Parul®
University

Cyber Security and Forensics - I
05201296

Prof. Dipak L. Agrawal, Assistant Professor
Faculty of IT & Computer Science

CHAPTER-2

Security Threats

Topics

- Types of security threats- worms, viruses, Trojan horse, malware, malicious spyware, adware, botnet, spam, phishing, stack and buffer overflow

1. Types of security threats

Introduction to Security Threats

- Network threats are known flaws or weaknesses in hardware, software, or other organizational possessions, which can be exploited by attackers.
- Types of Security Threats: There are four threats as below:
  - Enable your network visibility: The initial step for setting up your organization safeguard and different individuals from your security group to distinguish network dangers and weaknesses is to empower your entire organization deceivability.
  - Set up computer and network access: You need to build your computer and network access to control who can access your network and the level of grant they can have. Not every user should be given equal access to the entire network.

3. Firewall: Setting up a network firewall thwarts illegal access and internet-based outbreaks from diffusing into your computer networks. Your network firewall supervises the flow of computer data traffic permitted to traverse your network.
4. Bound access to updates and installations: Malicious hackers can penetrate your computer network through out-of-date software for antivirus, operating systems, device drivers, firmware, and other endpoint mechanisms.

The other threats are as under

- The other threats are as under,
- Viruses,
- Worms,
- Trojan horse,
- Malware,
- Malicious spyware,
- Adware,
- Botnet,
- Spam,
- Phishing,
- Stack,
- Buffer overflow

- **Virus:**

What is Virus?

A piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

Von Neumann's design for a self-reproducing computer program is considered the world's first computer virus, and he is considered to be the theoretical "father" of computer virology.

1. Resident Virus: OS file or program will be effected ,Loaded in RAM, corruption of files and programs
2. Multipartite Virus: Multiple parts, OS, Files
3. Direct Action Virus: attacks on .exe and .com
4. Web Browser Hijacker: bypass access controls, steal your information from your web browser. It will redirect to Some malicious web sites

5. Overwrite Virus: This includes worms, adware, malware, Trojan, and ransomware.

Worm? Replicates itself…like virus

Adware? Unwanted Advertisements

Malware? Creates all problems using malicious software.

Trojan? Can change the identity with legitimate software and to be entered as malicious software.

Ransomware? It is a subset of malware in which the data on a victim's computer is locked

6. Web Scripting Virus: virus lives links, ads and layouts of the website.
7. Boot Sector Virus: Harms the boot actions of PC., corrupt the O.S.
8. Macro Virus: Macro viruses target applications and software that contain macros(.doc, .xls, Documents)
9. Directory Virus: change file paths
10. Polymorphic Virus: method of encoding or encryption every time they infect a system
11. File Infector Virus: Slow down and affects the .exe or .com files
12. Encrypted Virus: Cannot be find by Anti-virus and affects the speed of computer

13. Companion Virus: Affects all the folders and files which are at same place
14. Network Virus: Affects the shared resources and spread through the LAN
15. Non-resident Virus: It affects when clicked but not stored on computer
16. Stealth Virus: Can’t be recognized by anti-virus because they will be temporarily removes itself and will not be deleted
17. Sparse Infector: Occasional affecter
18. Space filler Virus: space fillers attach themselves to the file and can alter the programs
19. FAT Virus: ruins file allocation system.

- **Worms:**
- A PC worm is a kind of malware that spreads duplicates of itself from PC to PC. A worm can repeat itself with no human connection, and it doesn't have to append itself to a product program so as to cause harm.
- Worms can be communicated through programming weaknesses. Or then again PC worms could show up as connections in spam messages or texts (IMs). When opened, these documents could give a connect to a malignant site or consequently download the PC worm.
- Worms can adjust and erase records, and they can even infuse extra pernicious programming onto a PC.

- There is no widespread characterization of PC worms, however they can be composed into types dependent on how they are conveyed between PCs. The five normal sorts are as per the following:

1. Web Worms

- As they do with PC organizations, PC worms likewise target famous sites with lacking security.

2. Email Worms

- Email worms are regularly dispersed through undermined email connections. They for the most part have twofold augmentations (for instance, .mp4.exe or .avi.exe) so the beneficiary would believe that they are media records and not vindictive PC programs.

3. Texting Worms

- Texting worms are actually equivalent to email worms, the main distinction being their strategy for appropriation. By and by, they are covered as connections or interactive connects to sites. They are frequently joined by short messages like "LOL" or "You need to see this!" to fool the casualty into imagining that their companion is sending them an entertaining video to take a gander at.

4. Record (File) Sharing Worms

- Albeit unlawful, document sharing and distributed record moves are as yet utilized by a great many individuals around the globe. Doing as such, they are accidentally presenting their PCs to the danger of record sharing worms. Like email and texting worms, these projects are veiled as media records with double expansions.

