UNIT -III: Tools and Methods Used in Cybercrime

Unit III: Tools and Methods used in Cybercrime: Proxy servers and Anonymizers – Phishing – Password Cracking – Keyloggers and Spywares –Virus and Worms –Trojan Horses and Backdoors – Steganography – DoS and DDoS attacks.

Introduction

Different forms of attacks through which attackers target the computer systems are as follows:

1. Initial uncovering:

- Two steps are involved here.

i. In the first step called as reconnaissance, the attacker gathers information about the target on the Internet websites.

ii. In the second step, the attacker finds the company's internal network, such as, Internet domain, machine names and the company's Internet Protocol (IP) address ranges to steal the data.

2. Network probe (investigation):

- At the network probe stage, the attacker scans the organization information through a "ping sweep" of the network IP addresses.
- Then a "port scanning" tool is used to discover exactly which services are runningon the target system.
- At this point, the attacker has still not done anything that would be considered as an abnormal activity on the network or anything that can be classified as an intrusion.

3. Crossing the line toward electronic crime (E-crime):

- Once the attackers are able to access a user account, then they will attempt furtherexploits to get an administrator or "root" access.
- Root access is a UNIX term and is associated with the system privileges required to run all services and access all files on the system (readers are expected to havea basic familiarity with Unix-based systems).
- "Root" is an administrator or super-user access and grants them the privileges to do anything on the system.

4. Capturing the network:

- At this stage, the attacker attempts to "own" the network. The attacker gains the internal network quickly and easily by target systems.
- The next step is to remove any evidence of the attack. The attacker will usually install a set of tools that replace existing files and services with Trojan files and services that have a backdoor password.

5. Grab the data:

- Now that the attacker has "captured the network," he/she takes advantage of his/her position to steal confidential data

6. Covering tracks:

- This is the last step in any cyber attack, which refers to the activities undertaken by the attacker to extend misuse of the system without being detected.
- The attacker can remain undetected for long periods.
- During this entire process, the attacker takes optimum care to hide his/her identity(ID) from the first step itself.

Proxy Servers and Anonymizers

Proxy server is a computer on a network which acts as an intermediary for connection with other computers on that network.

- The attacker first connects to a proxy server and establishes a connection with the target system through existing connection with proxy.
- This enables an attacker to surf on the Web anonymously and/or hide the attack.
- A client connects to the proxy server and requests some services (such as a file, webpage) available from a different server.
- The proxy server evaluates the request and provides the resource by establishing the connection to the respective server and/or requests the required service on behalf of the client.
- Using a proxy server can allow an attacker to hide ID (i.e., become anonymous on the network).

A proxy server has following purposes:

1. Keep the systems behind the curtain (mainly for security reasons).
2. Speed up access to a resource (through "caching"). It is usually used to cache the webpages from a web server.
3. Specialized proxy servers are used to filter unwanted content such as advertisements.
4. Proxy server can be used as IP address multiplexer to enable to connect number of computers on the Internet, whenever one has only one IP address

- One of the advantages of a proxy server is that its cache memory can serve all users.
- If one or more websites are requested frequently, may be by different users, it is likely to be in the proxy's cache memory, which will improve user response time.
- An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It accesses the Internet on the user's behalf, protecting personal information by hiding the source computer's identifying information.
- Anonymizers are services used to make Web surfing anonymous by utilizing a website that acts as a proxy server for the web client.

Phishing

"Phishing" refers to an attack using mail programs to deceive Internet users into disclosing confidential information that can be then exploited for illegal purposes.

- While checking electronic mail (E-Mail) one day a user finds a message from the bank threatening to close the bank account if he/she does not reply immediately.
- Although the message seems to be suspicious from the contents of the message, it is difficult to conclude that it is a fake/false E-Mail.
- This message and other such messages are examples of Phishing – in addition to stealing personal and financial data – and can infect systems with viruses and also a method of online ID theft in various cases.
- These messages look authentic and attempt to get users to reveal their personal information.
- It is believed that Phishing is an alternative spelling of "fishing," as in "to fish for information."
- The first documented use of the word "Phishing" was in 1996.

