# 4 Tools and Methods Used in Cybercrime

## Learning Objectives

After reading this chapter, you will be able to:

- Understand about proxy servers and anonymizers.
- Learn about password cracking.
- Learn what keyloggers and Spywares do.
- Get an overview of virus and worms.
- Learn about Trojan Horses and backdoors.
- Understand what steganography is.
- Learn about DoS and DDoS attacks.
- Learn about SQL injection.
- Understand buffer overflow.
- Get an overview of wireless network hacking.

## 4.1 Introduction

In Chapter 2, we have learnt about how criminals/attackers plan cyberoffenses against an individual and/or against an organization. In Chapter 3, we have learnt how mobile technology plays an important role to launch cyberattacks. With this background, in this chapter, we will focus upon different forms of attacks through which attackers target the computer systems. There are various tools and techniques (see Box 4.1) and complex methodologies used to launch attacks against the target. Although discussing all of them is virtually impossible in a single chapter, yet still, we have provided an insight toward these techniques to enable the reader to understand how the computer is an indispensable tool for almost all cybercrimes. As the Internet and computer networks are integral parts of information systems, attackers have in-depth knowledge about the technology and/or they gain thorough knowledge about it. (See Section 10.4.2, Chapter 10 in CD.)

Network attack incidents reveal that attackers are often very systematic in launching their attacks (see Section 7.13, Chapter 7). The basic stages of an attack are described here to understand how an attacker can compromise a network here:

1. **Initial uncovering:** We have explained this in Chapter 2. Two steps are involved here. In the first step called as *reconnaissance*, the attacker gathers information, as much as possible, about the target by legitimate means – searching the information about the target on the Internet by Googling social networking websites and people finder websites. The information can also be gathered by surfing the public websites/searching news articles/press releases if the target is an organization/institute. In the second step, the attacker uncovers as much information as possible on the company's internal network, such as, Internet domain, machine names and the company's Internet Protocol (IP) address ranges. From prevention perspective, at this stage, it is really not possible to detect the attackers because they have done nothing illegal as yet and so their information requests are considered legitimate.

## Box 4.1 Scareware, Malvertising, Clickjacking and Ransomware

1. **Scareware**: It comprises several classes of scam software with malicious payloads (explained in chapter 1), or of limited or no benefit, which are sold to consumers via certain unethical marketing practices. The selling approach uses social engineering to cause shock, anxiety or the perception of a threat, generally directed at an unsuspecting user. Some forms of Spyware and Adware also use scareware tactics. Some websites display pop-up advertisement windows or banners with text such as: "Your computer may be infected with harmful Spyware programs. Immediate removal may be required. To scan, click 'Yes' below." These websites can go as far as saying that a user's job, career or marriage would be at risk. Webpages displaying such advertisements for such products are often considered as scareware. Serious scareware applications qualify as rogue software.
2. **Malvertising:** It is a malicious advertising – malware + advertising – an online criminal methodology that appears focused on the installation of unwanted or outright malicious software through the use of Internet advertising media networks, exchanges and other user-supplied content publishing services common to the social networking space. Cybercriminals attempt to distribute malware through advertising. Possible vectors of attack include Malicious Code hidden within an advertisement, embedded into a webpage or within software which is available for download.
3. **Clickjacking:** It is a malicious technique of tricking netizens into revealing confidential information and/or taking control of their system while clicking on seemingly innocuous webpages. Clickjacking takes the form of embedded code and/or script which is executed without netizen's knowledge Cybercriminals take the advantage of vulnerability across a variety of browsers and platforms to launch this type of attack, for example clicking on a button that appears to perform another function. The term "clickjacking" was coined by Jeremiah Grossman and Robert Hansen in 2008. The exploit is also known as User-Interface (UI) redressing.
4. **Ransomware:** It is computer malware that holds a computer system, or the data it contains, hostage against its user by demanding a ransom for its restoration. It typically propagates as a conventional computer worm, entering a system through, for example, vulnerability in a network service or an E-Mail attachment. It may then
   - disable an essential system service or lock the display at system start-up and
   - encrypt some of the user's personal files.

   In both cases, the malware may extort by
   - prompting the user to enter a code obtainable only after wiring payment to the attacker or sending an SMS message and accruing a charge;
   - urging the user to buy a decryption or removal tool.

Sources: http://en.wikipedia.org/wiki/Scareware (10 January 10); http://www.anti-malvertising.com/ (10 January 10); http://en.wikipedia.org/wiki/Clickjacking (10 February 10); http://en.wikipedia.org/wiki/Ransomware_(malware) (10 January 10).

