CLOUD BASED INTRUSION DETECTION SYSTEM USING ML/DL

TEAM MEMBERS-Abhishek sanjeev , vipul choudhary , S GURUSARAN , APOORV KUMAR **Guide name-**Dr. Ganeshan R

Project Group ID:- 19

ABSTRACT

To alert the system of the incoming suspicious packet request which can lead to the Hijacking of the system as well as the servers and clouds.

We are trying to make the network intrusion detection system with the help of the AI and ML which can detect the intrusive incoming packets and halt the incoming attack for a particular period.

INTRODUCTION

- **Intrusion detection system** (**IDS**)
- typically, another separate computer, that monitor incoming data from the client side
- An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching.

MODULES AND METHODS

- Consists of five modules, such as IDS configuration module, network traffic capture module, IDS process core, IDS rule module, and IDS result module.
- the IDS configuration file was generated for the proposed detection approaches and rules. The pre-configuration information was obtained in two ways. First, there was self-learning from the real-time or captured normal traffic. Second, it included knowledge from the protocol specifications and practical operational experience.
- Network traffic capture module was developed for real-time capturing and parsing of MMS/SNTP traffic from the station layer network. The captured actual pcap files were also parsed by this module. In the module, the IEC 61850 protocol parsers were used

RESULTS

A cloud-based intrusion detection system (IDS) is essential for companies migrating workloads and services to public cloud infrastructure like Amazon Web Services (AWS) and Microsoft® Azure. That's because cloud environments pose a unique security challenge.

As we know that our world is now shifting to the 3rd Generation of Web (WEB 3.0) we are all depending upon the internet more and more.
Even it is now common that we use cloud everywhere from personal photos in Google photos to the commercial use of Google One and Google collab

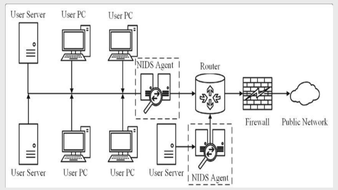

Figure 1. Label in 20pt Arial.

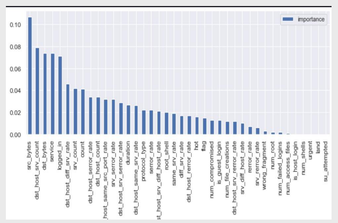

Chart 1..

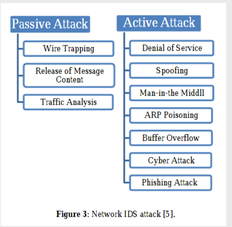

Figure 3: Network IDS attack [5].

Figure 2. .

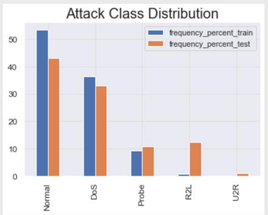

Table 1.

DISCUSSION

1. Since we know that IDS is based on the filtering of data from the log files stored in the csv files present in the network.

2. The machine learning algorithms are now days removing the Hardcore requirement of human , with that algorithms are getting more specific and correct as the technology is going.....

3. Most of the organizations would require a product which can directly and automatically check and apply prevention techniques at any time in the network.

CONCLUSIONS

- DS rule module ..it will implement the ACD(Access Control Detection), PWP(Protocol Whitelisting Detection), MBD(Model-based Detection), and MPD(Multi-Parameter based Detection). A database is set up for the DS, which stores critical status parameters of the system.

REFERENCES

- "What is an Intrusion Detection System (IDS)? | Check Point Software".
- ^ Martellini, Maurizio; Malizia, Andrea (2017-10-30). Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges: Threats and Counter Efforts. Springer. ISBN 9783319621081.
- ^ Axelsson, S (2000). "Intrusion Detection Systems: A Survey and Taxonomy" (retrieved 21 May 2018)