NFSU JOURNAL OF
CYBER SECURITY &
DIGITAL FORENSICS

CSDF
Volume: 1, Issue: 1 July 2022
E-ISSN: In Process

Intrusion Detection System: A Review on ML Based Methods

[1]Sachin Sharma, [2]Vishwas Sharma, [3]Dharmesh Shah

[1]School of Cyber Security and Digital Forensics, National Forensics Sciences University, Gandhinagar, India

sachin.sharma@nfsu.ac.in

[2]Electronics and Communication Department, Sankalchand Patel University, Visnagar, India

vishwas.ece@gmail.com

[3]Electronics and Communication Department, Sankalchand Patel University, Visnagar, India

djshah99@gmail.com

***Abstract*—Intrusion Detection System (IDS) is a kind of an application software that screens the network and sees if there is any attack or malicious activity going on. Internet usage is increasing at an exponential rate, which raises questions regarding how to safeguard digital information. As cybercrime has increased over time, the IDS technology has evolved dramatically. Hackers today employ a variety of techniques to access our computer's personal, secure data. Numerous intrusiondetection approaches, tactics, and algorithms will serve as a defense against these threats. The primary aim of this manuscript is to give a thorough analysis about intrusion detection, different methodologies including machine learning based, tools and approaches, and implementation issues of it.**

***Keywords*— Machine learning (ML), Intrusion detection system (IDS), Threats, Performance. Life process, Algorithm**

I. INTRODUCTION

All harmful network traffic and computer activity that a traditional firewall is unable to identify can be detected by a smart IDS. Thiscovers malware, host-based attacks such as privilege escalation, illegal logins, and access to private information, network attacks on services that are vulnerable, data-driven assaults on apps, and host-based assaults against hosts. Usersrequire security to protect their systems from outside forces that are undesirable. One of the common security methods used to secure the network is the firewall technique. IDS are utilizedby insurance companies, medical applications, credit card fraud, and network-related activities. The following three components make up an IDS: Sensors: - which detect system activity or network traffic and produce events. Console: Used for sensor control and tracking of events, notifications. Detection engine: Works on conditions and rules for generating warnings from security events it has collected and keeps a database of events logged by the sensors. Depending on the kind of sensor, where it is located, how the engine generates alerts, and otherfactors, an IDS can be categorized in a number of different ways. All three elements are frequently bundled in a single device or appliance in straightforward IDS solutions.

II. INTRUSION DETECTION

Intrusion detection can be considered as a possible solution for preventing computers and networks if designed to check possible security gaps, such as intrusions (attacks from outside the institution) and abuse, an ID system gathers and evaluates data from several computer or network systems (attacks from within the institution). ID employs vulnerability assessment, a method created to evaluate overall protection of a computer or computer network (also known as scanning).

A. Intrusion detection system

IDS are indeed recognized as a door bell. For example, the locking mechanism in the residence helps protect this from stealing. Even so, when someone breaks the locking mechanism and tries to enter the cottage, the buzzer detects the violation and notifies the holder by sounding an alarm. Moreover, security systems are very good at screening inbound online traffic to avoid the security software [1]. External stakeholders, for example, can interact to the internal network by ringing through a router finished installing in the group's secure network; this type of access is not detected by the firewall [1]. Different categories of IDS are:

- Host based IDS
- Network based IDS
- Application based IDS

Fig 1 shows the different types of IDS.

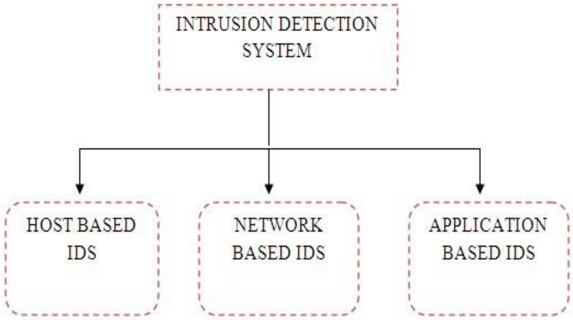


Fig 1. IDS types [1, 2]

