SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NAAC-UGC with ‘A’ Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

DEPARTMENT OF INFORMATION TECHNOLOGY

Course Code and Name : 19IT602– CRYPTOGRAPHY AND CYBER SECURITY

III YEAR / VI SEMESTER

Unit 1: INTRODUCTION TO NETWORK AND CYBER SECURITY

Topic : CYBER THREATS

CYBER THREATS- INTRODUCTION

- A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general.
- Cyber threats include computer viruses, data breaches, Denial of service (DoS) attacks, and other attack vectors.
- Cyber threats also refer to the possibility of a successful cyber attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property, or any other form of sensitive data.

TYPES OF CYBER THREATS

- Malware
- Ransomware
- Distributed denial of service (DDoS) attacks
- Spam and Phishing
- Corporate Account Takeover (CATO)
- Automated Teller Machine (ATM) Cash Out

MALWARE

- Malware is also known as malicious code or malicious software.
- It is done secretly and can affect your data, applications, or operating system.
- Malware has become one of the most significant external threat to systems.
- Malware can cause widespread damage and disruption, and requires huge efforts within most organizations.

RANSOMWARE

- Ransomware prevents or limits users from accessing their system via malware.
- Cyber criminals will request ransom for this private key.
- Cyber criminals are using encryption as a weapon to hold the data hostage.

DISTRIBUTED DENIAL OF SERVICE(DDOS) ATTACKS

- DDoS attacks make an online service unavailable by overwhelming it with excessive traffic from many locations and sources.
- Website response time slows down, preventing access during a DDoS attack.
- Cyber criminals develop large networks of infected computers called Botnets by planting malware.
- A DDoS attack may not be the primary cyber crime. The attacks often create a distraction while other types of fraud and cyber intrusion are attempted.

SPAM AND PHISHING

- Spam includes unwanted, unsolicited, or undesirable messages and emails.
- Phishing is a form of social engineering, including attempts to get sensitive information.
- Cyber criminals pretend to be an official representative sending you an email or message with a warning related to your account information.
- The message will often ask for a response by following a link to a fake website or email address where you will provide confidential information.
- The FBI developed tips for preventing phishing attacks.

CORPORATE ACCOUNT TAKEOVER (CATO)

- CATO is a business entity theft where cyber thieves impersonate the business and send unauthorized wire and ACH transactions.
- Many businesses are vulnerable to a CATO attack. Institutions with weak computer safeguards and minimal controls over online banking systems are easy targets.
- This form of cyber crime can result in large losses. Cyber criminals use malware to infect a computer through e-mail, websites, or malware disguised as software.

References

- William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006.
- Behrouz A. Foruzan, Cryptography and Network Security, Tata McGraw Hill 2007.