UNIT 4 NETWORK SECURITY-II

4.0 INTRODUCTION

Network security - A term which can be defined in different ways; Securing the hardware present in the network; securing the software/application or most importantly securing the information that is going to be exchanged among devices present in the network. In short, the security aspects that can be attributed to use of computer networks is known as network security. One must understand the term use of computer networks before understanding its security aspects.

Let's understand this with an example of distributed network of an organization. Suppose there is an organization XYZ which has several branches across the world. The data center of this organization is situated in its head office at New-York. All the other branches share their data and extract the information from this data center. Now, think about the following questions:

- Who can share and access the data from this data center?
- What data can be shared and accessed from this data center?
- How will you ensure that the data which you are receiving at your end, is exactly the same which is stored at the data center?

Let's talk about the first question: you might be thinking the employees which are the part of organization. Yes, you are right, but can only employees are the

stakeholders of the company. No, all the people are the stakeholders paying for the benefit of the services provided by this organization. So, it means those who have associated with the organization's services may share or access the data center. But, how can we find out whether some person is associated or not. Here, comes the term authentication which is the first part in network security. We'll discuss this in detail in further sections.

Coming to second question: Suppose a scheme for authenticating the user is adapted at data center and now only valid users are allowed to access the information. But, can each user access every information available on the data center. No, because we have many stakeholders one may be the employee, manager or client. They may be interested in variety of information, but complete data available on the data center may not be relevant to all of them. So, here comes the term accessibility/ permission/ rights which is the second part of network security. These rights ensure fetching or sharing the relevant information to the respective stakeholders. Many access mechanisms are there which can be used to provide these rights, we'll discuss it later.

Considering first two problems are solved by authentication and access rights. Now the last part of this scenario is to ensure the integrity of the data which means the data is not tempered in between the network. Let's understand this: Suppose you have authenticated by giving your identity and also shown your access rights to the data center for accessing the information. Data center has permitted you to access the data. You have acquired the relevant data which is coming through the public network/ Internet. It is quite possible that you may lose some of the data since it travels in form of packets in the network. There may be different reasons congestion, packet loss, delay or some kind of cyber-attacks. Therefore, the integrity of the data need to be ensured when our data travels through network. Here come the third term data-integrity mechanisms under network security. Thankfully, our researchers have developed so many mechanisms to ensure data loss due to congestion, packet loss and other network based problems. However, cyber-attacks are not very limited and increasing day by day with the rapid growth of internet and their users. Moreover, aforementioned reasons for impacting data-integrity only affects the information whereas these cyber-attacks possess capability to hamper the data as well as hardware and software inside the network. Therefore, everyone in today era who is using internet should have the understanding of such cyber-attacks and their counter-measures.

We have come across different problems in network security, but scope of this chapter is limited to the third question where we have to ensure the security of the networks from these cyber-attacks.

Thus, we'll focus on to exploring the various cyber threats, attacks and their impact in the network. We'll also cover the ideas to handle these cyber-attacks to ensure the security of the network.

4.1 OBJECTIVES

After going through this unit, you should be able to understand the following:

- Basic understanding of the cyber-crimes and cyber-attacks

- The different types of cyber-attacks in computer networks, and
- The mechanisms to ensure the data integrity and security of the networks encountering these cyber-attacks.

4.2 CYBER THREATS, ATTACKS AND COUNTER MEASURES

Let's start understanding these concepts with the history of computer crimes. In 1983, as the internet was introduced to the world, computer crimes also came into the existence. The momentous Morris worm, the first denial of service (DoS) attack came into 1988. This worm contains a few dozen lines of code that replicated rapidly and hampered almost 10% of all the computers over the internet. Apart from these attacks, flash and browser add on vulnerabilities were introduced in mid-90's by the hackers to control the computers from remote location. As the software industry grew rapidly in early 2000s, they were less bothered about the security concerns, and thus the multi-accessed and insecure software were more vulnerable. The hackers and attackers used this opportunity to manipulate these software including some of the Microsoft software. As people started spending more time over internet, phishing (a type of social engineering where an attacker sends a fraudulent message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.) has taken place large in number. Mobilization has created a massive market for spyware and monitoring. Mobile devices have expanded public networks and wireless connections, where hackers lurk. Since 2014, automotive and other machine software has also fallen victim. IoT, a market that continues to grow exponentially, has faced many security concerns as it sits at the center of software, cloud, network and physical access concerns.

In today's world of internet, everybody is prone to cyber-attacks. So, we need to understand the various cyber threats, attacks and its counter measures. In this section, we'll define these terms one by one.

4.2.1 Cyber-Threats

As per the definition available on Oxford Dictionary, cyber threat is "the possibility of a malicious attempt to damage or disrupt a computer network or system." But the scope of cyber threat is not only limited to damaging the networked systems. It also includes an attempt made for unauthorized access of networked systems as well as infiltrating or stealing the data from those systems.

In this definition, the threat is defined as a possibility. However, in the cybersecurity community, the threat is more closely identified with the actor or adversary attempting to gain access to a system. Or a threat might be identified

by the damage being done, what is being stolen or the Tactics, Techniques and Procedures (TTP) being used.

Types of Cyber Threats

The list of most common threats published by R. A. Grimes in 2012 consists of following unwanted means of attacks in user's system or account

(i) Unpatched Software (such as Java, Adobe Reader, Flash)
(ii) Phishing
(iii) Social Engineered Trojans
(iv) Network traveling worms
(v) Advanced Persistent Threats

However, these threats are still commonly occurring, but the various game changing technologies like big data, cloud computing, Internet of things and wide use of mobile device usage have also contributed and widened the landscape of these types of attacks. Although, these new technologies have made things easier and provide more mobility to people, some adverse effect can also be seen in terms of the number of threats possible after 2016.

Cyber threats typically consist, but not limited to, one or more of the following types of attacks:

- Advanced Persistent Threats
- Phishing
- Trojans
- Botnets
- Ransomware
- Distributed Denial of Service (DDoS)
- Wiper Attacks
- Intellectual Property Theft
- Theft of Money
- Data Manipulation
- Data Destruction
- Spyware/Malware
- Man in the Middle (MITM)
- Drive-By Downloads
- Malvertising
- Rogue Software

You will get a thorough knowledge of some of the attacks in later section. Before going to discuss these threats, we need to understand the source of such threats so that we can counter them. For prevention of such threats, one can argue that, first we must know the tactics, techniques and procedure (TTPs) being used by the attackers. However, digging deep into the TTPs can't give the significant way of prevention since these TTPs are evolving day by day. Since the way of such threats will change continuously, but the source of them

will remain same. Therefore, it is more important to know the real source of threat. For this researchers and the domain experts have clearly stated, “Behind any cyber threat, there is always a human element”. So, for identifying the cyber threat, we need to focus on to identifying the person with a motive behind all such activities. As we have seen at present every field is technology-driven. Cyber threats are taking advantage of this high technology and malicious attempt to damage the computer network & computer information system. These attackers also attack personal computers or applications.

Now the question arises, how do we react to these types of attacks. Instigators every time come up with new ideas/technology to target computers with malicious attacks. To mitigate this type of risk we should have a good plan with a listed set of actions to respond to these attacks. However, we should always keep in mind finding what type of cyber-attack it is, we should also emphasize the person behind this attack.

For instance, according to the details given by SecureWorks, in June 2016 Hillary Clinton's presidential campaign emails were attacked by Russian Threat Group-4127. Later. in September Hillary Clinton's emails were presumed to be attacked by some foreign intruders. However, in both the cases, the attack was not done as it was presumed. So, we can see in both cases target was the same, however, the technology behind this cyberattack was different.

