**Text

Description automatically generated with medium confidence**

# ROLE OF IDS AND IPS IN CYBERSECURITY

**FINAL PROJECT REPORT**

# UNIVERSITY OFHERTFORDSHIRE

School of Physics,EngineeringandComputerScience

SIDDHARTHAN GOWTHAMAN:19058239

23 September2022

**Course**: MSc Project: M.Sc. Cyber Security

7COM1039-0509-2021: Final Project Report

**Student Name**: Siddharthan Gowthaman

**Student Number**: 19058239

**Supervised by**: Shahrzad Shapoori

# Declaration

This report is submitted in partial fulfillment of requirement for the award of Master of Science in Cyber Security

It is my own work except where indicated in the report.

In my MSc project, I did not employ any human subjects.

I hereby give permission for the report to be posted on university website as long as the source is acknowledged**.**

Siddharthan Gowthaman

19058239

**ROLE OF IDS AND IPS IN CYBERSECURITY**

**Executive summary**

***In the chapter Introduction,*** several kinds of description of tools and techniques have been analyzed properly with the help of technical solution methods and its structures. Apart from that, the designing of the process of IPS and IDS under the cybersecurity have been defined to provide a vast idea of the project and the way it have been initiated for the compilation.

***In the chapter Methodology*,** the ideas of the applied research methods, design, and approaches have been provided. The first section has briefly explained the choice of the method in the most attractive way. Ten the justification of the chosen one has been discussed. The data collection and analysis of them have been done in a specific chapter. The ethical issues and the commercial risk have been illustrated in the research paper along with the ideas of the data validation of the collected data.

***The Quality and Results chapter*** highlights the results that have been collected from the experiments that have been done regarding the requirements. The practicality of the work along with the interpretation of the results has been added to this section. This section also shows the appropriate tools and techniques that can be used to fulfill the objectives of the project.

***In the evaluation and conclusion chapter,*** the discussion is based on the functions of intrusion detection system and intrusion prevention system and how that helps to detect all unethical activates.

Table of Contents

[Chapter 1: Specification of the project 7](#_Toc114831870)

[1.1 Abstract 7](#_Toc114831871)

[1.2 Introduction 7](#_Toc114831872)

[1.3 Specification of the project 7](#_Toc114831873)

[1.4 Aim and objectives 9](#_Toc114831874)

[1.5 Research Question 10](#_Toc114831875)

[1.6 Research Rationale 10](#_Toc114831876)

[1.7 Current issues 10](#_Toc114831877)

[1.8 Feasibility 11](#_Toc114831878)

[1.9 Summary 11](#_Toc114831879)

[Chapter 2: Research 12](#_Toc114831880)

[2.1 Quality of Background research 12](#_Toc114831881)

[2.2 Use of Literature 12](#_Toc114831882)

[2.2.1 Role of cyber security in Information Technology Education 13](#_Toc114831883)

[2.2.2 Diffrentiative factors between IDS and IPS 15](#_Toc114831884)

[2.2.3 Various technology management impacts on cyber security 17](#_Toc114831885)

[2.2.4 Work function of IDS and IPS 19](#_Toc114831886)

[2.5 Linkage to Aim 23](#_Toc114831887)

[2.6 Summary 23](#_Toc114831888)

[2.3 Critical Assessment 24](#_Toc114831889)

[2.4 Literature gap 25](#_Toc114831890)

[Chapter 3: Methodology 25](#_Toc114831891)

[3.1 Choice of methods 25](#_Toc114831892)

[3.2 Support and justification of choices 26](#_Toc114831893)

[3.3 Data Collection and Analysis 27](#_Toc114831894)

[3.4 Validation 27](#_Toc114831895)

[3.5 Ethical Issues 27](#_Toc114831896)

[3.6 Commercial risks and risk management 28](#_Toc114831897)

[3.7 Summary 28](#_Toc114831898)

[Chapter 4: Quality and Results 28](#_Toc114831899)

[4.1 Critical Analysis 28](#_Toc114831900)

[4.2 Evidence of practical work 29](#_Toc114831901)

[4.3 Awareness and solution to the technical challenges 36](#_Toc114831902)

[4.4 Novelty 36](#_Toc114831903)

[4.5 Interpretation of result 37](#_Toc114831904)

[4.6 Use of tools and techniques 37](#_Toc114831905)

[4.7 Appropriate tools for analysis 39](#_Toc114831906)

[4.8 Linkage to objectives and literature 39](#_Toc114831907)

[4.9 Summary 39](#_Toc114831908)

[Chapter 5: Evaluation and Conclusion 39](#_Toc114831909)

[5.1 Critical evaluation 40](#_Toc114831910)

[5.2 Summary of the achievement 41](#_Toc114831911)

[5.3 Reflection 41](#_Toc114831912)

[5.4 Research recommendation 42](#_Toc114831913)

[5.5 Achievements of the objectives 43](#_Toc114831914)

[5.6 Future work 43](#_Toc114831915)

[References 45](#_Toc114831916)

**List of figures**

[Figure 1.3.1: Stack workflow 8](#_Toc114831917)

[Figure 2.2.1.1: Roles of cyber security 14](#_Toc114831918)

[Figure 2.2.2.1: Role of IDS and IPS in network security 16](#_Toc114831919)

[Figure 2.2.3.1: Advantages of cyber security 18](#_Toc114831920)

[Figure 2.2.4.1: Architecture of IDS and IPS 20](#_Toc114831921)

[Figure 3.2.1: Applied Research Methodology of Cyber Security 26](#_Toc114831922)

[Figure 4.2.1: Console 29](#_Toc114831923)

[Figure 4.2.2: Core commands 30](#_Toc114831924)

[Figure 4.2.3: Module commands and job commands 31](#_Toc114831925)

[Figure 4.2.4: Matching modules 32](#_Toc114831926)

[Figure 4.2.5: Developer commands and credential backend commands 32](#_Toc114831927)

[Figure 4.2.6: List of options 33](#_Toc114831928)

[Figure 4.2.7: RHOST and RPOST 33](#_Toc114831929)

[Figure 4.2.8: Configuration 34](#_Toc114831930)

[Figure 4.2.9: Password 35](#_Toc114831931)

[Figure 4.2.10: Command for shadow 35](#_Toc114831932)

[Figure 4.5.1: Banner 37](#_Toc114831933)

**List of tables**

[Table 2.2.1.1: Impactful approaches of Cyber security 15](#_Toc114831934)

[Table 2.2.3.1: Different types of the importance of cyber security 19](#_Toc114831935)

[Table 3.1: Research Requirement for Methodology 26](#_Toc114831936)

[Table 4.6.1: Different tools and techniques 38](#_Toc114831937)

# Chapter 1: Specification of the project

## 1.1 Abstract

This research focuses on the specification of the IDS and IPS in the process of cyber security. The research has developed some of the important topics that have been implemented with several essential structures along with specified tables and figures that implement several essential images that have signified the role of both IPS and IDS that can affect the role of cyber security. The other part of the study focuses on the literature review that focuses very deeply on the several kinds of specifications of cyber security and the administrator violation of the system. The specified version of the system engineering has been attached to the research methods and the conclusion has been focused on the main role of the IDS and IPS in the role of cyber security.

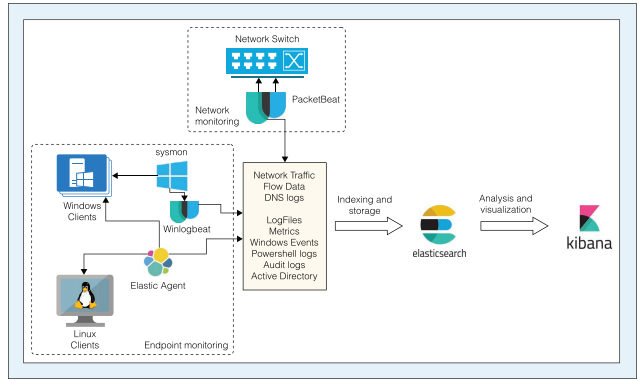
## 1.2 Introduction

Cyber security is one of the essential parts of the technology in the world that has to defend any kind of anonymous activities that contain cyberbullying or any kind of illegal activities on the internet on several systems that concludes of computers, mobile devices, different kinds of softwares, network along with several kinds of servers. Other than that, the effects of network technology and the specified version of the security that has an independent extra layer are also known as cyber security. There are several kinds of work that can be done with the help of cyber security such as any type of mobile computing in a business organization that can be predicted and resolved by cyber security. Different kinds of security have been provided in cyber security and the specification of the computer networks has been allowed.

Network security provides the rehearsal of providing security to the networks of the computer networks that allows the structures of defending malware version. Other than that, application security has been managing to develop the software with the device allocation along with resolving security threats. Apart from that, information security along with operational security has been one of the essential products of cyber security. For network traffic, the activities of IDS, and preventive intrusion the specification of IPS has been defined to perform the value of exploitation under cyber security.

## 1.3 Specification of the project

In this part of the project, the theory of the topic has been defined enough to provide the perspective of cyber security along with the required knowledge that needs to be essential for the study. Several kinds of miscellaneous activities have been provided in the cybersecurity under the cyber-attacks have been enormously enhanced due to the misconduct of the cyber security in the network activity of the system. Therefore, knowledge of cyber security is highly required to give the perspective of the computer networks along with the security regarding the application of the computer Other than that, the projected report has defined the role of IPS and IDS in the specification of cyber security. Some of the cyber-attacks contain different kinds of information removed from the internet, providing false information along with the network's activity and stealing several kinds of essential information from the users is one of the major dangerous activities that has been stated under the cyberbullying activities. The project focuses on the ***denial of service*** that has been enhanced due to the attacks and casting of the conducted networks that have been provided the cyber security of the technology (Mahboub*et al.* 2021).