2. **Network probe:** At the network probe stage, the attacker uses more invasive techniques to scan the information. Usually, a "ping sweep" of the network IP addresses is performed to seek out potential targets, and then a "port scanning" tool (see Table 2.2) 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):** Now the attacker is toward committing what is technically a "computer crime." He/she does this by exploiting possible holes on the target system. The attacker usually goes through several stages of exploits to gain access to the system. Certain programming errors can be used by attackers to compromise a system and are quite common in practice (see Table 4.1 for list of websites commonly browsed by attackers to obtain the information on the vulnerabilities). Exploits usually include vulnerabilities in common gateway interface (CGI) scripts or well-known buffer-overflow holes, but the easiest way to gain an entry is by checking for default login accounts with easily guessable (or empty) passwords. Once the attackers are able to access a user account without many privileges, they will attempt further exploits to get an administrator or "root" access. Root access is a Unix term

**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. |

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 a foothold in the internal network quickly and easily, by compromising low-priority 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 (*Trojan Horse* is further discussed in detail in this chapter) and services that have a backdoor password. There are a number of "hacking tools" which can clean up log files and remove any trace of an intrusion; most of the time, they are individual programs written by hackers. Such tools provide copies of system files that look and act like real thing, but in fact they provide the attacker a backdoor entry into the system and hide processes he/she might be running on that system and his/her user information. This allows the attacker to return to the system at will, which means that the attacker has "captured" the network. Once the attacker has gained access to one system, he/she will then repeat the process by using the system as a stepping stone to access other systems deeper within the network, as most networks have fewer defenses against attacks from internal sources.
5. **Grab the data:** Now that the attacker has "captured the network," he/she takes advantage of his/her position to steal confidential data, customer credit card information, deface webpages, alter processes and even launch attacks at other sites from your network, causing a potentially expensive and embarrassing situation for an individual and/or for an organization.
6. **Covering tracks:** This is the last step in any cyberattack, 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 or use this phase either to start a fresh reconnaissance to a related target system or continued use of resources, removing evidence of hacking, avoiding legal action, etc. (See Table 4.2 to know tools used to cover tracks.)

During this entire process, the attacker takes optimum care to hide his/her identity (ID) from the first step itself. How is it possible is described in the next section.

**Table 4.2** | Tools used to cover tracks

| Sr. No. | Website | Brief Description |
|---|---|---|
| 1 | http://www.ibt.ku.dk/jesper/ELSave/ | **ELSave:** It is a tool to save and/or clear an NT event log. ELSave is written by Jesper Lauritsen. The executable is available on the weblink, but source code is not available. |
| 2 | http://ntsecurity.nu/toolbox/winzapper/ | **WinZapper:** This tool enables to erase event records selectively from the security log in Windows NT 4.0 and Windows 2000. This program corrupts the event logs, therefore, they must be cleared completely. |
| 3 | http://www.evidence-eliminator.com/ | **Evidence eliminator:** It is simple and one of the top-quality professional PC cleaning program that is capable of defeating all known investigative Forensic Software. Evidence eliminator permanently wipes out evidence so that forensic analysis becomes impossible. |
| 4 | http://www.traceless.com/computer-forensics/ | **Traceless:** It is a privacy cleaner for Internet explorer (IE) that can delete common Internet tracks, including history, cache, typed URLs, cookies, etc. |

(*Continued*)

**Table 4.2** | *(Continued)*

| | | |
|---|---|---|
| 5 | http://www.acesoft.net/ | **Tracks Eraser Pro:** It deletes following history data:<br>• Delete address bar history of IE, Netscape, AOL, Opera.<br>• Delete cookies of IE, Netscape, AOL, Opera.<br>• Delete Internet cache (temporary Internet files).<br>• Delete Internet history files.<br>• Delete Internet search history.<br>• Delete history of autocomplete.<br>• Delete IE plugins (selectable).<br>• Delete index.dat file.<br>• Delete history of start menu run box.<br>• Delete history of start menu search box.<br>• Delete windows temp files.<br>• Delete history of open/save dialog box.<br>• Empty recycle bin. |

## 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, connection or other resource) 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 (visit http://www.multiproxy.org/multiproxy.htm for more information).

One of the advantages of a proxy server is that its cache memory can serve all users. If one or more websites are requested frequently, may be by different users, it is likely to be in the proxy's cache memory, which will improve user response time. In fact there are special servers available known as *cache servers*. A proxy can also do logging.

