TCP/IP Network Protocols- Security Threats, Flaws and Defense Methods

Manan Shah VishwaSoniHarshal Shah Meghav Desai
B.E. EXTC, D.J. Sanghvicollege B.E. EXTC, D.J. Sanghvi college B.E. EXTC, D.J. Sanghvi college B.E. EXTC, D.J. Sanghvi college
Mumbai, India Mumbai, India Mumbai, India Mumbai, India
Emai id: Emai id: Emai id: Emai id:
mananshah10595@gmail.comvishwasoni_21@yahoo.inharshal_shah7@yahoo.commeghav4495@gmail.com

Abstract – **Nowadays with the very mention of usage of internet, it is but understood that it is implemented, connected and run using TCP/IP reference architecture. The internet, since its invention has evolved boundlessly. There are no units to measure the growth of the internet over the last two decades. From being a small area of interests for a few researchers Internet has evolved to become a mammoth resource of information and data connecting the entire world. The internet was allowed to grow so much because of the innumerable benefits it reaped for us. However, what one cannot ignore is the fact the internet can, has and will be used for malicious purposes also. The TCP/IP protocols which were established in the initial days of the small internet, now seriously lack the necessary security features needed in an insecure network connection. In this paper we talk about a few popular attacks which can be harmful for a TCP/IP protocol based internet connection. Also we discussed some of the flaws which aid these attacks to be successfully implemented. With each of these attacks and flaws, we provide a possible defense method that can be used to prevent or avoid such attacks.**

NOMENCLATURE

TCP/IP – Transport Control Protocol/ Internet Protocol

I. INTRODUCTION

Intially the TCP/IP protocol suite was first implemented by the Defense Department of the USA military. At that time the internet was limited and small. The TCP/IP protocol was able to provide the required security. However, with time, the internet was grown at an exponential rate. But the TCP/IP layer has not been changed or upgraded much since its initial implementation. Thus today, the TCP/IP protocol is not safe and immune to attack. It is considered to be an insecure protocol and the hosts which are part of the shared network which are based on this protocol suite are vulnerable to attacks, which can cause a great amount of damage.

II. TCP/IP Protocols by Layers

A. Application Layer

Some of the important protocols defined in the application layer of the TCP/IP suite are mentioned below. These protocols are involved in the efficient working of the application layer as a whole.

FTP is File Transfer Protocol which is used to copy a file from one host to another by using aa login Id. Control and Data information are sent separately from host PC to the remote PC.
TFTP is Trivial File Transfer Protocol and its function is same as FTP except that, it doesn't require a login ID and also the control and data information are sent together.
SMTP is Simple Mail Transfer Protocol which is used for sending a mail via the internet by defining MTA client and server.
HTTP or Hyper Text Transfer Protocol 's main function is to access the WWW. Other important protocols of this layer are DHCP, BGP, EGP, IGP, RIP, OSPF, POP3, IMAP4, Telnet, etc.

B. Transport Layer

Some of the important protocols defined in the application layer of the TCP/IP suite are mentioned below. These protocols are involved in the efficient working of the application layer as a whole.
FTP is File Transfer Protocol which is used to copy a file from one host to another by using aa login Id. Control and Data information are sent separately from host PC to the remote PC.
TFTP is Trivial File Transfer Protocol and its function is same as FTP except that, it doesn't require a login ID and also the control and data information are sent together.
SMTP is Simple Mail Transfer Protocol which is used for sending a mail via the internet by defining MTA client and server.
HTTP or Hyper Text Transfer Protocol 's main function is to access the WWW.

ther important protocols of this layer are DHCP, BGP, EGP, IGP, RIP, OSPF, POP3, IMAP4, Telnet, etc.

C.Internet Layer

The internet layer is responsible for holding the entire architecture of the TCP/IP model together. Internetworking, addressing, routing, packetizing and fragmentation of data are some of the important functions of this layer.

978-9-3805-4421-2/16/$31.00

Address Resolution Protocol (ARP) is defined by RFC 826. It packages data into Ethernet packages and is used to define ethernet address from a specific IP address.

IP or the Internet Protocol is the most important protocol of this layer. It is a connectionless datagram protocol and is unreliable. But it can still detect the errors and discard the corrupt packets.

