March - April 2020
ISSN: 0193-4120 Page No. 9414 - 9420

Intrusion Detction System using Snort with Raspberry PI

Dr. M. Senthamil Selvi[1], Mr. G. Ram Sundar[2], Mrs. Jansirani Sankar[3]
[1]Professor & Head, Department of Information Technology, Sri Ramakrishna Engineering College, Coimbatore-22
[2,3]Assistant Professor, Department of Information Technology, Sri Ramakrishna Engineering College, Coimbatore-22
senthamilselvi@srec.ac.in[1], ramsundar.gurumoorthy@srec.ac.in[2], jansi.sankar@srec.ac.in[3]

Article Info
Volume 83
Page Number: 9414 - 9420
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 09 April 2020*

Abstract

In Today's world, important to maintain high level of security to guarantee the communication of information in day to day. However, transfer of data in a secure manner over a internet and intranet is very tough to achieve because of vulnerabilities and threats. Malicious traffic exploits the loopholeand thus, invades and further sabotages theentire network. In order to combat this issue, users areentrusted with the network security software for safeguarding their own system against unauthorized users. Unfortunately, the various techniques and approaches of the existing systems proved to be flawless for thwarting network intrusion activities though. Honey pot is used as a decoy for theattackers. It is intended to be vulnerable, so attacker can easily get into the system. Theaim for this research is to identify and review the given loophole within network security in contemplate of pinpointing the common network intrusion behavior. The performance test for Raspberry Pi is also conducted to prove whether Raspberry Pi capable to run snort.

Keywords; *network security,Raspberry pi,intruders,Honey pot,Intrusion detection*

I. INTRODUCTION

The internet has been used by all from larger companies to home but the attack is more irrespective of the usages and areas. Network vulnerability has always been an issue, given a new breath over the times. In modern home, lot of daily usage devices like TV, Lights moved to smart with internet and its stores lots of personal and financial data. Because of the smart devices and digital era, vulnerability towards the security also increased. Its presence possesses far more potential threat that it seems, unknown to household users, or even an avid web browser.However, lack of understanding regarding network intrusion behavior constitutes to unauthorized data mining, for unknown intention.In return, making it an unruly plague, which continually rotten and likewise, infiltrate the integrity/confidentiality of user information, circulating theInternet; Exposure toward the network attack and intrusion increases proportionally with the increases of internet usages. To prevent from the network intrusion and attack, user must aware of the network and its usage. An Intrusion Detection System (IDS) is software or hardware used to monitor the network and report if any intrusion happened in the implemented networks. So, IDS system is very useful for the home network to prevent and protect from unwanted entry from outside. With the low cost implementation and maintenance, the user of the IDS system ranges from Home to small size capanies. The potential solution to avoid from the attack is to implement/ install intrusion detection in the network; example is Snort on a Raspberry pi. The said device is portable because it run in any operating system and it is affordable and low cost to implement. So, it provides better protection in any network.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9414 - 9420

II. RELATED WORKS

The previous and related work with respect to both honey pots and the Raspberry Pi implementation in security mechanisms is discussed below:

I. Use of a Honey Pot in a Local Area Network(LAN)

In today's world, the growing threat of cyber attacks is something that weare not dealing with in an effectivemanner. Attacks are becoming moreand more dynamic in natureand defence mechanisms need to adopt an equal measure of dynamism.Most network administrators arefocused on repelling any attacks or intrusions and hence they fail to study the method or patterns of attacks.Hackers attempting to access information stored on the network or the server constantly keep bombarding the target with new variations of attacks.

As a result, sometimes the hacker can penetrate the system without the knowledge of the network administrators or users resulting in loss of data which is probably not noticed by the network security engineers.

The role or the use of a honey-pot is extremely simple yet valuable. We usea honey pot setup to actively monitor and defend the network from illegal access. If there is a network breach which is not noticed by the security mechanisms, the honey pot will do its job of attempting to lure theattackers towards it and thereby protect the important information. In addition, the methods used by theattacker to access the network are stored in the logs as evidenceand can be retrieved for future study of theattack patterns.

