**A PROJECT REPORT**

On

**Host Based Intrusion Detection System**

*A Project Report Submitted for partial fulfillment of the Requirements for the award of the Degree of*

**Bachelor of Computer Application**

*In*

**Cloud Technology and Information Security**

*Under*

**Assam Down Town University**



**SUBMITTED BY**

**Himjyoti Talukdar**

**Registration No: ADTU/2020-23/BCA/054**

**Nitish Kumar Sarma**

**Registration No: ADTU/2020-23/BCA/022**

**Debashish Bordoloi**

**Registration No: ADTU/2020-23/BCA/007**

**Under the Guidance of**

**Mr. Kandarpa Kalita**

*Assistant Professor*

**Faculty of Computer Technology**

**Department of Computer Technology**

**Assam Downtown University**

**Panikhaiti, Guwahati- 781026**

**A PROJECT REPORT**

On

**Host Based Intrusion Detection System**

*A Project Report Submitted for partial fulfillment of the Requirements for the award of the Degree of*

**Bachelor of Computer Application**

*In*

**Cloud Technology and Information Security**

*Under*

**Assam Down Town University**



**SUBMITTED BY**

**Himjyoti Talukdar**

**Registration No: ADTU/2020-23/BCA/054**

**Nitish Kumar Sarma**

**Registration No: ADTU/2020-23/BCA/022**

**Debashish Bordoloi**

**Registration No: ADTU/2020-23/BCA/007**

**Under the Guidance of**

**Mr. Kandarpa Kalita**

*Assistant Professor*

**Faculty of Computer Technology**

**Department of Computer Technology**

**Assam Downtown University**

**Panikhaiti, Guwahati- 781026**

**CERTIFICATE OF APPROVAL**

This is to certify that the project report entitled **“Host Based Intrusion Detection System”** submitted by **“Himjyoti Talukdar, Nitish Kumar Sarma, Debashish Bordoloi”** Registration No. ADTU/2020-23/BCA/054, ADTU/2020-23/BCA/022, ADTU/2020-23/BCA/007 is hereby accorded our approval as a study carried out in a manner required for acceptance in partial fulfillment for the award of the degree of Bachelor of Computer Application in Cloud Technology and Information Security under Assam Down Town University for approval does not necessarily endorse or accept every statement made opinion expressed or conclusion drawn as recorded in the report. It only signifies the acceptance of the project report for a purpose that is submitted.

DATE:

PLACE: Guwahati, Assam

……………………………..

**Dr. Utpal Barman**

Dean Faculty of Engineering & Technology

**CERTIFICATE FROM GUIDE**

This is to certify that the project report entitled **"Host Based Intrusion Detection System"** was submitted by **"Himjyoti Talukdar, Nitish Kumar Sarma, Debashish Bordoloi"** and Registration No.ADTU/2020-23/BCA/054,ADTU/2020-23/BCA/022,ADTU/2020-23/BCA/007, towards the partial fulfillment of the requirements for the award of the degree of Bachelor of Computer Application in Cloud Technology and Information Security under Assam down town University is a bonafide research work carried out by him under my supervision and guidance. This work has not been submitted previously for any other degree at this or any other University. I recommend that the thesis may be placed before the examiners for consideration of award of the degree of this University.

Date:

Place: Guwahati,Assam

…………………………

**Mr. Kandarpa Kalita**

Assistant Professor

Faculty of Engineering and Technology

**CERTIFICATE FROM EXTERNAL EXAMINER**

This is to certify that the project report entitled **"Host Based Intrusion Detection System"** submitted by **"Himjyoti Talukdar, Nitish Kumar Sarma, Debashish Bordoloi"** and registration no. ADTU/2020-23/BCA/054, ADTU/2020-23/BCA/022, ADTU/2020-23/BCA/007 towards the partial fulfillment of the requirements for the award of the degree of bachelor of computer application in cloud technology and information security under Assam Downtown University is a bonafide research work carried out by him under the supervision and guidance of **Mr. Kandarpa Kalita**, assistant professor, has been examined by me and found to be satisfactory. I recommendthe thesis for consideration for the award of the degree of bachelor of computer application in cloud technology and information security at Assam Downtown University.

