CSE-190011

UGC & Govt. Approved
Sonargaon University (SU)
We will rise up, We will shine

147/I,Green Road, Panthapath ,Dhaka

The Role of Cyber Security in Defending Computer Networks

Submitted By

Chinmoy Krishna Bala
ID:CSE1503006015

Md.Mainul Hossain
ID:CSE1503006016

Md.Tariq Ibne Zious
ID:CSE1503006014

Mst.Kulsum Khatun
ID:CSE1503006010

Supervised By

Mst.Sabrina Tasnim
Lecturer
Department Of Computer Science & Engineering
Sonargaon University

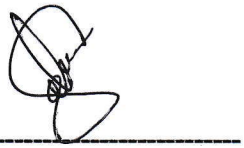
This Thesis has been submitted to the Department of the Computer Science & Engineering at Sonargaon University in the partial fulfillment of the requirement for the degree of Bachelor of Science in Computer Science and Engineering.

May, 2019

DECLARATION

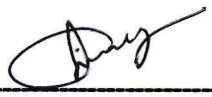
The project has been submitted to the department of the Computer Science & Engineering,Sonargaon University in the partial fulfillment of the requirement for the degree of Bachelor of CSE at Sonargaon University.we hereby declare that this project has not been submitted elsewhere for the requirement of any degree or diploma or any other purpose.

Supervised by:



Sabrina Tasnim
Lecturer
Department Of CSE
Sonargaon University

Submitted by:



Chinmoy Krishna Bala
ID:CSE1503006015



Md.Mainul Hossain
ID:CSE1503006016



Md.Tariq Ibne Zious
ID:CSE1503006014



Mst.Kulsum Khatun
ID:CSE1503006010

Letter of Acceptance

This project entitled "The role of Cyber Security Defending in Computer Networks", Submitted By Chinmoy Krishna Bala ID: CSE1503006015, MD. Mainul Hossain ID: CSE1503006016, Md.Tariq Ibne zious ID: CSE1503006014 , Mst. Kulsum Khatun ID: CSE1503006010, to the Department of Computer Science & Engineering, Sonargaon University, Dhaka Bangladesh. Has been accepted as satisfactory for the partial fulfillment of the requirement for the degree of Bachelor of Science in Computer Science & Engineering and approved as to its style and contents.

Board of Examiners

Examiner 1

Examiner 2

Examiner 3

Examiner 4

Acknowledgement

It has been great for us to thesis **"The Role of Cyber Security Defending in computer Networks"** We have gathered sufficient knowledge and experience during this thesis.

With the Name of Allah, the most effective and Merciful. We are very thankful to all anyone who has helped us in providing us support throughout carrying out our thesis. First of all, we wish to thank our supervisor Sabrina Tasnim, Lecturer, Department of CSE, Sonargaon University, who cultivated the mind with skills. who guided us to proper analysis of the system and helped to do this thesis efficient thesis. Her comments and correct feedback made us accomplish this goal. We are very grateful to him for his continuous support, advice and guidance.

Our Special thanks goes to course coordinator and entire department teachers who helped us relentlessly and we want to thank our vice chancellor sir for his moral support.

We would like to thank our entire course mate in Sonargaon University, who took part in this discuss while completing the course work.

Finally, we would like to convey my distinctive thanks to my parents whom have always given. Me tremendous support. Without their love and encouragement I would not had achieve this far.

Abstract

Communication of confidential data over the internet is becoming more frequent every day. Individuals and organizations are sending their confidential data electronically. It is also common that hackers target these networks. In current times, protecting the data, software and hardware from viruses is, now more than ever, a need and not just a concern. What you need to know about networks these days? What should we do for network security? How security is implemented to ensure a network? How is security managed? In this paper we try to address the above questions and give an idea of where we are now standing with the security of the network. By using those techniques, we can easily prevent the hacker's attack from our home and office networks.

TABLE OF CONTENTS

Chapter 1 INTRODUCTION

1.1 Motivation 1
1.2 Goal/Aim 1
1.3 Methodology 2
1.4 Literature Review 2

Chapter 2 NETWORKS AND PROTOCOLS

2.1 Network 3
2.2 The Open System Interconnected Model (OSI) 3
2.2.1 Physical Layer 4
2.2.2 Data Link Layer 4
2.2.3 Network Layer 5
2.2.4 Connection Mode 5
2.2.5 IP Addressing 5
2.2.6 Transport Layer 5
2.2.7 Session Layer 6
2.2.8 Presentation Layer 6
2.2.9 Application Layer 6
2.3 TCP/IP Protocol Suite 6
2.3.1 IGMP Protocol 7
2.3.2 Protocol 8
2.3.3 Protocol Identifier 8
2.3.4 Security Level Protocol 8
2.3.5 Internet Layer 8
2.3.6 Internet Protocol 8
2.3.7 Application Layer Protocol 9
2.3.8 SMTP Protocol 9
2.3.9 FTP Protocol 9
2.4 Source And Destination Port 9

Chapter 3 NETWORK SECURITY THREATS AND WEAKNESS

3.1 Network Security 10
3.2 Security Threats 10
3.3 Security Weakness 10
3.4 Unauthorized Access 11
3.5 Disruption Network Function 12
3.6 Common Threats 12
3.7 Errors and Omissions 12

Chapter 4 NETWORK SECURITY ATTACKS

4.1 General Categories of Security Attacks 13
4.2 Reconnaissance Attacks 15

4.3 Port Scan and Ping Sweep 16
4.4 Internet Information Queries 16
4.5 Access Attack 17
4.6 Password Attack 17
4.7 Unauthorized Modification 17
4.8 Types of Password Attack 18
4.9 Port Redirection 18
4.10 Man in the Middle Attack 18
4.11 Distributed Denial of Service (DDOS) 19
4.12 Buffer Overflow 19
4.13 Viruses and Other Malicious Program 19

Chapter 5 SECURITY COUNTERMEASURE TECHNIQUES AND TOOLS

5.1 Security Countermeasure Techniques 20
5.1.1 Security Policies 21
5.1.2 Authority Of Resources 21
5.1.3 Detect Malicious Activities 21
5.1.4 Mitigate possible attacks 21
5.1.5 Security Countermeasures Tools 21
5.1.6 Cryptography 21
5.1.7 Conventional or Symmetric Encryption 21
5.1.8 Asymmetric Algorithms 22
5.1.9 Asymmetric Key Encryption 22

Chapter 6 SECURITY SOLUTIONS

6.1 Application Level Solutions 23
6.1.1 Authentication Level 23
6.1.2 Email Level 23
6.1.3 IP Level 23
6.1.4Internet Protocol Security (IPSec) 23
6.1.5 Web Level 23
6.2 SSL/TLS 24
6.3 System Level Solutions 24
6.4 Intrusion Detection System (IDS) 24
6.4.1 Network based intrusion detection system (NIDS) 25
6.4.2 Host Based Intrusion detection system (HIDS) 25
6.4.3 Distributed intrusion detection system (DIDS) 26
6.4.4 Intrusion Prevention System (IPS) 26
6.5 Network Security Solution Steps 27
6.6 Antivirus Techniques 28
6.6.1 Antivirus Functional Technique 28
6.6.2 Generic Decryption (GD) 28
6.6.3 Digital Immune System 29

6.6.4 Behavior Blocking Software 30
6.7 Firewalls 30
6.7.1 Types of Firewalls 30
6.7.2 Packet Filter Firewall 31
6.7.3 Application Level Gateway 31
6.7.4 State full Inspection Firewall 31
6.8 Company Visit Information 32
6.9 After That Security Provide 33

Chapter 7TESTING RESULTS
7.1 Overview 34
7.3 Result 34

Chapter 8 CONCLUSION AND FUTURE WORK
8.1 Conclusion 35
8.2 Future Work 35

LIST OF FIGURE

Fig 2.1: OSI Reference Model Layer Architecture 4
Fig 2.2: Different Layers Protocols in TCP/IP suite 6
Fig 2.3: ICMP Message Encapsulation with IP Datagram 7
Fig 2.4: Transport Level Web Security 9
Fig.3.1: The number of found weakness 11
Fig.3.2: The number of reported events 11
Figure 3.3: IP Spoofing 12
Fig.4.1: Basic types of Security Attacks 14
Figure 4.3: Active Attacks 15
Table 4.4: Types of password Attacks 18
Figure 4.5: Port Redirection Attack 18
Figure 4.6: Distributed Denial of Service Attack 19
Fig 5.1: Network Lifestyle Phases 20
Figure 5.2: Asymmetric Key Encryption 22
Figure 5.3: Authentications Using Asymmetric Encryption 22
Fig 6.1: NIDS Based Network 25
Fig 6.2: HIDS Based Network 26
Fig 6.3: Network Security Solution Steps 27
Fig 6.4: Digital Immune System 29
Fig 6.5: Behavior Blocking Software Operation 30
Fig 6.6: Organization Using Security and their Collected Data 32
Fig 6.7: Gantt chart of before security level 32
Fig 6.8: Data of Security provide in organization 33
Fig 6.9: Gantt Chart Of after security provide 33

REFERENCES ..... 36 to 38

Chapter 1

INTRODUCTION

1.1 Motivation

"In this particular grow older associated with common digital online connectivity whenever globe has become a worldwide town, various risks such as infections as well as cyber-terrorist, eavesdropping as well as scams, indisputably there isn't any period where protection doesn't issue.
Unstable development within personal computers as well as systems offers elevated the actual reliance associated with each business as well as people about the info saved as well as conveyed utilizing these types of techniques. This particular results in the razor-sharp understanding of the requirement to safeguard information as well as assets in order to disclosure, to ensure the actual authenticity associated with information as well as communications, as well as safety associated with techniques through network-based attacks".

You will find people who think that protection difficulties confronted through house customers tend to be significantly over-stated, which the actual protection just worried about company computer systems which have substantial information together. And several think that just wide music group customers or even individuals with higher pace cable connections have to be regarded as.

The fact is which most of personal computers such as company types haven't any kind of risk concerning the information that they can consists of, instead these types of jeopardized techniques in many cases are employed for useful objective, for example in order to release the DDOS assault towards another systems.

Acquiring the system is really a complex work, in the past just skilled as well as competent specialists may cope with this. Nevertheless, because increasing numbers of people turn out to be irritated, there's a require associated with much more fatigued individuals who may realize the fundamentals associated with system protection globe.

Various amounts of protection work with regard to various businesses. Businesses as well as people may make sure much better protection by utilizing organized strategy which includes evaluation, style, execution as well as upkeep. The actual evaluation stage demands that you simply completely check out your whole system, each software program as well as equipment, through within as well as outdoors. This can help to determine in the event that you will find or even might be vulnerabilities. A good evaluation teaches you a definite image which what's in position these days as well as that which you may need with regard to the next day.

1.2 Goal/Aim

The primary concentrate of the dissertation is actually to generate a much better knowledge of system protection programs as well as requirements. Concentrate is going to be upon programs as well as requirements which are popular and also have already been broadly used.

1.3 Methodology

To achieve our goals, we will investigate following parameters.

- ✓ Networks and protocols
- ✓ Security threats and Weakness
- ✓ Security attacks
- ✓ Security countermeasures techniques and tools
- ✓ Security solutions
- ✓ Extracting results on the basis of simulations results.

1.4 Literature Review

Ransomware has been one of the biggest threats impacting businesses in the past two years, exploiting basic vulnerabilities including lack of network segmentation and backups, Gartner's Olyaeisaid.Today, threat actors are employing the same variants of ransomware previously used to encrypt data to ransom an organization's resources or systems to mine for cryptocurrency — a practice known as cryptojacking or cryptomining."These are strains of malware that are very similar to strains that different types of ransomware, like Petya and NotPetya, had in place, but instead it's kind of running in the background silently mining for cryptocurrency," Olyaeisaid.The rise of cryptojacking means the argument that many SMB leaders used in the past — that their business was too small to be attacked — goes out the window, Olyaei said. "You still have computers, you still have resources, you still have applications," he added. "And these application systems, computers, and resources can be used to mine for cryptocurrency. That's one of the biggest threats that we see from that standpoint. "More organizations are starting to consider where their products are based or implemented and where their data is stored, in terms of cybersecurity risks and regulations, Olyaeisaid. Base on this topic we are decide that how to prevent Ransomware attack in official sector.

Chapter 2

NETWORKS AND PROTOCOLS

With this section all of us may explain the fundamental idea of information conversation system. The actual system coating methods would be the main component inside a conversation system. This particular section consists of the actual explanation from the part associated with system coating methods inside a conversation design; additionally, it clarifies the actual practical guidelines of those methods in various degree of information conversation. These types of guidelines tend to be as process header areas. All of us may research the actual header area of those methods as well as evaluate which exactly how a good assailant may use or even alter these types of process header areas to complete his/her harmful objectives. The actual in-depth research from the framework associated with OSI coating methods & TCP/IP coating methods may execute this particular goal.