This can also be used to map and predict possible futureattacks by decoding the mechanism used by theattacker and progressively identifying the tools utilized for the same. This is essentially a mechanism of evolution for network defenseand security systems [1].

II . Using a honey pot as a proxy server The system architecture proposed by Supeno Djanali, FX Arunanto, Baskoro Adi Pratomo, Hudan Studiawan, Satrio Gita Nugraha [2] is essentially a system that uses a proxy server, combined with theactual server carrying the information and a honey pot. The proxy server receives the web requests and does analysis of the request and decides to forward it either to the honeypot or to the server.

Here the server cannot beaccessed directly over the internet as it is the proxy server that is connected to the internet. Theactual server is connected to the proxy server viaa private network. The honey pot is also linked up with the proxy server and can beaccessed via the internet itself.

Basically, the proxy server and the honeypot work in tandem and can be considered as one unit.The proxy server serves as a detector and analyzer for SQL injections andany such malicious requests are dealt by the honey pot.

III. LIMITATION

During 2013, the study was made on make use of Raspberry as on IDS system in a small network [5]. The study conducted with the following, the B+ Raspberry pi model runned on the IP Fire OS and software used is intrusion detection Snort. Based on the study, it is concluded that Raspberry pi can be used as intrusion detection system with the following limitations:

• Memory: Usage of how many snort – rules

• Some degradation in throughput when Snort was active.

We want to analyze the possibility of implementing the following intrusion detection system

1. Doesn't suffer when running Raspberry Pi B+ on Arch Linux ARM(Light weight and low system resources usage).

2. Also analyze running Raspberry Pi 2 model B with Arch Linux ARM.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9414 - 9420

The last model can provide better results when compared to Raspberry Pi B+ model. This study will only put effort on the prospect of using a Raspberry Pi as an intrusion detection system using the software Snort. Neither the Snort software or any of its rules will be optimized to find out which rules impacts the throughput performance the most. We will not examine how effectively Snort detects malicious activity with different rule-sets, nor which kinds of traffic is the most difficult to process by Snort.

IV. PROPOSED METHOD

The main aim of the proposed study is to find the performance of the network when the Intrusion Detection System uses Raspberry Pi. This study is useful for the intermediate user with deep knowledge on network traffic and security who are going to increase the awareness and security in the network. This also useful for small companies who want more secure network but with less capital and less maintenance compared to other IDS, the model with Raspberry pi provided enterprise solution. High speed Internet connection access not same for these two group of the uses, that may be limied by Raspberry Pi throughput capacity or need IDS that does not suffer any downtime. The latter part is important to take in consideration when deciding on the placement of the IDS. If the connection between the ISP and the home network the downtime will be a problematic, Raspberry Pi goes offline returns Internet will go down.

V. INTRUSION DETECTION SYSTEM MODEL

An intrusion detection system (IDS) is a system used to find the malicious activity in the network or single host system. The theory behind the IDS, the system make differ between the legitimate users and network traffic from malicious activity. IDS uses two methods to identify the malicious activity in the network. The figure 1 shows the component included in the IDS. The first component deals with the data collection related to the network, followed feature selction to extract the needed feature from the data collected next is a analyze phase and final one is action against the detected threat[3].

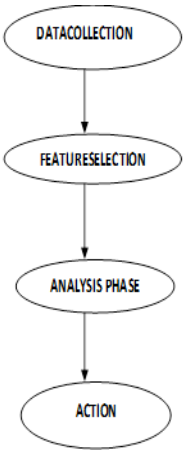

Fig 1: INTRUSION DETECTION SYSTEM MODEL

Data collection:

First phase:Data Collection, It captures and data in the implemented system and routed to next module for further process of intrusion identification. The phase is automatic for collection of data.

Feature Selection:

Next phase is Feature selction, in the collected data has many features like IP of source and target, Payload details, Protocol type, port number details etc [5]. This is dynamically analyze the logged data [4] . Thus, user must give the related set of rules for the alerts, this reduces the false positive and false negative responses of the system.

