“INTRUSION DETECTION SYSTEM”

*A*

***Seminar***

*submitted*

*in partial fulfillment*

*for the award of the Degree of*

***Bachelor of Technology***

***in Department of Computer Science & Engineering***



Submitted To: Submitted By:

Harshita Khangraot Mahesh Mundel

Assistant Professor 18EJICS085

### Department of Computer Science & Engineering Jodhpur Institute of Engineering & Technology, Jodhpur

**June 2021-2022**

# DECLARATION

I hereby declare that the work, which is being presented in the Seminar, entitled **“Intrusion Detection System”** in partial fulfillment for the award of Degree of “Bachelor of Technology” in “Computer Science & Engineering” **and submitted to the Department of Computer Science & Engineering, Jodhpur Institute of Engineering & Technology** , Bikaner Technical University is a record of my own WORK carried under the Guidance of Ms Surbhi Upadhyay Department of Computer Science & Engineering,**.**

Mahesh Mundel 18EJICS085

Jodhpur Institute of Engineering and Technology

Counter signed by Guide : Surbhi Upadhyay

# ACKNOWLEDGEMENT

A seminar research is a golden opportunity for learning and self-development. Fortunately, the two were satisfied when I researched on **Intrusion Detection System**.I consider myself very lucky and honored to have many wonderful people lead me through in completion of the seminar.

This acknowledgement is intended to thank all those involved with me directly or indirectly. When expressed in words, Feeling of gratitude is partially conveyed. I could not have completed this report without the assistance of these people.

It is my glowing feeling to place on record my best regards, deepest sense of gratitude to **Mrs. Surbhi Upadhyay, Assistant Professor & Guide,** for their judicious and precious guidance which were extremely valuable for my study both theoretically and practically.

I would like to express my gratitude towards my parents whose blessings are always with me. Their lifetime support and encouragement has provided the basic foundation of any success I will ever achieve.

For omission of credit, regrets are expressed.

**ABSTRACT**

Intrusion Detection System (IDS) defined as a Device or software application which monitors the network or system activities and finds if there is any malicious activity occur. Outstanding growth and usage of internet raises concerns about how to communicate and protect the digital information safely. In today's world hackers use different types of attacks for getting the valuable information. Many of the intrusion detection techniques, methods and algorithms help to detect those several attacks. The main objective of this paper is to provide a complete study about the intrusion detection, types of intrusion detection methods, types of attacks, different tools and techniques, research needs, challenges and finally develop the IDS Tool for Research Purpose That tool are capable of detect and prevent the intrusion from the intruder.

# TABLE OF CONTENTS

### Candidate’s Declaration ii Acknowledgment iii Abstract iv

**Table of Contents v**

### Introduction 1

1. **Literature survey 2**

### Chapters Describing Work 5

1. **Chapter 1**

### Intruders & Intrusion Detection System 5

### Chapter -2

### Classification of IDS 7

### Chapter-3

### Snort IDS 9

### Conclusions 12

1. **References 13**
   1. **Introduction**

The evolution of malicious software (malware) poses a critical challenge to the design of intrusion detection systems (IDS). Malicious attacks have become more sophisticated and the foremost challenge is to identify unknown and obfuscated malware, as the malware authors use different evasion techniques for information concealing to prevent detection by an IDS. In addition, there has been an increase in security threats such as zero-day attacks designed to target internet users. Therefore, computer security has become essential as the use of information technology has become part of our daily lives. As a result, various countries such as Australia and the US have been significantly impacted by the zero-day attacks. According to the 2017 Symantec Internet Security Threat Report, more than three billion zero-day attacks were reported in 2016, and the volume and intensity of the zero-day attacks were substantially greater than previously (Symantec, [2017](https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7#ref-CR109)). As highlighted in the Data Breach Statistics in 2017, approximately nine billion data records were lost or stolen by hackers since 2013 (Breach\_LeveL\_Index, [2017](https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7#ref-CR21)). A Symantec report found that the number of security breach incidents is on the rise. In the past, cybercriminals primarily focused on bank customers, robbing bank accounts or stealing credit cards (Symantec, [2017](https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7#ref-CR109)). However, the new generation of malware has become more ambitious and is targeting the banks themselves, sometimes trying to take millions of dollars in one attack (Symantec, [2017](https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7#ref-CR109)). For that reason, the detection of zero-day attacks has become the highest priority.

