastrophes by giving them crucial early warning. These can include apparatuses like flood warning systems, early warning systems for earthquakes, and tsunami warning systems.

Solutions for theft vulnerabilities:

1. Protect Your IT Assets:

   Ensure that all your IT assets, such as PCs, laptops, tablets, and other devices, are stored in a secure location and locked away when not in use. Deploy CCTV cameras to keep an eye on storage locations for IT assets, and whenever possible, limit access to these locations.

2. Employ Access Control:

   Restrict access to IT assets and data by employing access control technologies like passwords, biometrics, or card access systems.

3. Keep an eye out for Suspicious Activity:

   Keep an eye out for any strange activity in or around storage locations for IT assets. Install motion-detecting alarms and/or other security equipment to notify staff of any unwanted access.

Solutions for Insecure Perimeter vulnerabilities:

1. Install security measures like CCTV surveillance cameras, motion detectors, guard patrols, and access control systems on your physical property to properly secure it.

2. Use tight authentication protocols to limit physical access.

3. Assure regular testing and proper maintenance of all locks and security systems.

4. To keep on top of security risks and vulnerabilities, regularly evaluate and update security policies.

5. Orient staff to the rules and practices of physical security.

6. Protect important data and devices using encryption and other security methods.

7. Keep track of, log, and audit physical access to data centers and other off-limits locations.

8. Create a policy requiring all guests, contractors, and other outside parties that enter the property to abide by the same regulations as the on-site workers.

Solutions for Poorly maintained infrastructure vulnerabilities:

1. Track the performance of the infrastructure:

   Implementing monitoring systems to keep tabs on the functionality of the infrastructure's various parts can assist in spotting possible issues before they get out of hand. Also, routine inspections will give a clearer picture of the state of the infrastructure, enabling better maintenance and repair choices to be made.

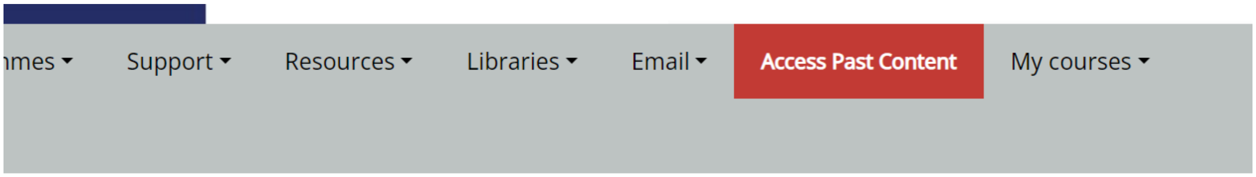
2. Boost organizational culture:

   Making sure the resources are allotted to keep infrastructure in good shape can be accomplished by fostering an organizational culture that stresses the significance of infrastructure maintenance. To guarantee that the necessary work is done correctly, it is also crucial to make sure that workers have received the proper training in infrastructure maintenance and repair.

Logical Vulnerabilities of SLIIT:

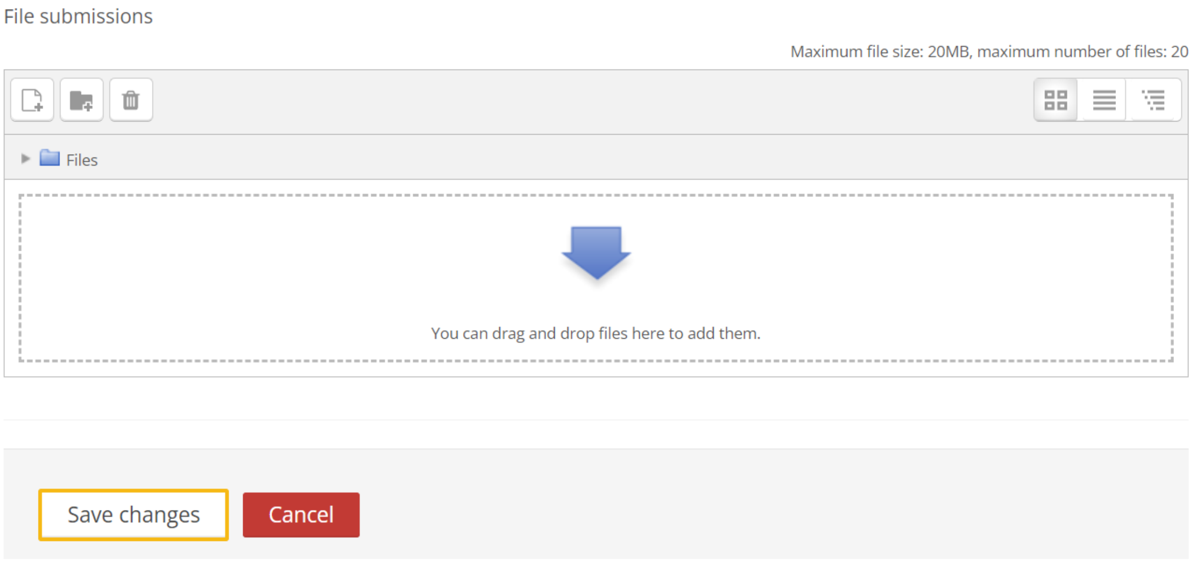
1. **Old Courseweb Authentication and authorization problem:**

