CYBER SECURITY (PS02EMCA37)

Unit-2 : Tools and Methods Used in Cybercrime

- Password Cracking
- Key Loggers and Spywares
- Virus and Worms
- Trojan Horses and Backdoors
- DoS and DDoS Attacks
- SQL Injection
- Buffer Overflow
- Phishing
- Identity Theft
- Networking Commands

Password Cracking

- It is is the process of attempting to gain Unauthorized access to restricted systems using common passwords or algorithms.

E.g.

- **Dictionary attack:** The dictionary attack uses a simple file containing words that can be found in a dictionary
- **Brute force attack:** All possible alpha-numeric combinations upto some length.

- **Purpose**
  - To recover a forgotten password.
  - As a Admin to check for easily crackable password
  - To gain access to unauthorized access to a system.

Password Cracking

- Manual password cracking means to logon with different passwords.
- Steps are as follow.
  - Find valid user account such as Administrator or Guest
  - Create a list of possible passwords.
  - Rank the passwords from high to low probability
  - key-in each password
  - Try again until a successful password is found.

Password Cracking

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;

9. Simple modification of one of the preceding, such as suffixing a digit, particularly 1, or reversing the order of letters.

Password Cracking

- To ensure the confidentiality of passwords, the password verification data is usually not stored in a clear text format.
- One-way function (Hash-function) is applied to the password, possibly in combination with other data, and the resulting value is stored.

Password Cracking

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).

Password Cracking

Online Attacks

- An attacker can create a script file (i.e. automated program) 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 eavesdropping 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 min-in-the-middle).
- This type of attack is used to obtain the passwords for E-Mail account on public websites such as Yahoo, Hotmail and Gmail .

Password Cracking

Type of Attack	*Description*	*Example of a Password*
Dictionary attack	Attempts to match all the words from the dictionary to get the password	Administrator
Hybrid attack	Substitutes numbers and symbols to get the password	Adm1n1strator
Brute force attack	Attempts all possible permutation-combinations of letters, numbers and special characters	Adm!n@09

Password Cracking

Offline Attacks

- Offline attacks usually require physical access to the computer and copying the password file from the system onto removable media.

Strong, Weak and Random Passwords

- A weak password is one, which could be easily guessed, short, common and a system default password that could be easily found by executing a brute force attack and by using a subset of all possible passwords.
- A strong password is long enough, random or otherwise difficult to guess – producible only by the user who chooses

Examples of Weak Password

1. **Susan:** Common personal name;
2. **aaaa:** repeated letters, can be guessed;
3. **rover:** common name for a pet, also a dictionary word;
4. **abc123:** can be easily guessed;
5. **admin:** can be easily guessed;
6. **1234:** can be easily guessed;
7. **QWERTY:** a sequence of adjacent letters on many keyboards;
8. **12/3/75:** date, possibly of personal importance;
9. **nbusr123:** probably a username, and if so, can be very easily guessed;
10. **p@$$\/\/0rd:** simple letter substitutions are preprogrammed into password cracking tools;
11. **password:** used very often – trivially guessed;
12. **December12:** using the date of a forced password change is very common.

Examples of Strong Password

Convert_£100 to Euros!: Such phrases are long, memorable and contain an extended symbol to increase the strength of the password.

382465304H: It is mix of numbers and a letter at the end, usually used on mass user accounts and such passwords can be generated randomly, for example, in schools and business.

4pRte!ai@3: It is not a dictionary word; however it has cases of alpha along with numeric and punctuation characters.

Password Cracking

Random Passwords

- **Password is stronger** if it includes a mix of

  upper and lower case letters,

  numbers and

  other symbols

- **Password is random**

  E.g. 26845 it seems random but it should be remember by the person who created it. It is just a 4 nos. selected on the square number board.

1	**2**	3
4	**5**	**6**
7	**8**	9

Password Cracking

The general guidelines applicable to the password policies are:

1. Passwords and user logon identities (IDs) should be unique to each authorized user.
2. Passwords should consist of a minimum of eight alphanumeric characters (no common names or phrases).
3. There should be computer-controlled lists of prescribed password rules and periodic testing (e.g., letter and number sequences, character repetition, initials, common words and standard names) to identify any password weaknesses.
4. Passwords should be kept private, that is, not shared with friends, colleagues, etc. They shall not be coded into programs or noted down anywhere.
5. Passwords shall be changed every 30/45 days or less. Most operating systems (OSs) can enforce a password with an automatic expiration and prevent repeated or reused passwords.
6. User accounts should be frozen after five failed logon attempts. All erroneous password entries should be recorded in an audit log for later inspection and action, as necessary.
7. Sessions should be suspended after 15 minutes (or other specified period) of inactivity and require the passwords to be re-entered.
8. Successful logons should display the date and time of the last logon and logoff.
9. Logon IDs and passwords should be suspended after a specified period of non-use.
10. For high-risk systems, after excessive violations, the system should generate an alarm and be able to simulate a continuing session (with dummy data) for the failed user (to keep this user connected while personnel attempt to investigate the incoming connection).

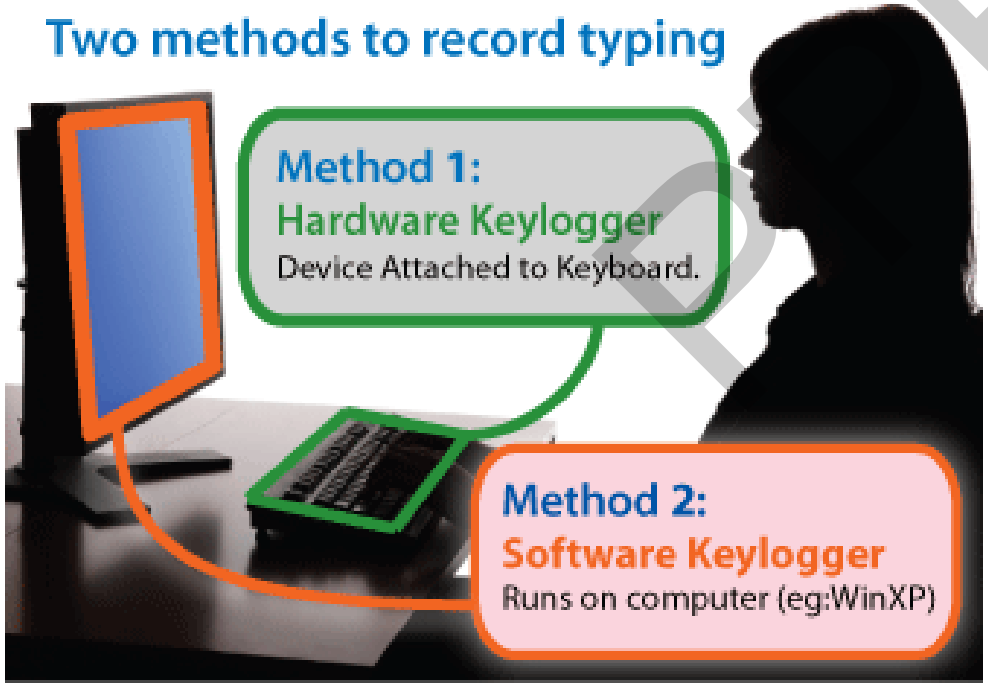
Password Cracking

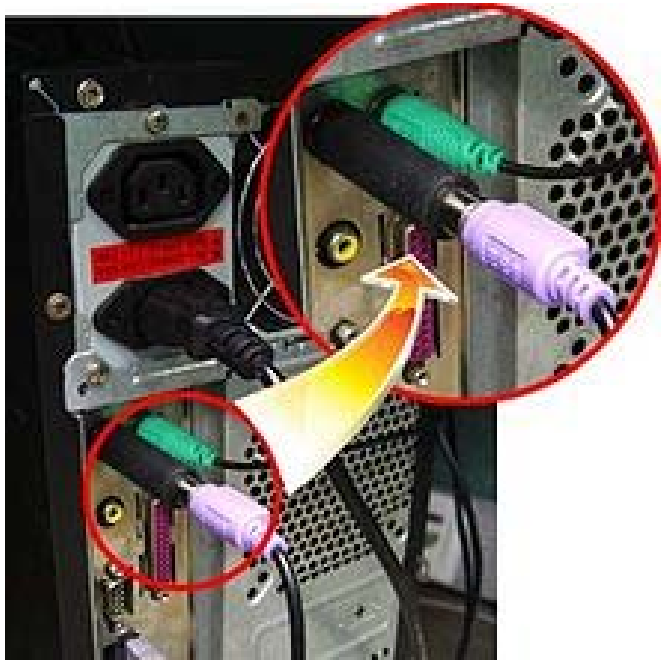
Password guidelines to safe email accounts:

1. Passwords used for business E-Mail accounts, personal E-Mail accounts (Yahoo/Hotmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading 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 (Yahoo/Hotmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading 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 cyber-attacks
8. In the case of receipt of an E-Mail from banking/financial institutions, instructing to change the passwords, before clicking the weblinks displayed in the E-Mail, legitimacy of the E-Mail should be ensured to avoid being a victim of Phishing attacks (we will explain Phishing attack in detail in
9. Similarly, in case of receipt of SMS from banking/financial institutions, instructing to change the passwords, legitimacy of the E-Mail should be ensured to avoid being a victim of Smishing attacks
10. In case E-Mail accounts/user accounts have been hacked, respective agencies/institutes should be contacted immediately.

