• Explain MAC spoofing and Email spoofing

MAC spoofing is a technique used to change a device's Media Access Control (MAC) address, which is a unique identifier for network hardware. Email spoofing involves forging the sender's address in an email to make it appear as if it came from a legitimate source, often for malicious purposes.

• Perform practical of MITM tool and social engineering Tool

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.

• Explain Kali Linux tool SYN Flooding Attack using Metasploit

#SYN flood,

and ICMP flood. SYN flood will keep sending requests to

the server until the open ports of the server are full of

requests and none of the ports can let the users connect.

Other than that, why the impact of the DoS attack is big for

an online business organization like eBay, Lazada, Shopee

and many more. Because if they got attacked by DoS attack,

the site will unable to receive the customer’s order and

because of this the organizations might lose income, it

happens when there are special events or promotions in the

online shopping site because the attackers knew there will

be many people going to buy stuff when there are

promotions and event and it is good timing for them to

launch the attack.

• Find online email encryption service

Several online email services offer encryption to enhance user privacy and security. Popular options include [ProtonMail](https://proton.me/mail), [Tutanota](https://tuta.com/), [Hushmail](https://www.hushmail.com/), and Mailfence. These services provide various features like end-to-end encryption, zero-access encryption, and options for sending encrypted emails to non-users.

• Types of Firewalls.

Firewalls come in various types, broadly categorized by their delivery method (hardware, software, or cloud) and their filtering method (packet filtering, stateful inspection, application layer, etc.)

• Explain Evading Firewalls.

Evading firewalls involves using techniques to bypass or circumvent a firewall's security measures, allowing malicious traffic or unauthorized access to a network. This can involve exploiting vulnerabilities in the firewall's configuration or using specific methods to disguise malicious traffic as legitimate.