Cyber security internship

Assignment-1

What is cyber security?

- Cybersecurity is the practice of protecting internet-connected systems, including hardware, software, and data, from cyber attacks. It involves preventing unauthorized access, exploitation, and theft of data while ensuring the integrity and availability of information. Cybersecurity measures are put in place to defend against a wide range of threats, including malware, ransomware, phishing attacks, and other malicious activities that can compromise the confidentiality, integrity, and availability of digital assets.
- Effective cybersecurity involves a combination of technologies, processes, and practices designed to safeguard networks, devices, and data from attack, damage, or unauthorized access. This includes implementing firewalls, encryption, antivirus software, multi-factor authentication, intrusion detection systems, and other tools to identify and thwart potential threats. Additionally, security policies, employee training, incident response plans, and ongoing risk assessments are essential components of a comprehensive cybersecurity program.
- As digital technologies continue to advance and become more integrated into our daily lives, the importance of strong cybersecurity practices cannot be overstated. From protecting personal information stored on our devices to safeguarding critical infrastructure and national security interests, cybersecurity efforts are crucial for maintaining trust, privacy, and security in the digital age.

Passive Attack

- A passive attack is a type of cyber attack in which an unauthorized party observes or monitors data transmissions without altering or disrupting the communication. The primary goal of a passive attack is to gain unauthorized access to sensitive information or data without alerting the target or the network's security measures.
- Unlike active attacks, which involve directly modifying or disrupting network communications, passive attacks are more covert in nature. Common methods of passive attacks include eavesdropping on network traffic, capturing data packets, and analyzing information flowing through a network without raising suspicion. These attacks are often carried out using tools and techniques that allow the attacker to intercept and analyze data without leaving any obvious traces.
- The information obtained through passive attacks can be used for various malicious purposes, including identity theft, espionage, or gaining insight into an organization's sensitive data. For example, an attacker might eavesdrop on unencrypted communication between two parties to capture login credentials, financial information, or other sensitive data. This stolen information can then be exploited for financial gain or as a means to compromise the security of a targeted system or network.

HACKERS CATEGORIES

Hackers can be categorized into several distinct groups based on their motivations, skills, and activities. Here are the common categories of hackers:

1. Black Hat Hackers:

Black hat hackers, also known as “crackers,” engage in hacking activities for malicious purposes. They exploit vulnerabilities in computer systems, networks, and software to gain unauthorized access, steal sensitive information, disrupt operations, deploy malware, or cause other forms of damage. Black hat hackers often operate with the intention of personal gain, financial profit, or to further their own agendas.

2. Grey Hat Hackers:

Grey hat hackers operate in a middle ground between black hat and white hat hackers. They may engage in hacking activities without malicious intent but without explicit authorization, sometimes for the purpose of demonstrating vulnerabilities or drawing attention to security shortcomings. While their actions may not be explicitly malicious, they still operate in legally ambiguous territory by accessing systems and data without permiKiddies

3. Script Kiddies:

Script kiddies are individuals who use pre-existing, automated scripts and tools, without necessarily having a deep understanding of how they work, to launch simple, unsophisticated attacks. They often lack the technical expertise and knowledge of more advanced hackers, and their activities are generally limited to executing known, easily accessible attack methods.

Essential Terminologies :

1. **Malware:** Malicious software designed to infiltrate or damage a computer system without the owner's consent. Common types of malware include viruses, worms, trojans, ransomware, and spyware.

2. **Phishing:** A type of cyber attack in which attackers impersonate legitimate entities through emails, messages, or websites to deceive individuals into providing sensitive information such as login credentials or financial details.

3. **Encryption:** The process of converting data into a code to prevent unauthorized access. Encrypted data can only be accessed by authorized parties who possess the required decryption key.

4. **Firewall:** A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewalls act as a barrier between trusted internal networks and untrusted external networks, such as the internet.

5. **Vulnerability:** A weakness in a system's defenses that could be exploited by an attacker to compromise the integrity, availability, or confidentiality of the system. Identifying and patching vulnerabilities is crucial for maintaining a secure environment.