Keyloggers

- Keystroke logging- practice of noting (or logging) the keys struck on a keyboard.
- 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**.





- It captures each key pressed on keyboard on a compromised system and transfer to attacker's computer.

Keyloggers

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.
- 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.

Hardware Keyloggers

- Hardware keyloggers are small hardware devices connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device.
- These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence.

Keyloggers

Antikeylogger

- Antikeylogger is a tool that can detect the keylogger installed on the computer system and also can remove the tool.

  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.

  3. Prevents Internet banking frauds.

  4. It prevents ID theft.

  5. It secures E-Mail and instant messaging/chatting.

- **Softwares :** Anti-Keylogger, SpyShelter, Apple Virtual Keyboard

Keyloggers

- **Windows** has a built-in Ease of Access tool called the **On-Screen Keyboard (OSK)** that can be used instead of a physical keyboard.

- You don't need a touchscreen to use the OSK. It displays a visual keyboard with all the standard keys, so you can use your mouse or another pointing device to select keys, or use a physical single key or group of keys to cycle through the keys on the screen.

To open the On-Screen Keyboard

- Go to **Start** , then select **Settings** > **Ease of Access** > **Keyboard**, and turn on the toggle under **Use the On-Screen Keyboard**. A keyboard that can be used to move around the screen and enter text will appear on the screen. The keyboard will remain on the screen until you close it.

Spywares

- Spyware is malicious software secretly installed on the user's personal computer.
- Spywares such as key loggers are installed by the owner of a shared, corporate or public computer on purpose to secretly monitor other users.

- It is a program that secretly record what you do on your computer.
- Its aim is usually to
  - Capture passwords of banking accounts, debit card, credit card etc.
  - Internet surfing habits / patterns
  - Website visited.

  and send them over the internet to fraudsters.

Virus and Worms

- Computer virus is a program that can “infect” genuine programs by modifying them to include a possibly “developed” copy of itself.
- A computer virus passes from computer to computer in a similar manner as a biological virus passes from person to person.
- 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 data such as Wednesday 31 March 2021)
  - 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;

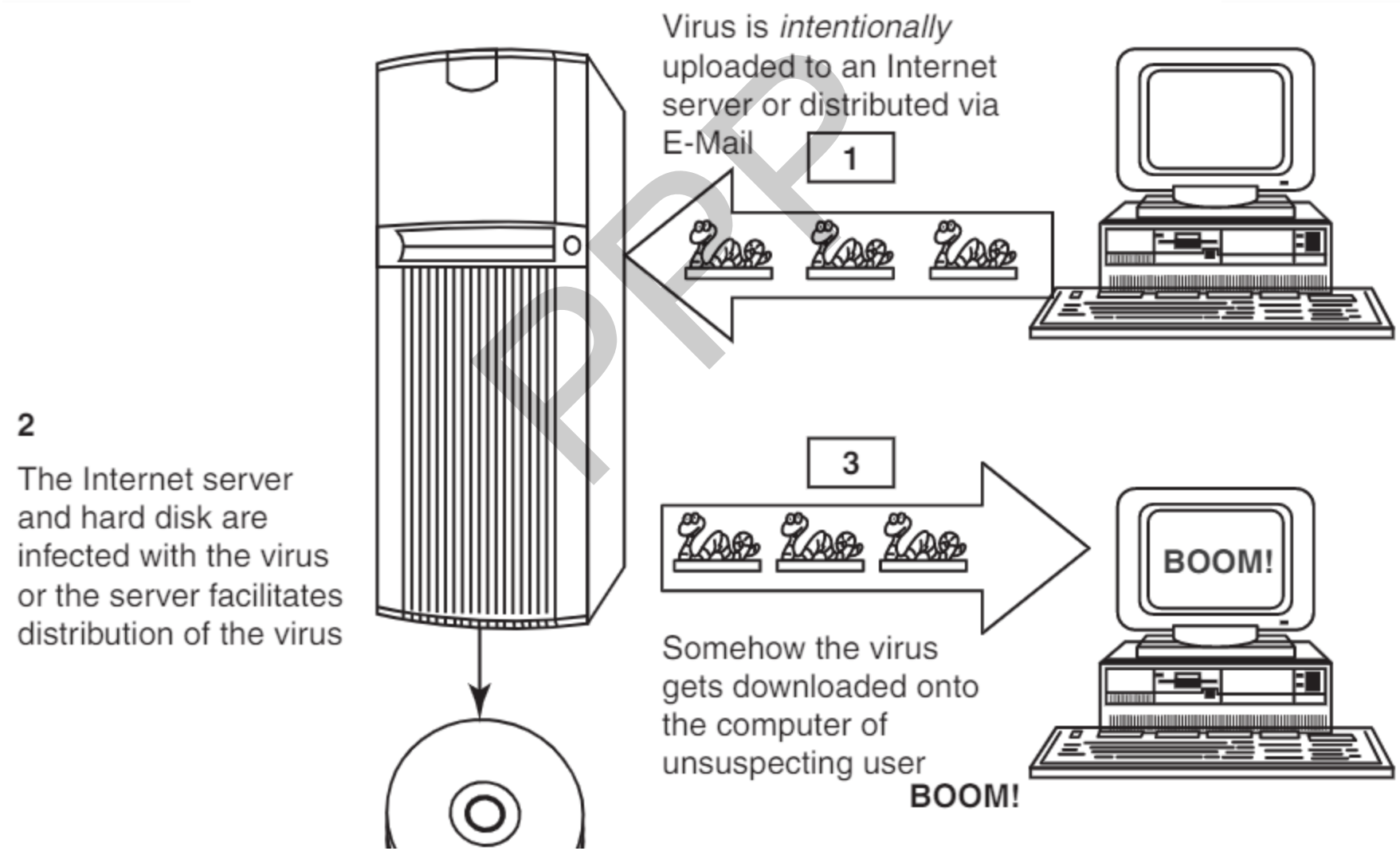
4. cause erratic screen behavior;

5. halt the system (PC);

