

A STUDY ON CYBER SECURITY

BY

ABdifatah Ahmed Mohamed

ID: 211-17-469

This Report Presented in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Management Information System

Supervised By

Dr. Sheak Rashed Haider Noori

Associate Professor

Department of CSE

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

JULY 2022

APPROVAL

This Thesis/Project titled “a study on cyber security”, submitted by **Abdifatah Ahmed Mohamed, ID 211-17-469** to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of MS in Management Information System and approved as to its style and contents. The presentation has been held on 27 June 2022.

BOARD OF EXAMINERS



Dr. Sheak Rashed Haider Noori
Associate Professor and Associate Head
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Chairman



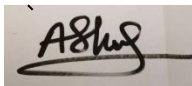
Naznin Sultan
Assistant Professor
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Mr. Md. Sadekur Rahman
Assistant Professor
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Dr. Md. Ashraful Islam
Associate Professor
Department of ICE
University of Rajshahi

External Examiner

DECLARATION

I hereby declare that this thesis has been done by me under the supervision of **Dr. Sheak Rashed Haider Noori, Associate Professor, Department of CSE** Daffodil International University. I also declare that neither this thesis nor any part of this thesis has been submitted elsewhere for award of any degree or diploma.

Supervised by:



Dr. Sheak Rashed Haider Noori,
Associate Professor & Associate Head,
Department of CSE
Daffodil International University

Submitted by:



ABdifatah Ahmed Mohamed

ID: -211-17-469

Program: M.S of MIS

Department of Management Information systems

Daffodil International University

ACKNOWLEDGEMENT

In the name of Allah, the most compassionate the most merciful praise be Allah for giving me the strength and commitment to complete this level in my master.

This thesis could not have been accomplished by myself a humble and lucky human like me Must seek Allah almighty to provide me the chance to go through this process **Sheak Rashed Haider Noori, Associate Professor & Associate Head**, Department of CSE Daffodil International University, Dhaka for the study opportunity and for the technical assistance during the last phase of finishing this thesis.

I am grateful to my beloved parents, both my father and mother may Allah protect them, they are always very understanding and supportive of my choices.

I would like to thank my entire course mate in Daffodil International University, who took part in this journey while completing the course work.

ABSTRACT

In recent years, a study on cyber security have become more prevalent. New mobile solutions are being created in the form of Internet-capable mobile devices like the iPhone and new wireless networks like LTE and WiMAX. From a security standpoint, this research will present, explain, and compare some of the most widely used wireless networks that support mobile payments. 3G networks with GSM and WLAN connectivity were chosen. Each network's primary security methods will be investigated, as well as how they function. Security needs will be highlighted, as well as some of the most serious dangers that any network confronts. The purpose of this technical paper is to solve the problem of cyber security. It looks into the growing risks and difficulties that the cyber world is facing. The rise in worldwide Internet usage has surely resulted in an expansion in internet-based services, as well as better information exchange and communications.

As a result of these substantial changes, traditional systems are no longer capable of dealing with ever-evolving threats. The goal of this document is to inform the industry on the effectiveness of existing countermeasures by addressing these dangers, problems, and potential hazards.

Table of Contents

| | |
|--|----------|
| Approval | ii |
| Declaration | iii |
| Acknowledgements | iv |
| Abstract | v |
| Chapter one | 1 |
| 1.0 Introduction | 1 |
| 1.1 Background | 4 |
| 1.2 Problem statement | 5 |
| 1.3 Objectives | 6 |
| 1.4 Justification | 7 |
| 1.5 Scope of Study | 7 |
| Chapter two | 8 |
| 2.1 Literature review | 8 |
| 2.2 Categories of security threats | 8 |
| 2.2.1 Unstructured threats | 9 |
| 2.2.2 Structured threats | 9 |
| 2.2.2.1 External threat | 9 |
| 2.2.2.2 Internal threat | 9 |
| 2.3 Physical installation attack | 10 |
| 2.4 Device communication attack | 11 |
| 2.4.1 Physical layer | 11 |
| 2.4.2 data link layer | 12 |
| 2.4.3 Network layer | 14 |
| 2.4.4 Transport layer | 15 |
| 2.4.5 Session layer | 15 |

| | |
|---|-----------|
| 2.4.6 presentation layer | 15 |
| 2.4.7 Application layer | 16 |
| 2.5 Reconnaissance attacks | 17 |
| 2.5.1 Access attack..... | 17 |
| 2.5.2 Password attacks | 17 |
| 2.5.2 Denial of Service attacks | 18 |
| 2.5.3 Worm, virus and trojan horse attacks | 18 |
| Chapter three | 20 |
| 3.1 Methodology | 20 |
| 3.2 Chosen methodology | 20 |
| 3.3 Requirement gathering technique | 21 |
| Chapter four | 24 |
| 4.0 Introduction..... | 24 |
| 4.1 Hardware threat mitigation | 24 |
| 4.2 Mitigation of environmental threats..... | 24 |
| 4.3 Electrical threats mitigations..... | 24 |
| 4.4 Maintenance-related threat mitigation | 25 |
| 4.5 Packet Sniffer attack mitigation | 25 |
| 4.6 Port scan and ping sweep attack mitigation..... | 26 |
| 4.7 Access attacks mitigation..... | 27 |
| 4.8 Trust exploitation attack mitigation | 27 |
| 4.9 Man-in-the-middle attack mitigation | 27 |
| 4.10 Denial of service attacks and mitigation..... | 27 |
| 4.11 Mitigating worm attacks | 28 |
| 4.12 Application layer attack mitigation..... | 29 |
| 4.13 Securing Remote Access..... | 29 |

| | |
|---|----|
| Chapter five | 24 |
| 5.0 Introduction..... | 30 |
| 5.1 Seeking out problems before they happen | 31 |
| 5.2 Basic risk | 31 |
| 5.3 Level of impact | 32 |
| 5.4 Everyone’s responsibility | 32 |
| 5.5 Risk management Techniques | 33 |
| 5.5.1 Reduce the Risk | 33 |
| 5.5.2 Risk avoidance..... | 34 |
| 5.5 Identify Vulnerabilities | 34 |
| 5.6 Gather Information..... | 35 |
| 5.7 Implement Recommendation | 35 |
| 5.8 Disaster Recovery Plan..... | 36 |
| 5.9 Keep Documentation Simple and Clear..... | 37 |
| 5.10 Communication and Consult..... | 38 |
| 5.11 Monitor and Review | 38 |
| 5.12 Investigate anomalous activities | 39 |
| 5.13 Summary of Risk Assessment | 40 |
| 5.14 Conclusion | 41 |
| REFERENCE | 42 |
| PLAGIARISM | 45 |

LIST OF FIGURES:

| FIGURES | PAGE NO |
|--|----------------|
| Figure 1.1: cyber security | 2 |
| Figure 1.2: diagrammatical Representation of DoS | 3 |
| Figure 2.1: Physical installation | 10 |
| Figure 2.2: physical layer | 12 |
| Figure 2.3: Data link layer | 13 |
| Figure 2.4: Network layer | 14 |
| Figure 3.1: SDL diagram | 21 |
| Figure 3.2: ER diagram | 22 |
| Figure 3.3: DFD diagram | 23 |
| Figure 4.1: packet addressed diagram | 26 |
| Figure 5.1: disaster recovery plan | 36 |

CHAPTER ONE

INTRODUCTION

1.0 Introduction

With the advent of the Internet and new networking technology, the world is becoming increasingly interconnected. On networking infrastructures around the world, there is a large amount of personal, commercial, military, and government data. Network safety is turning into of extraordinary significance due to highbrow belongings that may be without difficulty received thru the net. There are presently essentially specific networks, information networks and synchronous community created from switches. The net is taken into consideration an information community. Since the modern-day information community includes pc-primarily based totally routers, data may be received via way of means of unique programs, along with “Trojan horses,” planted with inside the routers. The synchronous community that includes switches does now no longer buffer information and consequently aren't threatened via way of means of attackers. That is why safety is emphasized in information networks, along with the net, and different networks that hyperlink to the net.

Cyber safety, frequently called IT safety or pc safety, is the safety of data structures in opposition to destruction, theft, and interruption, in addition to carrier misdirection. It involves restricting bodily get admission to in addition to safeguarding in opposition to threats along with code and information injections, unauthorized community get admission to, and malpractices. Because of the growing price of pc utilization throughout the global, this region is extraordinarily important. Apart from individualized information networks and the Internet, today`s pc structures incorporate a whole lot of clever gadgets, and networks encompass Wi-Fi and Bluetooth [1].

Cyber safety covers the mechanisms and techniques upon which data, virtual device and offerings are safeguarded from unauthorized or unlawful get admission to, destruction, or alteration and the procedure of enforcing security features purposely to make sure integrity, confidentiality, and availability of information.



Figure 1.1: cyber security.

History

Network safety became a factor while people started out information that there has been herbal really well worth in statistics. This took place in a development of activities because the Information and Digital Age unfurled with inside the remaining a part of the 20th century hundred years.

In the remaining a part of the Sixties and into the mid 1970`s, automatic ability became a reality. Huge, room measured centralized computer systems had been liable for setting away this information, and admittance to the one`s ability storehouses turned into conceded through preventing straightforwardly into the centralized laptop itself or attending to the centralized laptop's statistics from certainly considered one among several terminals with inside the shape. Early adopters of automatic stockpiling innovation did not have a problem safeguarding agency sensitive information as you absolutely have to be in the shape to get to the information.

Under 10 years after the fact, as an ever-growing quantity of statistics turned into placed away, there has been a extrude in thinking: Data had really well worth and full-size helpings of through and through recognizable information. During this shift, information started out becoming a product. Visa statistics, monetary stability numbers, gain and misfortune explanations, man or woman subtleties, section information on full-size population gatherings...