Analysis phase:

The suspicious threat or activity is analyzed based on the collected data. For the analyze and present to IDS be done by profiling and pattern recognition techniques [6]. The response in the phase is based applied rule. If the activities captured is deviated from the applied rule are considered to be malicious and same to indicate as intrusion.

Action **:**Final stage is action phase. When the system find the intrusion the response action will triggered.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9414 - 9420

The two response action are either by sending the alert notification with data evidence or implement the action against the intrusion in the network/ system.Example for action is drop the packets that are identified as malicious or close the connection from the source.

Intrusion detection system methodology:

Due to high risk in the networks and information system, to maintain the data integrity and confidentiality, IDS is very important. The IDS system is designed to act and response in the host system or network against the threat or malicious activites. IDS desgined system porcess to monitor, analyze, and respond to certain security breaches in real time event [7]. These attacks resulted from unauthorized intruders, either remotely or internally. Obviously, their intention to attack the system for personal gain.This can be also misconduct from Intruders users that are misusing their authority. The use of proposed methodologies like snort within intrusion detection system for handling different situation must be practiced in order to achieve optimal performance.

Network based Intrusion Detection Systems benefits :

- Low cost
- Easy Implementation
- Identify network based attacks
- Record evidence
- Detect faster and response quick
- Detection of false positive attacks

The effective behavior and protocol event are identified by APIDS (Application based IDS) [2]. Between the process and group of servers, the system or agent is placed, which monitors and analyzes the application protocol between devices [2]. Intentional attacks are the malignant attacks to cause harm to the organization by disgruntled employees and Unintentional attacks like deletion of important data file causes financial damage to the organization[2]. Many attacks are taken place in OSI layers.

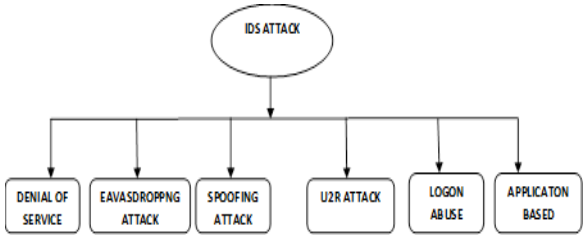

fig 2: Various IDS attacks

These are the three major intrusion detection system used widely for identifying intrusion.

- Anomaly Based Methodology,
- Signature Based Methodology
- Stateful Protocol Analysis Based Methodology.

VI. SYSTEM ARCHITECTURE

Design is the gist for turning all requirements into detailed specifications that covers all theaspect of the system. The chosen methodology will increse the accuracy and performance of the proposed intrusion detection system used for this research. Figure 3 is considered as blueprint on how the system will be architected and constructed. This method encompasses for the following steps are used to construct the proposed system, such as the installation of related software and a protected database module for protecting the generated evidence log files. SNORT uses six phases, the phases are data Identification phase, detection phase, investigation phase, reporting phase, attack collection phase and maintenance phase. For data collection phase, Raspberry Pi snort model is used as honey pot system in capturing network traffic. It acts as victim in real scenario. For example, comparing the sourceand destination IP address as well as ports to the rules defined. If it matches, it will notify the users about the intrusion activities. At the same time, it also record activities into evidence database, the investigation phase will observing network intrusion behavior later, such as activity rates for the given intrusion activities. The evidence

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9414 - 9420

collection phase involves storing of log files for malicious activities inside database, while the maintenance phase is for updating new rules in detecting new threat based on the collected evidence files. From the statistical report, users may be able to foreseeand predict the future attack before it actually happened. Preventive measure can be imposed before intrusion attacks being initiated.The research explores the use of genetic algorithm in detecting phase for malicious activities. It is used to predict intrusion types detected with network audit data (logged files) as input.