There are following major sources of Cyber Threats which can be explored with respect to target being attacked:

- Nation states or national governments
- Terrorists
- Industrial spies
- Organized crime groups
- Hacktivists and hackers
- Business competitors
- Disgruntled insiders

4.2.2 Cyber Attacks

In simple words, the term Cyber Attack can be defined as the threat which has already taken place. Although, various definitions can be found in literature, but all of them state the common aim to compromise the data integrity, data confidentiality and availability. As far as new technologies are concerned, new ways are being discovered to attack and remain untraced. Despite continuous growing new ways of attacks, traditional threats defined above are still the main source of such attacks.

There are various attacks given in the literature which results into different set of attacks: For example: Man in the middle attack (MITM): Suppose X and Y are two communication ends and Z is an external entity that wrongly enters in between X and Y. The real communicating entities X and Y don’t have any idea about the presence of Z. In this way, Z receives every

message sent from X or Y before its designated recipient. This leads to other attacks which breaches sensitive information and unauthorized access or it may also result into altering the messages.

- **Social engineering** can be defined as techniques which can be used to gain un-authentic access to information through human interaction.
- **DDoS** (Distributed Denial of Service) can be defined as unavailability of data or services by flooding the server with number of fake requests or commands, thus it leads to in-operational service or application.
- **Brute force attack**: When the repeated attempts are made by the attacker to get the sensitive information viz. passkeys, techniques of encryption or decryption etc.
- **Phishing** is a technique which aim to get personal and protected information from users through pretending that message is coming from the authentic sources for example: any repudiated website or mail.
- **Malware** is a generic term describing types of malicious software, used by the attacker to compromise the confidentiality, availability and integrity of data. Most common types of malware are: viruses, worms, trojans, spyware, ransomware, adware and scareware/rogware.

Although, it is hard to determine the exact number or percentage of different attack types, however the most common attacks are: denial of service, malicious codes, viruses, worms and trojans, malware, malicious insiders, stolen devices, phishing and social engineering, web-based attacks. Nevertheless, the results could easily be split into four categories, depending on the objective of the attack: cyber-crime, cyber espionage, cyber war and hacktivism.

4.2.3 Counter Measures

Generally, each organization issues some counter measures to prevent its systems from various attacks. Out of those counter measures, following is the list of actions that can be performed

1. **Train your Staff members** against fraudulent emails impersonating someone from the organization itself and revealing the secrecy of the organization in terms of sharing the key information for example access codes of internal servers, employee id and passwords etc. One of the powerful ways to protect the organizational privacy is to make your staff aware about current attacks and possible threats based on the designation and level.
   The possible steps to prevent these attacks:
   - One can verify the email addresses and then send the sensitive information.
   - Do not click the links which seems to inappropriate or one can verify by calling the person who has sent it.

2. **Fully Updated system and software** Its always a good practice for organizational people to keep their system and software up to date. Since, weaknesses in your systems provide an easy way to attackers to capture, access and stealing the information. Therefore, once must ensure to have the patch management systems that automatically updates the systems and software.

3. **Ensuring endpoint protection for remote devices** In today's era where IT is the backbone of most of the industries, remote access of organizational network is very common to ensure distributed nature of work among employees. On one side it provides parallel and distributed working environment, but on the other side it opens up the ways to security threats. So, these open paths need end to end security that can be achieved with endpoint protection software.

4. **Firewall** The most effective way to protect our network from any kind of cyber-attack is to use Firewall. It can be considered as a shield for our network and/or systems which helps to prevent brute force attacks.

5. **Always backup your data** The network of computer systems become more prone to cyber threats when they have always on connection with internet. In such a case, one must have backed up all the data for avoiding financial loss as well as personal loss

6. **Access management for your systems** Protecting your systems/networks by utilizing the access control mechanism is most important as you may believe or not, one of the possible attacks is the physical one and i.e. the most dangerous attack. Since these physical attacks are possible via capturing and injecting some infectious files in one of your system which can give access to the whole network. Therefore, one must ensure to have access control mechanisms to limit the perimeter of physical security of devices and networks.

7. **Enable WiFi Security Options** In 21st century, most of the devices are WiFi enabled. Due to this option, every device connects with different networks at different times. Out of those networks one may be infectious e. So, your device may get affected/infected by connecting with that network and once you connect your infectious device to your organizational network, it may also get infected if it is not secured. Thus, you must enable Wifi security options in your devices all the time.

8. **Secure Employee personal information** The systems and networks become more vulnerable to attacks when multiple users use the same credentials. It is the best practice in an organization that every

employee should have separate login credentials for enhancing the security up fronts.

9. **Passwords** Generally, in an organizational network/system or personal systems, people use to keep same password for various applications which cannot be considered a wise idea. Since, once an attacker gets your password, he/she can damage your system completely or can steal all the information from various applications. Therefore, it is always advised not to keep your passwords uniform across the applications and change your passwords frequently to make your system more secure.

   However, these are few guidelines/steps that can be followed to make our system/network secure, but a number of other steps can be taken into consideration based on the need of the organization. Basically, it depends on the size of the organization that what kind of security parameters are needed to fully secure our systems.

Check you progress 1

- ✓ How would you differentiate cyber threat and attacks?
  ……
  ……
  ……
  ……
- ✓ What are the necessary counter measures that would be preferred for big organization?
  ……
  ……
  ……
  ……

4.3 TAXONOMY OF VARIOUS CYBER ATTACKS

The term taxonomy can be defined as scientific classification of anything which means arranging things into groups. Cyber-attacks came into the existence in 1956, since then a variety of attacks are known in the field of computer security. Hence, a proper classification is needed to identify the type of attacks, its behavior and the impact. This not only helps in detecting the attacks, it also supports in identifying the counter measures that need to be adopted to mitigate and remediate these cyber vulnerabilities. So, in this section, we will see some known cyber-attacks, the possible attackers, the motive behind the attacks and consequences.