2.1 Network

The actual conversation funnel might contain any kind of bodily "wired" or even reasonable "wireless" moderate as well as associated with any kind of digital camera referred to as node.

The network consists of collection of systems connected to each other throughway

Conversation funnel. The actual attribute of the node within the system is actually which; it's its identification as its distinctive system id. Computer systems as well as ink jet printers tend to be a few of the types of nodes inside a pc system and when all of us discuss the actual telecommunication system these types of might be cell phones, hooking up systems gear as well as primary manage models.

The actual system below particular guidelines discover assets after which gives this between your nodes so which authenticity as well as protection problems tend to be assured. The primary performance associated with any kind of system would be to separate assets one of the nodes.

2.2 The Open System Interconnected Model (OSI)

Within 1997, the actual Worldwide Regular Business created a typical conversation construction with regard to heterogeneous techniques within system. According to performance associated with conversation program within open up globe, this technique is known as Open up Program Interconnection Design. The actual OSI research design supplies a construction in order to break up complicated inter- networks in to this kind of elements that may easier end up being recognized as well as employed. The objective of OSI would be to permit any kind of pc all over the world in order to contact every other, so long as each adheres to the actual OSI requirements. The actual OSI research design is actually used in to 7 amounts. Each and every degree within OSI Design offers its operating performance; these types of amounts tend to be remote however cascaded to one another and also have conversation performance inside a correct circulation in between all of them. With regards to over regular conversation construction, this particular group of levels referred to as OSI levels. Performance of every coating differs through every as well as every coating offers various degree as well as labeling.(Proven withinfig:2.1)

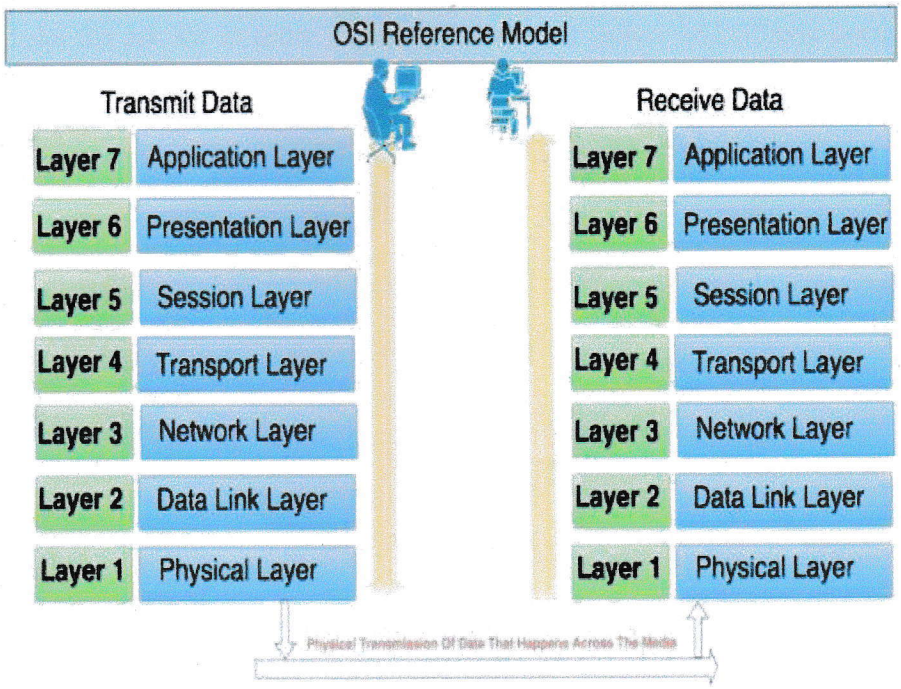


Fig 2.1: OSI Reference Model Layer Architecture

However, in the event that all of us begin to see the program structures associated with OSI, Three level of abstraction is actually clearly acknowledged; the actual structures, the actual support specs, and also the methods specs. The actual OSI support specs have the effect of particular providers in between person as well as program inside a particular coating. Parallel OSI process specs tend to be accountable which, which sort associated with process is actually operating from the particular conversation support. So, it's obvious how the mixture of both of these components turn out to be OSI program structures.

2.2.1 Physical Layer

The cheapest coating within OSI design is actually Bodily Coating; this allows for the actual online connectivity in between program user interface credit cards as well as bodily mediums. This particular coating knows as well as changes electrical/electronic indicators as pieces. In order that it administrates bodily "wire" and/or reasonable "wireless" link business between your equipment user interface credit cards as well as conversation moderate; example of physical layer standard includes RS-232, V.24 and Interfaces.

2.2.2 Data Link Layer

Within OSI Research Design the information Hyperlink Coating may be the 2nd coating. Information Hyperlink coating accounts for manage techniques which supplies correct structure associated with information also it may entry information circulation mistakes within bodily layer.

The information structure within information hyperlink coating is actually as structures. Consequently all of us state how the information hyperlink coating accounts for determining information platforms to incorporate the actual organization through which info is actually transferred. Mistake manage methods along with other hyperlink manage methods might happen within bodily coating. Such as cyclic redundancy examine; the actual mistake looking at system which operate during the time of tyranny of the body through supply aspect. Exactly the same system may operate in the location aspect when they discovered any kind of distinction following assessment after that recipient can make the ask for in order to supply in order to deliver which body once again. Information hyperlink coating accounts for subsequent support.

- **Encapsulation**
- **Frame Synchronization**
- **Logical link control(LLC)**

-Error control

-Flow control

#Collision

Detection

#Physical

Addressing

Whereas media access control is responsible for controlling the traffic congestion and physical address reorganization. The data link layer is further subdivided into two layers, Logical link Control (LLC) and Media Access Control. The logical link control is responsible for flow control and error detection in data.

2.2.3 Network Layer

The third layer in OSI Reference Model is the Network Layer. This layer is responsible to make a logical connection between source and destination. The data at this layer is in the form of packets. The network layer protocols provide the following services

2.2.4 Connection mode:

The network layer has two types of connection between source and destination, first one is known as connectionless communication which does not provide connection acknowledgement. The example of connectionless communication is Internet Protocol (IP). The second type of connection is connection- oriented which provides connection acknowledgement. TCP is an example of this connection.

2.2.5 IP Addressing:

In computer networks every node has its own unique ID. By this unique ID sender and receiver always make right connection. This is because of the functionality of network layer protocol, which has source address and destination address in their header fields. So, there is less chance of packet loss, traffic congestion and broadcasting.

2.2.6 Transport Layer

The fourth layer in OSI reference model is Transport Layer. It contains two types of protocols, first is Transport Control Protocol (TCP) which is connection-oriented protocol and supports some upper layer protocols like HTTP and SMTP. The second is User Datagram Protocol (UDP) which is a connection less protocol. Like TCP it also supports some upper layer protocols such as DNS, SNMP and FTP. The main thing in transport layer protocols is that they have port addresses in their header fields.

2.2.7 Session Layer

The fifth layer in OSI Reference Model is Session Layer. The Session Layer is responsible for session management i.e. start and end of sessions between end-user applications. It is used in applications like live TV, video conferencing, VoIP etc., in which sender establishes multiple sessions with receiver before sending the data. Session Initiation protocols (SIP) is an example.

2.2.8 Presentation Layer

The sixth layer in OSI Reference Model is Presentation Layer. This layer is responsible for presentation of transmitted/received data in graphical mode. Data compression and decompression is the main functionality of this layer. The data encryption is done before transmission in presentation layer.

2.2.9 Application Layer

The seventh and the last layer of OSI Reference Model is Application Layer. This layer organizes all system level applications like FTP, E-mail services etc.

2.3 TCP/IP Protocol Suite

The TCP/IP Protocol Suite was developed before OSI reference model. The OSI reference model consists of seven layers whereas TCP/IP protocol suite has only four layers. In comparison to OSI reference model, TCP Suite has high level of communication traffic awareness between sources to destination. The TCP/IP Suite has administrative communication controlled and reliable data processing. It has dozens of layer components and communication set of rules which provide reliable service performance and data security.

Each layer in TCP/IP suite is responsible for a specific communication service and all these layers are cascaded and support each other (fig 2.2). The main protocols of this suite are TCP and UDP, which exist in transport layer. TCP is an acknowledgeable protocol that provides reliability in data transmission while UDP is non acknowledgeable protocol and is used in data streaming services like video conferencing, VOIP, etc.

The layer structure of TCP/IP suite is similar to OSI Model. In TCP/IP Suite the Link Layer covers the last two layers (physical and data link layer) of OSI model. Presentation and Session Layers of OSI model

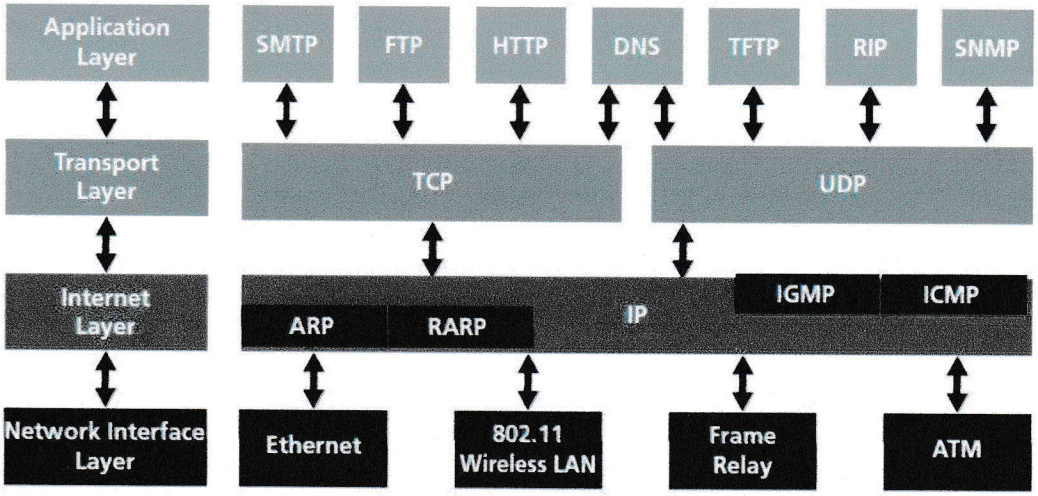


Fig 2.2: Different Layers Protocols in TCP/IP suite

2.3.1 IGMP Protocol:

Internet Group Management Protocol (IGMP) looks like internet Control Message Protocol. It exists in Internet layer in TCP/IP protocol suite. ICMP datagram also encapsulates with IP datagram for communication in a network. It supports multicasting concept between a group of hosts and between multicasting supported routers, in a physical network, which is against broadcasting. For the working of

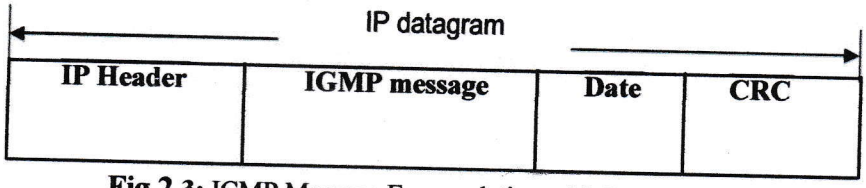


Fig 2.3: ICMP Message Encapsulation with IP Datagram

Multicasting, it provides the familiarities, how a class D and IP address are mapped with the hardware or Ethernet address.

By using net state query with some of its parameters we can get multicasting report or routing tables of our own system which is associated with hardware interface like net stat –nr

Route Table

Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	194.47.156.1	194.47.156.108	25
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
194.47.156.0	255.255.255.0	194.47.156.108	194.47.156.108	25
194.47.156.108	255.255.255.255	127.0.0.1	127.0.0.1	25
194.47.156.255	255.255.255.255	194.47.156.108	194.47.156.108	25
224.0.0.0	240.0.0.0	194.47.156.108	194.47.156.108	25
255.255.255.255	255.255.255.255	194.47.156.108	194.47.156.108	1
255.255.255.255	255.255.255.255	194.47.156.108	3	1
255.255.255.255	255.255.255.255	194.47.156.108	10005	1

Default Gateway: 194.47.156.1

chinmoy@sweet: netstat -nr

Kernel IP routing table

Microsoft Operating system is used in first output and in second Linux operating system is used. The output expression is little bit different.

2.3.2 Protocol

IPSec is an internet layer protocol which provides security at internet layer. The key principle of IPSec on internet layer is that, it provides the security to individual users at transparent level. It provides the data access authentication as well as data encryption on the same level.

IPSec covers three areas of security level, data encryption, traffic authentication and key management.

2.3.3 Protocol Identifier

The IPSec protocol has classified into two sub-level protocols on the basis of their different working algorithms.

- Authentication Header(AH)
- Encapsulation Security Payload(ESP)

2.3.4 Security Level Protocols

There are some protocols which provide security at transport layer. Protocols are:

- Secure Socket Layer(SSL)
- Transport Layer Security (TLS)
- Secure Shell(SSH)

2.3.5 Internet Layer

The second layer of TCP/IP suite protocol structure is Internet or network layer. It generates a service request to Data Link layer protocol and provides services against Transport layer application request.

