## IT5504/ IT5479 Information Security

**Lab 5 Threats to Computer Security**

**Due date and time**

This Lab tutorial is carried out in the session in week 5 of the course.

**Purpose**

This lab exercise enables us with a better understanding of concepts associated with “Threats to Computer Security”.

**Preparation**

Lecture notes, online research, journal articles and appropriate relevant resources.

**Submission**

Submit your answers to this exercise in a Word document and upload it to the Moodle dropbox provided.

**Activity 1)**

**Review Questions**

*(Briefly answer the following review questions)*

1. Define the following terms:

a) Threat – **An intent to steal, damage or disrupt data or digital systems. Potential danger to an asset such as data or network itself.**

b) Vulnerability – **Weakness or deficiency in a computer system or network.**

c) Risk – **Probability of exposure or loss resulting in a cyber attack or data breach on your organisation. The likelihood that a particular threat will exploit a particular asset that results in undesirable consequences.**

d) Exploit – **code that takes advantage of a software vulnerability or security flaw. A mechanism that is used to leverage**

e) Zero-day vulnerability – **Software or hardware flaw that has been discovered and for which no patch exists. Newly discovered software vulnerability for which developers have zero days to fix leaving a potential exploitation by hackers.**

1. Why is understanding threats, vulnerabilities, and risks important in the context of computer security? **Understanding threats, vulnerabilities and risks is important in the context of computer security because it helps you approach your business security strategy more effectively. Equipping this knowledge protects valuable information and safeguarding those who use or connect with the network.**
2. Provide an example of a threat to computer security in the public sector and explain its potential impact on the targeted organization.

**An example of a threat to computer security in the public sector could be a person such as an employee who destroys infrastructure/hardware. Resulting in costs to organisation to repair and fix the damaged equipment.**

1. How does a vulnerability differ from a threat? Give an example of a common vulnerability found in computer systems.

**Threat is any potential danger that could exploit a vulnerability while a vulnerability is a weakness in computer systems that could be exploited by a threat. An example of vulnerability could be an unpatched software system. Hackers could exploit this vulnerability and gain access to the system.**

1. Explain the concept of a zero-day vulnerability and its significance in the realm of computer security.

**Zero-day vulnerability is a flaw in the software programming that has been discovered before a programmer has been made aware of it. Its significance in the realm of computer security has increased regular patching fix up. This vulnerability can expose sensitive data or compromise the system.**

1. Identify two information sources that organizations can utilize to stay informed about the latest threats and vulnerabilities in the private sector.

**Two information sources that organizations can use to stay informed about the latest threats and vulnerabilities in the private sector would be ZX security and helix security.**

1. How does the public sector gather information about emerging threats and vulnerabilities? Mention two reliable sources for this sector.

**Public sector can check online for information on emerging threats and vulnerabilities using these websites National Cyber Security Centre or Netsafe.org.nz which helps provide guidance on personal security for staying sage online.**

1. What is the Common Vulnerability Scoring System (CVSS)? How does it help organizations assess the severity of vulnerabilities? **Common Vulnerability Scoring System that helps companies compare vulnerabilities and potentially prioritise protecting against them. CVSS scores from 0-10 where 0 is no threat and 10 is critical threat.**
2. Choose a real-world vulnerability, and describe how it would be scored using the CVSS. Explain the significance of the score from a risk management perspective.

**One example of a real-world vulnerability is CVE-2021-44228, also known as Log4Shell, which affects the Apache Log4j library used by many Java applications. This vulnerability allows remote code execution by sending specially crafted input to a vulnerable application that uses Log4j**

1. From a CIA (Confidentiality, Integrity, Availability) perspective, discuss the potential impact of a significant security breach on an organization. How can understanding the threat, vulnerability, and risk help mitigate such impacts?