   Still can be access to old courseweb via new courseweb. Old Courseweb is not any two-factor authentication method. It has only password authentication. If the website does not properly authenticate and authorize users, it can lead to logical vulnerabilities such as privilege escalation, session hijacking, or account takeover.



2. **Data validation:**

When we submit our document in SLIIT course web page, which does not check our document. Attacker can find the vulnerability and upload revershell and gain unauthorized access to the system. The website may be vulnerable to logical flaws including buffer overflows, format string attacks, and integer overflows if data is not properly validated and sanitized.



File submissions

Maximum file size: 20MB, maximum number of files: 20

You can drag and drop files here to add them.

3. **Unsecure channels of communication include non-encrypted emails and messaging:**

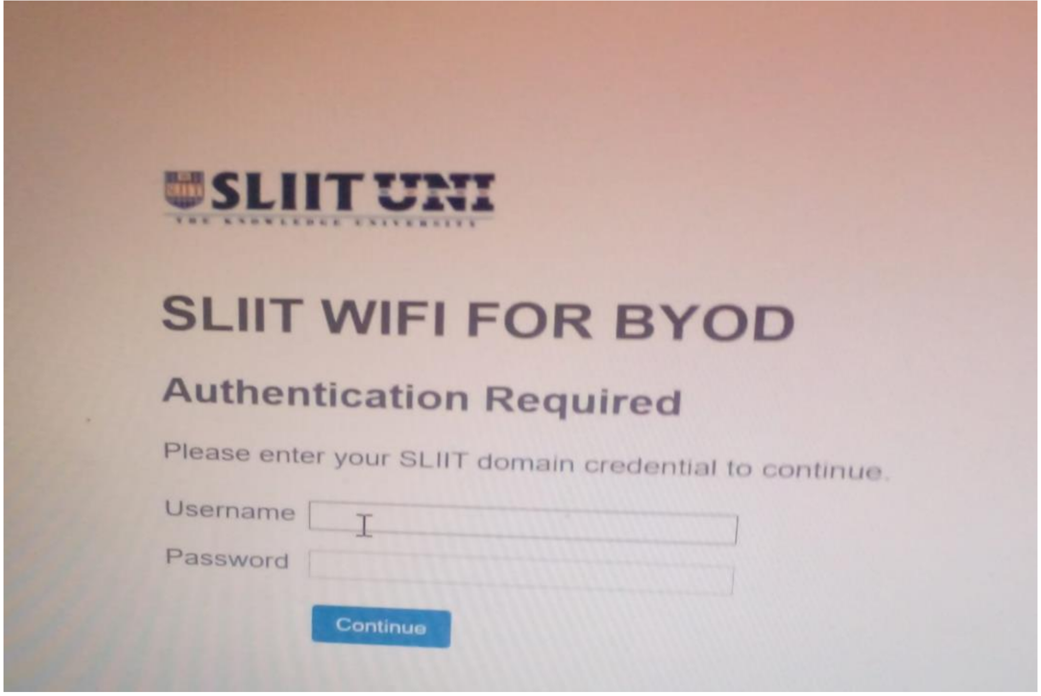
Every time SLIIT provide the non-encrypted email for student and calling person who ask about SLIIT degree programs(Message ID,DKIM security). By intercepting the transmission and reading its contents, an attacker could take advantage of the weakness of non-encrypted emails or messaging. Man-in-the-middle (MitM) attacks are this kind of assault. The attacker might snoop on the traffic and read the message that wasn't encrypted, change it, or give the recipient a false message.

