# UNIT -IV: Tools and Methods Used in Cybercrime

1. Introduction
2. Proxy Servers and Anonymizers,
3. Phishing
4. Password Cracking
5. Key loggers and Spywares
6. Virus and Worms
7. Trojan Horses and Backdoors
8. Steganography
9. DoS and DDoS Attacks
10. SQL Injection
11. Buffer Overflow
12. Attacks on Wireless Networks
13. Phishing and Identity Theft: Introduction - Phishing,
14. Identity Theft (ID Theft)

## 4.1 Introduction

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

**1. Initial uncovering:**

Two steps are involved here.

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

**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 basically an administrator or super-user access and grants them the privileges to do anything on the system.

**4. Capturing the network:**

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

**5. Grab the data:**

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

**6. Covering tracks:**

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

**Table 4.1** | 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. |
| 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). |
| 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. |

## 4.2 Proxy Servers and Anonymizers

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

**A proxy server has following purposes:**

**1.** Keep the systems behind the curtain (mainly for security reasons).

**2.** Speed up access to a resource (through "caching"). It is usually used to cache the webpages from a web server.

**3.** Specialized proxy servers are used to filter unwanted content such as advertisements.

**4.** Proxy server can be used as IP address multiplexer to enable to connect number of computers on the Internet, whenever one has only one IP address

Listed are few websites where free proxy servers can be found:

- http://www.proxy4free.com
- http://www.publicproxyservers.com
- http://www.proxz.com
- http://www.anonymitychecker.com
- http://www.surf24h.com

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

## 4.3 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.

### 4.3.1 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.

## 4.4 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.

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

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

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

The most commonly used hash functions can be computed rapidly and the attacker can test these hashes with the help of passwords cracking tools (see Table 4.3) to get the plain text password.

text pass... ...the plain

**Table 4.3 | 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. |
| 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. |

(*Continued*

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).

### 4.4.1 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.

### 4.4.2 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.

**Table 4.4** | Types of password cracking attacks

| *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 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 cyber cafes/hotels/libraries.
7. Passwords should not be stored under mobile phones/PDAs, as these devices are also prone to cyber attacks.
8. In case E-Mail accounts/user accounts have been hacked, respective agencies/institutes should be contacted immediately.

## 4.5 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.

### 4.5.1 Software Keyloggers

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

Some Important Keyloggers are as follows

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

**Table 4.5** | Software keyloggers

| *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. |
| 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:<br>• Internet conversation logging;<br>• disk activity logging;<br>• Window activity logging;<br>• application activity logging;<br>• clipboard activity logging;<br>• AOL/Internet explorer history;<br>• printed documents logging;<br>• keylogger keystroke monitoring;<br>• websites activity logging;<br>• screenshot capturing;<br>• WebWatch keyword alerting |

*(Continued)*

### 4.5.2 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.

Listed are few websites where more information about hardware keyloggers can be found:

- http://www.keyghost.com
- http://www.keelog.com
- http://www.keydevil.com
- http://www.keykatcher.com

### 4.5.3 Antikeylogger

Antikeylogger is a tool that can detect the keylogger installed on the computer system and also can remove the tool. (Visit http://www.anti-keyloggers.com for more information)

Advantages of using anti keylogger 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 anti-spy programs; if not updated, it does not serve the purpose, which makes the users at risk.
3. Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers.
4. It prevents ID theft (we will discuss it more in Chapter 5).
5. It secures E-Mail and instant messaging/chatting.

### 4.5.4 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.

Some Important Spywares are as follows

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

**Table 4.6 | Spywares**

| *Website* | *Brief Description* |
|---|---|
| http://www.e-spy-software.com | **007 Spy:** It has following key features:<br>• Capability of overriding "antispy" programs like "Ad-aware";<br>• record all websites URL visited in Internet;<br>• powerful keylogger engine to capture all passwords;<br>• view logs remotely from anywhere at anytime;<br>• export log report in HTML format to view it in the browser;<br>• automatically clean-up on outdated logs;<br>• password protection. |
| http://www.spectorsoft.com | **Spector Pro:** It has following key features:<br>• Captures and reviews all chats and instant messages;<br>• captures E-Mails (read, sent and received);<br>• captures websites visited;<br>• captures activities performed on social networking sites such as MySpace and Facebook;<br>• enables to block any particular website and/or chatting with anyone;<br>• 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. |
| 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. |

(*Continued*)

**Table 4.6 | (*Continued*)**

| *Website* | *Brief Description* |
|---|---|
| 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:<br>• Real-time MP3 recording via microphone, CD, line-in and stereo mixer as MP3, WMA or WAV formatted files;<br>• transferring via E-Mail or FTP, the recorded files to a user-defined E-Mail address or FTP automatically;<br>• controlling from a remote location;<br>• 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:<br>• Monitor visited websites;<br>• reports sent to an E-Mail address;<br>• daily log;<br>• global log for a specified period;<br>• log deletion after a specified period;<br>• hotkey and password protection;<br>• not visible in add/remove programs or task manager. |
| 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:<br>• Keep track on a printer/plotter usage;<br>• record every document printed;<br>• find out who and when certain paper printed with your hardware. |

**Box 4.3 | Malwares**

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

**1. Viruses and worms:** These are known as *infectious malware*. They spread from one computer

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

## 4.6 Virus and Worms

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

Viruses can take some typical actions:

