

INTRUSION DETECTION AND PREVENTION SYSTEM

A Report for the Evaluation 4 of Project2

Submitted by

TABISH KHAN

(1613101775 /16SCSE101826)

*in partial fulfillment for the award of
the degree of*

Bachelor of Technology

IN

**SCHOOL OF COMPUTING SCIENCE AND
ENGINEERING**

Under the Supervision of

MR. A. ARUL PRAKASH
Assistant Professor

APRIL / MAY – 2020

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
1.	Abstract	1
2.	Introduction	2
3.	Existing System	5
4.	Proposed system	7
5.	Implementation or architecture diagrams	10
6.	Output / Result / Screenshot	15
7.	Conclusion/Future Enhancement	18
8.	References	20

Abstract

Network Security is to protect computer network against hacking, misuse, unauthorized changes to the system and securing a computer network infrastructure. A firewall is a mechanism used to achieve network security. It can be either hardware or software based, that controls incoming and outgoing network traffic based on a set of rules. Network attack is the intrusion or threat can be defined as any deliberate action that attempts unauthorized access, information manipulation, or rendering the system unstable by exploiting the existing vulnerabilities in the system. An intrusion is any set of activities that attempt to compromise the integrity, confidentiality or availability of a resource. Intrusion Detection system (IDS) / Intrusion Prevention System (IPS) has become a prerequisite in computer networks. IDS/IPS is a device or software application that monitors network or system activities for malicious activities. These type of IDS/IPS used in the network is known as Network based IDS/IPS.

Network based Intrusion detection/prevention system (NIDPS) protects a network of hosts and systems. Based on the intrusion detection method, it is classified as Signature based and Anomaly based IDS/IPS. Signature based IDS/IPS is that they operate in much the same way as a virus scanner, by searching for a known identity or signature. It can only detect an intrusion attempt if it matches a pattern that is in the database, therefore the databases need to constantly be updated to detect the new attacks. An Anomaly based Intrusion Detection/Prevention System is a system for detecting computer intrusions by monitoring system activity and classifying it as either normal or anomalous. If malicious activity may be looks like normal traffic to the system, it will never send an alarm. Major drawback of anomaly-based IDS/IPS is that it generates more false positive alarm. Our proposed model is to implement the architecture of multi model based Anomaly IDS with time delay neural network based NIDS system. Virtual machine was used to implement the architecture of multimodal based anomaly IDS with Network based IDS system. Captured the packets in real time network traffic using the tool JPCAP. Packet features like Source IP, Destination IP, Port, Mac Address, format, Protocol type, etc

Introduction

The goal of this project is to design and develop fully implementable and tested Java based Intrusion Detection & Prevention System which can monitor network traffic from the host machine by capturing the network packets from the live network. I have made the assumption that this tool will be able to capture the network packets and allows the administrator to analyze the capture packets and can also be able to provide some feature to control network traffic. In order to control traffic from host machine a module called Firewall has been added, which allows administrator to create specific rules and it also allow administrator to delete the rule which are already created. This tool also able to dump (store) the captured information into a particular file format on local machine as well as on MySQL server. This project also employe's Honeypot which allows administrator capture hackers information.

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.

The goal of the Intrusion Detection & Prevention System is to identify the unauthorized of network access, it basically identity and scan the network for incoming and outgoing network packet from host machine. All this preferably in real time. The main functions to analyze incoming and outgoing packet from the network interface. The detection part in system to detect the communications of unauthorized packets from system. The pretension part in the system provides the set of option to block the network traffic an application part, it is a type of firewall to the system, allows application user to central the network traffic through selected network interface.

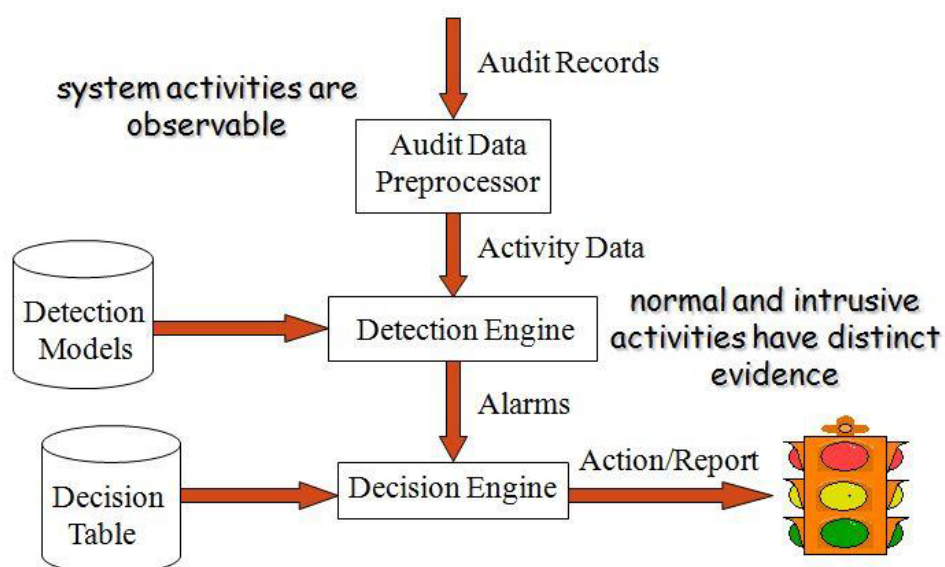
Information Security

Information security is the protection of information and minimize the risk of exposing