## Literature Survey

SURVEY OF INTRUSION DETECTION BASED ON DIFFERENT TECHNIQUES

This section presents an extensive study over the various intrusion detection classifier techniques and other techniques. A number of research papers regarding to intrusion detection are discussed below and are widely classified into

1. papers related to Neural network
2. papers related to Support vector machine
3. papers related to K-means classifier
4. papers related to hybrid technique and
5. paper related to other detection techniques.

### Neural network based intrusion detection

A brief review of two techniques related with neural network based intrusion detection is discussed in this section. In 2009 a lot of papers have been presented to represent the neural network based intrusion detection. Some of the papers have been discussed below. The following approach was presented in the year 2009. The concept of anomaly detection and use both neural network (NN) and decision tree (DT) for intrusion detection has been improved by Marjan Bahrololum et al. [15]. At the same time DTs were extremely victorious in discovering known attacks, NNs were more exciting to detect unknown attacks. They designed the system using together with DT and mixture of unsupervised and supervised NN for Intrusion Detection System (IDS). Known attacks were familiar with a quick implementation time by concerning DT. For collecting attacks into smaller categories, unknown attacks was identified by pertaining the unsupervised neural network based on hybrid of Self Organizing Map (SOM) and supervised NN based on Back propagation for complete grouping.

### Support vector machine based intrusion detection

A brief review of support vector machine classifier related is discussed in this section. In the period 2007-2012, a lot of papers have been presented to represent the Support vector machine based intrusion detection. Some of the papers have been discussed below. A revise for improving the training time of SVM has been presented by Latifur Khan et al. [17], particularly when contracting with large data sets using hierarchical clustering analysis in 2007. For gathering, they utilized the Dynamically Growing Self-Organizing Tree (DGSOT) algorithm since it had verified to triumph over the disadvantages of traditional hierarchical clustering algorithms (e.g., hierarchical agglomerative

clustering). Among two classes, clustering analysis assisted discover the boundary points, which were the most capable data points to coach SVM. Using the clustering arrangement created by the DGSOT algorithm, they offered an approach of amalgamation of SVM and DGSOT, which in progress with a first training set and enlarge it slowly. In terms of precision loss and training time gain by means of a single bench-mark real data set they match up to their approach with the Rocchio Bundling technique and casual choice.

### K-means algorithm based intrusion detection

In this section, we discuss the different papers that utilize k-means algorithm. In 2003-2004 some papers presented to represent the K-means algorithm based intrusion detection. Some of the papers have been discussed below. In the year 2003, a K-means based clustering algorithm, named Y-means, for incursion detection has been offered by Yu Guan et al. [21]. Y-means surmounts two failings of K-means: quantity of clusters dependency and degeneracy. The original number of clusters was no longer serious to the collecting results in the Y-means algorithm. A suitable number of clusters were divided by a data set routinely. This was one of the benefits of the Y-means algorithm for intrusion detection. The unprocessed log data of information systems can directly be applied as training data with-out being physically labeled was the another advantage.

### Hybrid technique based intrusion detection

In the period 2007-2012, a lot of papers have been presented to represent the hybrid technique based intrusion detection. Some of the papers have been discussed below. For categorizing irregular and normal activities in a computer network, a dynamic electronic circuit, and a motorized mass-beam system, Shekhar R. Gaddam et al. [23] have offered a method to flow k-Means grouping and the ID3 decision tree learning methods and this paper has been published in the year 2007. By means of Euclidean distance resemblance the k-Means grouping method first divided the training cases into k clusters. On every cluster, an ID3 decision tree on behalf of a density region of normal or anomaly instances has been constructed. By studying the subgroups inside the cluster the decision tree on every cluster purified the decision boundaries. The conclusions of the k-Means and ID3 methods were united using two rules to get a concluding decision on classification. The two rules are: 1) the Nearest-neighbor rule and 2) the Nearest-consensus rule. Testing were executed by them on three data sets: 1) Network Anomaly Data (NAD), 2) Duffing Equation Data (DED), and 3) Mechanical System Data (MSD), which enclosed measurements from three

separate application domains of computer networks, an electronic circuit applying a forced Duffing Equation, and a mechanical system, correspondingly.