Date

Place: Guwahati,Assam

……………………

**External Examiner**

**DECLARATION**

We, **“Himjyoti Talukdar, Nitish Kumar Sarma, Debashish Bordoloi"** and Registration No. ADTU/2020-23/BCA/054, ADTU/2020-23/BCA/022, ADTU/2020-23/BCA/007, hereby declare that the present thesis entitled **"Host Based Intrusion Detection System"** is an original work carried out in the Department of Computer Science and Engineering, Assam Downtown University. Guwahati with exception of guidance and suggestions received from my supervisor, **Mr. Kandarpa Kalita** Assistant Professor. Department of Computer Science and Engineering. Assam Downtown University, Guwahati, The data and the findings discussed in the thesis are the outcomes of my research work. This thesis is being submitted to Assam downtown University for the degree of Bachelor of Computer Application in Cloud Technology and Information Security.

Date:

Place: Guwahati, Assam **Himjyoti Talukdar**

(ADTU/2020-23/BCA/054)

BCA (CTIS) 6th Semester

**Nitish Kumar Sarma**

(ADTU/2020-23/BCA/022)

BCA (CTIS) 6th Semester

**Debashish Bordoloi**

(ADTU/2020-23/BCA/007)

BCA (CTIS) 6th Semester

**ACKNOWLEDGEMENT**

I would like to express our deep sense of gratitude and respect to our Sir, Mr. Kandarpa kalita, Assistant Professor, Department of Computer Science and Engineering, Assam Downtown University, Guwahati for guiding us immensely through the course of the project. Sir always helped me. His constructive advice and constant motivation have been responsible for the successful completion of the project. I would like to express our sincere thanks to the authorities of Assam Downtown University and both teaching and nonteaching staff of the Department of Computer Science & Engineering to allow us to carry out experiments in the department's laboratory, and also their outstanding support in completing this project work.

**Himjyoti Talukdar**

(ADTU/2020-23/BCA/054)

BCA (CTIS) 6th Semester

**Nitish Kumar Sarma**

(ADTU/2020-23/BCA/022)

BCA (CTIS) 6th Semester

**Debashish Bordoloi**

(ADTU/2020-23/BCA/007)

BCA (CTIS) 6th Semester

**ABSTRACT**

Intrusion Detection Systems (IDS) are vital tools for identifying and combating security breaches in computer systems and networks. This article focuses on the importance of IDS in detecting potential intrusions and notifying system administrators [1]. The main goal of IDS is to protect systems from viruses and unauthorized access. There are two types of IDS: network IDS and host IDS. As network attacks become more widespread and sophisticated, IDS has shifted its focus from hosts and operating systems to the network itself. However, network intrusion detection presents challenges due to the large volume of data generated during a network audit and the dispersion of events related to a single intrusion in the network [2].To solve these problems, this article presents a simple approach using the Python programming language and relevant frameworks. Python's flexibility and extensive libraries make it an ideal choice for developing an effective IDS. Python provides powerful data analysis and network packet processing tools that are essential for intrusion detection. By leveraging frameworks such as Scapy for packet manipulation. In conclusion, this article proposes a concise and practical approach to IDS development using Python and relevant frameworks. By leveraging Python's intuitive syntax and powerful capabilities, system administrators and security professionals can improve their ability to detect and effectively respond to network intrusions. The use of the Python programming language and frameworks streamlines the development process and enables the integration of advanced techniques such as machine learning algorithms to improve the accuracy and efficiency of intrusion detection. This approach serves as a valuable resource for security professionals looking to strengthen their defenses against evolving network threat.

**CONTENTS**

| ● | CERTIFICATE OF APPROVAL | i |
| --- | --- | --- |
| ● | CERTIFICATE FROM GUIDE | ii |
| ● | CERTIFICATE FROM EXTERNAL EXAMINER | iii |
| ● | DECLARATION | iv |
| ● | ACKNOWLEDGEMENT | v |
| ● | ABSTRACT | vi |
| ● | LIST OF FIGURES | vii |
| ● | LIST OF ABBREVIATIONS | viii |

1. **Introduction…………………………………………………………………..**13-16 1.1. Overview

1.2. Background Study

1.3. Motivation

1.4. Scope

1. **Project Analysis……………………………………………………………….**17-19 2.1. Project Requirements Analysis

2.2. Gantt Chart

2.3. Advantage & Disadvantage

1. **Project Design…………………………………………………………………**20-22 3.1. Implementation

3.2. Detecting brute force in SSH

3.3. Packet Capture

3.4. Packet Analysis

3.5. Rule Matching

3.6. Alert Generation and Response

1. **Project Implementation……………………………………………………**23-24

4.1. Tools and Technologies

4.2. Libraries / Frameworks

1. **Testing and Result…………………………………………………………...**25-26 5.1. Resources for Testing