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

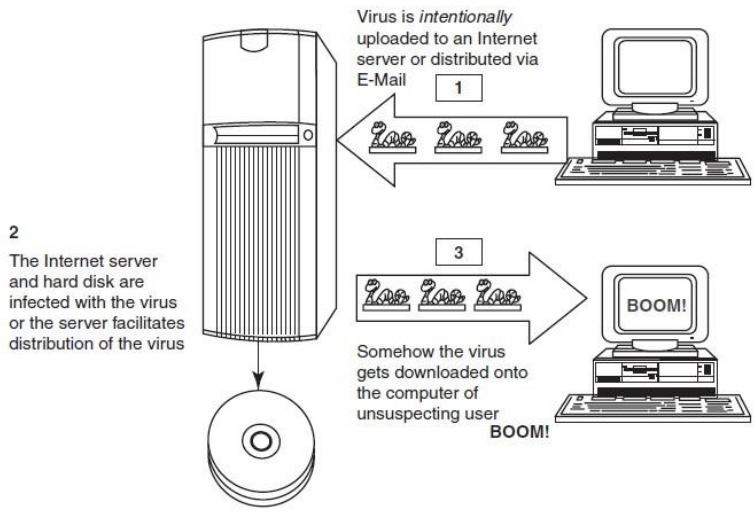


**Figure 4.1** | Virus spreads through the Internet.

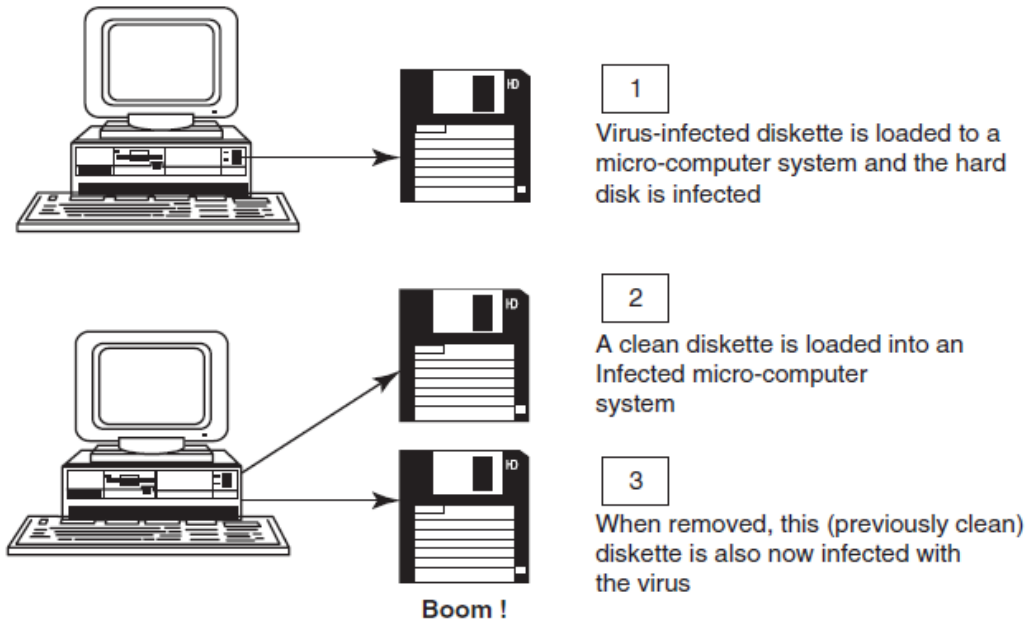


**Figure 4.2** | Virus spreads through stand-alone system.

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

### 4.6.1 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., macro languages). These macros are programmed as a macro embedded in a document. Once macro virus gets onto a victim's computer then every document he/she produces will become infected.
7. **Active X and Java Control:** All the web browsers have settings about Active X and Java Controls.

**World's worst worm attacks.**

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

**The world's worst virus and worm attacks.**

| | | | |
|---|---|---|---|
| Morris Worm | I LOVEYOU | Nimda | Jerusalem |
| Code Red | Melissa | MSBlast | |
| Sobig | Storm Worm | Michelangelo | |

Table 4.7 | Difference between computer virus and worm

| 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. |

*Source:* See [18] in References section.

## 4.7 Trojan Horses and Backdoors

- Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm, for example, ruining the file allocation table on the hard disk.
- A Trojan Horse may get widely redistributed as part of a computer virus.
- The term Trojan Horse comes from Greek mythology about the Trojan War.

- Like Spyware and Adware, Trojans can get into the system in a number of ways, including from a web browser, via E-Mail.
- It is possible that one could be forced to reformat USB flash drive or other portable device to eliminate infection and avoid transferring it to other machines
- Unlike viruses or worms, Trojans do not replicate themselves but they can be equally destructive.
- On the surface, Trojans appear benign and harmless, but once the infected code is executed, Trojans kick in and perform malicious functions to harm the computer system without the user's knowledge.
- For example, waterfalls.scr is a waterfall screen saver as originally claimed by the author; however, it can be associated with malware and become a Trojan to unload hidden programs and allow unauthorized access to the user's PC.

Some typical examples of threats by Trojans are as follows:

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

### 4.7.1 Backdoor

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

**Following are some functions of backdoor:**

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

**Following are a few examples of backdoor Trojans:**

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

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

**1. Stay away from suspect websites/weblinks:** Avoid downloading free/pirated softwares that often get

infected by Trojan's, worms, viruses and other things.

2. **Surf on the Web cautiously:** Avoid connecting with and /or downloading any information from peer-to-peer networks, which are most dangerous networks to spread Trojan horses and other threats.
3. **Install antivirus/Trojan remover software:** Now a days anti-virus software's has built in feature for protecting the system not only from viruses and worms but also from malware such as Trojan Horses. Free Trojan remover programs are also available on the web.

## 4.8 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".

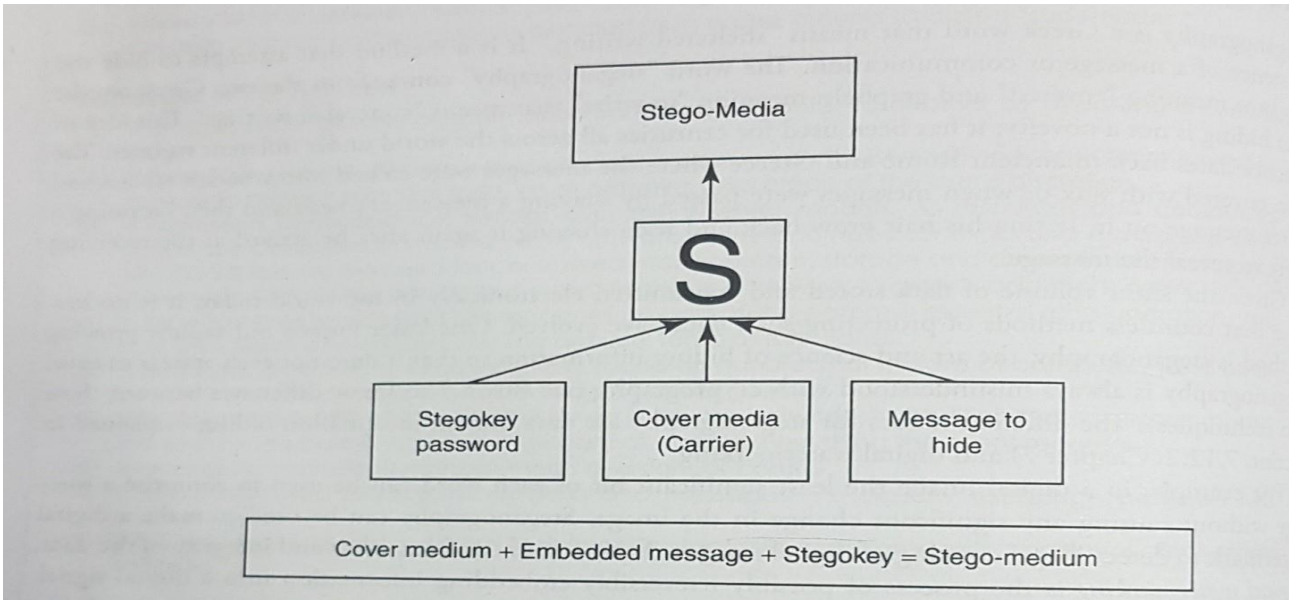


**Figure 4.4** How steganography works.
*Source:* http://www.cosc.iup.edu/sezekiel/Seminar/steg.ppt#452,15,Steganography%20of%20today's%20talk (11 May 10).

