TOOLS AND METHODS USED IN CYBERCRIME:

INTRODUCTION
PROXY SERVERS AND ANONYMIZERS
PHISHING
PASSWORD CRACKING
KEYLOGGERS AND SPYWARES
VIRUS AND WORMS
TROJAN HORSE AND BACKDOORS
STEGANOGRAPHY
DOS AND DDOS ATTACKS
SQL INJECTION
BUFFER OVERFLOW

UNIT-4

INTRODUCTION

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

1. Initial uncovering:
   - Two steps are involved here.

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

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

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

INTRODUCTION

3. Crossing the line toward electronic crime (E-crime):
   - Once the attackers are able to access a user account, then they will attempt further exploits to get an administrator or “root” access.
   - Root access is a UNIX term and is associated with the system privileges required to run all services and access all files on the system (readers are expected to have a basic familiarity with Unix-based systems).
   - “Root” is an administrator or super-user access and grants them the privileges to do anything on the system.

INTRODUCTION

Websites and tools used to find the common vulnerabilities

Website	*Brief Description*
http://www.us-cert.gov/	US-CERT is the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS). US-CERT also provides a way for citizens, businesses and other institutions to communicate and coordinate directly with the US government about cybersecurity. US-CERT publishes information about a variety of vulnerabilities under "US-CERT Vulnerabilities Notes."
http://cve.mitre.org/	Common Vulnerabilities and Exposures (CVE) is a dictionary of publicly known information security vulnerabilities and exposures and free for public use. CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.
http://secunia.com/	It has thousands of vulnerability lists that are updated periodically. It has vulnerability database and provides in-depth analysis about virus, worm alerts and software vulnerability.
http://www.hackerstorm.com/	This website was created for open-source vulnerability database (OSVBD) tool. Since then it has grown in popularity and provides additional information about penetration testing. The site is updated with whole bunch of news and alerts about vulnerability research.

INTRODUCTION

http://www.hackerwatch.org/	It is an online community where Internet users can report and share information to block and identify security threats and unwanted traffic.
http://www.zone-h.org/	It reports on recent web attacks and cybercrimes and lists them on the website. One can view numerous defaced webpages and details about them.
http://www.milworm.com/	It contains day-wise information about exploits.
http://www.osvdb.org/	**OSVDB:** This is an open-source vulnerability database providing a large quantity of technical information and resources about thousands of vulnerabilities.
http://www.metasploit.com/	Metasploit is an open-source computer security project that provides information about security vulnerabilities and aids in penetration testing. Its most well-known subproject is the Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. The Metasploit Project is also well-known for antiforensic and evasion tools, some of which are built into the Metasploit Framework.
http://www.w00w00.org/files/LibExploit	LibExploit is a generic exploit creation library. It helps cybersecurity community when writing exploits to test vulnerability.
http://www.immunitysec.com/products-canvas.shtml	Canvas is a commercial vulnerability exploitation tool from Dave Aitel's ImmunitySec. It includes more than 150 exploits and also available are VisualSploit Plugin for drag and drop GUI exploit creation (optional).

INTRODUCTION

CYBERSECURITY

http://www.coresecurity.com/content/core-impact-overview	Core Impact is widely considered to be the most powerful exploitation tool available. It sports a large, regularly updated database of professional exploits, and can do neat tricks such as exploiting one system and then establishing an encrypted tunnel through that system to reach and exploit other systems.

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

INTRODUCTION

5. Grab the data:
   - Now that the attacker has “captured the network,” he/she takes advantage of his/her position to steal confidential data.
6. Covering tracks:
   - This is the last step in any cyber attack, which refers to the activities undertaken by the attacker to extend misuse of the system without being detected.
   - The attacker can remain undetected for long periods.
   - During this entire process, the attacker takes optimum care to hide his/her identity(ID) from the first step itself.

INTRODUCTION

CYBERSECURITY

Tools used to cover tracks

Website	*Brief Description*
http://www.ibt.ku.dk/jesper/ELSave/	**ELSave:** It is a tool to save and/or clear an NT event log. ELSave is written by Jesper Lauritsen. The executable is available on the weblink, but source code is not available.
http://ntsecurity.nu/toolbox/winzapper/	**WinZapper:** This tool enables to erase event records selectively from the security log in Windows NT 4.0 and Windows 2000. This program corrupts the event logs, therefore, they must be cleared completely.
http://www.evidence-eliminator.com/	**Evidence eliminator:** It is simple and one of the top-quality professional PC cleaning program that is capable of defeating all known investigative Forensic Software. Evidence eliminator permanently wipes out evidence so that forensic analysis becomes impossible.
http://www.traceless.com/computer-forensics/	**Traceless:** It is a privacy cleaner for Internet explorer (IE) that can delete common Internet tracks, including history, cache, typed URLs, cookies, etc.

INTRODUCTION

CYBERSECURITY

Website	*Brief Description*
http://www.acesoft.net/	**Tracks Eraser Pro:** It deletes following history data: • Delete address bar history of IE, Netscape, AOL, Opera. • Delete cookies of IE, Netscape, AOL, Opera. • Delete Internet cache (temporary Internet files). • Delete Internet history files. • Delete Internet search history. • Delete history of autocomplete. • Delete IE plugins (selectable). • Delete index.dat file. • Delete history of start menu run box. • Delete history of start menu search box. • Delete windows temp files. • Delete history of open/save dialog box. • Empty recycle bin.

INTRODUCTION

Scareware:

- It comprises several classes of scam software with malicious payloads, or of limited or no benefit which ore sold to consumers via certain unethical marketing practices. The selling approach uses social engineering to cause shock, anxiety or the perception of a threat generally directed at an unsuspecting user.

Malvertising:

- It is a malicious advertising - malware + advertising - on online criminal methodology that appears focused on the installation of unwanted or outright malicious software through the use of Internet advertising media networks, exchanges and other user-supplied content publishing services common to the social networking space.

INTRODUCTION

ClickJacking:

- It is a malicious technique of tricking netizens into revealing confidential information and/or taking control of their system while clicking on seemingly innocuous webpages.

Ransomware:

- It is computer malware that holds a computer system or the data it contains hostage against its user by demanding a ransom for its restoration.

PROXY SERVERS AND ANONYMIZERS

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

PROXY SERVERS AND ANONYMIZERS

- A proxy server has following purposes:
  1. Keep the systems behind the curtain (mainly for security reasons).
  2. Speed up access to a resource (through “caching”). It is usually used to cache the web pages from a web server.
  3. Specialized proxy servers are used to filter unwanted content such as advertisements.
  4. Proxy server can be used as IP address multiplexer to enable to connect number of computers on the Internet, whenever one has only one IP address
- One of the advantages of a proxy server is that its cache memory can serve all users. If one or more websites are requested frequently, may be by different users, it is likely to be in the proxy’s cache memory, which will improve user response time.
- In fact there are special servers available known as *cache servers.* A proxy can also do logging.

PROXY SERVERS AND ANONYMIZERS

- Listed are few websites where free proxy servers can be found:
  1. http:// www.proxy4free.com
  2. http://www.publicproxyservers.com
  3. http://www.proxz.com
  4. http:// www.anonymicychecker.com
  5. http://www.surf24h.com
  6. http:// www.hidemyass.com

PROXY SERVERS AND ANONYMIZERS

- An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It accesses the Internet on the user's behalf, protecting personal information by hiding the source computer's identifying information.
- Anonymizers are services used to make Web surfing anonymous by utilizing a website that acts as a proxy server for the web client.
- The anonymizer hides/removes all the identifying information from a user's computer while the user surfs on the internet, which ensures the privacy of the user.
- Listed are few websites where more information about anonyrnizers can be found:
  1. http://www.aoonymizer.com
  2. http://www.browzar.com
  3. http://www.anonymize.net
  4. http://www.anonymouse.ws
  5. http://www.anonymousindex.com

PROXY SERVERS AND ANONYMIZERS

Google Cookie:

- Google was the first search engine to use a cookie. Google set the standard and nowadays cookies are commonplace among search engines. This cookie places a unique ID number on your hard disk. Anytime you visit Google. user gets a Google cookie if a user doesn't already have one. If a user has one then it will read and record the unique ID number. Google con build a detailed list of your search terms over many years.

Cookie:

- Cookie (also know as HTIP cookie/browser cookie) is a small text file that contains a string of alphanumeric characters and is used for storing netizen's website preferences/authentication while visiting the some webpage again and again or also acts as identifier for server-based session - such browser mechanism of setting and reading cookies invites attackers to use these cookies as "Spywore.“

PROXY SERVERS AND ANONYMIZERS

- There are two types of cookies:
  - Persistent cookie is stored by the web browser into the cookie folder on the PC's hard disk. It remains under the cookie folder. which is maintained by the web browser.
  - Session cookie is a temporary cookie and does not reside on the PC once the browser is closed.

G-Zapper

- G-Zapper helps to protect users' ID and search history. G-Zapper reads the Google cookie installed on users' PC, displays the date it was installed, determines how long user searches have been tracked and displays Google searches. G-Zapper allows user to automatically delete or entirely block the Google search cookie from future installation.

PROXY SERVERS AND ANONYMIZERS

DoubleClick

- It is a subsidiary of Google and provides Internet ad-serving services and paid search products listing *(DART* Search) and utilize the cookies, which are called DART cookie.
- The DART cookie is a persistent cookie, which consists of the name of the domain that has set the cookie, the lifetime of the cookie and a "value."
- DoubleClick's DART mechanism generates a unique series of characters for the "value" portion of the cookie. These DoubleClick DART cookies help marketers learn how well their Internet advertising campaigns or paid search listings perform. Many marketers and Internet websites use DoubleClick's DART technology to deliver and serve their advertisements or manage their paid search listings.

