# A Brief Overview of Network Attacks & Overcome Techniques

Muhammad Saleem [1], Mirza Naveed Jahangeer Baig [2], Mufeeza Manzoor [3], M.Tahir Usman [4], Saba Akram [5], Saira Khursheed [6]
[1,2,5,6] Virtual University of Pakistan, [3] Comsats University Islamabad, Pakistan, [4] University of Lahore
[1] ms170401272@vu.edu.pk , [2]ms160402266@vu.edu.pk , [3]mufeezamanzoor@gmail.com,
[4] ms160402266@vu.edu.pk , [5] sabaakram676@gmail.com , [6]zanikhan32@gmail.com

**In computer networks there are two types of attacks external and internal which are big security issues for any network security. Including these attacks, there are different types of malware like Trojan horse, virus, payload worms and so on. Now a day the internet becomes not safe until we did not use any security technique for sensitive information. To fix these issues we have used some techniques like send encrypted data over the net to ensure the security of data and to overcome malware and virus issue we have used antivirus programs. In this paper, we point out all the issue and threats also provide the overcome techniques and point out the area for future research. Security is the critical issue for financial organizations like bank there is a lot of work on the network security done and still we find the best techniques but in these days hackers have become more powerful and they crack the security of the network and try to access the sensitive data to avoid that we have used best techniques.**

**Keywords:** Threat, Denial of Service Attack (DoS), Sniffer attack, IP address spoofing, Distributed Denial of Service Attack (DDoS),

## I. INTRODUCTION

The network security has a critical role in sending sensitive data through the internet if we did not use any security tools the data might be access by a hacker. As we know internet can be accessible easily not only PC but also on smartphones we can make payment through ATM card by using internet as if we not use security tools for browsing it might be the loss of money through the hacking there are various type of program also on the internet that is very dangerous as they can get the control of the device and send the sensitive data to the hacker also share the personal information the program hide themselves execute silently. By the used of this information the hacker can attack the device, attack not only accesses the data but also be able to modify it [1]. Hacker bused powerful programs our old safety tools are not able to overcome these attacks. Hackers used various types of attacks if one fails [2], they can use another different type of attack our safety measures fail against the attacks and not so effective to overcome them. There are many kinds of security threats like internal as well as external threats [3]. In this paper, we have tried to describe all of them. we have also described some safety techniques, mechanisms, and tools to overcome said attacks. we point out the best method to send data over the network. After that finally, we conclude our opinion, and point of the future area of research in the network.

## II. WHAT ARE THE THREATS?

The word threat is used when any device breaks the security measures. The threats might be internal or external. Firstly, we see internal threats

### 2.1 Internal attacks

This is the type of threats occur by employees and EX-employees. In any organization, the employees know all the internal information about the network, so they are very dangerous for network security if the shared said information with any unauthorized person. Due to the help of that information any person can easily access the private information of this company and provide loss. Not only employees but EX-employees can also be knowing all the internal information they also know the weakness side of the system because they work for the said company for a lot of periods, they know the security holes within the organization. Companies hire them to run their business, for example, a bank hire employees for new branch they provide them access through intranet all the team member have an account through this they can check and balance system if anyone share such detail with unauthorized person [4] then bank faced a huge loss of memory and the data of the accounts also be hacked or modifier by attracter. So, companies should be very careful about their employees and ex-employees. Some greedy mind employees cannot see the progress of its company so they will do such attack to break down the system [5].

Mostly these types of threats are due to the computer or IT employees. These employees have a good knowledge of computer and internet and know all the weakness of their system so they can more easily do such tasks than an unaware person. IT employees are the backbone of any company. In IT employees team

there is also a system or network developer that develop all the system for the company surely he completes knowledge about weaknesses of the security system he will easily use this and attack the company more easily within less time he able to access sensitive information. This threat may also happen when any company call hardware engineer for system maintenance of the system the employee may instill some harm software or logic bomb. If he does so it create a lot of problem for the company data [6]

Employee Hacking is another kind of security threat it is also used in companies it mean the employee want to assess such data that was not be authorized to them for example in a bank system the cash officer will be seen the balance add and withdraw balance he will not be able to change or update account information of the client he just add and withdraw balance form the client This types of hacking is mostly done without the knowledge of his/her organization or company[7].

Darning working hours some employees download large files due to the downloading the internet will be slow for all other employees in the company so time waste for such tasks.

These employees can be harmful due to that they have full knowledge and all the weakness hole of the security system of his/her organization or company. They do not anything just wait for a suitable chance whenever the employees feel some holes in the system, they will be doing their work to access the company domain through an unauthorized manner. [8]

Some companies use the limited internet connection in such cases employees download data from the internet more than that data which can download. That will be the loss of money because on over downloading the internet company charges a large amount to the organization which used internet connection.