RARP is Reverse Address Resolution Protocol function, as the name suggests is somewhat reverse of the function of ARP. In a diskless workstation, sometimes we have to obtain the IP address corresponding to a given MAC address. This is done by RARP.

D. Host to Network Layer

The host to network layer is placed at the lowest position in the TCP/IP architecture below the Network layer. It deals with the actual transfer of data and transmission rates, conversion to bits , bit rate, etc are some of the important operations carried out by this player. Some of the important protocols of this layer are

- SLIP or Serial Line Internet Protocol using which packets are placed into data frames.
- CSLIP is compressed SLIP used for data compression
- PPP which is Point to Point Protocol is an upgradation of SLIP.

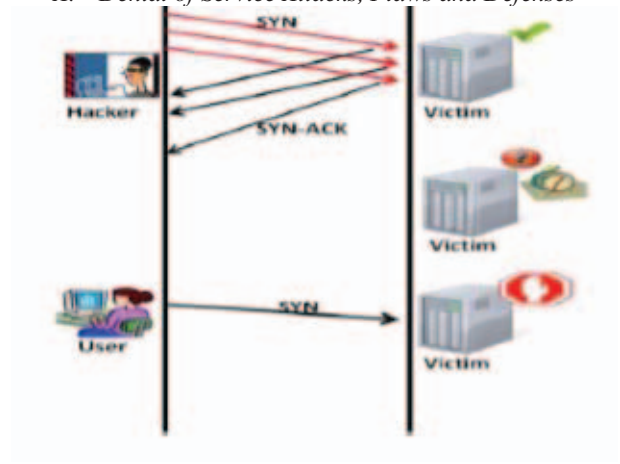
Ethernet- Ethernet is not a protocol and there are many types of ethernet. But the most common ethernet is used to control the handling of data at the lowest layer of the network model is 802.3 ethernet. 802.3 ethernet provides a means of encapsulating data frames to be sent between computers. It specifies how network data collisions are handled along with hardware addressing of network cards.[2]

III. ATTACKS

The TCP/IP protocol suite[3][4], which is very widely used today, was developed under the sponsorship of the Department of Defense. Despite that, there are a number of serious security flaws inherent in the protocols. Some of these flaws exist because hosts rely on IP source address for authentication; the Berkeley "*r*-utilities"[5] are a notable example. Others exist because network control mechanisms, and in particular routing protocols, have minimal or non-existent authentication.When describing such attacks, our basic assumption is that the attacker has more or less complete control over some machine connected to the Internet. This may be due to flaws in that machine's own protection mechanisms, or it may be because that machine is a microcomputer, and inherently unprotected. Indeed, the attacker may even be a rogue system administrator.[6]

Some of the most important attacks are described below. Also the flaws which facilitate these attacks and the defense methods that can be used to prevent such attacks are described in brief.

A. Denial of Service Attacks, Flaws and Defenses



a.

Fig. 1. Three way handshake. [7]

The three way handshake, which is an important feature of the TCP/IP oriented connections is a major flaw of which advantage is taken by SYN flooding, which is a type of DoS attack.

For establishing a connection between a client and a server, the process is that the client first sends a request message to the server to authenticate it and the server it turns sends back an acknowledgement message stating its approval to authentication. Only after this approval, the client is allowed on the server. In denial of service attack the hacker or the hijacking device connected to the internet, sends multiple requests to the server in a continuous manner. The return address of these requests are false and forged so when the server tries to approve the client, it is never actually able to find the client. After waiting for sometime (75 seconds in most cases) and the close the connection. When this happens i.e. when the server closes the connection the hijacking client again repeats the process of continuously sending fake requests. Because of this the server again goes through the same process and because of which the server is typed up indefinitely.

Denial of Service attack (Dos) is an action that prevents or impairs the authorized use of networks, systems or applications by exhausting resources such as central processing units (CPUs), memory bandwidth and disk space[8]. The DoS is typically capable of overloading or crashing the entire system network handling software and this it does, as mentioned above, by sending a specific type of data packets to utilize all the memory resources of the server. Hackers have been carrying out DDoS for more than a decade (400 M/s in 2002 100GB/s in 2010). CSI Computer and Security Survey states that 17%of respondents experienced some form of DoS attack in the year 2010. [9][10]

EXAMPLE OF DoS ATTACK IN ESTONIA IN 2007

From 27th of april until the 18th of may, Estonia a known Internet pioneer, was victim of probably the world's biggest DDoS attack ever[9][11]. The in general not very good relationship between Estonians and Russians escalated into a cyber-war after the removal of the Red Army monument 'Bronze Soldier' from a central place in Tallinn to a military cemetery(on 27th). While the monument is supposed to generally remind the people fallen in WW2, for Russians it is alsoa symbol for- embassy in Moscow has been besieged, and a 19 year old Russian Demonstrator has died.

