Network Intrusion Detection and Deduce System

Seethal Sasikumar, Abhay K S, C.N.S.Vinoth kumar

Department of Computer Science and Engineering, College of Engineering and Technology
SRM Institute of Science and Technology, Kattankulathur, Chennai
si2903@srmist.edu.in, as8091@srmist.edu.in, vinothks1@srmist.edu.in

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract—Network Intrusion Detection and Deduce Systems keep a track of network traffic for anomalies based on signatures and heuristics that differ from dealer to dealer and from implementation to implementation. Host Intrusion Detection System and Host Intrusion Prevention System applicable at endpoints where NIDDS applies to network boundaries and segmentation points such as the gateways to the internet or other untrusted networks. By assessing the traffic for certain anomalies, a NIDDS can ascertain malicious or other undesired or unforeseen data. When a match is found based on patterns, signatures, or other heuristics, the system can log it, send an alert to the monitoring system or to the server, or even take action such as blocking, redirecting, or resetting the connection depending on the organisation. NIDDS is a malicious intrusion prevention system that uses publicly released signatures containing malicious or other dubious trails, as well as generic trails gathered from different anti-virus records and directories with unique user identifiers, in which the route can be anything from a search engine. The proposed system, detects the attack using a Raspberry Pi, a low-powered computer.

Keywords—Network Intrusion Detection and Deduce System(NIDDS), Intrusion.Detection.System(IDS), Sensor,Raspberry Pi

I. INTRODUCTION

Nowadays everything is connected to the internet including IoT devices like cameras, smart tv, etc. Like this almost anything can be connected to the internet and access from anywhere from the world. And we have seen these advantages have been misused by cyber criminals. They started making unsecured devices become a part of their botnets, infecting and spreading crytominers and ransom wares over the networks. Also, they remotely access our devices to compromise bank accounts, private data, etc. Even though we install AVs in our computers and mobile devices other devices are still exposed to attacks. In Order to get protected from these we are developing a security device called NIDDS .This will be connected in between end devices and the internet and all tracks of malicious and suspicious traffic will be tracked and monitored. Our system can search for viruses and malware attacks using an online malware detection system (Virus Total) and open access dynamic blacklists, and even some existing precompiled blacklists from different antivirus distributors and our own definitions of block lists, to block access and generate accurate log reports. In [1-3], Luigi Manosperta, Network Based Intrusion Detection

System utilises single chip machine Raspberry Pi 3 model B+, which would be sensitive enough to discover a range of cyber security threats without compromising overall scalability and performance. It's an easy framework that can even detect attacks in custom applications and DDOS attacks at multiple layers. Venkatraman Subbarayalu, B.Surendiran and P. Arun Raj Kumar [4] used timed automata (TA) for restricted Smart objects and an automata controller (AC) to evaluate IoT device events. Furthermore, the paper offers an in-depth review of various signature-based and anomaly-based Network Intrusion Detection System in IoT applications. A legitimate network intrusion detection system focused on deep learning that combines big data, natural language processing, and deep learning technology [5]. Umi Najiah Ahmad Razimi, Mohammed Hazim Alkawaz, Shamla Devi Segar had advocated a knowledgeable home security system with help of Raspberry Pi [6].

In our work, we detect and monitor malicious attack from different blacklisted IP's and domain to the server [10-13]. We collect data from all the available platforms and sources to the detection centre. Normal IDS cannot monitor the attack and log whereas in our Network Intrusion Detection and Deduce System (NIDDS) we have built a solution for monitoring as well as detecting the same at low cost and increased efficiency.

II. RELATED WORK

The initial installation seeks to achieve high levels of precision when detecting a series of cyber-attacks on low-powered hardware like the Raspberry Pi, regardless of network traffic volume. It mainly focuses on detecting DDOS attack at different layers (Network and Application layer) and replay attacks that the system faces. Unfortunately the existing system does not block or redirect the attack since it mainly focus to create a lightweight NIDS for resource-constrained devices that provides a high level of accuracy while generating minimal computational overhead. This system uses simulation tools rather than depicting it in real scenarios. The proposed NIDDS system focuses on the usual suspects situations will be identified using real-life examples. It keeps track of all suspicious direct file downloads [7-8]. It may also cause a lot of false positives, but it can ultimately assist in the reconstruction of the infection chain.