An employee or ex-employee could sale the system weakness of his/her company or organization to the other companies that work same or sale to any hacker for that he got money and the hacker or companies get the sensitive information of the attacked company mostly employees do that due to the money get any furniture any other. That is also called employee financial theft.

Darning working hours some employees download large files due to the downloading the internet will be slow for all other employees in the company so time waste for such tasks. Some employees download sexual data from the internet and not do his/her work just watch the movies and waste the company time and money for personal interest.[9]

Another kind of employee financial theft is theft of intellectual property (IP). The term IP is very important for any company it provides the security measures, business plans, user list and so on [10]. If any employee shares or leaks this information the company causes a large loss.

Temporary or contract employees also a big hole for the security of any company system as the company must provide the account to the server and trust on these temporary employees because the company business not run without the co corporation of these employees. This type of worker just hire for a single task after completing the task the company will fire them and these temporary workers must leave the company. They will know the security hole of the system and will knowledge about the system so they can create different kinds of threats for the company. They can steal business plans, secret information, and company important data. They sell such data to the other same type of company to get money and provide a lot of lose to the previous company [11]

EX-employees of any company can also be very dangerous for the company. When they leave any company, they know about the security hole of the company they create various types of threats for the company without any job leaving issue because they already left the job and no tension of termination the jobs.

With the passage of time, these types of employees and EX-employee are increasing day by day. As a result of these frauds a company can bear reputational damage, financial loss, and personal data lake and so on.


Figure 1 Internal attacks

### *2.2 External Threats*

External attacks are launched from outside the organization. There are many kinds of external attack some of them are given below,

### *2.1 Sniffer attack*

In that attack the attacker needs to use a special software this type of software is called sniffer, the sniffer did various things over the internet, for example, a sniffer software can read the data when we send this data through the internet this will read it when the data is traveling over the internet. A sniffer can be able to corrupt the data or modify it [12]. A sniffer not only read the data, but it can be able to break the data packets also get all the secret information.

.

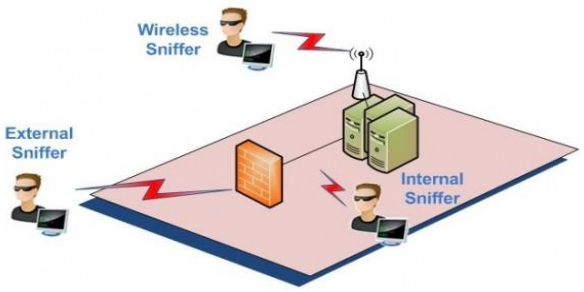


Figure 2 Sniffer Attack

### *2.2 Denial of Service attack (DoS)*

In which hackers or attackers can send a request for service to the server multiple time at least the capacity of the server to handle of request reached and the server not provide the services to the original user and mostly this case 500 error show or server display message that server is overload. Through this attacker stop the communication between client and server. Dos attack will stop or sometimes slow down the services originated from online gaming service. [13]

Denials of Service attacks are dangerous for network security because though that any authorized personal block the whole network. This will be done by UDP Intermittent and Flooding. In these days denial of service attacks is very common. This type of attack completed with two steps. The following diagram shows the DoS attack.

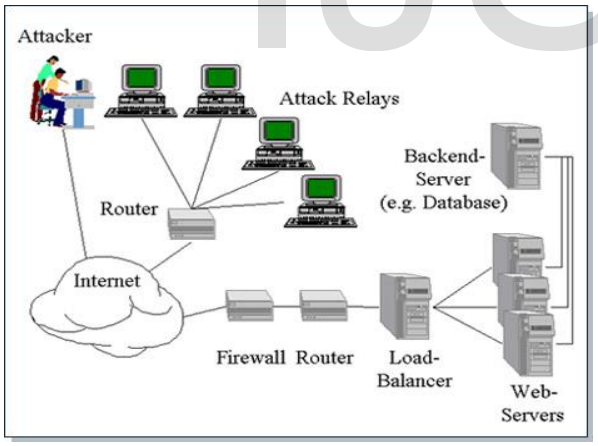


Figure 3 Denial of Service attack (DoS)

In DoS firstly the attacker or hackers get ready many computers for the attacks. In DoS one person can send multiple requests to the server until the server reached the full request handing stage and no more request will provide any service the device which the attacker used is called bot through these bots attacker busy the server and the server will not provide services to the original client due to the overload capacity.