From infections and worms to Advanced Persistent Threats (APTs) and disavowal of-administration (DoS) attacks, the refinement, scale and impact of virtual attacks have modified essentially at some stage in the lengthy term. Notwithstanding, because the wrongdoing is gradually turning into refined, the counter-measures have pursued a similar direction. Achievement episodes over the past 1 / 4 century it appears that evidently exemplify how the hazard scene has improved and the consequent protection efforts. During the remaining a part of the 80's, Robert Morris fostered a self-engendering, PC computer virus [1]. The contamination spreads fast and forcefully that it stimulated intensely on internet access. Albeit ensuing attacks are similarly developed, the computer virus turned into a putting incidence considering that it turned into the important instance of DoS assault (see discern 2-1).

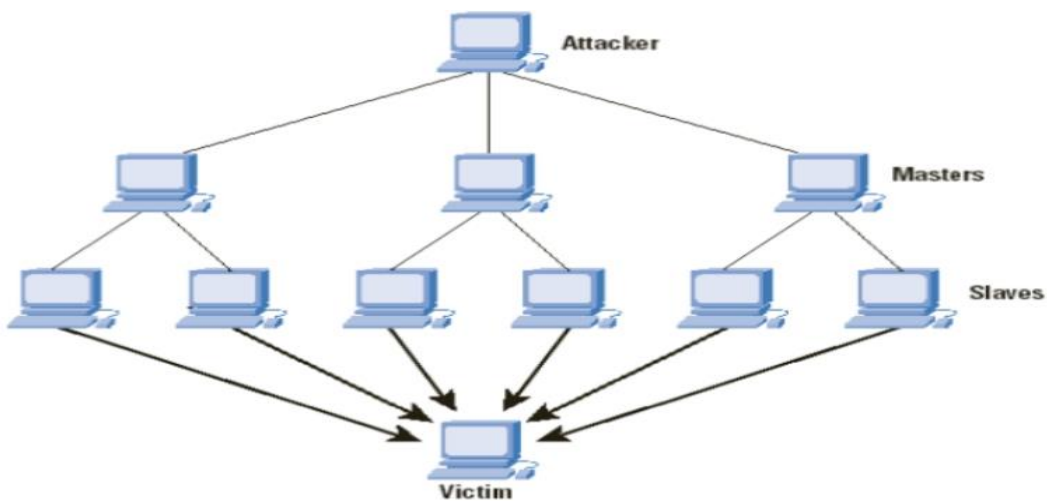


Figure 2-1: Diagrammatical Representation of DoS. [1]

However, since the Internet was at its infancy, the resultant impacts were less devastating. On the contrary, such developments formed the foundation of the security issues experienced today. Worms and other DoS attacks were some of the instances of dealing with- and responding to- cyber-security attacks. Ultimately, they led to the development of the cyber security industry, as well as CERTs as the hub for the co-ordination of responses. In the security industry, the current status is that cybercrime is highly sophisticated and seemingly impossible to control. Therefore, the emphasis is on the manner in which organizations respond to security breaches. Whilst it is impossible to prevent every incident, it is possible to control ways of managing the aftermath to ensure preparedness in terms of response. Such measures will foster development of organizational resilience to ensure possible threats are managed gracefully as other business processes [2].

1.1 Background

As the number of computers and networked systems grows in today's society, so does the demand for more and better computer and network security. Because of the rising use of computer networks.

Numerous networks have been exposed to various types of internet threats, and as an outcome of this exposure, better network security is essential for every business. Identity, authentication, and authorization, as well as surveillance cameras, may be used to ensure the integrity, availability, accountability, and authenticity of computer hardware or network equipment.

There appears to be no one-size-fits-all method for placing collectively a normalized. Network protection ought to be tailor-made to the desires of an unmarried affiliation company, now no longer to the desires of every other individual. For instance, a small regulated company would possibly permit accredited customers outdoor the company get admission to case statistics at the same time as making sure that complete net get admission to is constantly to be had to personnel inside the company, in case they want to get admission to a case record from the workplace or at the same time as out and about. Great company protection protects a company in a manner this is steady with its motivation and protection measures must be taken while choosing a company issuer for a company, specifically a regulation firm [3].

1.2 Problem statement

Malware, virus, Trojan horse, and hacker attacks are only a few examples of network security. Human nature and accidental human mistake both have the potential to disrupt network security.

The company's workers and their different faults are a typical network security concern (Employees) that most firms face at times. "Humans make errors," says Dr. Michael E. Whitman, CISM, CISSP, author of the textbook "Principals of Information Security." "Sometimes this is due to inexperience or bad training, and other times it is owing to an inaccurate assumption."

But regardless of the reason and the lack of malicious intent something as simple as a keyboarding error has the potential to cause a worldwide Internet outage”.

The issue of piracy is another normal organization issue.

Piracy is what occurs when scholarly properties are compromised, despite the fact that there are specialized components that assist in the implementation of intellectual property regulations to address the problem.

In any case, network security problems can be caused not only by human errors, but also by natural disasters such as fires, earthquakes, floods, and lightning strikes.

An undeniably powerful and actually testing risk climate has changed the way network managers think about getting networks.

To power enterprise forward, new techniques depend on open businesses with a couple of access points, reducing expenses and growing reaction to revenue. By leveraging the cap potential to quick change fundamental data, percentage enterprise data or envelopes, and develop their aggressive position, they devise a precious open door.

1.3 Objectives

This proposal gives an outline of strategies to moderating current attacks as well as suggestions for forestalling repeat since assault advancement is ceaseless. goals are to uncover and characterize the idea of a PC network assault and danger, to extra class relieving strategies used to stay away from dangers and assaults, to exhibit the method for carrying out best security rehearses, and to grow the acts of a pariah planning to get close enough to the organization to the organization engineer.

Security is a broad term that does not appear to be great in any circumstance. Known attacks can be reduced using a lot of techniques, including:

- The creation of a security strategy.
- Staff schooling on the best way to utilize the Internet appropriately.
- Set up security programming like MacAfee, Norton, ESSET, and others. VLAN (Virtual LAN) creation and substantially more [4].

1.4 justification of study

With the growing reliance on computer systems for data processing and storage throughout the world, the importance of authentic information and data security cannot be overstated. Unauthorized access, disclosure, or destruction of data can jeopardize individual privacy and potentially jeopardize an organization's existence. Because information is seen as an organization's lifeline, it is critical to protect computer systems and data stored on them.

1.5 scope of study

This thesis begins with an overview of how networking became associated with insecurity, as well as the security challenges that network administrators face as a result of the organization's need to expand.

It then actions directly to a examine the present-day trouble and the way it may be solved. The OSI layer is used to define recognized assaults and to explain the numerous channels via which an organization's community may be compromised. The advent of a server that ensures that no intruder can get admission to the community remotely is likewise covered, as are the numerous strategies of mitigating known attacks.

CHAPTER TWO

LITERATURE REVIEW

Rapid access to records on the Internet is becoming an increasingly essential part of expanding your business. As government agencies begin to extend multiple business functions to public networks, their own data protection is urgently needed, negatively impacting enterprise productivity and delaying capacity limits to compete with individual enterprises. Unauthorized access to the network can adversely affect transactions with customers and partners, and can question retailers' ability to protect private records. Moreover, as mentioned above, any part of the network can be vulnerable to attacks and fraudulent gains. Corporate resistance, or perhaps, member of staff can hurt routers, switches, or hosts. To determine the appropriate way to protect the assets of a for-profit organization from attackers, IT managers of such for-profit organizations understand the attacks and turmoil that can be brought to the infrastructure of the for-profit organization is needed.

2.1 literature review

Multiple network attacks detected due to the device trying to break in. Attacks are appeared to each be intentional or unintentional and technically able to intruder have been inquisitive about targeted at the protocols used for strong communication amongst networking devices. This assessment addresses how pretty brand-new intruders are penetrating internet networks irrespective of immoderate levels of security. But due to the fact the intruders increase, the network experts are deriving many techniques in preventing attackers from getting access to company networks.

2.2 categories of security threats

Security risk may be classified into four components and those classes are the approaches or paperwork via which threats may be achieved on a network [5].

2.2.1 Unstructured threats

Unstructured security danger is the type of risk made through a green person trying to benefit get right of passage to an organization. They regularly utilize generally to be expected spot hacking devices, similar to shell contents, and secret word saltines. A right security answer necessities to without issues obstruct this type of assault. In various words, programmers like that couldn't be undervalued because of the reality they could reason serious mischief to organize.

2.2.2 Structured threats

Unlike unstructured threats, based risk hackers are nicely skilled and extraordinarily state-of-the-art. They use state-of-the-art hacking equipment to penetrate networks and they could ruin into authorities or enterprise computer systems to extract information. On sure occasions, based threats are completed with the aid of using prepared crook gangs or enterprise competitors.

2.2.2.1 External threat

Some unauthorized humans out of doors the business enterprise who do now no longer have get admission to the business enterprise's laptop gadget or community may want to reason outside threat. They generally damage into business enterprise's community through the Internet or server. Both skilled and green hackers may want to pose outside threats [6].

2.2.2.2 Internal threat

This type of threat can be with the aid of using a disgruntled worker who has legal get admission to the corporation network. Like outside threats, the harm that might be resulting from the sort of hacker relies upon at the understanding of the hackers.

2.3 physical installation attack

Physical attacks because the choice proposes come from a few huge dangers that we see straightforwardly however will most likely be now no longer capable of forestall. To begin with, system risks are an exemplary example of truly completed assaults. This might be because of the age of the chosen framework, which makes the framework begin going for walks whimsically and degenerate some data in advance than it's far surely closed down. As referenced in advance than, ecological risks can be because of plant peculiarities like outrageous climatic temperatures, tremors, and tempests. Furthermore, electric powered perils should make essential harm your agency. This type of peril is absolutely anticipated in international locations wherein strength supply is suddenly and continuously interfered. Instances of this type of peril incorporate blackouts (abrupt blackouts of strength supply), voltage drops (negative strength supply), and relieving (genuine strength). Upkeep dangers can likewise activate agency issues. Instances of recovery risks incorporate awful wiring, negative wire marks, electrostatic release, and the absence of easy new parts.