Table 4.10 | Steganography tools

| 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. |
| http://www.securstar.com/products_drivecryptpp.php | **DriveCrypt Plus (DCPP):** It has following features:<br>• It allows secure hiding of an entire OS inside the free space of another OS.<br>• Full-disk encryption (encrypts parts or 100% of your hard disk including the OS).<br>• 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:<br>• Small video distortions after hiding information.<br>• It is possible to extract information after video compression.<br>• Information is protected with the password. |

### 4.8.1 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.

**Box 4.7 | Difference between Steganography and Cryptography**

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

## 4.9 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.

### 4.9.1 DoS Attacks

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

The United States Computer Emergency Response Team defines symptoms of DoS attacks to include:

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

### 4.9.2 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.

### 4.9.3 Types or Levels of DoS Attacks

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

1. **Flood attack:** This is the earliest form of DoS attack and is also known as *ping food*. It 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.

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.
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.**

### 4.9.4 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 diff erent 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.

### 4.9.5 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.

| Sr. No. | Tool | Brief Description |
|---|---|---|
| 1 | 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. |
| 2 | 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. |
| 3 | 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. |
| 4 | 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. |
| 5 | 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. |

### 4.9.6 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.[33]

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

**Table 4.15** | Tools for detecting DoS/DDoS attacks

| Sr. No. | Tool | Brief Description |
|---|---|---|
| 1 | Zombie Zapper | It is a free, open-source tool that can tell a zombie system flooding packets to stop flooding. It works against Trinoo, TFN and Stacheldraht. It assumes various defaults are still in place used by these attack tools, however, it allows you to put the zombies to sleep. |
| 2 | 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. |
| 3 | 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. |
| 4 | 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. |
| 5 | 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. |

## 4.10 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.

### 4.10.1 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>*

**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.

***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.

**Table 4.16** | Tools used for SQL Server penetration

| Sr. No. | Tool | Brief Description |
|---|---|---|
| 1 | 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. |
| 2 | 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. |
| 3 | 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. |

(*Continued*)

**Table 4.16** | (*Continued*)

| Sr. No. | Tool | Brief Description |
|---|---|---|
| 4 | 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. |
| 5 | 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. |
| 6 | 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 |

### 4.10.2 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.

## 4.11 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.

  For example,
  ```
  int main () { int buffer[10]; buffer[20] = 10; }
  ```
- This C program is a valid program and every compiler can compile it without any errors.
- However, the program attempts to write beyond the allocated memory for the buffer, which might result in an unexpected behavior.

### 4.11.1 Types of Buffer Overflow

***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.

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.

***NOPs:***

NOP or NOOP (short form of **no operation**) is an assembly language instruction/ command that effectively does nothing at all.

***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.

### 4.11.2 How to Minimize Buffer Overflow

Although it is difficult to prevent all possible attacks, the following methods will definitely help to minimize such attacks:

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 off er 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.

### 4.11.2 How to Minimize Buffer Overflow

Although it is difficult to prevent all possible attacks, the following methods will definitely help to minimize such attacks:

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 vulnerable functions available in C library, such as strcpy(), strcat(), sprintf() and vsprintf(), which operate on null-terminated strings and perform no bounds checking. The input validation after scanf() function that reads user input into a buffer is very essential.
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. Therefore, the simplest solution is to invalidate the stack to execute any instructions. However, the solution is not easy to implement. Although possible in Linux, some compilers [(including GNU Compliance Connection (GCC)] use trampoline functions to implement taking the address of a nested function that works on the system stack being executable. A trampoline is a small piece of code created at run-time when the address of a nested function is taken. It normally resides in the stack and in the stack frame of the containing function and thus requires the stack to be executable. However, a version of the Linux kernel that enforces the non-executable stack is freely available.
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

Table 4.17 | Tools used to defend/protect buffer overflow

| *Sr. No.* | *Tool* | *Brief Description* |
|---|---|---|
| 1 | 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. |
| 2 | 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. |
| 3 | 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 middleware 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. |

## 4.12 Attacks on Wireless Networks

- Wireless technologies have become increasingly popular in day-to-day business and personal lives.
- Hand-held devices such as the PDAs allow individuals to access calendars, E-Mail addresses, phone number lists and the Internet.
- Wireless networks extend the range of traditional wired networks by using radio waves to transmit

data to wireless-enabled devices such as laptops and PDAs.

- Wireless networks are generally composed of two basic elements:
  (a) access points (APs) and
  (b) other wireless-enabled devices, such as laptops radio transmitters and receivers to communicate or "connect" with each other (see Fig. 4.6).
- APs are connected through physical wiring to a conventional network, and they broadcast signals with which a wireless device can connect.
- Wireless access to networks has become very common by now in India – for organizations and for individuals.

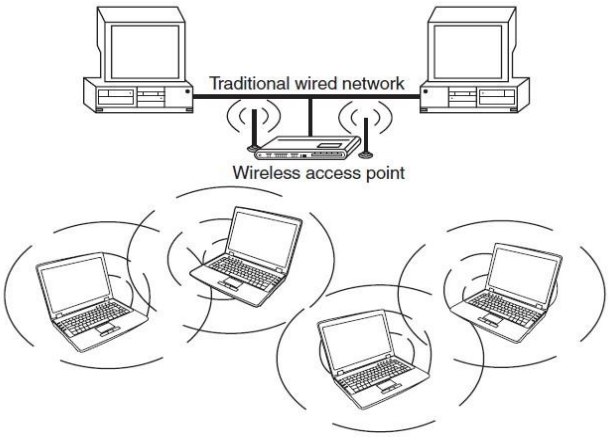


**Figure 4.6** | Wireless networks.

**The following are different types of "mobile workers":**

**1. Tethered/remote worker:** This is considered to be an employee who generally remains at a single point of work, but is remote to the central company systems.