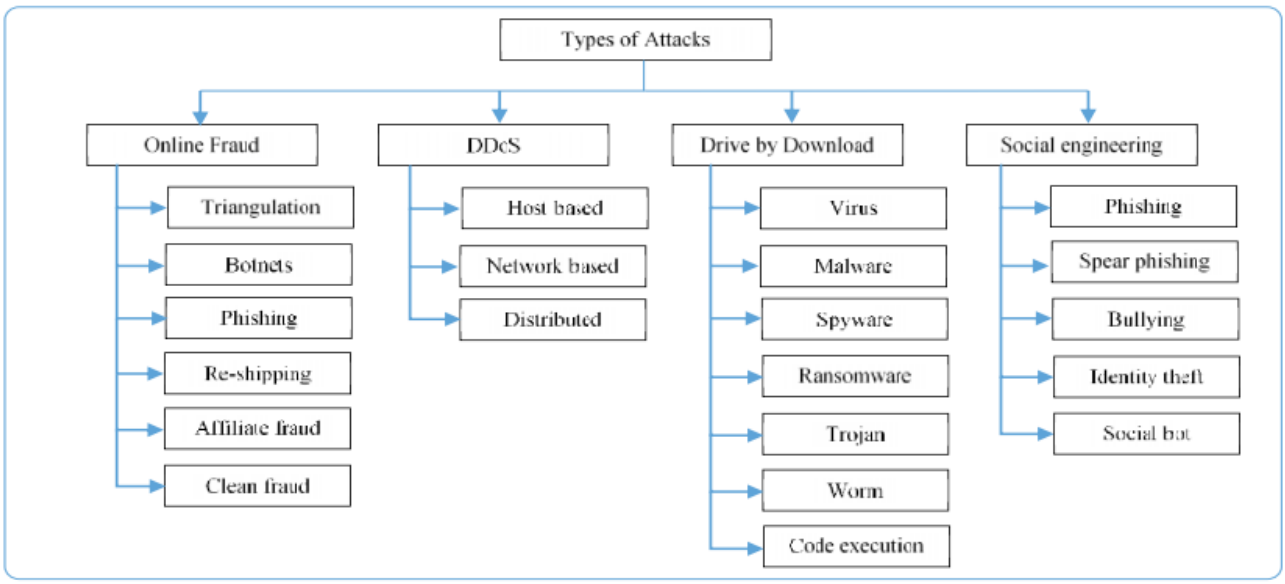

Figure 1: Classification of Attacks

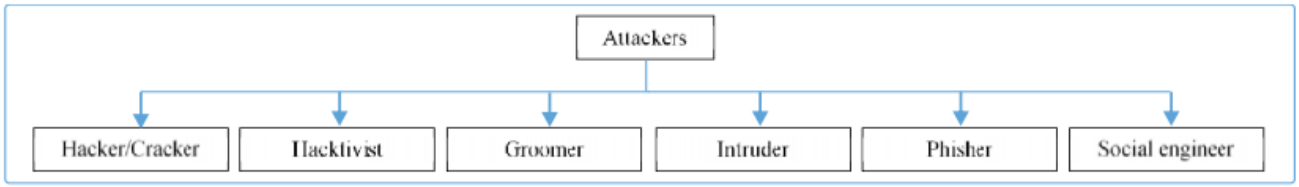

Figure 2: Possible Attackers

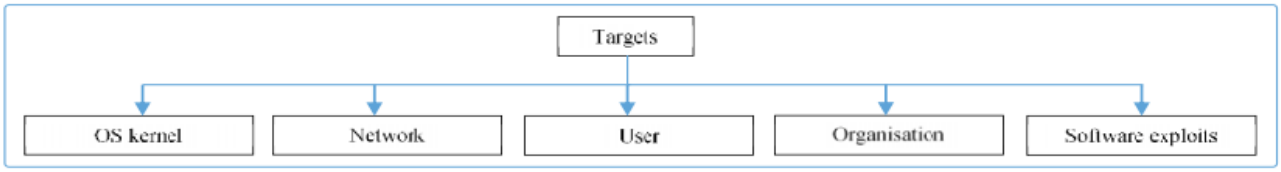

Figure 3: Targets

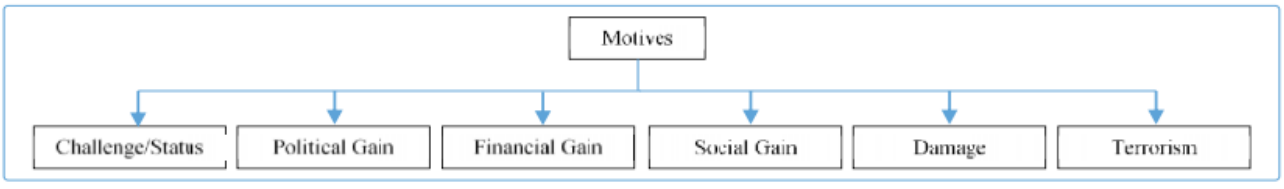

Figure 4: Motives

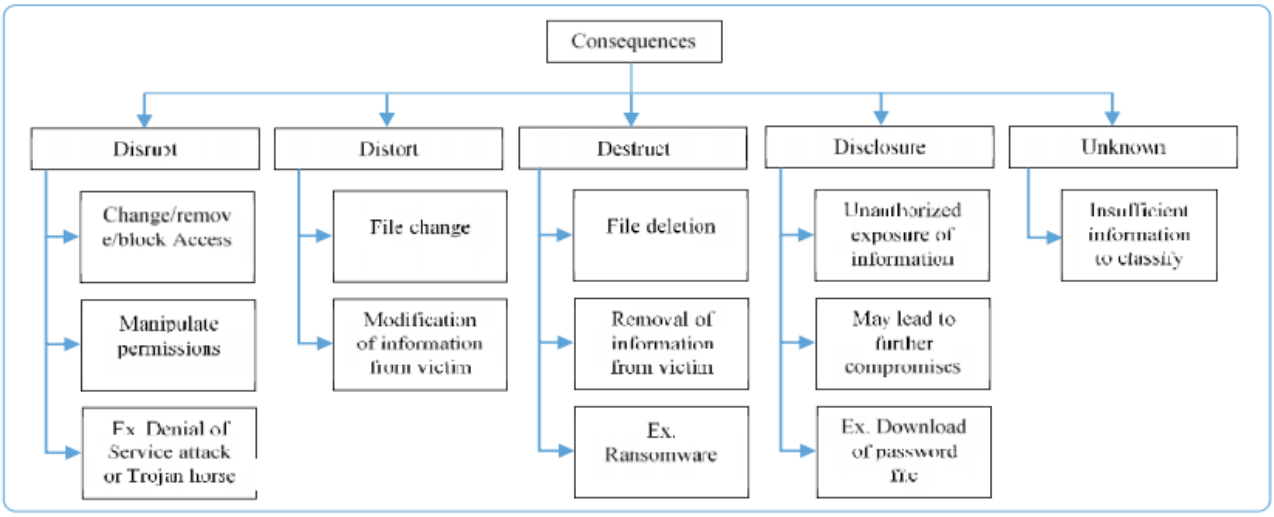

Figure 5: Consequences

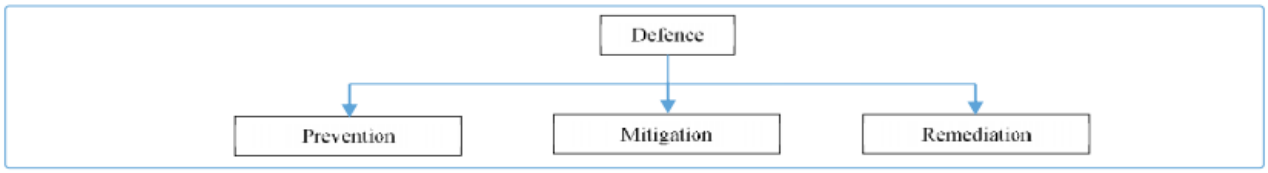

Figure 6: Defense Mechanism

4.4 VIRUS, WORM AND TROJAN, DOS ATTACK, DDOS ATTACK, PHISHING ATTACKS, MALWARE, RANSOM

Virus A self-replicating malicious computer program which affects the other programs in the system/network is known as computer virus. Alternatively, it can be defined as a software entity which is self-executable and holds the capability of affecting any code, files, systems or networks. The main objective of creating such an entity is to gain administrative rights and steal sensitive information of user by infecting the vulnerable systems. These entities can be easily spread through attaching the malicious code in the emails- a vulnerable user open this attachment and get easily infected or it can traverse through the infected sites, malicious executable code, the advertisements etc. There is one more very common way to get affected with such malicious code i.e. through the already infected storage devices such as external Hard Drive, USB etc.

There are following categories of computer viruses which are mentioned below:

(i) **Boot sector virus:** This category of virus attack directly when you start your system. It affects the boot process and prevents the system to start.

Systems may get affected with such type of viruses through external devices such as USB drive, external hard disk etc.

(ii) **Browser Hijacker:** You may have encountered one problem i.e. redirection from one site to another website several times while browsing over the internet. Such websites which redirect you to new websites are potential link for such viruses. These viruses first hijack your browser and then performs some unintended functionalities such as opening new links and applications frequently.

(iii) **Web Scripting Virus:** Such viruses use the codes written for web pages or browsers to control the functionality of any system. Once clicked on such webpages, it automatically gets into your systems and may infect your system.

(iv) **Resident Virus:** It is a different category of virus which resides in the memory of any computer and acts once the system starts.

(v) **Polymorphic Virus:** As the name suggests, Poly means many and morph means different forms; such viruses are very hard to detect since it changes its code each time when they are executed with an infected file.

(vi) **File Infector Virus:** One category of virus which generally hamper the designed functionality of the executable files by attaching some malicious codes.

(vii) **Multipartite Virus:** The category of virus works in many ways. It is not only able to infect the system boot sectors, it can also infect program files, application lead to temporarily or completely shut-down the applications or systems.

