Chapter 12

Security Aspects

12130CH12

"Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months."

— *Clifford Stoll*

In this Chapter

- *Threats and Prevention*
- *Malware*
- *Antivirus*
- *Spam*
- *HTTP vs HTTPS*
- *Firewall*
- *Cookies*
- *Hackers and Crackers*
- *Network Security Threats*

12.1 Threats and Prevention

Being alone is the most ideal situation for an individual in terms of security. It applies to computers as well. A computer with no link to an external device or computer is free from the security threats arising otherwise. However, it is not an ideal solution for a human being or a computer to stay aloof in order to mitigate any security threats, as the world at present is on its way to become fully connected. This connectedness of various devices and computers has brought into our focus the various network threats and its prevention.

Network security is concerned with protection of our device as well as data from illegitimate access or misuse. Threats include all the ways in which one can exploit any vulnerability or weakness in a network or communication system in order to cause harm or damage one's reputation.

12.2 MALWARE

Malware is a short term used for MALicious softWARE. It is any software developed with an intention to damage hardware devices, steal data, or cause any other trouble to the user. Various types of malware have been created from time-to-time, and large-scale damages have been inflicted. Many of these malware programs have been identified and counter measures have been initiated. However, different types of malware keep on coming on a regular basis that compromise the security of computer systems and cause intangible damages. Besides, each year, malware incur financial damages worth billions of dollars worldwide. Viruses, Worms, Ransomware, Trojans, and Spyware are some of the kinds of malware.

12.2.1 Virus

The term computer virus was coined by Fred Cohen in 1985 and has been borrowed from biological science with almost similar meaning and behavior, the only difference is that the victim is a computer system and the virus is a malicious software. A virus is a piece of software code created to perform malicious activities and hamper resources of a computer system like CPU time, memory, personal files, or sensitive information.

Mimicking the behaviour of a biological virus, the computer virus spreads on contact with another system, i.e. a computer virus infects other computer systems that it comes into contact with by copying or inserting its code into the computer programs or software (executable files). A virus remains dormant on a system and is activated as soon as the infected file is opened (executed) by a user.

Viruses behave differently, depending upon the reason or motivation behind their creation. Some of the most common intentions or motives behind viruses include stealing passwords or data, corrupting files, spamming the user's email contacts, and even taking control of the user's machine. Some well-known viruses include CryptoLocker, ILOVEYOU, MyDoom, Sasser and Netsky, Slammer, Stuxnet, etc.

12.2.2 Worms

The Worm is also a malware that incurs unexpected or damaging behaviour on an infected computer system. The major difference between a worm and a virus is that

unlike a virus, a worm does not need a host program or software to insert its code into. Worms are standalone programs that are capable of working on its own. Also, a virus needs human triggering for replication (i.e. when a user opens/executes the infected file), while a worm replicates on its own and can spread to other computers through the network. Some prominent examples of worms include Storm Worm, Sobig, MSBlast, Code Red, Nimda, Morris Worm, etc.

12.2.3 Ransomware

It is a type of malware that targets user data. It either blocks the user from accessing their own data or threatens to publish the personal data online and demands ransom payment against the same. Some ransomware simply block the access to the data while others encrypt data making it very difficult to access. In May 2017, a ransomware WannaCry infected almost 200,000 computers across 150 countries. It worked by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. It literally made its victims "cry" and hence the name.

Figure 12.1: A ransomware

12.2.4 Trojan

Since the ancient Greeks could not infiltrate the city of Troy using traditional warfare methods, they gifted the king of Troy with a big wooden horse with hidden soldiers inside and eventually defeated them. Borrowing

the concept, a Trojan is a malware, that looks like a legitimate software and once it tricks a user into installing it, it acts pretty much like a virus or worm. However, a Trojan does not self-replicate or infect other files, it spreads through user interaction such as opening an email attachment or downloading and executing a file from the Internet. Some Trojans create backdoors to give malicious users access to the system.