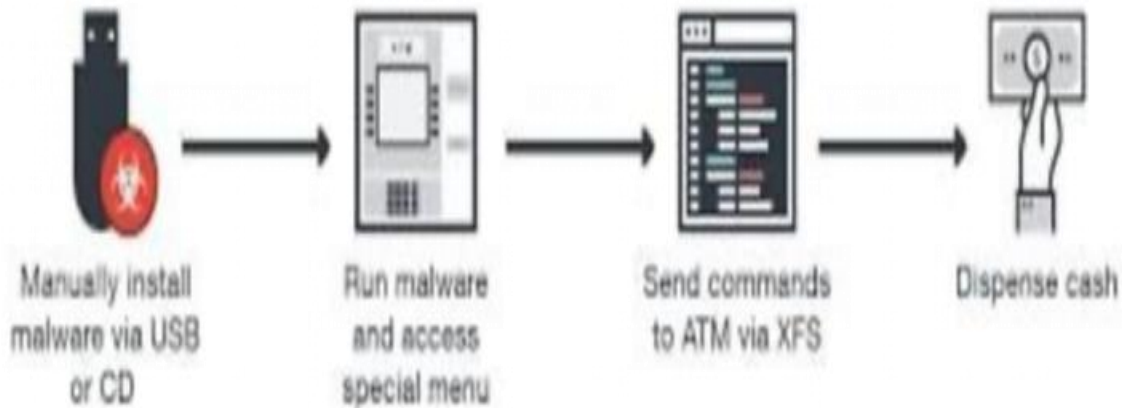


Figure 2.1: physical installation attack

2.4 device communication attack

Actually, capable hackers had been capable of layout a prepared attack centers on at communicate conventions. The OSI display has seven layers which are applied for communicate among organizing gadgets that are with vulnerabilities that may be controlled. Essentially, better layers can't be secured while the decrease layers are too now no longer being secured, but in later a long term there was limited attention to frailties on the bodily layer or statistics interface layer notwithstanding adjustments in prepare operational hone that comprise upgrades like nation-wide layer two systems and national and territorial optical systems. Right now, known dangers at lower levels of the OSI stack incorporate ARP spoofing, MITM (man-in-the-middle) assaults at layer two, and physical layer assaults such as inactive optical taps or the interferences of remote organize signals by aggressors. Whereas these assaults are well known, small investigate is right now centers on tending to those concerns

2.4.1 Physical layer

The Physical Layer is answerable for conveying information through verbal communication. It can also be called the most volatile and vulnerable layer. Small problems, such as unplugging a laptop's power cord or dropping a community cable, can sometimes cause significant havoc that cannot be found in a particular community, and can cause havoc. Significant damage to the laptop. There are a lot of holes that the body layer has to face, including: lack of environmental control, hardware and information damage, disconnection of bodily information links, strength loss, enter logging such as keystroke and other bodily robbery of information and hardware, and undetectable information interception.

If these vulnerabilities are not addressed in a timely manner, they will cause significant harm to community protection via physical layers. Nonetheless, there are always solutions available for any threat to a community [7].

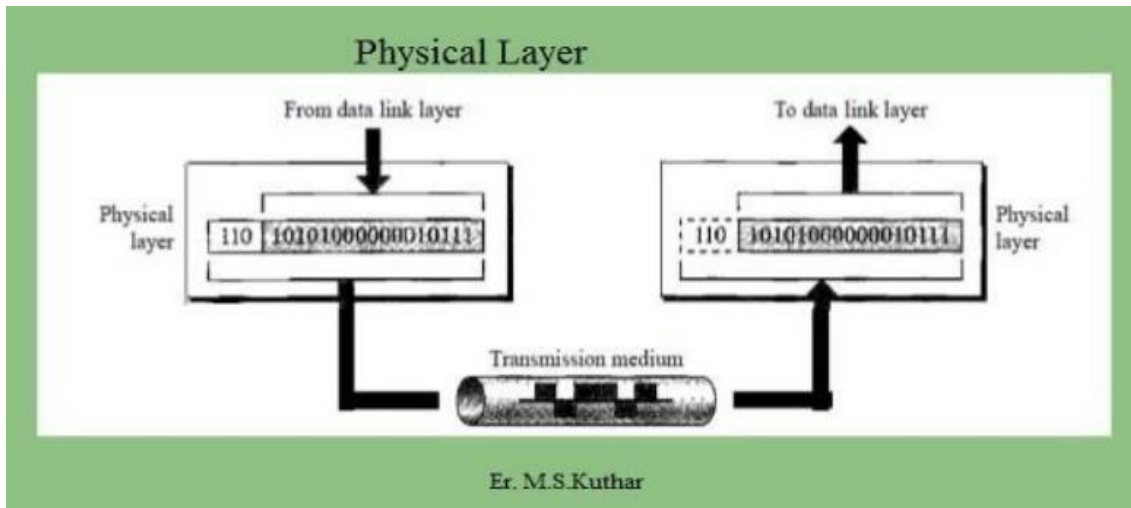


Figure 2.2: physical layer

2.4.2 Data link layer

This is the layer where transmission of information bundles has been arranged by the physical layer. Communication of the information interface is some way or another powerless in terms of security. The key component at layer 2 communications is the switch, which is additionally utilized for communication at layer 3. Information link is helpless to numerous layer 3 assaults. The prime case of the layer 2 component is 'war driving' the strategy of going around looking arrange with default security settings. Vlan in layer 2 switches are too defenseless to attacks. All the osi layers confront distinctive threat that influence them at their different stages. Highlighted underneath are the issues confronted by layer two of the osi demonstrate and the arrangement to the issues. Cam (content-addressable memory) table flood, mac (media access control) spoofing, stp (spanning tree protocol) control, arp (address resolution protocol) attacks, and vlan bouncing are the issues confronted by information data link layer cam may be managed through configuring port safety on

Broadcasting is a great way to provide mac access specifications on the broadcast port of your choice. This learns the mac access specification and saves it across the port, which can lead to

invalid execution on the port. Similar to cam, you can also use port security directives to control mac spoofing attacks.

This order might permit you to determine a security move each time a port security break happens in the exchange. Bpdu security is utilized to control the activity of STP. This extent of security is introduced for local area chiefs who will anticipate a local area Arp attack can be relieved involving the hold down clock in the

Design interface menu this can be finished by adding a passage for the leftover opportunity to the Arp reserve Vlan bouncing control can be performed by giving Vlan id to the storage compartment port, impairing unused sending ports, and putting them in unused Vlan.

.

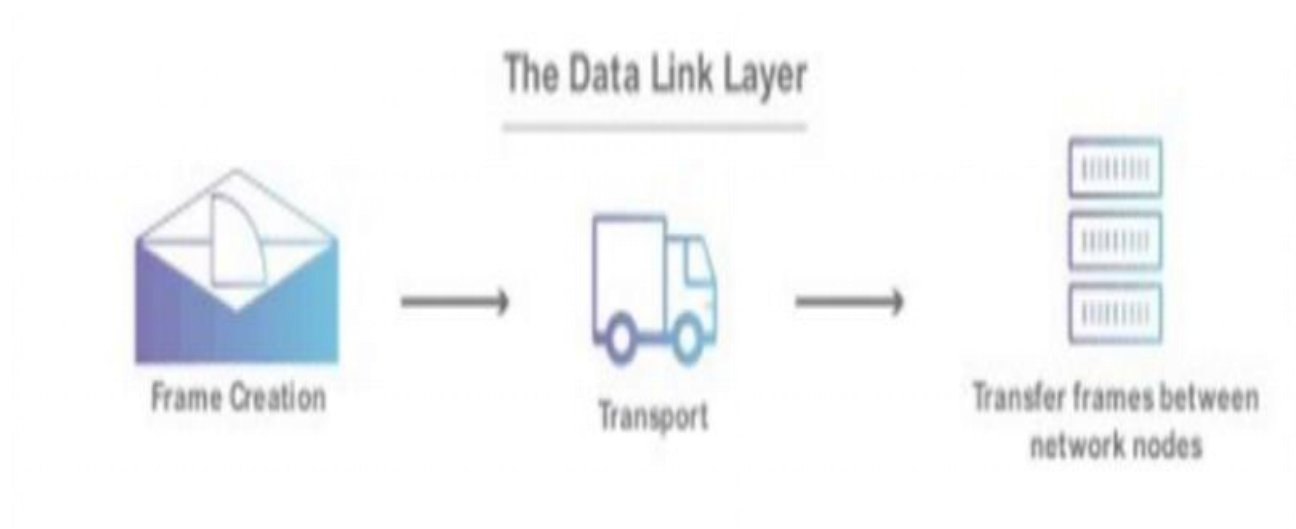


Figure 2.3: data link layer

2.4.3 Network layer

This layer is the medium utilized by a packet to go through numerous bits of information to its last objective. As referenced before in the past part, practically every layer has security challenges.

The third level at the lower part of the osi model is known to confront the difficulties of protection issues and forswearing of administration assaults. Web protocol (Ip) is a notable convention at the organization layer. There are numerous security chances related with network layer Ip. A portion of the security takes a chance with that influence the organization layer is network layer bundle ridiculing, course caricaturing, and Ip address mocking. Directing policy control - this relief gives network directors unlimited authority over the steering conduct of a specific framework.

This control likewise works on the security of the organization. Confirmation packet sniffing can be relieved in different ways. Utilizing major areas of strength for a period secret phrase is one relief technique. It can likewise be constrained by utilizing a changing foundation to balance the utilization of parcel sniffers.