The role of internet layer protocol (IP) is very important in internetworking data transmission and in receiving prospects; datagram delivery is the main task of this layer.

2.3.6 Internet protocol

Internet protocol is an important protocol of the internet layer as well for the whole internetworking communication. The protocol structure of internet layer is IP datagram and each IP datagram consists of the source IP address and destination IP address which is of 32-bit physical address.

Consider the layer traffic scenario; it receives UDP/TCP segment request form transport layer and add some layer information tags as a prefix and convert it into IP datagram. That is concerned with the exact datagram delivery in the form of source and destination IP address.

Similarly SSL and TLS provide security to web applications at transport level. (fig 2.20) .

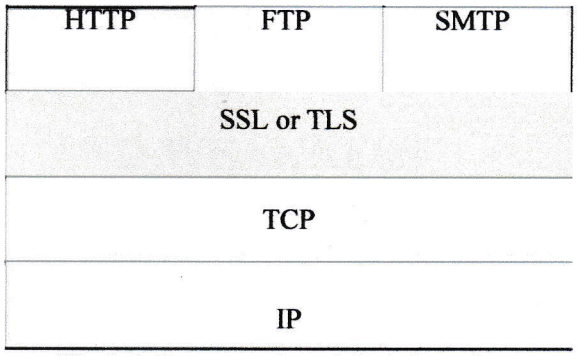


Fig 2.4: Transport Level Web Security

2.3.7 Application Layer Protocol: Application layer consist of applications and processes that works above the transport layer. These applications and processes do work by using the network or remaining lower layer protocols between two or more host in a network as an application-to-application or process- to-process communication level .It is clear that all application level protocols communicate on network through transport and internet level protocols.

There are number of protocols at application layer we will discuss some of them regarding our project prospective, detail of these protocols will explain in next chapters.

2.3.8 SMTP Protocol

Email (e-mail) utilized nearly all around the globe with regard to conversation associated with information within easy understandable textual content or even within GUI setting done software coating. The actual process employed for E-mail is actually Simple Mail Transport Protocol (SMTP). This particular software process is actually lounging upon TCP process. Determine two. twenty-two exhibits the actual structures associated with SMTP. Postal mail move broker is actually responsible with regard to moving the actual e- mail communications in one program to a different program on the neighborhood system, however in the event that e-mail is actually shipped upon broad region system after that this particular broker is called exchange postal mail move broker. Likewise, the person broker is actually responsible in order to deliver as well as obtain email through mail-server in order to mail-client, we. at the. Ms Perspective convey, Home windows reside postal mail and soon.

2.3.9 FTP Protocol:

The actual process that is employed for moving the actual document type supply in order to location is actually called File Transfer Protocol (FTP). FTP exchanges the actual document safely through supply in order to location over the neighborhood system or even broad region system. Prior to delivering the information FTP can make safe link in between server as well as customer based on person authentication. An additional function associated with FTP process is actually which, this determines twin TCP

2.4 Source and Destination Port:

TCP protocol provides the source and destination services port. There are many applications, services and system processes that are associated with unique ports. By allocating specific ports with specific services on server end administrators can allow/deny system services to specific client or group of clients, i.e. web services.

Chapter 3

NETWORK SECURITY THREATS AND WEAKNESS

3.1 Network Security

Whenever we discuss protection, the initial step is actually which the way you determine system protection. Should you request through 10 various managers concerning the description associated with system protection, you will likely obtain 10 various solutions. Nevertheless, because its title recommend system protection may be the safety associated with systems, their own programs or even providers towards unauthorized entry which helps prevent type customization, disclosure or even damage associated with information. Additionally, it guarantees how the system is actually carrying out properly without any dangerous unwanted effects. This really is of course, an extremely wide description; however an over-all description much better prepares system managers to cope with brand new kinds of episodes. Every business identifies its protection plan which explains the amount of entry, that is allowed or even refused. So it's essential for any kind of business to create this type of protection system that's wide within range as well as assists to cope with brand new kinds of assault.

3.2 Security Threats

When talking about threat it can be any person or event that can cause the damage of data or network. Threats can also be natural for example wind, lightning, flooding or can be accidental, such as accidentally deletion offile.

3.3 Security Weakness

Weakness understood to be the actual weak point in a system that may be used with a risk. Lately nearly in most places system systems happen to be used, for example financial, taxes, E-Commerce. These types of programs tend to be contained various system products as well as computer systems as well as it is crucial to safeguard these types of programs as well as products through harmful cyber-terrorist to ensure that probabilities in order to take advantage of the actual vulnerabilities might decrease. You will find various equipment as well as software program resources available for sale to safeguard towards these types of episodes, for example firewalls, Invasion Recognition Techniques (IDS), antivirus software program as well as susceptibility checking software program. Nevertheless, using these types of equipment as well as software program can't assure the actual system towards episodes. “The just genuinely safe program is actually what is actually driven away -- as well as i quickly possess my personal doubts”, the quote with a top protection professional.

Based on the figure in the reviews associated with Pc Crisis Reaction Team/Coordination Middle (CERT/CC), the amount of used weakness raises significantly. as shown in figure 3.1.

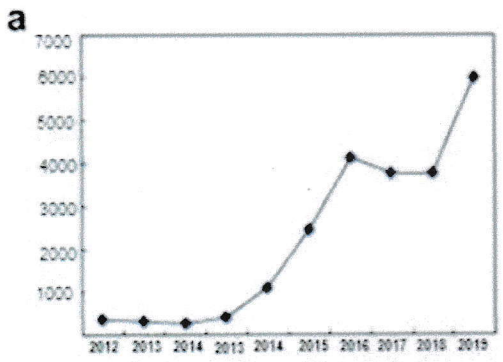


Fig.3.1 (A) The number of found weakness

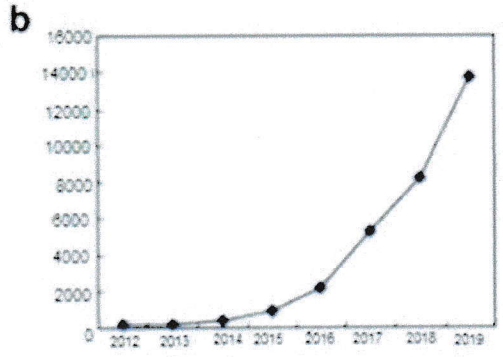


Fig.3.2.(B) The number of reported events

The impact of these threats and vulnerabilities points to the problems that result in disclosure, modification or denial of service. Below are some common threats to a network.

3.4 Unauthorized Access

If you're attempting to obtain an informal use of a good unprotected cellular system, you may be imprisoned upon place, even though you don't have any felony intention (besides robbing their own bandwidth, obviously). Within North America it's known as thievery associated with telecommunication. The benefit of any kind of system is actually source discussing. As part of system all of us reveal various kinds of providers such as document as well as inkjet printer discussing because of discussed assets anyone may attempt to obtain unlawful entry which could trigger unauthorized entry within system. Pass word discussing, speculating as well as recording tend to be 3 typical techniques to obtain unlawful entry. Pass word discussing as well as speculating aren't a brand new imply associated with unlawful entry, you will find various processes for speculating the pass word.

- Try default passwords
- Try all dictionary words.
- Try all short words, usually 1 to 3 characters long.
- Try user's personal number, mobile or phone number, home address, etc.
- By collecting user's personal information like his/her birth day, family names.

Password capturing is a technique in which a hacker unknowingly steals user's ID and password. Trojan horse program designed for this purpose that can capture the password. Below is some basic information that can prevent from unauthorized access.

- Use strong passwords, containsatleast10characters,containsatleastone alpha, one
- Numeric and one special character and use passwords that cannot contain dictionary words.
- Use hardware and software firewall.
- Use protection software against Trojan, spyware, viruses and other malwares.
- Carefullyhandleemails,usuallyviruses,spywareandothermalwareareredistrib utedthrough emails that have an e-mail attachment.

3.5 Disruption of Network Function

Basic function of any network is to share the resources and information. A disruption occurs when network did not provide the needed functionality on time. Interruption in network can effect on one type of functionality or on different functionalities. Several reasons may lay behind the disruption on network

- Network has no ability to detect the traffic, some time network goes down because of the useless traffic.
- Network with single point of failure.
- Hardware failure.
- Improper maintenance of network equipment.
- Unauthorized access to network components may cause the changing in the Configuration of the components which also disrupt the network function.

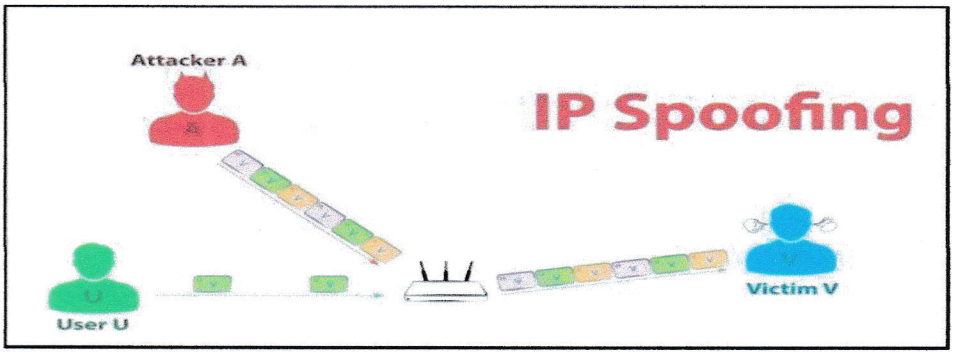


Figure 3.3 IP Spoofing

3.6 Common Threats

Security is really a constant procedure as well as constant battle in between assailant as well as defensive player. There isn't any protection system which is available which provides the entire safety. Various kinds episodes could be removed however other people will require their own location. Execution of the protection system a while price an excessive amount of consequently a few managers merely endure the actual anticipated deficits in order to find this the majority of economical answer.

Beneath all of us talk about a few risks as well as connected deficits using their anticipated development. The actual checklist isn't thorough a few risks might have a few typical components in order to the areas.

3.7 Errors and Omissions

There are numerous human being unintended mistakes that lead within protection difficulties. These types of may appear any place in the machine. At some point a little information admittance mistake may cause the machine accident, a few of the mistake happens throughout upkeep or even set up that may also be the risk with regard to protection. Mistakes tend to be an essential risk towards the ethics associated with information. These types of may create inadvertently through information admittance providers, program providers as well as designers. Individuals mainly presume how the info from the pc program is actually much more precise. Within previous couple of years enhancement within software program high quality decreases this particular risk.

Chapter 4

NETWORK SECURITY ATTACKS

4.1 General Categories of Security Attacks

In order to give up in between starting something as well as locking mechanism this lower to ensure that no-one can utilize it, is known as protection as well as any kind of motion which compromises the actual protection is known as the protection assault. Something that is supplying the actual providers needed through the person precisely as well as stopping the actual unlawful utilization of program assets is known as the safe program. Episodes could be classified in to subsequent fundamental groups.

- Being interrupted: With regard to while using information or even assets it's important that they're obtainable 24/7 for that sanctioned events, whenever as well as exactly where they require this. Assault about the accessibility to information is known as being interrupted. Accessibility may have deliberate or even un-intentional functions. Types of un-intentional functions tend to be, unintentionally program accident, removal as well as overwriting associated with information plus some period because of no human being elements such as ton, that will fire as well as earthquakes. While damage associated with national infrastructure because of conflicts, attacks plus some episodes through cyber-terrorist which failures the machine, for example denial of service *(DOS)* and distributed denial of service *(DDOS)* episodes would be the types of deliberate functions. Safety towards accessibility episodes consists of back-up as well as repair.

- Interception: The actual primary idea is actually how the information ought to be concealing through unauthorized customers. In the event that a few one that is actually unauthorized to determine personal information, can easily see or even duplicate the information that may additional supply within rigorous energetic assault. This assault is called assault upon discretion. Information ethics could be achieved through powerful authentication as well as rigid entry regulates, simply because a while sanctioned customer could also the risk with regard to discretion associated with information. They are able to acquire additional individual's qualifications.

- Customization: Ethics associated with information handles avoidance associated with deliberate or even unintended customization associated with information. Assault upon ethics associated with information known as customization. Various algorithms employed for affirmation associated with information that may avoid within modification associated with information. Safety associated with information through customization is actually primary issue compared to recognition. Ethics associated with information might preserve from numerous levels associated with OSIprogram design.