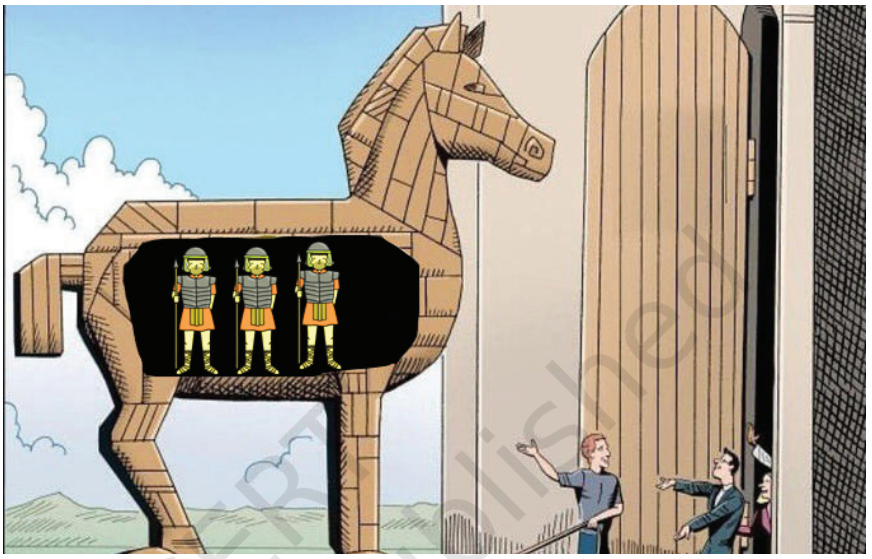

Figure 12.2: A trojan horse

12.2.5 Spyware

It is a type of malware that spies on a person or an organisation by gathering information about them, without the knowledge of the user. It records and sends the collected information to an external entity without consent or knowledge of the user.

Spyware usually tracks internet usage data and sells them to advertisers. They can also be used to track and capture credit card or bank account information, login and password information or user's personal identity.

12.2.6 Adware

An Adware is a malware that is created to generate revenue for its developer. An adware displays online advertisements using pop-ups, web pages, or installation screens. Once an adware has infected a substantial number of computer systems, it generates revenue either by displaying advertisements or using "pay per click" mechanism to charge its clients against the number of clicks on their displayed ads. Adware

is usually annoying, but harmless. However, it often paves way for other malware by displaying unsafe links as advertisements.

To implement a keylogger in hardware, a thin transparent keyboard is placed atop the actual keyboard or input pad of the intended machine, which then records the keystrokes pressed by the user.

12.2.7 Keyloggers

A keylogger can either be malware or hardware. The main purpose of this malware is to record the keys pressed by a user on the keyboard. A keylogger makes logs of daily keyboard usage and may send it to an external entity as well. In this way, very sensitive and personal information like passwords, emails, private conversations, etc. can be revealed to an external entity without the knowledge of the user. One strategy to avoid the threat of password leaks by keyloggers is to use a virtual keyboard while signing into your online accounts from an unknown computer.

(A) Online Virtual Keyboard Vs On-Screen Keyboard

The names "on-screen" and "virtual" keyboard refer to any software-based keyboard and are sometimes used interchangeably. But, there exists a notable difference between "on-screen" and "online virtual" keyboards. Both types of keyboards may look the same, but the difference is in terms of the layout or ordering of the keys. The on-screen keyboard of an operating system uses a fixed QWERTY key layout (Figure 12.3), which can be exploited by sophisticated keylogger software. However, an online virtual keyboard randomises the key layout every time it is used (Figure 12.4), thereby making it very difficult for a keylogger software to know or record the key(s) pressed by the user.

