Jump2Learn
PUBLICATION

www.jump2learn.com

E-COMMERCE & CYBER SECURITY

Jump2Learn - The Online Learning Place

Ms. Sonal B. Shah | Mrs. Krupali P. Patel | Mr. Nitesh G. Patel

History of Cyber Crime

Crime and cybercrime have become an increasingly large problem in our society, even with the criminal justice system in place. Both in the public web space and dark web, cybercriminals are highly skilled and are not easy to find. Cybercrime has created a major threat to those who use the internet, with millions of users' information stolen within the past few years.

Definition:

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money.

Distinction between Cyber Crime and Traditional Crime

1. This kind of Crime- Cybercrimes is quite different from traditional crimes as they are often harder to detect, investigate and prosecute and because of that cybercrimes cause greater damage to society than traditional crimes. Cybercrime also includes traditional crimes conducted through the internet or any other computer technology. For example; hate crimes, identity theft, terrorism, are considered to be cybercrimes.
2. Another difference is in the description of the criminals of both kinds of crimes. The hackers in cyber-crime are professional thieves, educated hackers, organized criminal gangs, ideological hackers etc. as compared to traditional crimes.
3. Evidence- The other difference between these two terms is based on the evidence of the offences. In the traditional crimes the criminals usually leave any proof of that crime like fingerprints or other physical proof. But in the cyber crimes cyber criminals commit their crimes through the internet and there are very less chances of leaving any physical proof.
4. Physical Force- Further, these two terms can be differentiated on the basis of use of force. In traditional crimes many of the crimes like rape, murder, and burglary etc. involve the use of excessive physical force which leads to physical injury on the victim. But in cybercrimes, there is no requirement of any type of physical force because in this type of crimes the criminals only use the identities or accounts of other person using computer technologies.

4.1 Category of Cyber Crimes

The cybercrimes may be broadly classified into four groups. They are:

1. **Crime against the Individuals:** Crimes that are committed by the cyber criminals against an individual or a person. A few cybercrimes against individuals are:
   - E-mail Spoofing -: A spoofed email is one that appears originate from one source but actually sent from another source.
   - Phishing -: Phishing is a special type of intended to trick you into entering your personal /A/C information to the purpose of breaching your account and committing theft or fraud.

- Cyber-stalking -: Cyber stalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail.
- Defamation -: Cyber defamation occurs when a computer connected to the internet is used as a tool, or a medium to defame a person or an entity.
- Password Sniffing -:Password sniffer is a software application that scans and records passwords that are used or broadcasted on a computer or network interface. It listens to all incoming and outgoing network traffic and records any instance of a data packet that contains a password.

2. Crimes against Property: These types of crimes includes vandalism of computers, Intellectual (Copyright, patented, trademark etc) Property Crimes etc. Intellectual property crime includes:

- Credit Card fraud - Credit card fraud happens when someone — a fraudster or a thief — uses your stolen credit card or the information from that card to make unauthorized purchases in your name or take out cash advances using your account.
- Intellectual Crime - Intellectual property crime is committed when someone manufactures, sells or distributes counterfeit or pirated goods, such as patents, trademarks, industrial designs or literary and artistic works, for commercial purpose.

- Internet Time theft- It refers to the theft in a manner where the unauthorized person uses internet hours paid by another person. The authorized person gets access to another person's ISP user ID and password, either by hacking or by illegal means without that person's knowledge.

3. Crime against Organization: Crimes done to threaten the international governments or any organization by using internet facilities. These cybercrimes are known as cybercrimes against Organization. These crimes are committed to spread terror among people. Cyber terrorism is referred as crimes against a government. Cybercrimes against Government includes cyber attack on the government website, military website or cyber terrorism etc.

- Unauthorized access / control over computer system.
- Cyber terrorism against the government organization.
- Possession of unauthorized information.
- Distribution of Pirate software.