How Phishing Works?

Phishers work in the following ways:

1. Planning: Criminals, usually called as phishers, decide the target.
2. Setup: Once phishers know which business/business house to spoof and who theirvictims.
3. Attack: the phisher sends a phony message that appears to be from a reputable source.
4. Collection: Phishers record the information of victims entering into webpages or pop-up windows.

5. Identity theft and fraud: Phishers use the information that they have gathered to makeillegal purchases or commit fraud.

Nowadays, more and more organizations/institutes provide greater online access for their customers and hence criminals are successfully using Phishing techniques to steal personal information and conduct ID theft at a global level.

Password Cracking

- Password is like a key to get an entry into computerized systems like a lock.
- Password cracking is a process of recovering passwords from data that have been storedin or transmitted by a computer system.
- Usually, an attacker follows a common approach – repeatedly making guesses forthe password.

The purpose of password cracking is as follows:

1. To recover a forgotten password.
2. As a preventive measure by system administrators to check for easily crackable passwords.
3. To gain unauthorized access to a system.

Manual password cracking is to attempt to logon with different passwords. The attackerfollows the following steps:

1. Find a valid user account such as an Administrator or Guest;
2. create a list of possible passwords;
3. rank the passwords from high to low probability;
4. key-in each password;
5. try again until a successful password is found.

Passwords can be guessed sometimes with knowledge of the user's personal information. Examples of guessable passwords include:

1. Blank (none);
2. the words like "password," "passcode" and "admin";
3. series of letters from the "QWERTY" keyboard, for example, qwerty, asdf or qwertyuiop;
4. user's name or login name;
5. name of user's friend/relative/pet;
6. user's birthplace or date of birth, or a relative's or a friend's;
7. user's vehicle number, office number, residence number or mobile number;
8. name of a celebrity who is considered to be an idol (e.g., actors, actress, spiritual gurus)by the user;

- An attacker can also create a script file (i.e., automated program) which will be executed to try each password in a list.
- This is still considered manual cracking, is time-consuming and not usually effective.
- Passwords are stored in a database and password verification process is established into the system when a user attempts to login or access a restricted resource.
- To ensure confidentiality of passwords, the password verification data is usually not stored in a clear text format.
- For example, one-way function (which may be either an encryption function or a cryptographic hash) is applied to the password, possibly in combination with other data, and the resulting value is stored.
- When a user attempts to login to the system by entering the password, the same function is applied to the entered value and the result is compared with the stored value. If they match, user gains the access; this process is called authentication.

The most commonly used hash functions can be computed rapidly and the attacker can test

these hashes with the help of passwords cracking tools (see Table 4.3) to get the plain text password.

Password cracking attacks can be classified under three categories as follows:

1. Online attacks;
2. offline attacks;
3. non-electronic attacks (e.g., social engineering, shoulder surfing and dumpster diving).

Online Attacks

- An attacker can create a script file that will be executed to try each password in a list and when matches, an attacker can gain the access to the system.
- The most popular online attack is man-in-the middle (MITM) attack, also termed as "bucket-brigade attack" or sometimes "Janus attack."
- It is a form of active stealing in which the attacker establishes a connection between a victim and the server to which a victim is connected.
- When a victim client connects to the fraudulent server, the MITM server intercepts the call, hashes the password and passes the connection to the victim server (e.g., an attacker within reception range of an unencrypted Wi-Fi wireless access point can insert himself as a man-in-the-middle).

- This type of attack is used to obtain the passwords for E-Mail accounts on public websites such as Yahoo, Hotmail and Gmail and can also used to get the passwords for financial websites that would like to gain the access to banking websites.

