**Assignment**

**Individual**

**KDS – Name SME**

**Session 02**

**To** **be Submitted Week 03**

**Tugas Personal ke-1**

1. **Apa tujuan atau mengapa penting untuk belajar IT Risk Management dan apa hubungannya dengan contingency planning?**

**Answer:**

**IT Risk Management is the process of identifying, analyzing, anticipating and monitoring risks to minimize the impact of a risk on the entire project** such as in a process of developing a software project, the risk might be that some of the systems or the server or the database might fail or stop functioning. So, **the risk management must be able to identify such risks and must take appropriate measures to minimize the impact of such risk on the entire project**.

**IT risk management relationship with Contingency Planning has the philosophy of a war expert from China, namely General Sun Tzu**, **he has the following concepts**:

***“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”***

In the philosophy above, if we know the strengths and abilities of the enemy and know our own strengths and abilities, we can predict the risks that will occur. If we don't know the opponent's strength and only know our own strengths and abilities then it's likely that we can take losses from risks that we don't know about. It is very dangerous if we do not know the strength of the enemy and also do not know our own strength.

**REFERENCES :**

Whitman, M.E., Mattoro, H.J. (2013). Principles of Incident Response and Disaster Recovery

1. **Jelaskan apa yang dimaksud Identify Risk, Control Risk, and Assessment Risk.**

**Answer:**

1. **Identify Risk**

The process begins with the listing of the belongings and categorized them. The belongings might be computer parts and tools, programs, people, or networks. The risk manager analyzes the effect of threats whether it is internal or external and rates them accordingly. The threats arise due to natural attacks or robbery, or software hit.

1. **Control Risk**

**This task involves four strategies, such as:**

1. **Avoidance**

A defensive tool is adapted to eliminate the risk such as illustrating the installation of fire wall to illegal use of LAN access.

1. **Mitigation**

Cautious preparation and arrangement have been made to lessen the effect of risk such as illustrating the design of recovery plan in case of natural disaster.

1. **Transference**

Transfers the risk to a different third party to reduce the risk such as illustrating during robbery claim the payment from the insurance company.

1. **Acceptance**

Accept the risk as no solution is left out except this.

1. **Assessment Risk**

In IT safety requisites, a risk is the crash of a hit multiplied by the chances of a liability being broken such as situation where crash has been rated 3 and a liability rated 9 which results to risk of 27. After computing and prioritizing the risk, one gets the critical risk in the list.

**REFERENCES :**

Whitman, M.E., Mattoro, H.J. (2013). Principles of Incident Response and Disaster Recovery

1. **Jelaskan bagaimana step step yang dilakukan oleh seorang penyerang atau hacker.**

**Answer:**

1. **Reconnaissance**

This is the primary phase where the Hacker tries to collect as much information as possible about the target. It includes Identifying the Target, finding out the target's IP Address Range, Network, DNS records, etc.

1. **Scanning**

It involves taking the information discovered during reconnaissance and using it to examine the network using tools during the scanning phase such as dialers, port scanners, network mappers, sweepers, and vulnerability scanners for seeking any information that can help perpetrate attack such as computer names, IP addresses, and user accounts.

1. **Gaining Access**

After scanning, the hacker designs the blueprint of the network of the target with the help of data collected during Phase 1 and Phase 2. Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access. The method of connection the hacker uses for an exploit can be a local area network (LAN, either wired or wireless), local access to a PC, the Internet, or offline such as stack-based buffer overflows, denial of service (DoS), and session hijacking.

1. **Maintaining Access**

Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Sometimes, hackers harden the system from other hackers or security personnel by securing their exclusive access with backdoors, rootkits, and Trojans. Once the hacker owns the system, they can use it as a base to launch additional attacks such as zombie system.

1. **Covering Tracks**

Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action by remove all traces of the attack, such as log files or intrusion detection system (IDS) alarms such as steganography, the use of tunneling protocols, and altering log files.

**REFERENCES :**

Whitman, M.E., Mattoro, H.J. (2013). Principles of Incident Response and Disaster Recovery

1. **Apa yang dimaksud dengan social engineering?**

**Answer:**

**Social engineering is a kind of attack that depends mostly on human interaction in order to gain access to systems, networks, or physical locations, or for financial needs by giving sensitive data by gaining their trust for exploiting them**.

**One Example is in 2011**, where there is data breach of security company RSA. The attacker sent two different phishing emails over two days to small groups of RSA employees. The emails contained the subject line "2011 Recruitment Plan" and contained an excel document attachment. The spreadsheet contained malicious code that installed a backdoor through an Adobe Flash vulnerability.

**Another Example is in 2015**, hackers accessed the individual AOL email account of John Brennan, at that point the chief of the CIA. One of the hackers disclosed to news sources how he utilized social engineering procedures to act like a Verizon professional and solicitation data about Brennan's account with the telecom goliath. When the hackers got Brennan's Verizon account subtleties, they reached AOL and utilized the data to accurately address security inquiries for Brennan's email account.

**REFERENCES :**

Whitman, M.E., Mattoro, H.J. (2013). Principles of Incident Response and Disaster Recovery

1. **Terangkan apa yang dimaksud dengan port? Bagaimana cara menutup atau membuka port?**

**Answer:**

**A port is an application-specific or process-specific software construct serving as a communications endpoint in a computer's host operating system associated with an IP address of the host**, as well as the **type of protocol used for communication to uniquely identify different applications or processes running on a single computer** and thereby **enable to share a single physical connection to a packet-switched network like the Internet**.

**How to Open or Close Port:**

1. **Enter the following with Zenmap Application:**

**nmap [ip\_address]**

1. **Replace the IP address with the IP address of the system testing.**

This is the basic format for Nmap, and it will return information about the ports on that system.

1. **After scanning, can Know Which be the Port is OPEN with command like:**

**nmap –open [ip\_address]**

1. **For OPENING port, with command prompt (Example Open Port 6624):**

netsh advfirewall firewall add rule name="TCP Port 6624" dir=in action=allow protocol=TCP localport=6624

1. **For CLOSING port, with command prompt (Example Close Port 8080):**

FOR /F "tokens=4 delims= " %%P IN ('netstat -a -n -o ^| findstr :8080') DO @ECHO TaskKill.exe /PID %%P

**REFERENCES :**

Whitman, M.E., Mattoro, H.J. (2013). Principles of Incident Response and Disaster Recovery