PHISHING

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

PHISHING

How Phishing Works?

- Phishers work in the following ways:
  1. Planning: Criminals, usually called as phishers, decide the target.
  2. Setup: Once phishers know which business/business house to spoof and who their victims.
  3. Attack: the phisher sends a phony message that appears to be from a reputable source.
  4. Collection: Phishers record the information of victims entering into webpages or pop-up windows.
  5. Identity theft and fraud: Phishers use the information that they have gathered to make illegal purchases or commit fraud.
- Nowadays, more and more organizations/institutes provide greater online access for their customers and hence criminals are successfully using Phishing techniques to steal personal information and conduct ID theft at a global level.

PASSWORD CRACKING

- Password is like a key to get an entry into computerized systems like a lock.
- Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.
- Usually, an attacker follows a common approach – repeatedly making guesses for the password.
- The purpose of password cracking is as follows:
  1. To recover a forgotten password.
  2. As a preventive measure by system administrators to check for easily crackable passwords.
  3. To gain unauthorized access to a system.
- Manual password cracking is to attempt to logon with different passwords. The attacker follows the following steps:
  1. Find a valid user account such as an Administrator or Guest;
  2. create a list of possible passwords;
  3. rank the passwords from high to low probability;
  4. key-in each password;
  5. try again until a successful password is found.

PASSWORD CRACKING

- Password is like a key to get an entry into computerized systems like a lock.
- Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.
- Usually, an attacker follows a common approach –repeatedly making guesses for the password.
- The purpose of password cracking is as follows:
  1. To recover a forgotten password.
  2. As a preventive measure by system administrators to check for easily crackable passwords.
  3. To gain unauthorized access to a system.
- Manual password cracking is to attempt to logon with different passwords. The attacker follows the following steps:
  1. Find a valid user account such as an Administrator or Guest;
  2. create a list of possible passwords;
  3. rank the passwords from high to low probability;
  4. key-in each password;
  5. try again until a successful password is found.

PASSWORD CRACKING

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

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

PASSWORD CRACKING

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

PASSWORD CRACKING

Password cracking tools

Website	*Brief Description*
www.defaultpassword.com	**Default password(s):** Network devices such as switches, hubs and routers are equipped with "default passwords" and usually these passwords are not changed after commissioning these devices into the network (i.e., into LAN). The intruders can gain the access using these default passwords by visiting the said website.
http://www.oxid.it/cain.html	**Cain & Abel:** This password recovery tool is typically used for Microsoft Operating Systems (OSs). It allows to crack the passwords by sniffing the network, cracking encrypted passwords using dictionary, brute force attacks, decoding scrambled passwords and recovering wireless network keys.
http://www.openwall.com/john	**John the Ripper:** This is a free and open-source software – fast password cracker, compatible with many OSs like different flavors of Unix, Windows, DOS, BeOS and OpenVMS. Its primary purpose is to detect weak Unix passwords.
http://freeworld.thc.org/thc-hydra	**THC-Hydra:** It is a very fast network logon cracker which supports many different services.
http://www.aircrack-ng.org	**Aircrack-ng:** It is a set of tools used for wireless networks. This tool is used for 802.11a/b/g wired equivalent privacy (WEP) and *Wi*-Fi *P*rotected *A*ccess (WPA) cracking. It can recover a 40 through 512-bit WEP key once enough encrypted packets have been gathered. It can also attack WPA 1 or 2 networks using advanced cryptographic methods or by brute force.

PASSWORD CRACKING

Website	*Brief Description*
http://www.solarwinds.com	**SolarWinds:** It is a plethora of network discovery/monitoring/attack tools and has created dozens of special-purpose tools targeted at systems administrators. Security-related tools include many network discovery scanners, a Simple Network Management Protocol (SNMP) brute force cracker, router password decryption and more.
http://www.foofus.net/fizzgig/pwdump	**Pwdump:** It is a Window password recovery tool. Pwdump is able to extract NTLM and LanMan hashes from a Windows target, regardless of whether Syskey is enabled. It is also capable of displaying password histories if they are available.
http://project-rainbowcrack.com	**RainbowCrack:** It is a hash cracker that makes use of a large-scale time-memory trade-off. A traditional brute force cracker tries all possible plain texts one by one, which can be time-consuming for complex passwords. RainbowCrack uses a time-memory trade-off to do all the cracking-time computation in advance and store the results in so-called "rainbow tables." It does take a long time to precompute the tables but RainbowCrack can be hundreds of times faster than a brute force cracker once the precomputation is finished.
http://www.hoobie.net/brutus	**Brutus:** It is one of the fastest, most flexible remote password crackers available for free. It is available for Windows 9x, NT and 2000. It supports HTTP, POP3, FTP, SMB, TELNET, IMAP, NTP and more.

PASSWORD CRACKING

http://www.l0phtcrack.com	**L0phtCrack:** It is used to crack Windows passwords from hashes which it can obtain from stand-alone Windows workstations, networked servers, primary domain controllers or Active Directory. It also has numerous methods of generating password guesses (dictionary, brute force, etc.).
http://airsnort.shmoo.com	**AirSnort:** It is a wireless LAN (WLAN) tool which recovers encryption keys. It operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered. It requires approximately 5–10 million encrypted packets to be gathered. Once enough packets have been gathered, AirSnort can guess the encryption password in under a second. It runs under Windows or Linux.

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 that will be executed to try each password in a list and when matches, an attacker can gain the access to the system.
- The most popular online attack is man – in - the middle (MITM) attack, also termed as “bucket - brigade attack” or sometimes “Janus attack.”
- It is a form of active stealing in which the attacker establishes a connection between a victim and the server to which a victim is connected.
- When a victim client connects to the fraudulent server, the MITM server intercepts the call, hashes the password and passes the connection to the victim server (e.g., an attacker within reception range of an unencrypted Wi-Fi wireless access point can insert himself as a man-in-the-middle).
- This type of attack is used to obtain the passwords for E-Mail accounts on public websites such as Yahoo, Hotmail and Gmail and can also used to get the passwords for financial websites that would like to gain the access to banking websites.

PASSWORD CRACKING

Offline Attacks

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

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

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, such as words in the dictionary, proper names and words based on the username or common variations on these themes. Ex: abcd, susan, 1234 etc..
- A strong password is long enough, random or otherwise difficult to guess - producible only by the user who chooses it. The length of time deemed to be too long will vary with the attacker, the attacker's resources, the ease with which a password can be tried and the value of the password to the attacker. Ex: 4pRte!ai@3
- Forcing users to use system-created random passwords ensures that the password will have no connection with that user and should not be found in any dictionary. Several *OS's* have included such a feature.

PASSWORD CRACKING

Password guidelines:

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

KEYLOGGERS AND SPYWARES

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

Software Keyloggers

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

KEYLOGGERS AND SPYWARES

Website	*Brief Description*
http://www.soft-central.net	**SC-KeyLog PRO:** It allows to secretly record computer user activities such as E-Mails, chat conversations, visited websites, clipboard usage, etc. in a protected logfile. SC-KeyLog PRO also captures Windows user logon passwords. The captured information is completely hidden from the user and allows to remotely install the monitoring system through an E-Mail attachment without the user recognizing the installation at all.
http://www.spytech-web.com	**Spytech SpyAgent Stealth:** It provides a large variety of essential computer monitoring features as well as website and application filtering, chat blocking and remote delivery of logs via E-Mail or FTP.
http://www.relytec.com	**All In One Keylogger:** It is an invisible keystrokes recorder and a spy software tool that registers every activity on the PC to encrypted logs. This keylogger allows secretly tracking of all activities from all computer users and automatically receiving logs to a desired E-Mail/FTP accounting. With this keylogger, one can read chat conversations, look at the E-Mails as well as watch the sites that have been surfed.
http://www.stealthkeylogger.org	**Stealth Keylogger:** It is a computer monitoring software that enables activity log report where the entire PC keyboard activities are registered either at specific time or hourly on daily basis. The entire log reports are generated either in text or HTML file format as defined by the user. The keylogger facilitates mailing of log report at the specified E-Mail address.

KEYLOGGERS AND SPYWARES

http://www.blazingtools.com	**Perfect Keylogger:** It has its advanced keyword detection and notification. User can create a list of "on alert" words or phrases and keylogger will continually monitor keyboard typing, URLs and webpages for these words or phrases – for example, "bomb," "sex," "visiting places around Mumbai" and "Windows vulnerabilities." When a keyword is detected, perfect keylogger makes screenshot and sends E-Mail notification to the user.
http://kgb-spy-software.en.softonic.com	**KGB Spy:** It is a multifunctional keyboard tracking software, widely used by both regular users and IT security specialists. This program does not just record keystrokes but is also capable of recording language-specific characters. It records all typed data/all keyboard activity. It can be used to monitor children's activity at home or to ensure employees do not use company's computers inappropriately. Visit www.refog.com to find more on this product.
http://www.spy-guide.net/spybuddy-spy-software.htm	**Spy Buddy:** This, along with keylogger, has following features: • Internet conversation logging; • disk activity logging; • Window activity logging; • application activity logging; • clipboard activity logging; • AOL/Internet explorer history; • printed documents logging; • keylogger keystroke monitoring; • websites activity logging; • screenshot capturing; • WebWatch keyword alerting

KEYLOGGERS AND SPYWARES

CYBERSECURITY

Website	*Brief Description*
http://www.elite-keylogger.com	**Elite Keylogger:** It captures every keystroke typed, all passwords (including Windows logon passwords), chats, instant messages, E-Mails, websites visited, all program launched, usernames and time they worked on the computer, desktop activity, clipboard, etc.
http://www.cyberspysoftware.com	**CyberSpy:** It provides an array of features and easy-to-use graphical interface along with computer monitoring capabilities such as keep tabs on the employees and keeps track of what children are viewing on the Internet. CyberSpy can be used as complete PC monitoring solution for any home or office. CyberSpy records all websites visited, instant message conversations, passwords, E-Mails and all keystrokes pressed. It also has the ability to provide screenshots at set intervals.
http://www.mykeylogger.com	**Powered Keylogger:** Powered keylogger can be used for the following: • *Surveillance:* It is for anyone to control what happens on the computer when the computer's owner is away. • *Network administration:* It is for network administrators to control outgoing traffic and sites visited. • *Shared PC activity tracking:* It is to analyze the usage of shared PC. • *Parental control:* It helps parents to monitor their children's computer and Internet activity. • *Employee productivity monitoring:* It helps managers to check and increase productivity of their stuff or just to prevent the leak of important information.