information to unauthorised parties. It is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational , human-oriented and legal) in order to keep information in all its locations (within and outside the organization perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats.

The value of information comes from the characteristics it possesses

- Availability
- Accuracy
- Authorization
- Confidentiality
- Integrity
- Utility



What is an intrusion detection system

An IDS is either a hardware device or software application that uses known intrusion signatures to detect and analyse both inbound and outbound network traffic for abnormal activities.

This is done through:

- System file comparisons against malware signatures.
- Scanning processes that detect signs of harmful patterns.
- Monitoring user behavior to detect malicious intent.
- Monitoring system settings and configurations.

What is an intrusion prevention system

An IPS complements an IDS configuration by proactively inspecting a system's incoming traffic to weed out malicious requests. A typical IPS configuration uses web application firewalls and traffic filtering solutions to secure applications.

An IPS prevents attacks by dropping malicious packets, blocking offending IPs and alerting security personnel to potential threats. Such a system usually uses a pre existing database for signature recognition and can be programmed to recognize attacks based on traffic and behavioral anomalies.

While being effective at blocking known attack vectors, some IPS systems come with limitations. These are commonly caused by an overreliance on predefined rules, making them susceptible to false positives.

An intrusion prevention system (IPS) is a form of network security that works to detect and prevent identified threats. Intrusion prevention systems continuously monitor your network, looking for possible malicious incidents and capturing information about them. The IPS reports these events to system administrators and takes preventative action, such as closing access points and configuring firewalls to prevent future attacks. IPS solutions can also be used to identify issues with corporate security policies, deterring employees and network guests from violating the rules these policies contain.

With so many access points present on a typical business network, it is essential that you have a way to monitor for signs of potential violations, incidents and imminent threats. Today's network threats are becoming more and more sophisticated and able to infiltrate even the most robust security solution.

Project Aim

The final project product is aimed at implementing the following:

1. To be able to list the network interfaces on host computer.
2. To be able to capture the packets on selected network interface.
3. To allow TCP port scanning
4. To be able to block the port on machine.
5. To be able to unblock the port on machine.
6. To be able to save the capture information in txt file format
7. To be able to save the capture information on remote SQL server.
8. To be able to run honeypot server on specific server
9. To be able to display number of Hacker connected to Main Server.

Advantages of Intrusion Detection Systems

- The network or computer is constantly monitored for any invasion or attack.
- The system can be modified and changed according to needs of specific client and can help outside as well as inner threats to the system and network.
- It effectively prevents any damage to the network.
- It provides user friendly interface which allows easy security management systems.
- Any alterations to files and directories on the system can be easily detected and reported

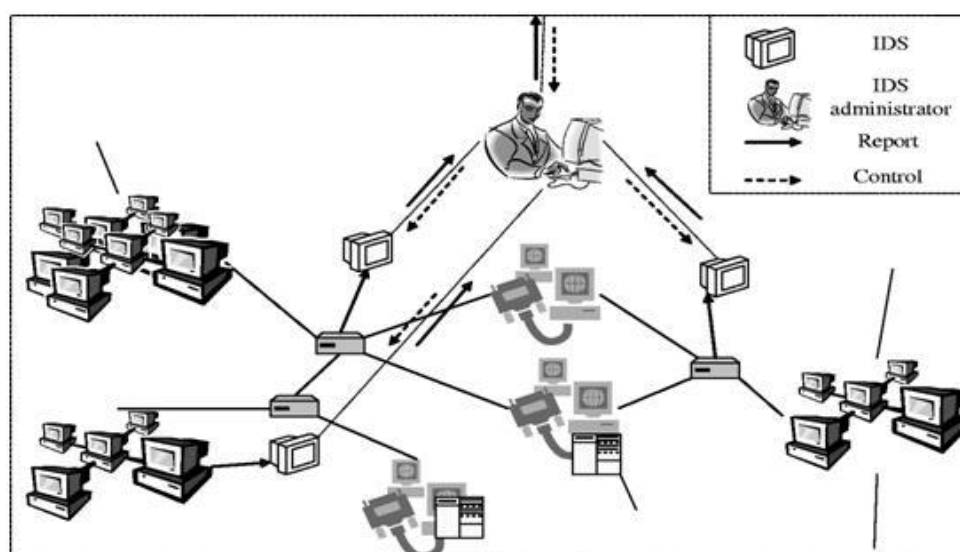
Classification of Intrusion Detection System