6. just replicate themselves to propagate further harm

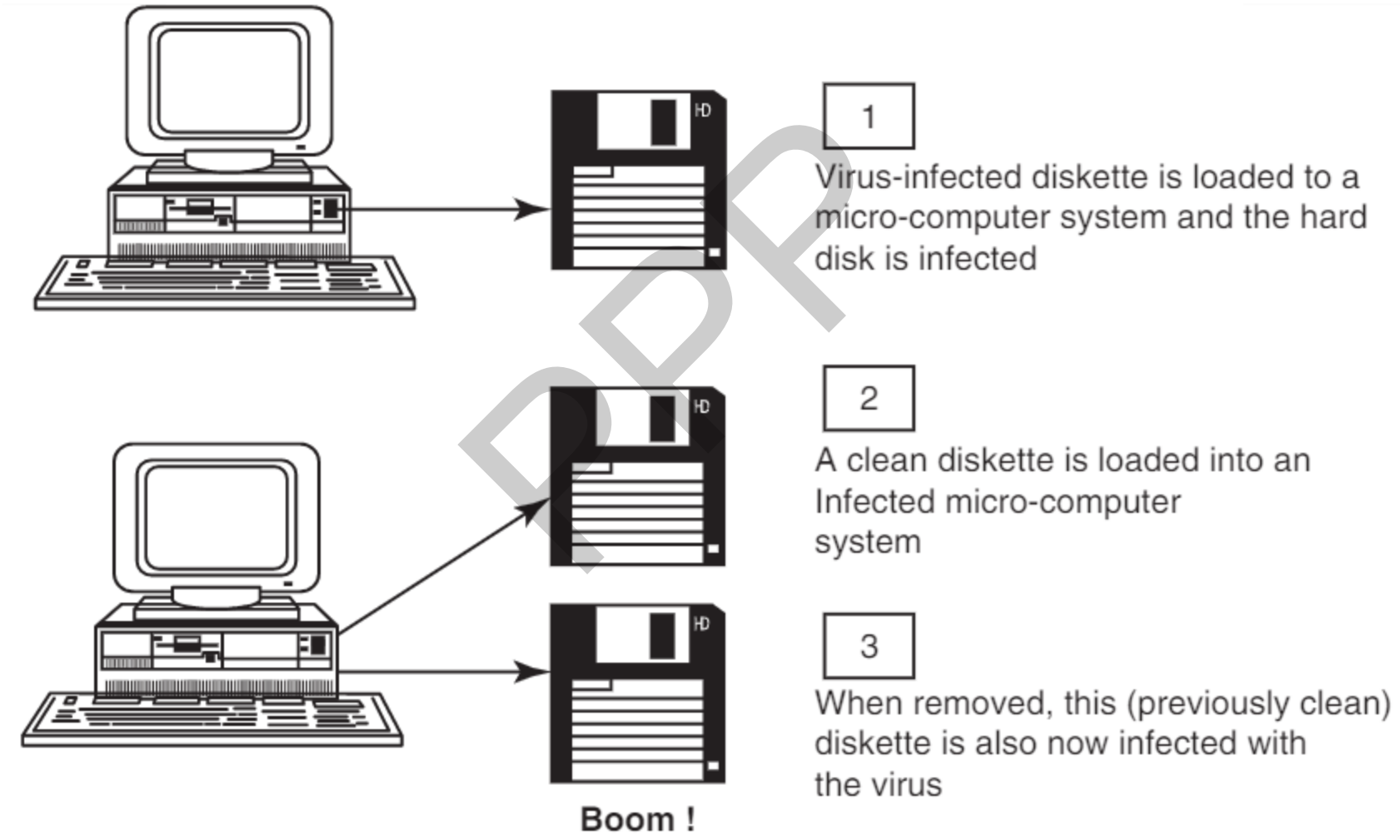
Virus and Worms

- **Virus spread through the Internet**



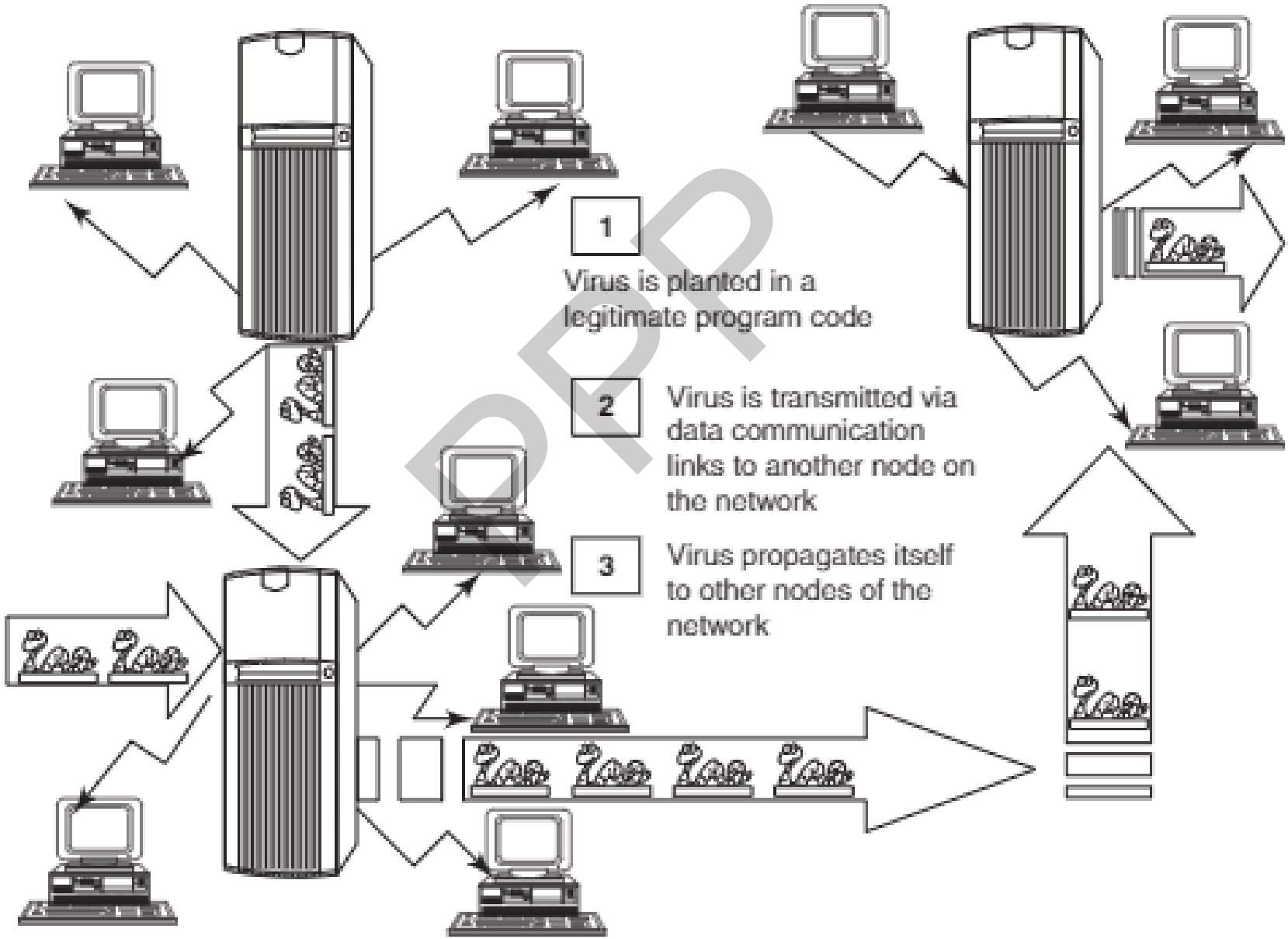
Virus and Worms

- **Virus spread through a stand-alone computer system**



Virus and Worms

- **Virus spread Through local network**



Virus and Worms

- 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.

E.g.

- When a user sent virus over the Internet or a network
- When carried it on a CD, DVD or USB drives.
- Virus 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.

Worms :

It is a software program, self-replicating in nature, which spreads through an network. It can send copies through the network with or without user intervention.

A worm spreads itself automatically to other computers through networks by exploiting security vulnerabilities.

Difference between Virus and Worms

Sr. No.	*Facet*	*Virus*	*Worm*
1	Different types	Stealth virus, self-modified virus, encryption with variable key virus, polymorphic code virus, metamorphic code virus	E-Mail worms, instant messaging worms, Internet worms, IRC worms, file-sharing networks worms
2	Spread mode	Needs a host program to spread	Self, without user intervention
3	What is it?	A computer virus is a software program that can copy itself and infect the data or information, without the users' knowledge. However, to spread to another computer, it needs a host program that carries the virus	A computer worm is a software program, self-replicating in nature, which spreads through a network. It can send copies through the network with or without user intervention
4	Inception	The creeper virus was considered as the first known virus. It was spread through ARPANET in the early 1970s. It spreads through the TENEX OS and uses connected modem to dial out to a remote computer and infect it.	The name worm originated from The Shockwave Rider, a science fiction novel published in 1975 by John Brunner. Later researchers John F Shock and Jon A Hupp at Xerox PARC published a paper in 1982, *The Worm Programs* and after that the name was adopted
5	Prevalence	Over 100,000 known computer viruses have been there though not all have attacked computers (till 2005)	Prevalence for virus is very high as against moderate prevalence for a worm.

Virus and Worms

Types of Viruses

- Computer viruses can be categorized based on attacks on various elements of the system and can put the system and personal data on the system in danger.

  1. Boot sector viruses :
  2. Program viruses
  3. Multipartite viruses
  4. Stealth viruses
  5. Polymorphic viruses
  6. Macroviruses
  7. Active X and Java Control

Virus and Worms

Types of Viruses

1.Boot sector viruses :

- It infects the storage media on which OS is stored and which is used to start the computer system.
- The data/program stored in the smallest sections called sectors.
- The first sector is called the BOOT and it carries the master boot record (MBR).
- MBR function is to read and load OS.
- If a virus attacks an MBR or infects the boot record of a disk, it infects victim hard drive when he/she will reboots the system.
- It is spread to other systems when shared infected disks and pirated software(s) are used.

2. Program viruses :

- It active when the program file is executed.
- Program extension like .exe , .bin , .ovl, .drv, .com.
- Once these files get infected, the virus infects other programs and make its copies itself.

Virus and Worms

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 camouflages and/or masks itself and so detecting this type of virus is very difficult.
- It alters its file size and hides itself in the computer memory to remain in the system undetected.
- Only a good antivirus can detect it.

5. Polymorphic viruses:

- It changes its virus signature(i.e. binary pattern) every time it spreads through the system.
- It can be linked with the existing viruses.

Virus and Worms

6. Macro viruses:

- Many applications, such as Microsoft word and excel support Macros.
- It is embedded in a document. Once it is activated then every document he/she produces will become infected.

7. Active X and Java Control:

- In browser settings about Active X and Java Controls.
- Managing and controlling these settings help to allow certain functions to work such as enabling or disabling pop-ups, downloading files etc.

Worms

A **computer worm** is a self-replicating malware computer program which uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention

Trojan Horse

– It is a program that looks very useful, but when you install the program, it also install a hidden malicious program.

Trojan Horse

- 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.
- Trojans can get into the system in a number of ways, including from a **web browser**, **via E-Mail** or **in a bundle with other software downloaded** from the Internet.
  - 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.
- E.g. waterfalls.scr is a waterfall screen saver as originally claimed by the author, however, it can be associated with malware and become a Torjan and unauthorized access to the user's PC.