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

1. http://www.proxy4free.com
2. http://www.publicproxyservers.com

3. http://www.proxz.com
4. http://www.anonymitychecker.com
5. http://www.surf24h.com
6. http://www.hidemyass.com

*An anonymizer* or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. t accesses the Internet on the user's behalf, protecting personal information by hiding the source computer's dentifying information.[1] Anonymizers are services used to make Web surfing anonymous by utilizing a vebsite that acts as a proxy server for the web client. In 1997 the first anonymizer software tool was created by Lance Cottrell, developed by Anonymizer.com. The anonymizer hides/removes all the identifying information from a user's computer while the user surfs on the Internet, which ensures the privacy of the user. (See Section 9.7, Chapter 9.)

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

1. http://www.anonymizer.com
2. http://www.browzar.com
3. http://www.anonymize.net
4. http://www.anonymouse.ws
5. http://www.anonymousindex.com

## Box 4.2 Being Anonymous While Searching on Google!

### Google Cookie

Google was the first search engine to use a cookie.[2] Google set the standard and nowadays cookies are commonplace among search engines. This cookie places a unique ID number on your hard disk. Anytime you visit Google, user gets a Google cookie if a user doesn't already have one. If a user has one then it will read and record the unique ID number. Google can build a detailed list of your search terms over many years. (Google's cookies are set to expire by the year 2038, unless a user deletes before its expiry.)

### Cookie

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

1. Persistent cookie and
2. session cookie.

Persistent cookie is stored by the web browser into the cookie folder on the PC's hard disk. It remains under the cookie folder, which is maintained by the web browser. Session cookie is a temporary cookie and does not reside on the PC once the browser is closed (see Boxes 9.2, 9.3 and 9.4, Chapter 9).

### DoubleClick

It is a subsidiary of Google and provides Internet ad-serving services and paid search products listing (*DART Search*[3]) and utilize the cookies, which are called DART cookie. Internet Advertising Network was started by Kevin O'Connor and Dwight Merriman in 1995. IAN and the DoubleClick division of Poppe-Tyson were merged into a new corporation named DoubleClick in 1996. DoubleClick was first in the online media representative business, that is, representing websites to sell advertising space to marketers. In 1997 it began offering the online ad serving and management technology they had

**Box 4.2 Being Anonymous . . . (*Continued*)**

developed to other publishers as the DART services. The DART cookie is a persistent cookie, which consists of the name of the domain that has set the cookie, the lifetime of the cookie and a "value." DoubleClick's DART mechanism generates a unique series of characters for the "value" portion of the cookie. These DoubleClick DART cookies help marketers learn how well their Internet advertising campaigns or paid search listings perform. Many marketers and Internet websites use DoubleClick's DART technology to deliver and serve their advertisements or manage their paid search listings. DoubleClick's DART products set or recognize a unique, persistent cookie when an ad is displayed or a paid listing is selected. The information that the DART cookie helps to give marketers includes the number of unique users their advertisements displayed to, how many users clicked on their Internet ads or paid listings and which ads or paid listings they clicked on.

**G-Zapper**

G-Zapper[4] utility helps to stay anonymous while searching Google. Google stores a unique identifier in a cookie on the computer (i.e., on the hard disk) which allows to track keywords that are searched for. This information is used to compile reports, track user habits and test features. In the future, it would be possible that this information is sold and/or shared with others.

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

This utility can be downloaded from http://www.dummysoftware.com/gzapper.html

## 4.3 Phishing

While checking electronic mail (E-Mail) one day a user finds a message from the bank threatening him/her 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. Most people associate Phishing with E-Mail messages that spoof or mimic banks, credit card companies or other business such as Amazon and eBay. 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[5]:

1. **Planning:** Criminals, usually called as phishers, decide the target (i.e., specific business/business house/an individual) and determine how to get E-Mail address of that target or customers of that business. Phishers often use mass mailing and address collection techniques as spammers.
2. **Setup:** Once phishers know which business/business house to spoof and who their victims are, they will create methods for delivering the message and to collect the data about the target. Most often this involves E-Mail addresses and a webpage.

3. **Attack:** This is the step people are most familiar with – 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.

Phishing started off as being part of popular hacking culture. 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. We have explained Phishing and Identity Theft in detail in Chapter 5.

## 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.[6] 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 (explained in Chapter 5). Examples of guessable passwords include:

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

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*.

Even though these functions create hashed passwords, which may be cryptographically secure, an attacker attempts to get possession of the hashed password, which will help to provide a quick way to test guesses for the password by applying the one-way function to each guess and comparing the result to the verification data. 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.

**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*)

**Table 4.3** | *(Continued)*

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

Password cracking 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 are explained in Chapter 2).