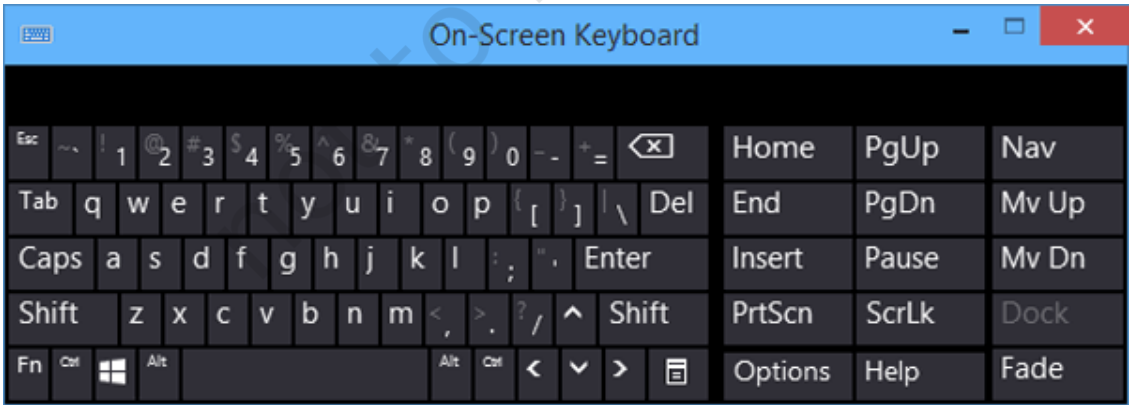

Figure 12.3: A QWERTY *keyboard layout*

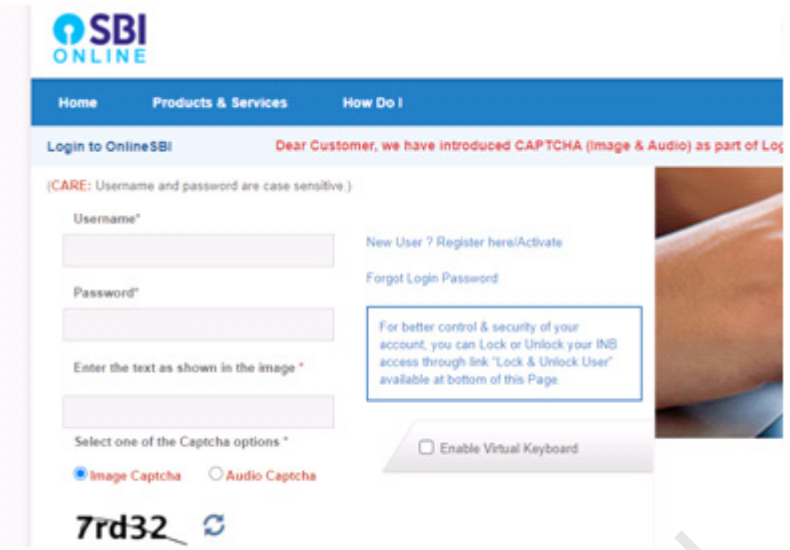

Figure 12.4: Online virtual keyboard

12.2.8 Modes of Malware distribution

A malware once designed, can take many routes to reach your computer. Some of the common distribution channels for malware are:

- **Downloaded from the Internet:** Most of the time, malware is unintentionally downloaded into the hard drive of a computer by the user. Of course, the malware designers are smart enough to disguise their malware, but we should be very careful while downloading files from the Internet (especially those highlighted as free stuff).
- **Spam Email:** We often receive an unsolicited email with embedded hyperlinks or attachment files. These links or attached files can be malware.
- **Removable Storage Devices:** Often, the replicating malware targets the removable storage media like pen drives, SSD cards, music players, mobile phones, etc. and infect them with malware that gets transferred to other systems that they are plugged into.
- **Network Propagation:** Some malware like Worms have the ability to propagate from one computer to another through a network connection.

12.2.9 Combating Malware

Common signs of some malware infection include the following:

- frequent pop-up windows prompting you to visit some website and/or download some software;
- changes to the default homepage of your web browser;
- mass emails being sent from your email account;
- unusually slow computer with frequent crashes;
- unknown programs startup as you turn on your computer;
- programs opening and closing automatically;
- sudden lack of storage space, random messages, sounds, or music start to appear;
- programs or files appear or disappear without your knowledge.