- Manufacturing: Assault upon authenticity known as manufacturing. Authenticity implies that information is actually arriving type the actual obvious supply. This guarantees that you're that a person state you're. Person title as well as pass word is actually the most typical method to accomplish authentication, other methods tend to be such as wise credit cards as well as electronic records

Above mentioned attacks are shown in figure 2.8

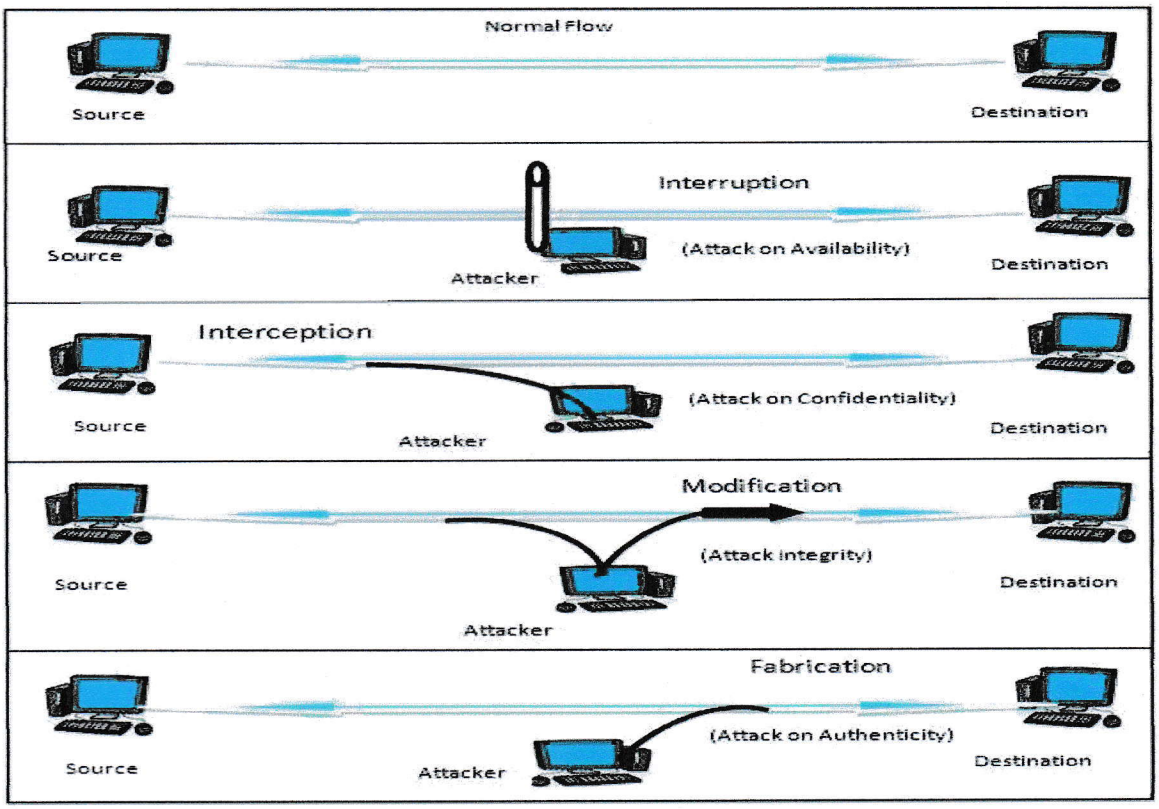


Fig.4.1 Basic types of Security Attacks

On the basis of these four attacks we can further classify security attacks as passive attacks and active attacks. Passive attacks are only involved in monitoring of the information (interception). The goal of this attack is to obtain transmitted information. Two types of passive attacks are "release of message content" and "traffic analysis". Passive attacks are hard to detect because they do not involve in any alteration. Different encryption schemes are used to prevent against these attacks.

Active attacks are involved in modification of data (interception, modification, fabrication) or creation of false data. These attacks are further subdivided into four categories, "masquerade", "and replay"," modification of data and denial of service". When an unauthorized user tries to pretend as an authorized user is called masquerade attack. Replay attacks involved in capturing the message between two communication parties and replay it to one or more parties. Bring the network down to its knees by flooding the useless traffic in network is called denial ofservice attack.

Attacks are either active or passive. Information which hackers obtained from a passive attack is used in more aggressive active attack. We will discuss in detail some common types of network attacks.

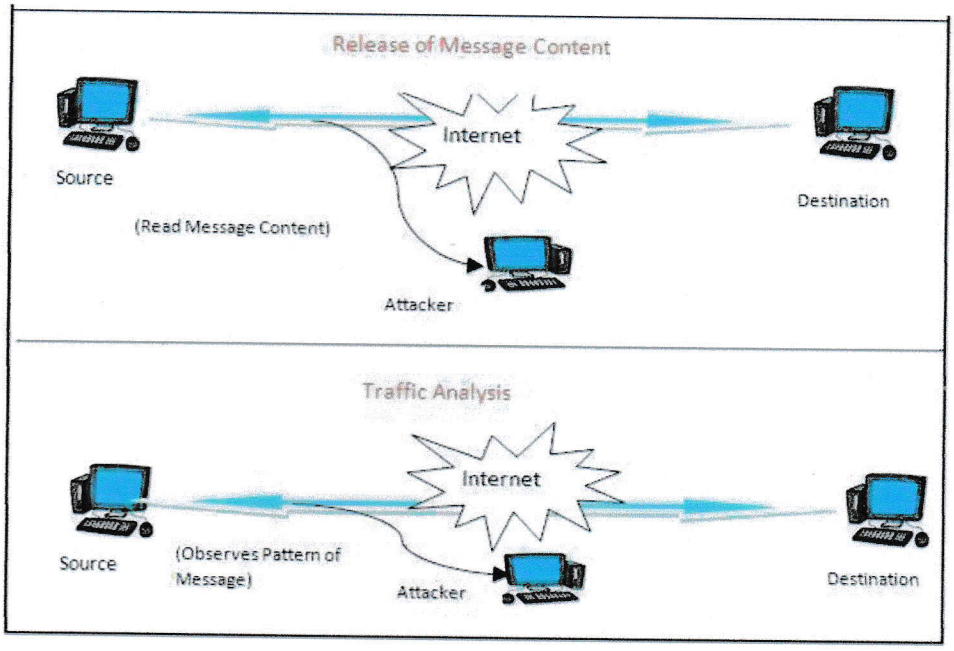


Figure 4.2 Passive Attacks

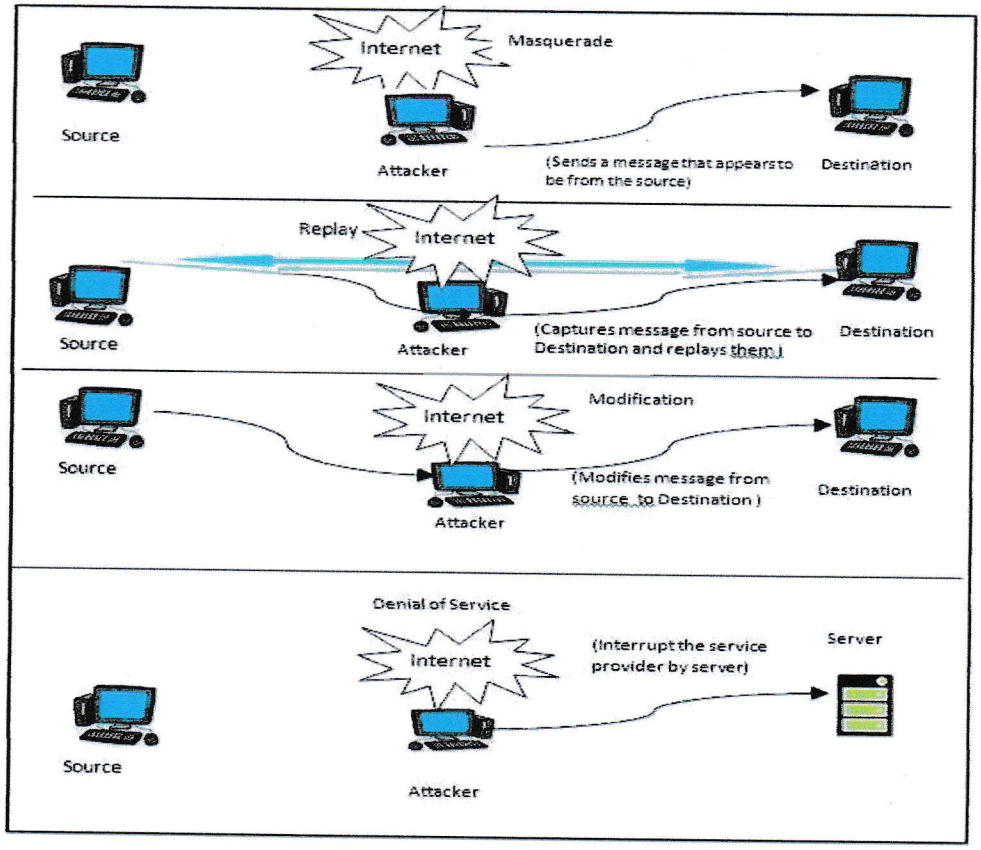


Figure 4.3 Active Attacks

4.2 Reconnaissance Attacks

Gathering information against a targeted host or network is called reconnaissance attack. Attacker analyze the target host and try to discover the details like alive IP addresses, open ports of the network, fail our of operating system, and types of services and protocols running on the network.

Reconnaissance attacks are common they are not so much dangerous because they are not involved in any kind of alteration or destruction of data but on the other hand they show the vulnerabilities in the network. They allow hackers to see which ways are open to access the system and provide enough information to them which they can further use in denial of service (DOS)attacks.

4.3 Port Scan and Ping Sweep

Port scan and ping sweep are two common network probes typically used to run various test against a host or device to find vulnerable services. They are helpful to examine the IP address and the services which are running on a device or host. In port scanning hacker sends a packet to each target port and reply message indicates that either the port is open or closed which is further helpful to launch an attack against a specific service. For example if hacker finds that port 143 (IMAP port) is open then on next step he/she tries to find out that which version of IMAP is running if that version is vulnerable then hacker can access the machine as a super user using an "*exploit*" program (program that automatically break the security hole) . The most popular probing tool is Nmap (Network Mapped).

Different types of N map scans are given below:

- **TCP Connect Scan**: It makes a complete TCP connection that's why is easy to detect.
- **TCP SYN Scan:** Attacker sends a SYN to each target port, if target port is open target sends SYN- ACK. The attacker then sends a RESET packet and aborts the connection. This type of scan is also called half- open because attacker connects to the port and breaks the connection just before full connection. These types of scans are hard to detect.
- **FIN Scan**: attacker sends a fin packet which is able to pass by firewalls without modification; open ports ignore the packet while close ports sent back a RESET packet.
- **ACK Scan**: ACK scan is good in network where firewalls are running. It did not classify the port as open or closed, if reset comes back from the target it classify the port as "unfiltered" otherwise "filtered".

The method of finding that which IP addresses are alive is called ping sweep. Attacker sends an ICMP packet to each machine (with in a range) to a targeted network. The aim is to find out the machines which are alive and which are not alive. These ICMP replies from different machines are logged into a file for future reference. Network administrators may also use ping sweep to figure out which systems are alive and which are not for diagnostic reasons.

ping is a tool used for performing ping sweep. Working on round robin function, takes a list of IP addresses, sends a ping packet to an IP address and immediately proceed toward next IP address. To detect ping sweep there are different tools available. Example is a protocol logger that has the ability to log ICMP, TCP and UDP packets.

4.4 Internet Information Queries

DNS queries provide the particular information of domain and the addresses associated with that particular domain. IP queries display the range of IP addresses and for which domain that addresses are associated. Ping sweep presents a clear picture of a particular environment. After these queries port scan start by the hacker which leads him to find out which ports are open and which services are running on these ports. Finally the whole information can be helpful when hacker tries to compromise any system through these services.

4.5 Access Attack

We discussed earlier that there are vulnerabilities in services which are running on a system like web services, FTP services and any authentication services that authenticates the user and hacker can exploit these vulnerabilities. Access attacks occur when a malicious hacker exploit these vulnerabilities and succeed to access the confidential information of any organization. Different types of network attacks are

- Password
- Attacks Trust
- Exploitation
- Port
  Redirection
  Man-in-the-middle attack

4.6 Password Attack

Several methods can be used for password attack. Trojan horse, IP spoofing and packet sniffers can show the detail of the user like user name and password. We may refer password attack as, repeated attempts to find the user information (user name or password). Once an intruder succeeds then he/she has the same access right which compromised account has.

4.7 Unauthorized Modification

Unauthorized modification of data is attack on data integrity. Any changing in data or software can create big problems; possibly can corrupt databases, spreadsheets or some other important applications. Any miner unauthorized change in software can damage the whole operating system or all applications which are related to that software and perhaps need to reinstall the software with all related applications.

This can be made by unauthorized as well as authorized users. Any change in the data or in application can divert the information to some other destinations. This information can be used by any outsider or hacker who can make some changes and again send to the destination.

Some reasons that can cause the unauthorized modification are

- Lack of encryption of data
- The user which only requires read permission granted write permissions
- also. Access control mechanism that allow unnecessary write permission.
- Lack of protection tools.
- Weak passwords.
- Default Passwords (most of the devices and applications have set on their default password which we forgot to change).
- Password are stored as plain-text.

We can mitigate password attacks by using strong and encrypted passwords; by change the password after some specific time and by selecting the property that after certain wrong login attempts the account should be locked.