### 4.4.1 Online Attacks

An attacker can create a script file (i.e., automated program) that will be executed to try each password in a list and when matches, an attacker can gain the access to the system. The most popular online attack is man-in-the middle (MITM) attack, also termed as "bucket-brigade attack" or sometimes "Janus attack." It is a form of active eavesdropping[7] 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

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 |

access to the computer and copying the password file from the system onto removable media. Different types of offline password attacks are described in Table 4.4. Few tools listed in Table 4.2 also use these techniques to get the password in the clear text format.

### 4.4.3 Strong, Weak and Random Passwords

A weak password is one, which could be easily guessed, short, common and a system default password that could be easily found by executing a brute force attack and by using a subset of all possible passwords, such as words in the dictionary, proper names and words based on the username or common variations on these themes. Passwords that can be easily guessed by acquaintances of the netizens (such as date of birth, pet's name and spouses' name) are considered to be very weak. Here are some of the examples of "weak passwords":

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

A strong password is long enough, random or otherwise difficult to guess – producible only by the user who chooses it. The length of time deemed to be too long will vary with the attacker, the attacker's resources, the ease with which a password can be tried and the value of the password to the attacker. A student's password might not be worth more than a few seconds of computer time, while a password controlling access to a large bank's electronic money transfer system might be worth many weeks of computer time for trying to crack it. Here are some examples of strong passwords:

1. **Convert_£100 to Euros!:** Such phrases are long, memorable and contain an extended symbol to increase the strength of the password.
2. **382465304H:** It is mix of numbers and a letter at the end, usually used on mass user accounts and such passwords can be generated randomly, for example, in schools and business.
3. **4pRte!ai@3:** It is not a dictionary word; however it has cases of alpha along with numeric and punctuation characters.

4. **MoOoOfIn245679:** It is long with both alphabets and numerals.
5. **t3wahSetyeT4:** It is not a dictionary word; however, it has both alphabets and numerals.

Visit http://www.microsoft.com/protect/fraud/passwords/checker.aspx to check the strength of your password.[8]

### 4.4.4 Random Passwords

We have explained in the previous section how most secure passwords are long with random strings of characters and how such passwords are generally most difficult to remember. Password is stronger if it includes a mix of upper and lower case letters, numbers and other symbols, when allowed, for the same number of characters. The difficulty in remembering such a password increases the chance that the user will write down the password, which makes it more vulnerable to a different attack (in this case, the paper being lost or stolen and the password discovered). Whether this represents a net reduction in security depends on whether the primary threat to security is internal (e.g., social engineering) or external. A password can, at first sight, be random, but if you really examine it, it is just a pattern. One of these types of passwords is 26845. Although short, it is not easily guessed. However, the person who created the password is able to remember it because it is just the four direction keys on the square number board (found at the right of most keyboards) plus a five in the middle. If you practice it, it is just one swift motion of moving two fingers around the board (which is very easy to use). Forcing users to use system-created random passwords ensures that the password will have no connection with that user and should not be found in any dictionary. Several OSs have included such a feature. Almost all the OSs also include password aging; the users are required to choose new passwords regularly, usually after 30 or 45 days. Many users dislike these measures, particularly when they have not been taken through security awareness training. The imposition of strong random passwords may encourage the users to write down passwords, store them in personal digital assistants (PDAs) or cell phones and share them with others against memory failure, increasing the risk of disclosure.

The general guidelines applicable to the password policies, which can be implemented organization-wide, are as follows:

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

Similarly, netizens should practice password guidelines to avoid being victim of getting their personal E-Mail accounts hacked/attacked by the attackers.

1. Passwords used for business E-Mail accounts, personal E-Mail accounts (Yahoo/Hotmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading accounts) should be kept separate.
2. Passwords should be of minimum eight alphanumeric characters (common names or phrases should be phrased).
3. Passwords should be changed every 30/45 days.
4. Passwords should not be shared with relatives and/or friends.
5. Password used previously should not be used while renewing the password.
6. Passwords of personal E-Mail accounts (Yahoo/Hotmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading accounts) should be changed from a secured system, within couple of days, if these E-Mail accounts has been accessed from public Internet facilities such as cybercafes/hotels/libraries.
7. Passwords should not be stored under mobile phones/PDAs, as these devices are also prone to cyber-attacks (explained in Section 3.8, Chapter 3).
8. In the case of receipt of an E-Mail from banking/financial institutions, instructing to change the passwords, before clicking the weblinks displayed in the E-Mail, legitimacy of the E-Mail should be ensured to avoid being a victim of Phishing attacks (we will explain Phishing attack in detail in Chapter 5).
9. Similarly, in case of receipt of SMS from banking/financial institutions, instructing to change the passwords, legitimacy of the E-Mail should be ensured to avoid being a victim of Smishing attacks (explained in detail in Chapter 3).
10. 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.[9]