4. Crime against Society: Those cybercrimes which affects the society interest at large are known as cybercrimes against society, which include:

- Forgery- When a perpetrator alters documents stored in computerized form, the crime committed may be forgery. ... In this instance, computer systems are the target of criminal activity. Computers, however, can also be used as instruments with which to commit forgery.
- Child pornography- Cyber Pornography means *the publishing, distributing or designing pornography by using cyberspace*. The technology has its pros and cons and cyber pornography is the result of the advancement of technology. With the easy availability of the Internet, people can now view thousands of porn on their mobile or laptops, they even have access to upload pornographic content online. Sale of illegal articles- This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, bulletin boards or simply by using e-mail communications.

4.2 Technical Aspects Of Cyber Crime

4.2.1 Unauthorized access and hacking

Unauthorized access:

It is an act of gaining access to a network, system, application or other resource without permission. Unauthorized access could occur if a user attempts to access an area of a system they should not be accessing. Unauthorized access could be result of unmodified default access policies or lack of clearly defined access policy documentation.

Hacking:

Hacking refers to an array of activities which are done to intrude someone else's personal information space so as to use it for malicious unwanted purposes.

Hacking is a term used to refer to activities aimed at exploiting security flaws to obtain critical information for gaining access to secured networks.

Who Is Hacker?

Hacker is a term that first started being used in the 1960s and described a programmer or someone who hacked computer code. Later the term evolved into an individual who had an advanced understanding of computers, networking, programming, or hardware, but did not have any malicious intent.

Today, a malicious hacker is usually referred to as a black hat or criminal hacker, which describes any individual who illegally breaks into computer systems to damage or steal information .

Hacking Methods

A typical attacker works in the following manner:

- Identify the target system.
- Gathering information on the target system.
- Finding a possible loophole in the target system
- Exploiting this loophole using exploit code.
- Removing all traces from the log files and escaping without a trace.

Types of Hacking

1. Website Hacking:

Hacking a website means taking control from the Website owner to a person who hacks the website.

2. Network hacking:

It is generally means gathering information about domain by using tools like telnet, Ns look UP, Ping, Tracert , Netstat, etc. Over the network.

3. Password hacking:

We have passwords for emails, databases, computer systems, servers, bank accounts, and virtually everything that we want to protect. Passwords are in general the keys to get access into a system or an account. Password Hacking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.

Types of hackers

1. Black Hat Hacker

These types of hackers always have a malicious intention and they access computer networks, websites in an unauthorized manner. The intent is for personal gain through stealing of confidential organizational data, stealing of funds from online bank accounts, privacy right violations to benefit criminal organizations etc. In today's scenario, most of the hackers belong to this category and carry on their activities.

2- Ethical Hacker/White Hat Hacker

They are recognized and officially stamped hackers who access systems to asses to identify and eliminate suspected weakness. Other responsibilities include vulnerability assessment, cracking of codes of illegal or anti-social setups, retrieval of crucial data required for security purposes. These are highly trained, certified and paid professionals.

3- Grey Hat Hacker

They lie between the above-mentioned type of hackers i.e. they take the recourse of unauthorized access to a system but not with any fraudulent intent. The objective is to reveal the vulnerabilities and weakness of the system's stakeholders.

4- Hacktivist

These hackers are those who are focussed on hacking websites and leaving contentious information on such websites. This is to spread political, social, religious messages. This can also take the form of targeting other nations.

Guard against hacking

Virtual Private Networks (VPN) is a protocol by which corporate networks connect to offsite and remote locations through a point to point tunnel like connectivity. VPN resources such as ExpressVPN, securely cover the transmitting and receiving IP addresses thereby preventing any hacker from making any unauthorized encroachment.

What should do after hacked?

- ✓ Shutdown the system or turn of the system
- ✓ Separate the system from network
- ✓ Connect the system to the network
- ✓ Restore the system with the backup or reinstall all programs
- ✓ It can be good to call a police

Advantages of hacking

- Can be used to recover lost information where the computer password has been lost
- To test how good security is on your own network

Disadvantages of hacking

- Criminals can use it to their advantage.
- It can harm someone privacy.
- It's illegal.