Offline Attacks

- Mostly offline attacks are performed from a location other than the target (i.e., either a computer system or while on the network) where these passwords reside or are used.
- Offline attacks usually require physical access to the computer and copying the password file from the system onto removable media.

Password guidelines.

1. Passwords used for business E-Mail accounts, personal E-Mail accounts and banking/financial user accounts should be kept separate.
2. Passwords should be of minimum eight alphanumeric characters (common names or phrases should be phrased).
3. Passwords should be changed every 30/45 days.
4. Passwords should not be shared with relatives and/or friends.
5. Password used previously should not be used while renewing the password.
6. Passwords of personal E-Mail accounts and banking/financial user accounts should be changed from a secured system, within couple of days, if these E-Mail accounts has been accessed from public Internet facilities such as cybercafes/hotels/libraries.
7. Passwords should not be stored under mobile phones/PDAs, as these devices are also prone to cyberattacks.
8. In case E-Mail accounts/user accounts have been hacked, respective agencies/institutes should be contacted immediately.

Keyloggers and Spywares

- Keystroke logging, often called keylogging, is the practice of noting (or logging) the keysstruck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions are being monitored.
- Keystroke logger or keylogger is quicker and easier way of capturing the passwords and monitoring the victims' IT savvy behavior. It can be classified as software keylogger and hardware keylogger.

Software Keyloggers

- Software keyloggers are software programs installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded.
- Software keyloggers are installed on a computer system by Trojans or viruses without the knowledge of the user.
- Cybercriminals always install such tools on the insecure computer systems available in public places (i.e., cybercafés, etc) and can obtain the required information about the victim very easily.
- A keylogger usually consists of two files that get installed in the same directory: a dynamic link library (DLL) file and an EXEcutable (EXE) file that installs the DLL file and triggers it to work. DLL does all the recording of keystrokes.
  Some Important Keyloggers are as follows

All In One Keylogger	Stealth Keylogger	Perfect Keylogger
KGB Spy	Spy Buddy	Elite Keylogger
CyberSpy	Powered Keylogger	

Hardware Keyloggers

- Hardware keyloggers are small hardware devices.
- These are connected to the PC and/or to the keyboard and save every keystroke into a fileor in the memory of the hardware device.
- Cybercriminals install such devices on ATM machines to capture ATM Cards' PINs.
- Each keypress on the keyboard of the ATM gets registered by these keyloggers.
- These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence.

Antikeylogger

- Antikeylogger is a tool that can detect the keylogger installed on the computer system and can remove the tool. (Visit http://www.anti-keyloggers.com for more information)
  Advantages of using antikeylogger are as follows:

1. Firewalls cannot detect the installations of keyloggers on the systems; hence,antikeyloggers can detect installations of keylogger.
2. This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs; if not updated, it does not serve the purpose, which makes the users at risk.
3. Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers.
4. It prevents ID theft (we will discuss it more in Chapter 5).
5. It secures E-Mail and instant messaging/chatting.

Spywares

- Spyware is a type of malware (i.e., malicious software) that is installed on computerswhich collects information about users without their knowledge.
- The presence of Spyware is typically hidden from the user; it is secretly installed on theuser's personal computer.
- Sometimes, however, Spywares such as keyloggers are installed by the owner of ashared, corporate or public computer on purpose to secretly monitor other users.

Some Important Spywares are as follows:

Spy.	Spector Pro.	Spector Pro.
eBlaster.	Remotespy .	Stealth Recorder Pro.
Stealth Website Logger.	Flexispy.	Wiretap Professional.
PC PhoneHome.	SpyArsenal Print Monitor Pro.	