Threats by Trojan Horse

- Erase, overwrite or corrupt data on a computer.
- Spread other malwares.
- Deactivate or interfere with antivirus ans firewall programs.
- Allow remote access to your computer
- Upload and Download files without your knowledge.
- Gather E-Mail addresses and use them for Spam.
- Log keystrokes to steal information such as passwords and credit card numbers.
- Copy fake links to false websites, display illegal sites, play sounds/videos and display images.
- Slow down, restart or shutdown the system.
- Reinstall themselves after being disabled.
- Disable the task manager.
- 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.

- An 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.

Functions of Backdoor

- Create, delete, rename, copy or edit any files, executes various commands, change system settings, windows registry, terminate applications, install softwares.
- Control computer hardware devices, shutdown or restart a computer without user permission.
- Steals sensitive personal information, valuable docs, Ids, web browsing habits, login names, passwords.
- It records keystrokes that a user types.
- Sends gathered data to a predefined E-Mail address to a FTP server.
- If infects files, corrupts installed apps and damages the entire system.
- Remote access of your computer system.
- Install hidden FTP server for illegal purposes.
- Reduce the speed of Internet connection.
- It provides no uninstall feature and hide processes to complication its removal.

Examples of Backdoor Trojans

- **Back Orifice:** Designed for remote system administration. To access Windows OS from a remote location.

- **Bifrost:** Allow a remote attacker to execute arbitrary code on the compromised machine.

- **SAP backdoors:** It present int SAP and get authentication information.

- **Onapsis Bizploit:** It helps security professionals in the discovery, exploration, vulnerability assessment and exploitation phases of specialized ERP penetration tests.

To Protect from Trojan Horses & Backdoors

- Stay away from suspect websites/weblinks
  - Avoid downloading free / pirated softwares.

- Surf on the Web cautiously
  - Avoid connecting with and/or downloading any information from peer-to-peer (P2P) networks. P2P networks create files packed with malicious software and rename them to files with the criteria of common search that are used while surfing the information on the web.

- Install antivirus/Trojan remover software

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 unavailable to its intended users.
- **DoS Attacks**
- The attacker floods the bandwidth of the victim's network or fills his E-Mail box with Spam mail, he is entitled to access or provide.
- 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:**

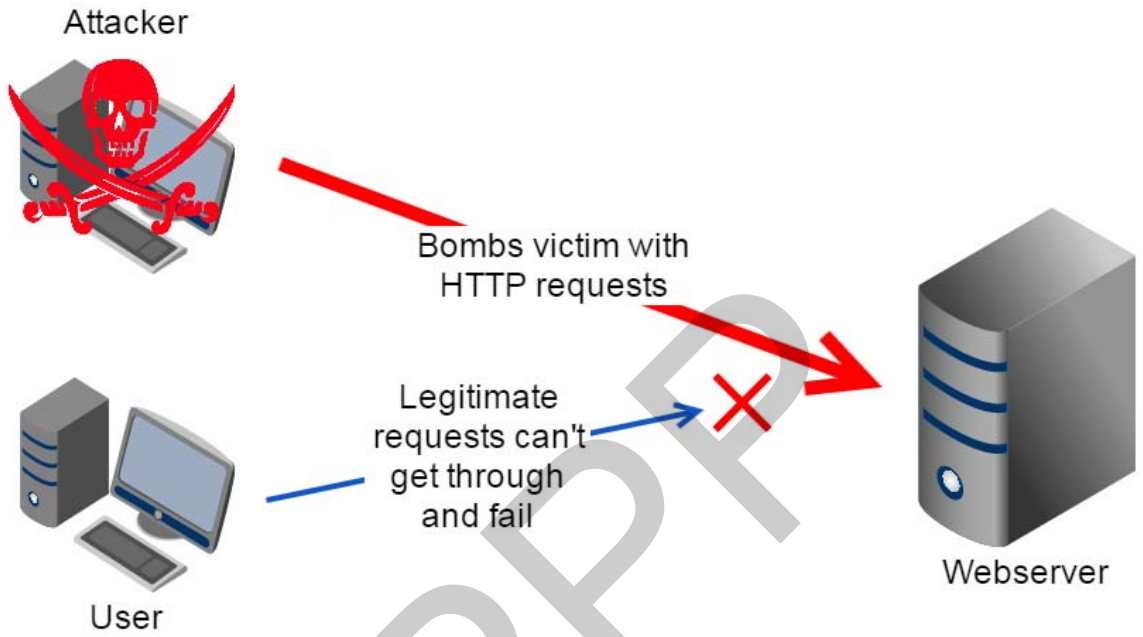
1. Flood a network with traffic, thereby stopping legitimate network traffic.

2. Disrupt connections between two systems, thereby preventing access to a service.

3. Prevent a particular individual from accessing a service.

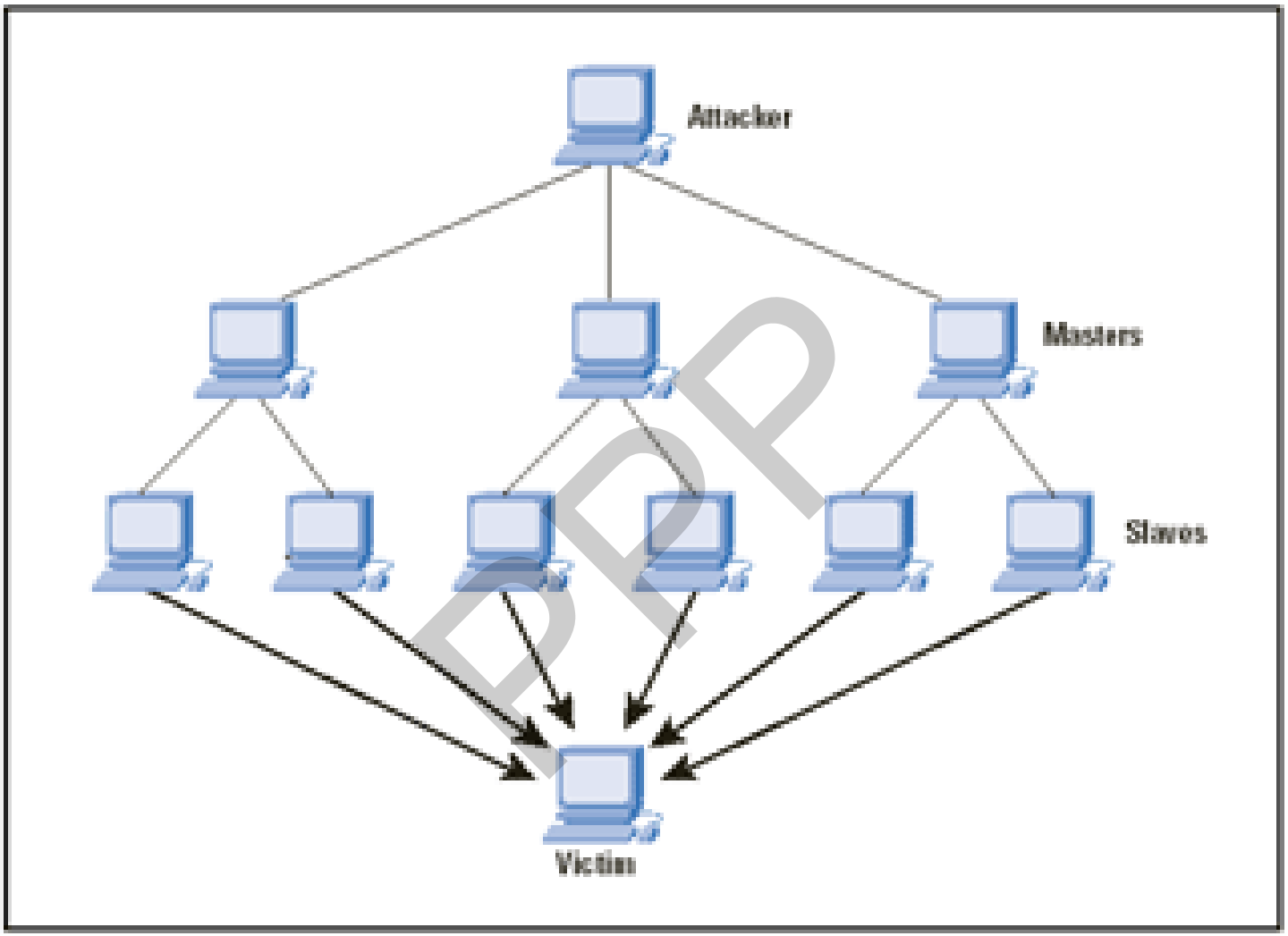
4. Disrupt service to a specific system or person.

DoS (Denial of Service)



- Attacker make the machine or network resource unavailable to its actual user by slow down or stop the services.

DDoS (Distributed Denial of Service)



- It is launched from multiple coordinated sources.
- Attacker target some master devices. Master devices target some slave devices. Slave devices attacks on server.