(viii) **Macro Virus:** This type of virus is written in the same macro language as software applications. It spreads when the infected document sent generally by email is opened.

There are various signs which show you that your system has been infected with one of the aforementioned viruses- homepage changes every time, slowing down the system, password changes every time you open an application, bulk emailing from your email address, frequent window popups. To protect yourself against such virus, make a good habit of adopting few steps while browsing over internet. Following are the steps that can save you from getting infected from viruses:

1) Use of any trusted Antivirus.
2) Always scan the files downloaded from internet before opening it.
3) Scan the external devices every time before use.
4) Do not click on unnecessary links/ pop ups.
5) Special attention need to pay when you are using the file sharing options using any application. Always scan such files.

Worm It is a type of computer malware. The malwares are self-replicating viruses. However, malwares known as worms have main functionality to replicate as much as it can and infect the other systems. While infecting the other systems it stays in its source system too and create each system capable of infecting other systems. It often spreads through exploiting the functionality of operating systems which are automated and not visible to user with bare eyes. It can only be noticed in systems when user experiences a lot of resource consumption without doing any activities. The other signs may be slowing down the systems or halting of the tasks.

The main difference between a computer virus and worm stated by "Security of Internet" report published in 1996 by the CERT: A software Engineering Institute at Carnegie Mello University, is that worms, once are in action, need no human intervention for its replication and spreading all around the network of systems.

On the contrary, viruses may also be self-replicating but they usually need some kind of action from the user for spreading and infecting the systems or programs.

The computer worms often use the vulnerabilities in networking protocols for propagating through the network. As soon as a computer worm infects any system, its main directive is to infect as many systems as it can. For instance, in Windows, there is a protocol known as resource sharing protocol which is a networking protocol. The very first version of one of such protocols was Server Message Block (SMBv1). WannaCry_ransomware was a worm which exploited the vulnerability of this protocol to infect the systems which were using this protocol for file sharing. As it uses the networking protocol for its propagation, it immediately starts a network search for finding out the potential systems. The systems in the same network who respond to such network query, get infected by this worm.

There are following categories of computer worms which are mentioned below:

(i) **Email worms** Generally, this type of computer worms use the user's email address book for sending out the emails carrying malicious code. Once the recipient of the mail receives such mail,

he/she thinks that the mail is from one of his/her colleague, friend or some authentic user. As soon as the mail is opened up, it infects the recipient's system. However, for encouraging to open up such type of malicious mails, it needs to perform strong social engineering and phishing techniques.

(ii) **File sharing worms** These worms are usually impersonate itself as a media files. These spread through the infected source files shared with using some external device like USB drive, Hard drive etc. It is mainly used to target the big industrial environments such as electricity supply services, water supply services etc. For example, Stuxnet is the well-known file sharing worm till date which has the capability to target big SCDA systems.

(iii) **Crypto-worms** The actions of these worms are defined to encrypt the files in infected system. One may wonder how all the files get encrypted, and is not able to open it. This comes under the category of ransomware attacks where perpetrators ask for money to decrypt the files.

(iv) **Internet worms** These are special type of worms that mainly target those websites which either not uses or uses a poor security protocols. Once such website is accessed by any user, first the system gets infected and thereafter, the private network attached to this system may get affected.

(v) **Instant messaging worms** This is similar to email worms. These worms are also come in the form of attachments or links though which the complete contacts may get infected. However, the propagating nature is different as compared to email worm, it propagates through any chat/instant messaging service.

For protecting one's system from such worms, these are the following measure that can be taken:

1) Regular updating the OS and its software patches
2) One can use the firewalls to prevent the unauthorized access to systems.
3) Use of any trusted Antivirus
4) Click only those links which you get from authentic people. Avoid checking of every link in messaging applications.
5) Encrypt your data.

Trojan It can be understood by a simple scenario- Everyone must have noticed, sometimes when you log-in in your system, everything gets popped-up or system behaves inappropriately. If such situation arises, it can be a possibility that a Trojan virus is there in your system. The Trojans are one of the most dangerous viruses which are not only able to steal your valuable and sensitive information, they can also open you up for potential cybercrimes by identity theft.

This type of virus generally comes under the category of malwares that impersonate itself as real/operational executable programs. It can be so destructive for your system once it is inside. It can also download and install other malwares to breach your security. Some other Trojans may directly try to breach the security. Based on this, there are two types of Trojans: one sits idle until it does not get any instructions from its host hacker, however others start reacting maliciously once they reached into your system.

There are following potential sources which make you vulnerable to Trojan attacks:

(i) **File sharing websites:** Every one of us must have used Torrent for sharing the files, movies, songs etc. There are other file sharing websites too over the Internet. The most appealing thing of these websites are we can have anything for free like games, movies, software etc. However, it makes you vulnerable to easily hacked by the hacker. For instance, a hacker has uploaded a cracked version of VLC media player or any popular software with a hidden Trojan on a file sharing website. Now, the clients who will download this file, may think that it is VLC software and execute it in their systems. But, unknowingly they are also installing hidden Trojan. Once this Trojan is installed, your system might be controlled by the hacker for performing any type of cyber-crime.

(ii) **Email Attachments:** This is a very common way to infect other's system. A hacker sends an email with attachment. As soon as anyone click on this attachment for downloading it to open, one may found himself infected.

(iii) **Spoofed messages:** The various desktop applications provides you the platform for chatting with others. This makes you vulnerable to Trojan attacks. Since the hackers can send you a spoofed message which seems like coming from a trustworthy person, but it is not. Apart from this, the attackers may also create a fake profile very similar to your trustworthy person. If you do not pay close attention to slightest variations in accounts, you may be victim of Trojan attacks.

(iv) **Unsecured/poorly secured Websites and Hacked WiFi Networks:** Sometimes hackers do not target the specific users. In that case they try to hijack the unsecured or poorly secured websites from where the files can be downloaded. Thereafter, redirect the clients request to fake websites and servers. Once the client downloads the file from fake/redirected website, it also downloads the Trojan. Hence, client's system can be compromised then by the hacker to perform various illegal activities.

Similarly, the fake WiFi networks can be created to compromise the client system. For instance, a hacker can create the hotspot with the same name on which a client can rely upon. When a client need to use Internet, he/she will

think that connection is going to be established with the right hotspot. However, he/she will be connected to hacker's hotspot. In that case, all the request will be forwarded through Hacker's WiFi. In such a case, all the information shared by you over that network may be compromised to perform any activity.

For protecting one's system from such Trojan attacks, these are the following measure that can be taken:

1) One should use the cloud services which supports the secure services and provide the recovery options.
2) One can use VPNs over public Wifi
3) Use any trusted Antivirus with real time protection
4) Make sure before opening any email attachments.

Denial of Service (DoS)/ Distributed Denial of Service (DDoS) attack

DoS An attack by a single system on a single system/network to reduce and restrict its access rights for the authorized users is known as DoS. There are two categories of DoS attacks:

1) **Flooding services:** In this type of DoS attack, generally system encounters with a lot of traffic which cannot be buffered in the server which leads to slowing down the system and eventually it stops working. The well-known flood attacks are as follows:

    (i) **Buffer overflow attacks** – Every system/network is designed to handle some finite/limited traffic. In such attacks, the idea is to increase the traffic to the network address of the system till that extent it crosses the limit so that it cannot be handled by the network administrator.

    (ii) **ICMP flood** – This type of attack occurs when there are some misconfigured network devices which can be leveraged by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.

    (iii) **SYN flood** – In such type of flooding attack, a continuous request made for establishing connection with server, but the handshaking never been completed

from the attacker side. This leads to saturate all the open ports with connection establishment request, consequently no legitimate user will be able to connect due to lack of open ports.

2) **Crashing services:** In these DoS attacks, attacker adopts those methods with which he/she can exploit vulnerabilities to cause system/service crash. Attacker takes an advantage of bugs present in the system and send that particular input which create this bug. Therefore, system crashes in some time and not available to access by the legitimate users.