**2. Roaming user:** This is either an employee who works in an environment (e.g., warehousing, shop floor, etc.) or in multiple areas (e.g., meeting rooms).

**3. Nomad:** This category covers employees requiring solutions in semi-tethered (connected) environments where modem use frequently.

**4. Road warrior:** This is the ultimate mobile user and spends little time in the office;

**Important components of wireless network**

**1. 802.11 networking standards:** Institute of Electrical and Electronics Engineers (IEEE)-802.11 is a family of standards for wireless local area network (WLAN), stating the specifications and/or requirements for computer communication.

**2. Access points:** It is also termed as AP. It is a hardware device and/or software that act as a central transmitter and receiver of WLAN radio signals. Users of wireless device, such as laptop/PDAs, get connected with these APs, which in turn get connected with the wired LAN. An AP acts as a communication hub for users to connect with the wired LAN.

**3. Wi-Fi hotspots:** A hotspot is a site that offers the Internet access by using Wi-Fi technology over a WLAN. Hotspots are found in public areas (such as coffee shops, public libraries, hotels and restaurants) and are commonly offered facility throughout much of North America and Europe.

• *Free Wi-Fi hotspots:* Wireless Internet service is offered in public areas, free of cost and that to without any authentication.

• *Commercial hotspots:* The users are redirected to authentication and online payment to avail the wireless Internet service in public areas.

**4. Service Set Identifier (SSID):** It is the name of 802.11i WLAN and all wireless devices on a WLAN must use the same SSID to communicate with each other. While setting up WLAN, the user (or WLAN administrator) sets the SSID, which can be up to 32 characters long so that only the users who knew the SSID will be able to connect the WLAN. It is always advised to turn OFF the broadcast of the SSID.

**5. Wired equivalence privacy (WEP):** Wireless transmission is susceptible to eavesdropping and to provide confidentiality, WEP was introduced as part of the original 802.11i Protocol in 1997. It is always

termed as deprecated security algorithm for IEEE 802.11i WLANs. SSID along with WEP delivers fair amount of secured wireless network.

**6. Wi-Fi protected access (WPA and WPA2):** WPA was introduced as an interim standard to replace WEP to improve upon the security features of WEP. WPA2 provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some corporate and government agencies.

**7. Media access control (MAC):** It is a unique identifier of each node (i.e., each network interfaces) of the network and it is assigned by the manufacturer of a network interface card (NIC) stored in its hardware. MAC address filtering allows only the devices with specific MAC addresses to access the network.

| **Tools used for hacking wireless networks** |
|---|
| **NetStumbler:** This tool is based on Windows OS and easily identifies wireless signals being broadcast within range.( http://www.netstumbler.com) |
| **Kismet:** This tool detects and displays SSIDs that are not being broadcast which 0is very critical in finding wireless networks. ( http://www.kismetwireless.com) |
| **Airsnort:** This tool is very easy and is usually used to sniff and crack WEP keys ( http://www.sourceforge.net) |
| **CowPatty:** This tool is used as a brute force tool for cracking WPA-PSK and is considered to be the "New WEP" for home wireless security. ( http://www.wirelessdefence.org) |
| **Wireshark (formerly ethereal):** Ethereal can scan wireless and Ethernet data and comes with some robust filtering capabilities. It can also be used to sniff out 802.11 management Beacons and probes, and subsequently could be used as a tool to sniff out non-broadcast SSIDs. ( http://www.wireshark.org) |

### 4.12.1 Traditional Techniques of Attacks on Wireless Networks

In security breaches, penetration of a wireless network through unauthorized access is termed as *wireless cracking*. There are various methods that demand high level of technological skill and knowledge, and availability of numerous software tools made it less sophisticated with minimal technological skill to crack WLANs.

**1. Sniffing:** The attacker usually installs the sniffers remotely on the victim's system and conducts activities such as

- Passive scanning of wireless network;
- detection of SSID;
- colleting the MAC address;
- collecting the frames to crack WEP.

**2. Spoofing:** The attacker often launches an attack on a wireless network by simply creating a new network with a stronger wireless signal and a copied SSID in the same area as a original network. Different types of Spoofing are as follows.

- *MAC address Spoofing*: It is a technique of changing an assigned Media Access Control of a networked device to a different one.
- *IP Spoofing:* It is a process of creating IP packets with a forged source IP address.
- *Frame Spoofing:* The attacker injects the frames whose content is carefully spoofed and which are valid as per 802.11 specifications.

**3. Denial of service (DoS):** We have explained this attack in detail in UNIT-2.

**4. Man-in-the-middle attack (MITM):** It refers to the scenario wherein an attacker on host *A* inserts *A* between all communications – between hosts *X* and *Y* without knowledge of *X* and *Y*. All messages sent by *X* do reach *Y* but through *A* and vice versa. The objective behind this attack is to merely observe the communication or modify it before sending it out.

**5. Encryption cracking:** It is always advised that the first step to protect wireless networks is to use WPA encryption. The attackers always devise new tools and techniques to deconstruct the older

encryption technology, which is quite easy for attackers due to continuous research in this field. Hence, the second step is to use a long and highly randomized encryption key; this is very important. It is a little pain to remember long random encryption; however, at the same time these keys are much harder to crack.

### 4.12.2 How to Secure the Wireless Networks

Nowadays, security features of Wi-Fi networking products are not that time-consuming and non-intuitive; however, they are still ignored, especially, by home users. Although following summarized steps will help to improve and strengthen the security of wireless network, to know the available tools to monitor and protect the wireless networks:

1. Change the default settings of all the equipment's /components of wireless network (e.g., IP address/ user IDs/administrator passwords, etc.).
2. Enable WPA/WEP encryption.
3. Change the default SSID.
4. Enable MAC address filtering.
5. Disable remote login.
6. Disable SSID broadcast.
7. Disable the features that are not used in the AP (e.g., printing/music support).
8. Avoid providing the network a name which can be easily identified (e.g., My_Home_Wifi ).
9. Connect only to secured wireless network (i.e., do not auto connect to open Wi-Fi hotspots).
10. Upgrade router's firmware periodically.
11. Assign static IP addresses to devices.
12. Enable firewalls on each computer and the router.
13. Position the router or AP safely.
14. Turn off the network during extended periods when not in use.
15. Periodic and regular monitor wireless network security.