5. IRC Worms

- Web Relay Chat (IRC) is an informing application that is generally obsolete these days yet was extremely popular when the new century rolled over. Same likewise with the present texting stages, PC worms were appropriated by means of messages containing connections and connections. The last was less powerful because of an additional layer of security that provoked clients to acknowledge approaching documents before any exchange could happen.
- Some Examples of worms: The Morris Worm, 1988
- The Storm Worm, 2007
- SQL Slammer, 2003

- **Trojan horse**
- A Trojan horse, or Trojan, is a type of malicious code or software that looks valid but can take control of your PC. A Trojan is aimed to damage, disrupt, steal, or in general inflict some other destructive actions on your computer data or on network.
- A Trojan horse, or Trojan, is a sort of malevolent code or programming that looks genuine yet can assume responsibility for your PC. A Trojan is intended to harm, disturb, take, or when all is said in done incur some other unsafe activity on your information or organization.

- **Malware**
- Malware is the united term for a number of nasty software variations, including viruses, ransomware and spyware. Shorthand for malicious software, malware typically contains of code developed by cyber attackers or hackers, designed to cause widespread damage to data and systems or to gain illegal access to a network.
- Malware is normally conveyed as a connection or document over email and requires the client to tap on the connection or open the record to execute the malware.

- **Malicious spyware**
- Spyware is undesirable programming that invades your computing gadget, taking your web utilization information and sensitive data. Spyware is delegated a sort of malware — noxious programming intended to access or harm your PC, regularly without your insight. Spyware assembles your own data and transfers it to publicists, information firms, or outside clients.
- Spyware is utilized for some reasons. Typically it plans to track and sell your web utilization information, catch your MasterCard or ledger data, or take your own personality. How? Spyware screens your web movement, following your login and secret phrase data, and keeping an eye on your delicate data.

- **Adware**
- Adware, or publicizing upheld programming, is programming that shows undesirable commercials on your PC. Adware projects will in general serve you spring up promotions, can change your program's landing page, include spyware and simply barrage your gadget with commercials. Adware is a more compact name for conceivably undesirable projects. It's not exactly an infection and it may not be as clearly malevolent as a great deal of other tricky code gliding around on the Internet.

- **Botnet**
- Botnets are Networks of PCs contaminated by malware, (for example, PC viruses, key loggers and different malevolent codes) and controlled distantly by criminals, typically for monetary profit or to dispatch assaults on sites or organizations.
- On the off chance that your PC is tainted with this malware and part of a botnet, it conveys and gets guidelines about what it should do from "order and control" PCs found anyplace around the world. What your PC does relies upon what the cybercriminals are attempting to achieve.

- **Spam**
- Spam is any sort of undesirable, spontaneous computerized correspondence, regularly an email that gets conveyed in mass. Spam is a gigantic exercise in futility and assets. The Internet specialist co-ops (ISP) convey and store the information. At the point when programmers can't take information data transmission from the ISPs, they take it from singular clients, hacking PCs and subjugating them in a zombie botnet. Programming suppliers contribute assets making email applications that attempt to sift a large portion of the spam through.

- **Phishing**
- Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity.
- Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.
- It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

- **Examples of Phishing**

Through Email

- Urgent Action is required
- Link of Fake website
- Popup
- Request for personal credentials
- Lottery Offers

Stack and Buffer overflow

- A buffer is a holding zone for data. To speed preparing online, numerous product programs utilize a memory area to store changes to information, at that point the data in the support is replicated to the disk.
- At the point when more data is placed into the support than it can deal with, a buffer overflow happens.
- Overflows can be caused purposely by the hackers and afterward abused to run noxious code.
- There are two kinds of floods: stack and heap. The stack and the pile are two territories of the memory structure that are assigned when a program is run.
- Capacity calls are put away in the stack, and powerfully assigned factors are put away in the load. A specific measure of memory is allotted to the cradle.

- Static variable stockpiling (factors characterized inside a capacity) is alluded to as stack, since they are really put away on the stack in memory. Load information is the memory that is progressively dispensed at runtime, for example, by C's malloc() function. This information isn't really put away on the stack, yet some place in the midst of a goliath "store" of brief, expendable memory utilized explicitly for this reason. All things considered abusing a load support flood is much more included, on the grounds that there are no advantageous edge pointers (as are on the stack) to overwrite.
- Assailants can utilize cushion floods in the store to overwrite a secret key, a filename, or other information. In the event that the filename is overwritten, an alternate record will be opened.

- Static variable stockpiling (factors characterized inside a capacity) is alluded to as stack, since they are really put away on the stack in memory. Load information is the memory that is progressively dispensed at runtime, for example, by C's malloc() function. This information isn't really put away on the stack, yet some place in the midst of a goliath "store" of brief, expendable memory utilized explicitly for this reason. All things considered abusing a load support flood is much more included, on the grounds that there are no advantageous edge pointers (as are on the stack) to overwrite.
- Assailants can utilize cushion floods in the store to overwrite a secret key, a filename, or other information. In the event that the filename is overwritten, an alternate record will be opened.

DIGITAL LEARNING CONTENT

Parul® University

www.paruluniversity.ac.in