Based on the type of systems the IDS protect

- Network Intrusion Detection System
- Signature based IDS/IPS
- Anomaly based Intrusion Detection System

Existing System

This system monitors the traffic on individual networks or subnets by continuously analyzing the traffic and comparing it with the known attacks in the library. If an attack is detected, an alert is sent to the system administration. It is placed mostly at important points in the network so that it can keep an eye on the traffic travelling to and from the different devices on the network. The IDS is placed along the network boundary or between the network and the server. An advantage of this system is that it can be deployed easily and at low cost, without having to be loaded for each system.



Network Intrusion Detection System

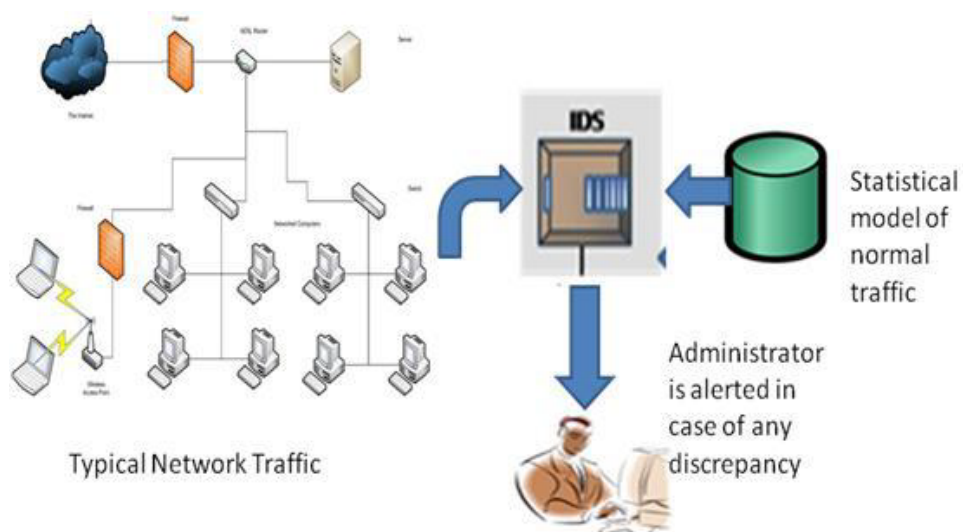
Signature based IDS/IPS

Signature based IDS/IPS is that they operate in much the same way as a virus scanner, by Searching for a known identity or signature.

An IDS can use signature-based detection, relying on known traffic data to analyze potentially unwanted traffic. This type of detection is very fast and easy to configure. However, an attacker can slightly modify an attack to render it undetectable by a signature-based IDS. Still, signature-based detection, although limited in its detection capability, can be very accurate. An advantage of this system is it has more accuracy and standard alarms understood by user.

Anomaly based Intrusion Detection System

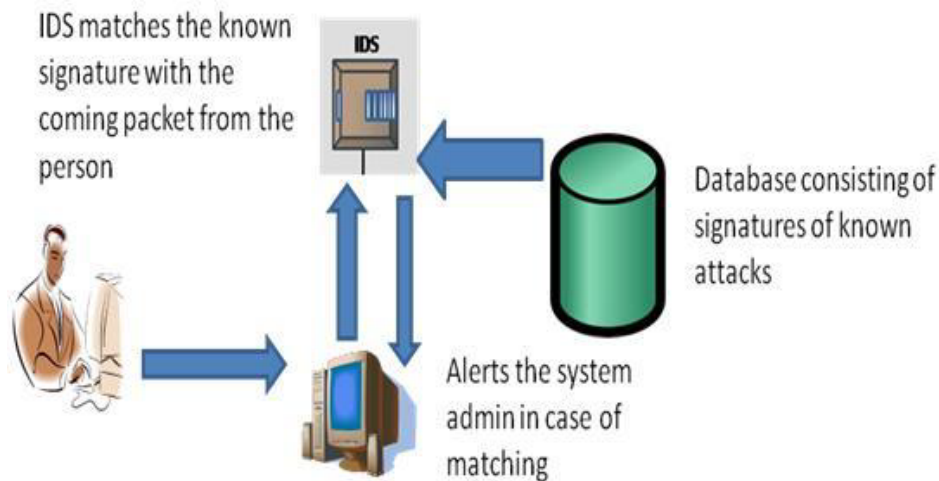
An Anomaly based Intrusion Detection/Prevention System is a system for detecting computer intrusions by monitoring system activity and classifying it as either normal or anomalous. It consists of a statistical model of a normal network traffic which consists of the bandwidth used, the protocols defined for the traffic, the ports and devices which are part of the network. It regularly monitors the network traffic and compares it with the statistical model. In case of any anomaly or discrepancy, the administrator is alerted. An advantage of this system is they can detect new and unique attacks.