KEYLOGGERS AND SPYWARES

http://www.x-pcsoft.com

XPC Spy: XPC Spy is one of the powerful keylogger spy software, runs stealthy under MS Windows and has the following features:

- Records all keystrokes typed;
- records all websites visited;
- records all programs executed, folders explored, files opened or edited, documents printed, etc.;
- records all windows opened;
- records all clipboard text content;
- records all system activities;
- records webmails sent (database update online, more and more webmail servers are supported);
- records all ICQ Messenger chat conversations;
- records all MSN Messenger chat conversations;
- records all AOL/AIM Messenger chat conversations;
- records all Yahoo! Messenger chat conversations;
- runs invisible in the background and is protected by password;
- is built-in screenshot pictures viewer;
- schedules monitor process, sets time to start or stop monitoring;
- sends logs report via E-Mail.

KEYLOGGERS AND SPYWARES

Hardware Keyloggers

- Hardware keyloggers are small hardware devices.
- These are connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device.
- Cybercriminals install such devices on ATM machines to capture ATM Cards' PINs.
- Each keypress on the keyboard of the ATM gets registered by these keyloggers.
- These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence.
- Hardware keyloggers can be found:
  1. hnp://www.keyghost.com
  2. hnp://www.keelog.com
  3. hrrp://www.keydevil.com
  4. hup://w.vw.keykatchcr.com

KEYLOGGERS AND SPYWARES

Antikeylogger

- Antikeylogger is a tool that can detect the keylogger installed on the computer system and can remove the tool. (Visit http://www.antikeyloggers.com for more information)
- Advantages of using antikeylogger are as follows:
  1. Firewalls cannot detect the installations of keyloggers on the systems; hence, antikeyloggers can detect installations of keylogger.
  2. This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs; if not updated, it does not serve the purpose, which makes the users at risk.
  3. Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers.
  4. It prevents ID theft.
  5. It secures E-Mail and instant messaging/chatting.

KEYLOGGERS AND SPYWARES

Spywares

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

KEYLOGGERS AND SPYWARES

CYBERSECURITY

Website	*Brief Description*
http://www.e-spy-software.com	**007 Spy:** It has following key features: • Capability of overriding "antispy" programs like "Ad-aware"; • record all websites URL visited in Internet; • powerful keylogger engine to capture all passwords; • view logs remotely from anywhere at anytime; • export log report in HTML format to view it in the browser; • automatically clean-up on outdated logs; • password protection.
http://www.spectorsoft.com	**Spector Pro:** It has following key features: • Captures and reviews all chats and instant messages; • captures E-Mails (read, sent and received); • captures websites visited; • captures activities performed on social networking sites such as MySpace and Facebook; • enables to block any particular website and/or chatting with anyone; • acts as a keylogger to capture every single keystroke (including usernames and passwords).
http://www.spectorsoft.com	**eBlaster:** Besides keylogger and website watcher, it also records E-Mails sent and received, files uploaded/downloaded, logging users' activities, record online searches, recording MySpace and Facebook activities and any other program activity.

KEYLOGGERS AND SPYWARES

http://www.remotespy.com	**Remotespy:** Besides remote computer monitoring, silently and invisibly, it also monitors and records users' PC without any need for physical access. Moreover, it records keystrokes (keylogger), screenshots, E-Mail, passwords, chats, instant messenger conversations and websites visited.
http://www.topofbestsoft.com	**Stealth Recorder Pro:** It is a new type of utility that enables to record a variety of sounds and transfer them automatically through Internet without being notified by original location or source. It has following features: • Real-time MP3 recording via microphone, CD, line-in and stereo mixer as MP3, WMA or WAV formatted files; • transferring via E-Mail or FTP, the recorded files to a user-defined E-Mail address or FTP automatically; • controlling from a remote location; • voice mail, records and sends the voice messages.
http://www.amplusnet.com	**Stealth Website Logger:** It records all accessed websites and a detailed report can be available on a specified E-Mail address. It has following key features: • Monitor visited websites; • reports sent to an E-Mail address; • daily log; • global log for a specified period; • log deletion after a specified period; • hotkey and password protection; • not visible in add/remove programs or task manager.

KEYLOGGERS AND SPYWARES

http://www.flexispy.com	**Flexispy:** It is a tool that can be installed on a cell/mobile phone. After installation, Flexispy secretly records coversation that happens on the phone and sends this information to a specified E-Mail address.
http://www.wiretappro.com	**Wiretap Professional:** It is an application for monitoring and capturing all activities on the system. It can capture the entire Internet activity. This spy software can monitor and record E-Mail, chat messages and websites visited. In addition, it helps in monitoring and recording of keystrokes, passwords entered and all documents, pictures and folders viewed.
http://www.pcphonehome.com	**PC PhoneHome:** It is a software that tracks and locates lost or stolen laptop and desktop computers. Every time a computer system on which PC PhoneHome has been installed, conneced to the Internet, a stealth E-Mail is sent to a specified E-Mail address of the user's choice and to PC PhoneHome Product Company.
http://www.spyarsenal.com	**SpyArsenal Print Monitor Pro:** It has following features: • Keep track on a printer/plotter usage; • record every document printed; • find out who and when certain paper printed with your hardware.

KEYLOGGERS AND SPYWARES

Malwares

- Malware, short for malicious software, is a software designed to infiltrate a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive or annoying software or program code. Malware can be classified as follows:
  1. **Viruses and worms:** These are known as *infectious malware*. They spread from one computer system to another with a particular behavior.
  2. **Trojan Horses:** A Trojan Horse, Trojan for short, is a term used to describe malware that appears,to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system
  3. **Rootkits:** Rootkits is a software system that consists of one or more programs designed to obscurethe fact that a system has been compromised.
  4. **Backdoors:** Backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plain text and so on while attempting to remain undetected
  5. **Spyware**
  6. **Botnets**
  7. **Keystroke loggers**

VIRUS AND WORMS

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

VIRUS AND WORMS

- 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.
- **Computer virus** has the ability to copy itself and infect the system.
- The term *virus* is also commonly but erroneously used to refer to other types of malware, Adware and Spyware programs that do not have reproductive ability.
- A true virus can only spread from one system to another (in some form of executable code) when its host is taken to the target computer; for instance, when a user sent it over the Internet or a network, or carried it on a removable media such as CD, DVD or USB drives.
- Viruses can increase their chances of spreading to other systems by infecting files on a network file system or a file system that is accessed by another system.