#### Figure 1.3.1: Stack workflow

(Source: Mahmoud *et al.* 2022)

Apart from that, the project mainly focuses on the detection of IDS and IPS of the security activity of the cyber activity. The scrutinization of tube traffic of the network that has been mainly reviewed to resolve the challenging factors of several kinds of suspicious activities that have been created in the servers of the web is helped with the help IDS and also known as ***Intrusion Detection System***. The malicious system of the administrator of the configuration of the cyber security has been initiated during the compilation of the project. Other than that, there are various kinds of classification that have been projected in the role of the ***Intrusion Detection System***. Apart from that, the requirements of tools and techniques that have been implemented to gather the information of software required with a Kali Linux operating system.

Other than that, the specification of IPS also known as ***Intrusion Prevention System*** is a verified detection system that keeps the managing technology of the exploitation of the network preventive measurement. Therefore, the preventive measures of the detecting security of the network that has been attacked by the technologies of the ***Intrusion Prevention System*** (Sadique*et al.* 2019). On the other hand, the vulnerability of the control of the gain has been measured by the system administrator of cyber security of the function performance. The work allocation of the deployed version of the detection system that has been viewed in this project provides an outline of the network system. The detection of the method that has been structured for the several kinds of network attacks that have been initiated is the structure of the pattern.

## 1.4 Aim and objectives

**Aim**

The main aim of the project is to create a specific design for the defense system regarding the system of IDS and IPS that resolves the issue of any kinds of attacks that have been created in cyber security.

**Objectives**

* To analyze the process of determining the defense system of IDS and IPS in cyber security.
* To scrutinize the work structure of IDS and IPS and the requirement of methods for cyber activities.
* To know all the essential information about cyber security and denial and service attacks under the network traffic.
* To process the collection of all kinds of tools and techniques that have been required to perform the hacking of websites with the help of IDS and IPS in the Kali Linux operating system.

## 1.5 Research Question

1. What is the process of determining the defense system regarding IDS and IPS under cyber security?
2. What are the work structures of IDS and IPS and the requirements of specific methods applicable for cyber security?
3. What is the essential information required for cyber security and DoS attacks under the traffic of networks?
4. What are the specifications of the Kali Linux operating system and the specific tools and techniques required to initiate the project?

## 1.6 Research Rationale

The essentiality of cyber security is enormously effective to perform the best defensive system among every server that has been created on the internet. Other than that, the requirements of several types of applications that have been initiated in the security structures that affect the accession of the several TCP ports and the performance of the distinguishing can be initiated. The main reason for the project is to develop the creation of a database that can be notified with the help of several web servers that has been developed to initiate the detecting connection of security. Other than that, the initiation of IDS and IPS can be a specific defensive structure to prevent any kind of attacks regarding cyber security and web server attacks.

## 1.7 Current issues

The definition of cyber security is enormously big to create the structure of the network detection system. Therefore, during the initiation of the project, there are several issues have been initiated to identify the networks of the subnet, and the collection of data immensely created pressure during the full compilation of the project. Other than that, the administrator of the installation process regarding cyber security has initiated some of the big challenging factors regarding the IDS and IPS (Salloum*et al.* 2020). The approaches regarding the issues of designing the cyber security visualization have been created.

## 1.8 Feasibility

The project focuses on the feasibility part that can be projected by designing a way of helping to evaluate the possible outcome by eliminating several issues regarding the compilation and selecting the process of functionality with some creative practical methods. On simpler note feasibility refers to the selection of a particular part that provides accession to selecting several kinds of key factors that have been analyzed properly along with evaluating the procedures to clear the initiation of the method that has been signifying as an easy strategy to compile the research. The mode of operation has been proceeding throughout the whole project. Apart from that, the definition of the requirements of several kinds of tools and techniques has been analyzed with specific necessities. The evaluation of the procedure form of application has been initiated throughout the feasibility of the project. Lastly, the action of the process has been discussed through specific cybersecurity options. The evaluation process helps to resolve the issues of selecting several steps that have been determined by various techniques of the research paper. All kinds of technical, operations along with economic strategies have been provided in this project to investigate the whole procedures of the research paper.

## 1.9 Summary

In this research, the introductory part has been focusing on the current topic that stated the role of ***Intrusion Detection Systems*** and ***Intrusion Prevention systems*** in the specification of cybersecurity. Other than that, to summarize the introduction several kinds of definitions of IDS and IPS have been described properly. Apart from that, the aims and objectives have been described properly to provide a complete idea of the subject that has been discussed in the research. Other than that, the compilation of the current issues has been described during the creation of the project.

# Chapter 2: Research

## 2.1 Quality of Background research

The main following agendas are getting assessed with various terms and conditions in the system decorum. Maintaining the execution process with great accurate values in hand is generally the primary objective in this detailed project (Ben Fredj*et al.* 2020). As per the objectives of the project all the attributes are taking affirmative approaches in different circumstances. Therefore, gaining all the considering elements in order to mitigate the overall risk factors are generally taking individual types of considerations in the following segment of this chapter. Mentioning all the roles of IDS is mainly taking various approaches to provide an alerting feature about the potential incident. Taking all attributes as mentioned in the previous segments security functions are generally taking various approaches in order to mitigate the risk factors. Assessing the quality of the background research allows the chapter to be more precise with the workflow as per the project requirements with fulfilling all objectives. The background of the overall research functions is generally a relation between some following agendas to take entire charge to maintain follow-ups to construct the appropriate context to minimize the problems in relation to research theory.

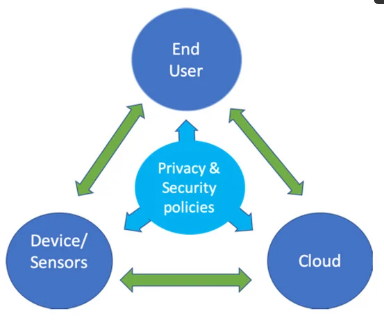
Taking all the scoping mechanisms into the system decorum is generating some valid and detailed allocations to fill all the gaps in research-taking approaches (Dwyer *et al.* 2022). Understanding the overall approach to enduring the project values is mentioned in this chapter with several segmented details. This segment mainly obtained some values to maximize the overall agendas of the entire project with affirmative approaches in hand. After assessing the overall approaches all circumstances are getting maintained with deep-level consecrating approaches. With the help of some authentication elements in several case scenarios, the project is finally getting possible valid outcomes. Lending many helping hands for the system decorum overall process is maintaining some accurate terms in formidable conditions (Davies *et al.* 2022). Maintaining all the agendas in order to maximize the values of the project are mentioned in this detailed chapter with great values in hand.

## 2.2 Use of Literature

This segment of this detailed chapter focused on providing different types of valid aspects within some chunk pieces of knowledge to get more precise in the workflow (Elsayess, 2020). To maintain the overall system criteria as mentioned in the previous terms with a detailed approach are mitigated in this segment with the help of various research papers to develop some awareness and maintain all the cultural aspects in order to deal with the outside world. This segment uses some journals and research papers to ensure the topic's values and also takes the overall charge to develop some understanding between the project and taken values. All the values are maintained with respect to cyber security agendas, the roles are generally maintained in IDS as well. The roles of IDS and IPS are deeply getting assessed with valuables aspects in hand as well. Thematic analysis is getting allocated to endure the topics values in this project, all the themes are mentioned in the following.

### 2.2.1 Role of cyber security in Information Technology Education

In recent years cyber security has become a generous approach to maintain the overall aspects in order to generate aspects in protection. Having detailed agenda in the system decorum of the management system of education industries is managing various approaches to be more secure in the implementation process (Faquir *et al.* 2021). Maintaining all the processes mainly protects various categorical agendas to generate some shield-like structure to defend the overall aspects.