Firstly, [9], this paper discusses the existing state of NIDS implementation tools and datasets, along with open source and freely network detecting applications. It then collects, analyses, and compares state-of-the-art NIDS proposals in the IoT framework in particular of architecture, detection methods, validation methods, managed risks, and algorithm functionalities.
Secondly, [10-12], this study describes a method that uses association rules to detect network intrusion. The approach is often used to build intrusion standards which would spot exploits in network data sets using detection techniques. This demonstrates the ability of the modified association rules algorithm to detect network intrusions.
Thirdly, [13], the paper identifies a Smart Intrusion Detection System (IDS) for Android phones that aids in the detection of intrusion and malicious activities. It has a GPS tracker, as well as finger print and password protection for the user. It takes a screenshot of the attacker as well.
On the other hand in [14], they suggest a tool in this framework that will alert the owner through an app if any appropriate intrusion is detected inside the home/office. When an intruder is detected, the system notifies the owner and, at the same time, an alarm is activated and begins to sound, alerting the neighbor and security guard.
Fourthly, [15] throughout this study, they introduce an Intrusion Detection Framework for the Internet of Things. Deployment of Snort on a Raspberry Pi, a low-powered device widely used during IoT applications. The Raspberry Pi's efficiency is reviewed. Fifthly,[16], the proposed study aims to recognize network intrusions utilizing a deep-learning-based strategy. A deep neural network is used to train the system with anomaly characteristics and differentiate network traffic between normal interactions and intrusions. In paper [17], they aimed at some of the frequently used datasets in network intrusion detection systems, as well as the researchers who performed on these datasets.
The objective of this experiment include to examine the performance, reliability, and feasibility of several open source IDS – Snort IDS as well as Bro IDS – on a multi-purpose, low-cost system called Raspberry Pi 2 (Model B), with the goal of using them in computer network settings wherein cost is a key determinant [18-20]. From the referred papers, we can come to the conclusion that some of them use assumptions; some could take only moderate network load and some could only detect the threat without blocking it [21-24]. While the NIDDS can determine threat in real time scenarios, can prevent the attack and can access the attack.

III. RESEARCH METHODOLOGY

The Network Intrusion Detection and Deduce System (NIDDS) aims to detect unauthorized computer system use, misuse, and abuse. We developed a methodology for analyzing NIDDS in response to the increased use and development of the technology.

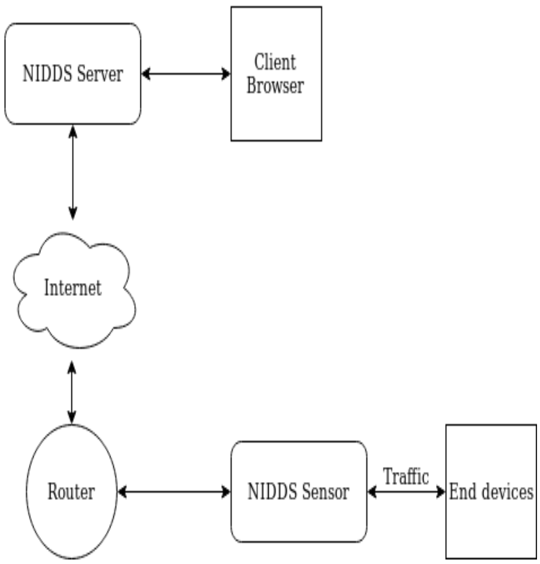
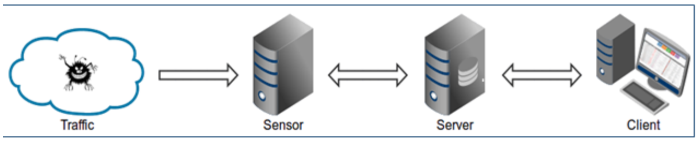


Fig (1): System Architecture

NIDDS is based on the Traffic →Sensor←→Server←→Client architecture.



Detection of a sensor

Sensor is a stand-alone component that monitors passing traffic on the monitoring or standalone system (e.g. Honey pot). The methodology describes a framework for identifying, blocking, saving, and classifying intruder addresses using Raspberry Pi [25].

There is a heavy traffic created by blocked items/trails. The event information has been sent to the (central) server and collected in the appropriate logging directory if there is a positive match. UDP responses are used to send logs from the sensor to the server. In, [26], a light and fully responsive firewall solution for tiny to mid-size businesses was modeled on a Raspberry Pi, along with a user-friendly interface that supports customers with hardly any understanding of firewall configuration and deployment to their firms. This research was carried in real time with only two hosts.