VIRUS AND WORMS

CYBERSECURITY

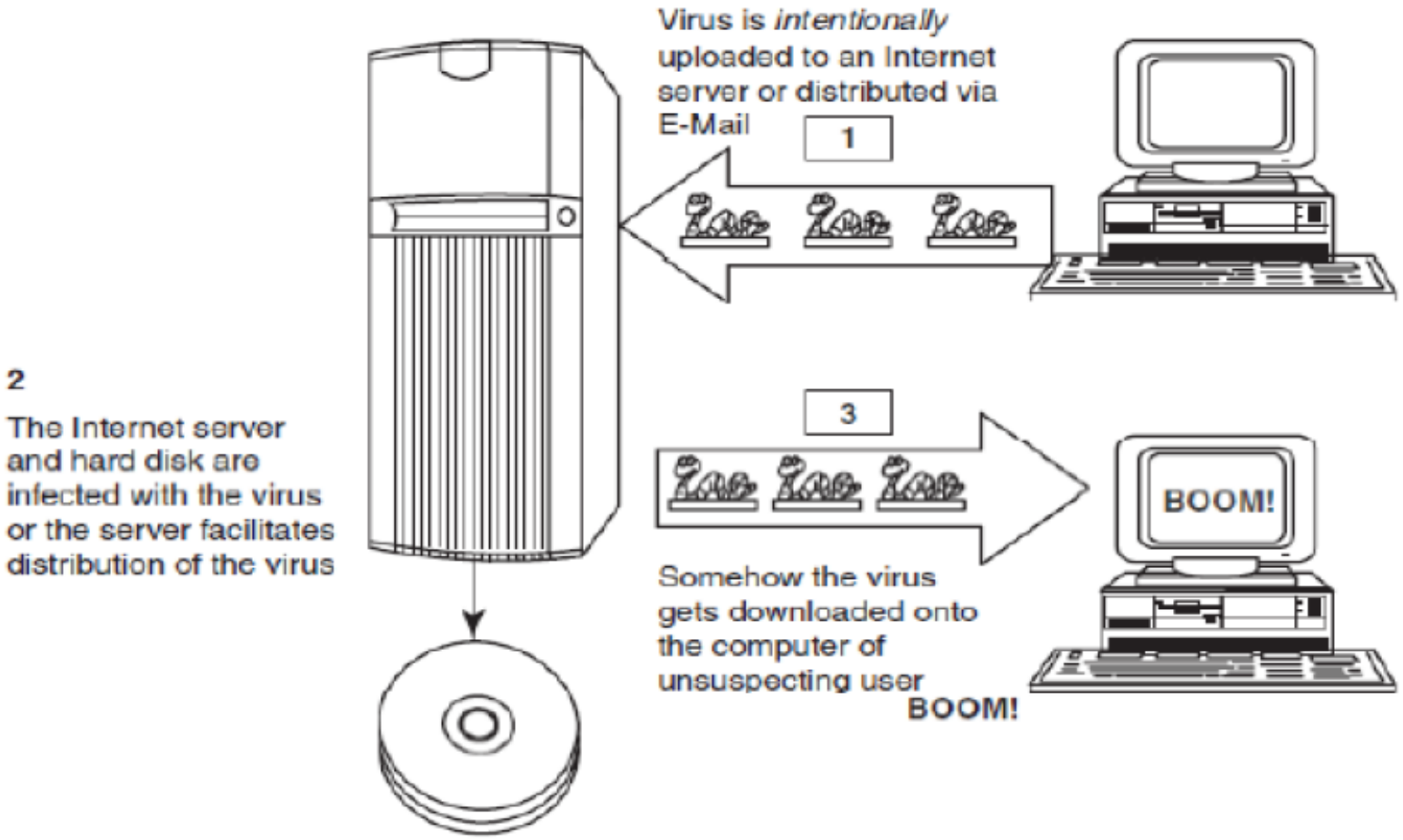
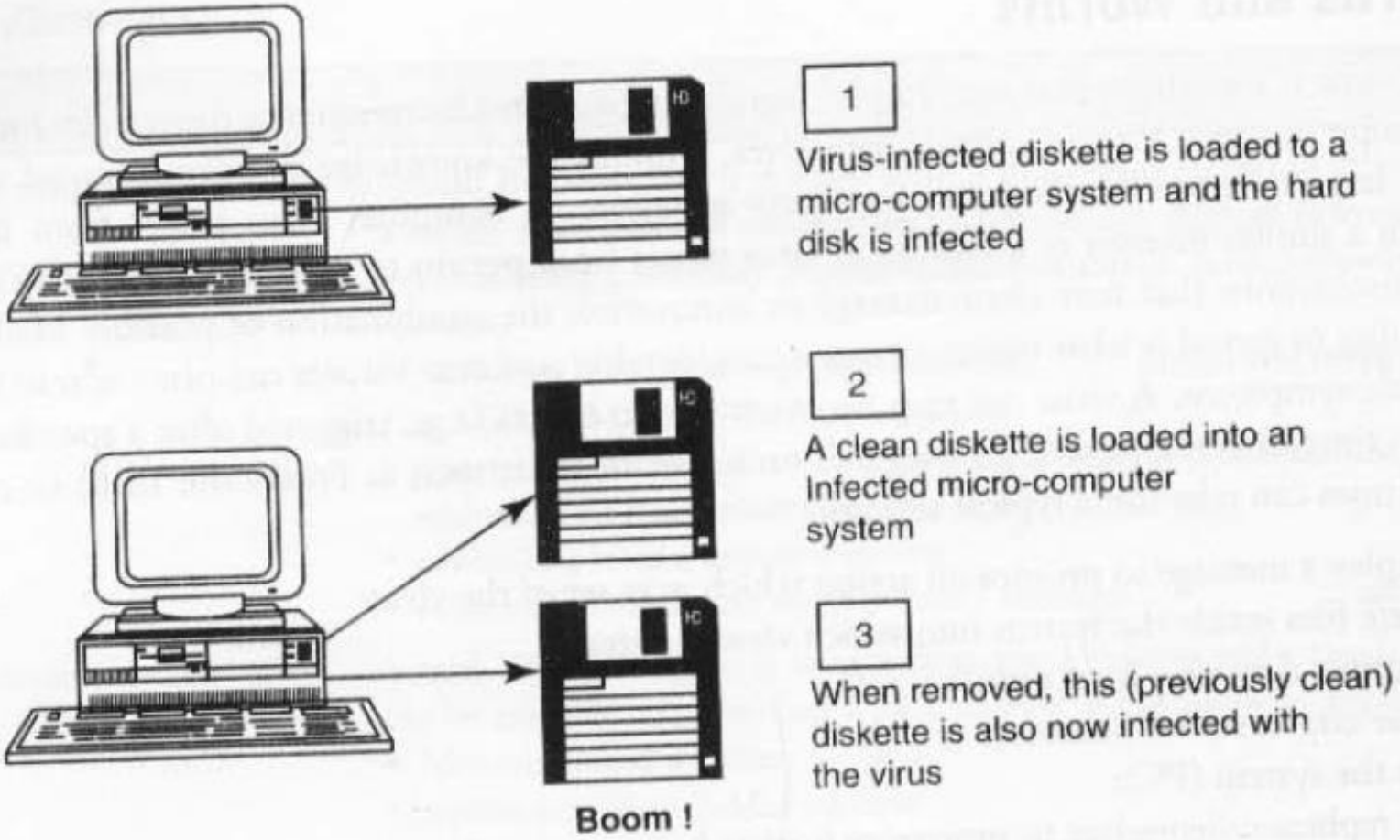


Figure: Virus Spread Through Internet

VIRUS AND WORMS

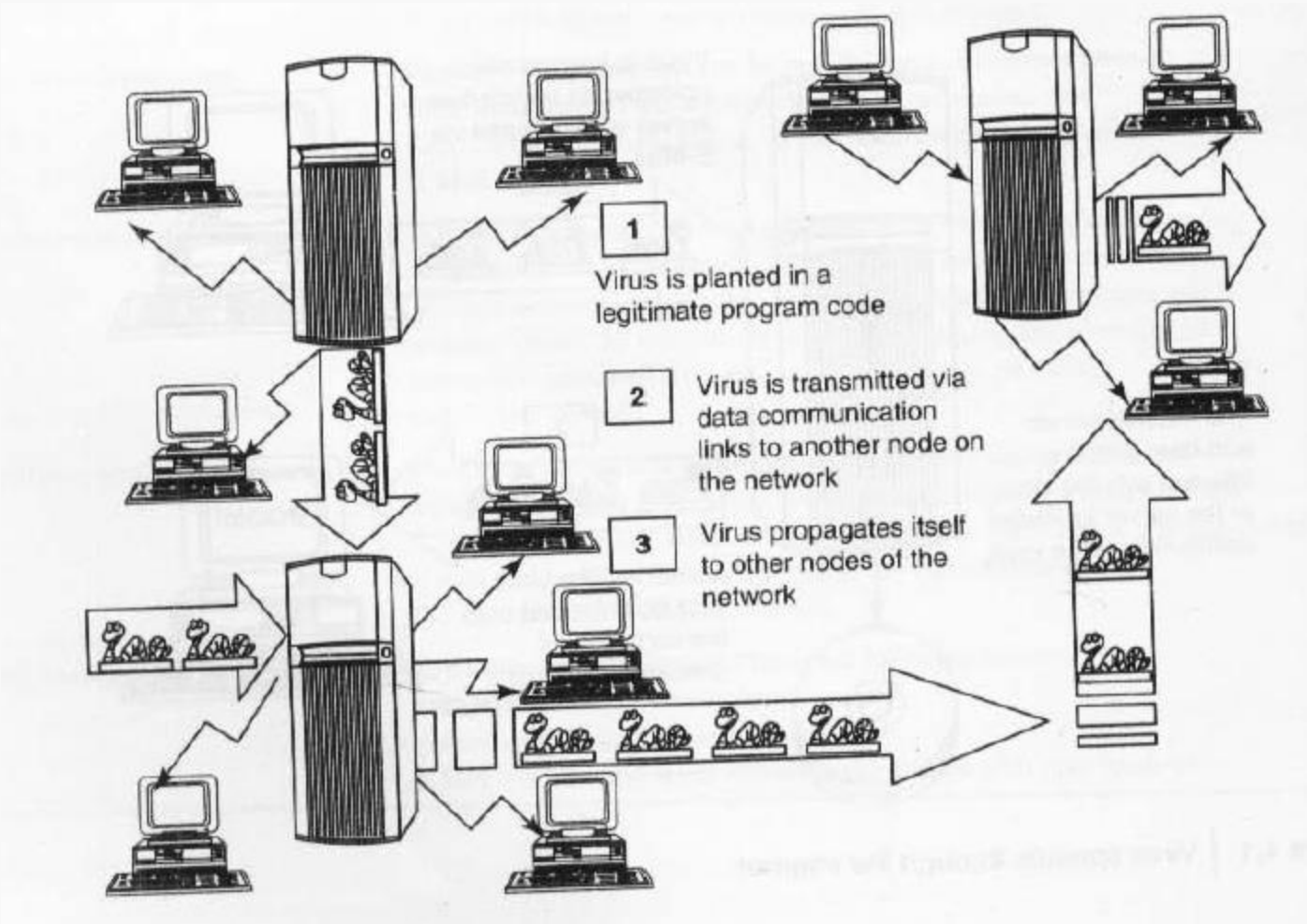
CYBERSECURITY



Virus spread through stand-alone system

VIRUS AND WORMS

CYBERSECURITY



Virus Spread through Local Networks

VIRUS AND WORMS

- Malware includes computer viruses, worms, Trojans, most Rootkits, Spyware, dishonest
- Adware, crimeware and other malicious and unwanted software as well as true viruses.
- Viruses are sometimes confused with computer worms and Trojan Horses, which are technically different.
- A worm spreads itself automatically to other computers through networks by exploiting security vulnerabilities, whereas a Trojan is a code/program that appears to be harmless but hides malicious functions.
- Worms and Trojans, such as viruses, may harm the system's data or performance.
- Some viruses and other malware have noticeable symptoms that enable computer user to take necessary corrective actions, but many viruses are surreptitious or simply do nothing for user's to take note of them.
- Some viruses do nothing beyond reproducing themselves.