Classification of DoS attacks

- **Bandwidth attacks:** Every site is given with a particular amount of bandwidth for its hosting for example 50 GB. If more visitors consume all 50 GB bandwidht then the hosting of the site can ban this site. The attacker opens 100 pages of a site and keeps on refreshing and consuming all the bandwidth, thus the site becomes out of service.
- **Logic attacks:** It can exploit vulnerabilities in network software such as web server or TCP/IP stack.
- **Protocol attacks:** It exploit a bug of some protocol installed at the victim's system.
- **Unintentional DoS attack:** It can be happen when an extremely popular website posts a prominent link to a second website(less well-prepared website) as part of a news story. So regular users of primary sites click the link of second website and effect as DDoS attack.

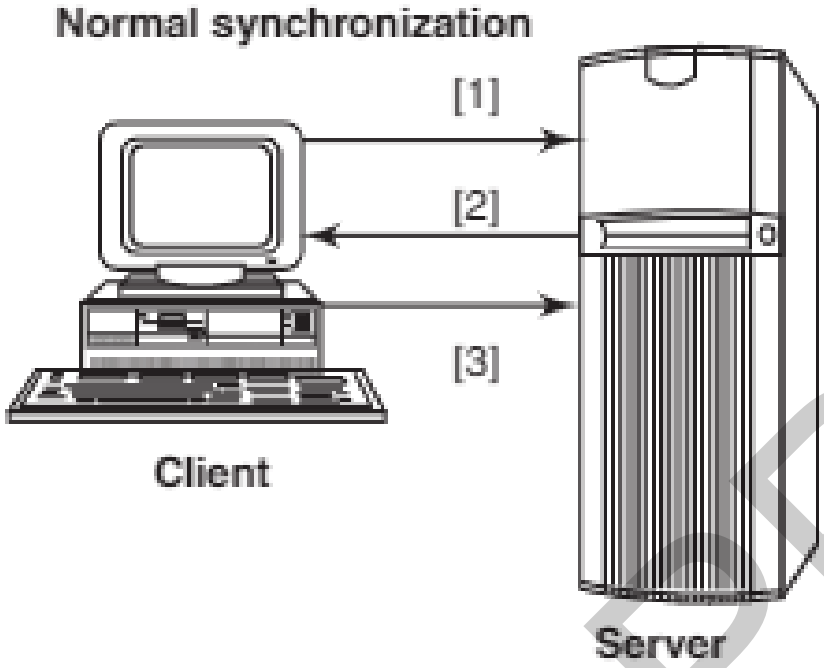
Types or Levels of DoS attacks

- **Flood attack:** Using ping command send a large number of ping packets to create more traffic than the victim can handle. Attacker needs faster network connection than the victim.

- **Ping of death attack:** It sends large number of ICMP (Internet Control Message Protocol) packets. It send error messages indicating (E.g. Requested service is not availble or host or router could not be reached) datagrams to the victim. It will crash, freeze or reboot system.

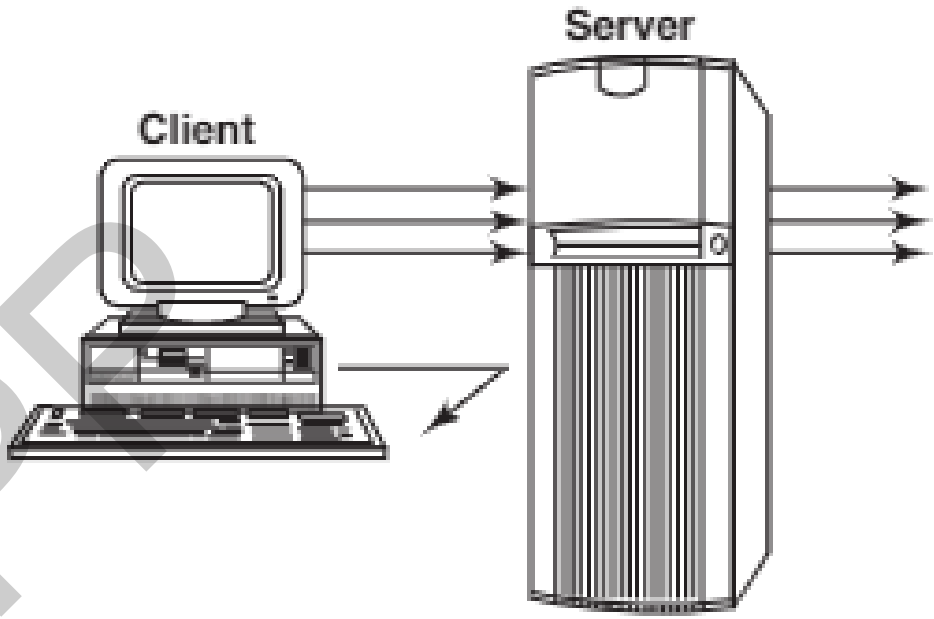
- **SYN attack (TCP SYN Flooding):** In TCP network connection is done with SYN and ACK messages. An attacker initiate a TCP connection to the server with an SYN. The server replies with SYN-ACK. The attacker does not send back an ACK, causing the server for wait. This fill up the buffer space for SYN messages on the targer system and stop its communication with other system.

DoS attack



3-way Handshake

- Client sends synchronize (syn) pkt to web server
- Server sends synchronize acknowledgment (syn-ack)
- Client replies with an acknowledgment pkt, the connect is established



Chaotic Handshake

- Client sends multiple synchronize (syn) pkts to web server – all with bad addresses
- Server sends synchronize acknowledgments to in correct addresses leaving half open connections and flooded queue
- Legitimate user is denied access because queue is full and additional connections cannot be accepted

Types or Levels of DoS attacks

- **Teardrop attack:** Fragmented packets are forged to overlap each other when the receiving host tries to reassemble them and system become hang. Windows (3.1x, 95, NT) Linux(prior to version 2.0.32 and 2.1.63) are vulnerable to this attack.

- **Smurf attack:** It is a way of generating significant computer network traffic on a victim network. Attacker sending an ICMP echo request (ping) by spoofed address of victim to a network broadcast address(N/w address with host part having all 1s). Every host in network sends ICMP response and increase network traffic. This creates flooding the victim.
- **Nuke:** It send invalid ICMP packets or framentation to the victim. It slow down the system until it comes to a complete stop. E.g. WinNuke send string of out-of-band data to TCP port 139 of the victim machine(Windows 95), causing it to lock up and display a Blue Screen of Death (BSOD).

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 take control of your computer.
- He/she could then force your computer to send huge amounts of data to a website or send Spam to particular E-Mail addresses.
- A DDoS attack is a distributed DoS wherein a large number of zombie systems are synchronized to attack a particular system. The zombie systems are called “secondary victims” and the main target is called “primary victim.”
- DDoS attacks involves hardcoding the target IP address prior to release of the malware, hence no further interaction is necessary to launch the attack.
- A system may also be compromised with a Trojan, allowing the attacker to download a zombie agent.

To Protect from DoS/DDoS Attacks

1. Implement router filters.

2. If such filters are available for your system, install patches to guard against TCP SYN flooding.

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.

To Protect from DoS/DDoS Attacks

7. Use Tripwire or a similar tool to detect changes in configuration information or other files.

8. Invest in and maintain “hot spares” – machines that can be placed into service quickly if a similar machine is disabled.

9. Invest in redundant and fault-tolerant network configurations.

10. Establish and maintain regular backup schedules and policies, particularly for important configuration information.

11. Establish and maintain appropriate password policies, especially access to highly privileged accounts such as Unix root or Microsoft Windows NT Administrator.

Tools used for detecting DoS/ DDoS attacks

- Zombie Zapper
- RID (Remote Intrusion Detector)
- SARA (Security Auditor's Research Assistant)
- DDoS Ping
- Find_DDoS

SQL Injection

- SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.
- The vulnerability is present when user input is either filtered incorrectly for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.
- Attackers target the SQL servers – common database servers used by many organizations to store confidential data.
- The main objective behind SQL injection attack is to obtain the information while accessing a database table that may contain personal information such as credit card / debit card numbers, social security numbers or passwords.
- During an SQL injection attack, Malicious Code is inserted into a web form field or the website's code to make a system execute a command shell or other arbitrary commands.

SQL Injection

- Just as a legitimate user enters queries and additions to the SQL database via a web form, the attacker can insert commands to the SQL server through the same web form field.
- **Example of SQL Vulnerabilities**
  - SELECT * FROM emp WHERE 1=1;

    NO NAME

    -- ------

    1 KARTIK

    2 KARVY
  - SELECT * FROM emp WHERE name = ' ' OR '1'='1‘

    NO NAME

    -- ------

    1 KARTIK

    2 KARVY

SQL Injection

- ***Blind SQL Injection***

- Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker.
- The page with the vulnerability may not be the one that displays data; however, it will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page.
- For such website automatic tools are used to find the weaknesses.
  - AppDetectivePro
  - DbProtect

SQL Injection

- **Using SQL injection attackers can**

1. Obtain some basic information like directory listing

2. May gain access to the database by obtaining username and their password.

   E.g. SELECT * FROM users WHERE name = 'OR '1'='1‘

3. Add new data to the database using INSERT command.

   E.g. Selling incorrect items on an E-commerce website.