### *2.3 Distributed Denial of Service*

DDoS is very dangerous in the security of any network because this is a planned attack in which not only one attack device is not used DDoS attacks take place through multiple devices or bots. This type of attack will be completed with two-step firstly the attacker manages various compromised computers for attack these are also called bots. After prepared bots the attacker executed them, these bots send multiple requests with short time and the server is busy to handle these request until the capacity of the server is overload and server will not be able to provide services to any clients that why client-server communication is blocked and it will slow down the network speed [14]

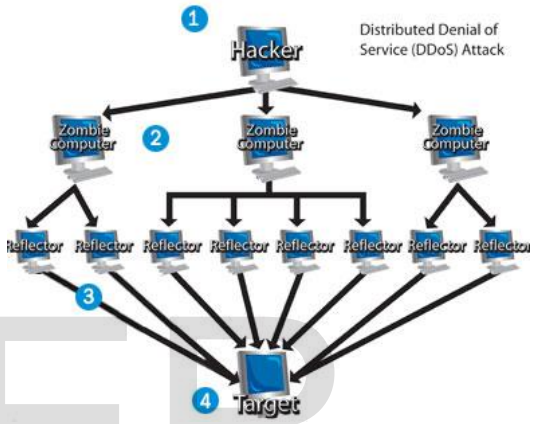


Figure 4 Distributed Denial of Service

### *2.4 IP address Spoofing*

This is an external attack in this type of attack the attacker hide their original IP address and use the false IP address for communication in the network he will use the valid IP address which server can be verified this address will be got through IP address stealing technique. In each blow, a complete diagram is provided for a better understanding of IP address spoofing through the trusted host. This address will be used for any communication and the server consider that this is the original client and send and receive data to this IP address [15].

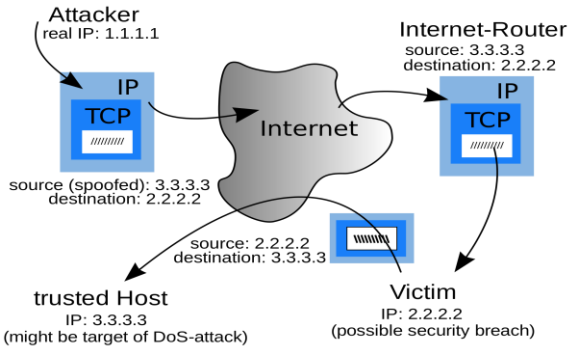


Figure 5 IP address Spoofing

### *2.5 Man in the middle attack*

This is another external attack in which a hacker gets the IP of the client and then communicates with a server to show itself as a client. The server did not recognize the hacker and thinks that this is an original user and sends data to that fake client. The attacker gets the message from the server and after reading this massage modify this and send it to the original user through this attacker can hijack the communication between two people. This is very harming for communication because the hacker can steal the IP of the one person and then watch all the communication silently. The attacker will be able to read the massage also can modify them and get the required information which he needs. [16]

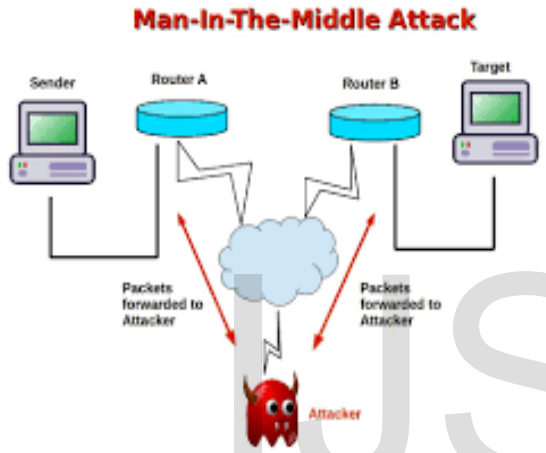


Figure 6 Man in the middle attack

In this attack the hacker will steal the IP address of the client which communicate with other person or server after get the IP address he will claim this address and show just like the original client he will also use IP spoofing for that to make a fake address that likes to the original client address and communicate with server as the client watch the whole activity get the information which he required.[17]

### *2.6 Application layer attack*

This is another type of network attack in these types of the attack mostly the attacker or the hacker can target the application program on the server. For that, the attacker needs a mechanism that will create fault to the software that was used for the server side. If an attacker does this task Successful and creates a bug in server-side software, then he will be able to get control of the system and create many problems. The attacker will get the administrator rights and can delete application accessing also be able to put a virus in the application, he can even destroy the whole operating system, the attacker can put a sniffer on the network to access the network traffic. This is a very alarming situation for the network administrator.[18]