#### Figure 2.2.1.1: Roles of cyber security

Source: (mdpi.com)

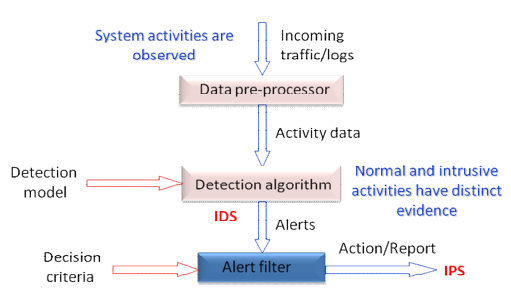
All these aspects are generally maintained with detailed affirmative approaches in the system decorum with generous values in hand. Data thefts are mitigated with great arbitrary values and confidential assessments in the system decorum. Taking all of these into the system can take the charge of overall protection in order to protect all sensitive information in the system decorum. Different types of impacting elements are listed down below for better grasping knowledgeable factors in for the system decorum.

| **Web systems** | Generally, web systems are in an external interface to get several engagements in management in order to take several values in the system decorum. These systems are taking various approaches to mitigate the overall risk factors in the system decorum for being more accurate in the workflow with great values in the program (Giannoutakis*et al.* 2020). A website is typically assessed publicly; different purposes are getting filled with values in cyberspace. Cyberspace is generally designed to be more defendable to prevent hackers in network systems. To get assisted with various aspects the particularly are maintained by XSS***.*** This is mainly a placement agenda to perform some course work during the work in progress (Kabanov and Madnick, 2021). Exploiting all malicious code controlled by an attacker is generally getting handy with overall system decorum. |
| --- | --- |
| **Human-Computer Interactions (HCI)** | These approaches to human-computer interactions are generally referred with several contexts with the help of cyber security (Khoulimi*et al.* 2022). This is a study that mainly takes some valuable approaches in the system to mitigate the overall risk factors with respect to interaction problem occurrence. Managing these terms can allow the system decorum to be more precise with the workflow and can the overall charge to deploy some inspection agendas to follow up. Maintaining the significance is generating some values to comprehend all the sections to build interactive elements in the system decorum. To get handier with the system these approaches are modified with dignifying elements in hand. |
| **Educational impacts** | Overall educational industries are generally taking several approaches to maintain the network functions of the students and staff as well. The cyber security agendas are keeping the system decorum to validate with valuable elements in hand as well. To get totally assessed with the system decorum anti-malware is installed using some encrypted allocations are taking various affirmative approaches in the system. The securable awareness is generally associated with defending elements to assess some course work. These functions are maintained by the system to prevent all cyber attacks in the educational industry. |

##### Table 2.2.1.1: Impactful approaches of Cyber security

### 2.2.2 Diffrentiative factors between IDS and IPS

This research paper mainly aims at the functions of providing some affirmative functions to detect the system configuration configurations. The differentiate element of the IDS and IPS is generally part of the system technologies. The detection methods are taking several conditions to deploy some course work in the system decorum to get more assessed in the implementation program. All the activities are taking various agendas to fulfill the detection methods in order to mitigate the feature of detection and prevention technologies as well (Kour*et al.* 2019). Mentioning these can ensure the data collection methods of the system as well. This paper takes various affirmative approaches to detect healthy connections to perform an accurate communication agenda with valid activities.



#### Figure 2.2.2.1: Role of IDS and IPS in network security

Source: (Ashoor, 2018)

The actual role of the IDS and IPS network security aspects are generally collected data and informative aspects. These aspects are generally generated to get more valuable data sources 9in order to alert the system from miscellaneous activities mentioned in the research papers with valid approaches in hand.

* In the primary segment of the detailed system decorum all the activities are mentioned with validating elements in the implementation program with detailed approaches as well. To generate some defendable approach the system needs to configure the system activities with observed elements as well (Larbaoui*et al.* 2021). The primary objectives are to assess the incoming traffic and logs to the system. Providing these terms in the system can mitigate the overall risk factors in the large data pre-processor section. Grasping various knowledgeable aspects of these agendas is getting noticed by the main system for assessing various project objectives. Taking these objectives as aspects the system allocates various active datasets in the decorum as shown in the above image.
* These active data sets are generally dispatched from the date pre-processor section. After dispatching the active data with valid informative details the system takes those data in detection algorithms to construct some detection model in the system decorum with dignifying elements as well (Panigrahi and Borah, 2018). Maintaining all the aspects of these behaviors can normally assess the intrusive active datasets and pieces of information by mentioning distinct shreds of evidence as well. With the help of the ***Intrusion Detection System,*** the monitoring process detects all suspicious activities in the system decorum.
* These approaches are maintained with valid detailed agendas in order to relocate the alerting elements in the system. To ensure the activities the alerting elements are processed into the alert filter to deploy some detection criteria. These detection criteria mainly allocate some activities in the process to assess the ***Intrusion Prevention System*** for maintaining all the affirmative approaches. The intrusion detection is mainly to assess the technological approaches in the system decorum with attempting activities (Larbaoui*et al.* 2021). All these approaches are taken as an aspect to assess all actions regarding alerting the miscellaneous activities in the system decorum. Taking an overall report to assess the overall agendas is maintained with various data and pieces of information.

### 2.2.3 Various technology management impacts on cyber security

In this research paper the main agendas are to assess the overall management aspect of various technologies. The impactful implementation approaches are generally taken to deploy the features in the system decorum with valuable aspects and valuable agendas in hand (Nygard *et al.* 2021). To get handier with the system criteria the allocation of recovery programs is mainly deployed in the system decorum. In the below section all the criteria are mentioned in detail to maintain all criteria to enhance the activities in cyber securable approaches.



#### Figure 2.2.3.1: Advantages of cyber security

Source: (semanticscholar.org, 2022)

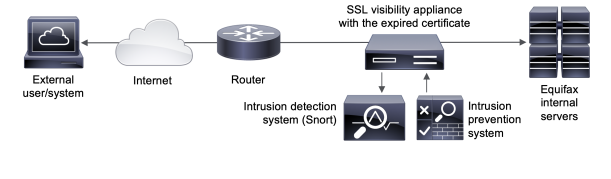
The technological aspects are mainly aligned in this segment with great accurate attributes in the system decorum. Taking all these terms in the section can take various affirmative approaches to healthcare management technological aspects (Larbaoui*et al.* 20021). To assess the overall agendas some elements are being added to the system to endure patient safety, medical technology, and financial stewardship. Also, the technological aspects can be aligned with some values to maintain various agendas to protect the overall system decorum of any industry. All these aspects are being assessed with various factors and functions that are taken place in the table below.

| **Protects system against viruses** | In the system all the disciplined agendas are aligned with formidable values in the segment to assess some course work. Taking all these aspects to engage the terms with mentioned considerations is getting various allocations to manage the evolving complexity. The viruses can destroy the overall data structure and crash the overall device. |
| --- | --- |
| **Protecting Information’s** | The system is an attribute that can endure all policies that can ensure the overall criteria with formidable values in the system decorum. To endure the assessments some criteria are mentioned in the system result from the management system. The antivirus aspects are getting noticed with formidable values in the system decorum with valuable aspects in the system decorum. |
| **Protect computers from being hacked** | Taking all the agendas as mentioned in the following various activities are getting allocated with formidable values in the system decorum with valuable aspects in hand. Allowing all the terms with conveying elements to protect the incoming threats. |
| **Minimizing computer freezing and crashes** | Maintaining the attributes in the system decorum in managing the overall safety measurements with no harm provisions (Lee and Kim, 2021). The computer threats are gradually managed and assessed by this approach with formidable values in hand. |
| **Privacy management for users** | The management allows all the terms and conditions with great accurate values in hand to get more precise with the project elements themselves. The privacy of a user is the most important agenda. All the management of this privacy is gradually done by the cyber securable approaches. |
| **Protection against the data from theft** | Data and information is collected by various methods and techniques in the system decorum. To deploy an approach that can endure data management with formidable values using cyber security is gaining various knowledgeable aspects during the course work (Durmus*et al.* 2019). Assessing these can get handy and several thefts are getting minimized with the help of this approach. |

##### Table 2.2.3.1: Different types of the importance of cyber security

### 2.2.4 Work function of IDS and IPS

Cybersecurity has enhanced the3 defensive system of the server system of the software allocation that has been provided in the security structure of the web application. Apart from that, the defensive systems of cybersecurity resolve several issues regarding the function of cyber-attacks along with the specification of the work process of the deep web and dark web (Walker and Benton, 2022). In this project, the specification of IDS and IPS has been critically analyzed for the process of resolving any technical issues related to cyberbullying on the internet. Therefore, the effective ways of investigating the action of requirement using potential techniques and methods to use the function of IDS and IPS (Moustakidis and Karlsson, 2020). The enhancement of the security operations has been determining the fact of the attention of the immediate structure that has been processed.



#### Figure 2.2.4.1: Architecture of IDS and IPS

(Kabanov and Madnick, 2021)

|  |  |  |
| --- | --- | --- |
| **Specific work functions** | **IPS** | **IDS** |
| * IPS refers to the ***Intrusion Prevention System*** that has been deployed to create the issues of the rolling network intrusion that can detect several kinds of miscellaneous activities that conclude various kinds of cyber activities regarding illegal specifications among the servers (Alhasani*et al.* 2022). Other than that, the activation of TAP along with the SPAN port has been organized to identify several kinds of attackers in the web technology. Apart from that, the intervention of the software is confirmed in several parts of the cyber security activities. * The detection strategies have been designed with the help of two kinds of techniques that have been considered as signature and anomaly-based systems (Jahwar*et al.* 2021). * Signature is known as one of the best methods of creating attacks that can be resolved by this system. Other than that, one of the most known codes for attacks from attackers has been diminished by the signature algorithm (Savin and Serban, 2019). The work function of the system is to analyze the attackers and removes the traffic creators that decrease the network speed in cyber security. * Anomalies create spots between the unusual traffic that has been initiated in the servers. Other than that, the creation of baseline triggers and the performance of responsiveness has been implemented through the cyber softwares (Rabelo*et al.* 2022). | * IDS signifies the ***Intrusion Detection System*** that initiates the designing process of the monitoring of the network traffic that has been created the resolution techniques of initiating suspicious activities throughout the whole project of cybersecurity-related port issues. * Like IPS, IDS detects the issues of any challenging factors regarding cybersecurity in the servers. Other than that in this scenario the two types of systems have been discussed like IPS. The two systems are signature and anomaly (Long *et al.* 2019). * IDS created in signature detect several kinds of malware and attacks of malware that have been initiated in the cyber system. Other than that, several kinds of malicious activities regarding unnecessary ads are detected by the signature-based system of IDS. * Anomaly detects the unnecessary and unidentified malware that has been compiled by the attackers that have been developed to create a rapid invention of viruses in the system (Bandyopadhyay *et al.* 2020). * Other than that, the observation of the network of t intrusion that has been provided in the security structure of the cyber activities contains several kinds of malware activities in the server web agave been completely implemented in the project. |

## 2.5 Linkage to Aim

The main aim of the project is completely described in this assessment. Apart from that, the specifications of all kinds of tools and techniques that have been performed to compile the project have been defined enough to create the project. Other than that, the research has been focusing on the operation of Kali Linux OS and the models that have been taken to perform the activities of cyber security with the help of IDS and IPS. The linkage between several aims has been completely discussed and the proper work structure has been initiated in the research to relocate the identifier that has been scrutinized in the facts of cyber security including IDS and IPS. Other than that, in the anomaly system, the work function machine learning system and the work function has been initiated to link the aim that can be signified by discussion g the proper identities of IDS and IPS at the same time the function of the defining model has been generalized properly in the research. The comparison between IDS and IPS defined the proper linkage between the actual aims of the project.