**Confidentiality – Breach expose sensitive or classified information to unauthorized parties, damaging reputation and trust of the organization.**

**Integrity – Breach can alter or corrupt the data systems that are inaccurate. This will affect the quality of the organizations service where financial records are lost.**

**Availability – Breach can deny access to data or systems of the organization making them unavailable. This can effect the continuity of the organization activities causing frustration.**

**Understanding theses risks we can mitigate the impacts by identifying and analysing the potential risks such as hackers, insider etc. Vulnerability by assessing the weaknesses or gaps in the data system. Risk estimating likelihood and impact of data.**

The above review questions cover a broad range of topics related to computer security. They encompass the fundamental concepts of threats, vulnerabilities, risks, exploits, and zero-day vulnerabilities' significance. The exercise also addresses the importance of staying informed about threats and vulnerabilities in both the private and public sectors and introduces the Common Vulnerability Scoring System (CVSS) and the Common Vulnerabilities and Exposures (CVE) system. By considering a scoring system and evaluating threats from the CIA perspective, the exercise aims to help individuals understand how to assess and mitigate potential impacts on computer systems.

**Activity 2)**

**Discussion Questions**

**Mini Case 1: Ransomware Attack on a Healthcare Institution**

In this real-life scenario, a healthcare institution faced a serious threat when it fell victim to a ransomware attack. The attackers exploited a vulnerability in the institution's remote desktop services, gaining unauthorized access to the system. They deployed a zero-day exploit that was not yet known to the security community, making it difficult to defend against. The attackers encrypted critical patient data, rendering it inaccessible to healthcare providers and demanding a hefty ransom in exchange for the decryption key.

**Discussion Points:**

* Reflecting on this case, briefly discuss the importance of keeping software and systems up to date to prevent known vulnerabilities from being exploited. You can also explore the challenges of dealing with zero-day vulnerabilities that lack available patches or solutions.

**Keeping software and systems up to date is important to prevent known vulnerabilities from being exploited by hackers. Fixing patches regularly will reduce chances of attack and improve performance. Dealing with zero day vulnerabilities can be using back up and recovery to restore data loss in cases of zero day exploit that causes data loss or corruption.**

* You might relate this case to your personal experiences with online security, discussing the significance of using strong, unique passwords, enabling two-factor authentication, and being cautious about suspicious links and email attachments to avoid falling victim to similar attacks.

**Using 2FA authentication has given myself the feeling the of being secure and using strong password managers to help safe guard this information. Organisations who recommend 2FA also provides confidence for us consumers.**

**Mini Case 2: Data Breach in a Government Agency**

In this second case, a government agency experienced a data breach due to a misconfigured cloud storage bucket. The agency stored sensitive citizen information on the cloud, but the bucket was unintentionally left publicly accessible without proper authentication. This vulnerability allowed threat actors to access and download sensitive data, compromising citizens' personal information.

**Discussion Points:**

* Discuss the importance of configuring cloud services securely and the potential consequences of misconfigurations in the public sector. What is the role of proper access controls and encryption in safeguarding sensitive data? **The importance of configuring cloud services potential helps with data recovery, high level of security and improved service quality. The misconfigurations consequences can lead to data breaches, loss of sensitive information. Access controls help you stay complaint with various industry standards and regulations. Encryption role is a process where it scrambles readable text and can only be read by the person who has the secret code or decryption key. This is an important privacy tool when sending sensitive, confidential or personal information across the internet.**
* Drawing from personal experiences, share how you handle data security in your digital lives and what measures you take to protect your information in the cloud and on personal devices.

**How I handle data security and protecting information in the cloud is by making sure there are multiple areas of saved data storage. Ensuring there is safe space and multiple layers of security measures to access this information.**

***Reflect on the following:***

1. *How do these cases illustrate the concepts of threats, vulnerabilities, and risks in computer security?*
2. *What measures could the affected organizations have taken to prevent or mitigate these incidents?*
3. *How can the use of zero-day exploits pose significant challenges for organizations and security professionals?*
4. *What are some key takeaways from these cases that you can apply to enhance your own online security practices?*
5. *Considering your experiences with digital security, what steps can you take to better protect your personal data and privacy?*

*Start thinking critically about these questions and share your insights, experiences, and ideas to foster a deeper understanding of the importance of computer security in both organizational and personal contexts.*