SYNOPSIS ON

"HOST-BASED INTRUSION DETECTION SYSTEM"

Assam Downtown University
Session: 2020-2023

Submitted By -
HIMJYOTI TALUKDAR
NITISH KUMAR SARMA
DEBASHISH BORDOLOI
Bachelor of Computer Application(CTIS)

Under the guidance of
MR. KANDARPA KALITA
Assistant Professor
Department of COMPUTER & TECHNOLOGY
Assam Down Town University

1. **Name** : Himjyoti Talukdar
   Roll No : ADTU/2020-23/BCA/054
   Email : himzyotitalukdar@gmail.com
   Telephone : 6000292834
2. **Name** : Nitish Kumar Sarma
   Roll No : ADTU/2020-23/BCA/022
   Email : nitishsarma8@gmail.com
   Telephone : 9365627698
3. **Name** : Debashish Bordoloi
   Roll No : ADTU/2020-23/BCA/007
   Email : webshack2018@gmail.com
   Telephone : 9365882910

Course : BCA (CTIS)
Semester : 6th
Department : Engineering and Technology

Batch : 2020-2023
Guide's Name : Mr. Kandarpa Kalita
Designation : Asst. Professor

Introduction

Using computer systems in all over the world has made computer security an international priority with Intrusion Detection Systems (IDS). Outstanding growth and usage of internet raises concerns about how to communicate and protect the digital information safely. It is not feasible to build a secure system without vulnerabilities, so intrusion detection system becomes a vital and essential area of research in the near future. Intrusion detection is a relatively new addition to set of security technologies. Intrusion-detection systems aim at detecting attacks against computer systems and networks or, in general, against information systems. Indeed, it is difficult to provide provably secure information systems and to maintain them in such a secure state during their lifetime and utilization. Sometimes, legacy or operational constraints do not even allow the definition of a fully secure information system. Therefore, intrusion–detection systems have the task of monitoring the usage of such systems to detect any apparition of insecure states. They detect attempts and active misuse either by legitimate users of the information systems or by external parties to abuse their privileges or exploit security vulnerabilities. A Host Based Intrusion Detection System (HIDS) is placed on a particular computer or server, known as the host, and monitors activity only on that system.

Feasibility Study

Economic Feasibility -

Cost-Effective Solutions: The development of cost-effective IDS systems that can be deployed easily and quickly has made it possible for businesses and individuals to implement these systems without incurring significant expenses.

Technical Feasibility -

Software and hardware Requirements: An IDS system is a software that can collect and analyze network traffic, system logs, and other data sources. This includes algorithms, data storage and other technical stuffs that can accurately identify and classify intrusions. An IDS system requires hardware to process and analyze large volumes of data in real-time. This includes servers and other systems, but it would be able to run on any basic computer system.

Operational Feasibility -

User Acceptance: The system must be user-friendly and easily adopted by security personnel who will be responsible for operating and maintaining it.

System : The system must be seamlessly integrated with existing IT systems and network infrastructure to avoid disruption to normal operations.

Aim and Objective

- To develop a Host-based Intrusion Detection System (IDS) using simple logic.
- To make it liable for detecting malicious network activities in a host and notify them as an alert .
- To develop a dashboard console that will run locally on the host system for monitoring such attacks, threats and activities.
- To test for adequate and efficient results for proper functioning of the system.

Problem Statement

- Businesses operate online and store sensitive information in servers proper security and monitoring has to be done in a systematic way.
- Protecting these credentials is crucial to prevent digital attacks and loss.
- An IDS can monitor and detect abnormal patterns and unauthorized activities within the system.
- The idea is to develop an IDS to protect small scale servers and virtual private servers.
- The IDS will provide a dashboard console to display active attacks and attempts on the system in detail.
- The software will focus on identifying malicious activities encountered by small scale servers or virtual private servers.

Methodology

Define the System Requirements: Determine the goals and objectives of the host-based IDS system, including the specific types of attacks to be detected, the types of data sources to be monitored, and the desired response to detected intrusions.

Select the Detection Techniques: Determine the appropriate detection techniques, such as signature-based, anomaly-based, or behavioral-based, that will be used to identify intrusions in the host-based environment.

Collect and Analyze Data: Collect data from the host-based environment, including system logs, user activity logs, and network traffic logs. Analyze the data to identify patterns and anomalies that may indicate the presence of an intrusion.

Develop the IDS System: Use the selected detection techniques and analysis to develop the IDS system.

Testing and reporting : Test the detection techniques used by the IDS to ensure that they can identify and classify different types of intrusions accurately. Test the IDS's false positive rate to ensure that it does not generate too many false.

Expected outcome and Features

We will be able to develop a host based IDS as a web application software that will consist a dashboard console and will notify alerts if any malicious activity is detected.

- It may help systems to identify and protect from any further attacks that could possibly damage the system.
- It may analyze different types of attacks and will identify patterns of malicious requests and help the administrators to tune, organize and implement effective controls.
- It may help any administrators or organization to maintain regulatory compliance and meet security regulations as it provides greater visibility across their system.

Facilities required for proposed work

- For this project we will have to use a general purpose programming language such as python or perl for the main core system.
- We will have to use HTML and CSS for the dashboard console for displaying active ports and details of connection that are being monitored.
- We will have to use language libraries to make it work and access network related configuration and operating system internals.
- We will may have to use javascript and databases for some purposes.
- We will have to deploy it on any Virtual private server (VPS) such as Amazon Web Services or Microsoft Azure for testing purpose.

Bibliography

An Introduction to Intrusion-Detection Systems Herv´e Debar IBM Research, Zurich Research Laboratory, S¨aumerstrasse 4, CH–8803 R¨uschlikon, Switzerland deb@zurich.ibm.com

International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com, Volume 5, Issue 2 (March - April 2017), PP. 38-44 38 | P a g e INTRUSION DETECTION SYSTEM 1 Mr Mohit Tiwari, 2 Raj Kumar, 3Akash Bharti, 4Jai Kishan