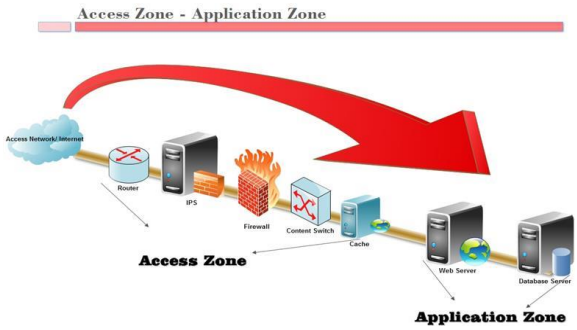


Figure 7 Application layer attack

### *2.7 Virus*

A very common and general type of computer malicious program is a virus. A computer virus can be an executable program that attaches itself with the host application. In these days we mostly used an antivirus program to clean the computer or network form viruses. As we know a virus is an executable program it very harms because it is spread when the host object executes. After this virus looks for any other object which can work itself as a carrier, after searching a carrier virus attach itself to the carrier and in this way, virus spread from one file to another. A virus has also been able to attach itself with any movable media like USB drives, floppy discs, CDs and many other such devices. Through these devices, it can spread one to another computer locally or through the internet widely [19].


Figure 8 Virus

### *2.8 Compromised Key attack*

In this attack, the attacker can get the secret key of the encrypted data that was encrypted by the sender. This is very hard to get the secret key because there are different and various key the algorithm is also different that way the secret key is not easy to get but some attacker can get this if they get the secret key then they can easily decrypt the ciphertext and get all required information from this plain text. If we send encrypted message then hacker will not be able to read this

message because this will be a binary format no one can read this massage until to decrypted this message into pain text for that we need secret key this attack will have happened when the key will be break or attack get the secret key [20] this is also called compromised key.

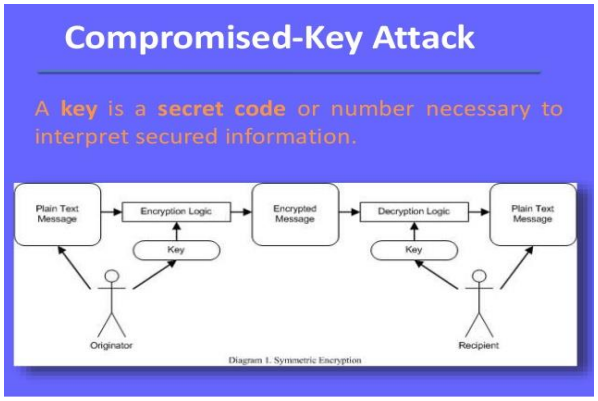


Figure 9 Compromised Key Attack

### *2.8 Rootkits*

This is another dangerous program that is very harmful it will take the administrator right from the system and hijack the complete system. These programs can hide from malware and antivirus systems that way they not detection form them because every Rootkits detector program can detect the specific Rootkit for which it is made to detect it. So, it's too much hard to detect them even it is impossible to find them through antivirus or other tools if they not detected so it's hard to destroy or remove them [21].

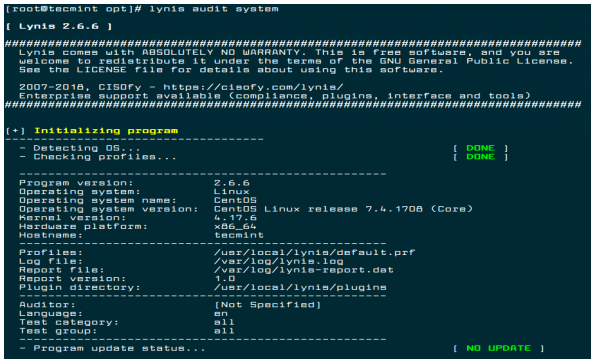


Figure 10 Rootkits

### *2.10 Trojan Horse*

In computer science, Trojan horse is very common, and every computer user almost familiar with them. This type of software shows that this is a useful software use the name or tag of the well know the software but acutely this is a different type of virus that is very harmful and creates many problems for the user. This is not like the computer virus and does not work like a virus, it has no ability to republic itself but virus can republic itself however it can be very dangerous because some Trojan Horses have so powerful and they have the ability to delete system file after delete the main system file it will take the name of said file and hide themselves in system file so it not be detected by any ordinary antivirus we need handwork to find them it can harm computer data or application data or both. Downloader is also the type of Trojan horse this is also very dangerous for the network user. This is an apparently small downloadable program. when the user clicks on it to download it starts downloading, even bigger program (Trojan horse) which can be very harmful to the victim or host computer.[22]