Malware exists and continues to evolve, and so is the mechanism to combat them. As the saying goes that prevention is better than cure, we list some preventive measures against the malware discussed earlier.

- ✓ Using antivirus, anti-malware, and other related software and updating them on a regular basis.
- ✓ Configure your browser security settings
- ✓ Always check for a lock button in the address bar while making payments.
- ✓ Never use pirated on unlicensed software. Instead go for Free and Open Source Software (FOSS).
- ✓ Applying software updates and patches released by its manufacturers.
- ✓ Taking a regular backup of important data.
- ✓ Enforcing firewall protection in the network.
- ✓ Avoid entering sensitive (passwords, pins) or personal information on unknown or public computers.
- ✓ Avoid entering sensitive data on an unknown network (like Wi-Fi in a public place) using your own computer also.
- ✓ Avoid clicking on links or downloading attachments from unsolicited emails.
- ✓ Scan any removable storage device with an antivirus software before transferring data to and from it.
- ✓ Never share your online account or banking password/pins with anyone.
- ✓ Remove all the programs that you don't recognise from your system.

- ✓ Do not install an anti-spyware or antivirus program presented to you in a pop-up or ad.
- ✓ Use the pop-up window's 'X' icon located on the top-right of the popup to close the ad instead of clicking on the 'close' button in the pop-up. If you notice an installation has been started, cancel immediately to avoid further damage.

12.3 Antivirus

Antivirus is a software, also known as anti-malware. Initially, antivirus software was developed to detect and remove viruses only and hence the name anti-virus. However, with time it has evolved and now comes bundled with the prevention, detection, and removal of a wide range of malware.

12.3.1 Methods of Malware Identification used by Antivirus

(A) Signature-based detection

In this method, an antivirus works with the help of a signature database known as "Virus Definition File (VDF)". This file consists of virus signatures and is updated continuously on a real-time basis. This makes the regular update of the antivirus software a must. If there is an antivirus software with an outdated VDF, it is as good as having no antivirus software installed, as the new malware will infect the system without getting detected. This method also fails to detect malware that has an ability to change its signature (polymorphic) and the malware that has some portion of its code encrypted.

Virus Signature
A virus signature is a consecutive sequence of bytes that is commonly found in a certain malware sample. That means it's contained within the malware or the infected file and not in unaffected files.

(B) Sandbox detection

In this method, a new application or file is executed in a virtual environment (sandbox) and its behavioural fingerprint is observed for a possible malware. Depending on its behaviour, the antivirus engine determines if it is a potential threat or not and proceeds accordingly. Although this method is a little slow, it is very safe as the new unknown application is not given access to actual resources of the system.

(C) Data mining techniques

This method employs various data mining and machine learning techniques to classify the behaviour of a file as either benign or malicious.

(D) Heuristics

Often, a malware infection follows a certain pattern. Here, the source code of a suspected program is compared to viruses that are already known and are in the heuristic database. If the majority of the source code matches with any code in the heuristic database, the code is flagged as a possible threat.

(E) Real-time protection

Some malware remains dormant or gets activated after some time. Such malware needs to be checked on a real-time basis. In this technique, the anti-malware software keeps running in the background and observes the behavior of an application or file for any suspicious activity while it is being executed i.e. when it resides in the active (main) memory of the computer system.

12.4 Spam

Spam is a broad term and applies to various digital platforms like messaging, forums, chatting, emailing, advertisement, etc. However, the widely recognised form is email spam. Depending on their requirements, organisations or individuals buy or create a mailing list (list of email addresses) and repeatedly send advertisement links and invitation emails to a large number of users. This creates unnecessary junk in the inbox of the receiver's email and often tricks a user into buying something or downloading a paid software or malware.

Nowadays, email services like Gmail, Hotmail, etc. have an automatic spam detection algorithm that filters emails and makes things easier for the end users. A user can also mark an undetected unsolicited email as "spam", thereby ensuring that such type of email is not delivered into the inbox as normal email in future.