B. *Intrusion detection attacks*

Denial-of-Service (DOS) Attack: This attack generally falls into two categories: flooding and flaw exploitation. Flooding attacks are frequently easy to execute. For instance, the ping command alone can be used to execute a DoS attack. A lot of ping packets will be sent to the victim as a result. Ifthe attacker is able to much more bandwidth than the target has, the target will be quickly and simply overwhelmed. A SYN flood attack is another illustration, in which a victim is barraged with TCP/SYN packets from a bogus source address [1, 4]. The victim must send a TCPSYN/ACK packet as well as wait for an Acknowledgement response in order to forcefully open partially closed TCP connections. The target will ultimately be out of resources and waiting for ACKs from an absent host because the ACK never arrives.

Eavesdropping Attack: Its communication will be obstructed by the attacker's scheme. Such an attack can be done over email or mobile.

Spoofing Attack: To generate data and benefit from illegal activities in the network, the attackerpretends as another user. One frequent example is IP spoofing, in which the system connects with a trustworthy user and thereby gains the access.

User to Root Attack or Intrusion Attack (U2R): A hacker attempts to access or penetrate the network. Data loss results from a well-known intrusion assault known as a "buffer overflow attack," that happens when web server gets added data compared to it is designed to manage.

Application-Level Attack: The application layer'slimitations are the attacker's focus.

C. *IDS functions*

Data gathering, feature selection, analysis, and action are the four main tasks that the IDS consist of as shown in figure 2.

Fig 2. IDS Functions [1]

D. *IDS techniques*

Anomaly based intrusion detection: These program, which are sometimes referred to as behavior-based ones, keep an eye on what happens within a predetermined area in search of instances of malevolent activity, at least according to their definition. This is quite a challenging work which occasionally gives false positives. Incoming URL of Internet activity, for instance, might be taken into account, and websites with domain specific names or URL lengths may dynamically be stopped, even when a person (not malware) is attempting to access the site and the user has a valid business reason [1].

Signature based intrusion detection: Misuse detection refers to intrusion detection that uses signatures. This strategy, often referred to as knowledge-based, includes probing for particular signatures, which are combinations, of byte which when they appear, nearly always indicate awful news. Due to the strict search restrictions, they give less false positives compared to anomaly solutions, but then again, they also only cover signatures which are present in the search file/record [1, 4]. The appropriate authorities should receive a reaction or notification to an alert dependent on significance and strength of a signature which is activated inside the system. Figure 3 illustrates how SIDS techniques function conceptually. For instance, a rule that reads "if: before to then: following could result in "if (source IP) classify the incident as an attack (address=destination IP address).

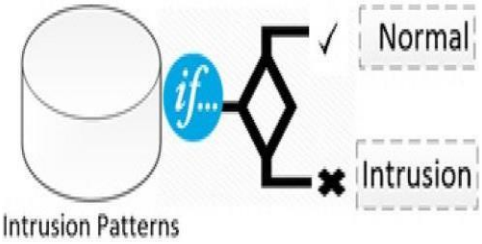


Fig 3. Signature based IDS [4]

E. *Intrusion detection tools*

A variety of organizational security objectives are addressed by an intrusion detection device now on the market. The topic of security tools is covered in this section.

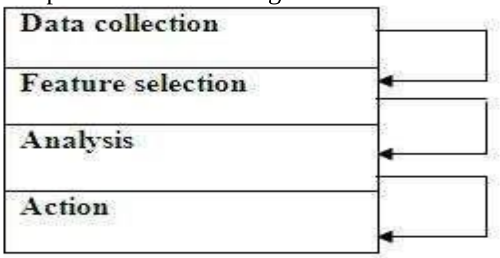
SNORT: It is a compact and open-source software. A rule-based syntax is used by Snort to describe the flow. It saves the message in readable form after obtaining an IP address. Snort may discover various types of worms, attempts to make use of vulnerabilities, scans of different ports, and various suspicious activity using protocol study and analysis, and a number of pre-processors [1].