VIRUS AND WORMS

CYBERSECURITY

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

- 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.

Types of Viruses

1. **Boot sector viruses:** It infects the storage media on which OS is stored (e.g., hard drives) and which is used to start the computer system.
2. **Program viruses:** These viruses become active when the program file (usually with extensions .bin, .com,.exe, .ovl, .drv) is excuted
3. **Multipartite viruses:** It is a hybrid of a boot sector and program viruses. It infects program files along with the boot record when the infected program is active.
4. **Stealth viruses:** It hides itself and so detecting this type of virus is very difficult. It can hiding itself such a way that antivirus software also cannot detect it. Example for Stealth virus is “Brain Virus”.
5. **Polymorphic viruses:** It acts like a “chameleon” that changes its virus signature (i.e., binary pattern) every time it spreads through the system (i.e., multiplies and infects a new file). Hence, it is always difficult to detect polymorphic virus with the help of an antivirus program.
6. **Macro viruses:** Many applications, such as Microsoft Word and Microsoft Excel, support MACROs (i.e., macrolanguages). These macros are programmed as a macro embedded in a document. Once macrovirus gets onto a victim’s computer then every document he/she produces will become infected.
7. **Active X and Java Control:** All the web browsers have settings about Active X and Java Controls.

VIRUS AND WORMS

CYBERSECURITY

Sr. No.	*Virus*	*Brief Description*
1	Conficker	It is also known as Downup, Downadup and Kido. It targets Microsoft Windows OS and was first detected in November 2008. It uses flaws in Windows software and dictionary attacks on administrator passwords to co-opt machines and link them into a virtual computer that can be commanded remotely by its authors. The name Conficker is blended from a English term "*configure*" and the German word "*Ficker*," which means "to have sex with" or "to mess with" in colloquial German.
2	INF/AutoRun	*AutoRun* and the companion feature *AutoPlay* are components of the Microsoft Windows OS that dictate what actions the system takes when a drive is mounted. This is the most common threat that infects a PC by creating an "autorun.inf" file. The file contains information about programs meant to run automatically when removable devices are connected to the computer. End-users must disable the AutoRun feature enabled by default in windows. AutoRun functionality is used in attack vector attacks.
3	Win32 PSW. OnLineGames	It is a dangerous virus that replicates itself as other viruses and spreads from one computer system to another carrying a payload of destruction. It can infect several computers within few minutes. It is more concerned with gamers around the world, stealing confidential and other financial credentials as well as gaining access to the victim's account. This virus is also termed as Trojan.

The world's worst virus attacks

VIRUS AND WORMS

4	Win32/Agent	This virus is also termed as Trojan. It copies itself into temporary locations and steals information from the infected system. It adds entries into the registry, creating several files at different places in the system folder, allowing it to run on every start-up, which enables to gather complete information about the infected system and then transferred to the intruder's system.
5	Win32/FlyStudio	It is known as Trojan with characteristics of backdoor. This virus does not replicate itself, but spreads only when the circumstances are beneficial. It is called as backdoors because the information stolen from a system is sent back to the intruder.
6	Win32/Pacex.Gen	This threat designates a wide range of malwares that makes use of an obfuscation layer to steal passwords and other information from the infected system.
7	Win32/Qhost	This virus copies itself to the System32 folder of the Windows directory giving control of the computer to the attacker. The attacker then modifies the Domain Name Server/System (DNS) settings redirecting the computer to other domains. This is done to compromise the infected machine from downloading any updates and redirect any attempts made to a website that downloads other malicious files on the victim's computer.
8	WMA/ TrojanDownloader. GetCodec	This threat as the suffix .GetCodec modifies the audio files present on the system to ".wma" format and adds a URL header that points to the location of the new codec. In this manner, the host computer is forced to download the new codec and along with the new codec several other Malicious Codes are also downloaded.

VIRUS AND WORMS

- A computer worm is self-replicating malware computer program. It 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.
- This is due to security shortcomings on the target computer.
- Unlike a virus, it does not need co attach itself to an existing program.
- Worms almost always cause at least *some* harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

VIRUS AND WORMS

CYBERSECURITY

Sr. No.	*Worm*	*Brief Description*
1	Morris Worm	It is also known as "Great Worm" or Internet Worm. It was written by a student, Robert Tappan Morris, at Cornell University and launched on 2 November 1988 from MIT. It was reported that around 6,000 major Unix machines were infected by the Morris worm and the total cost of the damage calculated was US$ 10–100 millions.
2	ILOVEYOU	It is also known as VBS/Loveletter or Love Bug Worm. It successfully attacked tens of millions of Windows computers in 2000. The E-Mail was sent with the subject line as "ILOVEYOU" and an attachment "LOVE-LETTER-FOR-YOU.TXT.vbs." The file extension "vbs" was hidden, hence the receiver downloads the attachment and opens it to see the contents.
3	Nimda	It is the most widespread computer worm and a file infector. It can affect Internet's within 22 minutes. Nimda affected both user workstations (i.e., clients) running on Windows 95, 98, Me, NT, 2000 or XP and Servers running on Windows NT and 2000. It is "admin" when this worm's name is spelled backward.
4	Code Red	This computer worm was observed on the Internet on 13 July 2001. It attacked computers running on Microsoft's IIS web server. The Code Red worm was first discovered and researched by eEye Digital Security employees, Marc Maiffret and Ryan Permeh. They named the worm Code Red because they were drinking Pepsi's "Mountain Dew Code Red" over the weekend. They analyzed it because of the phrase "Hacked by Chinese!" with which the worm defaced websites. On 4 August 2001 "Code Red II" appeared on the Internet and was found to be a variant of the original Code Red worm.

VIRUS AND WORMS

CYBERSECURITY

5	Melissa	It is also known as "Melissa," "Simpsons," "Kwyjibo" or "Kwejeebo." It is a mass-mailing macro worm. Melissa was written by David L. Smith in Aberdeen Township, New Jersey, who named it after a lap dancer he met in Florida. The worm was in a file called "List.DOC" which had passwords that allow the access into 80 pornographic websites. This worm in the original form was sent through an E-Mail to many Internet users. Melissa spread on Microsoft Word 97, Word 2000 and also on Microsoft Excel 97, 2000 and 2003. It can mass-mail itself from E-Mail client Microsoft Outlook 97 or Outlook 98.
6	MSBlast	The Blaster Worm: It is also known as Lovsan or Lovesan, found during August 2003, which spread across the systems running on Microsoft Windows XP and Windows 2000. The worm also creates an entry under OS registry to launch the worm every time Windows starts. This worm contains two messages hidden in strings. The first, "I just want to say LOVE YOU SAN!!" and so the worm sometimes was called "Lovesan worm." The second message, "Billy gates why do you make this possible? Stop making money and fix your software!!" This message was for Bill Gates, the co-founder of Microsoft and target of the worm.
7	Sobig	This worm, found during August 2003, infected millions of Internet-connected computers that were running on Microsoft Windows. It was written in Microsoft Visual C++ and compressed using a data compression tool, "tElock." This Worm not only replicates by itself but also a Trojan Horse that it masquerades as something other than malware. It will appear as an E-Mail with one of the following subjects: • Re: Approved • Re: Details

Etc..

TROJAN HORSES AND BACKDOORS

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

TROJAN HORSES AND BACKDOORS

- Some typical examples of threats by Trojans are as follows:
  1. They erase, overwrite or corrupt data on a computer.
  2. They help to spread other malware such as viruses (by a dropper Trojan).
  3. They deactivate or interfere with antivirus and firewall programs.
  4. They allow remote access to your computer (by a remote access Trojan).
  5. They upload and download files without your knowledge.
  6. They gather E-Mail addresses and use them for Spam.
  7. They log keystrokes to steal information such as passwords and credit card numbers.
  8. They copy fake links to false websites, display porno sites, play sounds/videos and display images.
  9. They slow down, restart or shutdown the system.
  10. They reinstall themselves after being disabled.
  11. They disable the task manager.
  12. They disable the control panel.

TROJAN HORSES AND BACKDOORS

Backdoor

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

TROJAN HORSES AND BACKDOORS

Following are some functions of backdoor:

1. It allows an attacker to create, delete, rename, copy or edit any file, execute various commands; change any system settings; alter the Windows registry; run, control and terminate applications; install arbitrary software and parasites.
2. It allows an attacker to control computer hardware devices, modify related settings, shutdown or restart a computer without asking for user permission.
3. It steals sensitive personal information, valuable documents, passwords, login names, ID details; logs user activity and tracks web browsing habits.
4. It records keystrokes that a user types on a computer's keyboard and captures screenshots.
5. It sends all gathered data to a predefined E-Mail address, uploads it to a predetermined FTP server or transfers it through a background Internet connection to a remote host.
6. It infects files, corrupts installed applications and damages the entire system.
7. It distributes infected files to remote computers with certain security vulnerabilities and performs attacks against hacker-defined remote hoses.
8. It installs hidden FTP server chat can be used by malicious persons for various illegal purposes.
9. It degrades Internet connection speed and overall system performance, decreases system security and causes software instability. Some parasites are badly programmed as they waste too many computer resources and conflict with installed applications.
10. It provides no uninstall feature, and hides processes, files and ocher objects to complicate its removal as much as possible.