12.5 HTTP vs HTTPS

Both the HTTP (Hyper Text Transfer Protocol) and its variant HTTPS (Hyper Text Transfer Protocol Secure) are a set of rules (protocol) that govern how data can be transmitted over the WWW (World Wide Web). In other words, they provide rules for the client web browser and servers to communicate.

HTTP sends information over the network as it is. It does not scramble the data to be transmitted, leaving

Always look for the "https://" at the beginning of the address (URL) of the websites while entering your banking, personal, or other sensitive information.

it vulnerable to attacks from hackers. Hence, HTTP is sufficient for websites with public information sharing like news portals, blogs, etc. However, when it comes to dealing with personal information, banking credentials and passwords, we need to communicate data more securely over the network using HTTPS. HTTPS encrypts the data before transmission. At the receiver end, it decrypts to recover the original data. The HTTPS based websites require SSL Digital Certificate.

Activity 12.1

Ask your teacher to show you how to enable and disable firewall on your computer.

12.6 Firewall

Computer firewall is a network security system designed to protect a trusted private network from unauthorised access or traffic originating from an untrusted outside network (e.g., the Internet or different sections of the same network) to which it is connected (Figure 12.5). Firewall can be implemented in software, hardware or both. As discussed earlier, a malware like worm has the capability to move across the networks and infect other computers. The firewall acts as the first barrier against malware.

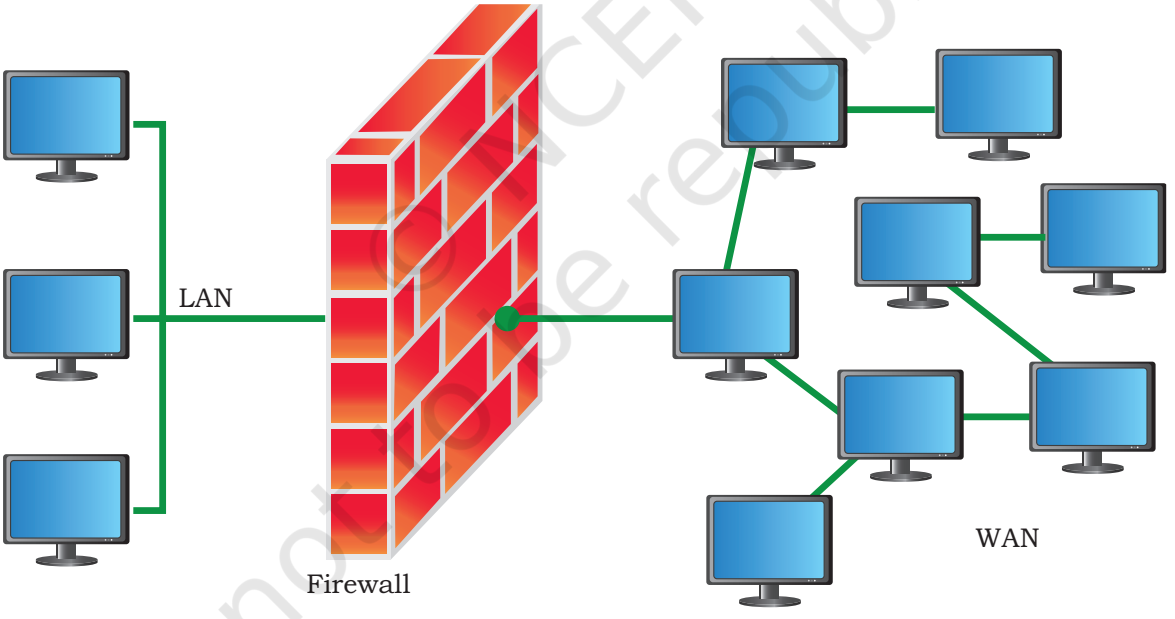

Figure 12.5: A firewall between two networks

A firewall acts as a network filter and based on the predefined security rules, it continuously monitors and controls the incoming and outgoing traffic. As an example, a rule can be set in the firewall of a school LAN, that a student cannot access data from the finance

server, while the school accountant can access the finance server.