## 2.6 Summary

To summarize the literature review of the research it has been seen several topics have been discovered by creating several specifications of the cybersecurity facts that conclude the reality of IDS and IPS. The literature review of the research has been focused on several facts that conclude the difference between the IDS and IPS in terms of cybersecurity and along with several definitions of IPS and IDS. Other than that, several issues have been discussed along with the process of work function in the encryption data and the cracking attack of the password selection that concludes with the credentials information of the work structures. On the other hand, the research has signified several formulas of IPS and IDS that define the work structure of detecting several kinds of malware regarding the illegal activities in the cyber security servers. Other than that, the research summarizes the facts of the difference between detecting and preventing under the cyber security of scrutinizing various kinds of malware in the cyber application. The system software of the operating system has been described properly to identify the facts of system activation of the system that affects cyberbullying in the series of cybersecurity. These are several steps that have been taken to conclude the literature review of the research.

## 2.3 Critical Assessment

The evaluating elements in the system are getting allocated with the help of some formidable affirmative approaches in the sector to become precise with the workflow. After gaining several attributes in the thematic analysis the prospect objective is maintained with great value in the implementation program (Sun *et al.* 2020). To get handier with the project values the decorum had assessed with various statements in order to mitigate the overall risk factors in the system decorum. For maintaining the system all allocation is done with extra dignifying active approaches in the project to become more precious with the workflow itself, taking some research papers as an aspect to assess the formidable structure of the report is mainly taken various considering elements in various circumstances to deploy more alternatives in the system decorum to enhance the viewpoints. Getting allocated with these values can take various chances to assess the overall objectives of the project. In the primary terms of this segment, the taken research papers is obtaining some elements with various viewpoints of information technologies used in the education sectors (Stamatescu*et al.* 2020). Various roles of IDS and IPS are then afetr4e taken place in this meant to be more precise with the entire workflow. After grasping various knowledgeable factors in the system decorum mentioning these aspects is taking various factors in the system decorum. To ensure the agendas in order to mitigate the overall aspects are generally taking various approaches to the system decorum to get handier in the implementation program. Becoming more precise with these values can take some valuable charge to engage the entire cyber security approach by gaining several terms in this segment by taking all the informative factors with great aspects in the system. Regarding to all the attributes it can be taken in the overall project to take charge to follow up the entire working progress that is generally taking several considerations in the system decorum.

## 2.4 Literature gap

In this detailed chapter this segment is using some approaches to consider the overall terms with formidable values in order to mitigate various risk functions. This segment is allocating some focus points to assess some course work to get handy with the overall system decorum with management criteria as well. Taking the approaches in hand to get more precise with the workflow is mentioned in this segment with detailed aspects as well. As the segment is taking several charges to deploy an approach that can fill all the gaps in reach journals. Mentioning these terms in the system can take the overall charge to assess the monitoring process more accurately in the system. To get handier with formidable values are maintaining some detection systems that are generating valid reasons to take the cyber surety in the system to implement the overall intrusions.

# Chapter 3: Methodology

## 3.1 Choice of methods

The choice of the method has helped to get the ideas of the upcoming outcomes of the research work and for that, the choice of the methods has been considered as one of the most crucial parts of the entire research methodology. The use of the latest tools and technology has helped to apply the most suitable research method in the most effective way.

| **Research Design** | **Research Approach** | **Research Philosophy** | **Data Collection Method** |
| --- | --- | --- | --- |
| Qualitative | Inductive Research Approach | Positivism | Secondary Data Collection |

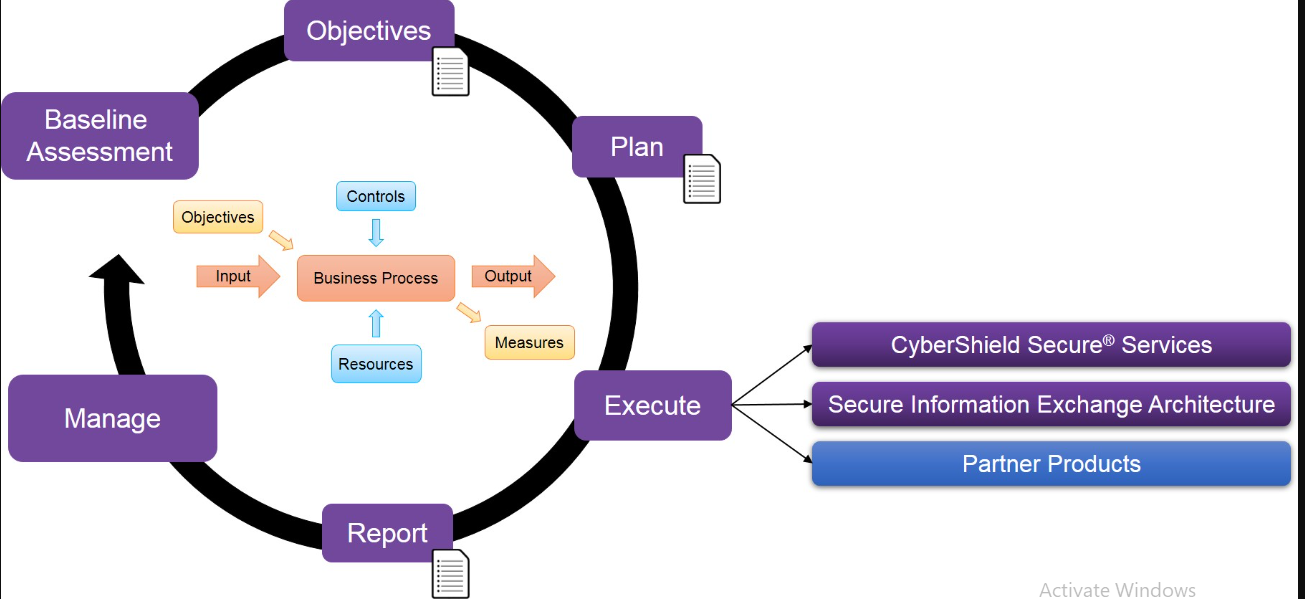
##### Table 3.1: Research Requirement for Methodology

(Source: Created by the Learner)

The choice of the research designs; approaches have been selected based on the requirements by focusing on getting maximum accuracy in the research work. The application of each of the tools has been done based on past research experiences related to the same research topic on the role of IDS and IPS in cybersecurity (Adawadkar and Kulkarni, 2022).

## 3.2 Support and justification of choices

The choice of the most suitable tools and technology for making the methodology of the entire research work has given the advantage to make it much more effective (Walker and Benton, 2022). The reasons behind choosing the most suitable research method and designs have been elaborated in this section so that the possibility of getting maximum accuracy in the specific research work can be possible at the maximum level.



#### Figure 3.2.1: Applied Research Methodology of Cyber Security

(Source: Iavich*et al*. 2022)

The qualitative research design has given the advantage to get all the qualitative data and information related to cyber security. This has helped to minimize the possibility of getting errors in the chosen data and information for the implementation of them in different phases of the research work.

## 3.3 Data Collection and Analysis

The data collection has given the advantage to make the application of the data much simpler in the entire research work. The presence of difficulties in the data collection method can be responsible for getting error full outcomes from the data analysis procedure. The collected data has been applied in kali Linux so that these data can be utilized to get the research outcomes within the minimum time. Secondary data research has given the advantage to make the utilization of the secondary data and information from past researchers related to the role of the IDS and IPS in cyber security (Deyannis *et al.* 2022). The secondary data and information has given the advantage to make the implementation of the collected data in the most specific range. The possibilities of elimination of the issues in cybersecurity have been increased to a peak level. The collected data has been applied in the input section of the applied tools and technology to get benefits of the time management. Time management has been possible as the implementation of the latest tools and technology for the collection of data has performed a huge role in this phase.

## 3.4 Validation

The collected data must be valid to get maximum accuracy in the implementation of the collected data in the research work. The application of the latest tools and technology along with the most suitable technical approaches has given benefits to the researchers to get the most accurate research outcomes within the minimum time. The application of the most suitable tools like different software or applications has helped to make the categorization of the collected data based on their requirements in the research work(Baci*et al.* 2022). The past experiences have given the researchers the opportunity to apply the collected data in the input section by eliminating unnecessary data from the collected data. The application of several data visualization software has given the benefits to visualize the data to make understanding the characteristics of the collected data the most effective way.