4. Modify data to the database using UPDATE command.

   E.g. Expensive items becomes high discounted

How to Prevent SQL Injection Attacks

- SQL injection attacks occur due to poor website administration and coding. The following steps can be taken to prevent SQL injection.

1.Input validation

- Replace all single quotes to two single quotes
- User input needs to be checked. if character such s ; , --, select, insert , delete can be considered as malicious purpose
- For numeric value should be checked while accepting a query string value with IsNumeric() function in ASP.
- Limit the length of text boxes and form fields as its requirement.

2. SQL error should not be displayed to outside users by configure the error reports.

SQL Injection

3. Other preventions:

- Never used the default system accounts.

- Isolate database server and web server.

- Most often attackers may make use of several extended stored procedures such as xp_cmdshell and xp_grantlogin in SQL injection attacks. In case such extended stored procedures are moved to an isolated server.

Buffer Overflow

- Buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold.
- As buffers are created to contain a finite amount of data, the extra information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.
- Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.
- In C and C++, there are no automatic bounds checking on the buffer means user can write past a buffer.

  E.g. Following code is compiled without any errors. But the result is an unexpected behavior.

```
int buffer[10]
buffer[15] = 212;
```

How to Minimize Buffer Overflow

- **The following methods will definitely help to minimize such attacks:**

1. **Assessment of secure code manually:** Do not use vulnerable functions in C library such as strcpy(), strcat(), sprintf() and vsprintf() which operates on null-terminated strings and perform no bounds checking. The input validation after scanf() function is very essential.
2. **Disable stack execution :** Stack is not allowed to execute any instructions.
3. **Compiler tools :** It warning on the use of unsafe constructs such as gets(), strcpy() etc. Developers need to change the structure of code.
4. **Various tools are used to detect/defend buffer overflow**

   StackGuard, ProPolice, LibSafe

Phishing

- It is the criminally fraudulent process of attempting to acquire sensitive information such as

  usernames,

  passwords,

  credit / debit card details

by masquerading as a trustworthy entity in an electronic communication.

Email is the popular medium used in the Phishing attacks and such emails are called Spams.

Spam E-Mails

- Also known as “junk E-Mails”
- Identical messages are sent to numerous recipients
- Popular medium for phishers to scam users to enter personal information on fake websites
- A person who creates electronic spam is called a spammer

Phishing

- **Types of SPAM Emails**

1. Unsolicited bulk E-Mail (UBE) : It is sent in large quantity.
2. Unsolicited commercial E-Mail (UCE) : It is sent in large quantity but from commercial perspective, for example advertising.

- **Tactics used by a phisher**

1. Names of legitimate organizations
2. “From” a real employee
3. URLs that “look right”
4. Urgent messages

- **Phrases used to entice the user**

1. “Verify your account”
2. “You have won the lottery”
3. “If you don’t respond within 48 hours, your account will be closed”

Phishing

Ways to reduce the SPAM E-mails

- Shared personal E-mail address with limited people and/or on public websites.
- Never reply or open any Spam E-mails.
- Write the E-mail address as Raj**AT**gmail**DOT**com. It is difficult for phishers to catch it with program.
- Keep separation between personal and business emails.
- Do not forward any E-mails from unknown recipients.
- Make a habit to preview an E-mail before opening it.
- Never use E-mail address as screen name in groups or rooms.
- Never respond to a Spam E-mail

Hoax E-Mails

✓Deliberate attempt to deceive or trick a user into believing or accepting that something is real.

✓Hoax E-Mails may or may not be Spam E-Mails.

Methods of Phishing

Methods used by phishers to gain personal information of netizen

1.Dragnet

- By false information in an E-mail to trigger an immediate response by victims.
- Clicking on links in the body of the E-mail to take the victims to the websites or pop-up windows where they are requested to enter bank or credit card account data or other personal data.

2. Rod-and-reel :

- Phishers identify specific victims in advance and covey false information to them to prompt their disclosure of personal and financial data.
- **E.g.** On false webpage show the product with better price which the victim may be searching for and upon visiting the webpage, victims were asked for credential information, before confirming that the "sale" and information is available to the phisher easily.

Methods of Phishing

3. Lobsterpot:

- If focuses upon use of spoofed website. Creating of bogus/phony websites, similar to legitimate corporate ones, targeting a narrowly defined class of victims.
- Once the netizen is access spoofed site, he/she send personal information.
- The attacker use that information to purchase goods, apply for a new credit card or steal your identity.

4. Gillnet

- Phishers introduce Malicious Code into E-Mails and websites
- By opening a particular E-mail or browsing a particular website, Trojan Horse comes into victim systems.
- Malicious code may redirect the victim from legitimate banking website to a phishing site.
- Malicious code may record user's keystrokes, passwords and use it for illegal access to users financial accounts.

Phishing Techniques

Techniques used by phisher to launch Phishing attacks

1. **URL (weblink) manipulation :** In this technique the URLs are misspelled. **E.g.** Instead of abcbank.com URL is provided as abcbank1.com or abcbank.edu or abebank.com

2. Filter evasion: Phishers have used images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing e-mails.

3. Website forgery: In this technique the phisher directs the netizens to the website designed and developed by him, to login into the website, by altering he browser address bar through JavaScript commands.

4. Flash Phishing: flash object contain video or animations and sound and are designed for efficient delivery over the web. Anti-Phishing toolbars are installed/enabled to help checking phishing attacks but have limitations that they do not analyze flash object at all. Netizens believe that the website is "clean" and is a real website because anti-phishing toolbar is unable to detect it.

Phishing

5. Social Phishing : Phisher attract the netizens to provide sensitive data

- Phisher sends a mail as if it is sent by a bank asking to call them back because there was a security breach.
- Victim calls the bank on the phone numbers displayed in the mail.
- The phone number provided in the mail is a false number and the victim gets redirected to the phisher.
- Phisher speaks with the victim in the similar fashion/style as a bank employee, asking to verify that the victim is the customer of the bank. For example, "Sir, we need to make usre that you are indeed our customer. Could you please supply your credit card information so that I can verify your identity?"
- Phisher gets the required details swimmingly.

6. Phone Phishing : Phisher can use a fake caller ID data to make it appear that the call is received from a trusted organization to entice the users to reveal their personal information such as account numbers and passwords.

Spear Phishing

- A method of sending a Phishing message to a particular organization to gain organizational information for more targeted social engineering.

- Spear phishers send E-Mail that appears genuine.

- The message might look like as if it has come from your employer, or from a colleague who might send an E-Mail message to everyone in the company (such as the person who manages the computer systems); it could include requests for usernames or passwords.

Whaling

- A specific form of “Phishing” and/or “Spear Phishing” – targeting executives from the top management in the organizations, usually from private companies.
- The objective is to fraud the executives into revealing confidential information.
- Whaling targets C-level executives sometimes with the help of information collected through Spear Phishing, aimed at installing malware for keylogging or other backdoor access mechanisms.
- E-Mails sent in the whaling scams are designed to masquerade as a critical business E-Mail sent from a legitimate business body and/or business authority.
- Whaling phishers have also forged official looking FBI summons E-Mails and claimed that the manager needs to click a link and install special software to view the summons.

Phishing Countermeasures

- ✓The countermeasures prevent malicious attacks that phisher may target to gain the unauthorized access to the system to steal the relevant personal information about the victim, from the system.

- ✓It is always challenging to recognize/judge the legitimacy of a website while Googling.

Phishing Countermeasures

Sr. No.	*Security Measures*	*Brief Description*
1	Keep antivirus up to date	Important aspect is to keep antivirus software up to date because most antivirus vendors have signatures that protect against some common technology exploits. This can prevent things such as a Trojan disguising the web address bar or mimicking the secure link (i.e., HTTPS)
2	Do not click on hyperlinks in E-Mails	It should always be practiced that, in case an E-Mail has been received from unknown source, clicking on any hyperlinks displayed in an E-Mail should be avoided. This may lead to either the link taking the victim to the website created by the phisher or triggering a Malicious Code installation on the system. Instead, to check out the link, manually retyping it into a web browser is highly recommended.
3	Take advantage of anti-Spam software	Anti-Spam software can help keep Phishing attacks at a minimum. A lot of attacks come in the form of Spam and by using anti-Spam software, many types of Phishing attacks are reduced because the messages will never end up in the mailboxes of end-users.
4	Verify https (SSL)	Ensure the address bar displays "https://" rather than just "http://" along with a secure lock icon than has been displayed at the bottom right-hand corner of the web browser while passing any sensitive information such as credit cards or bank information. One may like to check by double-clicking the lock to guarantee the third-party SSL certificate that provides the https service. Always ensure that the webpage is truly encrypted.