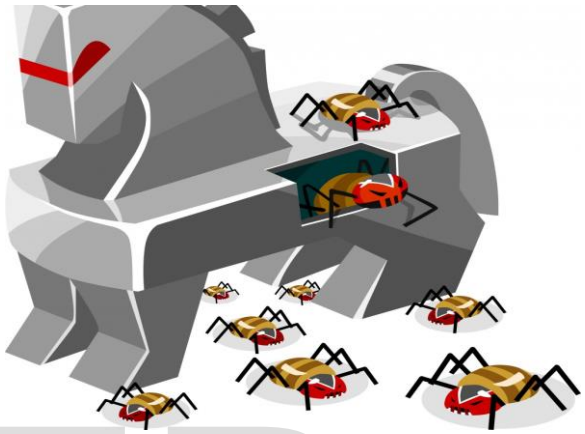

Figure 11 Trojan Horse

### *2.11 Worms*

This is another type of malicious program. It is different from the virus in a way but mostly it is the same as the virus. This type of program does not need anything to transfer from one place to another. A worm is batter then virus and has an advantage over virus due to that the worm can more easily use network services then virus so it can spread faster as compare to virus Mostly worms spread through email facility. Usually, worms use the network to transmit copies of the original code to other computers present on the network. These worms are harmful to network security [23]. Direct propagation is also the type of worms they have very fast and active spreading nature. They could jump from one computer to another within a few secs they move so fast normally they more through mail or jump from one to another computer within the network in the fraction of seconds.

Figure 12 Worms

### *2.12 Logic Bomb*

This is again virus type; logic Bomb is also working like a virus, but it is not do anything just keep silent and executed on a specific time or by doing a specific action. When they execute this will work, like a Trojan horse or virus.[24]

An attacker or hacker will use this logic bomb to blackmail the user or any company as know already aware of the loss of logic bomb so the attack demand to pay money otherwise the destroy the whole network.

We can call them as time bomb but there is a difference between time bomb and logic bomb as the time bomb can only execute on a predefined specific time, on the other hand, the logic bomb can be executed on specific day and time also when we click or do some action or open it.

Figure 13 Logic Bomb

### *2.13 Spyware*

This is the most common type of malicious program that is very harmful to a computer. These types of programs do not do any action just stealthily monitors the activities get the information and sends this information to the hacker or attacker. Another kind of spyware called camera spyware this spyware is so dangerous because they have the ability to turn on user camera without user permission and without user knowledge they can also use the microphone without permission and record the data then send it to the attacker silently.


Figure 14 Spyware

A keystroke logger is another type of spyware. That is also a very dangerous program present on the host computer. It will be able to store all pressed key records and send it to the hacker through that the attacker will get very sensitive information including the user personal pin code or any other codes. The attacker wills easily hacker the user accounts through this information. In this way, a keystroke logger can steal our password and other secret information. One spyware is more critically that is used by the hacker to get the account information for the user. They will develop the same interface and during the use of any social media account a message display you have logged out to get continue login again in this way the attacker will send the user on fake page where he/she put is username and password this information is saved by hacker page and they can easily get access or hack these account [25].

Another kind of spyware called data mining spyware works like the keystroke logger spyware. It searches for the data present on the hard disk of the victim computer. If the found such data during the searching the send it to the attacker.

## III. SOCIAL ENGINEERING

This is a technique that is used by the attacker for convincing the user to do such a task which goes in favor of the attacker. Some simple users can easily be trapped by such this.

In social Engineering, a malware program is presented to the user and presented in a good form which the user cannot refuse him for opening this software by the press or click to open this program. When a user clicks on this program the behind hide virus will be active and automatically start work to harm the computer.

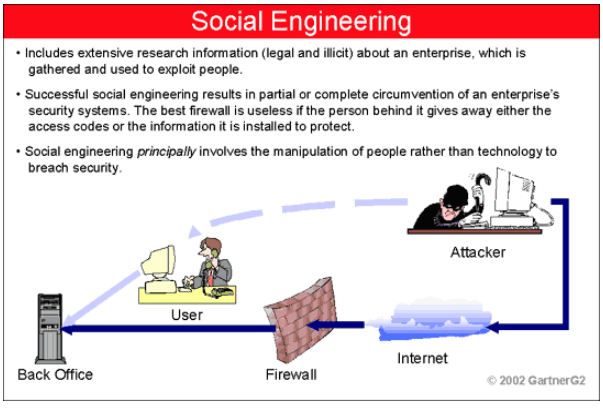


Figure 15 Social Engineering

This is a type of attack is very different from the other attacks and it is also very difficult to overcome without any safety measure.

We can overcome the dangerous results of these attacks. Until we adopt some safety measure otherwise this attack will not overcome these safety measures provide us a shield from network security threats.

We have used much time of security measures to overcome this attack this security measure include human, technical or mix of both

## IV. SAFETY MEASURES

After a complete go through network attacks now we discuss the safety measures against these attacks.

### *4.1 Security Measure Against Internal Attacks*

Firstly, we discuss the security measure against the internal attacks

Internal security attacks are very difficult to overcome because it is not possible for a company or organization to check and balance of the all staff member, what person do such actives but we have defined rules for employees and sickly fellow these rules through that a company can minimize the chance of the internal attack.

