SWAMI VIVEKANANDA INSTITUTE OF SCIENCE & TECHNOLOGY

Dakshin Gobindapur, Sonarpur, Kolkata – 7000145

Affiliated to

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL

(Formerly Known as West Bengal University of Technology)

Department of Computer Science & Engineering

Continuous Assessment – 2

Topic: Types of Cyber Attacks…….

Name of the Student : Aritri Thakur

University Roll No. : 24100121028

Year : 4th Semester : 8th

Name of the Subject: Cyber Law and Ethics

Subject Code : OEC-CS801B Session: 2024-2025

1. Introduction

In the digital age, the reliance on computer systems, networks, and data is paramount. However, with this reliance comes the growing threat of cyber attacks. These attacks can target individuals, organizations, and even governments, leading to significant financial and data losses. Understanding the types and nature of these cyber attacks is crucial for developing robust cybersecurity measures.

2. Definition of Cyber Attacks

A cyber attack is any attempt to gain unauthorized access to a computer system, network, or data, usually with the intent to cause harm. Cyber attacks can take many forms, from stealing sensitive information to disrupting critical systems. The motive behind these attacks can range from financial gain to political motives, or simply the desire to cause chaos.

3. Explanation of Different Types of Cyber Attacks

i. Malware

Malware is malicious software designed to damage, disrupt, or gain unauthorized access to computer systems. Common types of malware include viruses, worms, Trojan horses, and ransomware.
Example: WannaCry ransomware attack in 2017 affected over 200,000 computers across 150 countries, encrypting files and demanding ransom payments in Bitcoin.

ii. Phishing

Phishing attacks involve sending deceptive emails or messages that appear to come from legitimate sources, tricking individuals into revealing sensitive information such as passwords or credit card numbers.
Example: The 2016 phishing attack on the Democratic National Committee (DNC) led to the theft of thousands of emails, which were later leaked, influencing the U.S. presidential election.

iii. Distributed Denial of Service (DDoS)

DDoS attacks flood a target system with excessive traffic, rendering it unavailable to legitimate users. These attacks often involve multiple compromised systems.
Example: In 2016, a massive DDoS attack on DNS provider Dyn caused widespread internet outages, affecting major websites like Twitter, Netflix, and Reddit.

iv. Man-in-the-Middle (MitM)

MitM attacks occur when an attacker secretly intercepts and relays communications between two parties, often to steal data or manipulate the communication.

Example: The 2015 attack on GitHub involved MitM techniques that disrupted services by overwhelming the platform with traffic.

v. SQL Injection

SQL injection attacks target databases by inserting malicious SQL queries through vulnerable input fields, allowing attackers to manipulate or retrieve data.

Example: The 2019 SQL injection attack on the European Central Bank's website led to the theft of sensitive contact information.

vi. Zero-Day Exploit

A zero-day exploit takes advantage of software vulnerabilities that are unknown to the software developer. These attacks are particularly dangerous because they can be executed before a patch is available.

Example: The Stuxnet worm exploited a zero-day vulnerability to sabotage Iran's nuclear program in 2010.

4. Case Study: The Equifax Data Breach

i. Background

In 2017, Equifax, one of the largest credit reporting agencies in the U.S., suffered a massive data breach that exposed the personal information of approximately 147 million people.

ii. Attack Method

The breach was caused by a vulnerability in a web application, which was exploited using an Apache Struts framework vulnerability. This allowed attackers to gain access to sensitive data, including Social Security numbers, birth dates, addresses, and even driver's license numbers.

iii. Impact

The breach had significant consequences, including a $700 million settlement, widespread distrust among consumers, and a considerable drop in Equifax's stock price.

iv. Lessons Learned

The Equifax breach highlighted the importance of timely software updates, strong cybersecurity practices, and the need for organizations to protect sensitive data with multiple layers of security.

5. Conclusion

Cyber attacks are a growing threat in our increasingly connected world. Understanding the various types of attacks, their methods, and their potential impact is critical for developing effective cybersecurity strategies. As

technology continues to evolve, so too will the methods employed by cybercriminals. Continuous vigilance, education, and adaptation are necessary to protect against these ever-present threats.

6. Bibliography

i. Cloudflare. (2016). *What is a DDoS Attack? Causes and Mitigation*. Retrieved from https://www.cloudflare.com/learning/ddos/what-is-a-ddos/

ii. Crowdstrike. (2016). *Phishing Attack on the Democratic National Committee*. Retrieved from https://www.crowdstrike.com/blog/dnc-phishing-incident/

iii. Kaspersky. (2017). *WannaCry Ransomware: How It Happened and How to Protect Yourself*. Retrieved from https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

iv. Norton. (2010). *What is Stuxnet? A Guide to the World's First Digital Weapon*. Retrieved from https://us.norton.com/internetsecurity-emerging-threats-what-is-stuxnet.html

v. OWASP Foundation. (2019). *SQL Injection Overview and Mitigation*s. Retrieved from https://owasp.org/www-community/attacks/SQL_Injection

vi. Symantec. (2015). *GitHub DDoS and Man-in-the-Middle Attack*. Retrieved from https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/github-attack

vii. U.S. House of Representatives Committee on Oversight and Government Reform. (2018). *The Equifax Data Breach: How It Happened and What Needs to Change*. Retrieved from https://oversight.house.gov/report/the-equifax-data-breach/