Name: Mark Joshua Q. Pata Section:BSIT 3B

**Learning Activity 5**

1. Explain the concept of MITM (Man-in-the-Middle) attack and how to prevent it? (10 points)

**Answer:** A man-in-the-middle attack is a type of eavesdropping attack, where attackers interrupt an existing conversation or data transfer. After inserting themselves in the "middle" of the transfer, the attackers pretend to be both legitimate participants. This enables an attacker to intercept information and data from either party while also sending malicious links or other information to both legitimate participants in a way that might not be detected until it is too late. Ways to prevent it is Employ VPNs (Virtual Private Network) in order to ensure the secure connections from your organization. Get browser plugins like ForceTLS of HTTPS Everywhere to secure the sensitive online transactions.

1. Explain the concept of DDOS (Distributed Denial of Service) attack and how to prevent it? (10 points)

**Answer:** Distributed denial-of-service attacks target websites and online services. The aim is to overwhelm them with more traffic than the server or network can accommodate. The goal is to render the website or service inoperable. To prevent this from happening Deploy Firewalls for Sophisticated Application attack. A good practice is to use a [Web Application Firewall (WAF)](https://aws.amazon.com/waf/) against attacks, such as SQL injection or cross-site request forgery, that attempt to exploit a vulnerability in your application itself. Additionally, due to the unique nature of these attacks, you should be able to easily create customized mitigations against illegitimate requests which could have characteristics like disguising as [good traffic](https://aws.amazon.com/blogs/security/how-to-configure-rate-based-blacklisting-with-aws-waf-and-aws-lambda/) or coming from bad IPs, unexpected geographies, etc.

1. What is your understanding about Risk, Vulnerability and Threat in a network? (10 points)

**Answer:** Risk, Vulnerability and Threats in a Network are dangerous for a system because ones attackers find out the weakness and flaws of system or network that could be exploited to cause damage attackers can easily manipulate the system they can put viruses or take over to the system or network.

1. What is brute force attack? Explain how to prevent it. (10 points)

**Answer:** Brute force attacks are [simple and reliable](https://www.varonis.com/blog/brute-force-anatomy-of-an-attack/). Attackers let a computer do the work – trying different combinations of usernames and passwords, for example – until they find one that works. Catching and neutralizing a brute force attack in progress is the best counter: once attackers have access to the network, they’re much harder to catch. To prevent it you must Limit Login Attempts, Use Captcha, and Use Strong Passwords

1. Explain vulnerabilities in network security. (10 points)

**Answer:** Vulnerabilities in network security is where attackers finds a way to breach or access your system or network attackers can run code, access a system's memory, install [malware](https://www.upguard.com/blog/malware), and steal, destroy or modify [sensitive data](https://www.upguard.com/blog/sensitive-data).

1. How to make the user authentication process more secure? Elaborate your answer. (10 points)

**Answer:** Use Two Factor Authentication (2FA) 2FA adds another layer of security to your authentication. Once you login with appropriate credentials, you will need to enter a code which can only be accessed by you, such as an email or a unique code generated by an authentication tool.

1. What is Ethical Hacking? Explain its concept. (10 points)

**Answer:** Ethical Hacking or also known as “White Hat Hacker” are security experts who performs hacking to exploit the vulnerability of a system or network and Remove it so that bad hackers can’t do any attack on that system.

1. Differentiate Security Testing from Security Scanning. (10 points)

**Answer**. A **Security testing** is a detailed hands-on examination by a real person that tries to detect and exploit weaknesses in your system.  **Security scanning** is an automated, high-level test that looks for and reports potential vulnerabilities

1. Is it right to send login credentials through email? Justify your answer. (10 points)

**Answer:** Yes so that the users can monitor if someone is using his/her account and also for validating if the one that using that account is the real owner of it.

1. Explain the concept of session hijacking. (10 points)

**Answer:** Sessions are an essential part of internet communication and are mostly web-based. Session hijacking is a web attack carried out by exploiting active web sessions. A session is a period of communication between two computer systems. A web server needs authentication since every user communication via websites uses multiple TCP/IP channels.