### Other classifier based intrusion detection

Here, we discuss about the different papers of various intrusion detection techniques. In the year 2003-2012 a lot of papers have been presented to represent the classifier based intrusion detection. Some of the papers have been discussed below. In the year 2003, a model recognition approach to set of connections intrusion detection based on the combination of manifold classifiers has been developed by Giorgio Giacinto et al. [29]. Five decision mixture methods were evaluated by experiments and their presentations were compared. The potentialities of classifier fusion for the improvement of competent incursion detection systems were assessed and argued. The statement results explained that the MCS approach offers an improved trade-off among generalization abilities and false alarm generation than that offered by an individual classifier educated on the general feature set.

## CHAPTER 1

**INTRUDERS AND INTRUSION DETECTION SYSTEM**

Intrusion is some time also called as hacker or cracker attempting to break into or misuse your system. While introducing the concept of intrusion detection in 1980, defined an intrusion attempt or a threat to be the potential possibility of a deliberate unauthorized attempt to

* access information,
* manipulate information, or
* Render a system unreliable or unusable.

Intrusion detection systems do exactly as the name suggests: they detect possible intrusions. More specifically, IDS tools aim to detect computer attacks and/or computer misuse, and to alert the proper individuals upon detection. An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. An IDS installed on a network provides much the same purpose as a burglar alarm system installed in a house. Through various methods, both detect when an intruder/attacker/burglar is present, and both subsequently issue some type of warning or alert.

Due to increase connectivity (more specially on internet),and much chances of financial possibility that are opening more and more system are subject to attack by intruders(intruders are the hacker or cracker those are unauthorised usres),because completely secure system is still a dream.

Firewall and filtering router are not enough to protect electronic assets.so detection is needed. In terms of the relation intruder-victim, attacks are categorized as: -

**External Intruders:** who are unauthorised usres of the machines they attack,they coming from outside, frequently via the Internet.they can be any person which are not in our knowledge.

**Internal Intruders:** who has permission to access system but not some portion of it, they coming from own enterprise’s employees or their business partners or customers. further subdivided: -

**Masquerade:** Those user who masquerade another user means using others usre no or identification no access the non permitted information.

**Legitimate:**Those user who legally access the information but they are not allowed to access information.but using some kind of techniques they able to access sensitive data legally.They are most dangerous type.

**Clandestine:**User who have power to turnoff audit control for them selves and steal information.

## CHAPTER 2 CLASSIFICATION OF IDS

Basically IDS are of two type’s i.e.

--NIDS (Network Intrusion Detection Systems)

--HIDS (Host Intrusion Detection Systems)

Both of them has their own prone and cons. Let us discuss both of them one by one.

### Network Intrusion Detection Systems

A network IDS (NIDS) monitors all traffic on the network segment that it is placed on. This is generally accomplished by placing the network interface card in promiscuous mode to capture all network traffic that crosses its network segment. Network traffic on other segments can't be monitored unless the traffic is directed to the NIDS promiscuous interface. Network Intrusion Detection involves looking at the packets on the network as they pass by the NIDS. The NIDS can only see the packets that are carried on the network segment it’s attached to. Packets are considered to be of interest if they match a signature or certain behavior. Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. Ideally you would scan all inbound and outbound traffic; however doing so might create a bottleneck that would impair the overall speed of the network.

### Host Based Intrusion Detection Systems

A Host IDS (HIDS) uses a piece or pieces of software on the system to be monitored. The loaded software uses log files and/or the system's auditing agents as sources of data. In contrast, a NIDS monitors the traffic on its network segment as a data source. Host based intrusion detection involves not only looking at the network traffic in and out of a single computer, but also checking the integrity of your system files and

watching for suspicious processes. To get complete coverage at your network with HIDS, you must load the software on every computer. Host based Intrusion Detection is much more effective in detecting insider attacks than is NIDS. Host Intrusion Detection Systems are run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected

## CHAPTER 3 SNORT IDS

Snort is an open source network intrusion prevention system, capable of performing real time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more.

Snort has three primary uses: It can be used as a straight packet sniffer like tcpdump, a packet logger (useful for network traffic debugging, etc), or as a full blown network intrusion prevention system.