Box 4.3 | Malwares

Malware, short for malicious software, is a software designed to infiltrate a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive or annoying software or program code. Malware can be classified as follows:

1. Viruses and worms: These are known as *infectious malware*. They spread from one computersystem to another with a particular behavior.
2. Trojan Horses: A Trojan Horse,[14] Trojan for short, is a term used to describe malware that appears,to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system
3. Rootkits: Rootkits is a software system that consists of one or more programs designed toobscurethe fact that a system has been compromised.
4. Backdoors: Backdoor[16] in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plain text and so on while attempting to remain undetected.
5. Spyware:
6. Botnets:
7. Keystroke loggers:

Virus and Worms

- Computer virus is a program that can “infect” legitimate programs by modifying them to include a possibly “evolved” copy of itself.
- Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines.
- A computer virus passes from computer to computer in a similar manner as a biological virus passes from person to person.
- Viruses may also contain malicious instructions that may cause damage or annoyance; the combination of possibly Malicious Code with the ability to spread is what makes viruses a considerable concern.
- Viruses can often spread without any readily visible symptoms.
- A virus can start on event-driven effects (e.g., triggered after a specific number of executions), time-driven effects (e.g., triggered on a specific date, such as Friday the 13th) or can occur at random.

Viruses can take some typical actions:

1. Display a message to prompt an action which may set of the virus;
2. delete files inside the system into which viruses enter;
3. scramble data on a hard disk;
4. cause erratic screen behavior;
5. halt the system (PC);
6. just replicate themselves to propagate further harm.