Anomaly Based IDS/IPS

Limitations:

- If malicious activity may be looks like normal traffic to the system, it will never send an alarm.
- Major drawback of anomaly-based IDS/IPS is that it generates more false positive alarm.



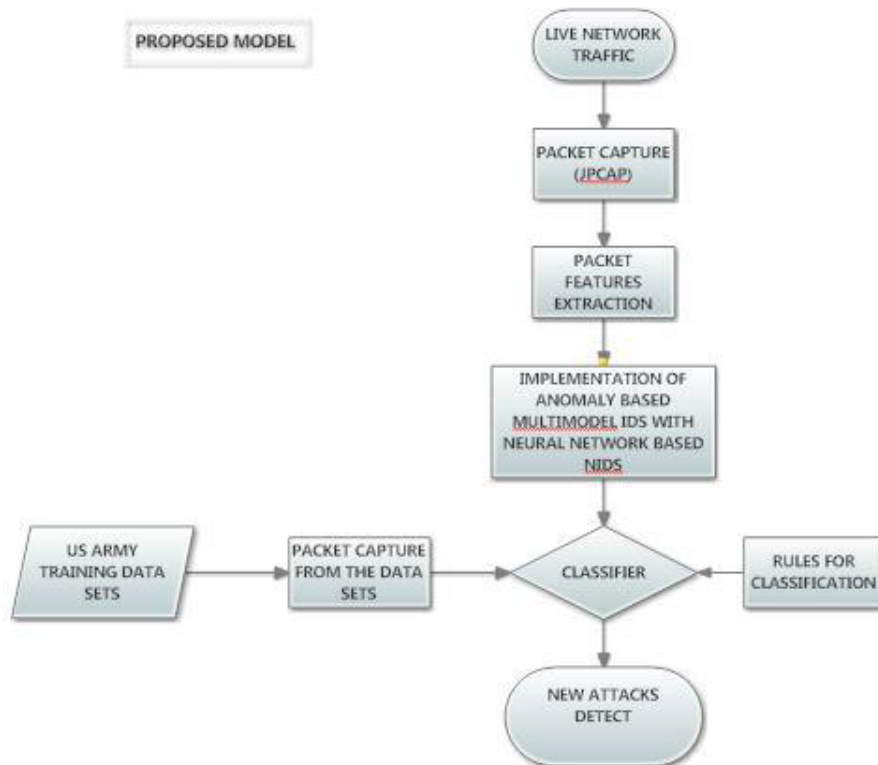
intrusion detection systems are often regarded as a core component in safeguarding production systems that house mission-critical data, IP, and other digital assets. Without an IDS in place, a business' production infrastructure and data are vulnerable to cyber attacks and other criminal activity. If the data is compromised by an unauthorized entity, the infrastructure of the entire company can quickly crumble, leaving much doubt about the organization's sustainability.

As part of an overarching security strategy that may include VPNs, virus protection, firewalls, or managed IT, an IDS has traditionally aided administrators in detecting intrusions and mitigating attacks. However, the role of IDS is slowly diminishing. The technology that hackers utilize to hijack a network and the counter-technology that administrators are implementing to combat these attacks have out-paced IDS scope and capacity. The need for real-time and zero day attack detection has rendered an IDS all but antiquated.

An intrusion detection system (IDS) is a device or a software application that performs any or all of these basic functions:

1. Monitors an entire network infrastructure for cyber attacks
2. Instantly detects a cyber attack as it occurs
3. Quickly deploys a countermeasure to stop the attack (intrusion prevention systems)
4. Submits reports to an administrator or security team

Proposed Model



- ∞ To write a Packet Capture Program using (JPCAP), to capture the real time network traffic
- ∞ Captured packets features can be analysed
- ∞ Planned to implement the multimodel based Anomaly IDS with Network IDS algorithm using JAVA code and make it to work with actual packets.
- ∞ Virtual machine can be used to implement the architecture of multimodal based anomaly IDS with Network based IDS system.
- ∞ Then Packet analysis and testing can be done by using the training data sets of US army.
- ∞ Classification of the packets can be done using the rules which differentiate the malicious and normal packets. With that it will detect the new attacks.

- Initially the connections have been made between the network traffic and Capturing tool using the interface datalink (Ethernet).
- Then the real time network packets were captured and save the packets in a file.
- After that read the captured packets from the file.

- Then sent the saved packets through the network interface.
- Packet features like Source IP, Destination IP, frames, Port, Mac Address, format, Protocol type, Datalink, Interface device name has been extracted.