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 (see Table 4.5) 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 (will discuss more on this in subsequent sections of this chapter) without the knowledge of the user. Cybercriminals always install such tools on the insecure computer systems available in public places (i.e., cybercafes, library – we have already discussed this in Chapter 2) 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.[10]

**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)*

Table 4.5 | (Continued)

| Website | Brief Description |
|---|---|
| http://www.elite-keylogger.com | **Elite Keylogger:** It captures every keystroke typed, all passwords (including Windows logon passwords), chats, instant messages, E-Mails, websites visited, all program launched, usernames and time they worked on the computer, desktop activity, clipboard, etc. |
| http://www.cyberspysoftware.com | **CyberSpy:** It provides an array of features and easy-to-use graphical interface along with computer monitoring capabilities such as keep tabs on the employees and keeps track of what children are viewing on the Internet. CyberSpy can be used as complete PC monitoring solution for any home or office. CyberSpy records all websites visited, instant message conversations, passwords, E-Mails and all keystrokes pressed. It also has the ability to provide screenshots at set intervals. |
| http://www.mykeylogger.com | **Powered Keylogger:** Powered keylogger can be used for the following:<br>• *Surveillance:* It is for anyone to control what happens on the computer when the computer's owner is away.<br>• *Network administration:* It is for network administrators to control outgoing traffic and sites visited.<br>• *Shared PC activity tracking:* It is to analyze the usage of shared PC.<br>• *Parental control:* It helps parents to monitor their children's computer and Internet activity.<br>• *Employee productivity monitoring:* It helps managers to check and increase productivity of their stuff or just to prevent the leak of important information. |
| http://www.x-pcsoft.com | **XPC Spy:** XPC Spy is one of the powerful keylogger spy software, runs stealthy under MS Windows and has the following features:<br>• Records all keystrokes typed;<br>• records all websites visited;<br>• records all programs executed, folders explored, files opened or edited, documents printed, etc.;<br>• records all windows opened;<br>• records all clipboard text content;<br>• records all system activities;<br>• records webmails sent (database update online, more and more webmail servers are supported);<br>• records all ICQ Messenger chat conversations;<br>• records all MSN Messenger chat conversations;<br>• records all AOL/AIM Messenger chat conversations;<br>• records all Yahoo! Messenger chat conversations;<br>• runs invisible in the background and is protected by password;<br>• is built-in screenshot pictures viewer;<br>• schedules monitor process, sets time to start or stop monitoring;<br>• sends logs report via E-Mail. |

### 4.5.2 Hardware Keyloggers

To install these keyloggers, physical access to the computer system is required. 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:

1. http://www.keyghost.com
2. http://www.keelog.com
3. http://www.keydevil.com
4. http://www.keykatcher.com

### 4.5.3 Antikeylogger

Antikeylogger[11] 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 antikeylogger are as follows:

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

### 4.5.4 Spywares

Spyware is a type of malware (i.e., malicious software – see Box 4.3 to know about different types of malwares) 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.[12]

It is clearly understood from the term *Spyware* that it secretly monitors the user. The features and functions of such Spywares are beyond simple monitoring. Spyware programs collect personal information about the victim, such as the Internet surfing habits/patterns and websites visited. The Spyware can also redirect Internet surfing activities by installing another stealth utility on the users' computer system. Spyware may also have an ability to change computer settings, which may result in slowing of the Internet connection speeds and slowing of response time that may result into user complaining about the Internet speed connection with Internet Service Provider (ISP). Various Spywares are available in the market and the one that are popular are listed in Table 4.6.

To overcome the emergence of Spywares that proved to be troublesome for the normal user, anti-Spyware softwares (refer to Appendix B: List of Useful Software Utilities and Websites in CD) are available in the market. Installation of anti-Spyware software has become a common element nowadays from computer security practices perspective.

## Box 4.3 Malwares

Malware, short for malicious software, is a software designed to infiltrate a computer system without the owner's informed consent (see Box 9.8, Chapter 9). 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.[13] 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 (will discuss more on this in Section 4.6).
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 (will discuss more on this in Section 4.7).
3. **Rootkits:** Rootkits[15] is a software system that consists of one or more programs designed to obscure the fact that a system has been compromised. For further details refer to Section 7.12.1, Chapter 7.
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:** For further details see Section 4.5.
6. **Botnets:** For further details see Section 2.6 in Chapter 2.
7. **Keystroke loggers:** For further details see Section 4.5.

**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-I 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. |