SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

Unit III- Network Threats

Topic : Worms –Virus – Spam's

worm virus

- The worm virus exploits vulnerabilities in your security software to steal sensitive information, install backdoors that can be used to access the system, corrupt files, and do other kinds of harm.
- Worms **consume large volumes of memory**, as well as bandwidth.

- A worm is **a harmful software** (virus) that repeats itself as it **moves from computer to computer**, **leaving copies** of itself in each computer's memory.

- Worms then **propagate through a user's email** account and address book to contacts.

Types of computer worms

Email worms

- To spread email worms **create and send outbound messages** to all addresses in a user's contact list.
- When the recipient opens the mail, it contains a **malicious(unwanted files) executable** file that infects the new system.
- Successful email worms typically use **social engineering and phishing approaches** to persuade users to open the linked file.

File-sharing worms

- File-sharing worms are **malicious programs** that hide as media files.
- A worm that **spreads malware via USB devices** infected with the host file and malware that targets supervisory control and data acquisition systems.

Crypto worms

- Crypto worms **encrypt data on the victim's computer system**.

- This worm can be used **in ransomware attacks**, in which the attackers contact the victim and seek payment in exchange for a key to decrypt their files.

Internet worms

- Some computer worms are designed to attack **important websites** that have weak security.

- They can infect a computer viewing the website if they can infect the site.

- **Internet worms then propagate to other devices connected to the infected PC via internet and private network connections.**

Worms that spread via instant messaging

Instant messaging worms, like email worms, are disguised as attachments or links, which the worm uses to spread throughout the infected user's contact list.

Prevent worms

- Make sure you have a **good internet security software** solution to help you block these dangers.
- **Anti-phishing technologies,** as well as defenses against viruses, spyware, ransomware, and other online threats, should be included in a solid solution.
- Another popular method for hackers to transmit worms is through **phishing (**and other types of malware).
- When opening unwanted emails, be particularly cautious, especially those from unknown senders that include attachments or questionable **URLs.**

virus

- A computer virus is a **type of malicious software**, or malware, that spreads between computers and causes damage to data and software.
- Computer **viruses aim to disrupt systems, cause major operational issues, and result in data loss and leakage.**
- or
- A virus is a **computer code or program**, which is capable of affecting your **computer data badly by corrupting or destroying them**.
- Computer virus has the tendency to make its **duplicate copies** at a swift pace, and also spread it across **every folder** and damage the data of your computer system.
- A computer virus is actually a **malicious software program** or "malware" that, when infecting your system, replicates itself by modifying other computer programs and inserting its own code.

Types of Virus

Worms

- This is a **computer program that replicates itself at a swift pace**.
- Unlike a computer virus, it is self-contained and hence does not need to be part of another program to propagate itself.

Trojan Horse

- A Trojan Horse is also a **sort of destructive program** that remains **disguised in a normal software program.**
- It is not exactly a virus, as it cannot replicate itself. However, there is possibility that virus program may remain concealed in the Trojan Horse.

Bombs

- It is similar to Trojan Horse, these include a timing device and hence it will go off only at a particular date and time.

How Does Virus Affect

- By downloading files from the Internet.
- During the removable of media or drives.
- Through pen drive.
- Through e-mail attachments.
- Through unpatched software & services.
- Through unprotected or poor administrator passwords.

Impact of Virus

- Disrupts the normal functionality of respective computer system.
- Disrupts system network use.
- Modifies configuration setting of the system.
- Destructs data.
- Disrupts computer network resources.
- Destructs of confidential data.

Virus Detection

- The most fundamental method of detection of virus is to **check the functionality of your computer system**
- A virus affected computer **does not take command properly**.
- if there is **antivirus software in your computer system**, then it can easily check programs and files on a system for virus signatures.

Virus Preventive Measures

- Installation of an effective antivirus software.
- Patching up the operating system.
- Patching up the client software.
- Putting highly secured Passwords.
- Use of Firewalls.

Most Effective Antivirus

- McAfee Antivirus Plus
- Symantec Norton Antivirus
- Avast Pro Antivirus
- Bitdefender Antivirus Plus
- Kaspersky Anti-Virus
- Avira Antivirus
- Webroot Secure Anywhere Antivirus
- Quick Heal Antivirus
- ESET NOD32 Antivirus

Spam

- Spam is defined as **irrelevant or unsolicited messages sent to a large number of Internet users,**

- For illegitimate advertising, and other activities such as phishing, and spreading malware.

Identification of a Spam :

1.Messages that basically do not include your email address in the TO: or CC: fields are common forms of spam.

2.The messages that contain poor spelling and grammar.

3.The message is asking for your personal details for example your bank details or the pin number.

4. The links in the message are dubious, for example, www.amazam.com instead of *www.amazon.com.*

5. The actual email address does not match the name displayed, example the name displayed on the email is “Amazon Customer Services” but the actual email id is shop123@buzz.com

6. Asking you to complete the action or the task, which you didn’t initiate, for example, it is showing to click on the link to get a lottery amount.

Protection Against Spam

There is a certain method through which the user can protect himself from spam messages :

1.Delete emails that are sent from completely unknown sources.

2.Keep software and security patches up to date.

3.If you suspect any spam message or email do not open any link.

4.Install a good antivirus and spam filtering or blocking software.

5.Do not buy anything advertised from spam emails.

Any Query????

Thank you……