- The company should define a strong policy against any fraud case.
- The company should be strict checks and balance over the workers of an organization. Most companies do not check and balance to their employee's activities
- Whenever a company need new staff and want to appoint new staff at that time the organization focus to find an honest, well reputed and hard worker and give perfectness to them
- It is clear to all employees that we have zero tolerance policy against any fraud.
- The criminal record of any person should check before the appointment of any new staff member checked the criminal record of the said person if he/she will involve such activates the job will not offer [26]

If an organization follows these safety measures it is believed that committing fraud by staff will be minimized. It is also the duty of organizations that honest and hardworking staff should not affect by these strict policies.

### *4.2 Safety Measures Against External Attack*

As we know when data is traveling over the network it is not secure until if we do not use safety measures against malware programs present over the network. We can avoid external attacks by using an updated antivirus. If we used old dated antivirus it will not catch the viruses and malware so antivirus programs should be updated.

To avoid external network security attack or minimized if we have used a method that is called should encryption. The encryption provides more security of the data as it will convert the data into ciphertext that was not be understandable to any person until we must decode it through the decryption method. The encryption has two types one is called symmetric encryption and the 2nd one is called asymmetric we have also used a Hybrid Encryption Schemes that is the combination of the both [26].

These encryption schemes provide integrity authentication and authorization of the data.

In case we face the have the threat of spoofing attack then we need a strong mechanism for the checking of data authentication, here we don't use our security password in plaintext section, there should be a Secure Sockets Layer. This layer provides our data security against cookies' abuse. In that way, cookies will not save the data about the username and passwords [27].

If we want to stop the danger of sniffing attack, we should encrypt our data completely and enforce authentication service on both sides. If we have faced a problem that someone modifies our data or tampering with our data then we updated our authorization mechanism strong to avoid this problem, also used a strong hashing algorithm, the best way to the used digital signature that will be used as a guarantee of the original data receiving. More ever if some person send data and denies that he/ she will not send data this problem is also be solved by digital signature through that any person is not denies

Denial of service attack is a big issue for any organization or website, it is very difficult to overcome such kinds of attack, yet we could minimize the risk of attack if we applied TCP/IP protocol in such way. If we do this we minimize the such attack as we aware that it is very harder for the attacker to break that layer, we should have a mechanism to decrease the connection establish period we can minimize the denial of service attack to zero levels if there is a mechanism that ensures that connection queue will not be worn out [28]

Password cracking is another network issue that can be very dangerous for the security of data. If the password is crack all the sensitive information will be a lake to overcome this issue we should always use a long and strong password that cannot be guessed by any person we should use upper case and small case latter with special symbol that makes password more secure which cannot be broken by an attacker or hacker. If our password length is small there is more chance of stealing passwords over the network. A long password can increase the work of the attacker.

All the security measures that we discuss very important in the security of the network. it is an alarming fact that attacks on the network are increasing with the passage of time. Having all encryption schemes and antivirus programs, we are unable to stop all the attacks on the network. But these

security measures do provide any guarantee that our network is safe from attack. Hacker is always waiting to find the hole of the network security whenever they got, they might be doing many attacks until they get there required data, so we need to always be active for said attacks and ready for overcoming them.

## *V. DISCUSSION*

In these days we are living in such an environment where we not secure, in this threat environment we must face many problems while sending data over the internet. It is very difficult to overcome these threats or attacks whenever we have not used any safety measure. Although the above-discussed mattes do not cover the whole of the threat environment a common user faces these kinds of threats on the network. We can escape from the attacks if we adopt some safety measure when we send data through the internet [28]

To minimize these security threats, we must adopt many safety measures for the safety of our data and network. The network security measures can be of many types. These security measures can be technical, human or mixture of technical and human.

These threats are two types they can be internal and external. Internal security threats are the threats that within the organization or company this type of threats normally an organization can face due to the employees and ex-employees because they know all the information about the network security system and they know the weakness and hole of the company. It is very difficult to overcome these internal threats because a company or an organization must trust its workers to keep the business running. To minimize the threats, we should define rules and before appointment new staff verify all the records of that person It is clear to all employees that we have zero tolerance policy against any fraud [29].
The criminal record of any person should be checked before the appointment of any new staff member checked the criminal record of the said person if he/she will involve such activates the job will not offer

We have different safety measures to overcome these threats. For example, we have a variety of utility and antivirus programs. While traveling over the network we use many encryption schemes to protect our data from attackers and hackers.

On the other hand, external security threats are very common over the network. These threats can be launched by the attacker or hacker. These threats are of different kinds. Like the man in the middle attack, password stealing, session hijacking, sniffing and spoofing. Another major kind of external security threat is a denial of service attack [30].