Application Design

This section provides an overview the application design process. The application includes the pre design decisions and the relevant design decisions. This section also describes the programming language chosen for development and the environment used for development, and then provides details of the main design decisions which includes Multi-threading design of the programs and the logging of the information as a text file. This section also includes the decisions on NoSQL database selection.

Development Language

We choose Java as a development language for specific reasons. The primary reason is that, we are very familiar with Java through our previous coursework and the working experience, which enable us to focus our time on the design and development as java provides rich set of library class to build best GUI. Secondly, Java provides a stable and easy to use high level Sockets implementation, allowing us to not have to learn low-level socket programming and allowing us to concentrate on design and development. Finally, Java provides an excellent thread library which makes application Multithreaded and ease the implementation of Honeypot and other units in application as a multi-threaded application.

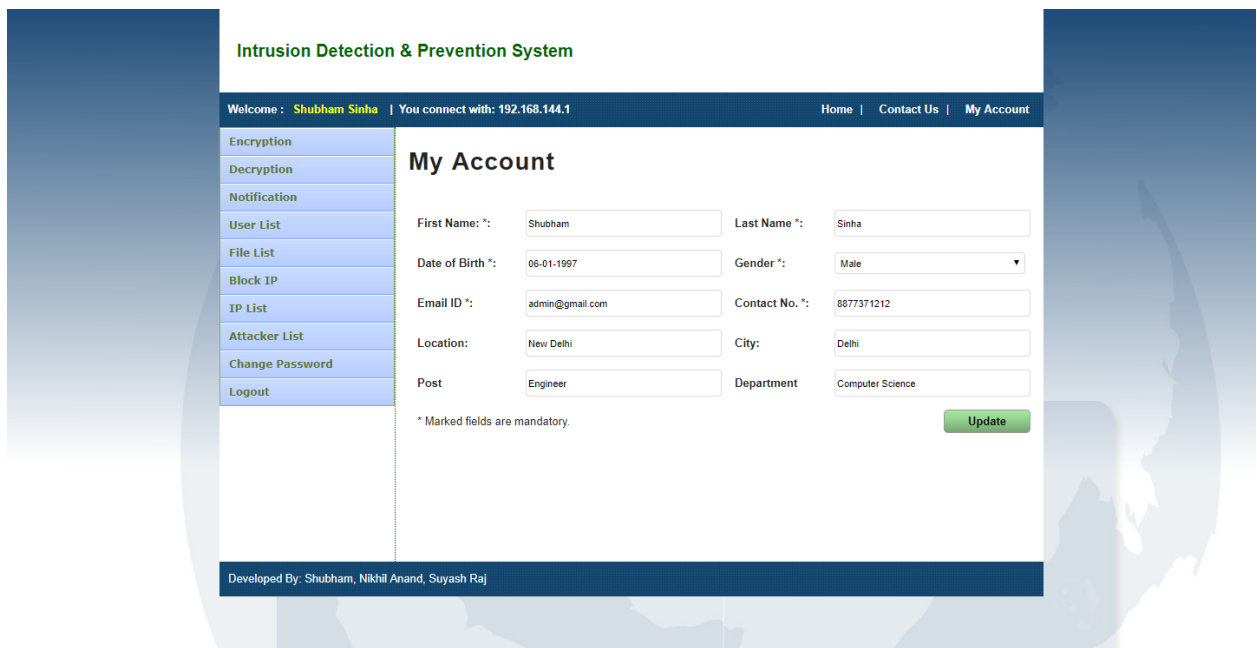
Integrated Development Environment (IDE)

An IDE is an application that provides software developers with an environment that eases tasks related to software programming as well as development. We choose NetBeans as the IDE in which we have developed the java application project. Eclipse is a free and open source product and is supported by the Athlone Institute of technology. It provides all the features of modern IDE such as code completion, refactoring and package management. Eclipse also has built in support for Java Documentation, which allowed easy generation of source code .

Implementation

Intrusion Detection & Prevention System supports the following features.

- **Graphical Interface** - Intrusion Detection & Prevention System provides a simple GUI to allow the user to control the application.



The screenshot displays the web interface of the Intrusion Detection & Prevention System. The page title is "Intrusion Detection & Prevention System". The user is logged in as "Shubham Sinha" and is connected to the IP address "192.168.144.1". The navigation menu includes "Home", "Contact Us", and "My Account". The left sidebar contains a list of menu items: Encryption, Decryption, Notification, User List, File List, Block IP, IP List, Attacker List, Change Password, and Logout. The main content area is titled "My Account" and contains a form with the following fields:

First Name *	<input type="text" value="Shubham"/>	Last Name *	<input type="text" value="Sinha"/>
Date of Birth *	<input type="text" value="06-01-1997"/>	Gender *	<input type="text" value="Male"/>
Email ID *	<input type="text" value="admin@gmail.com"/>	Contact No. *	<input type="text" value="8877371212"/>
Location:	<input type="text" value="New Delhi"/>	City:	<input type="text" value="Delhi"/>
Post	<input type="text" value="Engineer"/>	Department	<input type="text" value="Computer Science"/>

* Marked fields are mandatory.