Suricata: Among the IDS products now available on the market. This system uses signatures similar to Snort, has a similar design, and can even employ Snort's Emerging Threat rule set and VRT Snort rules. In the event that Snort is not a possibility for your firm, this is the closest free program that can be deployed on a business network.

OSSEC-HIDS: Open-source software that is free to use is called OSSEC. It utilizes a Client/Server design and is compatible with most major operating systems. The server can receive OS logs from OSSEC for analysis and storage. It is employed by ISPs, colleges.

OpenWIPS-NG: Free wireless IDS/IPS called OpenWIPS-NG is supported by a server, sensors, and interfaces. It is powered by common hardware. This solution, developed by the creator of Aircrack-NG, employs a lot of the features and services that are currently included in an administrator can download plug-ins for extra functions because OpenWIPS-NG is modular. Despite the less extensive documentation than that of some other systems, it nonetheless enables firms to implement WIPS on a tight budget.

FRAGROUTE: Fragmenting router is the name given to it. In this, the IP packet is sent to fragrouter from the attacker, where it is fragmented and changed before being sent to the party.



KISMET: It acts as a WIDS instruction (Wireless intrusion detection system). Packet payloads and WIDS actions are compromised by WIDS. It will identify a burglar's point of entry.

HONEYD: A utility called Honeyd is used to set up virtual hosts on a network. The host makes use of the services. In order to simulate networks, Honeyd enables a user host can request many addresses on a LAN. It is possible to track them or hit the virtual machines as they move.

BRO Ids: In that it employs methods other than IDS rules to identify the origin of attacks, Bro IDS is comparable to Security Onion. Bro IDS use a variety of tools. It once employed Bro-based signatures that had been derived from Snort signatures. This is no longer the case, as the Bro IDS now supports writing custom signatures. This system has beenin use for more than 15 years and is well documented.

III. Literature Review

A variety of methodologies from various fields have been developed to create effective and efficient IDS. The popular methodologies for IDS creation include artificial intelligence (AI) based, statistical based techniques. The advantages of AI/ML based techniques is: flexibility, pattern recognition, fast computing and learning capabilities. During the training phase, ML approaches can automatically learn from data without explicit programming [4].

Figure 4 illustrates the overall process of a machine learning project. Any ML project's data management phase is its first stage. It gathers the data and uses it for the training and validation of the ML model as test and training data. In order to ensure data quality and compatibility with the ML model, the data management phase also employs data cleaning management techniques for 1) data cleaning to eliminate missing values and noisy data, and 2) data transformation to normalize data, choose pertinent features, and discretize features. The data is pre-processed, divided into training and test datasets, and loaded for the ML model's training and testing.

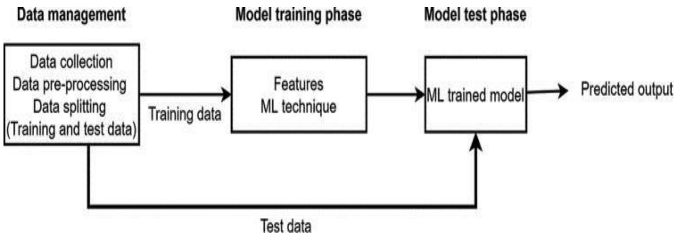


Fig 4: ML phases [3, 5]

Based on learning objectives like classification, regression, and clustering, a suitable ML model is selected. For the purpose of obtaining optimum parameters during the training phase, the training record or the data is provided to the AI/ML model [6, 7]. Then test dataset is used to evaluate the trained AI/ML by obtaining its predictions and contrasting them with the actual output. For checking how well the trained AI/ML model performed, confusion matrix is calculated whichincludes true positive, true negative, false positive and false negative parameters and from there we can calculate accuracy,precision, and recall. When the ML model's performance and validation metrics are satisfactory, it is used in a real-world setting to make predictions [2]. In order to update ML models with changing scenarios and achieve benchmark performance satisfaction, they are typically retrained using new trainingdata. Next section shows the different works carried out in past.