**Box 4.11 | The New "Wars" in the Internet Era!**

1. **Warwalking: Searching for wireless networks is done on foot rather than conducted from a moving vehicle.**
2. **Warbiking: Searching for wireless networks is done while on a moving bicycle or motor cycle.**
3. **Warkitting: This is a combination of wardriving and rootkitting.**
4. **WAPKitting: In this attack external software clutches the control of routers firmware that can be easily accomplished by exploiting open administrative access.**
5. **WAPjacking: This is similar to DNS poisoning attacks. It changes the settings of existing firmware.**

Table 4.19 | Tools to protect wireless network

| *Website* | *Brief Description* |
|---|---|
| http://www.zamzom.com/ | **Zamzom Wireless Network Tool:** New freeware tool helps to protect wireless networks and maintain computer security, detects all computer names, Mac and IP addresses utilizing a single wireless network, reveals all computers – both authorized and unauthorized – who have access to any given wireless network. Thus, it helps users to take vital steps toward securing their wireless networks and acts as a measure that should not be overlooked or skipped. |
| http://www.airdefense.net/ | **AirDefense Guard:** The tool provides advanced intrusion detection for wireless LANs and is based on signature analysis, policy deviation, protocol assessment policy deviation and statistically anomalous behavior. AirDefense detects responds to:<br>• Denial-of-service (DoS) attacks;<br>• man-in-the-middle attacks;<br>• identity theft. |
| http://www.loud-fat-bloke.co.uk/tools.html | **Wireless Intrusion Detection System (WIDZ):** This is an intrusion detection for wireless LANs for 802.11. It guards APs and monitors local frequencies for potentially malevolent activity. It can detect scans, association floods and bogus APs, and it can easily be integrated with other products such as SNORT or Realsecure. |
| http://www.dachb0den.com/projects/bsd-airtools.html | **BSD-Airtools:** This tool provides a complete toolset for wireless auditing (802.11b). It contains AP detection application, Dstumbler – similar to Netstumbler. It can be used to detect wireless access points and connected nodes, view signal-to-noise graphs, and interactively scroll through scanned APs and view statistics for each. It also contains a BSD-based WEP cracking application (called as Dweputils). |
| http://wifi.google.com/ | **Google Secure Access:** Google Wi-Fi is a free wireless Internet service offered to the city of Mountain View (California, USA). With your Wi-Fi-enabled device and a Google Account, one can go online for free by accessing the network name "GoogleWi-Fi," which is secured by Google's virtual private network (VPN). Google Secure Access encrypts the Internet traffic and sends it through Google's servers on the Internet. |

## 4.13 Phishing and Identity Theft: Introduction , Phishing

(Phishing: See 4.3 for more details)

Identity theft can be done thorough the following ways.

### A. Spam E-Mails

- Also known as "junk E-Mails" they involve nearly identical messages sent to numerous recipients. Spam E-Mails have steadily grown since the early 1990s. Botnets, networks of virus-infected computers, are used to send about 80% of Spam.
- Types of Spam E-Mails are as follows:

**1. Unsolicited bulk E-Mail (UBE):** It is *synonym for SPAM* unsolicited E-Mail sent in large quantities (see Box 5.2).

**2. Unsolicited commercial E-Mail (UCE):** Unsolicited E-Mails are sent in large quantities from commercial perspective, for example, advertising. See Box 5.3 to know more about US Act on Spam mails.

Examples:

**1. HSBC, Santander, Common Wealth Bank:** International Banks having large customer base, phishers always dive deep in such ocean to attempt to hook the fi sh.

**2. eBay:** It is a popular auction site, often mimicked to gain personal information.

**3. Amazon:** It was the top brand to be exploited by phishers till July 2009.

**4. Facebook:** Netizens, who liked to be on the most popular social networking sites such as Facebook, are always subject to threats within Facebook as well as through E-Mail. One can reduce chances of being victim of Phising attack by using the services – security settings to enable contact and E-Mail details as private.

The E-Mail will usually ask the user to provide valuable information about himself /herself or to "verify"

information that the user may have provided in the past while registering for online account. To maximize the chances that a recipient will respond, the phisher might employ any or all of the following tactics: [10]

**1. Names of legitimate organizations:** Instead of creating a phony company from scratch, the phisher might use a legitimate company's name and incorporate the look and feel of its website (i.e., including the color scheme and graphics) into the Spam E-Mail.
**2. "From" a real employee:** Real name of an official, who actually works for the organization. This way, if a user contacts the organization to confirm whether "Rajeev Arora" truly is "Vice President of Marketing" then the user gets a positive response and feels assured.
**3. URLs that "look right":** The E-Mail might contain a URL (i.e., weblink) which seems to be original website wherein user can enter the information the phisher would like to steal.
**4. Urgent messages:** Creating a fear to trigger a response is very common in Phishing attacks – the E-Mails warn that failure to respond will result in no longer having access to the account or E-Mails might claim that organization has detected suspicious activity in the users' account or that organization is implementing new privacy software for ID theft solutions.

**Here are a few examples of phrases used to entice the user to take the action.**

**1. "Verify your account":**
**2. "You have won the lottery":**
**3. "If you don't respond within 48 hours, your account will be closed":**

**Let us understand the ways to reduce the amount of Spam E-Mails we receive.**
**1.** Share personal E-Mail address with limited people and/or on public websites – the more it is exposed to the public, the more Spam E-Mails will be received.
**2.** Never reply or open any Spam E-Mails.
**3.** Disguise the E-Mail address on public website or groups by spelling out the sign "@" and the DOT (.); for example, Rajeev**AT**gmail**DOT**com. This usually prohibits phishers to catch valid E-Mail addresses while gathering E-Mail addresses through programs.
**4.** Use alternate E-Mail addresses to register for any personal or shopping website. Never ever use business E-Mail addresses.
**5.** Do not forward any E-Mails from unknown recipients.
**6.** Make a habit to preview an E-Mail before opening it.
**7.** Never use E-Mail address as the screen name in chat groups or rooms.
**8.** Never respond to a Spam E-Mail asking to remove your E-Mail address from the mailing distribution list. More often it confirms to the phishers that your E-Mail address is active.

**B. Hoax E-Mails** (deceive or trick E-Mail)

- These are deliberate attempt to deceive or trick a user into believing or accepting that something is real, when the hoaxer (the person or group creating the hoax) knows it is false.
- Hoax E-Mails may or may not be Spam E-Mails.
- It is difficult sometimes to recognize whether an E-Mail is a "Spam" or a "hoax."
- **The websites mentioned below** can be used to check the validity of such "hoax" E-Mails.