## 3.5 Ethical Issues

The most common issues have been categorized from all the identified issues with the help of the most suitable technical approaches (Alahmadi*et al.* 2022). The applied software has lots of ethical issues and for that mitigation of the issues in the applied software has been marked as one of the most crucial parts of the entire research work. The use of different strategies along with the different technologies has helped to make the categorization of the important factors of the research work based on the possibilities of having disturbances in the identification of the exact role of the IDS and IPS in cyber security. The possibility of the presence of vulnerabilities has been tried to minimize with the help of several technical approaches of auditing the applications or the software (Khoulimi*et al.* 2022).

## 3.6 Commercial risks and risk management

The identified issues have been tried to mitigate with the assurance of the applied strategies of the past research papers but any kinds of research requirements are not copied from the past research work. The concepts have been gathered so that it can be possible to implement them in the understanding of the role of the IDS and IPS in cyber security. The identified risks have been highlighted at first and then these have been categorized so that mitigation of the identified issues can be possible within a minimum time (Khan et al. 2022).

## 3.7 Summary

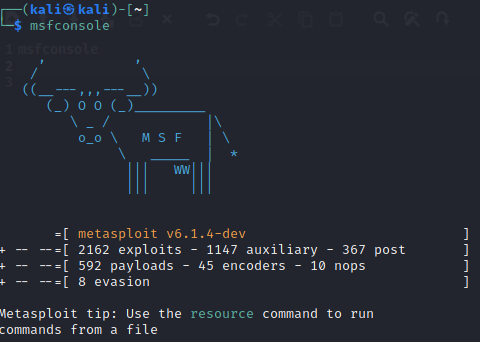
The presence of the research methodology has given the opportunity to make the understanding of the concept matters of the research work in the simplest way. The choice of the methods has been inserted in the very first section of the research methodology chapter for the representation of all the applied research followings. Then the justification of the research methods has been attached to these research methodologies in the form of words. The justification of the chosen one has been elaborated in a specific section of the research methodology. Then the data collection and the analysis related to the research work on the role of the IDS and IPS in cyber security have been discussed for a better understanding of the data collection method. Here the validation of the collected data has been also done and this has been elaborated on in a specific chapter. In the last, the information on the ethical issues and the commercial risks has been provided in two different sections.

# Chapter 4: Quality and Results

## 4.1 Critical Analysis

The greater role of the IDS and the IPS in cyber security has been checked with the help of the latest tools and technology. Here Kali Linux has been used to do penetration testing. This has helped to make the identification of the present loophole in the websites of the software. Based on the identification of the results the mitigation of them has been done in the most effective way. The achievement of the main aim of the research has been one of the simplest tasks by splitting the research aim into different objectives (Mahmoud *et al.* 2022). The mitigation of the identified issues has given the opportunity to the researchers to get the solutions to the research questions in the most attractive way. The categorization of the identified challenging factors has been done based on their impacts on the research outcomes.

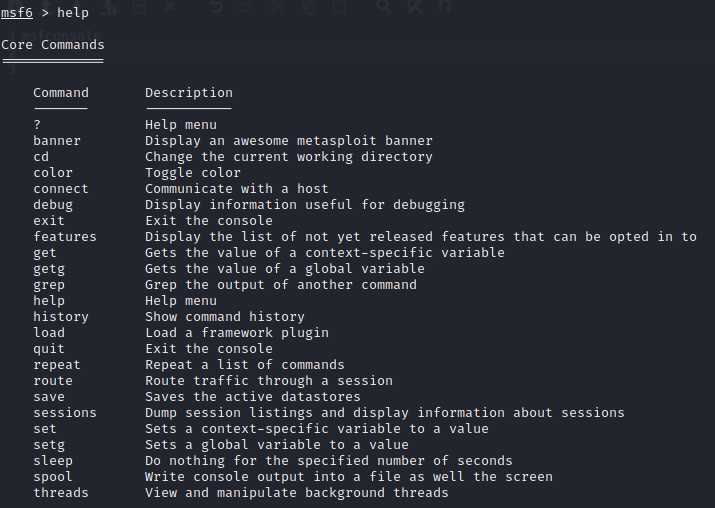
## 4.2 Evidence of practical work

****

#### Figure 4.2.1: Console

(Source: self-created)

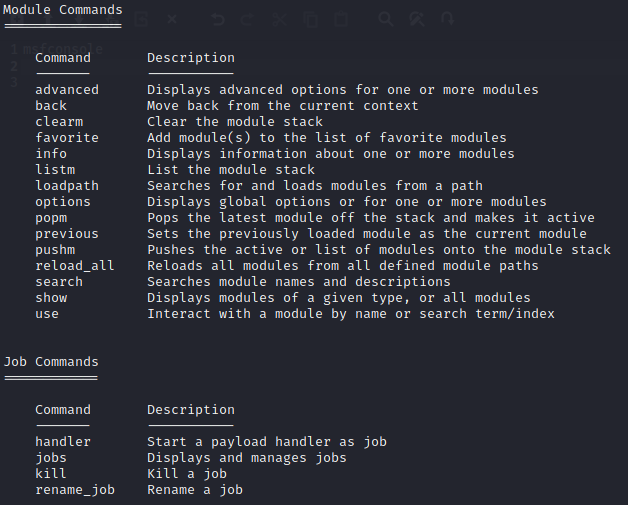
The above image shows the opening phase of the software which is “Kali Linux” in this case. It can be seen that exploits, auxiliary, posts and many other things can be applicable to this software. The numerical values of these things can also be seen in this case.

****

#### Figure 4.2.2: Core commands

(Source: self-created)

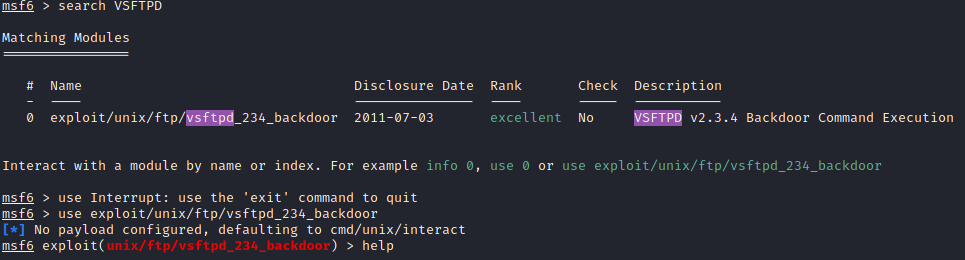
The image that has been used above is displaying the core command that can be used in this project so that the designers and the developers can do their required tasks. It can be seen that there are a lot of tasks they can fulfill with the help of this software. The commands are written on the left and their description is on the right side.

****

#### Figure 4.2.3: Module commands and job commands

(Source: self-created)

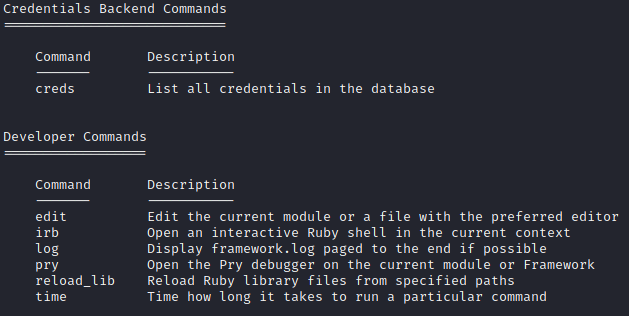
The job commands and the module commands that can be used in this case can be seen in the image above. There are 15 module commands in total and 4 job commands that can be seen in the image above. The description of the commands is also written in the image as well.

****

#### Figure 4.2.4: Matching modules

(Source: self-created)

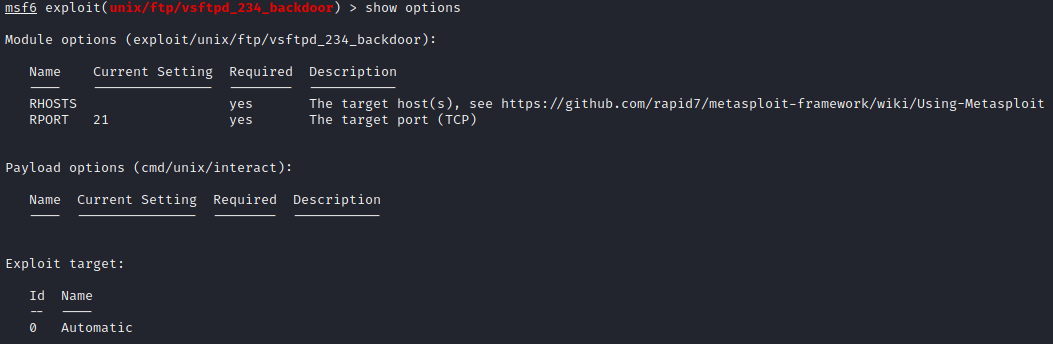
The above image shows the matching modules that are used in the project. A brief description of the module that has been taken care of has been added to this section. The selection of the module has been done based on the requirements of the tasks. The name of the module can be seen in the image above along with the disclosure date and description. It can be seen that the rank is excellent in this case.