Developed By: Shubham, Nikhil Anand, Suyash Raj

- **List the number of network interface** - The application displays the number of network interface on the host machine, user is allowed to select the interface to capture the packet from that interface.

Intrusion Detection & Prevention System

Welcome : **Shubham Sinha** | You connect with: 192.168.144.1 Home | Contact Us | My Account

Encryption

Decryption

Notification

User List

File List

Block IP

IP List

Attacker List

Change Password

Logout

Notifications

S.No	Activity	Date	IP Address	User Agent	Delete
1.	Login at 2019-05-07 00:06:59 with ip address - 192.168.144.1 and user agent Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36	2019-05-07 00:06:59	192.168.144.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36	
2.	Login at 2019-05-07 00:04:02 with ip address - 0:0:0:0:0:1 and user agent Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36	2019-05-07 00:04:02	0:0:0:0:0:1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36	
3.	Register at 2019-05-07 00:03:58 with ip address - 0:0:0:0:0:1 and user agent Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36	2019-05-07 00:03:58	0:0:0:0:0:1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36	
4.	Login at 2019-05-07 00:02:17 with ip address - 0:0:0:0:0:1 and user agent Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36	2019-05-07 00:02:17	0:0:0:0:0:1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36	
5.	Register at 2019-05-07 00:02:03 with ip address - 0:0:0:0:0:1 and user agent Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36	2019-05-07 00:02:03	0:0:0:0:0:1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36	

Developed By: Shubham, Nikhil Anand, Suyash Raj

- **Captures packet on selected interface** – The packets are captures from the selected interface, allowing to display the packet information on the application display area.
- **Displays captured packet information** – The application extracts the contents of the captured packet and project that contents on the display area allowing user to easily read them.
- **List the number of open pots on machine** – The application also performs port scanning on the host machine and displays information about all the TCP and UDP pots on machine. It also tells which port is listening.

Intrusion Detection & Prevention System

Welcome : **Shubham Sinha** | You connect with: 192.168.144.1 Home | Contact Us | My Account

Encryption

Decryption

Notification

User List

File List

Block IP

IP List

Attacker List

Change Password

Logout

IP Address List

S.No	IP Address	Blocked By	Block Date	Delete
1.	192.1.168.1	Shubham Sinha	2019-03-24 11:47:32	Delete
2.	127.0.0.1	Shubham Sinha	2019-03-24 11:42:57	Delete

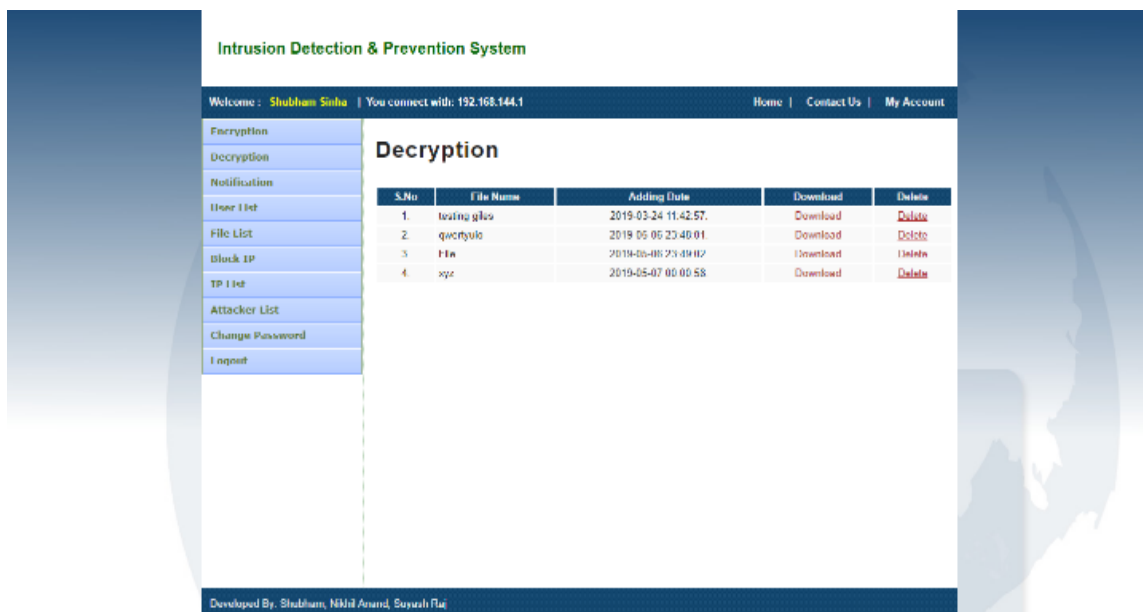
Developed By: Shubham, Nikhil Anand, Suyash Raj

- **Prevention** – The prevention module in the application is actually a firewall, it allows user to set rules for the host operating system. User can create rules such as TCP port 23 block, this rule blocks the port 23, any application on this port will not be able to communicate further,

application can only be able to communicate if the administrator deletes the rule using the unblock feature provided in the application.