5.2. Test Cases

1. **Conclusion & Future Scope**……………………………………………....…….27
2. **References…………………………………………………………………….….**28

**LIST OF FIGURES**

| **Chapter** |  | **Figure Description** | | | **Figure Number** | **Page** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
| 3 |  | High-level overview of how | | | 3.1.1 | 18 |
|  |  | Scapy can be used as a part of | | |  |  |
|  |  | Intrusion Detection System | | |  |  |
|  |  |  |  |  |  |  |
| 5 |  | Running the software from the | | | 5.2.1 | 21 |
|  |  | terminal | | |  |  |
|  |  |  |  |  |  |  |
| 5 |  | Launching attack from attacker | | | 5.2.2 | 21 |
|  |  | machine | | |  |  |
|  |  |  |  | |  |  |
| 5 |  | Login for the dashboard view | |  | 5.2.3 | 21 |
|  |  |  | | |  |  |
| 5 |  | Main dashboard alerts view |  | | 5.2.4 | 22 |
|  |  |  |  |  |  |  |

**LIST OF ABBREVIATIONS**

| IDS | - | Intrusion Detection System |
| --- | --- | --- |
| VPS | - | Virtual Private Server |
| IP | - | Internet Protocol |
| HIDS | - | Host-based Intrusion Detection System |
| NIDS | - | Network-based Intrusion Detection System |
| DOS | - | Denial-of-service |
| SSH | - | Secure shell |

**Chapter-I**

**Introduction**

**1.1. OVERVIEW**

Computer security has become a priority with Intrusion Detection Systems (IDS) due to the widespread usage of computer systems.The internet's rapid expansion and usage creates issues about how to properly transmit and safeguard digital information.The original type of IDS is HIDS (Host Based IDS), and its primary role is internal monitoring (inside a computer or machine), however several varieties of HIDS have emerged that may be used to monitor networks[3].Because it is impossible to construct a safe system without flaws, intrusion detection systems will become a critical topic of research in the near future. Intrusion detection is a relatively new addition to the security technology arsenal. Intrusion-detection systems are designed to identify assaults on computer systems and networks, as well as information systems in general.It is really challenging to establish provably secure information systems and to keep them secure throughout their lifetime and use. Legacy or operational restrictions may prevent the definition of a truly secure information system. As a result, intrusion-detection systems must monitor the use of such technologies to identify the appearance of unsafe states[4].The programme identifies both attempted and active misuse by legitimate users and other parties misusing privileges or exploiting security flaws.Firewalls and spam filters often utilize basic rules-based algorithms to allow or deny protocols, ports, or IP addresses. The disadvantage of these firewalls and filters is that they are often unable to manage complicated DoS (denial of service) assaults, and they are also unable of distinguishing between 'good traffic' and 'bad traffic[5].A Host Based Intrusion Detection System (HIDS) is installed on a single computer or server, known as the host, and monitors just that system's activity. The operation of intrusion detection systems is closely tied to firewall technique. It is built around firewall security. The firewall protects the organization from dangerous web-based assaults. If a malicious user attempts to breach the firewall security and get access to any system inside the organization, the ids is generated and the system administrator is notified.

**1.2. BACKGROUND STUDY**

Primarily there are two types of intrusion detection systems. These are network based intrusion detection system and host based intrusion detection system. Classifications where made on the basis of medium or method of intrusion Commonly there are two kinds of IDS that exists, namely :

1. **Network based intrusion detection system (NIDS):** Network-based attacks have become common and sophisticated. For this reason, intrusion detection systems are now shifting their focus from the hosts and their operating systems to the network itself[6**].** A Network-Based Intrusion Detection System (NIDS) is a type of intrusion detection system that monitors network traffic to detect and respond to potential security breaches. It focuses on analyzing the packets and flows of network data passing through specific network segments or devices.
2. **Host based intrusion detection system (HIDS):** The Host-Based Intrusion Detection System (HIDS) monitors the activities and events occurring on the individual host system. HIDS protects only the host system on which it resides, and its network card operates in non promiscuous mode[7].It operates at the host level, analyzing system logs, file integrity, and other host-specific data to detect potential security breaches. Traditionally, these IDS systems make the most and make use of the signatures of known attacks to identify the inbound attacks[8]