**1. www.breakthechain.org: T**his website contains a huge database of chain E-Mails, like we discussed, the phisher sends to entice the netizens to respond to such E-Mails
**2. www.hoaxbusters.org:** This is an excellent website containing a large database of common Internet hoaxes. It is maintained by the Computer Incident Advisory Capability, which is a division of the US Department of Energy.

### 5.2.1 Methods of Phishing

Let us understand the most frequent methods used by the phishers[13] to entice the netizens to reveal their personal information on the Internet.

1. **Dragnet:** This method involves the use of spammed E-Mails, bearing falsified corporate identification (e.g., corporate names, logos and trademarks), which are addressed to a large group of people (e.g., customers of a particular financial institution or members of a particular auction site) to websites or pop-up windows with similarly falsified identification. Dragnet phishers do not identify specific prospective victims in advance. Instead, they rely on false information included in an E-Mail to trigger an immediate response by victims – typically, clicking on links in the body of the E-Mail to take the victims to the websites or pop-up windows where they are requested to enter bank or credit card account data or other personal data.
2. **Rod-and-reel:** In this method, phishers identify specific prospective victims in advance, and convey false information to them to prompt their disclosure of personal and financial data. For example, on the phony webpage, availability of similar item for a better price (i.e., cheaper price) is displayed which the victims may be searching for and upon visiting the webpage, victims were asked for personal information such as name, bank account numbers and passwords, before confirming that the "sale" and the information is available to the phisher easily.
3. **Lobsterpot:** This method focuses upon use of spoofed websites. It consists of creating of bogus/phony websites, similar to legitimate corporate ones, targeting a narrowly defined class of victims, which is likely to seek out. See Box 5.4 to know more about other attacks launched on the legitimate websites to grab the user's personal information. These attacks are also known as "content injection Phishing." Visit http://www.microsoft.com/protect/fraud/phishing/symptoms.aspx to see the example of a deceptive URL address linking to a scam website. The phisher places a weblink into an E-Mail message to make it look more legitimate and actually takes the victim to a phony scam site, which appears to be a legitimate website or possibly a pop-up window that looks exactly like the official site. These fake sites are also called "spoofed" websites. Once the netizen is into one of these spoofed sites, he/she might unwittingly send personal information to the con artists. Then they often use your information to purchase goods, apply for a new credit card or otherwise steal your identity. Box 5.5 explains Phishing vis-à-vis Spoofing.
4. **Gillnet:** This technique relies far less on social engineering techniques and phishers introduce Malicious Code into E-Mails and websites. They can, for example, misuse browser functionality by injecting hostile content into another site's pop-up window. Merely by opening a particular E-Mail, or browsing a particular website, netizens may have a Trojan Horse introduced into their systems. In some cases, the Malicious Code will change settings in user's systems so that users who want to visit legitimate banking websites will be redirected to a look alike Phishing site. In other cases, the Malicious Code will record user's keystrokes and passwords when they visit legitimate banking sites, and then transmit those data to phishers for later illegal access to users' financial accounts. We will discuss more on this in the next section while understanding Phishing techniques used by phishers.

### 5.2.2 Phishing Techniques

In this section we will discuss common ways, the techniques[17] used by phishers to launch Phishing attacks.

1. **URL (weblink) manipulation:** URLs are the weblinks (i.e., Internet addresses) that direct the netizens/users to a specific website. In Phishing attack, these URLs are usually supplied as misspelled, for example, instead of www.abcbank.com, URL is provided as www.abcbank1.com. Phishers use Lobsterpot method of Phishing and make the difference of one or two letters in the URLs, which is ignored by netizens. This makes a big difference and it directs users to a fake/bogus website or a webpage. See Box 5.6 to know about an advanced Phishing attack known as homograph attack.
2. **Filter evasion:** This technique use graphics (i.e., images) instead of text to obviate from netting such E-Mails by anti-Phishing filters. Normally, these filters are inbuilt into the web browsers. For example,
   - Internet Explorer version 7 has inbuilt "Microsoft phishing filter." One can enable it during the installation or it can be enabled post-installation. It is important to note that it is *not enabled* by default.
   - Firefox 2.0 and above has inbuilt "Google Phishing filter," duly licensed from Google. It is enabled by default.
   - The Opera Phishing filter is dubbed Opera Fraud Protection and is included in version 9.5+.
3. **Website forgery:** In this technique the phisher directs the netizens to the website designed and developed by him, to login into the website, by altering the browser address bar through JavaScript commands. As the netizen logs into the fake/bogus website, phisher gets the confidential information very easily. Another technique used is known as "cloaked" URL – domain forwarding and/or inserting control characters into the URL while concealing the weblink address of the real website.
4. **Flash Phishing:** Anti-Phishing toolbars are installed/enabled (see Table 5.2) to help checking the webpage content for signs of Phishing, but have limitations that they do not analyze flash objects at all. Phishers use it to emulate the legitimate website. Netizens believe that the website is "clean" and is a real website because anti-Phishing toolbar is unable to detect it.
5. **Social Phishing:** Phishers entice the netizens to reveal sensitive data by other means and it works in a systematic manner.
   - Phisher sends a mail as if it is sent by a bank asking to call them back because there was a security breach.
   - The victim calls the bank on the phone numbers displayed in the mail.
   - The phone number provided in the mail is a false number and the victim gets redirected to the phisher.
   - Phisher speaks with the victim in the similar fashion/style as a bank employee, asking to verify that the victim is the customer of the bank. For example, "Sir, we need to make sure that you are indeed our customer. Could you please supply your credit card information so that I can verify your identity?"
   - Phisher gets the required details swimmingly.
6. **Phone Phishing:** We have explained "Mishing" – mobile Phishing attacks ("Vishing" and "Smishing") in Chapter 3. Besides such attacks, phisher can use a fake caller ID data to make it appear that the call is received from a trusted organization to entice the users to reveal their personal information such as account numbers and passwords. See Box 5.7 to understand the innovative Phishing attack launched on "Android Market" website.

## Spear Phishing:

It is a method of sending a Phishing message to a particular organization to gain organizational information for more targeted social engineering. It is a highly targeted phishing attacks. This phishing send E-mails that appears genuine to all the employees or members within a certain company or organization.

**Whaling:**

Targeting executives from the top management in the organization, usually from private companies. The objective is to swindle the executives into revealing confidential information.