Server Display

The server's core objective is to maintain track of events as well as provide back-end support for the monitoring user interface. By design, the server and sensor will function on the same CPU [27]. To minimize unnecessary sensor activity disruptions, the front-end monitoring involves analysing on the fat client architecture. The client receives the events for the chosen time(24hours).

In Client, the presentation is exclusively the responsibility of the reporting web application. The data is then compressed and sent to the client, where it is stored in order. The final report is written in a condensed format that allows for the presentation of an almost infinite number of incidents.

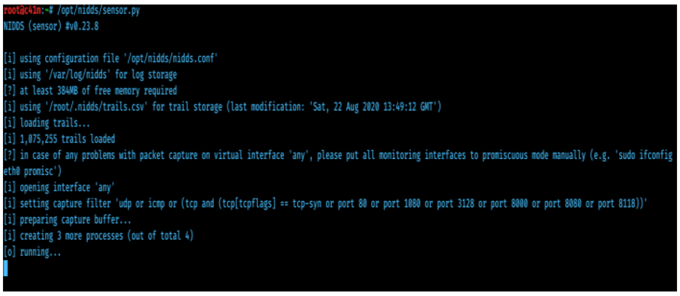
IV. EXPERIMENTAL ANALYSIS

Setting up Devices

Sensor on Ubuntu:-

Use below commands for setting your NIDDS sensor up and able to run with default configuration and the reporting interface set to “any”.

install_sensor.sh



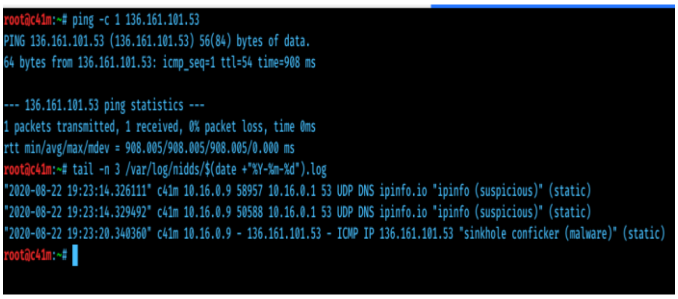
Sensor on Raspberry Pi with WiFi:-
You can run this sensor on a raspberry pi.

Server on AWS:-

In order to begin the server on the computer, use below commands.

install_server.sh

To check whether everything is up and running properly, we can execute the following: ping –c 1 136.161.101.53



Execute following commands to prevent the sensor and server instances:-

sudo pkill –f sensor.py
pkill –f server.py

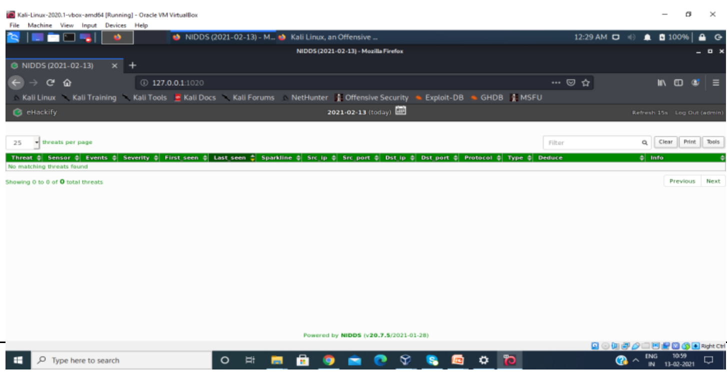
Following completion of the server and sensor configuration, we launched an assault on the server. After that, the sensor is used to detect the attack. After detecting malicious attacks from various blacklisted IP addresses and domains, which are obtained from all available channels and sources and sent to the detection centre, it is then monitored in the server. The client will view the details of the intrusion using the built web application. The client may, then, determine the severity of the attack or intrusion based on the details shown and takes appropriate action. Initially, when the sensor is powered on or following a prolonged time of inactivity, it will automatically change the routes based on trial preferences. It will actively monitor the configured interface after activation and either write the events to the provided remote tracking server or record them in the given document list.

In the complete network monitoring and protection, they checked the effectiveness of Raspberry Pi on IDS, a packet analyzer and a honeypot server. The Smart Mirror can be used as a home protection device, and it can accept three types of input commands: voice, touch, and mobile commands.

The model was proposed with Raspberry Pi hardware, Ubuntu Server as the operating system, and Snort as the intrusion detection system

The following figure represents various attacks and its details that are captured by the NIDDS.The details includesthreat,sensor,events,severiety, firstseen, lastseen,

sparkline, source ip, source ports, destination ip, destination ports, protocol, type, deduce and information about the attack. The below figure will show the display page:



The following table shows the accuracy of the identification of specific attacks and potential scanning.