The privacy of the Snort community is very important to Sourcefire. If you choose to optout, the information collected at the time of registration will not be used for any Sourcefire marketing efforts. In addition, Sourcefire will not sell or distribute any personal information to 3rd party companies.

SNORT can be configured to run in three modes:

1. Sniffer Mode
2. Packet Logger Mode
3. Network Intrusion Detection System Mode

### Sniffer Mode:

snort –v Print out the TCP/IP packets header on the screen

### Packet Logger Mode:

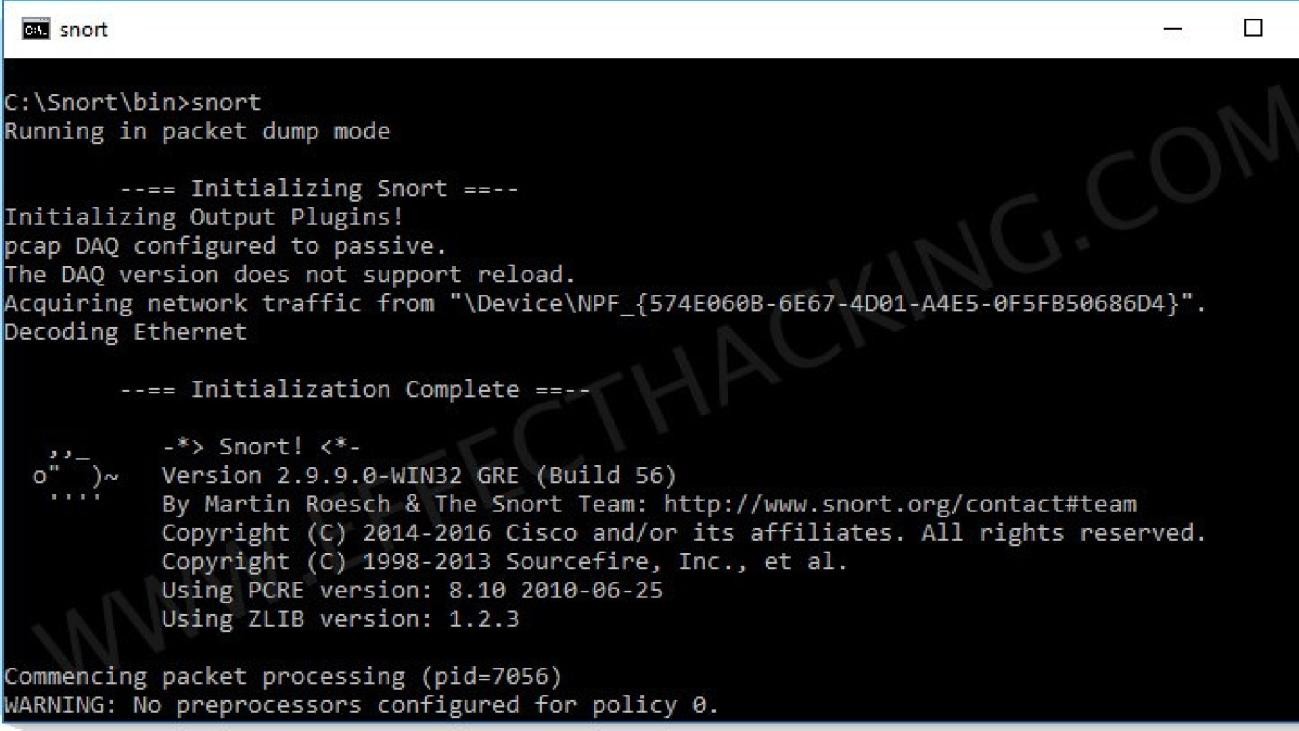
snort –dev –l c:\log [create this directory in the C drive]

snort will automatically know to go into packet logger mode, it collects every packet it sees and places it in log directory.

### Network Intrusion Detection System Mode:

snort –d c:\log –h ipaddress/24 –c nort.conf

This is a configuration file applies rule to each packet to decide it an action based upon the rule type in the file.