Phishing Countermeasures

4	Verify https (SSL)	Ensure the address bar displays "https://" rather than just "http://" along with a secure lock icon than has been displayed at the bottom right-hand corner of the web browser while passing any sensitive information such as credit cards or bank information. One may like to check by double-clicking the lock to guarantee the third-party SSL certificate that provides the https service. Always ensure that the webpage is truly encrypted.
5	Use anti-Spyware software	Keep Spyware down to a minimum by installing an active Spyware solution such as Microsoft anti-Spyware and also scanning with a passive solution such as Spybot. If for some reason your browser is hijacked, anti-Spyware software can often detect the problem and provide a fix.
6	Get educated	Always update the knowledge to know new tools and techniques used by phishers to entice the netizens and to understand how to prevent these types of attacks. Report any suspicious activity observed to nearest cyber-security cell.
7	Use the Microsoft Baseline Security Analyzer (MBSA)	The netizens on the Microsoft platform should use MBSA to ensure the system is up to date by applying all the security patches. MBSA is a free tool available on Microsoft's website. This protects the IT systems against known exploits in Internet Explorer and Outlook (and Outlook Express) that can be used in Phishing attacks.
8	Firewall	Firewall can prevent Malicious Code from entering into the system and hijacking the browser. Hence, a desktop (software) such as Microsoft's built-in software firewall in Windows-XP and/or network (hardware) firewall should be used. It should be up to date in case any cybersecurity patches have been released by the vendor.

Phishing Countermeasures

9	Use backup system images	Always keep a backup copy or image of all systems to enable to revert to a original system state in case of any foul play.
10	Do not enter sensitive or financial information into pop-up windows	A common Phishing technique is to launch a bogus pop-up window when someone clicks on a link in a Phishing E-Mail message. This window may even be positioned directly over a legitimate window a netizen trusts. Even if the pop-up window looks official or claims to be secure, entering sensitive information should be avoided because there is no way to check the security certificate.
11	Secure the hosts file	The attacker can compromise the hosts file on desktop system and send a netizen to a fraudulent site. Configuring the host file to read-only may alleviate the problem, but complete protection will depend on having a good desktop firewall such as Zone Alarm that protects against tampering by outside attackers and keeps browsing safe.
12	Protect against DNS Pharming attacks	This is a new type of Phishing attack that does not Spam you with E-Mails but poisons your local DNS server to redirect your web requests to a different website that looks similar to a company website (e.g., eBay or PayPal). This is explained in Box 5.11.

Identity Theft (ID Theft)

- Fraud that involves someone pretending to be someone else to steal money or get other benefits.

- The person whose identity is used can suffer various consequences when he/she is held responsible for the criminal's actions.

- **Major Identity Frauds**

1. Credit card fraud
2. Bank fraud
3. Employment fraud
4. Government fraud
5. Loan fraud

Personally Identifiable Information (PII)

Fraudsters attempts to steal the elements mentioned below:

1. Full name

2. National identification number (e.g., SSN (Social Security Number)

3. Telephone and mobile phone numbers

4. Driver's license number

5. Credit card numbers

6. Digital identity (e.g., E-Mail address, online account ID and password)

7. Birth date and Place name

9. Face and fingerprints

Identity Theft (ID Theft)

A fraudster generally searches the following about an individual:

1. First or last name
2. age
3. country, state or city of residence
4. gender
5. name of the school/college/workplace
6. job position, grades and/or salary
7. criminal record

Types of Identity Theft

1. **Financial Identity Theft :**

- It includes bank fraud, credit card fraud, tax refund fraud, mail fraud etc. Such frauds happen when a fraudster makes a use of someone else's identifying details such as name, SSN and bank account details.
- E.g. Open an new credit card account, open new bank account, purchase vehicle, home mortgage etc.

2. **Criminal Identity Theft :**

- It involves commit a crime such as enter into a country, get special permits, hide one's own identity or commit acts of terrorism. The criminar activities like Computer and cybercrimes, Organized crime, Drug trafficking, Unknown smuggling, Money laundering.
- Fraudster may give falsy document such as License, Birth certificate etc to a law enforcement officer and appear in court.
- The victim of criminal ID theft may not know what warrant has been issued under his/her name for quite some time.

Identity Theft (ID Theft)

3. **Identity Cloning :**

- Identity clone living a natural and usual life similar to a victim's life, may be a at a different location. Fradster may be able to give answer about the victim's life.
- Fraudster have following personal information about the victim.
  - Birth date, city, state
  - School details
  - Job details
  - Friends details
  - Parents and other family members
  - Various IDs and accounts

Identity Theft (ID Theft)

4. **Business Identity Theft :**

- A fraudster rents a space in the same building as victim's office. Then he applies for corporate credit cards using victim's firm name.
- The application passes a credit check because the company name and address match, but the cards are delivered to the fraudster's mailbox.
- He/She sells them before the victim discovers.

5. **Medical Identity Theft :**

- Lots of tourists, every year visit India with dual purpose - touring the country plus getting their medical problems (surgeries, health checkup etc.) because in India it is low price and good quality.
- Today multiple agencies like health officers, Doctors, Medial representative, Medical insurance organizations, hospitals etc. are connected over Internet.
- Medical Identity theft can be dangerous from a financial as well as medical perspective.

Identity Theft (ID Theft)

6. **Synthetic Identity Theft :**

- The fraudster will take parts of personal informatio from many victims and combine them.
- The new identity is not any specific person, but all the victims can be affected when it us used.

7. **Child Identity Theft :**

- Parents might use their children's identity to open bank account, loans or secure leases because their own credit history is insufficient to open such account.

Identity Theft (ID Theft) : Countermeasures

Sr. No.	*Security Measures*	*Brief Description*
1	Monitor your credit closely	The credit report contains information about your credit accounts and bill paying history so that you can be tipped off when someone is impersonating you. Watch for suspicious signs such as accounts you did not open. You can also consider identity protection services, which range from credit monitoring to database scanning, for extra security.
2	Keep records of your financial data and transactions	Review your statements regularly for any activity or charges you did not make.
3	Install security software	Install security software (firewall, antivirus and anti-Spyware software) and keep it up to date as a safety measure against online intrusions.
4	Use an updated Web browser	Use an updated web browser to make sure you're taking advantage of its current safety features.
5	Be wary of E-Mail attachments and links in both E-Mail and instant messages.	Use caution even when the message appears to come from a safe sender, as identity information in messages can easily be spoofed
6	Store sensitive data securely	Just as you keep sensitive paper documents under lock and key, secure sensitive online information. This can be done through file encryption software.

Identity Theft (ID Theft)

7	Shred documents	It is important to shred the documents that contain personal or financial information (both paper and electronic) before discarding them. This prevents dumpster diving and, in the online world, the ability for hackers to bypass information that has not been permanently deleted from your system.
8	Protect your PII	Be cautious about giving out your personally identifiable information (PII) to anyone. Find out why the information is needed, and if it's absolutely necessary to give out. Be careful about the details you provide about yourself online, such as on social networking sites.
9	Stay alert to the latest scams	Awareness and caution are effective methods to counter fraud. Create awareness among your friends and family members by sharing security tips you learn with them.

Networking Commands

PING (Packet Internet Groper)

- It is used detecting devices on network and troubleshooting network problems.
- It will help to see the connection between your device and another device on the network.
- If we receive a reply from the device then the device is working properly.
- We can use this command with an IP address and hostname.
- We have searched for the website. 0% data loss while sending the number of packages. Success result is present round trip times in milliseconds.
- The PING utility tests connectivity between two hosts. PING uses a special protocol called the Internet Control Message Protocol (ICMP) to determine whether the remote machine (website, server, etc.) can receive the test packet and reply.

Networking Commands

PING

- **Use for two main purposes**

  To find out a host is responding

  To find out if you can reach a host.

- Also a great way to verify whether you have TCP/IP installed and your Network Card is working.
- Pinging the loopback address (127.0.0.1) to verify that TCP/IP is installed and configured correctly on the local computer.
- > **ping URL / IP Address**

```
>ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_req=1 ttl=64 time=0.031 ms
64 bytes from 127.0.0.1: icmp_req=2 ttl=64 time=0.022 ms
64 bytes from 127.0.0.1: icmp_req=3 ttl=64 time=0.022 ms
64 bytes from 127.0.0.1: icmp_req=4 ttl=64 time=0.023 ms
64 bytes from 127.0.0.1: icmp_req=5 ttl=64 time=0.023 ms
64 bytes from 127.0.0.1: icmp_req=6 ttl=64 time=0.026 ms
```

Networking Commands

PING

```
C:\Users\Administrator>ping www.yahoo.com

Pinging new-fp-shed.wg1.b.yahoo.com [202.165.107.50] with 32 bytes of data:
Reply from 202.165.107.50: bytes=32 time=85ms TTL=48
Reply from 202.165.107.50: bytes=32 time=83ms TTL=48
Reply from 202.165.107.50: bytes=32 time=109ms TTL=48
Reply from 202.165.107.50: bytes=32 time=84ms TTL=48

Ping statistics for 202.165.107.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 83ms, Maximum = 109ms, Average = 90ms
```

Networking Commands

- ***Netstat*** **(Network Statistics)**
  - It is used for network statics, diagnostics, and analysis.
  - If we are managing a huge college campus network, then this tool is useful because it provides an advanced aspect of the network.
  - Netstat Displays network connections (both incoming and outgoing),
    - Number of network interface statistics.
    - Display packet counts
    - Display of input/output packet counts per interface
    - Display of TCP/UDP sockets in use on a host
    - Display of the routing tables for a host

Networking Commands

Netstat

- To know the usage of port
- Displays protocol statistics and current TCP/IP network connections.
- Without option it display current active connections.
- **Options**
  - -a Displays all connections and listening ports.
  - -r Displays the routing table.
  - -e Displays Ethernet statistics. No. of bytes sent, received etc.
  - -f Displays Fully Qualified Domain Names (FQDN) for foreign addresses.
  - -n Displays addresses and port numbers in numerical form.

