DAY 1

**Cyber Security:**

Cybersecurity refers to the practice of protecting systems, networks, and programs from digital attacks. It aims to reduce the risk of cyber attacks and unauthorized access to systems.

* Key components of cybersecurity include:
* Network Security: Focus onprotecting computer networks from unauthorized access, intrusion, and disruption.
* Application Security: Focus on ensuring the security of software applications.
* Information Security: protecting information in all its forms**.**
* System Security: Focus on protecting a computer system and its data from unauthorized access.
* Types of Cyber attacks:
* Malware attack: Malicious software that can steal data, damage systems, or make them inoperable. Malware can include viruses, worms, spyware.
* Phishing Attack: A cyber attack that uses social engineering to trick people into giving away personal information. Phishing attacks can be conducted via email, phone calls, or text messages.
* Password Attack: A cyberattack that attempts to gain access to a user's account by guessing or cracking their password.
* Ransomware Attack: Malware encrypts files and demands ransom for decryption, often spread via phishing emails or software vulnerabilities.
* DDoS (Distributed Denial of Service): Attackers overload a network or website with excessive traffic, causing service disruption. Mitigation includes firewalls, traffic monitoring, and DDoS protection services.
* DoD (Drive by Download): Malicious software is automatically downloaded when visiting compromised websites. Prevention includes updating browsers, using firewalls, and avoiding suspicious links.
* Cybersecurity Best Practices:
* Strong passwords
* Software updates
* Use antivirus software
* Back up your data

**Asset Management**:

Asset management is the process of managing a company's assets to maximize their value and achieve business goals.

**IT asset management (ITAM)**: IT asset management is the process of managing an organization's IT assets throughout their lifecycle. This includes hardware, software, and network resources.

* Benefits of ITAM:
* Cost control
* Efficiency
* Risk management
* Key aspects of IT Asset Management:
* Hardware Asset Management
* Software Asset Management
* Licenses Management
* Compliance Management

**How does IT Asset Management work ?**

1. Discovery and inventory
2. Reporting
3. Classification and categorization
4. Optimization
5. Asset tracking and monitoring
6. Software license management
7. Retirement

**Cyber Security Asset Management:**

Cybersecurity asset management (CSAM) is the process of identifying, tracking, and managing all the things in your organization's IT environment that are important for security.

* Benefits of CSAM:
* Improved security posture**:** Reduced risk of cyberattacks and data breaches.
* Increased efficiency**:** Streamlined security operations and faster incident response.
* Reduced costs**:** Avoiding costly security incidents and regulatory fines.

**Emerging trends in Cyber Security:**

1. AI and machine learning:

* AI can automate threat detection and response, analyze data for patterns, and predict potential threats.
* AI and machine learning can also be used to create more sophisticated attacks, such as phishing emails.

1. Remote work:

* The rise of remote work has increased the need for data protection.
* Remote work has also created new targets for ransomware.

1. IoT vulnerabilities:

* As the number of IoT devices increases, so do the attack vectors for cybercriminals
* Cybercriminals can exploit unpatched devices in smart homes, industrial environments, and critical infrastructure.

**Case Study on any Cyber Attack:**

Case Study: Password Attack on Yahoo (2013-2014)

Overview

Yahoo suffered one of the largest password attacks in history, affecting 3 billion user accounts. The breach, which began in 2013 and was discovered in 2016, involved hackers stealing usernames, passwords, security questions, and personal data.

How the Attack Happened

1. Credential Theft – Hackers used phishing to gain access to Yahoo’s internal systems.
2. Password Cracking – Weakly encrypted or reused passwords were exploited to access multiple accounts.
3. Data Exfiltration – Hackers stole email addresses, phone numbers, and hashed passwords.

Impact

* 3Billion Accounts compromised, exposing personal and financial data.
* Reputational Damage led to Yahoo’s valuation dropping by $350 million during its Verizon acquisition.
* Legal Consequences, including multiple lawsuits and a $35 million SEC fine for failing to disclose the breach.

**Cyber security asset management vs it asset management difference and similarities**

* Difference

|  |  |  |
| --- | --- | --- |
| **Feature** | **IT Asset Management (ITAM)** | **Cybersecurity Asset Management (CSAM)** |
| Primary Goal | Optimize IT asset lifecycle for efficiency and cost-effectiveness | Identify and manage assets to reduce cyber risks |
| Focus | Hardware, software, licenses, contracts | Devices, users, cloud |

* Similarities
* **Lifecycle management:** Both track assets throughout their lifecycle, from purchase to disposal. This helps with efficient use (ITAM) and ensuring security throughout (CSAM).
* **CMDBs:** Configuration Management Databases are often used to store and manage asset information for both ITAM and CSAM.
* **Reliance on data:** Both need accurate and up-to-date data about assets. This data informs decisions about cost optimization (ITAM) and security measures (CSAM).