****

#### Figure 4.2.5: Developer commands and credential backend commands

(Source: self-created)

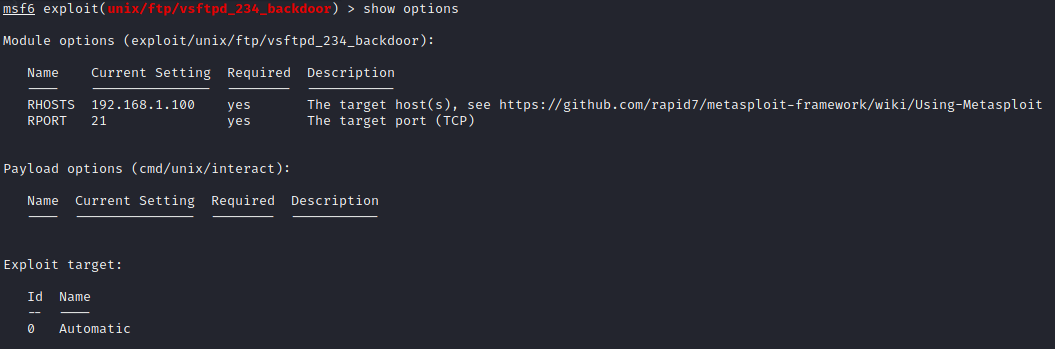
The above image displays the developer command and the credential backend commands along with their descriptions. It can be seen that only one credential command has been used in this case. The command is ***“cred”*** and it is used to list all the credentials that can be used in this case. There are 6 developers commands that have been used in the project and their descriptions have also been listed in the image above.

****

#### Figure 4.2.6: List of options

(Source: self-created)

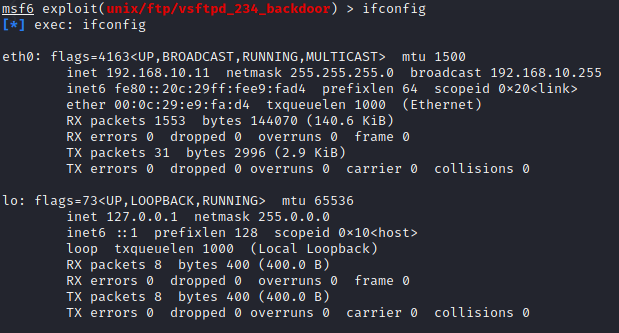
The above image is the output of the commands ***“show options”*** and it can be seen that the RHOST and RPOST are blank in this case, but the requirements of these can also be seen. Thus these are required to be imported into this section as soon as possible. The description of these parts has also been stated in this case as well. It can also be seen that there are no target devices at all.

****

#### Figure 4.2.7: RHOST and RPOST

(Source: self-created)

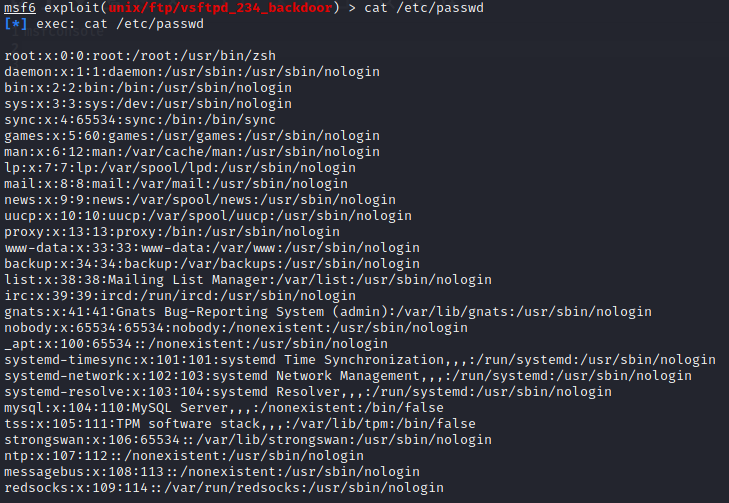
The above image shows the credentials that were required before the step. These credentials have been provided to the system after seeing the requirements. The provided credentials can be seen in the image above. It can be seen that an IP address has been added for the RHOST and in the other part, 21 is the number.

****

#### Figure 4.2.8: Configuration

(Source: self-created)

The configuration of the target system can be seen in the image above and it can be seen that the configuration has been classified into two parts. The name of the targeted system and its IP address can also be seen in the image above with the help of the commands that have been used in this case.

****

#### Figure 4.2.9: Password

(Source: self-created)

The above image shows the result that has come from the commands that can also be seen in the image above. It can be seen that a wide range of passwords has been used in the system that has been targeted in the task. The different password that has been used for different purposes can be seen in brief.

****

#### Figure 4.2.10: Command for shadow

(Source: self-created)

The required commands to see the shadow of the target system can be seen in the image above. In the result section, it can also be seen that the permission has been denied due to a strong protection system that has already been imported to the target system.

The result that has cropped up after the implementation of the software reflects the required sections of the tasks. The main purpose of the software was to identify whether the system is protected or not. It can be seen that the target system is not that much vulnerable so the intrusion process is not possible for that particular system.

## 4.3 Awareness and solution to the technical challenges

The designers and the developers had to face a few challenges regarding the implementation of the system. The challenges are mainly technical challenges and those have been stated in the following section.

* The vulnerability of the target system can be a real issue or challenge for the developers (Ring *et al.* 2018).
* The software that has been used in this case is very slow compared to other software that can be used for the same task. Thus it takes a lot of time for the designers and developers to fulfill the tasks.
* The operating system is penetration oriented, thus it is not very easy to use (Sadique*et al.* 2019).

## 4.4 Novelty

Novelty in research or any work can be defined as the newness and uniqueness of the task that has been implemented by the authority. It is one of the most important parts of the designers and developers to identify the novelty of their task so that it does not match with any others task. The novelty should be maintained throughout the entire work. It can be maintained using many procedures such as the different approaches to the methods that are to be applied in the research work and the entire project. On the other hand, the research process can be new or the model that has been used in the task can be unique.

The task that has been done in this project has been done with the help of “Kali Linux” and it can be seen that a different approach has been taken care of in this section. The model that has been created is based on the mindset of the developer.

## 4.5 Interpretation of result

This section has been added to the dissertation so that the readers can able to understand the analysis that has been done based on the result that has been gathered from the experiments and software work.

****

#### Figure 4.5.1: Banner

(Source: self-created)

The above image shows a banner that has been implemented in this project. It can be seen that the banner is shaped like a “reverse” sign. The banner has been made with the help of the alphabet and symbols.

## 4.6 Use of tools and techniques

The selection of tools is one of the most important parts of a project that requires software. It can be seen that the topic that has been taken into account can be done with the help of different tools and techniques. The different operating systems can be used to fulfill the task and the different tools have been listed in this section.

| **Tools and techniques** | **Features** |
| --- | --- |
| 1. Invicti | It is used to detect the dead vulnerability of a system that can be targeted by cybercriminals (Mahboub*et al.* 2021).  A minimum number of configurations are used for the implementation of this particular tool. |
| 2. Can and Able | It can be defined as an operating system that is mostly used to gather passwords (Mahmoud *et al.* 2022).  It uses dictionary attacks to crack encrypted passwords. |
| 3. Nmap (network mapper) | It is used to scan the ports of different devices that are selected for hacking.  It can discover different services and be used as a host to a network (Mathew, 2020). |
| 4. Nikto | One of the main features of this system is that it is an open-source tool and it can check the servers that are outdated.  It can also be used to identify insecure files and programmes (Rantos*et al.* 2020). |

##### Table 4.6.1: Different tools and techniques

The table that has been used above and in this section shows the different tools and techniques that can be used to serve the purposes based on the topic that has been selected in the case. The table highlights the tools that can be used along with the main features.

## 4.7 Appropriate tools for analysis

Among the tools and techniques that can be used for the IPS and IDS, it can be seen that appropriate software and approach have been taken care of in this project. The selection of the tools is based on the requirements of the project. Different tools are required to serve different tasks. Thus it is one of the main functions of the developers to identify the objective of the project and select the appropriate software.

## 4.8 Linkage to objectives and literature

The main aim has been divided into different objectives for better outcomes of the main aim of the research work. The analysis of the most suitable process has been possible to view so that the determination of the defense system of the IDS and IPS in cyber security can be one of the easiest tasks. The scrutiny of the work structure of the IDS and IPS in cybersecurity has been possible for this research work. The understanding of all the most appropriate tools and technologies has been possible so that the essential information about cyber security and denial and service attacks under the network traffic can be gathered in the most accurate way.

## 4.9 Summary

The summary of the results has given the overall ideas of the results of the role of the IDS and IPS in cyber security. The critical analysis chapter has given the ideas of the applied tools and technologies in the practical section of the research works. The evidence of the practical work has been elaborated in a specific chapter for a better understanding of the software work and its implementation in real-time. Then the awareness and the solution to the technical challenges have been illustrated in the results chapter in the most attractive way. The applied new tools and technology and strategies have been introduced in the novelty section. The practical outputs have been inserted in the interpretation of the results chapter. The uses of the tools and technology have given them all the ideas of the applied technologies for making the understanding of their application of them in practical work. Then the analysis of them has been also previewed in the research paper. In the last, the linkage to the objectives has been noted down in the results chapter for representation of the overall progress of the research work.