TROJAN HORSES AND BACKDOORS

Following are a few examples of backdoor Trojans:

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

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

1. Stay away from suspect web sites/web links: Avoid downloading free/pirated software's that often get infected by Trojans, worms, viruses and other things.
2. Surf on the Web cautiously: Avoid connecting with and/or downloading any information from peer-to-peer (P2P) networks, which are most dangerous networks co spread Trojan Horses and other threats.
3. Install antivirus/Trojan remover software: Nowadays antivirus software(s) have built-in feature for protecting the system not only from viruses and worms bur also from malware such as Trojan Horses.

STEGANOGRAPHY

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

STEGANOGRAPHY

Steganalysis

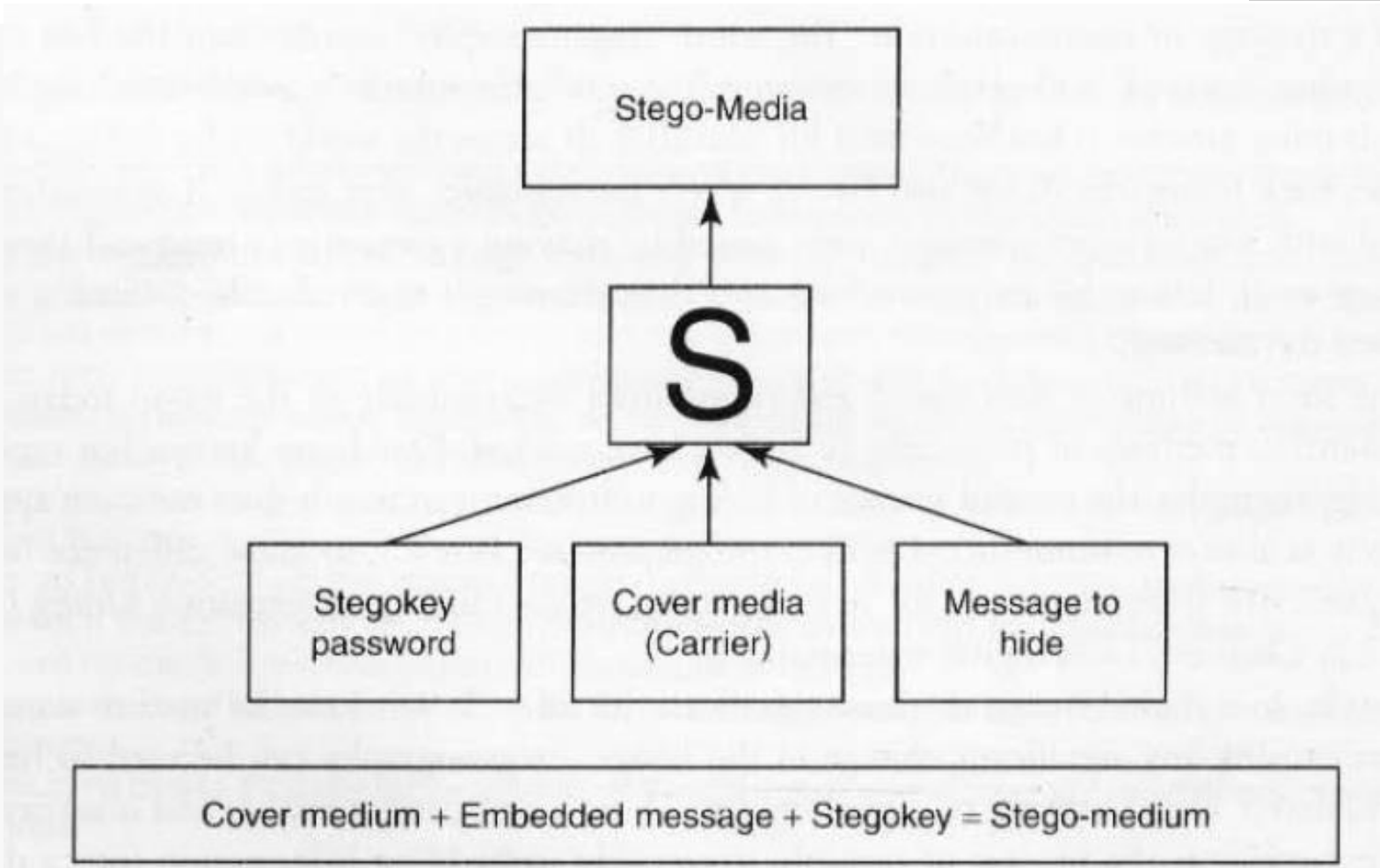
- Steganalysis is the art and science of detecting messages that are hidden in images, audio/video files using steganography.
- The goal of steganalysis is to identify suspected packages and to determine whether or not they have a payload encoded into them, and if possible recover it.
- Automated tools are used to detect such steganographed data/information hidden in the image and audio and/or video files.

Difference between Steganography and Cryptography

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

STEGANOGRAPHY

CYBERSECURITY



How steganography works.

STEGANOGRAPHY

CYBERSECURITY

Website	*Brief Description*
http://www.securityfocus.com	**DiSi-Steganograph:** It is a very small, DOS-based steganographic program that embeds data in PCX images.
http://www.brothersoft.com/invisible-folders-54597.html	**Invisible Folders:** It has the ability to make any file or folder invisible to anyone using your PC even on a network.
http://www.invisiblesecrets.com	**Invisible Secrets:** It not only encrypts the data and files for safe-keeping or for secure transfer across the Net but also hides them in places such as picture or sound files or webpages. These types of files are a perfect disguise for sensitive information.
http://www.programurl.com/stealth-files.htm	**Stealth Files:** It hides any type of file in almost any other type of file. Using steganography technique, Stealth Files compresses, encrypts and then hides any type of file inside various types of files (including EXE, DLL, OCX, COM, JPG, GIF, ART, MP3, AVI, WAV, DOC, BMP) and other types of video, image and executable files.
http://www.programurl.com/hermetic-stego.htm	**Hermetic Stego:** It is a steganography program that allows to encrypt and hide contents of any data file in another file so that the addition of the data to the container file will not noticeably change the appearance of that file. This program allows hiding a file of any size in one or more BMP image files with or without the use of a user-specified stego/encryption key so that (a) the presence of the hidden file is undetectable (even by forensic software using statistical methods) and (b) if a user-specified stego key is used then the hidden file can be extracted only by someone, using this software, who knows that stego key.

STEGANOGRAPHY

CYBERSECURITY

http://www.securstar.com/products_drivecryptpp.php	**DriveCrypt Plus (DCPP):** It has following features: • It allows secure hiding of an entire OS inside the free space of another OS. • Full-disk encryption (encrypts parts or 100% of your hard disk including the OS). • Preboot authentication (before the machines boots, a password is requested to decrypt the disk and start your machine).
http://www.petitcolas.net/fabien/steganography/mp3stego	**MP3Stego:** It hides information in MP3 files during the compression process. The data is first compressed, encrypted and then hidden in the MP3 bit stream.
http://compression.ru/video/stego_video/index_en.html	**MSU StegoVideo:** It allows hiding any file in a video sequence. Main features are as follows: • Small video distortions after hiding information. • It is possible to extract information after video compression. • Information is protected with the password.

Steganography tools

DOS AND DDOS ATTACKS

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

DoS Attacks

- In this type of criminal act, **the attacker floods the bandwidth of the victim's network** or fills his E-Mail box with Spam mail depriving him of the services he is entitled to access or provide.
- **The attackers typically target sites or services hosted on high-profile web servers** such as banks, credit card payment gateways, mobile phone networks and even root name servers. Buffer overflow technique is employed to commit such kind of criminal attack known as *Spoofing*.
- The term IP address Spoofing refers to the creation of IP packets with a forged (spoofed) source IP address with the purpose of concealing the ID of the sender or impersonating another computing system.
- A packet is a formatted unit of data carried by a packet mode computer network. The attacker spoofs the IP address and floods the network of the victim with repeated requests.
- As the IP address is fake, the victim machine keeps waiting for response from the attacker's machine for each request. This consumes the bandwidth of the network which then fails to serve the legitimate requests and ultimately breaks down.

DOS AND DDOS ATTACKS

- The United States Computer Emergency Response Team defines symptoms of DoS attacks to include:
  1. Unusually slow network performance (opening fi les or accessing websites);
  2. unavailability of a particular website;
  3. inability to access any website;
  4. dramatic increase in the number of Spam E-Mails received (this type of DoS attack is termed as an E-Mail bomb).
- The goal of DoS is not to gain unauthorized access to systems or data, but to prevent intended users (i.e., legitimate users) of a service from using it.
- A DoS attack may do the following:
  1. Flood a network with traffic, thereby preventing legitimate network traffic.
  2. Disrupt connections between two systems, thereby preventing access to a service.
  3. Prevent a particular individual from accessing a service.
  4. Disrupt service to a specific system or person.

DOS AND DDOS ATTACKS

Classification of DoS Attacks

1. **Bandwidth attacks:** Loading any website takes certain time. Loading means complete webpage appearing on the screen and system is awaiting user's input.
2. **Logic attacks:** These kind of attacks can exploit vulnerabilities in network software such as web server or TCP/IP stack.
3. **Protocol attacks**: Protocols here are rules that are to be followed to send data over network.
4. **Unintentional DoS attack :** This is a scenario where a website ends up denied not due to a attack by a single individual or group of individuals, but simply due to a sudden enormous spike in popularity.