DDoS An attack which is initiated simultaneously from multiple compromised systems to attack a single system/network is known as **DDoS**. The authorized users of such system/network find themselves not able to access the targets system/network. In other words, DDoS can be defined as DoS which are performed by multiple systems simultaneously

For performing the DDoS attack, an attacker selects the zombie systems to attack on a single system/network. Once these zombie systems are compromised, the attacker sets up the command and controller which controls these zombie systems to attack. These zombies are controlled with the use of bot which is a special type of malicious software. A group of zombies installed with bot is known as botnet. Figure 7 shows the flow of DDoS attack.

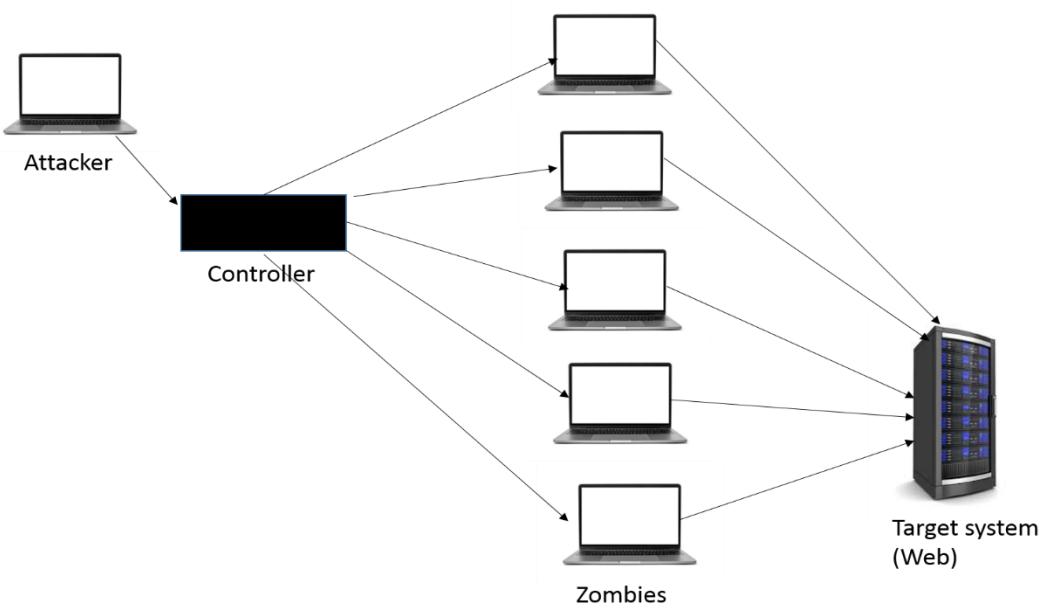

Figure 7 Distributed Denial of Service Attack (DDoS)

Phishing Attack It requires a social engineering techniques to target some specific users. Attackers performs such attacks by establishing the fraud communication with the users which seems to come from an authentic source. The main objective is to get the sensitive information of users such as debit/credit card information or login details and installing any malware over victim's system. Generally, it is performed through emails. There are two categories of phishing attacks based on impact of attack on individual:

1) For financial gain, the attackers try to get the victim's sensitive information like debit/credit card details or any other personal data which may be helpful in carrying out the fraud transactions.
2) For attack against an organization, attackers try to get the login information of employees for doing some advanced attacks. Advanced Persistent Threats (APTs) and Ransomware usually being performed with Phishing.

   Below are the following measures that can be taken to protect from such attacks:
   1) Educate the users/employees to recognize such phishing emails.
   2) Adopting the network security technologies such as email and web security services, antivirus to protect from malwares, access control mechanisms and behavior monitoring.

Malware It a malicious software, once installed on victim's device opens up for breaching the cybersecurity and make your device prone to several threats. For gaining unauthorized access or personal information, cyber-attackers create such malicious executable codes which can be run without the user's consent. It is usually performed for financial gain or completely damaging the device. It can affect any device whether it is macOS, iOS or windows. There are different malwares which are as follows:

1) Viruses
2) Spyware
3) Ransomware
4) Trojan horses

Apart from these malwares, there are different categories of malware attacks under which these malwares can be classified:

1) Exploit Kit It is kind of malicious toolkits which usually used by the attackers to find out loop-holes/vulnerabilities in victim's system/device. The task of pre-written codes in such kits is to get the details of software vulnerabilities. Once the task is performed successfully in one's computer, this kit injects the malware into the system using the loop-holes. In order to protect from such type of attacks, one has to always install software updates and security patches which make itself unavailable to such exploit kits.

2) **Malicious Websites and Drive-by-Downloads** Some malicious websites are specifically designed for malware attacks also use these exploit kits. Such websites work as a host for these kits. Once a user visits such website, exploit kit hosted start working and search for vulnerabilities present on the browser. In this way, malwares can found their way and driven by downloads to infect the system.
3) **Malvertising** As the name suggest- the attacks which are performed using malicious advertising are comes under this category. In malvertising, attackers purchase some advertising space on repudiated websites and embed the malicious code in their advertisements. Once clicked, it starts infecting without the knowledge of user. This is very similar to Malicious websites and drive-by-download.
4) **Man in the Middle attack (MitM)** This type of attack can easily be understood with real life scenario such as two persons are communicating with each other but they are at some distance. Third person comes in between the communication and changes the information passed from one to other person. In computer network, this is performed with the help of employing the poorly secured network or over the weak WiFi network. First, attackers find out the vulnerabilities for example, default passcodes or weak keys. Then, they intercept the communication between two entities over that network by putting themselves in between. Therefore, the sensitive information like credit/debit card details, employee login details can be captured easily.

5) **Man in the Browser attack (MitB)**This is very much similar to MitM. However, in this type of attack, the attackers need not to present nearby the router as in case of MitM. Here, attackers inject the malwares in target system, and once it is installed over the browser all the information will be collected by malware. Then the programmed malware sends this data to attacker, and thus it can be used for any cyber-crime.

   Below mentioned measures can be taken to be protected from such malware attacks:
   (i) One should always keep their software updated
   (ii) One should take back-up of files at regular interval
   (iii) One should always scan the executable files before opening it.

Ransom It is also a malicious software which is used by the cyber criminals to infect the target system. When any target system is infected with ransomware, it completely blocks the system for use or it encrypts all the data available on the system. The main aim of such type of attack is to get handsome amount of ransom from victim to release its data or provide access to his/her own computer. There are three steps that can be carried out by the victim after getting infected: a) One option is to give the money asked by the attacker and get access of files and system; b) Completely remove the malware from your

system by using any Antivirus software; c) Restart the device in safe mode. For protecting your system against such attacks, cyber security experts have suggested to use trustful security software. There are well-known examples of ransomware which recently came into existence like Locky, WannaCry, Bad Rabbit, Crypto Locker, GoldenEye, Jigsaw, MADO ransomware and Fair Ransomware.

There are mainly two categories of ransomware which are popular nowadays:

1) **Locker Ransomware:** As the name suggested, it works like a locker. Until and unless, you get the key, you cannot open the system. In other words, this type of attacks has the capability to block some of the system functionalities such as interaction with I/O devices with the OS. After getting infected, one can pay the amount asked by the attacker to allow you to use your system. Despite the fact that it stops operations of computer device, it doesn't affect the files stored on your system. Thus, damage to your files and sensitive information is still safe in such attacks.
2) **Crypto Ransomware:** This works exactly opposite to locker ransomware. It attacks on your data rather than system. Once a target system is infected with such ransomware, all the files, documents and other data files get encrypted. In this case, user may able to see their data but not able to use it. This leads to panic in user's mind. With this type of attack, cyber criminals usually add a countdown for paying the amount asked, otherwise you may lose all your data since they can delete all the captured files. One way to secure your system and data from such cyber threats is to always backup your important data in cloud.