**1.3. MOTIVATION**

Till date a lot of work has been done in the field of security but still there is a lot of scope for its improvement. No system with 100% security has been designed, there are some security flaws in every system added by all the attacks and intrusion attempts are not yet known. A host-based IDS focuses on the individual host or endpoint level, allowing for targeted detection and protection against attacks that may bypass network-based security measures. By monitoring and analyzing the activities and behavior of a specific host, it can identify and respond to threats in real-time, helping to prevent potential breaches and data compromises Host-based IDS can be particularly useful in detecting insider threats, where malicious activities are carried out by authorized users within the network. By monitoring host-level activities, it can identify unauthorized access attempts, suspicious behavior, data exfiltration, or other indicators of internal abuse or compromise. Certain industries, such as healthcare, finance, and government, have stringent regulatory compliance requirements. Host-based IDS can help meet these requirements by providing continuous monitoring and audit capabilities. It enables organizations to demonstrate compliance by detecting and responding to security incidents promptly and effectively. For small businesses with limited resources and technical expertise, implementing a less sophisticated but still effective Intrusion Detection System (IDS) can provide valuable security insights. An open source IDS can be a cost-effective choice. basic network-based intrusion detection capabilities and can be deployed on a dedicated server or a network gateway to monitor network traffic for suspicious activities and known attack patterns will help individuals and small organizations to monitor and detect possible threats.The purpose of this paper is to demonstrate a method for detecting open ports and scanning them for any malicious network activities. It may help in developing a low cost and less sophisticated Host Based Intrusion Detection System to monitor networks on a particular host in which the system is installed.

**1.4. SCOPE**

The scope of a Host-based Intrusion Detection System (HIDS) for network monitoring primarily focuses on monitoring and protecting individual hosts or endpoints within a network environment. While network-based IDS systems primarily analyze network traffic, HIDS operates at the host level, providing granular visibility and protection for specific devices.As the attack disturbs the host being monitored, HIDS recognizes unidentified assaults more than network based IDS[9].HIDS can identify suspicious activities originating from within the system, including unauthorized access attempts, privilege escalation, or abnormal behavior by privileged users.It can identify malicious software, such as malware or ransomware, and alert administrators before significant damage occurs.Here are the key aspects of HIDS within the scope of network monitoring:

* **ENDPOINT PROTECTION:** HIDS focuses on monitoring and safeguarding individual endpoints, such as servers, workstations, laptops, and other network-connected devices.It aims to detect and prevent intrusions, malware infections, unauthorized access, and other security incidents targeting these specific hosts.
* **THREAT DETECTION:** HIDS employs various techniques to detect threats and security incidents. It utilizes signature-based detection, anomaly detection, behavior analysis, and heuristic algorithms to identify known attack patterns, deviations from normal behavior, and potential indicators of compromise. It provides alerts or triggers responses when suspicious activities or malicious events are detected.
* **INCIDENT RESPONSE SUPPORT:** HIDS plays a vital role in incident response by providing real-time alerts and actionable information when a security incident occurs. It assists security teams in identifying the source of the incident, understanding the extent of the compromise, and facilitating effective incident containment, eradication, and recovery.

**Chapter – II**

**Project Analysis**

**2.1. PROJECT REQUIREMENTS ANALYSIS**

The purpose of this project is to develop a light-weight and less sophisticated host-based Intrusion Detection System (IDS). The IDS will be designed to monitor and detect unauthorized activities and potential security threats on individual hosts or endpoints within a network. Unlike traditional IDS solutions, this system aims to be resource-efficient and suitable for deployment on low-specification systems with limited processing power and memory.

* **LIGHTWEIGHT**: The IDS should have minimal impact on system performance, requiring low CPU and memory usage. It should be optimized for efficient resource utilization, allowing it to run effectively on low-end hardware.
* **SIMPLICITY**: The system should be easy to deploy, configure, and maintain. It should not require advanced technical knowledge for setup and operation.
* **HOST-BASED MONITORING**: The IDS should focus on monitoring and analyzing events and activities occurring on individual hosts or endpoints, rather than network-wide traffic analysis