# Chapter 5: Evaluation and Conclusion

## 5.1 Critical evaluation

This project is based on the role of IDS and IPS in cyber security. IDS are an intrusion detection system which is a monitoring system that monitors all disbelieving and unethical activities. It helps to detect all unethical activities. It helps to create responsible data alerts for securing the data system. It helps to detect system alerts for databases which help to detect direct data. It is installed in the system for protecting against unethical hacking. Intrusion detection systems are important to know about the functions of IDS for cyber security. Its monitoring system catches unethical actions and generates alerts. Those alerts are security sanctions which indicate unethical activities in the system. This kind of data function is important for security issuers. This data allows various objects for this specific project. All data are associated with the fundamentals of this project. IPS is an instruction prevention system which is also known as an instruction detection prevention system. This technology briefly monitors the system for malicious activities. This kind of data allows for the system allocation process. IPS technology system holds an eye on a network for malicious movements. It accesses every system packages for securing data models. For completing this project it is important to gather knowledge about IPS and IDS. For completing this project all data are collected from a specific website. This kind of data allows various kinds of activities for the project guideline. In this critical evaluation part, the discussion is based on the discussion about IDS and IPS. These works are similar but in different ways. This kind of data protests all ethical activities performed in a secure system. It affects all kinds of data values for ethical activities. Various kinds of activities are used in this project to detect all the values. To complete this project first verifies and analyses all the data about cyber security. Early performance of technology was deployed in detect method on the machine. This kind of data value is affected by digital data which is affected all ethical values. This kind of data source isactivating various kinds of data for applying data methods. All the data methods are equally affected by the data allocation system. This kind of data is affected by the data allocation process. Various data activities are all used for the data allocation process. This kind of data is used in this project. Kali Linux software is used in this project which is advanced penetration testing software (Thapa and Mailewa, 2020). IDS technology is a monitoring system which simplifies the project guideline. This project needs some specific effect on system hacking. This project is simplified for generating all the effects of IPS and IDS against unethical hacking.

## 5.2 Summary of the achievement

IDS indicate default tools for this software which perform in a specific manner for smooth packages. This kind of data value is affected by a web application. It detects all the instructions prevention systems for the application detection system. This kind of data value is affected by the system software so which can be harmful to this allocation system. These database systems are associated with the functions. To complete this project first data collection process is associated with the functions which are allocated with the facts and data. First, analyze all the specific data which is important for this project. Then all important data are saved on a specific website. Which is important for this project guideline? This data allocation is processed for software data applications (Mahboub*et al.* 2021). For completing this project all the data are associated with the fundamentals of this project. For this project, Kali Linux software is used for this project guideline. This project was completed for a specific software application. In this case, Kali Linux is used for the development of cyber security projects. In this case, the web application is fairly used for project guidelines. This kind of data allocation is used for secure system data. In this project, penetration testing is allocated with kali Linux associated with the substance.

## 5.3 Reflection

The project work is mainly based on the discussion which complicity innovate the application of this project. This kind of data allows for various kinds of objects which are allocated with the fundamentals of this project. For completing this project the project guideline is associated with the information of this project. This project is based on information about IDS and IPS. In this project, the main work is to define the weakness of the system by penetration testing. In this project, the project work is associated with the system allocation process. In this project, the project work is associate is associated with the fundamentals of this project. First, to complete this project it is important to gather knowledge about IDS and IPS. So, first I gather knowledge about IPS and IDS from a specific website. Then briefly analyses all the different aspects of the project guideline. This kind of data is important for completing this project. After analyzing all the data it is important to analyses aspects of the project guideline. This data is associated with the fundamentals of this project. Then penetration testing is performed for the testing of this project. This project guideline is associated which is founded on the data allocation process. For completing this project this project guideline is associated with the fundamentals of this project guideline. This project is associated with the data allocation process which is a various object of this project. In this process, all data are related to the role of IDS and IPS. This data is associated with various data which is related to unethical hacking. A simple analysis process is done for this project.

## 5.4 Research recommendation

In this research recommendation part, the discussion is based on the project development works. The main focus to complete this project is the development of this project. This project verified by developing this project guideline. It is important to develop the project by gathering knowledge about the title. This project is associated with the fundamentals of this project. This project is associated with the data allocation process. This kind of data is associated with the project guideline in this project. This project is associated with the fundamentals of this project which is allocated with the associate of this project. This project guideline is the main allocation process which is based on the data allocation process. This data allocation process is the project guideline in this project. This kind of data is associated with ethical data (Jaber *et al.* 2020). This kind of data is formatted for the digital data allocation system. For completing this project it is necessary to discuss similar instructions about this project. It is important for security instructions which are allocated with a secure data process. This kind of data is associated with the formation of this project. For completing this project penetration test is associated with the project guideline. This kind of project is formatted for the system operator which is regulated by this project guideline. This kind of data is associated with the allocation system. In this case, penetration work is a testing work which finds the weak functions of the system. This data allocation process is associated with finding the weakness of the system. For this research, the recommendation is the requirements of this project guideline. This project is related to the objects. This data allocation system is important to improve the values and all data sets are equal to produce the aspects. This project is associated with the fundamentals of this project. Kali Linux is important in this project to find the loops of the system. It is the main purpose of this project to find loopholes in the system and detect them by IDS.

## 5.5 Achievements of the objectives

In this achievement of the objectives parts, the achievements are discussed for the project. The first object is to analyze the method of deciding on the guard system of IDS and IPS in cyber security. This is the main function of these objects. This kind of data is associated with the data which defines different systems of IDS AND IPS in cyber security. The second objective is to explore the process of choosing the defence system of IDS and IPS in cyber security. In this second objective, it is important to gather knowledge about IDS and IPS. It helps to detect all the aspects of this project which is associated with the fundamentals of this project. This work is to define the system for IDS. The third objective is to gather essential knowledge about cyber security. This data is important for gathering knowledge about data allocation systems. It is important to know about the data which is related to IDS and IPS. This project is mainly based on the functions which process some digital values for this project. This data allocation process is simplified for data objects. Due to completing this project, it is important to know about cyber security. This kind of data is allocated with the objects which are associated with the data. This kind of data is processed for the project title. The fourth objective is to process the grouping of all kinds of tools and methods that have been needed to complete the hacking of websites with the use of IDS and IPS in the Kali Linux operating system. This kind of operating system is generated for the grouping of values which is important for the evaluation of this project. Due to completing this project, all ethical guidelines are followed for the concept of this project. This system is operated for the project guideline. This data is important for gathering knowledge about cyber security. This data is necessary to complete the objects for this project. These data objects are associated with the fundamentals of this project. In this project, all ethical adats are associated with the project guideline. For verifying all the objects it is important to collect the data for data objects. So finally the objects are important for this project to verify all the data for all the data objects. The role of the project is to define all ethical values for this project guideline. This project needs a brief discussion about the data objects which is allocated for data formation. In this project, using Kali Linux software for folding system loops is related to ethical hacking. In this part, the mainly discussion is associated with the data objects which is used in this project.

## 5.6 Future work

In this project, the future work is to verify all the results which would be helpful in future. In this generation, this work is related to the functions of this project. This project's results would be very useful in future because of cyber security. Technology is everywhere for technical work. This kind of work is related to future work. In this project mainly discussion is based on the IPS and IDS. This project mainly defines the cybersecurity-related work which is associated with the fundamentals of this project. This project work is related to the objects which are related to the fundamentals of this project. In this project ethical consideration is necessary to give complete meaning. All sources are reliable for this project to discuss the data objects. These data are related to the guideline in this project. This data allocation system is important for the project guideline. The technical requirement is important for this project. It gives a complete menacing for the project guideline. This data allocation process is important for the guideline of this project. All data values are ethical for the guideline of this project. In this project, Kali Linux is used for completing the tasks. This kind of data is important in future to control the guideline. This data is important to improve the values. In future, it would be important for founding the weakness of the system. In this part, the discussion is based on the future benefits of this project.

# References

Adawadkar, A.M.K. and Kulkarni, N., 2022. Cyber-security and reinforcement learning—A brief survey. *Engineering Applications of Artificial Intelligence*, *114*, p.105116.

Alahmadi, A.N., Rehman, S.U., Alhazmi, H.S., Glynn, D.G., Shoaib, H. and Solé, P., 2022. Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture. *Sensors*, *22*(9), p.3520.

Alhasani, A., Alzahrani, T., alFahhad, R. and Alotaibi, M., 2022. Role of Machine Learning in Intrusion Detection System: A Systematic Review. *International Journal of Computer Science & Network Security*, *22*(3), pp.155-162.

Baci, N., Vukatana, K. and Baci, M., 2022. Machine learning approach for intrusion detection systems as a cyber security strategy for Small and Medium Enterprises. *WSEAS Transactions on Business and Economics*, *19*, pp.474-480.

Bandyopadhyay, S., Chowdhury, R., Roy, A. and Saha, B., 2020. A step forward to revolutioniseintrusiondetection system using deep convolution neural network.

Ben Fredj, O., Mihoub, A., Krichen, M., Cheikhrouhou, O. and Derhab, A., 2020, November. CyberSecurity attack prediction: a deep learning approach. In *13th International Conference on Security of Information and Networks* (pp. 1-6).

Davies, G., Mison, A. and Eden, P., 2022, March. Addressing the Skills Shortage in Cybersecurity. In *International Conference on Cyber Warfare and Security* (Vol. 17, No. 1, pp. 544-551).