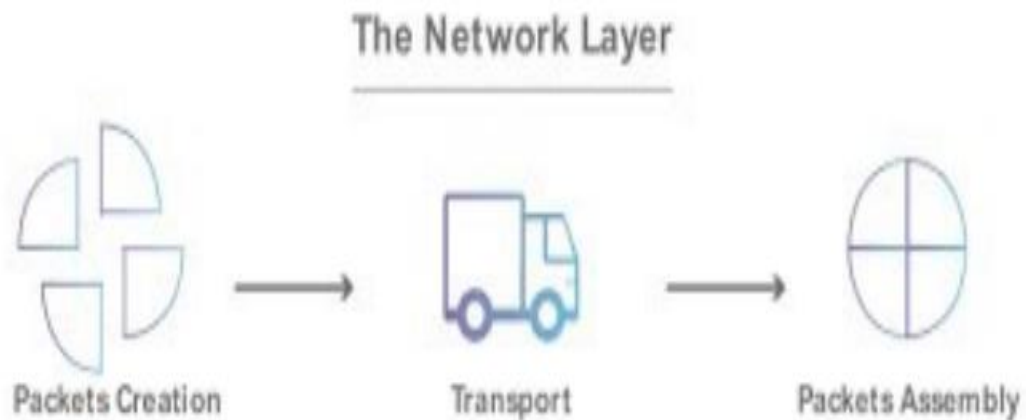


Figure 2.4: network layer

2.4.4 Transport layer

(Transmission Control Protocol) and UDP (User Datagram Protocol) provide uninterrupted communication services to allow data to reach its destination. One of the problems this deposit faces is poor handling of undefined situations. Overuse of certain ports on some features is inadequate in handling undefined situations, as well as differences in delivery protocol implementations and overloading delivery layer mechanisms at the delivery layer. Vulnerability can also occur. The transport layer uses mechanisms such as TCP firewall policies to limit access to specific transmission protocols, and sub protocol statistics must be rigorous. As another countermeasure, the firewall analyses the layer to prevent packets from entering the boundary from overseas, and by applying a stronger ID method to send and retrieve the layer, an attacker can hijack the communication. To prevent [8].

2.4.5 Session layer

The session layer tracks records communications and organizes them into logical flows. This tier additionally creates, manages, and terminates durations among programs and manages report modifications among presentation tier entities. An attacker could use this medium to compromise an organization's network by attempting a myriad of passwords. It can also use more crude methods to exploit possible password chains. Weaknesses in the authentication mechanism used, consulting ID hijacking and spoofing attempts, failed authentication attempts can leak statistics, and an infinitely long failure period helps attackers access their credentials.

2.4.6 Presentation layer

The presentation layer is in charge of receiving carrier requests from the utility layer and issuing carrier requests to the session layer.

Data compression and decompression, and data compression and decompression are the three functions understood by the presentation layer. The presentation layer is one of the safest layers in many OSI models, but it is also one of the most dangerous. Faux certificate assaults and man-in-the-center assaults are commonplace in this residue.

Care must be taken while coping with sudden enter, due to the fact it may crash applications, privateers' safety may be exploited via way of means of cryptography flaws and far off manipulation or data leakage should arise while the use of outside deliver enters unintentionally.

The answer that must be installed location to counter the above-cited vulnerabilities encompass enter getting into the software feature must be cautiously detailed and checked keeping apart consumer enter and software manipulate functions; cryptography answers must be reviewed constantly to make sure modern protection as opposed to rising threats.

2.4.7 Application layer

The software layer is the nearest to the cease client, and it presents customers to assist out the software and the associations.

This affiliation factor may be a possible intention for unapproved use and abuse over the affiliation if the software is frail or unauthenticated. For instance, an intruder has no take a look at in hypothesizing report names in TFTP show, thinking about the manner that username or maybe thriller specific is not alleged to will review with inside the TFTP show. Standard safety manage is bypassed via the roundabout receives to and alertness plan. If safety controls pressure technique is not adequate, it achieves intense get entry to or missing get entry to; whilst software safety is exorbitantly astounding, it's miles a part of the time hard for customers to understand; and application reasoning defects may a part of the time at any factor make applications crash or undesired technique to acting. The use of cause stage get entry to controls to explain permission to software resources, utilization of benchmark in assessing software execution, for instance, software codes evaluations and trendy testing. Using of host-primarily based totally firewall structures to coordinate traffic, software sports and solicitations checked via way of means of the usage of IDs systems are manner to manipulate the shortcomings of cause layers.

2.5 reconnaissance attacks

Administrators have to forget about those attacks because of the form they take to penetrate the community. It generally makes this sort of noise, which leads the administrator to agree with its far simply network noise. Hackers usually use reconnaissance assaults to accumulate facts approximately a selected center community, which they then use to advantage get admission to the community or as dos attacks.

- Packet sniffers, as the name suggests, are a phenomenal instrument utilized by network directors to identify any kind of issue inside the organization. As it is a great device for directors to follow or examine an organization, it is likewise a magnificent instrument for assailants to catch pictures of parcels sent across networks.
- Port scans and ping sweeps are programs that run a series of tests on hosts and devices to identify vulnerable services that must be addressed. These assaults have the ability to try and all offerings at the community. Recognize all hosts and gadgets in the community.
- Information query "who is" is a net weapon used by attackers to view addresses via DNS queries in order to present a targeted company live hosts a focused organization live host. A few facts can be discovered by querying the IP addresses, including the number of addresses and domains associated with the addresses. All discovered facts may inspire an attacker to carry out any attack they intend to carry out.

2.5.1 Access attack

External hackers or internal customers who gain unauthorized access to the community and steal confidential and private data from structures are examples of access attackers. When you delete a material, you can also contact us to hide some statistics that lead to the asset. Different attacks have different motives. Intruders use access to attack networks or structures for three reasons: data collection, access, and enhanced access.

2.5.2 Password attacks

Hashes of passwords might be taken with the aid of using l0phtcrack and the affordable textual content passwords might be made out of them; a savage electricity mystery key attack gives admittance to bills that may be applied to regulate primary agency administrations and records. A common version for such attack that compromises the agency trustworthiness is the factor at which an assailant adjustments the agency's steerage tables. Thusly, the aggressor ensures that every one agency parcels are suggested to the assailant previous to being dispatched to their ultimate objective. In such cases, a gate crasher can display all agency traffic.

There are strategies for figuring passwords with l0phtcrack Dictionary breaking the mystery key hashes for all phrases in a phrase reference report are checked out and registered in opposition to all the mystery phrase hashes for the clients. This is a really short method that tracks down relatively honest passwords [9].

2.5.2 Denial of service attacks

Dos attacks can damage or destroy laptop devices, or the hacking community may be unable to access a network, structure, or offering. Dos attacks are less serious, and people usually view them as very bad because it is easier to carry out. Running dos is simple and harmless, but attacks require special attention by security administrators.

Dos attacks include internet protocol spoofing Ip spoofing this is the method used to gain unauthorized access to your computer. In this method, an intruder sends a message to a laptop with an Ip address that suggests the message came from a trusted and trusted host. Hackers use a variety of techniques to find an Ip address to spoof.

2.5.3 Worm, virus and Trojan horse attacks

A couple of risks are depicted as having minor or fundamental shortcomings for the end-client, which can be dealt with by a layman simply by figuring out what the singular necessities to do. These attacks could be directed by using antivirus programming or resetting the affected machine to handling plant default settings.

- **Virus**

Viruses so-called malicious software, can be related with different applications and perform chosen undesirable or undesirable capabilities on an individual's workstation. The lethal sickness for the most part spreads by tainting different applications on a similar pc in which it dwells.

Viruses can cause serious harm, such as deleting entire garage media or deleting and manipulating files. These types of viruses cannot affect new pcs without staff, usually through document sharing, by inserting a deadly disease-infected document into a cd or as an email attachment.

- **Worms**

The laptop virus is a self-reproducing malware that executes unpredictable code and places a duplicate of itself with inside the memory of an of a tainted PC. The inflamed computer can then taint various hosts. Malevolent obligations are furthermore programming that spreads like infections, however one of a kind to infections that need to spread human media, pernicious obligations can likewise be mechanically spread from PC to next PC with inside the path of the community area. I have. They are usually the use of and advocating the cap potential to deliver and get virtual facts tracked down in numerous PC frameworks [10].

- **Trojan Horse**

Trojans can do two things at the same time it can infected are transmitted and altered, and Trojan horses can attack in three ways. Like a computer virus, it can attack itself like a virus. A virus called a love virus is a classic example of a bug. The love virus contains only dangerous programs, but it pretends to be a love letter. The love computer virus is absolutely annoying as it infects all the photo documents on the compromised hard drive and turns them into new Trojan horses. Finally, the love virus is a computer virus because it spreads over the Internet by hiding in Trojan horses that are sent using the contact address of the attacked email. Make sure the community has not been tampered with or in the hands of malicious people. Accessing the community with the help of hackers and disgruntled employees can disrupt your business.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Methodology

According to methodology, "a context in which to do research" is "a unified as well as rational structure according to ideas, attitudes, and values that guides the decisions Scientists [or even other users] come up with new ideas. It involves a theoretical analysis of a situation branch of the corpus of knowledge procedures and concepts, as well as methods from different Disciplines differed according to their historical development. As a result, a variety of approaches spanning varying viewpoints on the how information and truth are best understood have emerged. This situates procedures inside a larger framework of concepts and approaches. Methodology can be viewed as a continuum spanning from a strictly statistical approach to a primarily qualitative approach.

Regardless of whether a methodology falls into such categories, researchers may combine methodologies to test the research hypotheses, resulting in multimethod and/or mixed method research integral part of managing [11].

3.2 Chosen methodology

System development that we use to develop this system is system development life cycle (SDLC) model specially waterfall model. One of the system developments (SDLC) models is the waterfall model. If the current phase is complete, users can go on to the next step.