2.2. **GANTT CHART**



**2.3. ADVANTAGE & DISADVANTAGE**

**ADVANTAGES OF HOST-BASED IDS:**

1. **GRANULAR VISIBILITY**: Host-based IDS provides detailed visibility into activities and events occurring on individual hosts or endpoints. It monitors system logs, file modifications, process executions, network connections, and user activities, allowing for comprehensive analysis and detection of potential threats.
2. **LOCALIZED DETECTION**: Host-based IDS focuses on the specific host it is deployed on, allowing it to detect intrusions and suspicious activities that may not be visible at the network level. It can identify threats that bypass network-based security measures, such as encrypted traffic or insider attacks.
3. **BEHAVIORAL ANALYSIS**: Host-based IDS can analyze the behavior of processes, applications, and users on a host to detect anomalies and suspicious patterns. By comparing current behavior against established baselines, it can identify deviations that may indicate unauthorized activities or malware infections.
4. **RAPID RESPONSE**: Since host-based IDS operates on the host itself, it can quickly respond to detected threats. It can trigger real-time alerts, initiate

containment measures, or execute response actions, minimizing the time

between detection and mitigation.

**DISADVANTAGES OF HOST-BASED IDS:**

1. **LIMITED NETWORK VISIBILITY**: Host-based IDS focuses solely on the activities occurring on the host it is installed on, which means it has limited visibility into network-wide traffic and activities. It may miss threats that are only detectable at the network level, such as distributed denial-of-service (DDoS) attacks or lateral movement by an attacker.
2. **RESOURCE OVERHEAD**: Depending on the implementation, host-based IDS can consume system resources, such as CPU and memory, especially if it performs deep packet inspection or real-time analysis. This overhead can potentially impact system performance, particularly on low-specification or resource-constrained hosts.
3. **ENDPOINT COVERAGE**: To provide comprehensive protection, host-based IDS needs to be deployed on each individual host or endpoint within a network. This can be challenging to manage and maintain, especially in large-scale environments with numerous endpoints.

**Chapter –III**

**Project Design**

**3.1. IMPLEMENTATION**

Implementing a complete Intrusion Detection System (IDS) solely with Scapy can be little challenging, as Scapy is primarily a packet manipulation library but it can be used to make an IDS that will surely monitor and detect network intrusions and achieve full IDS functionalities. However, utilizing Scapy for certain tasks, such as packet capture, packet analysis, and rule matching will help in developing a fully operated Intrusion detection system. Here's a high-level overview of how scapy can be used as a part of Intrusion Detection System:

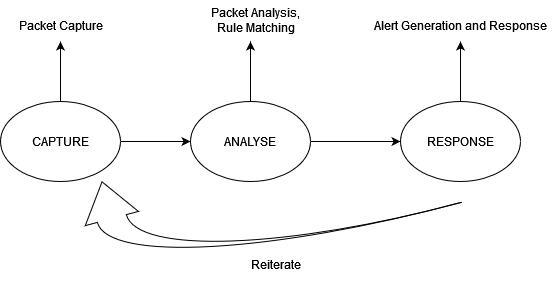


Fig.3.1.1

**3.2. DETECTING BRUTE FORCE IN SSH:**

We can leverage Scapy to analyze network traffic and look for patterns that indicate SSH brute force attempts. Here's an example of how you can use Scapy to detect SSH brute force attacks by monitoring network traffic. First we have implemented sniffing and then packet analysis after analyzing the detection function is executed.

**3.3. PACKET CAPTURE:**

By using Scapy's packet sniffing capabilities to capture network traffic.

Capture packets for detection -

if packet.haslayer(TCP) and packet.haslayer(Raw)

**3.4. PACKET ANALYSIS:**

Analyze captured packets using Scapy to extract relevant information, such as source and destination IP addresses, ports, protocols, and payload data. Perform analysis on packet headers and payloads to identify potential threats or suspicious patterns.

Check for port 22 or SSH

if tcp.dport == 22 or tcp.sport == 22:

payload = str(raw.load)

**3.5. RULE MATCHING:**

Implement rule-based pattern matching logic using Scapy to compare packet attributes against predefined signatures or rules that indicate malicious behavior. Define a set of rules or signatures that represent known attack patterns and trigger alerts or actions when a match is found.

Check for SSH Authentication Failure

if "SSH-2.0-" in payload and "failure" in payload:

src\_ip = packet[IP].src

Count the number of login attempts for each source IP define a threshold. If a threshold is reached, it can be considered a brute force attempt.

**3.6. ALERT GENERATION AND RESPONSE:**

Generate alerts or take appropriate actions when suspicious activity is detected. This can involve sending notifications, logging events, blocking traffic, or inciting incident response procedures.