Types of Phishing scams:

**Phishing Counter Measures:**

| | |
|---|---|
| • Keep Antivirus up to date | • Use the Microsoft baseline security analyzer. |
| • Do not click on hyperlinks | • Firewall |
| • Take advantage of anti-spam software | • Use backup system images |
| • Verify https (SSL) | • Do not enter sensitive or financial information into pop-up windows |
| • Use anti-Spyware software | • Secure the host file |
| • Get educated | • Protect against DNS pharming attacks |

**SPS Algorithm (Sanitizing Proxy System**)

It is a simple filtering algorithm, the key idea behind the SPS is that web Phishing attack can be immunized by removing the part of the content that encourages the netizens into entering their personal information. The characteristics of SPS in the following points.

1. **Two level filtering:**
   - **Strict URL filtering**
   - **HTTP response sanitizing**
2. **Flexibility of the rule set**
3. **Simplicity of the filtering algorithm**
4. **Accountability of the response sanitizing**
5. **Robustness against both misbehavior of novice user and evasion techniques.**

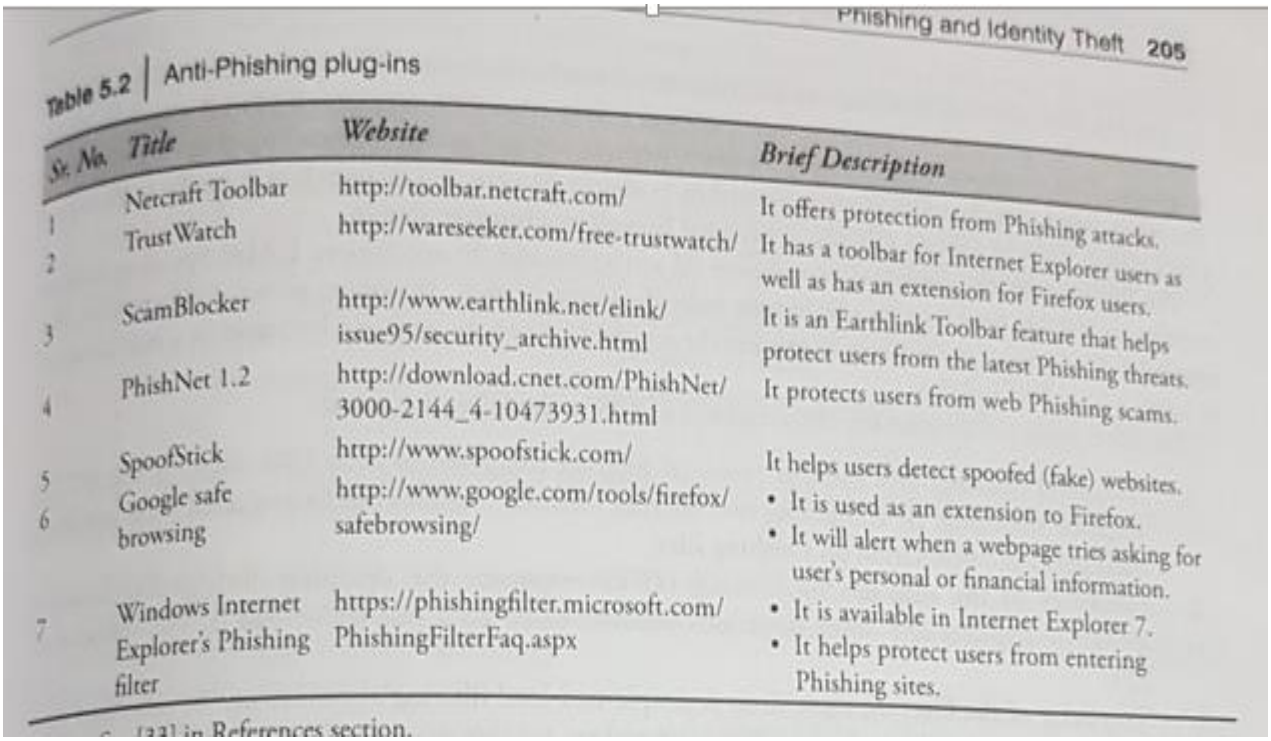



Table 5.2 | Anti-Phishing plug-ins

| Sr. No. | Title | Website | Brief Description |
|---|---|---|---|
| 1 | Netcraft Toolbar | http://toolbar.netcraft.com/ | It offers protection from Phishing attacks. |
| 2 | TrustWatch | http://wareseeker.com/free-trustwatch/ | It has a toolbar for Internet Explorer users as well as has an extension for Firefox users. |
| 3 | ScamBlocker | http://www.earthlink.net/elink/issue95/security_archive.html | It is an Earthlink Toolbar feature that helps protect users from the latest Phishing threats. |
| 4 | PhishNet 1.2 | http://download.cnet.com/PhishNet/3000-2144_4-10473931.html | It protects users from web Phishing scams. |
| 5 | SpoofStick | http://www.spoofstick.com/ | It helps users detect spoofed (fake) websites. |
| 6 | Google safe browsing | http://www.google.com/tools/firefox/safebrowsing/ | • It is used as an extension to Firefox.<br>• It will alert when a webpage tries asking for user's personal or financial information. |
| 7 | Windows Internet Explorer's Phishing filter | https://phishingfilter.microsoft.com/PhishingFilterFaq.aspx | • It is available in Internet Explorer 7.<br>• It helps protect users from entering Phishing sites. |

[33] in References section.

