1. Cybersecurity is the practice of protecting computer systems, networks, and data from digital attacks or unauthorized access. It encompasses various strategies;

   Some of the examples of it is.

   - Network Security: Securing networks to prevent unauthorized access or misuse. Example: Configuring firewalls to filter incoming traffic

   - Endpoint Security: Protecting individual devices like computers, smartphones, and tablets from threats. Example: Installing antivirus software to detect and remove malware from a computer

   - Cloud Security: Safeguarding data stored in cloud platforms from breaches or data loss. Example: Encrypting data before uploading it to a cloud storage service.

2. Now seen we understand what is cyber security I will give some examples of the attacks that it has .
   - Phishing: Deceptive attempts via emails or sites to gather sensitive data like passwords or credit card info by posing as a legitimate entity.
   - Malware: Software designed to harm or gain unauthorized access to systems. Includes viruses, ransomware, trojans, etc.
   - DDoS (Distributed Denial of Service): Overloads a network or system with high traffic, making it inaccessible to users.
   - Man-in-the-Middle (MitM): Intruders intercept and potentially modify or eavesdrop on communication between two parties.
   - SQL Injection: Exploits weaknesses in web applications, letting attackers access or manipulate databases by injecting malicious SQL queries.

3. Now I will tack bout the kill chain ;

   The Cyber Kill Chain is a strategic framework used to understand and combat cyber threats. It outlines the stages an attacker typically goes through to infiltrate a system.

   - Reconnaissance: Learning about potential targets within a company.
   - Weaponization: Crafting deceptive emails with malicious links or attachments.
   - Delivery: Sending these emails to targeted employees.
   - Exploitation: Employee opening the malicious link or attachment.
   - Installation: Malware gaining access to the system.
   - Command and Control: Attacker gaining control and potentially stealing sensitive data.

- Actions on Objectives: Exploiting stolen information for financial gain or causing disruptions.

4. And we have CIA triangle ;
   the CIA triangle in cybersecurity represents three core principles: Confidentiality, Integrity, and Availability.

   - Confidentiality: Protecting customer account information with encryption to prevent unauthorized access.
   - Integrity: Using checksums to verify that financial transactions have not been altered during processing or transmission.
   - Availability: Implementing redundant servers to ensure continuous availability of banking services, even during peak usage times or in the event of a hardware failure.

5. SOME OF THE ACTIVETIS THAT I DID .

- Ipconfig (Windows) / Ifconfig (Unix/Linux): Displays and manages network configuration details.
- ifconfig: Configures and displays network interface info (IP addresses, network status) in Unix/Linux.
- whoami: Displays the username of the active session/user in Unix-like systems.
- Tracing Hops to a Website: Shows the intermediary points ("hops") data travels through to reach a website.
- Finding Primary Nameservers: Identifies the primary nameservers managing a website's DNS.
- whois: Retrieves domain registration details (registrar, registration date, contact info) for a domain.
- ping: Checks network connectivity by sending data packets and measuring round-trip time.
- Querying MX Records: Uses nslookup to find Mail Exchange (MX) servers handling email delivery for a domain.
- This condensed version offers a brief overview of each command's purpose without extensive detail.
- Nmap: Scans networks to discover hosts, services, and vulnerabilities.
- Whois: Retrieves domain registration information.

6. Now I will go to the IOT

   IoT, or the Internet of Things, refers to the network of interconnected devices embedded with sensors, software, and connectivity, allowing them to collect and exchange data.So if any one remember when we where visited by the smart rasa and they explain to use about the IOT and how its going to change the word and I will go thro some staff the they explained to us so

    - one of these this is the first iot that was appled to a vending machines in 1982 connected a Coca-Cola vending machine to the internet. o remotely check the status of the machine and see if it was stocked with cold drinks
7. some of the items that use the iot in our life rghit now like the ring pull and the smoke detecter

8. there are some layers in the IOT which is
    - Devices: Examples - Sensors, actuators, wearables, smart appliances (thermostats, cameras, lights).

    - Connections: Examples - Wi-Fi, Bluetooth, Zigbee, cellular networks.

    - Platform: Examples - Microcontrollers, embedded systems, edge computing platforms (AWS IoT Greengrass, Azure IoT Edge).

    - Cloud: Examples - Cloud computing platforms (AWS, Azure, Google Cloud), IoT application development platforms (IBM Watson IoT, ThingWorx).

    - Applications: Examples - Smart city solutions, healthcare monitoring, predictive maintenance, consumer applications (smart home apps).

9. "Through this course, I've expanded my understanding of cybersecurity, website safety, and protecting my devices. I've encountered situations where my laptop was compromised due to unknown downloads or unsafe websites, resulting in frustrating resets. Learning about the kill chain, CIA triangle, and various cyber threats has equipped me with fundamental safety measures. Now, I have the knowledge to safeguard my devices and guide others to prevent hacking incidents."