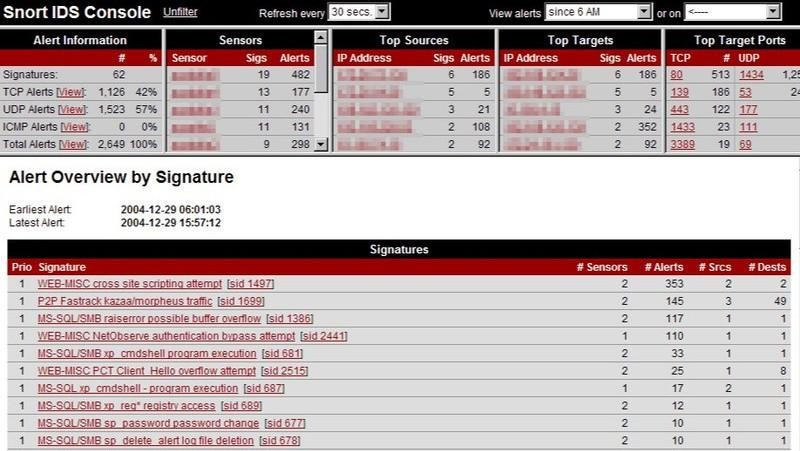


Working with Snort:

1. Go to the web site [www.snort.org/start/download](http://www.snort.org/start/download)
2. Click on download option and support path to save the setup file.
3. Double click on Snort Installation icon to run setup.
4. Accept License agreement and Specify path for installation, and then Click on Next.
5. Install snort with or without database support.
6. Skip the WinPcap driver installation
7. Select all the components and Click Next.
8. Install and Close.
9. Add the path variable in windows environment variable by selecting new classpath.
10. Create a path variable and point it at snort.exe variable name: path and variable value as c:\snort\bin.

Click OK button and then close all dialog boxes.

1. Type the following commands:
2. Go to command prompt and get into Snort/bin directory and run Snort.exe file.
3. An editor window displays the complete details of packets flowing across the system, the IP Address of packet generator, date &amp; Time, length of Packet, Time to live(TTL) Etc at Realtime.
4. By analyzing these details Intruders can be traced at real time.



## 4. Conclusion

As security incidents become more numerous, IDS tools are becoming increasingly necessary. They round out the security arsenal, working in conjunction with other information security tools, such as firewalls, and allow for the complete supervision of all network activity. Intrusion detection systems add an early warning capability to your defenses, alerting you to any type of suspicious activity that typically occurs before and during an attack. Since most cannot stop an attack, intrusion detection systems should not be considered an alternative to traditional good security practices. There is no substitute for a carefully thought out corporate security policy, backed up by effective security procedures which are carried out by skilled staff using the necessary tools. Instead, intrusion detection systems should be viewed as an additional tool in the continuing battle against hackers and crackers.

## 4. References

* + ["What is an Intrusion Detection System (IDS)? | Check Point Software"](https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/).
  + ["Intrusion Detection Systems: A Survey and Taxonomy"](http://neuro.bstu.by/ai/To-dom/My_research/Paper-0-again/For-research/D-mining/Anomaly-D/Intrusion-detection/taxonomy.pdf)
  + [*Computer Security: Protecting Digital Resources*](https://books.google.com/books?id=_R5ndK-i3vkC&q=%22intrusion%2Bprevention%2Bsystem%22%2BAND%2B(reaction%2BOR%2Breactive)&pg=PA266)
  + *Vacca, John R. (2009-05-04).* [*Computer and Information Security Handbook*](https://books.google.com/books?id=TnE85sckwMAC&q=IDS%2Bnetwork%2Bhost%2Bsignature&pg=PA64)*. Morgan Kaufmann.*
  + [*"Gartner report: Market Guide for User and Entity Behavior Analytics"*](https://www.gartner.com/doc/3134524?ref=SiteSearch&sthkw=avivah%20litan&fnl=search&srcId=1-3478922254)
  + [*Network Security: Current Status and Future Directions*](https://books.google.com/books?id=dHys9OXMFMIC&q=signature%2BIDS%2Bdisadvantage&pg=PA86)
  + Rajabi, Samira, Shahram Jamali, and Javad Javidan. "An Intrusion Detection System in Computer Networks using the Firefly Algorithm and the Fast Learning Network." *International Journal of Web Research* 3.1 (2020): 50-56.