4.2.2 Trojan, Virus and Worm Attacks

Malware

Malware, short for malicious software, is a blanket term for viruses, worms, Trojans and other harmful computer programs hackers use to wreak destruction and gain access to sensitive information.

The most common blunder people make when the topic of a computer virus arises is to refer to a worm or Trojan horse as a virus. While the words Trojan, worm and virus are often used interchangeably, they are not the same. Viruses, worms and Trojan Horses are all malicious programs that can cause damage to your computer, but there are differences among the three, and knowing those differences can help you to better protect your computer from their often damaging effects.

Virus

"A Computer Virus is a malicious software program "Malware" that can infect a computer by modifying or deleting data files, boot sector of a hard disk drive or causes a software program to work in an unexpected manner".

A computer virus resides on a host computer and can replicate itself when executed. Virus can steal user data, delete or modify files & documents, records keystrokes & web sessions of a user. It can also steal or damage hard disk space, it can slowdown CPU processing.

Activation Of Virus

When the computer virus starts working, it is called the activation of virus. A virus normally runs all the time in the computer. Different viruses are activated in different ways. Many viruses are activated on a certain data. For example, a popular virus "Friday, the 13th" is activated only if the date is 13 and the day is Friday.

Damages Caused By Virus

Computer virus cannot damage computer hardware. It may cause many damages to a computer system. A virus can:

1. A computer virus can damage data or software on the computer.
2. It can delete some or all files on the computer system.
3. It can destroy all the data by formatting hard drive.
4. It may display a false message very few times.

Virus infects computer system if latest and updated version of an Antivirus program is not installed. Latest Antivirus software should be installed on Computer to protect it from viruses.

A computer system can be protected from virus by following these precautions.

1. The latest and updated version of Anti-Virus and firewall should be installed on the computer.
2. The Anti-Virus software must be upgraded regularly.
3. USB drives should be scanned for viruses, and should not be used on infected computers.
4. Junk or unknown emails should not be opened and must be deleted straightaway.
5. Unauthorized or pirated software should not be installed on the computer.
6. Your best protection is your common sense. Never click on suspicious links, never download songs, videos or files from suspicious websites. Never share your personal data with people you don't know over the internet.

Different types of computer virus classification are given below.

• Boot Sector Virus:

A Boot Sector Virus infects the first sector of the hard drive, where the Master Boot Record (MBR) is stored. The Master Boot Record (MBR) stores the disk's primary partition table and to store bootstrapping instructions which are executed after the computer's BIOS passes execution to machine code. If a computer is infected with Boot Sector Virus, when the computer is turned on, the virus launches immediately and is loaded into memory, enabling it to control the computer.

• File Deleting Viruses:

A File Deleting Virus is designed to delete critical files which are the part of Operating System or data files.

• Mass Mailer Viruses:

Mass Mailer Viruses search e-mail programs like MS outlook for e-mail addresses which are stored in the address book and replicate by e-mailing themselves to the addresses stored in the address book of the e-mail program.

• Macro viruses:

Macro viruses are written by using the Macro programming languages like VBA, which is a feature of MS office package. A macro is a way to automate and simplify a task that you perform repeatedly in MS office suit (MS Excel, MS word etc). These macros are usually stored as part of the document or spreadsheet and can travel to other systems when these files are transferred to another computers.

• **Polymorphic Viruses:**
Polymorphic Viruses have the capability to change their appearance and change their code every time they infect a different system. This helps the Polymorphic Viruses to hide from anti-virus software.

• **Stealth viruses:**
Stealth viruses have the capability to hide from operating system or anti-virus software by making changes to file sizes or directory structure. Stealth viruses are anti-heuristic nature which helps them to hide from heuristic detection.

• **Retro virus:**
Retrovirus is another type virus which tries to attack and disable the anti-virus application running on the computer. A retrovirus can be considered anti-antivirus. Some Retroviruses attack the anti-virus application and stop it from running or some other destroys the virus definition database.