Deyannis, D., Papadogiannaki, E., Chrysos, G., Georgopoulos, K. and Ioannidis, S., 2022. The Diversification and Enhancement of an IDS Scheme for the Cybersecurity Needs of Modern Supply Chains. *Electronics*, *11*(13), p.1944.

Durmus, Ö., Varol, A. and Varol, N., 2019, November. Infrastructure Requirements for Cybersecurity. In *2019 1st International Informatics and Software Engineering Conference (UBMYK)* (pp. 1-5). IEEE.

Dwyer, A.C., Stevens, C., Muller, L.P., Cavelty, M.D., Coles-Kemp, L. and Thornton, P., 2022. What Can a Critical Cybersecurity Do?. *International Political Sociology*, *16*(3), p.olac013.

Elsayess, M., 2020. Cyber Security and Normalization Theory. *International Journal of Computer Engineering and Technology*, *11*(3).

Faquir, D., Chouliaras, N., Sofia, V., Olga, K. and Maglaras, L., 2021. Cybersecurity in smart grids, challenges and solutions. *AIMS Electronics and Electrical Engineering*, *5*(1), pp.24-37.

Giannoutakis, K.M., Spathoulas, G., Filelis-Papadopoulos, C.K., Collen, A., Anagnostopoulos, M., Votis, K. and Nijdam, N.A., 2020, November. A blockchain solution for enhancing cybersecurity defence of IoT. In *2020 IEEE International Conference on Blockchain (Blockchain)* (pp. 490-495). IEEE.

Iavich, M., Bocu, R. and Gagnidze, A., 2022, April. Real Time Self-developing Cybersecurity Function for 5G. In *International Conference on Advanced Information Networking and Applications* (pp. 380-387). Springer, Cham.

Jaber, A.N., Anwar, S., Khidzir, N.Z.B. and Anbar, M., 2020, December. The Importance of IDS and IPS in Cloud Computing Environment: Intensive Review and Future Directions. In *International Conference on Advances in Cyber Security* (pp. 479-491). Springer, Singapore.

Jahwar, A.F. and Ameen, S.Y., 2021. A Review on Cybersecurity based on Machine Learning and Deep Learning Algorithms. *Journal of Soft Computing and Data Mining*, *2*(2), pp.14-25.

Kabanov, I. and Madnick, S., 2021. Applying the Lessons from the Equifax Cybersecurity Incident to Build a Better Defense. *MIS Quarterly Executive*, *20*(2), p.4.

Kabanov, I. and Madnick, S., 2021. Applying the Lessons from the Equifax Cybersecurity Incident to Build a Better Defense. *MIS Quarterly Executive*, *20*(2), p.4.

Khan, S.U., Eusufzai, F., Azharuddin Redwan, M., Ahmed, M. and Sabuj, S.R., 2022. Artificial Intelligence for Cyber Security: Performance Analysis of Network Intrusion Detection. In *Explainable Artificial Intelligence for Cyber Security* (pp. 113-139). Springer, Cham.

Khoulimi, H., Lahby, M. and Benammar, O., 2022. An Overview of Explainable Artificial Intelligence for Cyber Security. *Explainable Artificial Intelligence for Cyber Security*, pp.31-58.

Khoulimi, H., Lahby, M. and Benammar, O., 2022. An Overview of Explainable Artificial Intelligence for Cyber Security. *Explainable Artificial Intelligence for Cyber Security*, pp.31-58.

Kour, R., Thaduri, A. and Karim, R., 2019. Railway Defender Kill Chain for Cybersecurity. *eMaintenance*, p.20.

Larbaoui, Y., Naddami, A. and Fahli, A., 2021. Implicated Factors in the Success of E-learning Platforms and Online Laboratories of Experimenting along with Enhancement of their Cybersecurity. *International Journal*, *9*(12).

Larbaoui, Y., Naddami, A. and Fahli, A., 2021. Implicated Factors in the Success of E-learning Platforms and Online Laboratories of Experimenting along with Enhancement of their Cybersecurity. *International Journal*, *9*(12).

Lee, D. and Kim, H.K., 2021. Real-time security Monitroing assessment model for cybersecurity vulnerabilities in network separation situations. *Convergence Security Journal*, *21*(1), pp.45-53.

Long, Z., Tan, L., Zhou, S., He, C. and Liu, X., 2019, July. Collecting indicators of compromise from unstructured text of cybersecurity articles using neural-based sequence labelling. In *2019 international joint conference on neural networks (IJCNN)* (pp. 1-8). IEEE.

Mahboub, S.A., Ahmed, E.S.A. and Saeed, R.A., 2021. Smart IDS and IPS for cyber-physical systems. In *Artificial intelligence paradigms for smart cyber-physical systems* (pp. 109-136). IGI Global.

Mahboub, S.A., Ahmed, E.S.A. and Saeed, R.A., 2021. Smart IDS and IPS for cyber-physical systems. In *Artificial intelligence paradigms for smart cyber-physical systems* (pp. 109-136). IGI Global.

Mahboub, S.A., Ahmed, E.S.A. and Saeed, R.A., 2021. Smart IDS and IPS for cyber-physical systems. In *Artificial intelligence paradigms for smart cyber-physical systems* (pp. 109-136). IGI Global.

Mahmoud, R.V., Anagnostopoulos, M. and Pedersen, J.M., 2022. Detecting Cyber Attacks through Measurements: Learnings from a Cyber Range. *IEEE Instrumentation & Measurement Magazine*, *25*(6), pp.31-36.

Mahmoud, R.V., Anagnostopoulos, M. and Pedersen, J.M., 2022. Detecting Cyber Attacks through Measurements: Learnings from a Cyber Range. *IEEE Instrumentation & Measurement Magazine*, *25*(6), pp.31-36.

Mahmoud, R.V., Anagnostopoulos, M. and Pedersen, J.M., 2022. Detecting Cyber Attacks through Measurements: Learnings from a Cyber Range. *IEEE Instrumentation & Measurement Magazine*, *25*(6), pp.31-36.

Mathew, A.R., 2020. Cybersecurity pros warn–covid-19 pandemic as a tool. *International Journal of Engineering and Advanced Technology (IJEAT)*, *9*(4).

Moustakidis, S. and Karlsson, P., 2020. A novel feature extraction methodology using Siamese convolutional neural networks for intrusion detection. *Cybersecurity*, *3*(1), pp.1-13.

Nygard, K.E., Rastogi, A., Ahsan, M. and Satyal, R., 2021. Dimensions of Cybersecurity Risk Management. In *Advances in Cybersecurity Management* (pp. 369-395). Springer, Cham.

Panigrahi, R. and Borah, S., 2018. A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems. *International Journal of Engineering & Technology*, *7*(3.24), pp.479-482.

Rabelo, L., Ballestas, A., Valdez, J. and Ibrahim, B., 2022. Using Delphi and System Dynamics to Study the Cybersecurity of the IoT-Based Smart Grids. *ParadigmPlus*, *3*(1), pp.19-36.

Rantos, K., Spyros, A., Papanikolaou, A., Kritsas, A., Ilioudis, C. and Katos, V., 2020. Interoperability challenges in the cybersecurity information sharing ecosystem. *Computers*, *9*(1), p.18.

Ring, M., Frkat, D. and Schmiedecker, M., 2018. Cybersecurity evaluation of automotive e/e architectures. In *ACM Computer Science In Cars Symposium (CSCS 2018)*.

Sadique, F., Bakhshaliyev, K., Springer, J. and Sengupta, S., 2019, January. System architecture of cybersecurity information exchange with privacy (cybex-p). In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0493-0498). IEEE.

Sadique, F., Bakhshaliyev, K., Springer, J. and Sengupta, S., 2019, January. A system architecture of cybersecurity information exchange with privacy (cybex-p). In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0493-0498). IEEE.

Salloum, S.A., Alshurideh, M., Elnagar, A. and Shaalan, K., 2020, April. Machine learning and deep learning techniques for cybersecurity: a review. In *The International Conference on Artificial Intelligence and Computer Vision* (pp. 50-57). Springer, Cham.

Savin, V.D. and Serban, C., 2019. Cybersecurity Vulnerabilities and Threats of Scada Systems in Critical Infrastructures. *Proceedings of the IMC, Amsterdam, The Netherlands*, pp.1-3.

Stamatescu, G., Stamatescu, I., Arghira, N. and Făgărășan, I., 2020, June. Cybersecurity Perspectives for Smart Building Automation Systems. In *2020 12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)* (pp. 1-5). IEEE.

Sun, C.C., Cardenas, D.J.S., Hahn, A. and Liu, C.C., 2020. Intrusion detection for cybersecurity of smart meters. *IEEE Transactions on Smart Grid*, *12*(1), pp.612-622.

Thapa, S. and Mailewa, A., 2020, April. The role of intrusion detection/prevention systems in modern computer networks: A review. In *Conference: Midwest Instruction and Computing Symposium (MICS)* (Vol. 53, pp. 1-14).

Walker, A. and Benton, D., 2022. *Cybersecurity Standards for Photovoltaic Operations* (No. NREL/PR-5C00-82588). National Renewable Energy Lab.(NREL), Golden, CO (United States).

Walker, A. and Benton, D., 2022. *Cybersecurity Standards for Photovoltaic Operations* (No. NREL/PR-5C00-82588). National Renewable Energy Lab.(NREL), Golden, CO (United States).