Attack details

According to NAZARIO from Arbor Netwokrs, 128 unique DDoS attacks on Estonian websites were registered. " Of these 115 were ICMP floods, 4 were TCP SYN floods, and 9 were generic traffic floods. Attacks were not distributed uniformly, with some sites seeing more attacks than others."[12]

Defenses

As a way to avoid the Dos attack, one can implement a filter or a sniffer to block such attacks. Before a stream of data reaches a server on a network it will go through this filter and if it is a continuous request of forged addresses it will be blocked by the filter and thus protecting the server from the attack. The filters keeps looking for a pattern in the incoming stream of data or requests. If this pattern is observed to be coming in frequently to be accepted by the server, the filter will block all the messages and requests containing such a pattern. This is how a DoS attack can be prevented. [16]

2.1 Packet Sniffing Attack

Attack and Flaws

Packet sniffing can be considered as one of the most dangerous attacks on a network system as it enables the hacking device to intercept and read all the data that is being transmitted from a client to a server over a shared network via internet. This attack is achieved in a shared network connection. One might argue, that, when a shared network is not immune to this threat, why to use a shared network at all. The answer is simple, implemented a direct and dedicated network from a client to server over the internet is simple too expensive and because of the number of users connected by the internet, the idea is too complicated and almost unimaginable to implement. . Sharing means that computers can receive information that was intended for other machines. To capture the information going over the network is called sniffing.[16] A shared network connection is made using Ethernet which works by sending data to all the computers connected to the host in the shared network. The data has a header which contains the address of the destination host. Only this host is able to receive and read this data. However, a host can be implemented in promiscuous mode in which it can read and receive all the data which is sent over in the shared Ethernet network. Configuring the device is this mode is not that difficult afterall. This is because, in the Ethernet oriented network system, the account details like the account name/number and the password are sent in plaintext i.e. they are not encrypted by using some hard- to- decode algorithm. Once the hackers gets hold of this information it can reconfigure a computer in this network in the promiscuous mode and there after it can easily access all the data packets that are being sent over the shared network. Packet sniffing can be harmful for applications which make use of protocols such as SMTP,IMAP, POP etc. By sniffing the entire actually email can be read and just imagine if important emails like your bank statements were sniffed. Even Telnet, HTTP FTP are not completely immune to this type of attack. Passwords sent over the Telnet connection, files transfers over FTP connection can all be intercepted and read by the hacker. Credit card information and other important financial transactions can be read by the hacker if this type of attack is carried out on a SQL database. Packet sniffing attack not only is harmful, because it can read all the vital information being shared across the network, but it can in a bigger scenario complement the implementation of even more serious and bigger attacks that can cause even more harm to the users, companies, banks or even governments for that matter.

Example: Packet Sniffer

A packet sniffer is a device or program that allows the user to eavesdrop on traffic traveling between networked computers. The program will capture data that is addressed to other machines, saving it for later analysis.

All information that travels across a network is sent in "packets." For example, when an email is sent from one computer to another, it is first broken up into smaller segments. Each segment has the destination address attached, the source address, and other information such as the number of packets and reassembly order. Once they arrive at the destination, the packet's headers and footers are stripped away, and the packets are reconstituted.[17] Such packet sniffers are readily and legally available all over the internet. These are mostly used for troubleshooting however a smart hacker maybe able to use these software very easily to carry out malicious activities. Packet require only three components for implementation viz. Standard network adapters, a capture filter which captures the network traffic from the wire and a buffer which is used for storing the captured frames of data by the filter. The filter filters out only the specific data which is required. Real- Time analyszer is module used in packet sniffer and also a decoder is used for protocol analysis. The sniffer works only over a shared Ethernet or a switched Ethernet network, it is a must.