However, password cracking is also helpful to build and maintain a more secure system like;

- To sense the security of the password.
- Password cracking can be used to recover forgotten password. To migrate users.
- To maintain check and balance system.

4.8 Types of Password Attack.

Strong, long and encrypted passwords do not mean that they are unbreakable; it's just a matter of time. Few years earlier the time to break a password was may be 100 days but now it's just a matter of two or three weeks.

Different types of password cracking attacks are:

- Dictionary Attack
- Brute force attack
- Hybrid Attack

	Dictionary Attack	Brute force Attack	Hybrid Attack
Speed of the Attack	Fast	Slow	Medium
Passwords Cracked	Finds only words	Finds every password(A-Z, 0-9, special characters)	Finds only the password that have a dictionary word as the base

Table 4.4 Types of password Attacks

4.9 Port Redirection:

It is another type of trust exploitation attack in which a hacker bypasses the security mechanism. Consider the below network in which hacker on the outside have the ability to access the public computer but not the computers which are in DMZ or which are inside the firewall. If public computer compromised by the hacker then hacker installs a software that can redirect the traffic towards the hacker, directly to the inside computers. In this way hacker makes a tunnel for communication and bypasses the security firewall. See figure 4.7 for port redirection attack.

4.10 Man-in-the-Middle Attack

When hackers succeed to intrude himself between two communication parties this type of attack is called MITM (Man-in-the-Middle) attack. In this way hacker can intercept data between source and destination host, can modify data and retransmit it to the destination host and can also inject any type of false data.

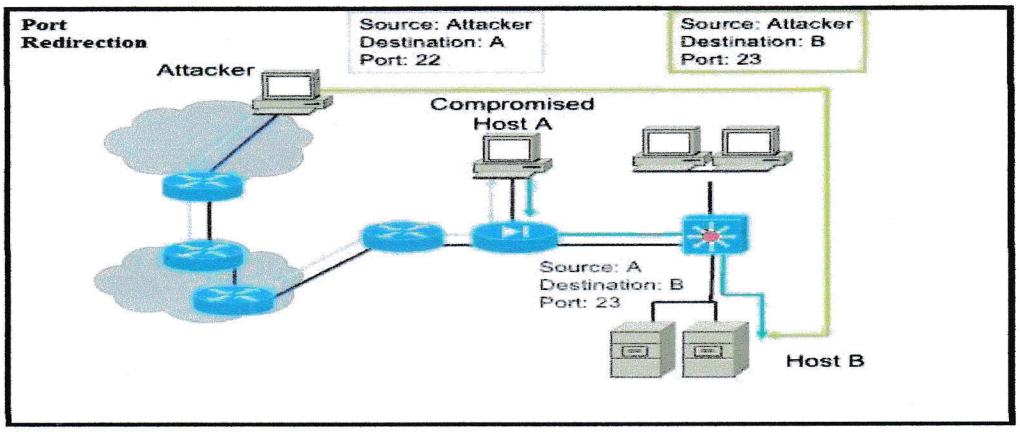


Figure 4.5 Port Redirection Attack

4.11 Distributed Denial of Service (DDOS)

In DDOS attacks several compromised systems are used to launch an attack against a targeted host or network. For targeting a host attacker first compromise some other hosts on network and install some software for controlling them usually these compromised hosts are called agents or zombies. Using these agent's attacker launch overwhelm attack against the target.

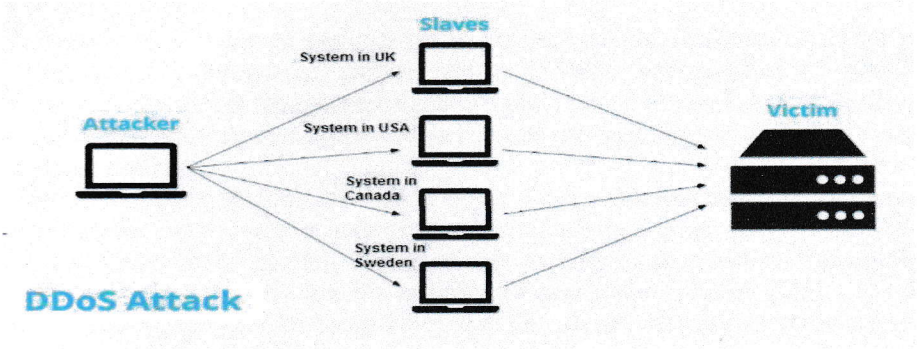


Figure 4.6 Distributed Denial of Service Attack

Systems control with different software like Trion and Shaft. Example of DDOS attacks are SMURF, MYDoom and TFN. DDOS attacks are very hard to defend. To trace out the intruder is also very difficult as they are on back side and using other hosts against the victim. Figure 4.6 is describing distributed denial of service attack.

4.12 Buffer Overflow

We can define buffer overflow as when a hacker tries to store too much data in buffer which it cannot hold. Take an example of glass which can hold 5 ounces of water if we put 8 ounces what will happen? Obviously water overflows from the edges. Buffer overflow is similar to this example;

where glass corresponds to buffer and water corresponds to data. The overall goal of this attack is to weaken the function of victim's program so that hacker can easily take control of that program. Buffer overflow is the best-known attack on security which can cause attack against availability, integrity and confidentiality of data. Examples are NetMeeting Buffer overflow, Linux Buffer Overflow, Outlook Buffer Overflow.

4.13 Viruses and Other Malicious Program

Viruses and other malicious program have the ability to make duplicate copies of them on an ever increasing number of computers. A "Virus" is just like a computer program that spread by copying itself into other programs. Another malicious program "Worm" is spread through the network. Without the network it cannot spread and can eliminate only when whole network or system is shutdown. Examples of popular worms are Code Red, Slammer, Storm Bot. A malicious

program that resides in system and execute on an event like date or time is called "Logic Bomb", "Trojan Horse" is another type of malicious program that hackers use to steal useful information like user name, password and bank account codes.

Chapter 5

SECURITY COUNTERMEASURE TECHNIQUES AND TOOLS

5.1 Security Countermeasure Techniques

All the security and safety countermeasure systems really are exclusively connected to these sorts of parameters which usually live through also known as mobile phone network discrepancies or possibly weakness and additionally most of the outcome within the correspondence mobile phone network. Subsequently after assessing the effects the hands down parameters, you can easily decide a lot of primary security and safety countermeasure ways of a fabulous mobile phone network.

The choice and additionally implementation the hands down countermeasure systems for mobile phone network natural world hinges on all the mobile phone network governing administration party. This will depend regarding most of the new skills and additionally curiosity approximately mobile phone network, basic mobile phone network structures, website visitors parameters also known as practical application routine (OSI and additionally TCP/IP layer network protocols knowledge and working role), mobile phone network electronic general performance, security and safety risks and additionally old disadvantages for mobile phone network. A fabulous rowdy or possibly expired skill may be an underlying cause about mobile phone network discrepancies and additionally vulnerabilities.

Just by everything in this article weights various explore agency experience allocated a lot of a large number of imperative primary security and safety countermeasure ways of a basic tier mobile phone network commercial infrastructure.

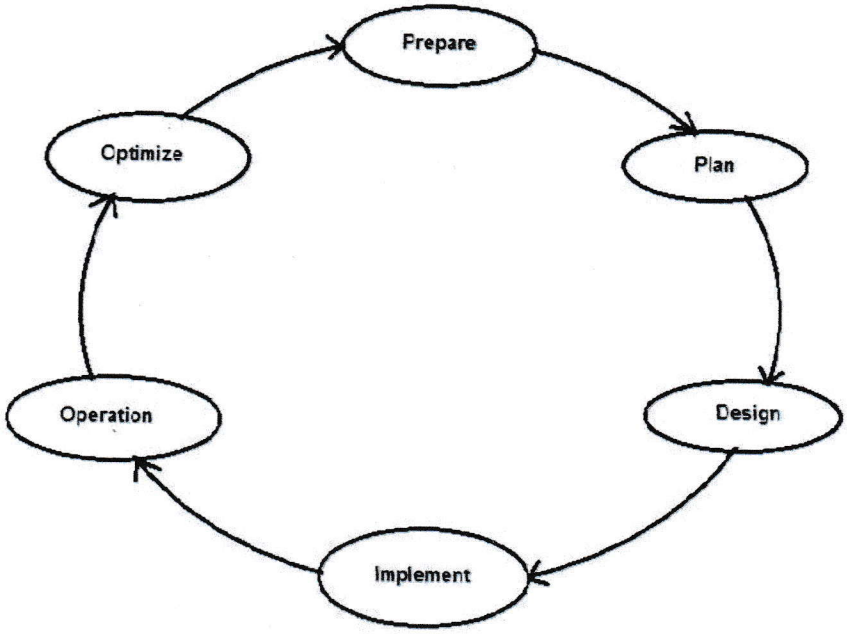


Fig 5.1: Network Lifestyle Phases

5.1.1 Security Policies

A strong security policy performs an efficient role in a network. If policy develops after analyzing the network and behavior of its components then it results a much secure and smooth network.

5.1.2 Authority of resources

The authorization of systems or network resources has an important role in security countermeasure. After a fair survey of network, we may assign a proper level of authority for accessing the system resources. The policies of antivirus or the access control list of router or firewall can define an authority for accessing network resources in a proper manner.

5.1.3 Detect malicious activities

The presence of intrusion detection system has an important role in security countermeasure. The study and analyzing the log files against malicious activities in network can save a system. It provides a futuristic safety approach against many other malicious aims.

5.1.4 Mitigate possible attacks

The symptoms of a malicious attack give us an idea about which type of protection is required for a system against that attack. We can re-adjust or re-configure our security system parameters by generate a strong resistive block against the attack.

5.1.5 Security Countermeasures Tools

We will now discuss tools to defend against the attacks, we have discussed earlier.

5.1.6 Cryptography

Cryptography is used to protect data from interception. We have to be sure that our confidential data cannot be understood by an unintended user. Cryptography is the study of methods to send data in unrecognizable form so that only the intended user can recognize and read the message. There are two basic cryptographic terms, Plain Text, the text or data which we want to encrypt, and Cipher Text, the encrypted form of plaintext.

5.1.7 Conventional or Symmetric Encryption

It was the only encryption scheme available before the public-key encryption. One secret key is shared among the sender and the receiver. Whole procedure of conventional encryption consists of five stages:

1. Plain Text: The original message or data which we want to be encrypted.
2. Encryption Algorithm: Encryption algorithm performs different transformations on the data.
3. Secret Key: Secret key is the input to the encryption algorithm. Different transformations performed by the encryption algorithms depend on the secret key.
4. Cipher Text: This is the output of scrambled message.
5. Decryption Algorithm: Reverse of the encryption algorithm, it produces the plain text with the help of same secret key and the cipher text.

5.1.8 Asymmetric Algorithms

Asymmetric cryptography depends on the cryptographic algorithms based on two keys.
There are some conditions which every algorithm must fulfill:

- It must be easy for any party to generate public and private key.
- It must be easy for sender A to encrypt the message by using public key to produce the cipher text.
- It must be easy for recipient B to decrypt that message with private key to recover the original text.
- Determining the private key is not possible for any party even if they know the public keys.
- It should not possible for any opponent to recover the original message by using the public key and cipher text.
- Anyone can use any key for encryption whiles other for decryption.

5.1.9 Asymmetric Key Encryption

Public key encryption could be used in another way (as illustrated in figure 5.3). Some time we are more interested in data integrity and data authenticity than eavesdropping. For example, if user A wants to send a message to user B, instead of data confidentiality user B only want to assure that the data is coming from user A.

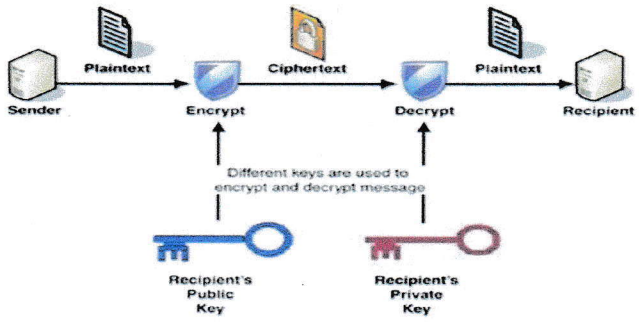


Figure 5.2 Asymmetric Key Encryption

In this case A uses his own private key to encrypt the data, when B receives the cipher text; he/she can decrypt the data with A's public key which proves that message has been encrypted by A. Encrypting the message Using recipient's public key provides confidentiality while encrypting the message using sender's private key provides authenticity, the term used

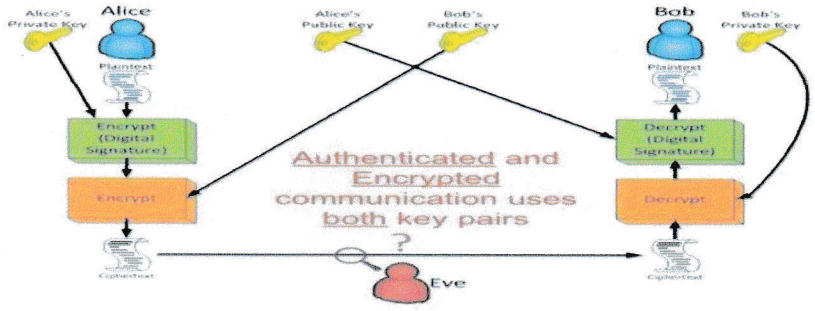


Figure 5.3 Authentications Using Asymmetric Encryption

Chapter 6

SECURITY SOLUTIONS

In this chapter we will discuss different security tools and applications which are widely used now a days.