Worms

A computer worm is a type of malicious program whose primary function is to infect other computers while remaining active on infected systems.

A computer worm is self-replicating malware that duplicates itself to spread to uninfected computers. Worms often use parts of an operating system that are automatic and invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

Actions of Computer Worm

- Bandwidth is consumed and servers are overloaded that causes harm to the network.
- Also rather than spreading and destroying the network, codes are written inside the worm so that the systems are destroyed with these codes. These codes steal data or create backdoors so that other systems can control the system.
- The codes also called payloads to destroy the system in a way that the infected systems are used to spread spams and destroy the entire network.
- Computer worms need no assistance and also they replicate by themselves.
- Worms either modify or delete the files of the system thereby overloading the system and hence the network.
- The worm creates space for a hacker to enter the system and destroy the entire network.
- Computer worms destroy the data worth years and are very malicious. Protecting our data from worms is very important.
- Security features are mostly exploited by the worms.
- Some worms also try to change the system settings.
- Examples of worms include Morris Worm, Storm Worm, SQL Slammer.
- Morris developed a few lines of code to know how vast the internet is but the codes had bugs that destroyed the host systems and caused damage worth millions.
- Storm worm, as the name suggests sends mails of a news report regarding the storm. Once opened the system is affected and other contacts are also sent emails.

This worm was created in 2007. Many believe that the systems are still affected by this worm which the user does not know.

- Stuxnet is a famous computer worm that was intended to destroy Iran's nuclear plans.

Types of computer worms

- **Email Worms:** Email Worms spread through malicious email as an attachment or a link of a malicious website.
- **Instant Messaging Worms:** Instant Messaging Worms spread by sending links to the contact list of instant messaging applications such as Messenger, WhatsApp, Skype, etc.
- **Internet Worms:** Internet worm searches all available network resources using local operating system services and/or scans compromised computers over the Internet.
- **IRC Worms:** IRC Worms spread through Internet Relay Chat (IRC) chat channels, sending infected files or links to infected websites.
- **File sharing Worms:** File sharing Worms place a copy of them in a shared folder and distribute them via Peer To Peer network.

Prevention from Worm

- Using firewalls will help reduce access to systems by malicious software.
- Using antivirus software will help prevent malicious software from running.
- Being careful not to click on attachments or links in email or other messaging applications that may expose systems to malicious software.
- Encrypt files to protect sensitive data stored on computers, servers and mobile devices.

Some symptoms that may indicate the presence of a worm include:

- Computer performance issues, including degraded system performance, system freezing or crashing unexpectedly.
- Unusual system behavior, including programs that execute or terminate without user interaction; unusual sounds, images or messages; the sudden appearance of unfamiliar files or icons, or the unexpected disappearance of files or icons; warning messages from the operating system or antivirus software; and email messages sent to contacts without user action.

One of the most damaging computer worms ever was the ILOVEYOU virus. ILOVEYOU primarily spread when targeted victims opened an email attachment, and the malware resent itself to all of the victim's contacts in Microsoft Outlook.

Trojan

A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate or harmless but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.

Viruses can execute and replicate themselves. A Trojan cannot. A user has to execute Trojans. Even so, Trojan malware and Trojan virus are often used interchangeably.

Trojans working :

Here's a Trojan malware example to show how it works.

You might think you've received an email from someone you know and click on what looks like a legitimate attachment. But you've been fooled. The email is from a cybercriminal, and the file you clicked on — and downloaded and opened — has gone on to install malware on your device.

When you execute the program, the malware can spread to other files and damage your computer.

Types of Trojan

- **Backdoor Trojan**

This Trojan can create a "backdoor" on your computer. It lets an attacker access your computer and control it. Your data can be downloaded by a third party and stolen. Or more malware can be uploaded to your device.

- **Distributed Denial of Service (DDoS) attack Trojan**

This Trojan performs DDoS attacks. The idea is to take down a network by flooding it with traffic. That traffic comes from your infected computer and others.