Check you progress 2

- ✓ List out the main differences between MiTM and MiTB attacks?
  ……
  ……
  ……
  ……
- ✓ What does make ransomware more dangerous in comparison to other attacks?
  .....
  .....
  .....
  .....

4.5 Vulnerabilities

Cyber criminals are nowadays very active to take an advantage of weaknesses present in the systems/networks. These weaknesses/loop holes are known as

vulnerabilities. Though, using these vulnerabilities, objectives of different types of attacks may vary from one to other. Attackers may perform such activities for financial gain, personal gain or due to some political motives. Knowing these vulnerabilities plays a vital role in protection of the system. As one having knowledge of these vulnerabilities can effectively work against modern cyber-attacks. Due to lack of such knowledge and awareness, people do not get the specific mechanisms to adopt which can work against the attacks.

Before going to dive into the details of these system vulnerabilities, lets first understand the term vulnerability: Computer security vulnerabilities can be defined as flaws and weaknesses present inside the system which are exploited by the attackers to manipulate or damage the system. These vulnerabilities are differentiated from cyber-threats as they reside in the system itself. In the absence of any possible threat, there is no harm with these weaknesses or flaws. However, they maybe used by the cyber threat i.e. usually considered as an external entity.

There are different security vulnerability types which one should know before going to analyze any type of cyber-attack. The knowledge of these vulnerabilities provide the clear picture how an attacker can approach to your system for financial or personal gain. Following are the few major categories of vulnerabilities, we will discuss few in later sections in detail.

1) **Network Vulnerabilities:** This type of vulnerabilities is usually found in hardware or software managing the network such as WiFi routers, switches, hubs in big organizations or the poorly configured firewalls. The attackers exploit these weaknesses to intrude inside the network first, and then infect all the system connected inside the network.
2) **Operating System Vulnerabilities:** These are user specific vulnerabilities which can be exploited by attackers to attempt to damage a particular's system. This type of flaws generally present in the one's operating system. For instance, default admin account created in some OS through which anyone can install any software hidden programs.
3) **Human Vulnerabilities:** This is the most common vulnerability present in the area of computer networking. Since, people those who are not from the networking background also use Internet for different tasks in their day to day life. Due to the lack of adequate knowledge they leave their network open/public. In case of individual system, they don't worry about the firewalls, antivirus software etc. that leads to being an easy target for attackers. So, in the context of such vulnerabilities, humans are the weakest link in overall network security architecture.
4) **Process Vulnerabilities:** There are various vulnerabilities which exist in specific processes such as process for setting up the login id and passwords for any application. However, most of the process vulnerabilities are the result of human error/unawareness.

4.6 BUFFER OVERFLOW

Buffer overflow is a specific type of process vulnerability which is caused by constrained resources availability in software development phases. Specifically, buffer overflow is a situation where temporary space supported by any software consumed to its defined storage capacity. In such a case, the excess data take place into already occupied memory locations which leads to corrupting or overwriting the data present earlier at those locations. This flaw is generally used by the hackers to infect the users of the software. Moreover, it can be described as a vulnerability which is caused by software coding error at run time. Every software has some limitation, and those limitations are exploited by the attackers for unauthorized access to damage any corporate system. Buffer overflow is one of the well-known software vulnerabilities since it can occur in so many ways. Every time hackers find out the different way to attack, thus there is no specific strategy to prevent from such attack. Therefore, usually cybersecurity team works along with the development team for handling such cases.

The hackers exploit this vulnerability to manipulate the coding error to use infected system for unauthorized access to perform malicious activities. However, manipulating the error is not an easy process. This includes changing the complete execution path of the software and overwriting the contents already present at the location. It typically occurs when:

- The code is based on some outside data for controlling the functionality of the software.
- The complexity of code creates problems in accurately predicting the functionality of the software.

As a result of such attack, there are following impacts that may occur in your system:

1) Complete System Crash: The consequence of buffer flow attack may result into full system crash. Moreover, such attack may also lead to temporary unavailability of services provided by the software.

2) Access control: The arbitrary code is generally used for commencing a buffer overflow attack which is usually not defined in any software policies. Thus, losing the access rights.

3) Additional Security concerns: When an attacker uses such arbitrary code it also leads to breaching the other security policies defined in the program. Consequently, other vulnerabilities also exposed to be exploited.

The most common buffer flow attacks are:

1) Stack based: In this type of attack, an attacker replaces and send the data required by the application with a malicious code. This contagious data is stored in stack buffer of the application which

changes/overwrites the actual data on the stack, and then application returns a pointer to this data in the stack. As soon as attacker gets this return pointer, he/she get control over the complete stack and misuses the application on the target system.

2) Heap based: It is more difficult in comparison to stack based buffer flow attack. It floods the memory of the program once program gets into the execution state which is not a simple task.
3) Format input string attack: The attack with formatting input stack takes place when the program takes input data as a command and not able to validate it. This exposes opportunities to the attacker to modify the input string and takes control over the process and results into segmentation fault etc. Hence, triggers malicious actions in the system.

4.7 SQL Injection

SQL stands for structured query language which is used for querying and modifying the databases. In the internet world, any web service hosted over the internet uses database to store the information it's users and other details. Cyber criminals mainly try to intrude in database to capture the information from a web service. This intrusion is databases are possible with some sort of query language. Therefore, SQL injection is a way to intrude into the databases through which hackers try to gain unauthorized access and sensitive information. SQL injection is nothing but a simple piece of code to manipulate the database. It's one of the most prevalent and threatening types of attack because it can potentially be used against any web application or website that uses an SQL-based database.

For example, consider a website which give access rights to its clients only when user enter the login information over the website. These login details are generally taken through webforms hosted by the website. Once a user fills these login details in the form, the information entered by user is matched with the entries already existing in database at the backend. In case of mismatch, user asked to enter the correct login details. Otherwise, user allowed to use the website.

However, instead of these login details one can fill any information in these web forms. This provides a way to hackers/attackers to intrude in the database through their own requests. These web applications are generally designed in such a way that every request must be processed by checking through the database. So, these false request also go for search in the databases which leads to malicious activities such stealing valuable information of clients or modifying already existing entries.

Preventive measures that can be taken to handle SQL injection attack:

1) Use a trusted web application firewall

2) Use a trusted Antivirus software which provides the real-time security

4.8 BROWSER Vulnerabilities

Revolution in world of Internet came with the introduction of web browsers. Every employee, be it from small or large organization, use these browsers to access internet to perform their jobs. However, it has dramatically increased the productivity, but also exposes the organization's security breach points. Cyber-criminals found the easiest way to enter any system i.e. browsers used by its employees. Since every browser contains the information of cookies (simply a file which keeps records of last visit of a user) and uses plugins, so by entering into a browser an attacker can use these vulnerabilities to get the sensitive information of any user. Using the login details of any user, an attacker can enter into the complete system of an organization.

Apart from these cookies, cyber criminals also try to attack by injecting a malware into the browsers. These malwares reside in some malicious websites which is specially designed to do false activities. As soon as a user visits such websites, it automatically gets injected in user's browser and handed over the control to hacker. By exploiting the information transmitted from the browser, an attacker steals the sensitive information, and thus performs the malicious activities.

In addition to cookies and plugins, many other vulnerabilities are making things worse due to which various threats such as MItM, MiTB etc, are hard to detect.

4.9 OS Vulnerabilities

In an operating system, user uses various application software which exposes any system through many source of vulnerabilities such as browser vulnerabilities, client application vulnerabilities etc. Though, OS vulnerabilities are classified as follows:

1) **Client side vulnerabilities:** In this category, an attacker tries to infiltrate via different applications installed/supported by operating system. These applications may be any web-browsers, different office software where client interaction is mandatory, email client applications or media players.
2) **Server side vulnerabilities:** These vulnerabilities generally found on server side computer system or in between the client and server. For instance, this can be understood by a simple scenario in which an attacker can attack thorough SQL injection method on any web application. This leads to get access of the database and employing any malicious activity at the sever side. In other words, a server side vulnerability is exposed due to vulnerabilities present at the client side, web browser as mentioned in the above scenario.