DOS AND DDOS ATTACKS

Types or Levels of DoS Attacks

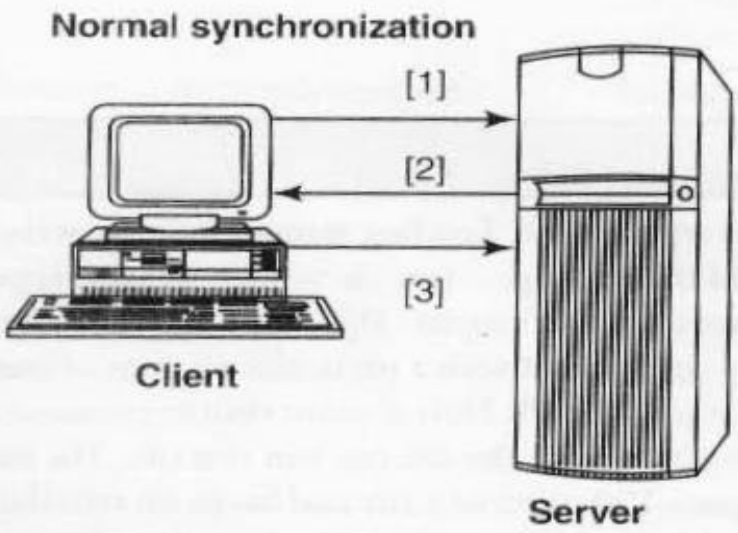
- **1. Flood attack:** This is the earliest form of DoS attack and is also known as *ping flood*. It is based on an attacker simply sending the victim overwhelming number of ping packets, usually by using the "ping" command, which result into more traffic than the victim can handle.
- 2. **Ping of death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

DOS AND DDOS ATTACKS

- 3. **SYN attack:** It is also termed as ***TCP SYN Flooding***. In the TCP, handshaking of network connections is done with SYN and ACK messages.
  - An attacker initiates a TCP connection to the server with an SYN.
  - The server replies with an SYN-ACK.
  - The client then does not send back an ACK, causing the server to allocate memory for the pending connection and wait.
  - This fills up the buffer space for SYN messages on the target system, preventing other systems on the network from communicating with the target system.
- **4. Teardrop attack:** The teardrop attack is an attack where **fragmented packets are forged to overlap each other when the receiving host tries to reassemble them**. IP's packet fragmentation algorithm is used to send corrupted packets to confuse the victim and may hang the system. This attack can crash various OSs due to a bug in their TCP/IP fragmentation reassembly code.

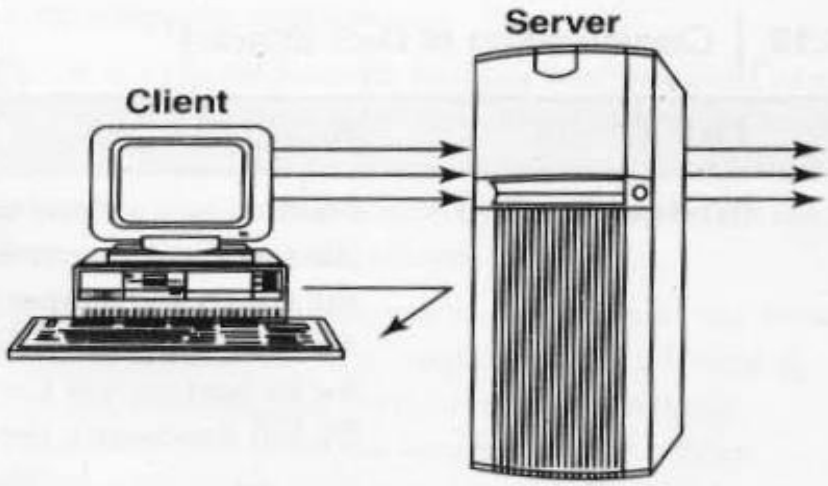
DOS AND DDOS ATTACKS

CYBERSECURITY



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

DOS AND DDOS ATTACKS

- **5. Smurf attack:** This is a type of DoS attack that **floods a target system via spoofed broadcast ping messages.** This attack consists of a host sending an echo request (ping) to a network broadcast address.
- **6. Nuke:** Nuke is an old DoS attack against computer networks consisting of **fragmented or invalid packets sent to the target.**

Tools Used to Launch DoS Attack

1. **Jolt2 :** The vulnerability allows remote attackers to cause a DoS attack against Windows-based machines –the attack causes the target machine to consume of the CPU time on processing of illegal packets.
2. **Nemesy :** This program generates random packets of spoofed source IP to enable the attacker to launch DoS attack.
3. **Targa :** It is a program that can be used to run eight different DoS attacks. The attacker has the option to launch either individual attacks or try all the attacks until one is successful.
4. **Crazy Pinger :** This tool could send large packets of ICMP(Internet Control Message Protocol) to a remote target network.
5. **SomeTrouble:** It is a remote flooder and bomber. It is developed in Delphi.

DOS AND DDOS ATTACKS

Blended Threat

- Blended threat is a more sophisticated attack that bundles some or the worst aspects of viruses, worms, Trojan Horses and Malicious Code into one single threat. Blended threats can use server and Internet vulnerabilities to initiate transmit and thereafter spread on attack. Characteristics or blended threats are that:
  1. They cause harm to the infected system or network.
  2. They propagate using multiple methods as attack may come from multiple points.
  3. They also exploit vulnerabilities.

Permanent Denial-of-Service (PDoS) Attack

- A PDoS attack damages a system so badly that ii requires replacement or reinstallation of hardware.
- Unlike DDoS attack - which is used to sabotage a service or website or as a cover for malware delivery - PDoS is a pure hardware sabotage. It exploits security flows that allow remote administration on the management interfaces of the victim's hardware such as routers, printers or other networking hardware.
- The attacker uses these vulnerabilities to replace a device's firmware with a modified. corrupt or defective firmware image - a process which when done legitimately is known as flashing.

DOS AND DDOS ATTACKS

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.
- The attack is “distributed” because the attacker is using multiple computers, including yours, to launch the DoS attack.
- 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.”
- Malware can carry DDoS attack mechanisms – one of the better-known examples of this is MyDoom.
- Botnet is the popular medium to launch DoS/DDoS attacks.
- Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts.

DOS AND DDOS ATTACKS

CYBERSECURITY

Tools used to launch DDoS attack

Tool	*Brief Description*
Trinoo	It is a set of computer programs to conduct a DDoS attack. It is believed that Trinoo networks have been set up on thousands of systems on the Internet that have been compromised by remote buffer overrun exploit.
Tribe Flood Network (TFN)	It is a set of computer programs to conduct various DDoS attacks such as ICMP flood, SYN flood, UDP flood and Smurf attack.
Stacheldraht	It is written by Random for Linux and Solaris systems, which acts as a DDoS agent. It combines features of Trinoo with TFN and adds encryption.
Shaft	This network looks conceptually similar to a Trinoo; it is a packet flooding attack and the client controls the size of the flooding packets and duration of the attack.
MStream	It uses spoofed TCP packets with the ACK flag set to attack the target. Communication is not encrypted and is performed through TCP and UDP packets. Access to the handler is password protected. This program has a feature not found in other DDoS tools. It informs all connected users of access, successful or not, to the handler(s) by competing parties.

DOS AND DDOS ATTACKS

How to Protect from DoS/DDoS Attacks

- Computer Emergency Response Team Coordination Center (CERT/CC) offers many preventive measures from being a victim of DoS attack.
  1. Implement router **filters**. This will lessen your exposure to certain DoS attacks.
  2. If such filters are available for your system, **install patches** to 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.
  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
  11. Establish and maintain appropriate password policies

DOS AND DDOS ATTACKS

Tools for detecting DoS/DDoS attacks

Tool	*Brief Description*
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. It assumes various defaults are still in place used by these attack tools, however, it allows you to put the zombies to sleep.
Remote Intrusion Detector (RID)	It is a tool developed in "C" computer language, which is a highly configurable packet snooper and generator. It works by sending out packets defined in the config.txt file, then listening for appropriate replies. It detects the presence of Trinoo, TFN or Stacheldraht clients.
Security Auditor's Research Assistant (SARA)	It gathers information about remote hosts and networks by examining network services. This includes information about the network information services as well as potential security flaws such as incorrectly set up or configured network services, well-known bugs in the system or network utilities system software vulnerabilities listed in the Common Vulnerabilities and Exposures (CVE) database and weak policy decisions.
Find_DDoS	It is a tool that scans a local system that likely contains a DDoS program. It can detect several known DoS attack tools.
DDoSPing	It is a remote network scanner for the most common DDoS programs. It can detect Trinoo, Stacheldraht and Tribe Flood Network programs running with their default settings.

SQL INJECTION

- Structured Query Language (SQL) is a database computer language designed for managing data in relational database management systems (RDBMS).
- SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.
- SQL injection attacks are also known as SQL insertion attacks.
- Attackers target the SQL servers –common database servers used by many organizations to store confidential data.
- The prime objective behind SQL injection attack is to obtain the information while accessing a database table that may contain personal information such as credit 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.
- For example, when a user logs in with username and password, an SQL query is sent to the database to check if a user has valid name and password.
- With SQL injection, it is possible for an attacker to send crafted username and/or password field that will change the SQL query.

SQL INJECTION

Steps for SQL Injection Attack

- Following are some steps for SQL injection attack:
- 1. The attacker looks for the webpages that allow submitting data, that is, login page, search page, feedback, etc. The attacker also looks for the webpages that display the HTML commands such as POST or GET by checking the site's source code.
- 2. To check the source code of any website, right click on the webpage and click on "view source" – source code is displayed in the notepad. The attacker checks the source code of the HTML, and look for "FORM" tag in the HTML code.
  - Everything between the <FORM> and </FORM> have potential parameters that might be useful to find the vulnerabilities.