1. **Paper Title**: Enhanced intrusion detection system via agent clustering and classification based on outlier detection [8].
   Method: In this study, authors put forth the EIDS-ACCOD framework, which stands for Enhanced Intrusion Detection System employing Agent Clustering and Classification based on Outlier Detection.
   Outcome: Outlier identification is used in the primary step of pre-processing to remove unnecessary spaces. Then segmentation of data based on K-means clustering is developed. It classifies attacks using K- Nearest Neighbor (KNN).
   Limitation: Unfit for IDS in a highly complicated network.

2. **Paper Title:** Research on DoS Traffic Detection Model Based on Random Forest and Multilayer Perceptron [9]**.**
   Method: This study proposes a method for RF-MLP model that assesses traffic of the network, analyses it, and creates a prediction model which can precisely detect DoS assaults in network.
   Outcome: Used CICIDS2017 and UNSW-NB15 dataset to estimate the method in this manuscript. Accuracy was found around 99.83 percent and 93.51 percent, with quite a huge reduction in the false alarms. The results also suggest that the proposed system can efficiently detect and categorize DOS attacks.
   Limitation: Not suitable for real network environments.

3. **Paper Title**: The detection of low-rate DoS attacks using the SADBSCAN algorithm [10].
   Method: In order to detect whether a collection of network traffic comprises DoS assaults, they devised the SADBSCAN method, that groups the traffic of the network and uses cosine similarity.
   Outcome: Outcomes demonstrate that the method increases detection rate, lowers the number of false negatives, and is adaptable to large-scale complex network situations.

4. **Paper Title**: Detection of DoS/DDoS attacks: the UBM and GMM approach [11].
   Method: The UBM and GMM are powerful methods which can be applied in a varied range of situations, including the classification of security assaults in networking, where the data needed to create models and test algorithm is less expensive.
   Outcome: UBM and GMM techniques are used to demonstrate their potential in this basic problem, and novel applications were explored in more complicated situations.
   Limitation: We discovered that the model begins to exhibit over fitting with more Gaussians.The UBM technique's accuracy result may be due to its inability to adequately describe the phenomenon of the extracted features used to construct the UBM.

5. **Paper Title**: An efficient metaheuristic algorithm-based

feature selection and recurrent neural network forDoS attack detection in cloud computing environment [12].
Method: They combined the crow search algorithm (CSA) and objection-based learning (OBL) to create an opposing crow search algorithm (OCSA) DoS attack traffic detection system. This system selects features using the OCSA algorithm before passing a portion of the data to an RNN classifier.
Outcome: The proposed technique performs better than the other conventional methods by 94.12%, 98.18%, 93.56%, 95.13% in terms of accuracy, precision, f-measure and recall respectively. Additionally, based on an average of all the indicators, the suggested job performs 3 percent better than the competition.
Limitation: Unsuitable for use in cloud-based systems' Attack Prevention System implementation.

6. **Paper Title**: A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning [13].
Method: Built a modular system that trains IDS with the aid of six AI/ML based models, including support vector machines (SVM), random trees, MLP, REP trees, RF, and J48, and increases the detection rate of DoS.
Outcome: Despite the challenge of identifying LR-DoS attacks, the calculation shows that the technique attains a rate of detection of 95%. In addition to this in order to make the deployment as similar to actual production networks as feasible, they used the ONOS controller which was running on a virtual machine called Mininet.
Limitation: More deep learning techniques will eventually be included as they show promise in detecting LR-DDoS attacks.

IV. CONCLUSION

The main objective of this manuscript was to give a summary of IDS's necessity, the comprehensive study of IDS kinds, life cycles, various domains, attacks, and tools. IDS are becoming increasingly important for modern network user and corporate security. IPS outlines the security preventative measures. The lifecycle's phases and stages are represented. There are still more challenges to overcome. In addition to the methods specifically mentioned and demonstrated for anomaly and misuse detection, other methods can be used. Utilizing approaches for selective feedback, a classification-based IDS will be enhanced. Additionally, work will be done on a comparison of various widely used data mining algorithms used for IDS.