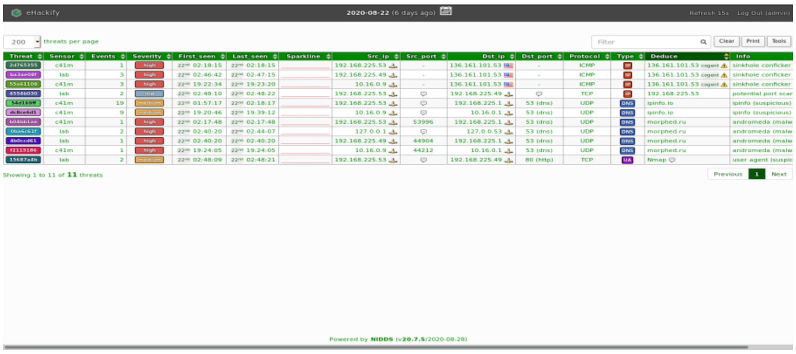


Table 1: Accuracy

Test Case	Attack	Accuracy
1	Mass scans	94-97
2	Anonymous Attackers	94-97
3	Service Attackers	95-96
4	Malware	94-96
5	Suspicious Domain Lookups	96-97
6	Suspicious IP Info Request	98
7	Suspicious Direct File Download	95
8	Suspicious HTTPS Request	97
9	Port Scanning	98
10	DNS Resource Exhaustion	95
11	Data Leakage	96
12	False Positives	98

V. CONCLUSION

All in all, the proposed Network Intrusion Detection and Deduce System (NIDDS) is modest and effective. It gives successive updating of the mark information to the data set in genuine world and gives alert if there is any disruption. Less equipment is needed for this system. The equipment and programming utilized are versatile so they are monetarily suitable**.** NIDDS can be used for commercial purposes by varying the limit of the hardware and software used.It is easy to trace the attack and to obtain the details about the attacker. Local users can also use the same due to its low cost.

REFERENCES

[1] Luigi Manosperta,"A Quantitative Analysis of a novel Network based Intrusion Detection System over Raspberry Pi",Thesis-September 2019
[2] Obinna Cyril Onyedeke, Matthew C.Okoronkwo, Uchechi Ihedioha "Signature based Network Intrusion Detection System using Feature Selection using Feature Selection on Android", Article in International Journal of Advanced Computer Science and Applications, January 2020
[3] Nadia Chaabouni, Mohamed Mosabah, Akka Zemmari, Cyrille Sauvignac and Paryez Faruki, "Network Intrusion Detection for IoT Security based on Learning Techniques",IEEE Communications Surveys And Tutorials,vol.00,No.0,November

[4] Alessandro Sforzin and Mauro Conti, F’elix G’omez M’amol and Jens-Matthias Bohli, “RPiDS: Raspberry Pi IDS A Fruitful Intrusion Detection System for IoT”,2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People and Smart World

[5] Venkatraman Subbaraylu,B. Surendiran and P. Arun Raj Kumar,”Hybrid Network Intrusion Detection System for Smart Environments based on Internet of Things”,The British Computer Society

[6] Sandeep Gurung,Mimal KAnti Ghose, Aroj Subedi,”Deep Learning Approach on Network Intrusion Detection System using NSL-KDD Dataset”,I.J. Computer Network and Information Security, 2019,3,8-14,08 March 2019

[7] Flora S. Tsai,”Network Intrusion Detection using Association Rules”,International Journal of Recent Trends in Engineering,Vol 2,No.2,November 2009

[8] A.Saranya, R.Naresh “Cloud Based Efficient Authentication for Mobile Payments using Key Distribution Method”, Journal of Ambient Intelligence and Humanized Computing, Springer, 02 January, 2021. https://link.springer.com/article/10.1007%2Fs12652-020-02765-7

[9] R.Naresh, P.Vijayakumar, L. Jegatha Deborah, R. Sivakumar, “A Novel Trust Model for Secure Group Communication in Distributed Computing”, Special Issue for Security and Privacy in Cloud Computing, Journal of Organizational and End User Computing, IGI Global, Vol.32, No. 3, Septemer 2020, Pp. 1-14. DOI: 10.4018/JOEUC.2020070101

[10] R Divya Mounika, R.Naresh, “The concept of Privacy and Standardization of Microservice Architectures in cloud computing”, European Journal of Molecular & Clinical Medicine, Vol 7, No 2, Pages 5349-5370, Dec 2020.