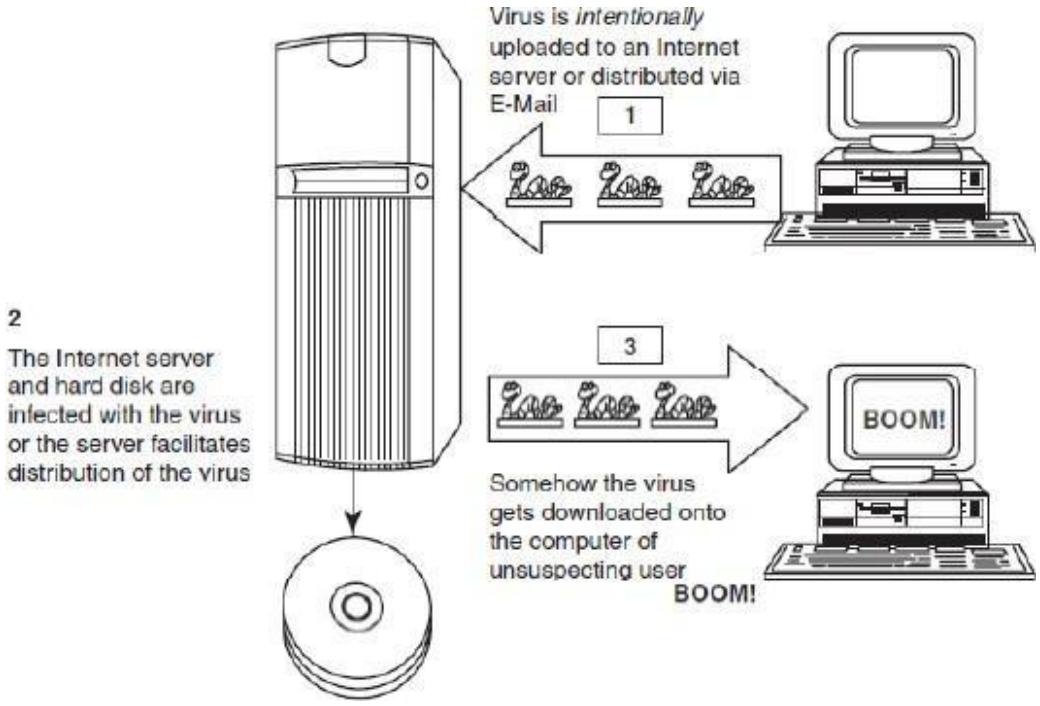

Figure: Virus Spread Through Internet

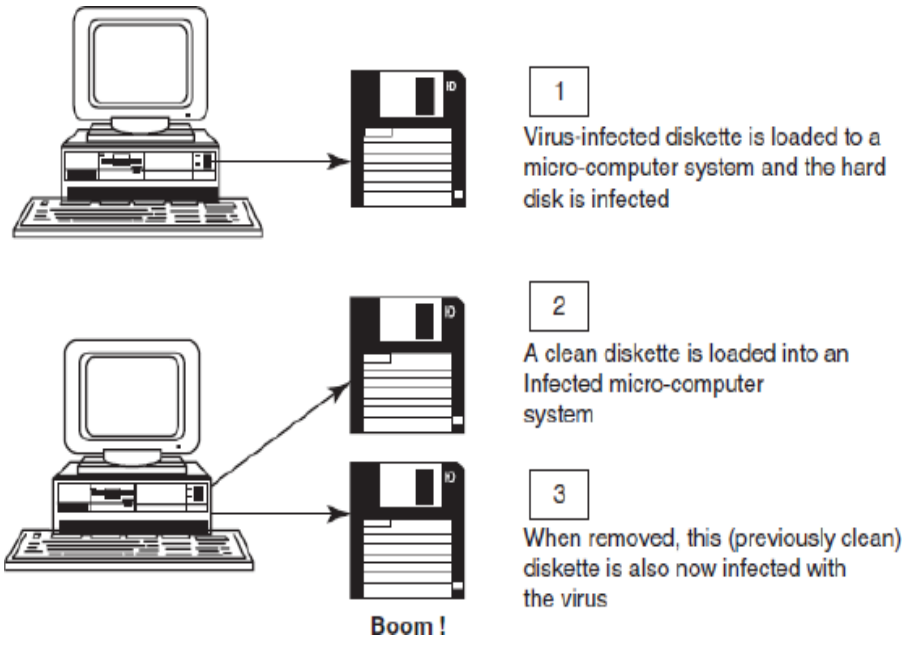

Figure: Virus Spread Through stand alone System

- **Computer virus** has the ability to copy itself and infect the system.
- The term *virus* is also commonly but erroneously used to refer to other types of malware, Adware and Spyware programs that do not have reproductive ability.
- A true virus can only spread from one system to another (in some form of executable code) when its host is taken to the target computer; for instance, when a user sent it over the Internet or a network, or carried it on a removable media such as CD, DVD or USB drives.
- Viruses can increase their chances of spreading to other systems by infecting files on a network file system or a file system that is accessed by another system.
- Malware includes computer viruses, worms, Trojans, most Rootkits, Spyware, dishonest Adware, crimeware and other malicious and unwanted software as well as true viruses.
- Viruses are sometimes confused with computer worms and Trojan Horses, which are technically different (see Table 4.7 to understand the difference between computer virus and worm).
- A worm spreads itself automatically to other computers through networks by exploiting security vulnerabilities, whereas a Trojan is a code/program that appears to be harmless but hides malicious functions.
- Worms and Trojans, such as viruses, may harm the system's data or performance.
- Some viruses and other malware have noticeable symptoms that enable computer user to take necessary corrective actions, but many viruses are surreptitious or simply do nothing for user's to take note of them.
- Some viruses do nothing beyond reproducing themselves.

Types of Viruses

1. **Boot sector viruses:** It infects the storage media on which OS is stored (e.g., hard drives) and which is used to start the computer system.
2. **Program viruses:** These viruses become active when the program file (usually with extensions .bin, .com,.exe, .ovl, .drv) is excuted
3. **Multipartite viruses:** It is a hybrid of a boot sector and program viruses. It infects program files along with the boot record when the infected program is active.
4. **Stealth viruses:** It hides itself and so detecting this type of virus is very difficult. It can hiding itself such a way that antivirus software also cannot detect it. Example for Stealth virus is

"Brain Virus".