Defenses

Detection of this malicious attack is very difficult and it is rarely caught.However a defesne method to this type of attack is also easily available. But even when this solution is readily available most of the users rarely implement it which in turns makes their computer vulnerable to such types of attack. Simple ignorance and lack of knowledge is what works best for the hackers in this case. Authentication schemes such as MD4 and MD5, KERBEROS, and SSH can prevent the clear text transmission of user names and passwords across a network[16] Also PGP is a public key encryption program which can avoid this attack. It can encrypt an E-mail so that it cannot be read without a tool called Privtool. Only the systems which have privtool installed in them, can decrypt the email

and read the contents of the mail. Password hashing algorithms like Windows NT's password hashing algorithmmakes our systems apparently look more safe, however this is not the true case and using of such faulty algorithms should be avoided as in reality they are actually vulnerable to this type of attack. TELNET packets bound for an NT server, for example, can be intercepted and decrypted by someone knowing the password hashing weakness.[16] Also, when it comes to detecting packet sniffers, finding out whether your connection is bugged with a sniffer or not is very simple . There are three main methods that can be used to detect a sniffer in the network .The are ping method, ARP method, DNS method. To nullify the effects of sniffers authentication, switched infrastructure, antisniffer tools and cryptography can be used.

2.2 Spoofing Attack

Attack and Flaws

Spoofing, as the name suggests means the ways in which a computer is system in the network can be footed. Spoofing is usually used for non harmful purposes, for instance for reducing the traffic in the network. However, it can and is also being used an attack. In spoofing attack the hacker is able to gain unauthorized access of another remote computer or server. Only information that the hacker needs is the IP address of a trusted port. Once the hacker knows the IP address of the remote computer, by spoofing it sends messages to that computer as if the message is being sent from a trusted port. However a prerequisite for IP spoofing is that the hacker first has to find out the IP address of a trusted port which he can then use for spoofing attack. Once he has hold of this IP address of the trusted port he can easily change and modify the packet address and spoof the receiving computer by showing as if the packet is coming from a trusted port. The computer readily accepts the packets once it sees the IP address of a trusted port.

For establishing a reliable connection in a TCP oriented connection network, three way handshake signaling is used. All that the attacker needs is to predict the initial sequence number predicted by the server. The major flaw in the LINUX kernel is that the data is allowed to be delivered to a server even before the three way handshake signal process is completed. The hackers take advantage of this flaw to attack servers. This flaw Vulnerable Linux kernels accept data segments that do not have the ACK flag set and hence the sequence number is not verified. This allows an attacker to send data over a spoofed connection without knowing the target's current or initial sequence number. Thus, an attacker cannot successfully spoof a TCP transaction to a Linux host without somehow completing the TCP handshake[16].

Basically there are two main type of IP spoofing. i.e. nonblind spoofing and blind spoofing. Non blind spoofing is used when the attacker and the host computer or the server are a part of the same subnet. The sequence and knowledgement number of the clinet and the server are sniffed by the attacker. Blind spoofing is when several data packets are being sent to the server for sampling of the sequence numbers. What actually happens here is that an attacker computer sniffs the sequence and acknowledgement number of another client(say clientA) and sends data to a server as if the client A is sending the message. Now the server sends back its responses to te actual client A. However, by prior SYN flooding client A has been discarded or made inactive in the network system. Now the attacker agains sends to the reply to the server as if the client A has received the acknowledgement message from the server and is sending the next set of messages in the sequence of data. This is how, the server is fooled into believing that it is client A with whom the server is getting the messages from and with whom it is exchanging the request and acknowledgement messages.

Defenses

Detecting an IP spoofing attack is very difficult however as a measure to stay protected from IP spoofing there are a few steps that can be taken. One of the most simple thing to do is that you should disable the Javascript, Java or ActiveX on your browser as these are known to aid this type of attack. By doing so, the attacker wont be able to hide the proof that he/she had attacked this particular host computer or server. Also you should always make sure that the browser's location line is always visible and also that URL displayed in this line is the address of the server you think you are currently connected to. Doing this, will not completely protect you or make your PC immune to spoofing attacks but however it will sure help you lower the chances of being attacked. Filtering is another way of preventing such attacks. The packets entering and leaving the network should be checked and filtered. It should be verified whether the incoming packets to a server are actually coming from the IP address that the claim to have in their packet header. Also if it is found that the outgoing message is malicious, than the packet should immediately blocked and discarded and not be allowed to leave the network. Filtering can be used not only at the server or at the client end but also at the router's end. Authentication and encryption should be used. Not just simple authentication, but cryptographic authentication techniques should be used as a countermeasure against spoofing attacks.