As it discusses before that, we use many antivirus programs to save our computer from malicious programs and while sending our data over the network we use many encryption schemes but after doing all this, our network is not secure so far. While browsing the website on the internet we may have a virus attack, or any Trojan horse can enter our system without our information [30]. This is not a secure environment; this is not the environment for which we are struggling and wasting our time and money on it. We should have to adopt some new mechanism to overcome the abuse of network attacks and we should also create some strong antivirus programs which should have the ability to change their behavior dynamically according to the nature of the virus or any other malicious program.

We should always use try encryption scheme to send any data over the internet which are so strong that it is impossible for an attacker or hacker to breach our security mechanism. Any our key should be saved in a safe place where no one can get this.

But this is the imaginary world I am talking. So far, we have no such mechanism to adopt so we should take care while searching on the internet or while sending our data over the network. We should use available anti-malicious programs so efficiently that there is no chance of a virus attack on our system.[31]

## *VI. CONCLUSION*

After providing an overall overview of the networks attacks also provide the batter methodologies for said attacks. I would not say that our whole network is not secure. Internet has many advantages but nowadays it is not good for sharing sensitive information so far, we almost spend lack of time and money for the security of our network because we want a secure system in which our data will not be readable by any unauthorized person but hackers and attackers are so fast they also spend too many resources and energy to find any security hole of our network though that they get access to our network to get the required information,. Although our network security measures are very efficient and strong yet there are many gaps and holes between them. I am not saying that our whole network is not secure, but it is possibilities that approximately 70 to 80 not secure maybe it will 90 to 100%.In these days should be used security technique for secure brows otherwise we should face many problems including financial and loss of private data. In case we are using a wireless network 0f any public network then it must be required to use a network security key. The admin of the network just login to complete the task after that he should not rain login, whenever task completed, he should immediately logout from the network.

In a local or a small network, we always should be used and run the antivirus program on every computer that is linked with this network. If we just run an antivirus on a server the virus will not be permanently

removed from the network, through scan all Pc we keep the virus out of the network. In case we need to share our internet then should be used router it will provide better security form attacker.

In network always update the system and used a register antivirus and regularly scan all the computers in the network to avoid the internal and external attacks.

## *VII. FUTURE RESEARCH DIRECTIONS*

This paper covers various types of attacks and overcomes mythologies for the security of the network yet there need more research because many weakness and security holes are still there. It is need of the few days to be work on that topic and find the best algorithm and protocols that will be used to overcome these threats provides such architecture, algorithms, security protocols, and advanced research

In these days most challenging network threats are Denial of Service Attack and the 2nd most important challenging is Distributed Denial of Service Attack. These threats are an open challenge for researchers and programs. It is the need of the hour to accept these challenges and try to overcome the threats faced by network users.

### *Author biographical statements*

**Muhammad Saleem**: Received bachelor's degree in computer science from UOS, in 2016 received Master of computer science degree from Virtual University of Pakistan and started Master of Sciences in Computer Science. His area of interest Ad-hoc network, and research on vehicle ad- hoc network.

**Mufeeza Manzoor**: Received BSIT degree form GCWUF and started MSCS form Comsats University Islamabad, Experience as Lecturer in UOS.

**Mirza Naveed Jahangeer Baig**: Received degree MS in Mathematics from Virtual University of Pakistan. Recently working as Teacher in Govt High School Feroz Pur Chishtian Pakpattan.

**M.Tahir Usman**: Received MPhil in Mathematics from The University of Lahore, working as Teacher in Govt High School Feroz Pur Chishtian Pakpattan.

**Saba Akram**: Received BSCS form Virtual University of Pakistan. In 2019 received MSCS degree form Virtual University of Pakistan.

**Saira Khursheed**: Received MIT from Virtual University of Pakistan, doing MSCS specialization in Software Engineering from Virtual University of Pakistan.

## *REFERENCES*

[1] Gupta, Ayasha Malik1 Vishal. "Comprehensive survey on Blackhole attack with various Detection/Prevention techniques in Ad-hoc network." *International Journal of Applied Engineering Research* 14.8 (2019): 2009-2017.

[2] Gupta, Neha, et al. "DDoS attack algorithm using ICMP flood." *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, 2016.

[3] Rosso, Martin, et al. "An Attack Simulation Methodology for Empirical SOC Performance Evaluation." (2019).

[4] Varol, Nurhayat, Ahmet Furkan Aydogan, and Asaf Varol. "Cyber-attacks targeting Android cellphones." *2017 5th International Symposium on Digital Forensic and Security (ISDFS)*. IEEE, 2017.

[5] Arjuman, Navaneethan C., Selvakumar Manickam, and Shankar Karuppayah. "Lightweight Secure Router Discovery Mechanism To Overcome DOS Attack In IPv6 Network." *International Journal of Computing and Digital Systems* 8.02 (2019): 179-187.

