LAB

2

Current Cyberattack Scenario

By the end of this section, you should be able to:

- Collecting Information on Cyber Attack from the internet sources.
- Review cyberattack incidents.

2.1 Introduction

Hacking is a malicious activity that could disrupt a network infrastructure and cause millions of dollar losses as well as giving a bad reputation towards an organization or company. In recent years hackers attack are more rapid and complex, the availability of hacking tools that is freely available from the internet make it possible for any attack to being launch easily. In order to prevent any attack, a security administrator need to be alert and detect any attack before it takes place. To identify an attack at early stage a security personnel need to know the trade and techniques a hacker will use in launching an attack. Threat Intelligent is one of the area most of current researcher are exploring nowadays. Threat intelligence is information about threats and threat actors that helps mitigate harmful events in cyberspace. In Threat intelligence, data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors. Threat intelligence enables us to make faster, more informed, data-backed security decisions and change their behavior from reactive to proactive in the fight against threat actors. One of the information collected is news and event related to cyber incidents from social media, news portal or security blog. By collecting this information, a security analyst can get a firsthand news and predict the future cyberattack trend.

Task 1

Collecting and reviewing Cyberattack incident.

*****in a group of 2 members***

1. Collect and review at least 5 current cyber attack incidents takes place between 2019 until 2021 from any news portal, blogs, social media and cybersecurity agency/company.
2. Each incident collected should have an official and valid references.
3. Each incident needs to be reviewed based on
    a. Date / target the incident take place.
    b. The target
    c. The damage/malicious activity done.
    d. Suspect/criminal who responsible in launching the attack.
    e. What vulnerabilities/ opportunity that has been exploit by the attacker.
    f. Losses involved.
    g. Your opinion in preventing/mitigating the incident from happening to your organization.

4. Report your finding in a Microsoft office document file with a front page with your group members name and upload the report on ulearn.