6.1 Application Level Solutions

Security solutions at application level further divided for different applications, discussed one by one.

6.1.1 Authentication Level

The verification of any identity called authentication which also verify the integrity of data. If an individual request generated for an operation, without knowledge of that individual it is often difficult to decide that either this operation is allowed or not. Traditional authentication methods are not suitable for computer networks having sensitive data. We will discuss little bit about most important authentication specifications which are currently in use.

6.1.2 Email Level

The most widely used and growing network application across all platforms is electronic mail. We are using security in SSL/TLS.

6.1.3 IP Level

Which IP Using Organization we select, class-less IP or Class full IP Address, Provide Real IP. Applying security on IP level can ensure the secure communication for the applications that has security mechanism also for the security ignorant applications.

6.1.4 Internet Protocol Security (IPSec)

IPSec is not a single protocol. It is a general framework by using a set of algorithms it allows different entities to communicate securely with each other. It provides encryption and authentication to all traffic at IP level with the help of strong cryptography. Authentication and encapsulation are two basics of IPSec. Two protocols that provide authentication and encapsulation are Authentication Header (AH) and Encapsulation Security Payload (ESP). These two protocols used in combination or alone to provide a desired set of security services for the IP layer. Figure 6.1 shows the document overview of IPSec.

6.1.5 Web Level

Web is visible for everyone, most of the users are not aware of the risks. Browser side risks, wrong configuration in web servers are some types of risk that helps intruders to unauthorized remote access and interception of data which sent form client/server to browser and browser to client/server. We will discuss two standardized schemes Secure Socket Layer (SSL)/Transport Layer Security (TLS) and Secure Electronic Transaction (SET) that are used for web security.

6.2 SSL/TLS

One way is to provide web security at IP layer level which we already discussed earlier. Various approaches are used for web security and they have different scope of applicability with corresponding location in TCP/IP protocol suite. One advantage of using IPSec is that it is transparent to end users and we can filter the traffic. Another solution is that to provide security just above TCP (see figure 6.2). SSL is one of the most commonly used security mechanism available on Internet. Like other security protocols SSL is also based on cryptography. After SSLv3, Internet Engineering Task Force (IETF) renamed it as TLS which now considered as standard. TLS is almost same like SSLv3. SSL/TLS encrypt the data at transport layer. Instead of HTTP normal port 80, SSL comes up with a special URL identity "HTTPS" which uses port 443 to establish a secure SSL session. SSL supported browsers are used mostly for sensitive data like credit card information.

SSL protocol further consists of two sub protocols. SSL Record Protocol and SSL Handshake Protocol). SSL record protocol describes the format used to transmit data. The most complex part of SSL is handshake protocol that allows server and client to authenticate each other and by using SSL record protocol transfer the data between SSL enabled server and client.TLS/SSL authenticates to both communication parties (servers and clients) and provide data integrity, that's why can helpful against replay attack, man-in-the middle attack and masquerade attacks.

6.3 System Level Solutions

These security solutions are further dived into two main categories, application level security solutions and system level security solutions. On the basis of the security countermeasure techniques and tools, we proposed different security solutions. Due to differentiation of user base and software base trespasses, system level security solutions are further divided into IDS, IPS, antivirus applications and firewalls.

6.4Intrusion Detection System (IDS)

It means that an IDS in a network only detects or identifies any changes in network but does not perform a resistive action against such changes. The IDS is the system which detects any unauthorized access or intrusion in a system or network. It is a security solution which has a passive position in a system or network against these intrusions. In a network deployment the function of the IDS is to monitor the traffic or network activity without impacting the traffic.
These customize rule based IDS are fixed by network/system administrator on the basis of previous behavior of the network.
The IDS system uses two approaches for notification of intrusion in a network.

- **Statistical detection**
  It depends on the statistical behavior of the network; the statistical detection approach has further division into two sub categories.

- **Threshold detection**
  In threshold detection, the IDS can monitor the number of established connections in a specific time or the number of new user requests for a specific application that runs on a network.

- **Profile based detection**
  In profile based detection, the IDS system monitors the behavior of a user at different time slots. It monitors the user login/logoff session times on the network also counts the number of password failure attempts by user in short time intervals.

Classifications:

The IDS security solutions are further classified into three main categories.

1) Network based intrusion detection system(NIDS)
2) Host based intrusion detection system (HIDS)
3) Distributed intrusion detection system (DIDS)

6.4.1Network based intrusion detection system (NIDS)

Network based intrusion detection system works in a network. It monitors all the network traffic especially at hardware layer based traffic. The communication and working functionality of hardware layers in TCP/IP suite are already discussed in chapter two, like in link layer hardware interface card can communicate with another system via communication medium through hardware address (MAC address).

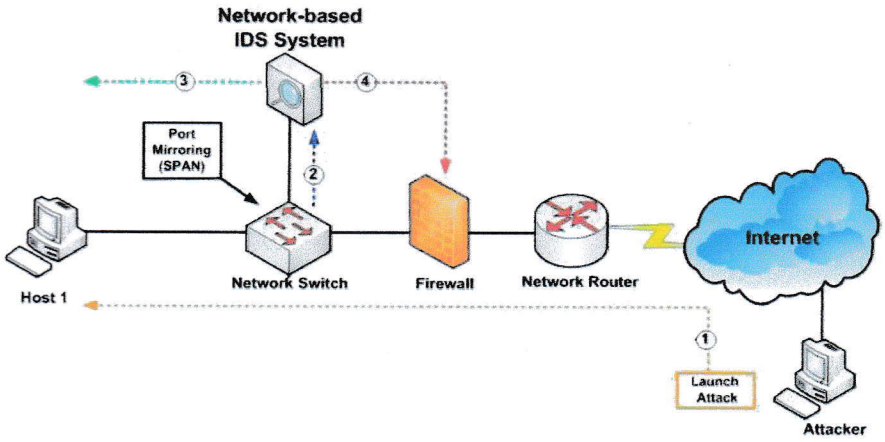


Fig 6.1: NIDS Based Network

Consider the working functionality of NIC is that first it generates an ICMP request for acquiring a physical address (IP address). This request is broadcast on network. Sometime NIC gets bulk of ICMP requests which can create a chance of network congestion situation. NIDS monitors all the same types of intrusions with appropriate NICs and creates a log file. Similarly, NIDS has a feature to monitor all the network switches communication, if it observes any network intrusion through these switches then it makes a report. NIDS connects to network via any port of network switch. (See fig 6.1).

6.4.2Host Based Intrusion detection system (HIDS)

The role and placement of Host based IDS is slightly different from NIDS. Host-based intrusion detection system is deployed only on a local machine or system. It is responsible to monitor local system-based activities or intrusions i.e. CPU performance, file sharing resources and functionality of system applications like web-server application and mail-service. (see fig 6.2)

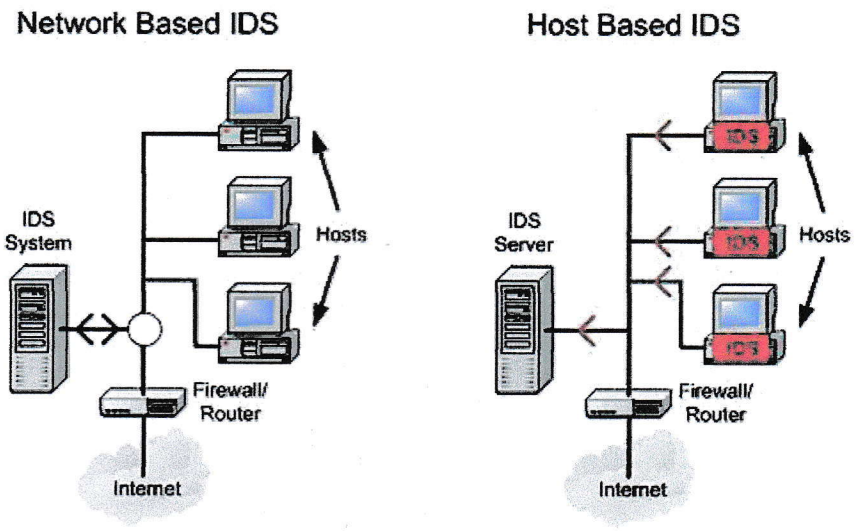


Fig 6.2: HIDS Based Network

6.4.2 Distributed intrusion detection system (DIDS)

These IDS-sensors are in the form of NIDS, HIDS or both. So we can say that the DIDS is a combination of both NIDS and HIDS systems. The one main feature of DIDS system is that all IDS sensors send their reports of network and local system based intrusions to the IDS manager and an IDS manager is responsible to update its IDS sensor patches or signature database against new bugs and intrusions that occurs in the network.

In DIDS there is one central control machine that performs a role of administrator or manager and all remaining IDS systems behave like clients. These IDS client machines normally called IDS-sensors. All these IDS sensors can detect the intrusions in the network or system and send a report to the main IDS manager.

6.4.3 Intrusion Prevention System (IPS)

The intrusion Prevention System performs a role of protection against intrusions that occurs in a network or local system. It works on the basis of output of IDS system log files. Due to this reason we can say that the IPS system is an extension of the IDS system.

But there are some differences between IDS and IPS. IDS system works in a passive mode, i.e. it only has the ability to detect any intrusion in the network, whereas an IPS works in an active mode. An IPS performs action when it founds any packet dropping or unauthorized connection.

6.5 Network Security Solution Steps :

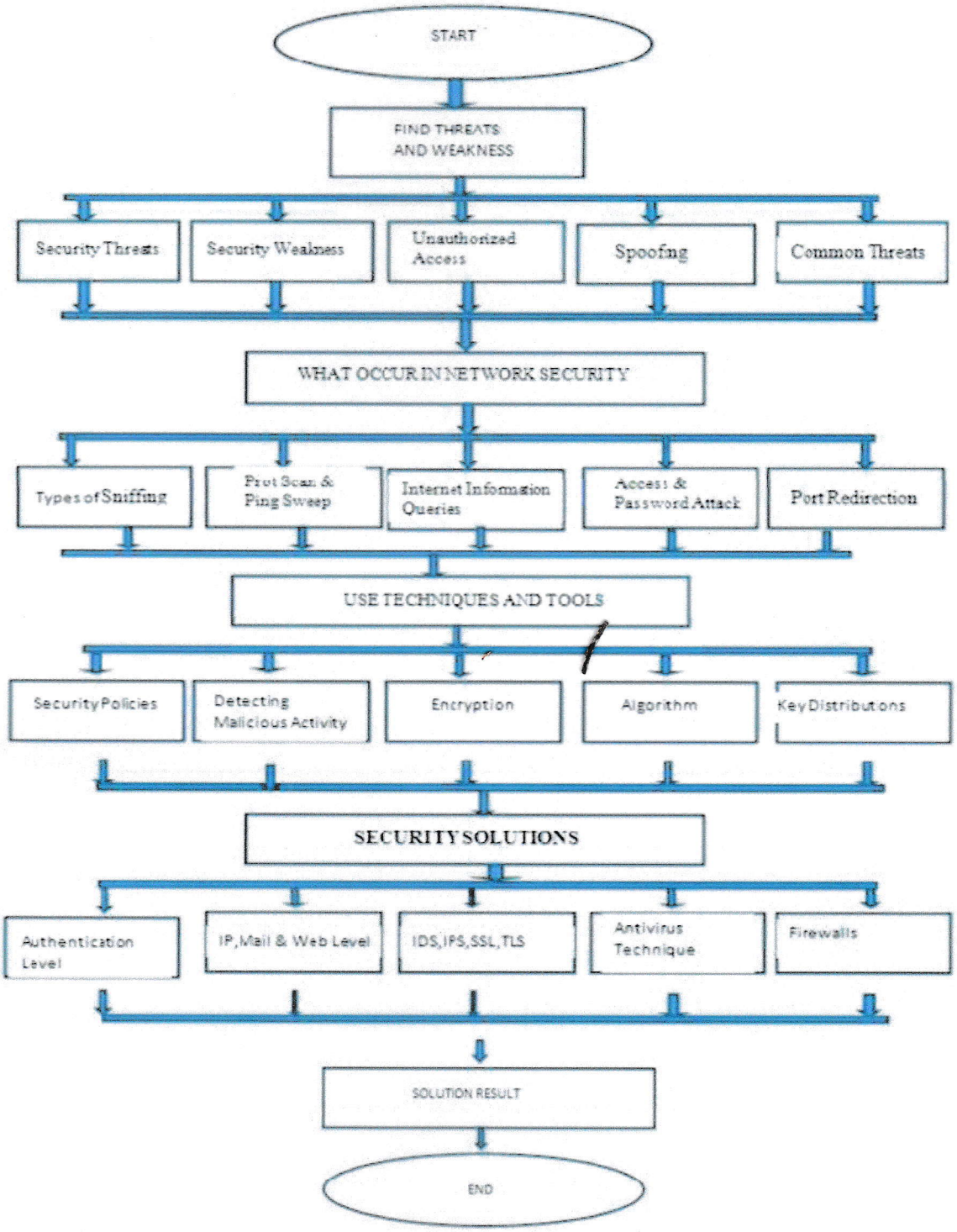


Fig 6.3: Network Security Solution Steps

6.6 Antivirus Techniques

Antivirus techniques are already explained in chapter 5, there are number of malicious applications/software which perform harmful activities within a local system or on network. Using Kespersky and Semantic antivirus.