[6] Aslam, Abida, et al. "Analysis of Network layer attacks and their solutions in MANET." *INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY SCIENCES AND ENGINEERING* 8.1 (2017): p1-4.

[7] Singh, Pranav Kumar, et al. "Impact of Security Attacks on Cooperative Driving Use Case: CACC Platooning." *TENCON 2018-2018 IEEE Region 10 Conference*. IEEE, 2018.

[8] Wang, Qian, et al. "DoS attacks and countermeasures on network devices." *2017 26th Wireless and Optical Communication Conference (WOCC)*. IEEE, 2017.

[9] Sardana, Anjali, et al. "Black hole attack's effect mobile ad-hoc networks (MANET)." *2015 International Conference on Advances in Computer Engineering and Applications*. IEEE, 2015.

[10] Swami, Rochak, Mayank Dave, and Virender Ranga. "Software-defined Networking-based

DDoS Defense Mechanisms." *ACM Computing Surveys (CSUR)* 52.2 (2019): 28.

[11] Radlein, Anton Stephen, et al. "Identifying sources of network attacks." U.S. Patent No. 9,794,281. 17 Oct. 2017.

[12] Prasad, Ramjee, and Vandana Rohokale. "Cyber Threats and Attack Overview." *Cyber Security: The Lifeline of Information and Communication Technology*. Springer, Cham, 2020. 15-31.

[13] Yaar, A., Perrig, A., and Song, D. (2003). Pi: a path identification mechanism to defend against DoS attacks. Proceedings of IEEE Symposium on Security and Privacy.

[14] Haque, Muhammad Reazul, et al. "DDos attack monitoring using smart controller placement in software defined networking architecture." *Computational Science and Technology*. Springer, Singapore, 2019. 195-203.

[15] Harvey, Elaine, and Matthew Walnock. "Spoofing detection for a wireless system." U.S. Patent No. 10,320,840. 11 Jun. 2019.

[16] Rahim, Robbi. "Man-in-the-middle-attack prevention using interlock protocol method." *ARPN J. Eng. Appl. Sci* 12.22 (2017): 6483-6487.

[17] Venkatraman, K., J. Vijay Daniel, and G. Murugaboopathi. "Various attacks in wireless sensor network: Survey." *International Journal of Soft Computing and Engineering (IJSCE)* 3.1 (2013): 208-212.

[18] Singh, Karanpreet, Paramvir Singh, and Krishan Kumar. "Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges." *Computers & security* 65 (2017): 344-372.

[19] Avram, Traian, Seungchan Oh, and Salim Hariri. "Analyzing attacks in wireless ad hoc network with self-organizing maps." *Fifth Annual Conference on Communication Networks and Services Research (CNSR'07)*. IEEE, 2007.

[20] Lopez Becerra, José Miguel, et al. "An offline dictionary attack against zkPAKE protocol." *An offline dictionary attack against zkPAKE protocol* (2019).

[21] Matrosov, Alex, Eugene Rodionov, and Sergey Bratus. *Rootkits and bootkits: reversing modern malware and next generation threats*. No Starch Press, 2019.

[22] Stallings, William, et al. *Computer security: principles and practice*. Upper Saddle River (NJ: Pearson Education, 2012.

[23] Fayssal, Samer, Salim Hariri, and Youssif Al-Nashif. "Anomaly-based behavior analysis of wireless network security." *2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous)*. IEEE, 2007.

[24] Xiao, Yang, et al. "Wireless network security." (2009): 532434.

[25] Nanz, Sebastian, and Chris Hankin. "A framework for security analysis of mobile wireless networks." *Theoretical Computer Science* 367.1-2 (2006): 203-227.

[26] Guo, Rui. "Survey on WiFi infrastructure attacks." *International Journal of Wireless and Mobile Computing* 16.2 (2019): 97-101.

[27] Anwar, Ahmed H., et al. "Pinball attacks against Dynamic Channel assignment in wireless networks." *Computer Communications* 140 (2019): 23-37.

[28] Mookiah, Prathaban, et al. "Reconfigurable antenna-based solutions for device authentication and intrusion detection in wireless networks." U.S. Patent No. 10,178,124. 8 Jan. 2019.

[29] Balakrishnan, Sarankumar, et al. "Physical Layer Identification based on Spatial-temporal Beam Features for Millimeter Wave Wireless Networks." *arXiv preprint arXiv:1902.03649* (2019).

[30] Sultana, Najiya. "A Framework of Wireless Network Security Threats: Solution for Various Information Security Problems." (2019).

[31] Fadele, Alaba Ayotunde, et al. "A novel countermeasure technique for reactive jamming attack in internet of things." *Multimedia Tools and Applications* 78.21 (2019): 29899-29920.