We know popular operating systems such as Windows 7/8/X, Linux, Unix, MacOS etc. All the operating system carries some vulnerabilities; however, vulnerabilities present in Windows OS are easy to understand since most users are well familiar with functionality of windows. All of us must have used Remote desktop connection (RDC) in our Windows OS. This RDC client is known as popular OS vulnerability since they allow to execute the external codes for establishing the connection. Attackers exploits this for running their malicious code, and thus infiltrate in the user's system and damage the system or steal their sensitive information. Similarly, one more very popular functionality provided by Windows OS i.e. Windows Remote Desktop Gateway (RDG). An attacker can run their arbitrary code similar to RDC, but there is no interaction required from the user in RDG. Hence, it can be used to attack and get unauthorized access of the system with specially designed requests. In contrast to this, client based OS vulnerability are supposed to exploit by a compromised user for connecting with malicious server.

Check you progress 3

- ✓ Which type of vulnerability is found as the easiest way for intrusion by the cyber-criminals, and why?
  ……
  ……
  ……
  ……
- ✓ List out some of the OS vulnerabilities in Linux and MacOS.
  ……
  ……
  ……
  ……

4.10 BASIC COMPUTER FORENSICS

Computer forensics is an art which describes the present state of a digital artifact such as mobile phones/devices, computer systems, hard drives, pen drives. Moreover, it also includes investigating and linking the data present in the computer systems, email applications etc. for describing any event. The field of computer forensics is comparatively new than cyber security, however recent advancements done in the past twenty years have overwhelmed this field to contribute in various legal proceedings in the court. A formal definition of computer forensics is given by Kruse and Heiser in year 2002. According to the authors, it is defined as involving

"the preservation, identification, extraction, documentation and interpretation of computer data".

The existence of computer forensics starts from 1980s when computers/digital devices have started revolutionizing. This revolution in digital world has increased productivity of employees and industries along with various criminal activities such as online frauds, hacking and cracking. This leads to several cyber security experts to design specific techniques to investigate the fraud and crimes. Specifically, these come under the emerging field of computer forensics. Although, it started in 1980s, but a rapid growth has been recorded in year 2002-2003 when cyber-crimes were increased by 67%. Currently, it is being used in investigating various frauds and crimes such as murders, rapes, child pornography, cyber stalking etc. forensic investigations are generally performed on static system rather dynamic. In this, the process of investigations usually follows a set of digital forensic phases which are as follows:

- Acquisition of digital artifacts.
- Examination of acquired these digital artifacts.
- Analysis of examined artifacts.
- Preparation of reports for legal issues.

Following are some major techniques being used in investigations by forensics team:

1) **Cross-Drive Analysis:** This technique is used where typical source of information (from where the data is obtained) remains distributed in nature and forensic teams do cross examination of data to correlate and analyze the findings. Researchers are still working to develop such techniques which can give more insightful results. This is generally used in identification of social networks and detecting anomalies present in the digital artifacts.
2) **Live Analysis:** This technique is used where computer systems are on and in working condition. Forensic team uses such techniques to extract the evidences with the help of custom forensics or SysAdmin tools. These tools examine the systems starting from operating system and are able to deal with encrypted files.
3) **Analysis by recovery:** Techniques used in recovering deleted files from the system for finding out the cause of incident/fraud happened. Forensic team exploits the nature of some operating systems which do not always allow to delete data from physical disk sectors. File carving is a technique which can be used to find out the headers representing the disk sectors of such files in physical space. After getting such headers, team reconstruct the deleted files for further analysis.
4) **Stochastic forensics:** This technique is used in case of data theft. Forensic team uses the probability theory or stochastic properties of systems for investigating the digital artifacts.
5) **Stenography analysis:** The term stenography defines a way to hide the data in image files Attackers used this technique to hide pornographic pictures of children or the information they do not want to get

discovered by anyone. However, forensic team exploits the technical details of an image where pixel information gets hash information. When any change occurs in original picture, this hash file changes which leads to detect alteration or hidden information.

4.11 Recent Cyber Attacks

In 21st century, cyber security is essential for every individual and organization due to vast use of Internet. Although, various self-learning/experience based solutions and software solutions such as antiviruses exists, but cyber criminals are in continuous search for getting success in breaching out these solutions. Various vulnerabilities that still exist in system/network exposes them to attackers to think about an alternative way to infect. Thus, it becomes more important to educate people about these vulnerabilities which are discussed in previous sections. Now in this section, we will see few recent cyber-attacks which happened against well-known organizations. The impact of attacks on an individual or organization can be understood with the details given in each of the attack. Herein, the following are some recent attacks from last two years:

1) **Attack on Popular Social media website Facebook:** In the month of APRIL 2019, it was reported that around 540 million user data exposed and published over Amazon's cloud service. It was found that two third party application developer were involved in this activity. At later stage it was reported that there were some political firms behind this attack. The captured data from millions of Facebook profile users were then used for false political advertisements. In the end of the month, Facebook again revealed about one more such leak. However, it was not done by attackers, whereas millions of user mail ids were made public unintentionally by the Facebook itself.
   From these two incidents, one can understand that how much data these large organizations are handling- and one small mistake can put the information of millions of people at risk.
2) **Attack on graphic design website CANVA:** This is another recent example of cyber-attack where around 140 million user's data got exposed. The hackers intruded into main servers of this website and get access of the information such as user login IDs, passkeys and other profile information. However, these details were encrypted but still put millions of users at risk.
3) **Attack on Servers of MGM hotel:** Similar to CANVA attack was recorded in February 2020 with MGM hotel. More than 10 million people's information got exposed who stayed there in past. The hocking agency got several personal information such as name of the customers, address, contact details, email addresses, DOB. Few of those information belongs to well-known business personals,

celebrities, employees working in government agencies and tourists. However, there was no loss occurred in monetary terms to any customer. Hence, it can be inferred that no card details were leaked in this attack.

4) **Ransomware attack on California university:** In June 2020, attackers had attacked the university servers with a malware known as Ransomware. They had targeted various servers with aim to get a handsome amount from the university to release their data store on those servers. With this all data became inaccessible due to encryption posed by the malware. This results into paying the amount hackers had asked for. According to the reports, university had given around $1.25 million to the hackers for releasing their servers.
5) **Attack on World Health Organization:** In march 2019, when COVID pandemic broke across the world, WHO had played a crucial role to find out the ways to fight with this novel corona virus. Many of the international agencies were working together to fight against COVID. But, in april 2020, it was revealed that around 25000 email addresses were hacked by the hackers. All the email addresses and passwords leaked online along with other information such as the names of the different agencies and groups who were fighting against the pandemic. The names in the list includes National Institute of Health (NIH), Gates Foundation and US centers for Disease control and prevention (CDC).
6) **Attack on Zoom video conferencing service:** During pandemic in 2019, the various industries had adopted work from home culture. This resulted in high demands of applications like zoom video conferencing, webex, google meet etc. People started using these applications for their personal and professional meetings. Now, it became easy for cyber criminals to attack on an individual or organization using the vulnerabilities present in such applications. For instance, ZoomBombing was one such attack which enabled attackers to join personal/professional meetings and gain access of the conversation made. Moreover, they had distracted the host and other members by sharing the offensive picture and videos. However, the security levels were increased in zoom after this attack.