- **Downloader Trojan**

This Trojan targets your already-infected computer. It downloads and installs new versions of malicious programs. These can include Trojans and adware.

- **Fake AV Trojan**

This Trojan behaves like an antivirus software, but demands money from you to detect and remove threats, whether they're real or fake.

- **Game-thief Trojan**

The losers here may be online gamers. This Trojan seeks to steal their account information.

- **Remote Access Trojan**

This Trojan can give an attacker full control over your computer via a remote network connection. Its uses include stealing your information or spying on you.

Examples of Trojan malware attacks

1. Rakhni Trojan - This malware has been around since 2013. More recently, it can deliver ransomware (allowing criminals to use your device to mine for cryptocurrency) to infected computers.

2. ZeuS/Zbot - This banking Trojan source code was first released in 2011. It uses keystroke logging — recording your keystrokes as you log into your bank account, for instance — to steal your credentials and perhaps your account balance as well.

- Don't visit unsafe websites. Some internet security software will alert you that you're about to visit an unsafe site, such as Norton Safe Web.
- Don't open a link in an email unless you're confident it comes from a legitimate source. In general, avoid opening unsolicited emails from senders you don't know.
- Don't download or install programs if you don't have complete trust in the publisher.
- Don't click on pop-up windows that promise free programs that perform useful tasks.

- Don't ever open a link in an email unless you know exactly what it is.

Signs of Trojan

- Desktop changes
- Increase of spam or pop-ups
- Poor device performance
- Unfamiliar downloads, add-ons, or applications
- Changes to display color, clarity, or orientation
- Strange device behavior

4.2.3 E-mail related crimes

4.2.3.1 Email spoofing and spamming

Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is a popular tactic used in Phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate or familiar source. The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation.

Although most spoofed emails can be easily detected and require little action other than deletion, the more malicious varieties can cause serious problems and pose security risks. For example, a spoofed email may pretend to be from a well-known shopping website, asking the recipient to provide sensitive data such as a password or credit card number. Alternatively, a spoofed email may include a link that installs malware on the recipient's device if clicked.

While email spoofing is most popularly used to execute phishing attacks, a cybercriminal may also use this technique to avoid spam email blacklists, commit identity theft .
Mail spoofing can be easily achieved with a working Simple Mail Transfer Protocol (SMTP) server and mailing software like Outlook or Gmail. Once an email message is composed, the scammer can forge fields found within the message header such as the FROM, REPLY-TO and RETURN-PATH addresses. After the email is sent, it will appear in the recipient's mailbox that appears to come from the address that was entered.
This is possible to execute because the SMTP does not provide a mechanism for addressing authentication. Although email sender authentication protocols and mechanisms have been developed to combat email spoofing, adoption of those mechanisms has been slow.

Prevention from Email Spoofing

To prevent becoming a victim of email spoofing, the following practices should be put into place:

- Keep antimalware software up to date.
- Do not share private or financial information through email.
- Turn spam filters on to the strongest settings, or use tools like Gmail's Priority Inbox.
- Avoid clicking suspicious links or downloading suspicious attachments.

- Never enter sensitive information into links that are not secure.
- Conduct reverse IP lookups to verify the real sender.

Mail spoofing can be easily achieved with a working Simple Mail Transfer Protocol (SMTP) server and mailing software like Outlook or Gmail. Once an email message is composed, the scammer can forge fields found within the message header such as the FROM, REPLY-TO and RETURN-PATH addresses. After the email is sent, it will appear in the recipient's mailbox that appears to come from the address that was entered.

This is possible to execute because the SMTP does not provide a mechanism for addressing authentication. Although email sender authentication protocols and mechanisms have been developed to combat email spoofing, adoption of those mechanisms has been slow.

Email spamming

Email spam also referred to as junk email, is unsolicited messages sent in bulk by email. Spammers collect email addresses from chat rooms, websites, customer lists, newsgroups, and viruses that harvest users' address books. These collected email addresses are sometimes also sold to other spammers.