**Chapter –IV**

**Project Implementation**

**4.1. TOOLS AND TECHNOLOGY**

There are numerous tools and technologies used in the process of software development. Here are the mostly used ones:

* System requirement : Any Linux distro with minimum 512 gb of RAM, Minimum 15 gb of storage and 1 vCPU.
* Offensive Tool : Hydra for brute forcing SSH on the system.
* Version Control Systems (VCS): Git
* Cloud Platforms: Amazon Web Services (AWS)
* Integrated Development Environments (IDEs): Visual Studio Code.
* Programming Languages: Common programming languages and markup languages used in software development include - Python, JavaScript, Shell, HTML and CSS.

**4.2. LIBRARY / FRAMEWORK**

* *Flask* - Flask is a micro web framework written in Python. It is classified as a microframework because it does not require particular tools or libraries. It has no database abstraction layer, form validation, or any other components where pre-existing third-party libraries provide common functions.
* *Werkzeug* - Werkzeug is a comprehensive WSGI web application library. It began as a simple collection of various utilities for WSGI applications and has become one of the most advanced WSGI utility libraries.
* *Scapy* - Scapy is a packet manipulation tool for computer networks, originally written in Python by Philippe Biondi. It can forge or decode packets, send them on the wire, capture them, and match requests and replies.
* *Socket* - This module provides access to the BSD *socket* interface. It is

available on all modern Unix systems, Windows, MacOS, and probably additional platforms.

**Chapter –V**

**Testing and Result**

**5.1. RESOURCES FOR TESTING**

For testing purposes we will need two virtual private servers (VPS). Python3 and important libraries should be installed in our system. And in the attacker VPS we have to install hydra for initiating the brute force attack on shh.

**5.2. TEST CASES**

For demonstration purposes we have created a small application with a dashboard console to monitor and analyze and to detect brute force in ssh which will show open ports, alert ports and source ip. We are testing the IDS on a virtual private server and the attack has also been conducted by another virtual private server.



Fig 5.2.1

We have created a python flask application and installed all requirements for the application with networking and server library which includes : scapy and flask. (Note : We have to navigate to the server’s IP address and dedicated port for running the application i.e. “[http://IP:port](about:blank)”)

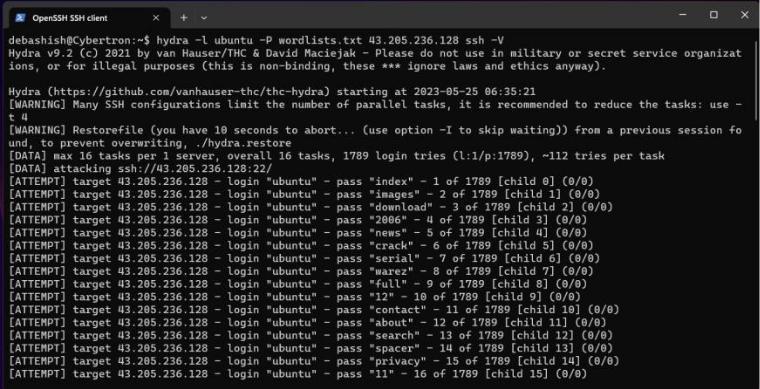


Fig 5.2.2

For testing we have conducted a brute force attack on port 22 which is SSH from another system as an Attacker System.

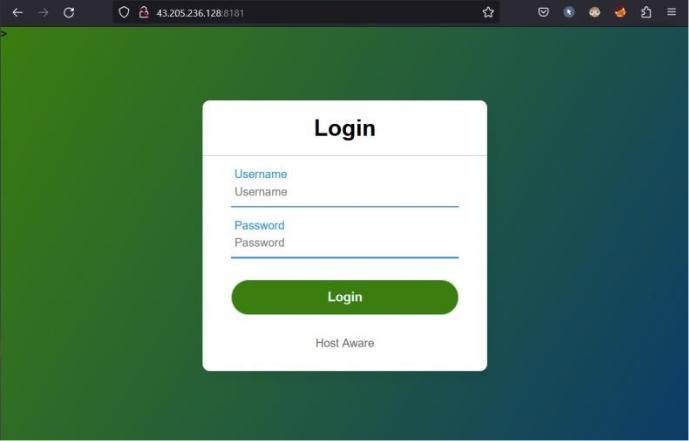


Fig 5.2.3

After running the application and navigating to the url and entering the user and pass which is user:admin and pass:admin.