12.6.1 Types of Firewall

- Network Firewall: If the firewall is placed between two or more networks and monitors the network traffic between different networks, it is termed as Network Firewall.
- Host-based Firewall: If the firewall is placed on a computer and monitors the network traffic to and from that computer, it is called a host-based firewall.

12.7 Cookies

The term "cookie" was derived from the term "magic cookie" used by Unix programmers to indicate a packet of data that a program receives and sends it back unchanged. A computer cookie is a small file or data packet, which is stored by a website on the client's computer. A cookie is edited only by the website that created it, the client's computer acts as a host to store the cookie. Cookies are used by the websites to store browsing information of the user. For example, while going through an e-commerce website, when a user adds items to cart, the website usually uses cookies to record the items in the cart. A cookie can also be used to store other user-centric information like login credentials, language preference, search queries, recently viewed web pages, music choice, favorite cuisine, etc., that helps in enhancing the user experience and making browsing time more productive.

Depending upon their task, there are different types of cookies. Session cookies keep track of the current session and even terminate the session when there is a time-out (banking website). So, if you accidentally left your e-banking page open, it will automatically close after the time-out. Similarly, authentication cookies are used by a website to check if the user is previously logged in (authenticated) or not. This way, you don't need to login again and again while visiting different web pages or links of the same website. You might have also noticed that certain information like your Name, Address, Contact, D.O.B, etc. automatically fills up while filling an online form. This auto-fill feature is also implemented by websites using cookies.

Think and Reflect

Assume students in a class are to finish their project. For this, the access to the Internet has also been given. To ensure maximum output i.e timely completion, can you utilise Firewall to prevent distraction while surfing the net?

Activity 12.2

Open your internet browser and check the settings for cookies. Also, try to locate some cookie files on your computer system.

12.7.1 Threats due to Cookies

Usually, cookies are used for enhancing the user's browsing experience and do not infect your computer with malware. However, some malware might disguise as cookies e.g. "supercookies". There is another type of cookie known as "Zombie cookie" that gets recreated after being deleted. Some third-party cookies might share user data without the consent of the user for advertising or tracking purposes. As a common example, if you search for a particular item using your search engine, a third-party cookie will display advertisements showing similar items on other websites that you visit later. So, one should be careful while granting permission to any websites to create and store cookies on the user computer.

12.8 Hackers and Crackers

Hackers and crackers are people having a thorough knowledge of the computer systems, system software (operating system), computer networks, and programming. They use this knowledge to find loopholes and vulnerabilities in computer systems or computer networks and gain access to unauthorised information. In simple terms, a hacker is a person that is skilled enough to hack or take control of a computer system. Depending on the intent, there are different types of hackers.

A hacktivist is a hacker with an aim to bring about political and social change.

12.8.1 White Hats: Ethical Hacker

If a hacker uses its knowledge to find and help in fixing the security flaws in the system, its termed as White Hat hacker. These are the hackers with good intentions. They are actually security experts. Organisations hire ethical or white hat hackers to check and fix their systems for potential security threats and loopholes. Technically, white hats work against black hats.

12.8.2 Black Hats: Crackers

If hackers use their knowledge unethically to break the law and disrupt security by exploiting the flaws and loopholes in a system, then they are called black hat hackers.

12.8.3 Grey Hats

The distinction between different hackers is not always clear. There exists a grey area in between, which

represents the class of hackers that are neutral, they hack systems by exploiting its vulnerabilities, but they don't do so for monetary or political gains. The grey hats take system security as a challenge and just hack systems for the fun of it.

12.9 Network Security Threats

12.9.1 Denial of Service

Denial of Service (DoS) is a scenario, wherein an attacker (Hacker) limits or stops an authorised user to access a service, device, or any such resource by overloading that resource with illegitimate requests. The DoS attack floods the victim resource with traffic, making the resource appear busy. If attackers carry out a DoS attack on a website, they will flood it with a very large number of network packets by using different IP addresses. This way, the web server would be overloaded and will not be able to provide service to a legitimate user. The users will think that the website is not working, causing damage to the victim's organisation. Same way, DoS attacks can be done on resources like email servers, network storage, disrupting connection between two machines or disrupting the state of information (resetting of sessions).