Networking Commands

ARP (Address Resolution Protocol)

- ARP stands for Address Resolution Protocol.

- The arp cache results are dynamic and displays the IP and MAC address of devices (computers, routers) your computer network communicated with recently that are on your network.

- To start the Command Prompt in “administrative mode”, open the Search programs dialog (not Run dialog) in the Start Menu, type cmd or cmd.exe and press [CTRL]+[SHIFT]+[ENTER] together.

Networking Commands

ARP (Address Resolution Protocol)

- **Options:**

  -a Displays current ARP entries by interrogating the current protocol data. more than one network interface uses ARP, entries for each ARP table are displayed.

  -s Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is given as six hexadecimal bytes separated by hyphens. The entry is permanent.

arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.

Networking Commands

Nslookup (Name Server lookup)

- It is a useful tool for finding out information about a domain name.
- it will translate a domain name to an IP address (or vice versa).
- When we want to know the IP address of the domain we can use this command.
- If we run this command over and over, we will get different IP addresses for a website like google, yahoo, Flipkart because these domains have spread to different machines.
- Example

  >**nslookup microsoft.com**

  Server: 8.8.8.8 //Address of DNS Server

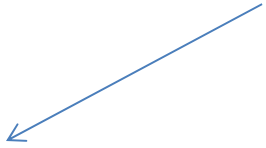
  Address: 8.8.8.8#53 // Port number of DNS Server to accept query

  Non-authoritative answer:

  Name: microsoft.com

  Address: 134.170.185.46  //You may be directed to either of server

  Name: microsoft.com

  Address: 134.170.188.221 

Networking Commands

Nslookup (Name Server lookup)

```
C:\Users\Administrator>nslookup www.yahoo.com
Server:  UnKnown
Address:  172.16.16.250

Non-authoritative answer:
Name:    new-fp-shed.wg1.b.yahoo.com
Addresses:  2406:2000:e4:1605::9001
          2406:2000:e4:1605::9000
          202.165.107.49
          202.165.107.50
Aliases:  www.yahoo.com
```

- **Reverse Nslookup (IP address to Domain Name)**

> nslookup 134.170.185.46

Server: UnKnown

Address: 172.16.16.250

Name: conformite-logiciels.com

Address: 134.170.185.46

Networking Commands

- **Querying The NS Record Of A Domain**
- The NS Record of a domain is a map of all name servers that are authoritative for that domain.
- You can query a domain's NS Record using the option **-type=ns**, like this:
- > **nslookup -type=ns microsoft.com**

Server: UnKnown

Address: 172.16.16.250

Non-authoritative answer:

microsoft.com nameserver = ns4-205.azure-dns.info

microsoft.com nameserver = ns1-205.azure-dns.com

microsoft.com nameserver = ns3-205.azure-dns.org

microsoft.com nameserver = ns2-205.azure-dns.net

Networking Commands

- **Querying The MX Record**
- The MX Record is a map of mail exchange servers for a domain.
- When you send email to a domain, for example "@microsoft.com", mail is routed to Microsoft's MX servers.
- You can query a domain for its MX Record using the

  -type=mx option.

For example:

> nslookup -type=mx microsoft.com

Server: UnKnown

Address: 172.16.16.250

Non-authoritative answer:

microsoft.com   MX preference = 10,

mail exchanger = microsoft-com.mail.protection.outlook.com

Networking Commands

traceroute

> traceroute remote system name / ip address

- when we face any network issue and to troubleshoot this issue Traceroute will send the route of the packet from server to server as hope.
- It will show a delay between user and hop.
- The IP address of the hop will be shown.
- It Print the route that packets take to the specified network host.
- It may not be your computer but something that is down along the way.
- It can also tell you if communication is slow because a link has gone down between you and the destination.

Networking Commands

TRACEROUTE

> traceroute remote system name / ip address

Example

> tracert www.google.com

Tracing route to www.google.com [142.250.194.196]
over a maximum of 30 hops:

1	1 ms	1 ms	1 ms	172.16.40.254
2	1 ms	1 ms	1 ms	172.16.16.251
3	3 ms	2 ms	3 ms	10.119.237.57
4	27 ms	19 ms	19 ms	10.154.7.129
5	34 ms	32 ms	34 ms	10.255.238.181
6	37 ms	41 ms	41 ms	10.1.200.138
7	19 ms	22 ms	23 ms	10.119.234.162
8	70 ms	55 ms	67 ms	72.14.195.56
9	59 ms	53 ms	76 ms	108.170.251.97
10	62 ms	55 ms	54 ms	142.251.52.207
11	55 ms	56 ms	55 ms	**del12s07-in-f4.1e100.net [142.250.194.196]**

Trace complete.

- **Three latency reading per hop because tracert will send 3 packets per hop**

Networking Commands

TRACEROUTE

Options:

- **-d** Do not resolve addresses to hostnames.
- **-h maximum_hops** Maximum number of hops to search for target.

–d to disable IP address and host name mapping

> tracert -d www.google.com

Tracing route to www.google.com [216.58.221.36]
over a maximum of 30 hops:

1	36 ms	21 ms	20 ms	172.16.40.254
2	1 ms	1 ms	1 ms	172.16.16.251
3	12 ms	7 ms	6 ms	10.119.237.57
4	32 ms	21 ms	20 ms	10.154.7.129
5	19 ms	35 ms	33 ms	10.255.238.181
6	24 ms	20 ms	19 ms	10.1.200.138
7	20 ms	33 ms	19 ms	10.119.234.162
8	72 ms	65 ms	68 ms	72.14.194.160
9	55 ms	55 ms	56 ms	108.170.251.113
10	61 ms	55 ms	63 ms	216.239.57.113
11	64 ms	66 ms	71 ms	**216.58.221.36**

Trace complete.

Networking Commands

Traceroute

-h maximum_hops Maximum number of hops to search for target.

> tracert -h 4 www.google.com

Tracing route to www.google.com [142.250.194.164]
over a **maximum of 4 hops:**

1	1 ms	1 ms	1 ms	172.16.40.254
2	42 ms	40 ms	43 ms	172.16.16.251
3	28 ms	32 ms	16 ms	10.119.237.57
4	51 ms	49 ms	54 ms	10.154.7.129

Trace complete.

Networking Commands

IPConfig

- find network information local devices like IP Address and default gateway.
- ipconfig (Internet Protocol configuration) is among the most common networking tool that allows you to query and show current TCP/IP (Transmission Control Protocol/Internet Protocol) network configuration.
- **> ipconfig**

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::9c53:fb03:3119:6fbf%19
IPv4 Address. . . . . : 172.16.40.112
Subnet Mask . . . . . : 255.255.255.0
IPv4 Address. . . . . : 192.168.8.48
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.40.254

Networking Commands

IPConfig

> ipconfig /all

Windows IP Configuration

Host Name . . . . . : GDCST-203-48

Primary Dns Suffix . . . . . :

Node Type . . . . . : Hybrid

IP Routing Enabled. . . . . : No

WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

Description . . . . . : Realtek PCIe GbE Family Controller

Physical Address. . . . . : 8C-EC-4B-56-4E-3A

DHCP Enabled. . . . . : No

Autoconfiguration Enabled . . . . : Yes

Link-local IPv6 Address . . . . . : fe80::9c53:fb03:3119:6fbf%19(Preferred)

IPv4 Address. . . . . : 172.16.40.112(Preferred)

Subnet Mask . . . . . : 255.255.255.0

IPv4 Address. . . . . : 192.168.8.48(Preferred)

Subnet Mask . . . . . : 255.255.255.0

Networking Commands

IPConfig (output continue of pevious command : ipconfig /all)

Default Gateway . . . . . : 172.16.40.254
DHCPv6 IAID . . . . . : 378334283
DHCPv6 Client DUID. . . . . : 00-01-00-01-22-DB-0A-C9-8C-EC-4B-56-4E-3A
DNS Servers . . . . . : 172.16.16.250
NetBIOS over Tcpip. . . . . : Enabled
Ethernet adapter Bluetooth Network Connection 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Bluetooth Device (Personal Area Network) #2
Physical Address. . . . . : 9C-30-5B-E7-4A-B2
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

- **To remove the current network configuration and press Enter:**
  > ipconfig /release
- **To reconfigure the network configuration and press Enter:**
  > ipconfig /renew