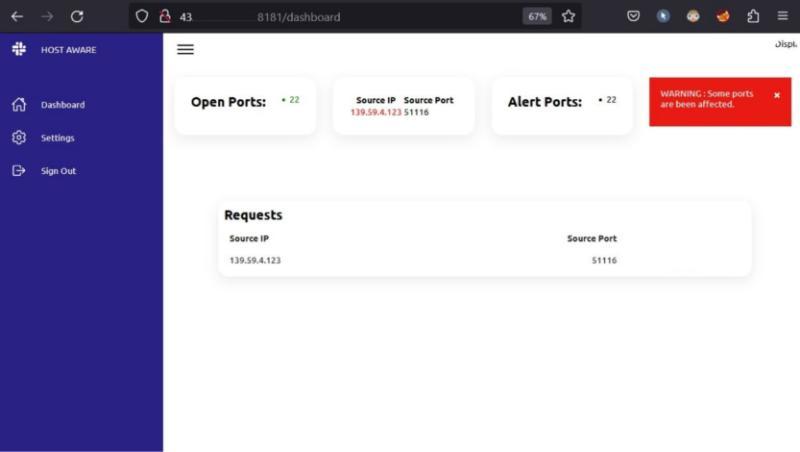


Fig 5.2.4

On the dashboard we are able to see Open Ports, Source IP, Source Port and alert Ports.

The alert box on the upper right corner has notified us that port 22 might have been attacked.

Hence we are able to get alerts for ports that may get attacked or being poked.

**Chapter –VI**

**Conclusion & Future Scope**

In conclusion, the development and implementation of a host-based Intrusion Detection System (IDS) have significant implications for enhancing the security of computer systems. Throughout this research, we have explored the various aspects of host-based IDS, including its fundamentals, techniques, implementation, and benefits. By creating a custom host-based IDS system, we can have the potential to achieve a tailored and effective security solution for organizations. Our research has highlighted the benefits of utilizing rule-based pattern matching logic for host-based IDS systems, enabling the detection of potential intrusions, insider threats and abnormal behaviors.

Integration with Threat Intelligence Platforms: HIDS can benefit from integration with threat intelligence platforms to leverage up-to-date information about known threats, vulnerabilities, and indicators of compromise (IOCs). By continuously receiving and analyzing threat intelligence feeds, HIDS can proactively detect and respond to emerging threats. Improved visualization and reporting capabilities can aid security analysts in understanding and responding to detected threats more efficiently. Future HIDS solutions may provide intuitive visualizations, advanced analytics, and customizable reporting options, allowing analysts to gain fun ctionability.

**Chapter –VII**

**REFERENCES**

[1]Vokoroks,L., and A. Baláž. "Host-based intrusion detection system." *2010 IEEE 14th International Conference on Intelligent Engineering Systems*. IEEE, 2010.

1. NetSTAT: a network-based intrusion detection approach (G. Vigna; R.A. Kemmerer. Reliable Software Group, Department of Computer Science, University of California,슠Santa Barbara, USA.)
2. Analysis of Host-Based and Network-Based Intrusion Detection System (Amrit Pal Singh Assistant Professor, GTBIT, GGSIPU, New-Delhi, India Email: amritpal.ipu@gmail.com Manik Deep Singh GTBIT, GGSIPU, New-Delhi)
3. Research Trends in Network-Based Intrusion Detection Systems: A Review (Satish Kumar; Sunanda Gupta; Sakshi Arora)
4. An Introduction to Intrusion-Detection Systems(**Hervé Debar** Télécom SudParis - Institut Mines-Télécom)
5. NetSTAT: a network-based intrusion detection approach (G. Vigna; R.A. Kemmerer)
6. [Ninja](https://www.sciencedirect.com/science/book/9781597495882) Hacking(Unconventional Penetration Testing Tactics and Techniques 2011, Pages 119-134) Thomas Wilhelm, Jason Andress
7. INTRUSION DETECTION SYSTEM (Ambermani Pratap Singh Vanishree K. Dept. of ISE Assistant Professor Dept. of ISE RV College of Engineering RV College of Engineering Bangalore, Karnataka, India Bangalore,Karnataka)
8. Analysis on HIDS and the Network-Based Intrusion Detection Approach (NIDS) (Sheetal Munjal\*, Ramesh Kumar, in Journal of Advances and Scholarly Researches in Allied Education | Multidisciplinary Academic Research).