If a DoS attack makes a server crash, the server or resource can be restarted to recover from the attack. However, a flooding attack is difficult to recover from, as there can be some genuine legitimate requests in it as well.

A variant of DoS, known as Distributed Denial of Service (DDoS) is an attack, where the flooded requests come from compromised computer (Zombies) systems distributed across the globe or over a very large area. The attacker installs a malicious software known as Bot on the Zombie machines, which gives it control over these machines. Depending upon the requirement and availability, the attacker activates a network of these Zombie computers known as Bot-Net to carry out the DDoS attack. While as a simple DoS attack may be countered by blocking requests or network packets from a single source, DDoS is very difficult to resolve, as the attack is carried from multiple distributed locations.

12.9.2 Intrusion Problems

Network Intrusion refers to any unauthorised activity on a computer network. These activities may involve unauthorised use of network resources (DoS) or threatening the security of the network and the data. Network intrusion is a very serious problem and the network administrator needs to devise strategy and implement various security measures to protect the network. We have already discussed some of the intrusion attacks such as DoS, Trojans, and Worms. The remaining attacks are briefly discussed below.

(A) Asymmetric Routing

The attacker tends to avoid detection by sending the intrusion packets through multiple paths, thereby bypassing the network intrusion sensors.

(B) Buffer Overflow Attacks

In this attack, the attacker overwrites certain memory areas of the computers within the network with code (set of commands) that will be executed later when the buffer overflow (programming error) occurs. Once the malicious code is executed, an attacker can initiate a DoS attack or gain access to the network.

(C) Traffic Flooding

It is one of the most trivial methods of network intrusion. It involves flooding the network intrusion detection system with message packets. This huge load leaves the network detection system incapable of monitoring the packets adequately. The hacker takes advantage of this congested and chaotic network environment to sneak into the system undetected.

12.9.3 Snooping

Snooping means secretly listening to a conversation. In the context of networking, it refers to the process of secret capture and analysis of network traffic. It is a computer program or utility that has a network traffic monitoring capability. In this attack, the hacker taps or listens to a channel of communication by picking all of the traffic passing through it. Once the network packets are analysed by the snooping device or software, it reproduces the exact traffic packets and places them back in the channel, as if nothing has happened. So, if the data that is being sent over the network is not encrypted, it is vulnerable to snooping and eventually

URL Snooping

It is a software package that downloads and stores a web stream as a file, that can be viewed or used later. The common online video downloaders use the same techniques to download videos from the Web.

may cause serious damage, depending upon the type of information leak. However, snooping is not always an attack, at times it is also used by network administrators for troubleshooting various network issues. Snooping is also known as Sniffing.

Various snooping software exist that act as network traffic analyser. Besides, various network hubs and switches have a SPAN (Sniffer Port Analyser) port function for snooping.

12.9.4 Eavesdropping

The term eavesdropping has been derived from the literal practice of secretly listening to the conversations of people by standing under the eaves of a house. Unlike snooping, where the network traffic can be stored for later analysis, eavesdropping is an unauthorised real-time interception or monitoring of private communication between two entities over a network. Also, the targets

Figure 12.6: Eavesdropping

are usually the private communication channels like phone calls (VoIP), instant messages, video conference, fax transmission, etc. In older days, eavesdropping was performed on the conventional telephone line and was known as wiretapping. Digital devices like laptops and cell phones that have a built-in microphone or camera can be easily hacked and eavesdropped using rootkit malware.

Eavesdropping is different from Snooping. While the former happens in real time, the latter does not. As an

example, in eavesdropping, imagine someone listening to your private conversation with the help of a hidden microphone in your room or by physically standing near the window of your room. However, in snooping, that person may make a copy of a letter that is addressed to your friend and keep the copy with himself and send the original letter to the intended address.