4. **Misconfigured security settings:**

Incorrect configuration of the Wi-Fi network's security settings can make the network open to intrusion.

5. **Weak or easily guessable passwords:**

Sometime Wi-Fi can be used in out of gate but near the SLIIT main gate. So most of student using their national identity card number for Wi-Fi password and the SLIIT ID number use for username of SLIIT Wi-Fi system. The Wi-Fi network may be subject to brute force assaults, in which an attacker attempts a password several times to guess it, if it employs weak passwords or passwords that are simple to guess.



SLIIT WIFI FOR BYOD

Authentication Required

Please enter your SLIIT domain credential to continue.

Solutions for logical vulnerabilities

1. **Solutions for Old Courseweb Authentication and authorization problem:**

- Multi-factor authentication:

  Users must submit two or more authentication factors in order to access a system or application using the security mechanism known as multi-factor authentication (MFA). A security token, for example, a password, or something the user is aware of can all be included in this (e.g., biometric data). Multiple-factor authentication (MFA) adds an extra layer of security and makes it more difficult for attackers to get illegal access.

- Role-based access control:

  The method of restricting access to resources based on the responsibilities of certain users within an organization is known as role-based access control (RBAC). Users are given roles in RBAC, and access to resources is determined by those roles. As a result, the risk of illegal access is decreased, and users are guaranteed to only have access to the SLIIT courseweb they require to do their duties.

- Single sign-on:

  With a single set of login credentials, users can access different apps and services using the single sign-on (SSO) authentication approach. Users no longer need to remember several passwords, and IT staff can control user access more easily as a result. Enforcing robust authentication policies throughout the entire SLIIT old course online can increase security and benefit from SSO.

2. Solutions for Data validation:

- Data type checking:

  Data validation problems can be avoided by making sure that data entered a system matches the anticipated data type. For instance, if a system anticipates a date in a specific format, it can verify that the entered date adheres to that format.

- Regular expressions:

  Data can be checked against certain patterns using regular expressions. For instance, a regular expression can be used to check an email address for the presence of the "@" symbol and a legitimate domain name.

3. Solution for Non-encrypted emails or messaging are examples of insecure routes of communication:

- Use encrypted email services:

  Services that offer end-to-end encryption, like ProtonMail, Tutanota, or Google, can aid to protect email communication.

- Use encrypted messaging apps:

  Signal, WhatsApp, or Telegram are examples of encrypted messaging applications that can offer secure messaging.

- Use SLIIT's internal messaging system:

  SLIIT's internal messaging system may provide more secure communication, as it is likely protected by the school's security protocols.

4. Solution for Misconfigured security settings:

- Use a web application firewall (WAF):

  By removing harmful traffic and preventing requests that transgress security policies, a WAF can aid in the prevention of attacks.

- Update software and plugins:

  Ensure that any plugins and applications utilized on the website have the most recent security updates.

- Use secure cookies:

  Install secure cookies to stop session hijacking and make sure that cookies are encrypted and only sent over HTTPS.

5. Solution for Weak or easily guessable passwords:

- Regularly change passwords:

  Change the Wi-Fi network passwords frequently to make sure that outdated passwords are no longer valid for extended periods of time and are less vulnerable to being compromised..

- Implement a password manager:

  To create and securely store complicated passwords, encourage users to use password managers.

- Use two-factor authentication:

  Use two-factor authentication, such as biometric authentication or one-time passwords, to add an extra layer of security to the Wi-Fi network's access procedures.

References

- https://www.securitymagazine.com/blogs/14-security-blog/post/79415-logical-and-physical-vulnerabilities-according-to-the-black-hats-1
- https://www.acunetix.com/blog/web-security-zone/logical-and-technical-vulnerabilities/
- https://portswigger.net/web-security/logic-flaws#:~:text=What%20are%20business%20logic%20vulnerabilities,to%20achieve%20a%20malicious%20goal.