- **Logging** - Intrusion Detection & Prevention System creates log file for the information captures while application is running. This log is stored locally in C:/Temp folder. The format of the file is normal text so that user can easily read the captured information. The name of the log file is given automatically by the application, it uses time and date as a file name, this way of naming allows administrator to identify particular log file according to the date.



- **Remote logging** - Intrusion Detection & Prevention System also have additional feature for storing the log on remote server. This module in application allows application to store the captured information on remote SQL database in MySQL server. The information stored in MySQL is in the form of document. The main advantage of using MySQL is its scalability, the MySQL is highly scalable, and it can easily handle large amount of data sets. Application does not need to use local storage to store the log files. Storing captured information on Mongo Server also enable advanced feature of extra back of files, administrator can easily all files from the Mongo Server.

- **Honeypot Plus** – This module in Intrusion Detection & Prevention System with Honeypot Plus application allows the administrator to host the fake FTP or IRC server on the hot operating system. This server will be running in virtual machine but pretends and behave like an actual server, any client connected to this server can not able to make out that actually interacting with a fake system rather than actual system. This servers host only those services which are set by application programmer or the application administrator, so there is no chance that hacker can get into more information than provided. This module also displays the numbers of hackers connected with the honeypot.

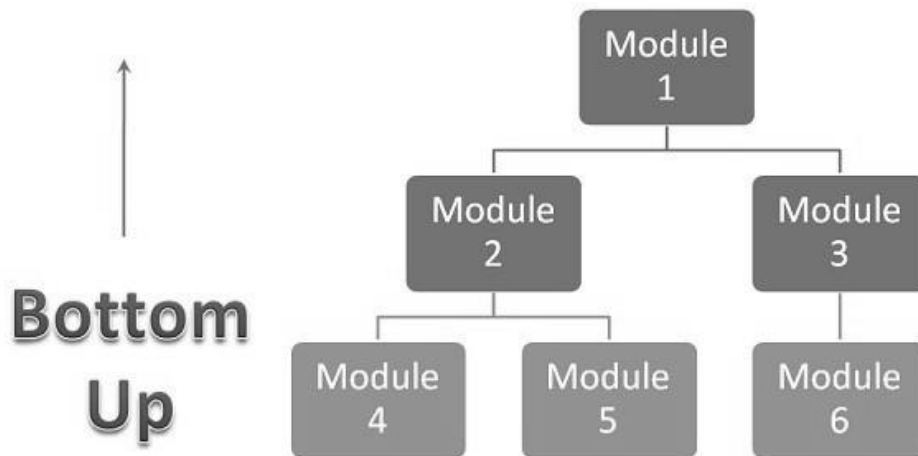
Result

Intrusion Detection & Prevention System is developed using incremental development approach, in which number of units is created, then units are integrated to create module and finally modules are combined to create the complete system. The various testing techniques has been employed to test the system.

- **Unit Testing** - Intrusion Detection & Prevention System is developed in small unites, this unit contains specific functionality for the overall system. The best example of unit is the function written for the button click. Here each unit is test as java console application in order to identify the proper output. Every unit is tested separately. This approach is taking in order to find the bugs hidden in the code at early stage and it also simplify the debugging process. Individual codes are tested before integration.

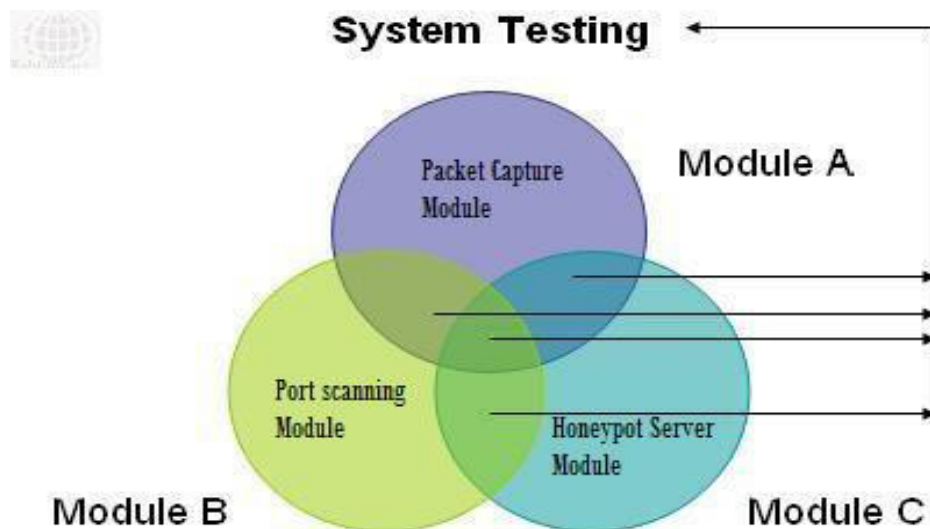
- **Integration Testing** – Every unit is combined to make a module; this module is collection of numbers of unites which works together to achieve specific functionality in the system. Intrusion Detection &