5. **Polymorphic viruses:** It acts like a "chameleon" that changes its virus signature (i.e., binary pattern) every time it spreads through the system (i.e., multiplies and infects a new file). Hence, it is always difficult to detect polymorphic virus with the help of an antivirus program.
6. **Macro viruses:** Many applications, such as Microsoft Word and Microsoft Excel, support MACROs (i.e., macrolanguages). These macros are programmed as a macro embedded in a document. Once macrovirus gets onto a victim's computer then every document he/she produces will become infected.
7. **Active X and Java Control:** All the web browsers have settings about Active X and Java Controls.

World's worst worm attacks.

Conficker	INF/AutoRun	Win32 PSW	Win32/Agent
Win32/FlyStudio	Win32/Pacex.Gen	Win32/Qhost	WMA/ TrojanDownloader

The world's worst virus and worm attacks!!!

Morris Worm	ILOVEYOU	Nimda	Jerusalem
Code Red	Melissa	Melissa	
Sobig	Storm Worm	Michelangelo	

Trojan Horses and Backdoors

- Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm, for example, ruining the file allocation table on the hard disk.
- A Trojan Horse may get widely redistributed as part of a computer virus.
- The term Trojan Horse comes from Greek mythology about the Trojan War.
- Like Spyware and Adware, Trojans can get into the system in a number of ways,including from a web browser, via E-Mail.
- It is possible that one could be forced to reformat USB flash drive or other portable device to eliminate infection and avoid transferring it to other machines.
- Unlike viruses or worms, Trojans do not replicate themselves but they can be equally destructive.
- On the surface, Trojans appear benign and harmless, but once the infected code is executed, Trojans kick in and perform malicious functions to harm the computer system without the user's knowledge.
- For example, waterfalls.scr is a waterfall screen saver as originally claimed by the author; however, it can be associated with malware and become a Trojan to unload hidden programs and allow unauthorized access to the user's PC.

Some typical examples of threats by Trojans are as follows:

1. They erase, overwrite or corrupt data on a computer.
2. They help to spread other malware such as viruses (by a dropper Trojan).
3. They deactivate or interfere with antivirus and firewall programs.

4. They allow remote access to your computer (by a remote access Trojan).
5. They upload and download files without your knowledge.

6. They gather E-Mail addresses and use them for Spam.

7. They log keystrokes to steal information such as passwords and credit card numbers.
8. They copy fake links to false websites, display porno sites, play sounds/videos and display images.
9. They slow down, restart or shutdown the system.
10. They reinstall themselves after being disabled.
11. They disable the task manager.
12. They disable the control panel.

Backdoor

- A backdoor is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes.
- However, attackers often use backdoors that they detect or install themselves as part of an exploit.
- In some cases, a worm is designed to take advantage of a backdoor created by an earlier attack.
- A backdoor works in background and hides from the user.
- It is very similar to a virus and, therefore, is quite difficult to detect and completely disable.
- A backdoor is one of the most dangerous parasite, as it allows a malicious person to perform any possible action on a compromised system.

Following are some functions of backdoor:

1. It allows an attacker to create, delete, rename, copy or edit any file, execute various commands; change any system settings; alter the Windows registry; run, control and terminate applications; install arbitrary software and parasites.
2. It allows an attacker to control computer hardware devices, modify related settings, shutdown or restart a computer without asking for user permission.
3. It steals sensitive personal information, valuable documents, passwords, login names, ID details; logs user activity and tracks web browsing habits.
4. It records keystrokes that a user types on a computer's keyboard and captures screenshots.
5. It sends all gathered data to a predefined E-Mail address, uploads it to a predeterminedFTP server or transfers it through a background Internet connection to a remote host.
6. It infects files, corrupts installed applications and damages the entire system.