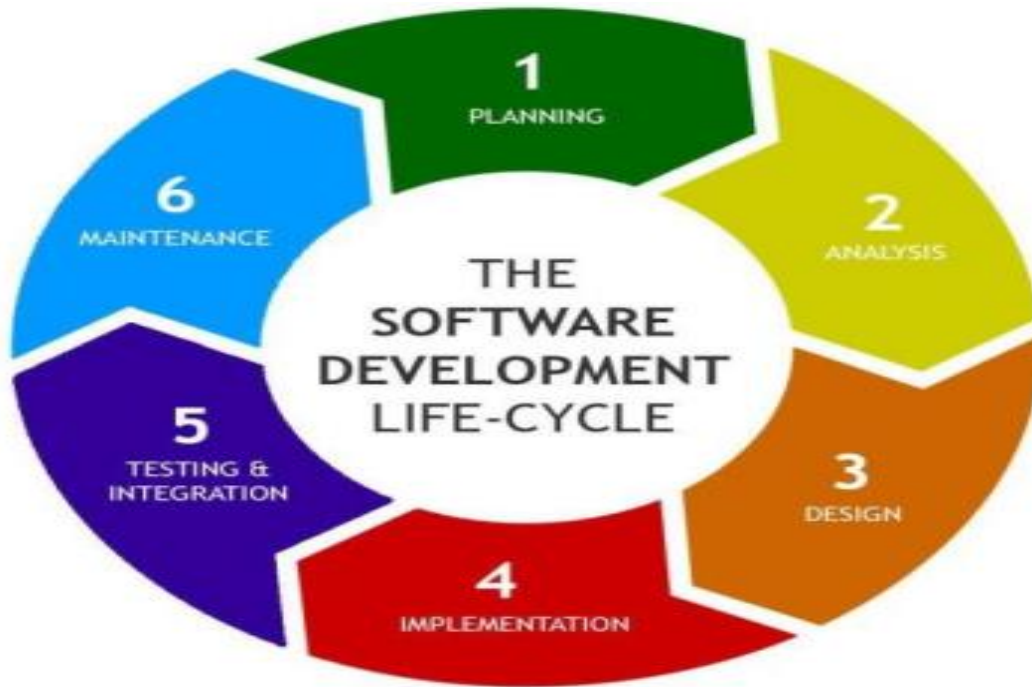


Figure 3.1: SDLC diagram

3.3. Requirement gathering technique

Data collection methods are crucial for component and evaluation study in order to obtain data, thus we used information we gathered in different ways to collect data in our research.

The following are the methods we utilized to acquire data for this study:

- Observations
- Research

ER diagram

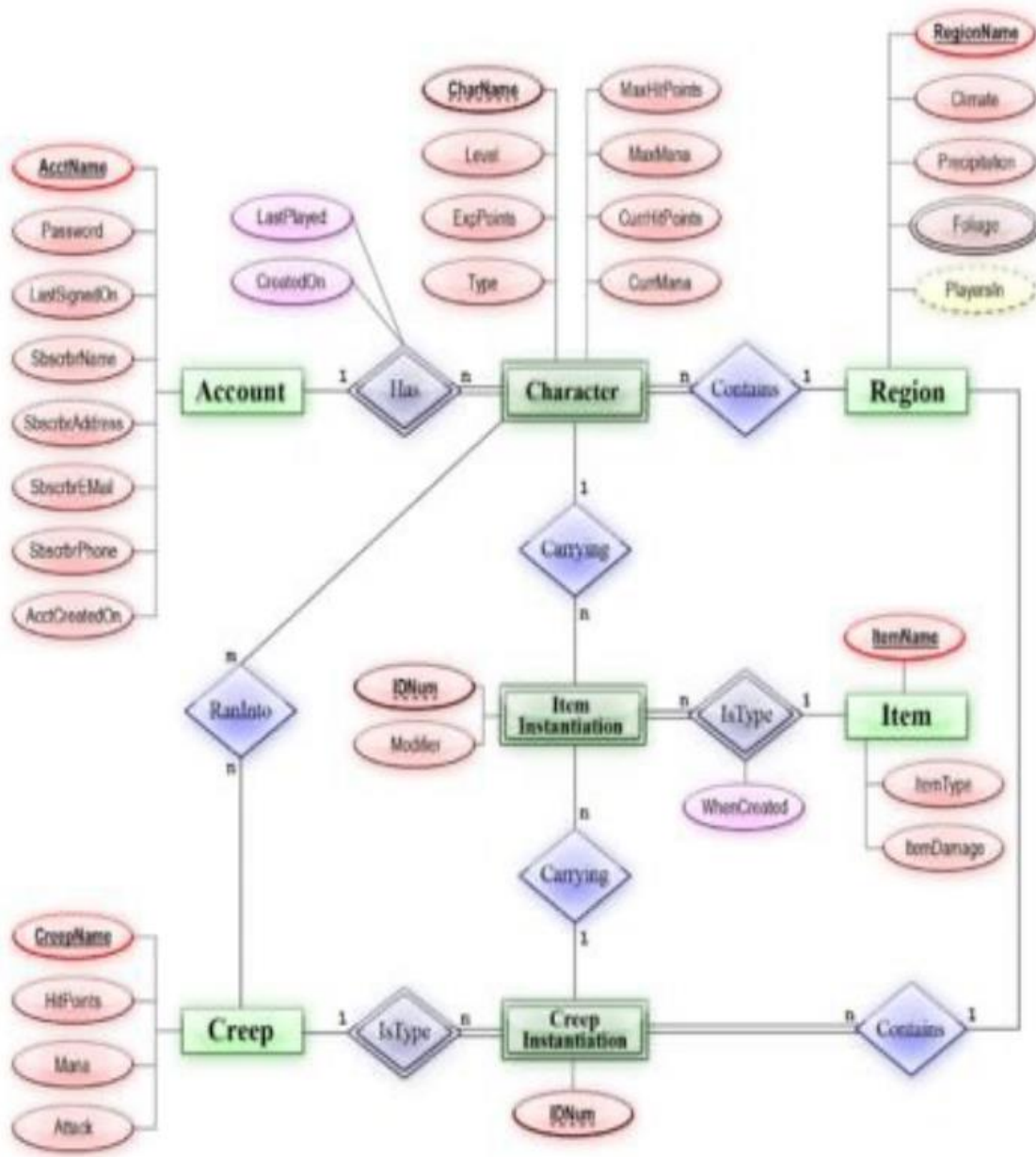


Figure 3.2: ER diagram

Data flow diagram

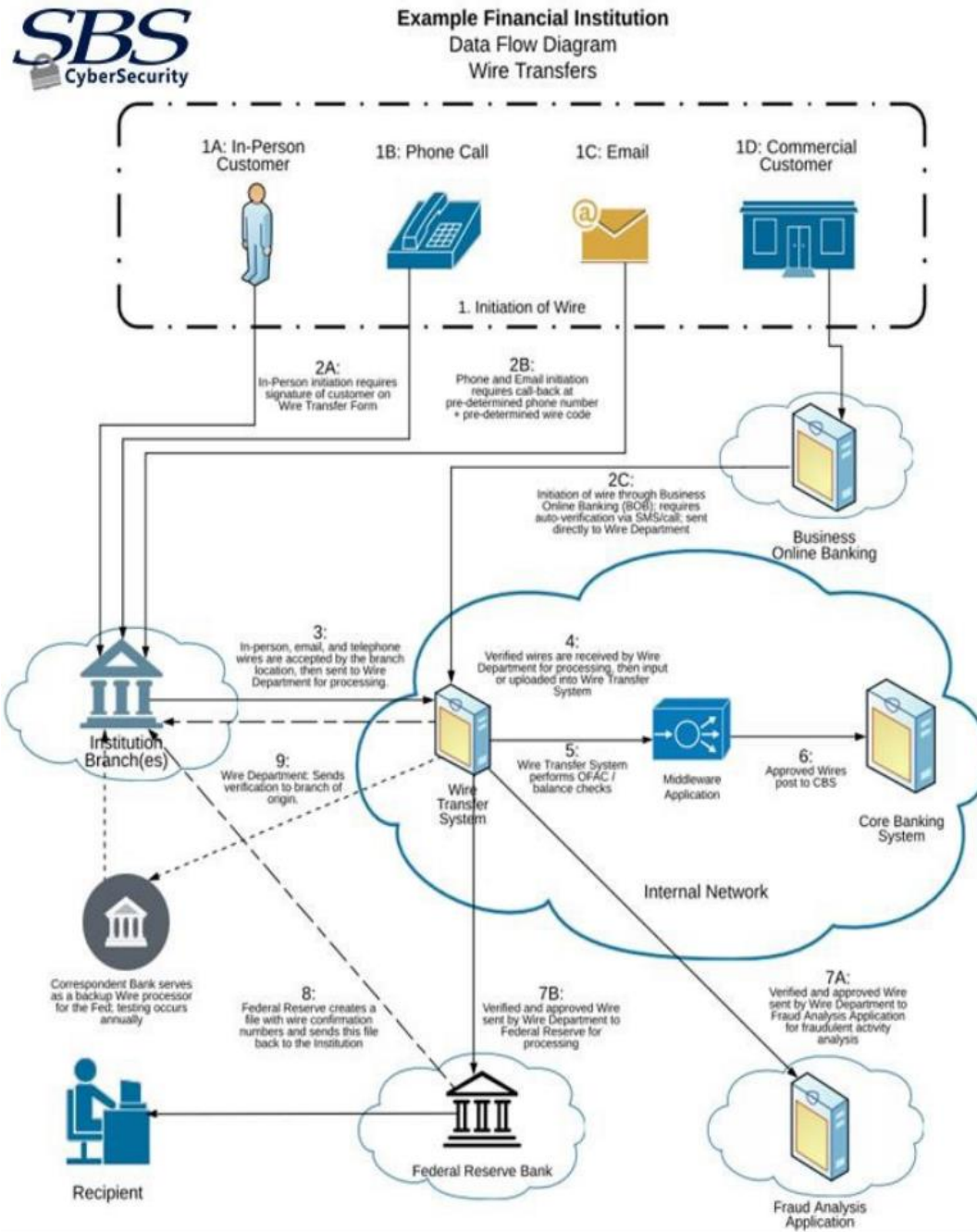


Figure 3.3: DFD diagram

CHAPTER FOUR

DATA ANALYSIS

4.0 Introduction

Finding solutions to mitigate each assault is crucial given the unpleasant situation of multiple attacks and threats which have bedeviled the networking industry. Chapters three and four examine the remedies for the risks stated in the preceding chapters. Section 2 above discussed the many forms of danger facing network security.