[11] P.Vijayakumar, R.Naresh, L. Jegatha Deborah, SK Hafizul Islam, “An efficient group key agreement protocol for secure P2P communication”, Security and Communication Networks, Wiley, Vol.9, No.17, pp.3952–3965, 2016 http://onlinelibrary.wiley.com/doi/10.1002/sec.1578/abstract

[12] P.Vijayakumar, R.Naresh, SK Hafizul Islam, L. Jegatha Deborah “An Effective Key Distribution for Secure Internet Pay-TV using Access Key Hierarchies”, Security and Communication Networks, Wiley, Vol.9, No.18, pp.5085–5097, 2016.

[13] R. Naresh, M Meenakshi, G Niranjana, “Efficient study of Smart Garbage Collection for Ecofriendly Environment”, Journal of Green Engineering, Vol.10, No.1, pp.1-10,Feb 2020.

[14] Oguzhan Karahan ,Berat Kaya,”Raspberry Pi Firewall and Inrusion Detection System”, Research Article Journal of Intelligent Systems:Theory and Applications 3(2) 2020: 21-24 .

[15] J. Verma, A Bhandari and G Singh,”Review of Existing Data Sets for Network Intrusion Detection System”, Advances in Mathematics; Scientific Journal 9(2020),no.6, 3849-3854 ISSN:1857-8365 (printed):1857-8438(electronic)

[16] Harsha Jitendra Kurane,Disha Rajan Londhe,Dnyaneshwari Balasaheb Shinde, Shinde S K,,Mohini Sadashiv Naik,”IOT Based Intrusion Detection System”,International Journal of Progressive Research in Science and Engineering Volume-1,Issue-4,July-2020

[17] Sumanth R,Bhanu K N,”Raspberry Pi Based Intrusion Detection System Using K-Means Clustering Algorithm”,Proceedings of the Second International Conference on Inventive Research in Computing Applications(ICIRCA-2020)

[18] Shyava Tripathi,Rishi Kumar,”Raspberry Pi as an Intrusion Detection System,a Honeypot and a Packet Analyzer”,2018 International Conference on Computational Techniques, Electronics and Mechanical Systems(CTEMS)

[19] June Jeremiah,” Intrusion Detection System to Enhance Network Security Using Raspberry Pi Honeypot in Kali Linux”, 2019 International Conference on Cyber security(ICoCSec)

[20] Ar Kar Kyaw,Yuzhu chen,Justin Joseph,”Pi-IDS:evaluation of Open-Source Intrusion detection Systems on Raspberry Pi 2”,2015 Second International Conference on Information Security and Cyber Forensics(InfoSec)

[21] Raju Nadaf,Vasudha Bonal,”Smart Mirror using Raspberry Pi as a Security and Vigilance System”, Proceedings of the Third International Conference on Trends in Electronics and Infomatics(ICOEI 2019)

[22] Yuan Sheng Dong, Rong Wang and Juan He, “Real-Time Network Intrusion Detection System Based on Deep Learning”,12th International Conference on Software Engineering and Service Science(ICSESS)

[23] Lalit Mohan,Sourabh Jain,Priyanka Suyal, Aravind Kumar,”Data mining Classification Techniques for Intrusion Detection System”,12th International Conference on Computational Intelligence and Communication Networks

[24] Umi Najiah Ahmad Razimi,Mohammed Hazim Alkawaz,Shamla Devi Segar,”Indoor Intrusion Detection And Fitering System Using Raspberry Pi”,2020 16th IEEE International Colloquium on Signal Processing & its Application(CSPA 2020),28-29 February 2020

[25] Younes Laaboudi, Alexis Olivereau,Nouha Oualha,” An Intrusion Detection and Response Scheme for CP-ABE Encrypted IoT Networks”, 2019 10th IFIP International Conference on New Technologies, Mobility and Security(NTMS)
[26] Jose Emmanual Cruz de la Cruz,Christian Augusto Romero Goyzueta,Cristian Delgado Cahuana,”Intrusion Detection and Prevention System for Production Supervision in Small Business Based on Raspberry Pi and Snort”, 2020 IEEE XXVII International Conference on Electronics, Electrical Engineering and Computing(INTERCON)
[27] Vasaka Visoottiviseth,Gannasut Chutpom,Sorakrit Kungyanruttana,Jirapas Paisamduangjan,”PITI: Protecting Internet of Things via Intrusion Detection System on Raspberry Pi”,2020 International Conference on Information and Communication Technology Convergence(ICTC)