2.3 IP Half Scan Attack

Attack and Flaws

The most basic flaw in the TCP/IP which encourages this type of attack is the three way handshake signaling process used for establishing connection. In this attack the connection is never completely established. The client party wishing to establish a TCP connection with a server sends a packet with SYN flag on, to this the server replies with either RST or SYN and ACK flag on. It sends RST when the port is closed and sends the other two flags on when the port is open. When the server replies with the ACK and SYN flag on , the client sends back a packet with its ACK flag on. After receiving this packet, the connection is established and the client knows whether the port is listening or not. An attacker takes advantage of this flaw and learns whether which ports listen to which type of services. Often the attacker is able to pull off this information from the victim computer even without an attempt of threat even being detected by the victim. During a Stealth Scan, the client sends a RST signal instead of ACK signal as a response to the ACK

signal of the server. This ends the connection. From this, the attacker is able to learn that a particular service is listening on a particular port without actually establishing a connection with the target machine.[7]. By this attack is possible threat is put on the target server in the sense that the attacker is able to gain the information about the target server computer. This information than encourages future threats as it can be used to implement other types malicious attacks on that server.

Defenses

The IP Half Scan attack is not as malicious as spoofing, sniffing or Dos. A variety of countermeasures to avoid this attack are widely available in the market. Using a firewall is one of the most popular ways of avoiding this attack. The firewall can read the current status of the TCP connection and avoid or block malicious packets. Sniffers, they are available online, can be used to see and read the status of the traffic. If the traffic is not behaving as being reported, there are chances that the device has been attacked. Netmon is a type a sniffer which is available over the internet. Detecting and solving the problem of IP half scan is comparatively easy to deal with.

If you get a warning from your TMG server which reads something like this- **'Forefront TMG detected a possible Internet Protocol (IP) half-scan attack from IP address 192.168.1.89.' then** log the address from which the scan occurs. If appropriate, configure the ISA Server policy rules or Internet Protocol (IP) packet filters to block traffic from the source of the scans.[15]

IV. TRIVIAL ATTACKS

Unlike the above mentioned attacks, some attacks are not that serious a threat when it comes to the level of harm that they can cause. However they are also not that trivial that they can be completed ignored and not considered at all. Here are some

3.1 Vulnerability of the Local Network [19]

The Ethernet networks, and other similar LANs are not immune to eavesdropping and spoofing. This is because of the lack of many important security features and also the implementation flaws of which benefit is taken by the attacker. In general access to other computer systems should be rejected because. Access shall only be granted to trusted and authorized systems with cryptographic authentication asking for a password which shall be known only to a trusted client. Even if the attacker is not able to edit the information in the traffic in the channel over which the data is being sent, it can still read the information and use to for later purposes. DoS and other malicious attacks which need some prior information about the data being sent or the system sending or receiving the data, make use of this flaw and are able to gain information about these systems. It is possible to launch DoS attacks by triggering broadcast storms. Most easy method to achieve this by storming the network with packets having fake or more over non-existent IP addresses. By doing so, each host PC in the network receives these packets and they forward it further in the network to make these packets reach the destination address. Furthermore, each host not only does forward these packets but also receives multiple copies of these packets which are forwarded by others hosts in the network. This will create a lot of congestion and traffic in the network system and the attacker and take advantage of this by broadcasting an ARP message over a network with fake IP address. The attacker then follows these packets that in turn pose a threat on the system.

3.2 Trivial FTP

The service is used to copy a file from one computer to another. Unlike, FTP there is no login Id required to gain access of a remote host from which the file is needed to be copied into the requesting host. So without any sort of authentication requirements, all the files in the host server can be copied by anyone using the internet. Obviously there are beneficial uses of this protocol, but at the same time it can be used for harmful activities as well. To avoid copying of files without authentication, i.e. for allowing only authorized users to gain access of the remote computer, FTP instead of TFTP should be used as the servicing protocol.