Types of spam

Appending

If a marketer has one database containing names, addresses, and telephone numbers of customers, they can pay to have their database matched against an external database containing email addresses. The company then has the means to send email to people who have not requested email, which may include people who have deliberately withheld their email address

Image spam

Image spam or image-based spam is an method by which text of the message is stored as a GIF or JPEG image and displayed in the email. This prevents text-based spam filters from detecting and blocking spam messages. Image spam was reportedly used in the mid-2000s to advertise.

Blank spam

Blank spam is spam lacking a payload advertisement. Often the message body is missing altogether, as well as the subject line. Still, it fits the definition of spam because of its nature as bulk and unsolicited email. Blank spam may be originated in different ways, either intentionally or unintentionally.

Backscatter spam

Backscatter is a side-effect of email spam, viruses, and worms. It happens when email servers are misconfigured to send a bogus bounce message to the sender.

If the sender's address was forged, then the bounce may go to an innocent party. Since these messages were not solicited by the recipients, are substantially similar to each other, and are delivered in bulk quantities.

4.2.3.2 Email bombing

An email bomb is a form of net abuse consisting of sending large volumes of email to an address in an attempt to overflow the mailbox, overwhelm the server where the email address is hosted .

There are three methods of an email bomb:

1. Mass mailing
2. List linking
3. Zip bombing

1. Mass mailing

Mass mailing consists of sending numerous duplicate mails to the same email address. These types of mail bombs are simple to design but their extreme simplicity means they can be easily detected by spam filters. Email-bombing using mass mailing is also commonly performed as a DDoS attack by employing the use of botnets ; hierarchical networks of computers compromised by malware and under the attacker's control. Similar to their use in spamming, the attacker instructs the botnet to send out millions or even billions of emails, but unlike normal botnet spamming, the emails are all addressed to only one or a few addresses the attacker wishes to flood. This form of email bombing is similar in purpose to other DDoS flooding attacks.

This type of attack is more difficult to defend against than a simple mass-mailing bomb because of the multiple source addresses and the possibility of each zombie computer sending a different message or employing stealth techniques to defeat spam filters.

2.List linking

List linking, also known as "email cluster bomb", means signing a particular email address up to several email list subscriptions. The victim then has to unsubscribe from these unwanted services manually. The attack can be carried out automatically with simple scripts: this is easy, almost impossible to trace back to the perpetrator, and potentially very destructive. A massive attack of this kind targeting .gov email addresses was observed in August 2016.

A large amount of confirmation emails initiated by registration bots signing up a specific email address to a multitude of services can be used to distract the view from important emails indicating that a security breach has happened elsewhere. If for example an Amazon account has been hacked, the hacker may contrive to have a flood of confirmation emails sent to the email address associated with the account to mask the fact that the Amazon shipment address has been changed and purchases have been made by the hacker.

3.ZIP bombing

A ZIP bomb is a variant of mail-bombing. After most commercial mail servers began checking mail with anti-virus software and filtering certain malicious file types, EXE, RAR, Zip, Zip, mail server software was then configured to unpack archives and check their contents as well .

4.2.3.3 Denial of Service attacks

Dos means Denial of service attack. Dos attack is an attempt to make a computer or network resources unavailable to its intended users. When a denial of service (DOS) attack occurs, a computer or a network user is unable to access resources like e-mail and the Internet. An attack can be directed at an operating system or at the network. These attacks had to be "manually" synchronized by a lot of attackers in order to cause an effective damage.

The subject came to public awareness only after a massive attack on public sites on February 2000. During a period of three days the sites of Yahoo.com, amazon.com, buy.com, cnn.com & eBay.com were under attack. Analysts estimated that Yahoo! Lost $500,000 in e-commerce and advertising revenue when it was knocked offline for three hours

Dos attacks include

- Slow the network.
- Unavailability of website.
- Increase the no of spam emails.
- Disrupt connection between two systems.
- Prevent the individual from accessing services

Classification of DOS attacks:

1. **Bandwidth attacks:**

Loading any website takes certain time. Loading means complete webpage (i.e. With entire content of the webpage – text along with images) appearing on the screen and system is awaiting user's input. This loading consumes some amount of memory. Every site is given with a particular amount of bandwidth for its hosting. Say for example, 50 GB. Now if more visitor consume all 50 GB bandwidth then the hosting of the site can ban this site.