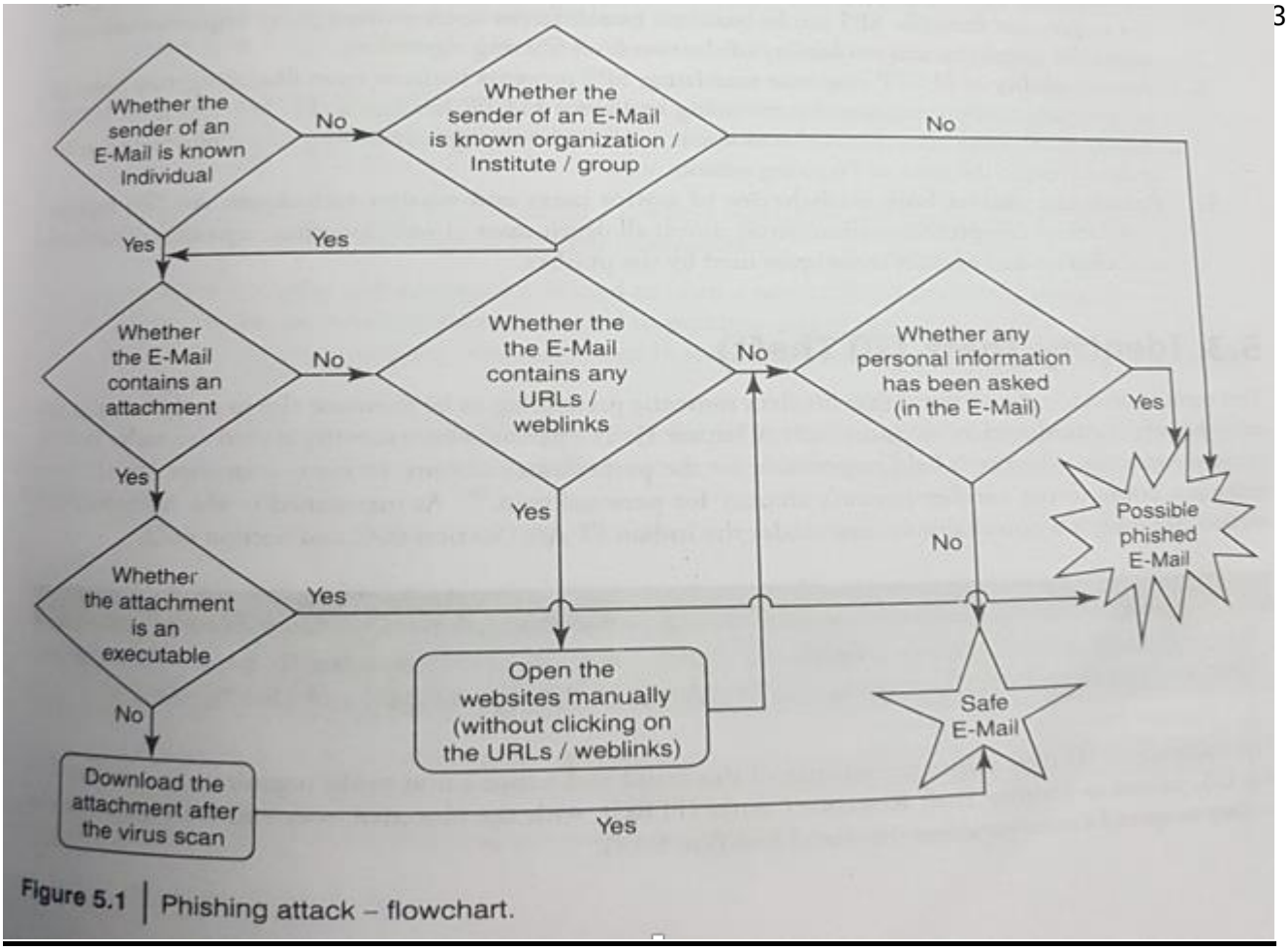


**Figure 5.1** | Phishing attack – flowchart.

## 4. 14. Identity Theft (ID Theft)

- This term is used to refer to fraud that involves someone pretending to be someone else to steal money or get other benefits.
- ID theft is a punishable offense under the Indian IT Act (Section 66C and Section 66D).
- The statistics on ID theft proves the severity of this fraud and hence a non-profit organization was found in the US, named as **Identity Theft Resource Center (ITRC)**, with the objective to extend the support to the society to spread awareness about this fraud.
- Federal Trade Commission (FTC) has provided the statistics about each one of the identity fraud mentioning prime frauds presented below.

**1. Credit card fraud (26%):**

**2. Bank fraud (17%):** Besides credit card fraud, cheque theft and Automatic Teller Machines (ATM) pass code theft have been reported that are possible with ID theft

**3. Employment fraud (12%):** In this fraud, the attacker borrows the victim's valid SSN to obtain a job.

**4. Government fraud (9%):** This type of fraud includes SSN, driver license and income tax fraud.

**5. Loan fraud (5%):** It occurs when the attacker applies for a loan on the victim's name and this can occur even if the SSN does not match the name exactly.

**It is important to note the various usage of ID theft information.**

**1.** 66% of victims' personal information is used **to open a new credit account** in their name.

**2.** 28% of victims' personal information is used **to purchase cell phone service**.

**3.** 12% of victims end up having **warrants issued in their name** for financial crimes committed by the identity thief.

### 5.3.1 Personally Identifiable Information (PII)

The fraudsters attempts to steal the elements mentioned below, which can express the purpose of distinguishing individual identity:

**1.** Full name;

**2.** national identification number (e.g., SSN);
**3.** telephone number and mobile phone number;
**4.** driver's license number;
**5.** credit card numbers;
**6.** digital identity (e.g., E-Mail address, online account ID and password);
**7.** birth date/birth day;
**8.** birthplace;
**9.** face and fingerprints.

The information can be further classified as
(a) non-classified and
(b) classified.

**1. Non-classified information**

- **Public information:**
- **Personal information:**
- **Routine business information:**
- **Private information:**

**2. Classified information**

- **Confidential:** Information that requires protection and unauthorized disclosure could damage national security (e.g., information about strength of armed forces and technical information about weapons).
- **Secret:** Information that requires substantial protection and unauthorized disclosure could seriously damage national security (e.g., national security policy, military plans or intelligence operations).
- **Top secret:** Information that requires the highest degree of protection and unauthorized disclosure could severely damage national security (e.g., vital defense plans and cryptologic intelligence systems).

ID theft fraudsters and/or industrial/international spies target to gain the access to private, confidential, secret and top secret information.

### 5.3.2 Types of Identity Theft

**1.** Financial identity theft;
**2.** Criminal identity theft;
- Computer and cyber crimes
- Organized crime
- Drug trafficking
- Alien smuggling
- Money laundering

**3.** Identity cloning;
**4.** Business identity theft;
**5.** Medical identity theft;
**6.** Synthetic identity theft;
**7.** Child identity theft.

### 5.3.3 Techniques of ID Theft

**1. Human-based methods:**
- *Direct access to information:*
- *Dumpster diving:*
- *Theft of a purse or wallet:*
- *Mail theft and rerouting:*
- *Shoulder surfing:*

- *Dishonest or mistreated employees:*
- *Telemarketing and fake telephone calls:*

**2. Computer-based technique:**

- *Backup theft:*
- *Hacking, unauthorized access to systems and database theft:*
- *Phishing:*
- *Pharming:*
- *Hardware:*

**Business Identity theft – Counter measures**

| | |
|---|---|
| • Secure your business premises with locks and alarms | • Protect the IT systems from hackers |
| • Put your business records under lock and key | • Create the awareness that internet is a dangerous place |
| • Shred | • Avoid broadcasting information |
| • Be cautious on the phone | • Create organizational security policy |
| • Limit access to your IT systems | • Disconnect the access of ex- employees immediately |