These applications can be in the form of different "viruses" which may infect or modify the system files or applications, or can be in the form of "worms" that may create their own replicas in a system and utilize the vacant space in system.

Some of these applications perform their role only on local system or some of them travel from one machine to other machine through network resources or other medium like usb and floppies.

For protection from these types of malicious applications we use antivirus techniques on our network or system known as antivirus applications.

The functional architecture of an antivirus technique can be followed up in the given below sequence of operations.

- **Detection**

  The first step of an antivirus application is that it has the ability to detect the occurrence of a virus or other malicious program in system application or in data file.

- **Identification**

  After detection function the second step of an antivirus is that it has the ability to identify the type of virus with its malicious aims.

- **Removal**

The virus removal is the last step of an antivirus application.

6.6.1 Antivirus Functional Techniques

There are many functional techniques used by antivirus applications for detection, identification and finally removal of viruses from a system or a network. Some of these important techniques are:

6.6.2 Generic Decryption (GD)

The generic decryption is an antivirus technique designed for the polymorphic type of viruses. The architecture of polymorphic virus is described in chapter 5. Polymorphic virus contains total encryption architecture. It contains an encrypted virus signature as well as an encrypted key in its internal body; whereas it has an outer body cover which is also encrypted. The outer cover decrypt by its internal key. So, it is very complicated to detect the virus signature through a simple antivirus.
The generic decryption antivirus technique has the ability to detect and clean the type of viruses which have polymorphic architecture. It followed some steps described below

- Generic decryption technique first generates a virtual machine into a real machine. This virtual machine has complete hardware and applications same like in actual machine.

- In the process of scanning or diagnosing, system and data files are placed in virtual machine one by one.

- If the polymorphic virus exists in any placed file, then polymorphic virus performs act to this file first it decrypt is outer cover body by its own internal key.

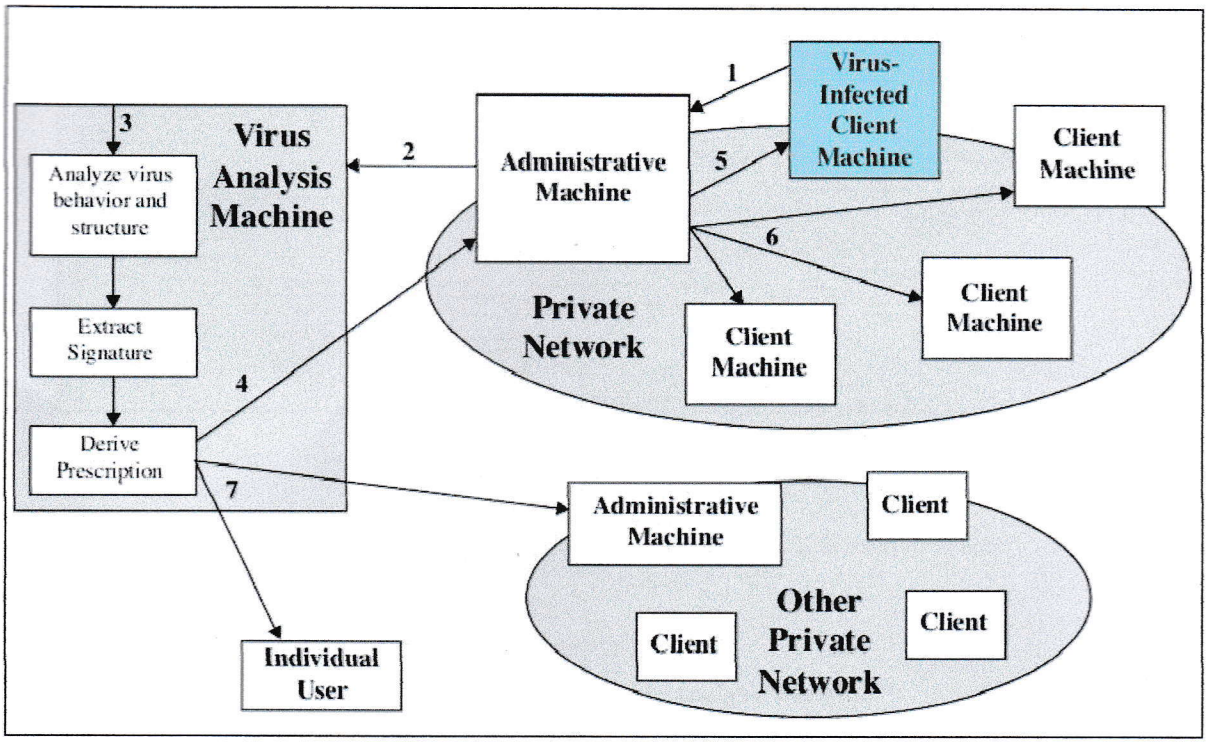


Fig 6.4: Digital Immune System

- As it decrypts its own outer body. It has opened its internal structure, specially its virus signature, in front of any generic decryption antivirus, And then generic decryption antivirus can easily remove this virus from this file.

This process occurs only in virtual machine that is created by generic decryption antivirus; this virtual machine is also totally isolated to actual machine and its applications. In this way polymorphic virus does not have an effect on the actual machine at the time of its operation.

6.6.3 Digital Immune System

A digital immune system or digital immune antivirus is a technique that provides a protection against those types of viruses which have the characteristics to spreading from one computer to other computer through a network. Normally "*worm*" is considered such type of virus.

Digital immune system has its own scanner elements on every client machine in a network; these scanner elements first detect such type of viruses on local client machine, then the scanner client machine sends this information to the main administrator machine, which is also a part of the same network. Administrator machine collect the information and send it to virus analysis machine.

The virus analysis machine may exist on same network or may be on wide area network. The virus analysis machine has some working blocks in its architecture.

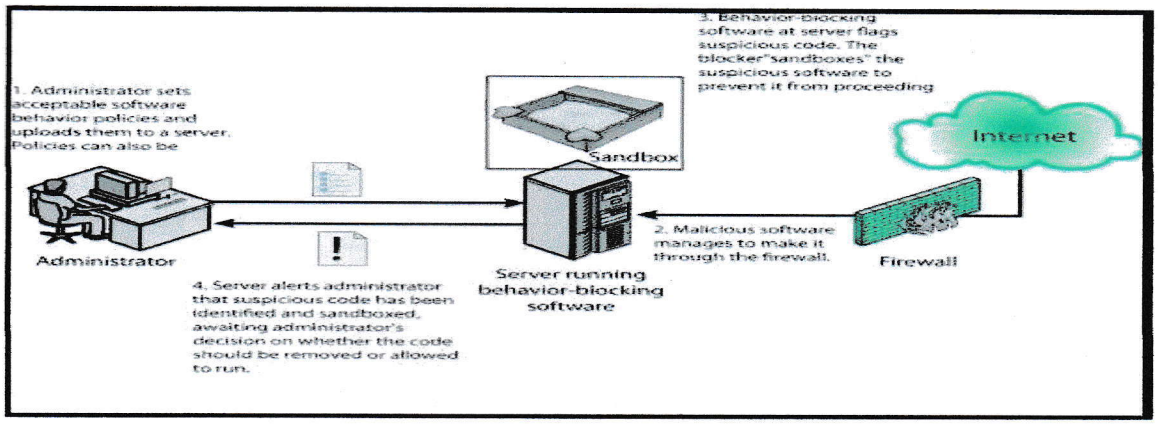


Fig 6.5: Behavior Blocking Software Operation

- 1st block; this block is isolated with other blocks. It is used to detect the virus and read out its structure, i.e. virus type.
- 2nd block; it detects virus signature.
- 3rd block; this is the last block of virus analysis machine, it removes the viruses form the infected files.

After removing viruses from that file, virus analysis machine sends this information to the whole network clients. All network clients update this virus signature information in their databases. A digital immune system is very efficient to detect and remove such type of viruses which spread over the network. (Fig 6.4)

6.6.4 Behavior Blocking Software

The behavior blocking antivirus software integrates with the operating system of a host computer and monitors program's *behavior* in real time . This application runs on both, server and clients but the main protection is done by the server side.

The behavior blocking system can monitor the system files with operating system's behavior. So if any changes occur in system files it detects and send a report to the administrator and wait for an action from the administrator. Updating the main server is the responsibility of administrator. (See fig 6.5).

6.7 Firewalls

A firewall is a barrier which performs isolation between two different networks or systems. It decides that which kind of traffic can pass through a network and in which direction. Firewalls.

Provides an additional level of defense system providing the capabilities to add much tighter and more complex rules of communication between different network segments or zones .

A firewall may contain only one system or it may consist of more than one system. The role of firewall is to provide protection of one network from other network. The connection architecture of a firewall in a network is that it creates a barrier between two networks. For this it must have at least two network interfaces one for the network which is intended to protect and other for the network that is exposed to. Simply a firewall protects the internal network from external network.

6.7.1 Types of firewall:

There are many types of firewalls. Administrators have to decide that which type of firewall is right for a given control architecture. However firewalls can be divided into four categories.

1) Packet filter firewall
2) Application gateway
3) Circuit level gateway
4) State full filter firewall

6.7.2 Packet Filter Firewall

A packet filter firewall monitors all incoming and outgoing network based packets. It allows or denies packet to pass through one network to another network. It checks the packet parameters and compares them with its own tables that contains packet parameters after that a packet filter firewall decides to allow or deny the packet.

The packet parameter field normally contains, source/destination IP address, source/destination services ports, types of packets (either TCP or UDP) and information flags that notify the purpose of packet.

Due to its packet filtering functionality, it may allow specific packets form specific interfaces for communication. This rule can be implemented for both inside and outside traffic. Packet filter firewall is easy to implement and does not require a high level of configuration in a standard network. It is also known as first generation level firewall.

A packet filter can remove the bug which exists in TCP (three way handshake) communication, which a hacker can as a SNY flood attack.

6.7.3 Application Level Gateway

An application level firewall provides more shelter and reliability than a typical packet filter firewall. Application level firewall works on application level and they can better analyze the traffic at application layer. It provides a client-server network environment. All hosts that want to communicate with outside the world use the firewall as a gateway, hosts are considered as client while the application level firewall performs as a server. So we can say that an application level firewall is also an application level gateway.

Since all traffic must pass through the firewall so it has full command on authentication and authorization of data traffic. It filters the traffic at very high level that's why it provides a high level of security.

6.7.4 State full Inspection Firewall

State full inspection firewall is a combination of multiple firewalls, especially with packet filter firewall and application level gateway. It scans the packets at network level and read packet content at application level. It provides more security and is called 3rd generation level firewall.

6.8 Company Visit Information: Before Security Provide-

At first we have visited 10 companies and observed their security system, also collect different types of information. According to companies authority information we can understand that maximum companies are dependent only antivirus security but antivirus security is not a strong security for protects hacking. If this company are using only antivirus then they are unsecure, in this position hacker can easily hacked office information. Companies are Sometimes Face Hacking Problem and there loss their Important data.

Before Security:

	Uses Security												
	Antivirus		Firewall		Email-Level		IP Level		Web Label		Server		Out Of 100
Company Name	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Percentage
1.Group Danny	✓			✓		✓		✓		✓		✓	10
2.Orchid Fashion	✓		✓			✓		✓		✓		✓	20
3.Jemtex BD	✓			✓		✓		✓		✓		✓	10
4.ENMS	✓			✓		✓		✓		✓		✓	10
5.Asian Fashion	✓		✓			✓		✓		✓		✓	20
6.NTKC	✓		✓			✓		✓		✓		✓	20
7.AMC Sweater	✓		✓		✓			✓		✓		✓	30
8.KJF IT	✓		✓			✓		✓		✓		✓	20
9.Weabers INC	✓			✓		✓		✓	✓		✓		30
10.Ostin		✓		✓		✓		✓		✓		✓	5

Fig 6.6 : Organization Using Security and their Collected Data

Here we have used a table by using this table we have mentioned company security details info and find out a percentage and shown their security level in grant chart.