4.1 Hardware threat mitigation

Because physical installation mistakes can lead to equipment damage or theft during the installation process, physical security preparation is crucial. Making sure that there is no unwanted entry from of the doors, ceiling, elevated floor, windows, or ducts is only one of the many methods that this activity might be monitored or controlled or vents, keeping an eye on and controlling cupboard entry using electronic logs, using security cameras, and, if it's feasible, using digital access control should all be done. Security systems should also register all entry attempts and be under the authority of security professionals. In Chapter 4 of the thesis, physical security is covered in considerable detail [12].

4.2 Mitigation of environmental threats

Every attack has started with a focus on environmental control, which may be remedied by generating a proper working environment through the regulation of temperature, humidity, and positive ventilation.

4.3 Electrical threat mitigation

A controlled network could be breached during a power outage, which could have been

prevented or regulated in various ways, not all of which are covered here; by ensuring that network devices always have power, by adhering to a preventative maintenance schedule created specifically for the purpose, and by using remote warning and monitoring, electrical hazard can be reduced.

4.4 Maintenance-related threat mitigation

Any firm that employs hardware knows how important maintenance is. Threats linked to maintenance can be reduced by:

- employing tidy cable runs
- Marking important connections and parts
- Utilizing ESD techniques and keeping supply of essential spare parts
- limiting who has entry to console ports

Neither the console nor any console port should be left open, and administrative interfaces should be closed before departing. The primary protection for electronics should not be a locked room. No room is completely safe, and even if someone manages to enter a room that is, there is nothing keeping them from connecting to the console of a switch or a router.

4.5 Packet sniffer attack mitigation

The tools which can be used to prevent packet sniffer attacks are as follows:

Authentication: The usage of identity verification should have been the first available mitigation strategy for protection against packet sniffers. Multifactor authentication is a method of user authentication that is difficult to defeat. Strong authentication is clearly demonstrated by One Time Passwords (OTPs). When an application requires a password, just one password is a security measure that generates a new password using a mobile device [13].

Switched infrastructure: In a network context, this method thwarts use of packet sniffers. Intruders can only access the traffic flow of the linked port, for example, if an organization adopts a layer-2 switched Ethernet. Although packet sniffers still pose a

threat, a switched infrastructure significantly reduces their effectiveness.

Anti-sniffer tools: There is always a defense against a threat. An anti-sniffer tool is a piece of hardware or software that can be used to identify the use of sniffers on a network

When a packet sniffer only finds cipher text—a random string of bits—and not the original message, an information transfer is cryptographically secure, according to cryptography. Network-level cryptography is used by Cisco and is based on IP Security (Internet protocol security), a widely used security protocol for networking devices when interacting privately over the Internet Protocol (IP). (CANS 2011) Other cryptographic methods for managing networks include Secure Socket Layer 1 (SSL) and Transport Layer security (tls Protocol (SSH).

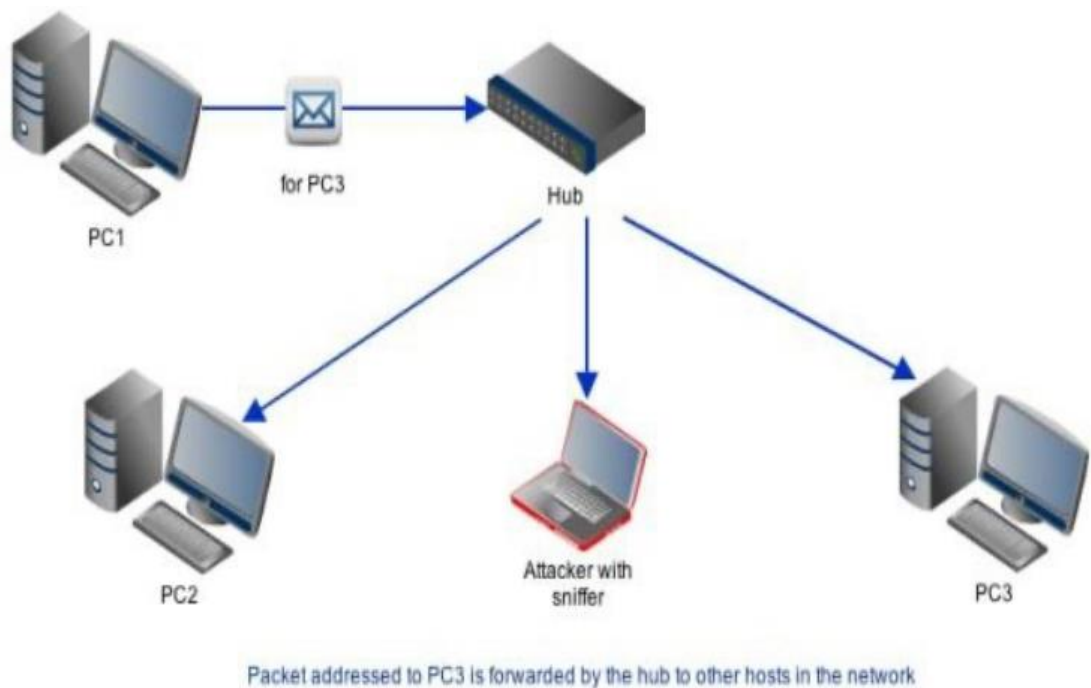


Figure 4.1: packet addressed diagram 16

4.6 Port scan and ping sweep attack mitigation

It appears to be challenging to stop port searches and ping sweeps without sacrificing network performance. However, it is advised to deploy intrusion prevention solutions at the host and network levels to minimize any harm. If ICMP (International command message protocol) echo and echo-reply are disabled on edge routers, ping sweeps can be prevented. An administrator is typically alerted when a reconnaissance assault is underway by network-based intrusion prevention (IPSs), which match traffic coming to signatures in their database, and host-based intrusion detection and prevention systems (HIPS). Working at the kernel level is essential to obtain stealth scans [14].

4.7 Access attacks mitigation

The following are password attack mitigation strategies:

- 4.7.1 The same passwords should not be used by users on different computers.
- 4.7.2 After detecting a particular number of unsuccessful login attempts, accounts should be disabled.
- 4.7.3 Ordinary text passwords shouldn't be used, ever.
- 4.7.4 Use secure passwords, such as "mY8! Rthd8y@," rather than your or my birthday.

4.8 Trust exploitation attack mitigation

Tight restrictions on the amount of trust within networks can be used to minimize trust exploitation-based attacks. When feasible, trust should be restricted to specific protocols, and it should also be confirmed by other criteria other than an IP address, so that the inner systems of a firewall do not entirely trust the outside systems.

4.9 Man-in-the-middle attack mitigation

The only effective defense against Man-in-the-Middle attacks is cryptography (encryption). The encrypting of information in a Standard Ip tunnel can prevent man-in-the-middle attacks. Hackers or intruders can only see cipher text while using this encryption method.

4.10 Denial of service attacks and mitigation

1. Attack mitigation by Ip spoofing although Ip spoofing remains a problem, it can be lessened by taking the following steps:

- 4.10.1 Configuring access control is necessary to prevent any traffic from the external network with a source Ip address that belongs on the corporate network in order to lessen the impact of session hijacking.
- 4.10.2 Encryption: By encryption all network communication to protect the source and destination sites from becoming hacked, encryption is another potential method for preventing Spoofing.
- 4.10.3 Additional authentication: The adoption of additional authentication techniques makes IP spoofing attacks ineffective. The ideal method for additional authentication is cryptographic authentication.

2. Attack mitigation for dos (denial of service) the following methods can help lessen the threat of dos (denial of service) attacks:

Anti-spoof features: The likelihood of a DoS attack can be decreased by properly configuring anti-spoof characteristics on routers and firewalls. Filtering up to an RFC 2827 level is part of this configuration.

Hackers won't launch an attack since they won't be able to hide their identities.

Anti-DoS features: Anti-DoS (denial of service) measures enabled on routers and firewalls reduce an attack's efficacy. Limiting the number of Tcp that a system can have open at once is a common component of anti-DoS measures.

Restriction the amount of traffic: Some ISPs offer traffic rate limiting.

Filtering limits the amount of unwanted traffic that can pass through different network sections at a given speed.

4.11 Mitigating worm attacks

To lessen worm attacks, do the following actions:

- Inoculation is a technique for repairing all systems and may also involve scanning for weak points.
- Find every contaminated computer inside a network and placing it in quarantine. Any infected device needs to be disconnected from the network, blocked, or eliminated.

4.12 Application layer attack mitigation

The following are some changes that could be made to lower risks:

- Reading network and operating system log files, or having log analysis software analyze them.
- Joining mailing groups that announce security holes.
- Maintaining the most recent fixes for the windows os and apps.
- Scanning known attacks with IDS/IPS, watching and logging attempts, and occasionally stopping attacks

4.13 Securing remote access

Utilizing line passwords, a local security database, or distant security server databases, Cisco networking devices enable Authentication Authorization and Accounting (AAA) access control. Using the username xyz and the strong password command, the local security database is set up on the router for a collection of network users. Providing AAA services for several network devices and a sizable number of network users, a remote security database is a separate server that runs an AAA security protocol. AAA is used by users and router administrators who want to dial in or use the Internet to access the corporate LAN [15].

CHAPTER FIVE

RISK ASSESSMENT AND MANAGEMENT

5.0 Introduction

Network security threat assessments are designed to understand, manage, control, and mitigate cyber threats across your organization. Underwriting is nothing new, and whether you like it or not, if you focus on the certainty of the facts, you are in the business of controlling threats. Risk assessment and management is critical to the success of any business. However, many institutions no longer accept it all the time.

Important precautions ending in a disaster. Good management of hazards can prevent mistakes, leading to a safer painting environment, happier employees, and increased productivity.

You can make your business successful by following a few basic steps.

Objective The purpose of the opportunity assessment process is to assess hazards and incorporate management actions as needed to eliminate or scale the opportunity.