Following are a few examples of backdoor Trojans:

1. Back Orifice
2. Bifrost:
3. SAP backdoors
4. Onapsis Bizploit:

Follow the following steps to protect your systems from Trojan Horses and backdoors:

1. Stay away from suspect websites/weblinks:
2. Surf on the Web cautiously:
3. Install antivirus/Trojan remover software:

Steganography

- Steganography is the practice of concealing (hiding) a file, message, image, or video within another file, message, image, or video. The word steganography combines the Greek words steganos , meaning "covered, concealed, or protected", and graphein meaning "writing".
- It is a method that attempts to hide the existence of a message or communication.
- Steganography is always misunderstood with cryptography
- The different names for steganography are data hiding, information hiding and digital watermarking.
- Steganography can be used to make a digital watermark to detect illegal copying of digital images. Thus, it aids confidentiality and integrity of the data.
- *Digital watermarking* is the process of possibly irreversibly embedding information intoa digital signal.
- The Digital signal may be, for example, audio, pictures or video.
- If the signal is copied then the information is also carried in the copy.
- In other words, when steganography is used to place a hidden “trademark” in images,music and software, the result is a technique referred to as “watermarking”

Steganalysis

- Steganalysis is the art and science of detecting messages that are hidden in images, audio/video files using steganography.
- The goal of steganalysis is to identify suspected packages and to determine whether ornot they have a payload encoded into them, and if possible recover it.
- Automated tools are used to detect such steganographed data/information hidden in theimage and audio and/or video files.

Box 4.7 | Difference between Steganography and Cryptography
Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows the existence of the message; this is in contrast to cryptography, of the message itself is not disguised, but the content is obscured. It is said that terrorists use where the existence steganography techniques to hide their communication in images on the Internet; most popular images are used such as those of film actresses or other celebrities. In its basic form, steganography is simple.

DoS and DDoS Attacks

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource (i.e., information systems) unavailable to its intended users.

DoS Attacks

- In this type of criminal act, **the attacker floods the bandwidth of the victim's network** or fills his E-Mail box with Spam mail depriving him of the services he is entitled to access or provide.
- **The attackers typically target sites or services hosted on high-profile web servers** such as banks, credit card payment gateways, mobile phone networks and even root name servers.
- Buffer overflow technique is employed to commit such kind of criminal attack known as *Spoofing*.

- The term IP address Spoofing refers to the creation of IP packets with a forged (spoofed) source IP address with the purpose of concealing the ID of the sender or impersonating another computing system.
- A packet is a formatted unit of data carried by a packet mode computer network.
- The attacker spoofs the IP address and floods the network of the victim with repeated requests.
- As the IP address is fake, the victim machine keeps waiting for response from the attacker's machine for each request.
- This consumes the bandwidth of the network which then fails to serve the legitimate requests and ultimately breaks down.
- The United States Computer Emergency Response Team defines symptoms of DoS attacks to include:

1. Unusually slow network performance (opening fi les or accessing websites);
2. unavailability of a particular website;
3. inability to access any website;
4. dramatic increase in the number of Spam E-Mails received (this type of DoSattack is termed as an E-Mail bomb).

The goal of DoS is not to gain unauthorized access to systems or data, but to prevent intended users (i.e., legitimate users) of a service from using it.

A DoS attack may do the following:

1. Flood a network with traffic, thereby preventing legitimate network traffic.
2. Disrupt connections between two systems, thereby preventing access to a service.
3. Prevent a particular individual from accessing a service.
4. Disrupt service to a specific system or person.

Classification of DoS Attacks

1. **Bandwidth attacks:** Loading any website takes certain time. Loading means completewebpage appearing on the screen and system is awaiting user's input.

2. **Logic attacks:** These kind of attacks can exploit vulnerabilities in network software suchas web server or TCP/IP stack.
3. **Protocol attacks**: Protocols here are rules that are to be followed to send data over network.
4. **Unintentional DoS attack :** This is a scenario where a website ends up denied not due toa attack by a single individual or group of individuals, but simply due to a sudden enormous spike in popularity.