V. GENERAL DEFENSES

We have so far detailed out the defense countermeasures which should be taken to avoid particular attacks. But in reality implemented these countermeasures to your system may result in improper functioning of your system. For instance, when the Javascript is disabled on your browser to avoid spoofing attack, it may cause failures of some other important services provided by this function. Also implementing one type of defense method does not make your system immune to other types of attacks. So there are some common defense methods that should be implemented in your systems to lower the chances of being threatened by these attacks. Some of these countermeasures are as follows.

4.1 Authentication

Most of the authentication schemes implemented in a TCP/IP oriented network make use of IP source address for control access and login in. However as seen above, we have learnt that there are various ways of spoofing this IP address. Thus authentication alone cannot be used to avoid such threats.

A form of cryptographic authentication is needed[6]. One way to do this is to make use of keys. For authentication, each host shares its private with the host server for establishing a network connection. On receiveing this key from the client, the server sends back sealed and packets to the client for that particular session. Needham-Schroeder algorithm is one of the best known approaches used for cryptographic authentications [20][21][22]. Both public and private key sharing algorithms are available for implementing cryptographic authentication.

4.2 Encryption

Encryption techniques if employed provides an efficient defense mechanism against such attacks. However the reason that these mechanisms are not often employed that the cost of these devices is usually high and the also the systems implementing these schemes are very complex and not feasible

to be implemented by individuals users. Encrypted packets sent over a connection channel are hard to be attacked and read. To get more details in this sector, readers are recommended to consult Voydock and Kent[23] or Davies and Price[24].
There are endless encryption techniques that can be employed at different levels of the TCP/IP model. However detailing out each and every techniques it not the main concern of this paper.

4.3 Trusted Systems

The TCP/IP protocol suite was first designed for the Defense Department, so the question of whether to what extent the Orange book and the Red book criteria will be able to prevent an attacker to hijack a host system is worth asking. For instance, if a target host were rated to a particular level, could the above mentioned attacks penetrate the security system of this host. This depends on the clearance level assigned to that host. Again, for instance, a host system rated a B-2 will be able to withstand an above mentioned attack. However for a lower rated host, this cannot be guaranteed. A host system rated C-2 is surely vulnerable to all the above mentioned attacks where as B-1 ratings are still immune to some of these attacks.
Labeling a data within a host is necessary. And each process, willing to access this data should be assigned a clearance level. Let us consider an example by assuming the following details:-

a) A process with clearance level 1 shall be able to access files and data labeled as top secret, secret, confidential as well as non classified data.
b) A process with clearance level 2 shall be able to access files and data labeled as secret, confidential and non classified.
c) A process with clearance level 3 shall only be able to access files that are non classified.

According to this, a process 3 cannot and will not be able to read/write or carry out any kinds of operations on a data type labeled above its level. A process 2 cannot have any sort of access to data rated above its clearance level. i.e. it cannot work on data labeled above secret.

Another labeling system that can be implemented can be based on the following assumption:-

a) Any process labeled with any particular level of clearance can only read, write , edit or operate on a data or a file which has a clearance level exactly equivalent to the level assigned to that particular process. A file labeled above or below cannot be operated by a process which is not labeled at the exact same equivalent level.

What this does is, even if the attacker is able to hack into the host system, each a every file within has a particular label, so even if the attacker is able to access non classified or confidential level files, it is still not able to break in to the more important and highly sensitive secret and top secret files. This assures a certain threshold level of security even after the system has been attacked.
Bottom line is that, by rating systems as C-2, B-1, or B-2,etc. the sensitivity and the level of information with which the system can be trusted can be predetermined. A highly sensitive and top secret information thus should not be loaded into a C-2 rated system. A highly secure system has to be used for fulfilling this requirement.

4.4 Upgrade to a more secure protocol

Even though TCP/IP is the most widely used protocol all over the internet, from the above discussion it is safe to say that it is not the most secure one. It is vulnerable to a lot of different kinds of attacks. So upgrading to a protocol suite that assures a higher level security, even though might be considered as a futuristic approach, seem to be a wise one. IPsec is one such protocol which assures a higher level of security compared to TCP/IP suite. Even if the data in being sent over a network is obtained by an attacker, he cannot do much harm with this data, because this data is encrypted.