By doing so, you have created a safer and healthier workplace. The motivation for writing technical statements and chance checks in the long run is that you develop suitability and protection management for your work, properly reduce and manage risks, and protect your personnel and those who may be exposed. Is to do. The

Journal of the American Society of Safety Engineers explains the difference between random evaluation and random control as follows: Random control is a period that describes an organization-wide effort to mitigate workplace injuries, while random assessment is a specific problem, the process of assessment. Please.

Research has consistently found that connecting is easier and faster [16].

5.1 Seeking Out Problems Before They Happen

The motivation behind danger evaluation is to search for issues before they happen. This evades wounds and crises. Or possibly it assists with coordinating more in case of a crisis. This requires exchanging organization aptitude and cautiousness. By focusing on the

Ability questions, you can work on the general wellness and satisfaction of the for-benefit organization.

Exceptional to your organization every exchanging organization might have its own concerns. For instance, the danger to the retail business can be very not the same as the dangers that an assembling association might confront.

Drug organizations will confront remarkable perils more than financial foundations. Enormous organizations with numerous dress-ups may likewise find it supportive to isolate expertise issues in every division.

There are some significant gamble classes to recollect when you know precisely exact thing your business is [17].

5.2 Basic Risks:

Cybersecurity risk is the probability of exposure or loss resulting from a cyber-attack or data breach on your organization. A superior, seriously enveloping definition is the expected misfortune or damage connected with specialized framework, utilization of innovation or notoriety of an association.

Associations are turning out to be more defenseless against digital dangers because of the rising dependence on PCs, organizations, programs, virtual entertainment and information around the world. Information breaks, a typical digital assault, have gigantic negative business influence and frequently emerge from deficiently safeguarded information.

Worldwide availability and expanding utilization of cloud administrations with unfortunate default security boundaries implies the gamble of digital assaults from outside your association is expanding. What could generally be tended to by IT risk the board and access control currently should be supplemented by modern digital protection experts, programming and network safety risk the executives.

5.3 Levels of Impact:

Less impact: If a mess occurs, it has little impact on the for-profit company and can be easily fixed.

Moderate Impact: Anger is very important. However, it does affect your organization.

High Impact: This is a serious problem that disrupts your business. Determining the magnitude of the impact determines the first problem to be addressed. 37 External Events No matter how organized you are, problems are always easy to predict. This is mainly for external events. You have a greater influence on internal events, but external events are more unpredictable. When it comes to external events, you need to be prepared for all sorts of problems.

These opportunities are basically all work that is not internal.

5.4 Everyone`s Responsibility

Overseeing risks in all actuality does now never again forestall with the control group. Everybody is chargeable for the security of the endeavor climate. Staff should completely comprehend the dangers and execution issues confronting the association. Everybody can encounter a protected and simple to-utilize painting climate by taking care of related issues before every one beginning. Kindly see the report! At the point when everybody and everybody is liable for risk the board, all representatives really must comprehend how to record expertise issues. The machine ought to be found near you with the goal that you can undoubtedly report the issue. Likewise, everybody has to know how the machine functions.

Representatives ought to be effectively urged to record risks and expertise issues. Try not to be confounded about this assumption. Make a noticeable update on the risk release board that staff ought to know about alongside work environment crisis data. Make noticeable updates by posting a rundown of perils that staff ought to know about, alongside work environment crisis records.

Employees are the target of cybercriminals looking for an easy way to break into a company. Effective and practical accountability requires human-centric attack protection tools. Skilled employees reduce the chances of a successful attack [18].

To build a resilient human firewall, we need to change our mindset. This change in thinking is based on good security education, tools, and countermeasures that enable employees and other non-employees to identify and address other scams such as phishing and Business Email Compromise (BEC). Creates a built cyber security culture.

5.5 Risk Management Techniques

When the risks are evaluated, they should be controlled cautiously. There are principal danger control procedures, and your business endeavor probably utilizes every one of them. The control technique which you use will go predictable with those verity the risk and the advanced solidness of the association.

You will select among bringing down the peril, moving the danger, taking off the risk, and tolerating the danger while sorting out which technique to utilize.

5.5.1 Reduce the Risk

Risk markdown is a to be expected spot approach used in business. It is fundamental while there no chance of discarding the danger comprising of in the use of machines. At the point when you decrease the danger, you confine the seriousness of the danger and the likelihood of the danger happening. While sorting out an approach to wonderful reduce the danger, it far crucial for set up which approach of rebate can be the most extreme powerful. For instance, one danger rebate approach may likewise reduce the danger of misfortune more

noteworthy than others, but it can also be more noteworthy profoundly valued to carry out [19].

5.5.2 Risk avoidance

Risk evasion Risk aversion is the act of eliminating the weak part of the framework or even the actual framework,

Since certain dangers may possibly get back to OK levels on the off chance that the movement is ended Risks to data frameworks exist from many referred to and obscure danger sources and subsequently endeavoring to keep away from it turns out to be essentially unthinkable. It is incredibly hard for an association to keep away from dangers to its delicate data while as yet giving admittance to approved clients, applications and frameworks. This present circumstance applies to optional schools where risk evasion might be troublesome because of the way that various clients access the school network for various reasons. Thusly, the administration ought to investigate other gamble treatment systems.

5.5 Identify Vulnerabilities

Every agency has threats and vulnerabilities. The dangers diagnosed with inside the hazard evaluation will facilitate the identity of threats. The threats to the corporation which could have an effect on the operations of the agency turn out to be vulnerabilities.

Weaknesses are limit crises. The technique for sorting out weaknesses calls for list dangers and contemplating how your basic strategies are in danger of those dangers.

Investigate Information once you got gathered records and analyzed weaknesses, you could look at records to choose your needs. The initial step to perusing records is approving it. You can approve the realities you gathered through doing eye to eye interviews with the individuals who outfitted the records.

5.6 Gather Information

Conducting an enterprise effect evaluation calls for accumulating statistics. The statistics collected ought to be very precise approximately a designated important function. For example, the information for an income branch might attention at the promoting process, roles, responsibilities, etc.

The standard techniques for accumulating statistics are used with inside the enterprise effect evaluation:

- Reports
- Research
- Interviews
- Questionnaires

Conference calls

Interviews and questionnaires are the principle re assets of statistics due to the fact they offer you with the possibility to create questions precise to the subject you're researching. When growing Questions for interview sand questionnaires, you could need to seek advice from a professional with inside the important area. For example, you can seek advice from an IT professional to accumulate information approximately net security.

5.7 Implement Recommendations

Once the facts are analyzed, draft reports primarily based totally in your findings. These reports hold encompass their commendations. In order for his or her commendations to be implemented, you want to shop for in of superiors. Successful implementation calls for some fundamental steps:

- Identify the satisfactory venue for implementation.
- Review recommendations.
- Confirm dedication from participants.
Schedule the implementation process.
- After imposing the recommendations, you want to speak with every person concerned and assessment the outcomes as scheduled.

5.8 Disaster Recovery Plan

Every business enterprise desires a catastrophe restoration plan. The catastrophe restoration plan outlines the processes that want to be accompanied withinside the occasion of a catastrophe to shield it. By thinking about the outcomes of screw ups beforehand of time, the restoration plan will mitigate their effects. The catastrophe restoration plan is mounted for specific screw ups, along with herbal and artificial screw ups which includes excessive climate or era crashes.

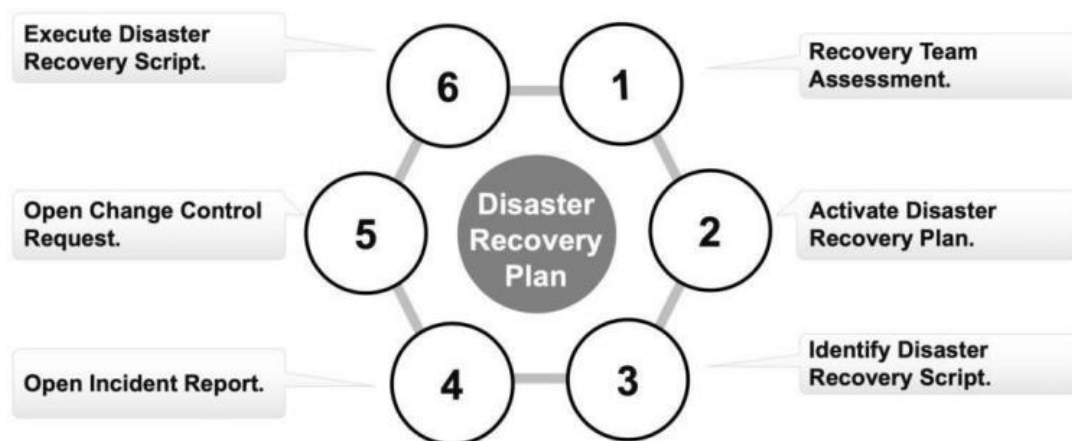


Figure 5.8: disaster recovery plan

5.9 Keep Documentation Simple and Clear

It is pivotal to document the fiasco rebuilding plan. While developing the record, keep up with the designing and phrasing basic. Make the message of the arrangement exceptionally clear.

There is a basic characterize that might be utilized to manual recording a calamity reclamation plan.

Data to record:

Objective

Suppositions

Standards to summon the arrangement

Jobs and obligations

Possibility methodology

Asset plan

Methodology for getting back to the first space

Methodology for data recuperation

5.10 Communication and Consult

Communication and Consultation Successful risk management requires communication with all stakeholders to improve risk understanding and management. Risk communication involves interactive dialogue between users and risk assessors and risk managers who actively inform other processes.

Information about the risks and controls identified through the risk assessment and analysis process is communicated using the appropriate copy of the risk assessment. These copies are available to administrators and all affected CIS users.

5.11 Monitor and Review

Effective risk management requires a reporting and review structure to effectively identify and assess risk and ensure that appropriate management and response are in place (Insurance and Risk Management Association, Risk). Management National Forum ALARM, and Risk Management Institute This Step ensures that your organization's risk management program is appropriate and that all input data, including probabilities and results, is up-to-date.