    <FORM action=Search/search.asp method=post>

    <input type=hidden name=A value=C>

    </FORM>

SQL INJECTION

- 3. The attacker inputs a *single quote* under the text box provided on the webpage to accept the username and password. This checks whether the user-input variable is interpreted literally by the server. If the response is an error message such as *use "a" = "a"* then the website is found to be susceptible to an SQL injection attack.
- 4. The attacker uses SQL commands such as SELECT statement command to retrieve data from the database or INSERT statement to add information to the database.
- Here are few examples of variable field text the attacker uses on a webpage to test for SQL vulnerabilities:
  - 1. *Blah' or 1=1--*
  - 2. *Login:blah' or 1=1--*
  - 3. *Password::blah' or 1=1--*
  - 4. *http://search/index.asp?id=blah' or 1=1--*
- Similar SQL commands may allow bypassing of a login and may return many rows in a table or even an entire database table because the SQL server is interpreting the terms literally.
- The double dashes near the end of the command tell SQL to ignore the rest of the command as a comment.

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.
- This type of attack can become time-intensive because a new statement must be crafted for each bit recovered.
- There are several tools that can automate these attacks once the location of the vulnerability and the target information have been established.

SQL INJECTION

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.
  - Sanitize the input: User input needs to be checked and cleaned of any characters or strings that could possibly be used maliciously. For example, character sequences such as ; , --, select, insert and xp_ can be used to perform an SQL injection attack.
  - Numeric values should be checked while accepting a query string value. Function –IsNumeric() for Active Server Pages (ASP) should be used to check these numeric values.
  - Keep all text boxes and form fields as short as possible to limit the length of user input.
- **2. Modify error reports:**
  - SQL errors should not be displayed to outside users
- **3. Other preventions**
  - The default system accounts for SQL server 2000 should never be used.
  - Isolate database server and web server.
  - Most often attackers may make use of several extended stored procedures

SQL INJECTION

Tool	*Brief Description*
http://www.appsecinc.com	**AppDetectivePro:** It is a network-based, discovery and vulnerability assessment scanner that discovers database applications within the infrastructure and assesses security strength. It locates, examines, reports and fixes security holes and misconfigurations as well as identify user rights and privilege levels based on its security methodology and extensive knowledge based on application-level vulnerabilities. Thus, organizations can harden their database applications.
http://www.appsecinc.com	**DbProtect:** It enables organizations with complex, heterogeneous environments to optimize database security, manage risk and bolster regulatory compliance. It integrates database asset management, vulnerability management, audit and threat management, policy management, and reporting and analytics for a complete enterprise solution.
http://www.iss.net	**Database Scanner:** It is an integrated part of Internet Security Systems' (ISS) Dynamic Threat Protection platform that assesses online business risks by identifying security exposures in the database applications. Database scanner offers security policy generation and reporting functionality, which instantly measures policy compliance and automates the process of securing critical online business data. Database scanner runs independently of the database and quickly generates detailed reports with all the information needed to correctly configure and secure databases.

SQL INJECTION

CYBERSECURITY

Tool	*Brief Description*
http://www.ca.com/us/securityadvisor	**SQLPoke:** It is an NT-based tool that locates Microsoft SQL (MSSQL) servers and tries to connect with the default System Administrator (SA) account. A list of SQL commands are executed if the connection is successful.
http://www.ngssoftware.com/	**NGSSQLCrack:** It can guard against weak passwords that make the network susceptible to attack. This is a password cracking utility for Microsoft SQL server 7 and 2000 and identifies user accounts with weak passwords so that they can be reset with stronger ones, thus, protecting the overall integrity of the system.
http://www.security-database.com/toolswatch	**Microsoft SQL Server Fingerprint (MSSQLFP) Tool:** This is a tool that performs fingerprinting version on Microsoft SQL Server 2000, 2005 and 2008, using well-known techniques based on several public tools that identifies the SQL version and also can be used to identify vulnerable versions of Microsoft SQL Server

Tools used for SQL Server penetration

BUFFER OVERFLOW

- Buffer overflow, or buffer overrun, is an anomaly where a process stores data in a buffer outside the memory the programmer has set aside for it.
- This may result unreliable program behavior, including memory access errors, incorrect results, program termination (a crash) or a breach of system security.
- Buffer overflows can be triggered by inputs that are designed to execute code or alter the way the program operates. They are, thus, the basis of many software vulnerabilities and can be maliciously exploited.
- Bounds checking can prevent buffer overflows.
- Programming languages commonly associated with buffer overflows include C and C++, which provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to an array.
- 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.
- Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.
- The knowledge of C, C++ or any other high-level computer language (i.e., assembly language) is essential to understand buffer overflow.

Ex:

```
int main () {
        int buffer[10];
        buffer[20] = 10;
} //
```

However, the program attempts to write beyond the allocated memory for the buffer, which might result in an unexpected behavior

BUFFER OVERFLOW

Types of Buffer Overflow

1. Stack-Based Buffer Overflow

- Stack buffer overflow occurs when a program writes to a memory address on the program's call stack outside the intended data structure – usually a fixed length buffer. Here are the characteristics of stack-based programming:
  1. "Stack" is a memory space in which automatic variables (and often function parameters) are allocated.
  2. Function parameters are allocated on the stack and are not automatically initialized by the system, so they usually have garbage in them until they are initialized.
  3. Once a function has completed its cycle, the reference to the variable in the stack is removed.

BUFFER OVERFLOW

- The attacker may exploit stack-based buffer overflows to manipulate the program in various ways by overwriting:
  1. A local variable that is near the buffer in memory on the stack to change the behavior of the program that may benefit the attacker.
  2. The return address in a stack frame. Once the function returns, execution will resume at the return address as specified by the attacker, usually a user input-filled buffer.
  3. A function pointer, or exception handler, which is subsequently executed.
- The factors that contribute to overcome the exploits are
  1. Null bytes in addresses;
  2. Variability in the location of shell code;
  3. Differences between environments. A shell code is a small piece of code used as a payload in the exploitation of software vulnerability.
- It is called “shell code” because it starts with command shell from which the attacker can control the compromised machine.

BUFFER OVERFLOW

2. NOPs

- NOP or NOOP (short form of **no operation**) is an assembly language instruction/ command that effectively does nothing at all.
- The explicit purpose of chis command is nor to change the state of status flags or memory locations in the code. This means NOP enables the developer to force memory alignment to act as a place holder to be replaced by active instructions later on in program development.
- It is the oldest and most widely used technique for successfully exploiting a stack buffer overflow, It helps to know/locate the exact address of the buffer by effectively increasing the size of the target stack buffer area. The attacker can increase the odds of findings the right memory address by padding his/her code with NOP operation.

BUFFER OVERFLOW

3. Heap Buffer Overflow

- Heap buffer overflow occurs in the heap data area and may be introduced accidentally by an application programmer, or it may result from a deliberate exploit. The characteristics of stack based and heap-based programming are as follows:
  1. “Heap” is a “free store” that is a memory space, where dynamic objects are allocated.
  2. The heap is the memory space that is dynamically allocated new(), malloc() and calloc() functions; it is different from the memory space allocated for stack and code.
  3. Dynamically created variables (i.e., declared variables) are created on the heap before the execution program is initialized to zero
- Memory on the heap is dynamically allocated by the application at run-time and normally contains program data. Exploitation is performed by corrupting this data in specific ways to cause the application to overwrite internal structures such as linked list pointers.

BUFFER OVERFLOW

How to Minimize Buffer Overflow

1. **Assessment of secure code manually:** Buffer overflow occurs when a program or process tries to store more data in a buffer than it was intended to hold. Developers should be educated about minimizing the use of functions like strcpy(), strcat(), sprintf() and vsprintf() in C Language.
2. **Disable stack execution:** Malicious Code causes input argument to the program, and it resides in the stack and not in the code segment. Any code that attempts to execute any other code residing in the stack will cause a segmentation violation.
3. **Compiler tools:** Over the years, compilers have become more and more aggressive in optimizations and the checks they perform. Various compiler tools already offer warnings on the use of unsafe constructs such as gets(), strcpy(), etc. Developers should be educated to restructure the programming code if such warnings are displayed.
4. **Dynamic run-time checks:** In this scheme, an application has restricted access to prevent attacks. This method primarily relies on the safety code being preloaded before an application is executed. This preloaded component can either provide safer versions of the standard unsafe functions or it can ensure that return addresses are not overwritten. One example of such a tool is libsafe. The libsafe library provides a way to secure calls to these functions, even if the function is not available.

BUFFER OVERFLOW

CYBERSECURITY

5. Various tools are used co detect/defend buffer overflow

Tool	*Brief Description*
StackGuard	It was released for GCC in 1997 and published at USENIX Security 1998. It is an extension to GCC that provides buffer overflow protection. It was invented by Crispin Cowan. It is a compiler approach for defending programs and systems against "stack-smashing" attacks. These attacks are the most common form of security vulnerability. Programs that have been compiled with StackGuard are largely immune to stack-smashing attack. Whenever vulnerability is exploited, it detects the attack in progress, raises an intrusion alert and halts the victim program.
ProPolice	The "stack-smashing protector" or SSP, also known as ProPolice, is an enhancement of the StackGuard concept written and maintained by Hiroaki Etoh of IBM. Its name derives from the word propolis. The stack protection provided by ProPolice is specifically for the C and C++ languages. It is also optionally available in Gentoo Linux with the hardened USE flag.
LibSafe	It was released in April 2000 and gained popularity in the Linux community. It does not need access to the source code of the program to be protected. Libsafe protection is system wide and automatically gets attached to the applications. It is based on a middle-ware software layer that intercepts all function calls made to library functions known to be vulnerable. A substitute version of the corresponding function implements the original function in a way that ensures that any buffer overflows are contained within the current stack frame, which prevents attackers from overwriting the return address and hijacking the control flow of a running program. The real benefit of using libsafe is protection against future attacks on programs not yet known to be vulnerable.