VI. CONCLUSIONS AND FUTURE SCOPE

We understand that TCP/IP is not the most secure type of protocol suite. However because of various reasons associated, we find that it is still the most used protocol suite all over the internet. We have discussed this in the introduction of our paper.We than talk about the overall TCP/IP reference model, its layers and the protocols in each layer of this model. The working and functioning of each of these protocols is mentioned in brief. The TCP/ IP is vulnerable to a variety of attacks. We have discussed some of these attacks in details like Denial of Service attacks, Sniffing attacks, spoofing attacks and IP half scan attack. These attacks are a threat to the networks connections based on TCP/IP suite because of various flaws and shortcomings in the protocol suite itself. We talk in brief about these attacks, the flaws that encourage these attacks and further we go on to discuss a few defense mechanisms that can be employed to prevent such malicious attacks. We make sure to mention some trivial attacks and some comprehensive defense measures that can be taken to avoid these attacks. Even though there are countermeasures available to avoid and counterfeit these attacks, we find that most of the systems connected to the internet are still insecure. These defense mechanisms are not implemented by most of the systems because of various reasons like lack of knowledge, ignorance, high cost of defense systems, high complexity, etc. It is because of these reasons that we, at the near end of this paper recommend to upgrade to a better and more secure protocol suite like IPsec. It has more security features compared to TCP/IP and the data being sent over the connection is encrypted. IPSec ensures confidentiality, integrity, and authenticity of data communications across a public network[16]. We can go on to discuss other appealing features of IPsec in detail, however it is beyond the scope of this paper.

REFERENCES

[1]. Book by Techmax Publications on 'Computer Communication Networks' by J. S. Katre (Code: ETC603)
[2]. http://www.comptechdoc.org/independent/networking/protocol/protnet.html
[3]. E.J. Feinler, O.J. Jacobsen, M.K. Stahl, C.A. Ward, eds. DDN Protocol Handbook. DDN Network
Information Center, SRI International, 1985.
[4]. Comer, D. Internetworking with TCP/IP : Principles, Protocols, and Architecture. Prentice Hall, 1988
[5]. Blum, M. and Micali, S. "How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits". SIAM J. Computing, vol. 13, no. 4, pp. 850-864, Nov. 1984.
[6]. Security Problems in the TCP/IP Protocol Suite, S.M. Bellovin* smb@ulysses.att.com
AT&T Bell Laboratories Murray Hill, New Jersey 07974.
[7]. TCP / IP Protocol Suite , Attacks and Security Tools by Aruna Tiwari*, Dr. MangleshJaiswal**, NutanVarma***,Dr. B. L. Joshi*** Computer Science And Enginerring , RKDF University Bhopal M.P.
[8]. NIST comp Security Incident Handling Guide, source: Stallings/ Brown(2012) p.244
[9]. www.slideshare.net/pfloeshel/deial-of-service-attacks
[10]. Stallings/Brown(2012). p.243 f. Risk & Security Management- DoS Attacks 09.11.2012, University of Liechtenstein
[11]. Muir &Weiss Denial of Services Attacks 2000
[12]. Details of DDoSAttakcs against Estonia
[13]. Rotzer(2007), Lischka (2007)
[14]. Rotzers (2007)
[15]. Lischka (2007), Warner (2007)
[16]. TCP/IP Protocol Possible attacks by Saleh Almanei, Mohammad Alqattan, RabahKhamis, YousafHussain.
[17]. www.wisegeek.org/what-is-a-packet-sniffer.html
[18]. https://technet.microsoft.com/en-us/library/cc722757.aspx
[19]. Security Problems in the TCP/IP Protocol Suite, S.M. Bellovin* smb@ulysses.att.com
AT&T Bell Laboratories Murray Hill, New Jersey 07974.
[20]. Needham, R.M. and Schroeder, M.D. ''Using Encryption for Authentication in Large Networks of Computers''. Communications of the ACM, vol. 21, no. 12, pp. 993-999, December 1978.
[21]. Denning, D.E. and Sacco, G.M. ''Timestamps in Key Distribution Protocols'', Communications of the ACM, vol. 24, no. 8, pp. 533-536, August 1981.
[22]. Needham, R.M. and Schroeder, M.D. ''Authentication Revisited'', Operating Systems Review, vol. 21, no. 1, p. 7, January 1987.
[23]. Voydock, V.L. and Kent, S.T. ''Security Mechanisms in High-Level Network Protocols''. ACM Computer Surveys, vol. 15, no. 2, pp. 135-171, June 1983.
[24]. Davies, D.W. and Price, W.L. Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer. Wiley. 1984.