Prevention System is divided and developed in modules. Each module is tested separately. The best examples for modules in this system is capture module, save module and port scanning module. Here the bottom up approach is taken to perform integration testing, in this approach the development and testing is done together so that application will becomes efficient as per the requirements. The testing is done on each module once they are created without waiting for other modules to create



- **System Testing** – In this stage where all the modules are integrated to make the whole system. It is a final stage of testing where all functional and not-functional testing is done. All the module is interfaced to each other to make the complete system. The main idea behind this testing is to test the behavior of the whole application is to be tested as defined in scope and the requirement

specifications. It also clears how the system is interacting with the host operation system.



Bug Found

The current major bug in the system which is found while system testing is that system other components gets freeze when honeypot server component is executed, the execution of server freezes the system but this component keep running with updating contents on the application GUI, the only thing is other components stop updating and system goes into the freeze mode.

Conclusion

In conclusion, as we know that day by day network services are getting increased which increases number of servers and computing devices on the network to support the internet services. It is very important for any organization to protect and secured their servers from attackers and hackers. Intrusion Detection & Prevention System is the most common approach to protect network resources. Intrusion Detection & Prevention Systems are used worldwide by network administrators to monitor network traffic in order to find out unauthorized activity on their network. It is also important to improve the prevention mechanism in order to make system as well as network more protective. Firewall feature must be improving to deal with new and latest type of threads.

We also know that today because of technology advancement the network connections are encrypted, and the encryption mechanisms are increasing time to time. The Intrusion Detection & Prevention Systems are unable to monitor such encrypted connections, to overcome this problem Honeypot comes to help, they can be taken as alternative to Intrusion Detection & Prevention System to locate the source of malicious and unauthorized traffic to network.

Intrusion Detection & Prevention are the new approach to the network security and are advancing in the field of network security.

The final software product of this project is the combination of three different network security tool in order to improve the network security at the highest level. The outcome of this project demonstrates that it is possible to combine various functionalities, architectures and concepts of network security to develop an application which provides maximum functionalities to network security domain.

Intrusion Detection & Prevention System is the tool which provides features of packet inspection, control over the network traffic and spying subsystems, which can collect the information about the hackers allowing network administrators to protect network in more advanced ways.

References

- [1] <https://www.youtube.com/watch?v=Uump9bPIER8>
- [2] <http://www.cs.wustl.edu/~jain/cse571-09/ftp/honey/#sec1.1>
- [3] <http://www.techopedia.com/definition/10278/honeypot>
- [4] <http://www.cs.wustl.edu/~jain/cse571-09/ftp/honey.pdf>
- [5] http://www.academia.edu/1275290/JPCAP_WINPCAP_USED_FOR_NETWORK_INTRUSION_DETECTION_SYSTEM
- [6] <http://jnetpcap.com/>
- [7] Honeypot Definition - PC Magazine. pcmag.com. 24 March 2009.
http://www.pcmag.com/encyclopedia_term/0,2542,t=honeypot&i=44335,00.asp
PC Magazine's encyclopedia entry for honeypot.
- [8] Talabis Ryan. "Honeypots 101: A Honeypot by Any Other Name." 2007.
A non-technical introduction to honeypots. Provides helpful analogies for understanding the way honeypots work
- [9] <http://searchmidmarketsecurity.techtarget.com/definition/intrusion-detection>
- [10] http://www.sans.org/security-resources/idfaq/what_is_id.php
- [11] <https://docs.oracle.com/javase/7/docs/api/java/lang/Runtime.html>
- [12] http://www.tutorialspoint.com/java/lang/runtime_exec.htm
- [13] <http://www.rgagnon.com/javadetails/java-0014.html>
- [14] [http://en.wikipedia.org/wiki/Honeypot_\(computing\)](http://en.wikipedia.org/wiki/Honeypot_(computing))
- [15] <http://searchsecurity.techtarget.com/definition/honey-pot>
- [16] <http://www.cs.wustl.edu/~jain/cse571-09/ftp/honey.pdf>
- [17] <http://en.wikipedia.org/wiki/MySQL>
- [18] <http://www.tcpdump.org/papers/bpf-usenix93.pdf>
- [19] "http://www.tcpdump.org/wpcap.html"