2. **Logic attacks :**

This kind of attack can exploit vulnerabilities in network software such as web server or TCP/IP attack.

3. **Protocol attack:**

Protocol here are rules that are to be followed to send data over network. These kind of attacks exploit a specific feature of implementations bug .of some protocol installed at the victim's system to consume excess amounts of its resources.

Protection from Dos Attack:

- Implements router filter. This will lessen your exposure to certain dos attacks.
- If such filters are available for your system, installed patches to guard against TCP SYN flooding.
- Routinely examine your physical security with regard to your currents needs.
- Establish and maintain regular backup schedule and policies, particularly for important configuration information.
- Disable any unused network service. This can limit the abillty of an attacker to take advantage of these service to execute a Dos attack.

Types of dos attacks

2. **Flood attack:-**

This is the earliest from of DOS attacks and is also known as ping flood. It is based on 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.

3. **Ping of death attack:**

The ping of death attack sends oversized internet control message protocol packets, and it is one of the core protocol of the IP suite. It is mainly used by networked computer OS to send error message indicating (e.g. that a requested service is not available) to the victim. The maximum size of packets is allowed 65,536 octets. Some system, upon receiving the overprized packet, will crash resulting in DOS.

3. SYN Attack:-

It is also termed as TCP SYN flooding. In the transmission control protocol handshaking of network connection is done by 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 does not send back an ACK , causing the server allocate memory for the pending connection and wait.

4. **Smurf attack:-**

It is a way of generating significant computer network traffic on a victim network. This is a type of Dos attack that flood a target system via spoofed broadcast ping message. This attack consist of a host sending an ICMP echo request to a network broadcast address. Every host on the network receive the ICMP echo request and send back an ICMP echo response with the network traffic.

4.2.3.4. A distributed denial of service attack

This is the complicated but powerful version of DOS attack in which many attacking systems are involved. In DDOS attacks, many computers start performing DOS attacks on the same target server. As the DOS attack is distributed over large group of computers, it is known as a distributed denial of service attack.

To perform a DDOS attack, attackers use a zombie network, which is a group of infected computers on which the attacker has silently installed the DOS attacking tool. Whenever he wants to perform DDOS, he can use all the computers of ZOMBIE network to perform the attack. In simple words, when a server system is being flooded from fake requests coming from multiple sources (potentially hundreds of thousands), it is known as a DDOS attack.

For creating the zombie network, hackers generally use a Trojan. The more members in the zombie network, more powerful the attack it .The wave of DDoS attacks that targeted major Websites such as Yahoo and Amazon in 2000 was estimated cumulatively to have cost over $1.2 billion in damages.

Protection from DDOS attack

1. Implements router filters. This will lesson your exposure to certain DoS attacks.
2. Disable any unused or inessential network service. This can limit the ability of an attacker to take advantage of these service to execute a dos attack.
3. Enable quota system on your OS if they are available.
4. Routinely examine your physical security with regard to your current needs.
5. Establish and maintain regular backup schedules and policies, particularly for important configuration information.
6. Establish and maintain appropriate password policies, especially access to highly privileged accounts such as Unix root or Microsoft windows NT administrator.

Tools for detecting DDOS attack

1.Zombie Zapper:

It is a free, open source tool that can tell a zombie system flooding packets to stop flooding. It works against Trinoo, TFN and Stacheldraht.

2.Remote Intrusion Detector (RID):

It is tool develop in "C" computer language, which is a highly configurable packet snooper and generator. It detects the presence of Trinoo, TFN or Stacheldrhat .