4.12 FIREWALLS AND INTRUSION DETECTION SYSTEMS

In this section, you will study about the most important preventive measures that can be considered to protect any individual or an organization from cyber-attacks. A firewall and Intrusion detection system both works for protecting you from various cyber-attacks at different levels. However, there are some similarities and differences in the working of both firewall and an IDS.A firewall can be considered as security watchman standing at the front door of

your home whereas an IDS can be considered as security cameras installed inside your home. As watchman standing at the door can stop any person entering into the home, firewall can stop/block the incoming connection in the network/system. Similarly, the security cameras installed cannot block any person from entering in the house, but it can detect any intrusion attempts made by the person already there in the house. In the same way, an IDS cannot block the incoming connection, but reports or generates alarm in case of intrusion. Before going to explore the various firewalls and IDS available in the market, first we need to understand the basic concepts of firewall and IDS.

Firewall A firewall can be a software or hardware both, it depends on the nature of the system where security restrictions are required. The main functionality of a firewall is to provide access rights to authorized individuals whereas it denies/blocks the permission to unauthorized users. This mainly works in networked environment and resides in between local network and internet. Apart from giving access rights, it filters the unnecessary traffic coming from internet to your local network that might be harmful and cause problems in systems.

Intrusion Detection System (IDS) An IDS can also be a software or hardware installed on the network or host to detect and report intrusion attempts to the network. There are two types of IDS, one is network IDS (NIDS) and other one is Host IDS (HIDS) depending upon where exactly it is installed.

The table given below consists the major differences between firewall and IDS:

Firewall	Intrusion detection system
A firewall cannot detect security breaches for traffic that does not pass through it (E.g. a gateman can watch only at front gate. He is not aware of wall-jumpers)	IDS is fully capable of internal security by collecting information from a variety of system and network resources and analyzing the symptoms of security problems
Firewall doesn't inspect content of permitted traffic. (A gateman will never suspect an employee of the company)	IDS keeps a check of overall network
No man-power is required to manage a firewall.	An administrator (man-power) is required to respond to threats issued by IDS
Firewalls are most visible part of a network to an outsider. Hence, more vulnerable to be attacked first. (A gateman will be the first person attacked by a thief!!)	IDS are very difficult to be spotted in a network (especially stealth mode of IDS).

Table 1 Firewall and IDS

There are various firewalls and IDS available in market. One can choose based on the level of security required in the system/network. A list of firewalls and IDS is given as follows which can be explored further:

Firewall software	Intrusion detection system software
FortiGate NGFW	SolarWinds Security Event manager
Juniper Firewall Check Point Next Generation Firewalls (NGFWs)	Bro
Sophos XG Firewall	OSSEC
Huawei Firewall	Snort
WatchGuard Network Security	Suricata
Palo Alto Networks Next-Generation Firewall	Security onion

GlassWire Firewall	Open WIPS-NG
Cisco Next-Generation Firewall Virtual (NGFWv)	Sagan
CrowdSec	McAfee Network Security Pl
Azure Firewall	Palo Alto Networks

Table 2 List of few Firewall and IDS software available in market

Check you progress 4

- ✓ How does forensic expert find out the hidden information in an image and what is the name of technique to hide such information?
  ……
  ……
  ……
  ……
- ✓ Comparing a firewall and an IDS, which one is more powerful in context of securing your system/network?
  ……
  ……
  ……
  ……

4.13 SUMMARY

In preceding sections of this chapter, best efforts are made to present available knowledge in the domain of network security. Currently, extreme use of computers in distributed manner require networking strategies to make them connected with each other. This implementation further poses a lot of security concerns for the systems involved in such networks. So, this chapter gives a detailed overview of security concerns like threats which can result into many cyber-attacks. After that discussion move towards defining the major reasons due to which one may be exposed to these attacks are known as vulnerabilities. Finally, the preventive measures are discussed through which individuals can protect themselves from these cyber-attacks. In addition to this, few recent cyber-attacks are also discussed which includes the popular attack on

Facebook. At last, readers are suggested to explore topics such as firewall or an IDS for effective solution which may fight against these threats.

The objective of this chapter is to make aware of the importance of cybersecurity area to students and readers of this book so that techniques mentioned in various sections may be implemented to work in secure environment. Although, topics covered are presented in a very general way so that beginners can easily understand and implement in their day to day life. Furthermore, the topics can be explored for more details following the material link provided in Further Reading section.

4.14 SOLUTIONS AND ANSWERS

Check you progress 1

1. Both the terms cyber-attack and cyber threat are correlated with each other. A threat is a possibility of occurrence of an attack whereas an attack is a malicious activity which has already taken place to breach the security of system/network.
2. The necessary counter measures in big organization include the following points:

- Educating the employee of the organization at every level since one weak link may damage the complete network of systems.
- Use of good firewall, antivirus and an IDS to ensure safety from outside, inside and from intermediate networks.

Check you progress 2

1. The main differences between MiTM and MiTB attack are as follows:
    - an attacker need to be nearby the router in MiTM, whereas in MiTB, the attacker need not to be there near the connecting router or switches.
    - In MiTM, an attacker needs to watch the network traffic continuously, whereas in MiTB this is not the case since hacker already get control of browser.
2. In comparison to other type of attacks, ransomware is more dangerous because it completely blocks the system by encrypting all the files that leads to make user feel helpless. Thus, user gets forced to pay the ransom to attackers for releasing the encrypted information.

Check you progress 3

1. Exploiting browser vulnerability is the easiest way for attackers to attack on system. Since it requires least effort from attacker. In this, attacker only creates links consisting malicious code, and once user click on that link it automatically get installed on user's system.
2. OS vulnerabilities in Linux and MacOS are as follows:

- In Linux: Dual boot with Windows

Physical theft is always an option with Linux

Open source Operating system where every line of code is public.

- In MacOS: security holes in software

App Store vulnerability

Inflexibility of hardware and software upgradation.

Check you progress 4

1. Computer forensic experts find out the hidden information behind the image using hash. Since, hash information gets changed when any alteration being performed on an original image. The name of technique to hide such information is stenography.
2. We cannot perform any comparison between firewall and an IDS in terms of power since the functionalities are different for both. Firewall provides security by blocking the incoming traffic whereas an IDS secures the system/network from internally by detecting the intrusion activity.

4.15 FURTHER READINGS

1. Kizza JM. Computer network security. Springer Science & Business Media; 2005 Apr 7.
2. Kizza JM, Kizza, Wheeler. Guide to computer network security. Heidelberg, Germany: Springer; 2013 Jan 3.
3. Pawar MV, Anuradha J. Network security and types of attacks in network. Procedia Computer Science. 2015 Jan 1;48:503-6.
4. Zhu B, Joseph A, Sastry S. A taxonomy of cyber attacks on SCADA systems. In2011 International conference on internet of things and 4th international conference on cyber, physical and social computing 2011 Oct 19 (pp. 380-388). IEEE.
5. Cashell B, Jackson WD, Jickling M, Webel B. The economic impact of cyber-attacks. Congressional research service documents, CRS RL32331 (Washington DC). 2004 Apr 1;2.
6. Kumar V, Srivastava J, Lazarevic A, editors. Managing cyber threats: issues, approaches, and challenges. Springer Science & Business Media; 2006 Mar 30.
7. Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials. 2015 Oct 26;18(2):1153-76.

8. Mahmoud MS, Hamdan MM, Baroudi UA. Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges. Neurocomputing. 2019 Apr 21;338:101-15.
9. Albahar M. Cyber attacks and terrorism: A twenty-first century conundrum. Science and engineering ethics. 2019 Aug;25(4):993-1006.
10. Beavers J, Pournouri S. Recent cyber attacks and vulnerabilities in medical devices and healthcare institutions. InBlockchain and Clinical Trial 2019 (pp. 249-267). Springer, Cham.
11. Rot A, Olszewski B. Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection. InFedCSIS (Position Papers) 2017 Sep (pp. 113-117).
12. Gupta BB, editor. Computer and cyber security: principles, algorithm, applications, and perspectives. CRC Press; 2018 Nov 19.