Types or Levels of DoS Attacks

There are several types or levels of DoS attacks as follows:

1. **Flood attack:** This is the earliest form of DoS attack and is also known as *ping food*. It isbased on an attacker simply sending the victim overwhelming number of ping packets, usually by using the "ping" command, which result into more traffic than the victim can handle.
2. **Ping of death attack:** The ping of death attack **sends oversized Internet Control Message Protocol (ICMP) packets,** and it is one of the core protocols of the IP Suite. It is mainly used by networked computers' OSs to send error messages indicating (e.g., that a requested service is not available or that a host or router could not be reached) datagrams (encapsulated in IP packets) to the victim.
3. **SYN attack:** It is also termed as ***TCP SYN Flooding***. In the TCP, handshaking of network connections is done with SYN and ACK messages.

- An attacker initiates a TCP connection to the server with an SYN.
- The server replies with an SYN-ACK.
- The client then does not send back an ACK, causing the server to allocate memory forthe pending connection and wait.
- This fills up the buffer space for SYN messages on the target system, preventing other systems on the network from communicating with the target system.

4. **Teardrop attack:** The teardrop attack is an attack where **fragmented packets are forged to overlap each other when the receiving host tries to reassemble them**. IP's packet fragmentation algorithm is used to send corrupted packets to confuse the victim
   and may hang the system. This attack can crash various OSs due to a bug in their TCP/IP fragmentation reassembly code.
5. **Smurf attack:** This is a type of DoS attack that **floods a target system via spoofed broadcast ping messages.** This attack consists of a host sending an echo request (ping)to a network broadcast address.
6. **Nuke:** Nuke is an old DoS attack against computer networks consisting of **fragmented or invalid packets sent to the target.**

Tools Used to Launch DoS Attack

1. **Jolt2 :** The vulnerability allows remote attackers to cause a DoS attack against Windows-based machines – the attack causes the target machine to consume of the CPU time on processing of illegal packets.
2. **Nemesy :** This program generates random packets of spoofed source IP to enable the attacker to launch DoS attack.
3. **Targa :** It is a program that can be used to run eight different DoS attacks.

The attacker has the option to launch either individual attacks or try all the attacks until one issuccessful.

4. **Crazy Pinger :** This tool could send large packets of ICMP(Internet Control Message Protocol) to a remote target network.
5. **SomeTrouble:** It is a remote flooder and bomber. It is developed in Delphi.

DDoS Attacks

- In a DDoS attack, an attacker may use your computer to attack another computer.
- By taking advantage of security vulnerabilities or weaknesses, an attacker could takecontrol of your computer.
- He/she could then force your computer to send huge amounts of data to a website or sendSpam to particular E-Mail addresses.
- The attack is "distributed" because the attacker is using multiple computers, includingyours, to launch the DoS attack.
- A DDoS attack is a distributed DoS wherein a large number of zombie systems aresynchronized to attack a particular system.

- The zombie systems are called "secondary victims" and the maintarget is called"primary victim."
- Malware can carry DDoS attack mechanisms – one of the better-knownexamples of thisis MyDoom.
- Botnet is the popular medium to launch DoS/DDoS attacks.
- Attackers can also break into systems using automated tools that exploit flaws inprograms that listen for connections from remote hosts.

How to Protect from DoS/DDoS Attacks

Computer Emergency Response Team Coordination Center (CERT/CC)offers manypreventive measures from being a victim of DoS attack.

1. Implement router **filters**. This will lessen your exposure to certain DoS attacks.
2. If such filters are available for your system, **install patches** to guardagainst TCP SYNflooding.
3. Disable any unused or inessential network service.
4. Enable quota systems on your OS if they are available.
5. Observe your system's performance and establish baselines for ordinary activity.
6. Routinely examine your physical security with regard to your current needs.
7. Use Tripwire or a similar tool to detect changes in configurationinformation or otherfiles.
8. Invest in and maintain "hot spares" – machines that can be placed intoservice quickly if asimilar machine is disabled.
9. Invest in redundant and fault-tolerant network configurations.
10. Establish and maintain regular backup schedules
11. Establish and maintain appropriate password policies