Top 10 Most Notorious Hackers Of All Time In This Internet World:

- 1.Kevin Mitnik
- 2.Anonymous
- 3.Adrian Lamo
- 4.Albert Gonzalez
- 5.Matthew Bevan And Richard Pryac
- 6.Jeanson James Ancheta
- 7.Michael Calce
- 8.Kevin Poulsen
- 9.Jonathan James
- 10.Astra

Phases of Hacking

- Hacking can encompass different phases, depending on the nature of the attack and the intentions of the hacker. While not all hacking activities are malicious, it is essential to understand the common phases involved in unauthorized or illicit hacking attempts. Here are the typical phases of a hacking process:
- 1. **Reconnaissance** (Information Gathering):** This phase involves gathering information about the target, such as its network infrastructure, operating systems, applications, and potential vulnerabilities. Hackers may use open-source intelligence (OSINT) techniques, network scanning tools, and social engineering to collect data.
- 2. **Scanning:** In this phase, the hacker uses various tools to identify specific information about the target, such as open ports, network services, and system architecture. The goal is to identify potential entry points and weak spots within the target's infrastructure.
- 3. **Gaining Access:** Once the hacker identifies potential vulnerabilities or entry points, they attempt to exploit them to gain unauthorized access to the target system or network. This may involve using techniques such as password cracking, exploiting software vulnerabilities, or leveraging social engineering to compromise user credentials.
- 4. **Maintaining Access:** After successfully penetrating the target system, the hacker may take steps to ensure continued access and control over the compromised environment. This involves installing backdoors, creating additional user accounts, or establishing remote access tools to maintain a persistent presence within the system.

Introduction To Networking

Networking is a fundamental concept in the field of information technology, serving as the backbone for communication and data exchange between devices, systems, and users.

components and concepts in networking include:

1. **Devices:** Devices such as computers, routers, switches, and access points form the building blocks of a network. These devices play specific roles in facilitating communication, routing data, and providing connectivity.
2. **Protocols:** Networking protocols define the rules and conventions for communication between devices on a network. Examples of protocols include TCP/IP (Transmission Control Protocol/Internet Protocol), which underpins the internet, and HTTP (Hypertext Transfer Protocol), used for web browsing
3. **Topologies:** Network topologies refer to the physical or logical layout of devices and connections within a network. Common topologies include star, bus, ring, and mesh configurations, each with its own advantasing and Routing

OSI model layers

- **Application Layer:**The Application layer is the top layer of the OSI model.Its closest to the user –application.The user facing software directly interacts with the applications layer through sharing,msg handling or data base access.
- Protocols :Http,FTP, SMTP.
- **Presentation layer:**The P.L is about data translation and formatting.In this layer,protocols things like encryption,decryption,compression and decompression.
- The main goal of P.L is transform data.
- **Session Layer:** The session layer handles the communication between two or more computers,protocols are to create a session b/w entities.The S.L handles the connection and authentication b/w a client or server.
- **Transport Layer:**Transport layer is to accept data from the S.L,split it up into small units if need be,pass these to the n/w layer and ensure that all the poeces arrive correctly at other layer.

- **Network Layer:** The N/L converts the received data into data packets for sharing communication channel.
- **Data link layer:** The data link layer is responsible for transferring messgaes from a given node to all other nodes in n/w.
- Organizes bits into frames
- **Physical Layer:** It describes the way data is actually transmitted on the n/w medium.

What is webhook

- A webhook is a method for enabling real-time communication between different applications or systems over the web. It allows one application to send automatic notifications or trigger a specific action in another application when a certain event occurs. This can be accomplished by setting up a webhook in one application and providing a URL endpoint where the other application can send data.
- When a specific event, such as a new order being placed or a customer signing up, occurs in the originating application, it will send a HTTP POST request to the URL specified in the webhook. The receiving application then processes the data and can take appropriate actions based on the information received.
- Webhooks are commonly used for integrating different systems and automating processes. For example, an e-commerce platform could use webhooks to notify a shipping service when a new order is placed, triggering the shipment process. Similarly, a messaging app could utilize webhooks to send notifications to an external system when a user completes a certain action.

- CYBER SENSE+ COMMON SENSE=CYBER SECURITY