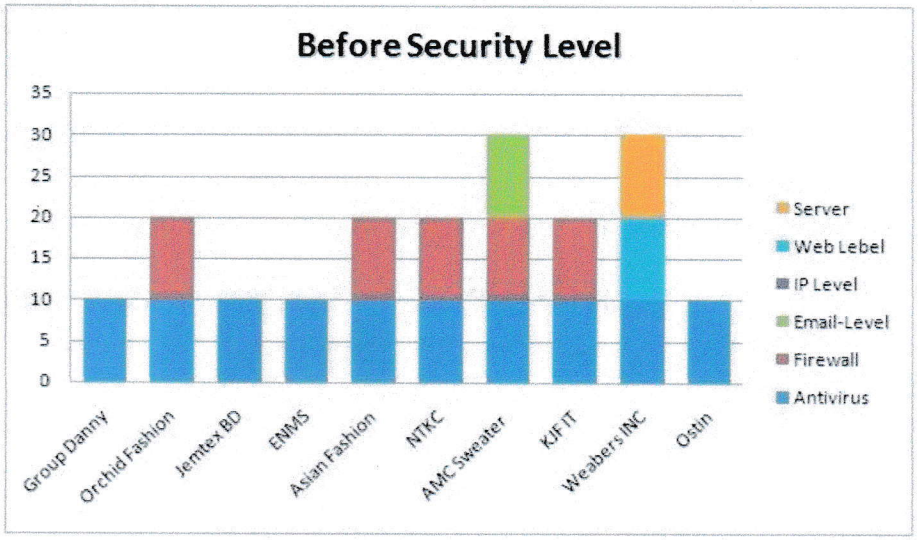


Fig 6.7: Gantt chart of before security level

6.9 After That Security Provide:

After all we have selected some company; that security level is so poor. Then we have provided their advance security and resolve all weakness of their network. Now these company are 80% secured from hacker thread.

After Security:

	Provide Security																			
	Antivirus		Firewall		Email-Level		Authentication Level		IP Level		Web Label		PGP		IDS		IPS		Server		Out Of 100
Company Name	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Percentage
1.Group Danny	✓		✓		✓		✓		✓		✓		✓		✓		✓		✓		100
2. Orchid Fashion	✓		✓		✓		✓		✓		✓		✓		✓		✓		✓		100
3. Asian Fashion	✓		✓		✓		✓		✓		✓		✓		✓		✓		✓		100

Fig 6.8: Data of Security provide in organization

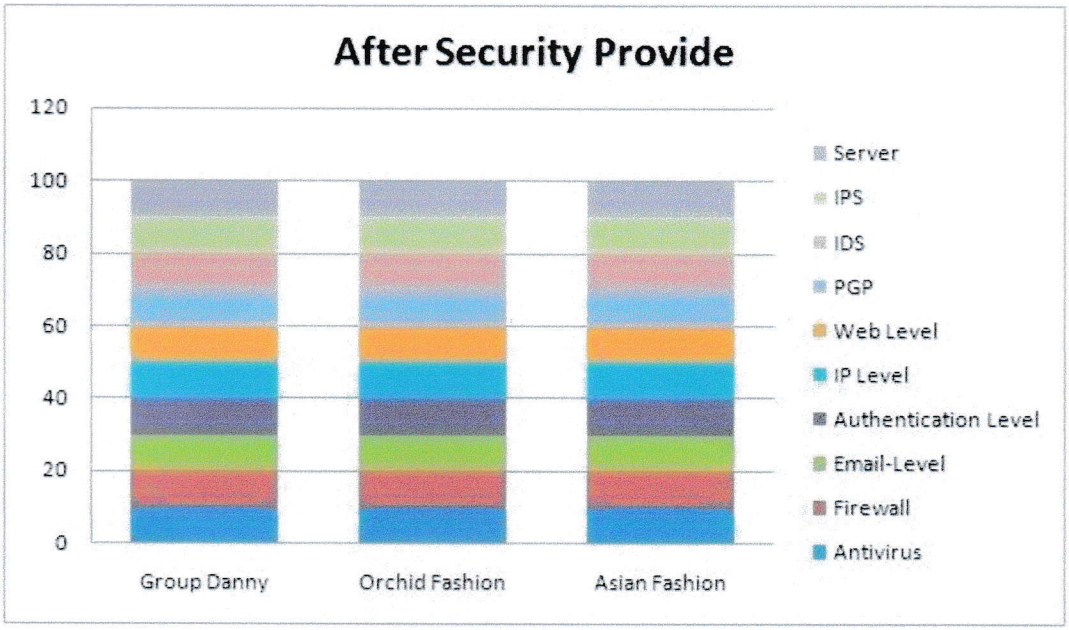


Fig 6.9: Gantt Chart Of after security provide

Chapter 7

TESTING RESULTS

7.1 Overview

As detail study of the network elements "*hardware & Protocols*", we can find out the existence network vulnerabilities, which can be examined by design and implementation of a real network.

7.3 Result

We think we succeed to give advance level security for official sector and they are satisfied to get our security solution and now they are 80% secured, for safe their data from hacker's. Because we have able to protect our targeted office from cyber attack in network, and secured their office all pc's from dangerous virus infection.

Chapter 8

CONCLUSION AND FUTURE WORK

8.1 Conclusion

The aim of this thesis was to explore the network vulnerabilities and in-depth analysis of different security attacks and security solutions. Security is not about a specific firewall, product, brand and operating system. Properly configured firewalls, strong passwords that changed on regular basis, antivirus update on regular basis etc all these elements used collectively to good security practices. Deficiencies in bad products can defeat with good practice, whereas bad process can be diluted otherwise excellent products. It is better to have no security devices instead of incorrectly configured security devices. As we observed in first scenario of simulation, in which configuring the network parameters on default mode will allow resources even to use by unauthorized users. Similarly in second scenario setting the network on deny everyone will cause to stop working even network administrators. Some time deployment of security can affect the Quos of network as we observed in third scenario that tunnel mode utilizes half of the network bandwidth which decreases Quos and introduces delay factor. The bottom line is that a network cannot 100 percent secure. However we can guarantee better security by analysis our network. This analysis will helpful to find out the vulnerabilities in network. For example before introducing a firewall in network first analyze it that, does it integrate with the network, will it fulfills your future demands, will it reliable, scalable and maintainable, is it possible to upgrade it and compatible with new products and new software's. This analysis will use as a baseline for designing a better security plan.

"The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable."

8.2 Future Work

Experts agree that today's major challenge is not the security technology itself but how to make appropriate procedures and controls for achieving IT security. Hackers will still remain in the market and even their numbers seem to be growing. Emerging trends in IT arena will leading the world to a point where computers will do even more for us than they are doing now. Technology development never
stands stills. Attacking tools will continue to advance, as will security solutions. If someone tries to stay up-to-date with every new threat soon he/she will be stress. It is better to look for the major vulnerabilities and try to eliminate them using with existing resources. It will be our continuous process, always we will find new method or tricks for prevent hacking. And day-by-day our security level will be stronger.

References:

1. TCP/IP Guide,http://www.tcpipguide.com/free/t_TheBenefitsofNetworkingModels.htm
2. Data Link Layer ,https://en.wikipedia.org/wiki/Data_link_layer
3. TCP/IPTutorial,http://www.fujitsu.com/downloads/TEL/fnc/pdfservices/TCPIPTutorial.pdf
4. TheJavaTutorial,http://java.sun.com/docs/books/tutorial/networking/sockets/definition.html
5. Application layer,https://en.wikipedia.org/wiki/Application_layer
6. Message transfer agent ,http://en.wikipedia.org/wiki/Message_transfer_agent
7. Glossary of Internet Security Terms,http://www.auditmypc.com/glossary-of-internet-security-terms.asp
8. Introduction to System Software, http://en.wikiversity.org/wiki/Introduction_to_Computers/System_software
9. Unauthorized Access Computer Network Crime, http://www.dba-oracle.com/t_unauthorized_access_computer_network_crime.htm
10. Book Ref 1:W. Richard Stevens ,TCP/IP Illustrated, The Protocols, volume1
11. Book Ref 3:William Stallings, Network Security Essential, Applications and Standards
12. Book Ref 4:Uyless Black, Internet Security Protocols, Protecting IP Traffic
13. Book Ref 5:Craig Hunt, TCP/IP network administration
14. Book-Computer Systems Laboratory,http://csrc.nist.gov/publications/nistbul/csl94-03.txt
15. Book of Hacker,http://www.webopedia.com/TERM/H/hacker.html
16. Book Bryant Advantage,http://www.thebryantadvantage.com/CCNASecurityCCNPISCWT CPIntercept.htm
17. What is Packet Sniffer,http://www.wisegeek.com/what-is-a-packet-sniffer.htm
18. Understanding Port Scans and Ping Sweeps,http://www.linuxjournal.com/article/4234
19. Cisco Security Intelli Shield Alert Manager Service,http://www.cisco.com/en/US/services/ps2827/ps6834/services_overview0900aecd8 03e85ee.pdf

20. Network Security Attack,www.sanog.org/sanog1/networksecurity1.ppt

21. Intrusion Prevention System ,http://en.wikipedia.org/wiki/Intrusion_prevention_system

22. Cisco Security Intelli Shield Alert Manager Service,
URL:http://www.cisco.com/en/US/services/ps2827/ps6834/services_overview0900aecd803
e85ee.pdf

23. AsymmetricCryptography,https://searchsecurity.techtarget.com/definition/asymmetric-cryptography

24. Key Distribution,
https://www.techopedia.com/definition/12883/key- distribution-
center-kdc- cryptography,https://www.instantssl.com/https-
tutorials/digital-signature.html

25. Asymmetric,https://cryptography.io/en/latest/hazmat/primitives/asymmetric/

26. Symmetric
cryptography,https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.14/gt
ps7/s7symm.html

27. Secret Key Algorithm,https://searchsecurity.techtarget.com/definition/secret-key-algorithm

28. Cryptography,https://en.wikipedia.org/wiki/Cryptography

29. What is the Conventional Encryption
Model,https://www.electronicsmedia.info/2017/12/22/what-is-the-conventional-
encryption-model/

30. InternetProtocolSecurity,https://searchsecurity.techtarget.com/definition/IPsec-Internet-Protocol-Security

31. Web Application Security, https://en.wikipedia.org/wiki/Web_application_security

32. What is SSL/TLS/HTTPS,https://www.websecurity.symantec.com/security-topics/what-is-ssl-tls-https

33. Transport Layer Security,https://en.wikipedia.org/wiki/Transport_Layer_Security

34. Intrusion Prevention System,http://en.wikipedia.org/wiki/Intrusion_prevention_system

35. Secure Electronic Transaction,https://www.geeksforgeeks.org/secure-electronic-transaction-set-protocol/

36. System Level Solution,https://www.indiamart.com/system-level-pvtltd/profile.html

37. Intrusion Detection System ,https://searchsecurity.techtarget.com/definition/intrusion-detection-system

38. Intrusion Detection System ,https://en.wikipedia.org/wiki/Intrusion_detection_system

39. Network Based Intrusion Detection,https://www.comparitech.com/net-admin/nids-tools-software/

40. Network Intrusion Detection System,http://www.real-time.com/linuxsolutions/nids.html

41. Host Based Intrusion Detection Systemhttps://www.techopedia.com/definition/12826/host-based-intrusion-detection-system-hids

42. Host Based Intrusion Detection System https://sites.google.com/site/idpsinfo498/home/host-based-intrusion-detection-systems---hids

43. Distributed Intrusion Detection System,http://seclab.cs.ucdavis.edu/papers/DIDS.ncsc91.pdf

44. Intrusion Detection Prevention Systems,http://www.just.edu.jo/~tawalbeh/aabfs/iss6750/presentations/IDPS.ppt

47. Intrusion Detection Prevention Systems, https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

48. Authentication Level Security, https://docs.microsoft.com/en-us/windows/desktop/com/authentication- level

49. Authentication Level,http://ec.europa.eu/information_society/activities/ict_psp/documents/authen_level_status.pdf

50. Anti Virus Protection,

51. http://www.symantec.com/connect/articles/behavior-blocking-next-step-anti-virus-protection

52. Kaspersky,https://www.kaspersky.com/internet-security

53. Digital Immune System,http://www.ques10.com/p/7642/explain-digital-immune-system/

54. Malicious Software, https://docplayer.net/4045958-Malicious-software-chapter-21-1-21-1-types-of- malicious-software-backdoor-logic-bomb-trojan-horses-mobile-code-multiple-threat-malware-21.html

55. Firewall,http://en.wikipedia.org/wiki/Firewall_%28computing%29\

56. Firewall Knowledge,http://www.vicomsoft.com/knowledge/reference/firewalls1.html

57. Network Denial of Service Attacks,http://etutorials.org/Linux+systems/unix+internet+security/Part+V+Handling+Security+Incidents/Chapter +24.+D enial+of+Service+Attacks+and+Solutions/24.4+Network+Denial+of+Service+Attacks/