Monitoring and review are a risk management workflow. The importance of the monitoring and review process is that the organization's activities are properly managed, procedures are understood and adhered to. Monitoring and verification exercises are audited. Or it depends on the results of previous analysis and evaluation that contributed to this study.

5.12 Investigate anomalous activities

You most likely gather reams of log information from your web confronting servers: Unix syslog's, Windows occasion logs, firewall logs, IDS cautions, antivirus reports, dial-up access logs or any of various other different review trails. However, what might be said about your inside LAN.

Not at all like outer assailants, insiders by and large aren't cautious about covering their tracks. "Maybe the aggressor doesn't anticipate being gotten. For the most part, none of the insider assaults we have seen were challenging to research," said Peter Vestergaard, previous specialized chief at Danish security consultancy Protego. "The most concerning issue has been that organizations don't have adequate logging. In one case, basically nobody knew that signing on a no domain regulator server is crippled as a matter of course. Thusly, practically no log material was accessible [20].

Control Measure

Most groups have managed measures in area. Control measures are moves or sports which can be in area to restriction or save you dangers. There are six primary varieties of manage measures. The measures used depend upon the danger this is concerned and the way effortlessly than may be avoided. There is a primary hierarchy to manipulate measures, with the pinnacle measures being the maximum desirable.

Control Measure Hierarchy:

Eliminate: Remove the hazard.

Substitute: Trade for a lesser danger.

Isolate: Limit get right of entry to the danger.

Engineered controls: Designs to save you get right of entry to dangers and hazards.

Administrative controls: Safe paintings practices and procedures

Protective device: Personal shielding device is worn round hazards.

You`re Business Procedures.

Every commercial enterprise has one-of-a-kind wishes. The wishes of the commercial enterprise decide the way you broaden your commercial enterprise techniques and you manage measures.

Remember that each enterprise is precise and should broaden techniques independently; you cannot depend on not unusual place techniques and manage measures. You want to decide what's nice in your business enterprise.

Many commercial enterprise techniques are primarily based totally on unique manage measures. For example, analyzing gadget is a manage measure. The coverage and method for the inspection system will range in keeping with every business enterprise. A busier

business enterprise would require extra common an in-intensity inspections. Additionally, positive portions of gadget might also additionally require extra common inspections than others. The Adequate Control measures and strategies will want to alternate because the corporation does.

Measures which can be essential three hundred and sixty-five days won't be essential the next, or they not be ok to fill the company`s needs. Determining if the mounted manipulate measures and strategies are ok calls for common evaluation.

5.13 Summary of Risk Assessment

The hazard evaluation is critical to hazard control and plenty of different strategies. This calls for a know-how of hazard evaluation and hazard evaluation strategies. The capacity to use hazard evaluation strategies with inside the workplace will enhance protection for personnel and the employer.

5.14 Conclusion

It has gone through the steps of Network Security inventory creation, the threats of the hackers and their methods, and also Network Security fundamentals is to develop and implement security measures to prevent Network attacks, Network Security breaches are the result of secure information being released to a treacherous environment. It has explained many ways to help prevent identity theft. The objective of Network Security is to prevent or mitigate harm. The importance of this topic is to be wary of cybercrime. Even though not everyone is a victim of cybercrime, they are nevertheless vulnerable.

Computer-based crimes are diverse and do not always occur in front of a computer, but they are always committed by a computer. Hackers range in age from 12 to 67.

The hacker may be on the other side of the world from the victim and will not know that he was hacked. Computer crime is a 21st century problem. Thanks to advances in technology, criminals no longer have to rob banks or go out and commit crimes. They have everything they need on their knees.

Their weapons are no longer firearms instead, they employ mouse cursors and passwords to attack. In recent years, threat actors have become more numerous and destructive, and this trend is only expected to increase. Due to the necessity for businesses to acquire qualified personnel to counteract the danger, there are numerous chances for everyone.

Reference

- [1] M. Bishop, "Computer Security: Art and Science," 2003.
- [2] US Computer Emergency Readiness Team (US-CERT), "Security Tip (ST04-014) Avoiding Social Engineering and Phishing Attacks," Department of Homeland Security, 2014. [Online]. Available: <http://www.us-cert.gov/ncas/tips/ST04-014>. [Accessed 16 February 2014].
- [3] G. Dieter, W. and S. John, "Computer security 2ed," 1999.
- [4] Symantec Corporation, "Security Response Publications: Internet Security Threat Report 2013 Vol.18 (2012 Trends, Volume 18, Published April 2013)," Symantec Corporation, April 2013.
- [5] P. Hyman, "Cybercrime: It's Serious, But Exactly How Serious?" COMMUNICATIONS OF THE ACM, vol. 56, no. 3, pp. 18-20, 2013.
- [6] Anti-Phishing Working Group, Inc. (APWG), "Resources: APWG Phishing Attack Trends Reports," Anti-Phishing Working Group, Inc. (APWG), 20 February 2014.
- [7] <https://economictimes.indiatimes.com/definition/emotional-intelligences>
- [8] Multiple authors, Handbook of wireless local area networks, 2005, Book
- [9] Thuraisingham, Bhavani M, Database and applications security: integrating information security and data management, 2005, Book.
- [10] Brumley, Billy, A3/A8 & COMP 128, Helsinki University of Technology, 2004, PDF.
- [11] Rao, K. Ramamohan (Kamisetty Ramamohan), Wireless multimedia communications, 2009, Book] RichardThaler.
- [12] Frankel, Eydt, Owens and Scarfone, Establishing Wireless Robust Security Networks:

- [13] A Guide to IEEE 802.11i, National institute of standards and technology, 2007, PDF [41Network Security Products and Services. (2016). Itgovernance.co.uk. Retrieved 25 November 2016, from <http://www.itgovernance.co.uk/cyber-security-solutions>.
- [14] Cyber Security Products and Services. (2016). Itgovernance.co.uk. Retrieved 25 November 2016, from <http://www.itgovernance.co.uk/cyber-security-solutions.aspx>.
- [15] EBSCO, (2016). Ebscovideos.ebscohost.com. Retrieved 26 November 2016, From <http://ebscovideos.ebscohost.com/v/103100997/fbi-chieftalks-terrorism-and-cyber-crime.html>
- [16] Adeyinka, O., "Internet Attack Methods and Internet Security Technology, " Modeling &Simulation, 2008.
- [17] Al Salqan, Y.Y., " Future trends in Internet security and Distributed Computing Systems, 1997., Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends of, vol., no., pp.216 217, 29 31 Oct 1997Address "IPv6: the next internet protocol," April2005, www.usenix.com/publications/login/200504/pdfs/andress0504.pdf.Bidou, R. 2000. Denial of service attacks. Retrieved: May 10 2012. Available at: <http://www.docstoc.com/docs/85149779/Denial-of-ServiceAttacks> Cisco Security. 2005.
- [18] Retrieved: May 5 2012. Available at: <http://www.orbit-computersolutions.com/Threats-to-Physical> and Network Infrastructure Paul, A. May 13 2003. Implementing secure access to Cisco devices using TACACS+ and SSH.

[19] Q. Jeremy, "Security in the system," AusMobile, 2004.

[20] Wikipedia, "Cyber-security Regulation," Wikipedia, 7 November 2013. [Online]. Available: <http://en.wikipedia.org/wiki/Cyber-securityjregulation>. [Accessed 20 March 2014].

final_thesis_book_abdifatah.pdf

ORIGINALITY REPORT

22%

SIMILARITY INDEX

18%

INTERNET SOURCES

0%

PUBLICATIONS

17%

STUDENT PAPERS

PRIMARY SOURCES

1

publications.theseus.fi

Internet Source

5%

2

dspace.daffodilvarsity.edu.bd:8080

Internet Source

2%

3

Submitted to Daffodil International University

Student Paper

1%

4

Submitted to Kampala International University

Student Paper

1%

5

no1homeworkhelp.com

Internet Source

1%

6

Submitted to Fresno Pacific University

Student Paper

1%

7

uir.unisa.ac.za

Internet Source

1%

8

Submitted to University of Bedfordshire

Student Paper

1%

9

Submitted to St. Patrick's College

Student Paper

1%

| | | |
|----|--|------|
| 10 | Submitted to Study Group Australia Student Paper | 1 % |
| 11 | Submitted to Southampton Solent University Student Paper | 1 % |
| 12 | ios.ipmanager.ir Internet Source | 1 % |
| 13 | www.iiste.org Internet Source | 1 % |
| 14 | etd.uum.edu.my Internet Source | 1 % |
| 15 | Submitted to Harrisburg University of Science and Technology Student Paper | 1 % |
| 16 | Submitted to Taylor's Education Group Student Paper | <1 % |
| 17 | Submitted to Harare Institute of Technology Student Paper | <1 % |
| 18 | www.worldconferences.org Internet Source | <1 % |
| 19 | www.brighthub.com Internet Source | <1 % |
| 20 | www.coursehero.com Internet Source | <1 % |
| 21 | Submitted to Fiji National University Student Paper | |

| | | |
|----|--|------|
| | | <1 % |
| 22 | Submitted to American Public University System Student Paper | <1 % |
| 23 | Submitted to ebsu Student Paper | <1 % |
| 24 | Submitted to Southern Cross University Student Paper | <1 % |
| 25 | Www.Upguard.Com Internet Source | <1 % |
| 26 | dspace.unza.zm Internet Source | <1 % |
| 27 | Submitted to University of Teesside Student Paper | <1 % |
| 28 | Submitted to Middlesex University Student Paper | <1 % |
| 29 | Submitted to University of Maryland, University College Student Paper | <1 % |
| 30 | Submitted to University of Lancaster Student Paper | <1 % |
| 31 | www.riverstreetconsultant.com Internet Source | <1 % |

32

digitalcommons.fiu.edu

Internet Source

<1 %

33

Submitted to Institute of Graduate Studies,

UiTM

Student Paper

<1 %

Exclude quotes On

Exclude matches < 10 words

Exclude bibliography On