SUMMARY

- Malware is a software developed with an intention to damage computer hardware, software, steal data, or cause any other trouble to a user.
- A virus is a piece of software code created to perform malicious activities and hamper resources of a computer system.
- The Worm is also a malware that incurs unexpected or damaging behaviour on an infected computer system.
- Worms are standalone programs that are capable of working on its own.
- Ransomware is a type of malware that targets user data.
- Ransomware either blocks the user from accessing their own data or threatens to publish their personal data online and demands ransom payment against the same.
- Trojan is a malware, that looks like a legitimate software and once it tricks a user into installing it, it acts pretty much like a virus or a worm.
- Spyware records and sends the collected information to an external entity without the consent or knowledge of a user.
- An adware displays unwanted online advertisements using pop-ups, web pages, or installation screens.
- A keylogger makes logs of daily keyboard usage and may send it to an external entity as well.
- The on-screen keyboard is an application software that uses a fixed QWERTY key layout.
- Online virtual keyboard is a web-based or a standalone software with a randomised key layout every time it is used.
- A malware can take many routes to reach your computer, which include: Downloaded from the

Internet, Spam Email, using infected Removable Storage Devices, and network propagation.

- An antivirus software is used to detect and remove viruses and hence the name anti-virus.
- Antiviruses now come bundled with the prevention, detection, and removal of a wide range of malware.
- Some of the prominent methods of malware identification used by an antivirus include: Signature-based detection, Sandbox detection, Heuristics.
- Any unwanted data, information, email, advertisement, etc. is called Spam.
- HTTP (Hyper Text Transfer Protocol) and HTTPS (Hyper Text Transfer Protocol Secure) are a set of rules or protocol that govern how data can be transmitted over the World Wide Web.
- Firewall is a network security system designed to protect a trusted private network from unauthorised access or traffic originating from an untrusted external network.
- There are two basic types of firewalls — Network Firewall and Host-based Firewall.
- A computer cookie is a small file or data packet, which is stored by a website on the client's computer.
- Cookies are used by the websites to store browsing information of the user.
- Hackers/Crackers find loopholes and vulnerabilities in computer systems or computer networks and gain access to unauthorised information.
- If a hacker uses its knowledge to find and help in fixing the security flaws in the system, its termed as White Hat hacker.
- If hackers use their knowledge unethically to break the law and disrupt security by exploiting the flaws and loopholes in a system, then they are called black hat hackers.
- The grey hats take system security as a challenge and just hack systems for the fun of it.
- The Denial of Service (DoS) attack floods the victim resource with traffic, making the resource appear busy.
- Distributed Denial of Service (DDoS) is an attack, where the flooded requests come from

compromised computer (Zombies) systems distributed across the globe or over a very large area.

- Network Intrusion refers to any unauthorised activity on a computer network.
- Snooping is the process of secret capture and analysis of network traffic by malicious users.
- Eavesdropping is an unauthorised real-time interception or monitoring of private communication between two entities over a network.

EXERCISE

1. Why is a computer considered to be safe if it is not connected to a network or Internet?
2. What is a computer virus? Name some computer viruses that were popular in recent years.
3. How is a computer worm different from a virus?
4. How is Ransomware used to extract money from users?
5. How did a Trojan get its name?
6. How does an adware generate revenue for its creator?
7. Briefly explain two threats that may arise due to a keylogger installed on a computer.
8. How is a Virtual Keyboard safer than On Screen Keyboard?
9. List and briefly explain different modes of malware distribution.
10. List some common signs of malware infection.
11. List some preventive measures against malware infection.
12. Write a short note on different methods of malware identification used by antivirus software.
13. What are the risks associated with HTTP? How can we resolve these risks by using HTTPS?
14. List one advantage and disadvantage of using Cookies.
15. Write a short note on White, Black, and Grey Hat Hackers.
16. Differentiate between DoS and DDoS attack.
17. How is Snooping different from Eavesdropping?