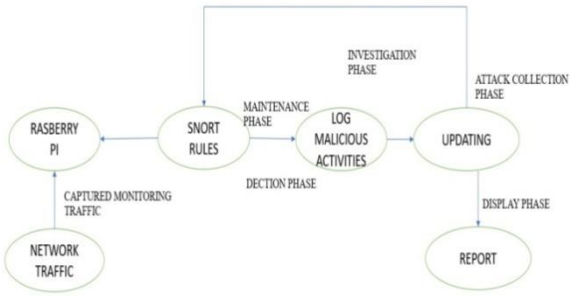

Fig 3: System Architecture

VII. CONFIGURATION FILE

The most important file present in the Snort environment is the configuration file. Snort

can be configured using the command

sudo gedit /etc/snort/snort.conf

This file contains nine basic sections:

1.Set the***network variables***: the Snort configuration fileallows a user to declareand use variables for configuring Snort. Variables may contain a string (such as to be used in a path), IPs, or ports.

2. Configure the***decoder***: incoming Packets in snort are first processed using a decoder.

Snort. The decoder is used to determining which underlying protocols are used in the packet (such as Ethernet, IP, TCP, etc.) and saves this data .Decoder does not decode the application data .

3. Configure the***base detectionengine***: Snort rules are applied to base detection engine to find intrusion activity.Based on the intrusion detected the appropriate rules will be applied. Time processing depends upon the configuration and power of machines.

4. Configure***dynamic loadedlibraries***: Load libraries are used to load the modules that can be used with snort. The dynamic API are further used to apply rules to snort.

5. Configure***preprocessors***: Before the packets are analyzed the preprocessors defragment the packet into single string .By using this method IDS will check individual packets events the packets were altered by attacker.

6. Configure***output plug-in***: they allow Snort to be much more flexible in the formatting and presentation of output to its users. The output modules are run when the alert or logging subsystems of Snort are called, after the preprocessors and detection engine. For example if attacker sends two packets, preprocessor combine it and check it for any intrusion

7. Customize***your ruleset***: Rule set can be customized based on the possible attacks .These ruleset have been updated constantly by the snort community. User can customize or frame new ruleset .

VIII. WRITING SNORT RULES

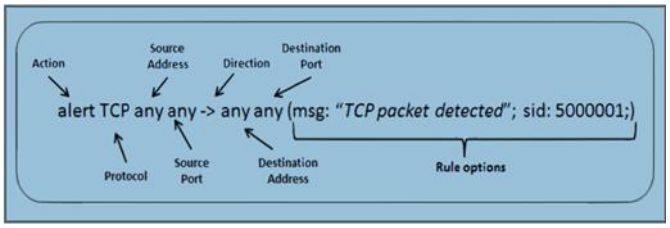

Fig 4: Screenshot of Writing SNORT rules

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9414 - 9420

The rule header contains the information that defines the who, where, and what of a packet,as well as what to do in theevent that a packet with all theattributes indicated in the ruleshould show up.The first item in a rule is the rule**action**. The ruleaction tells Snort what to do when it findsa packet that matches the rule criteria.Thereare 5 available default actions in Snort, alert, log, pass, activate, and dynamic. In addition, if you are running Snort in inline mode,

Youhaveadditional options which include drop, reject, and sdrop.

1. ***alert*** - used for generating alert

2. ***log*** – maintains logs

3. ***pass*** - ignore the packet

4. ***activate*** – Used to activate alert for dynamic rules

5. ***dynamic*** – Activate rule to activate from idele

6. ***drop*** – used for block and dropping the packet.

7. ***reject*** – If TCP protocol, TCP rest sent after block the packet, log it or if UDP protocol, message ICMP port unreachable.

8. ***sdrop*** – Does not log it, it block the packet.

The next field in a rule is the **protocol**.

TCP, UDP, ICMP, and IP protocols were supported by snort for analyzing suspicious behavior.

IX. PING ATTACK

One now could have the tools to writea rule to detect a simple ping from an host on the

EXTERNAL_NET directed to an host inside the HOME_NET. To do so the local.rules filecan be opened typing on the router's terminalwhere:

sudo gedit /etc/snort/rules/local.rules

Sample rule in snort:

alert ICMP $EXTERNAL_NET any -> $HOME_NET any (msg: "Ping detected"; itype: 8; sid: 500001;)

• the***itype***keyword is used to identify ICMP value

• The***msg*** field is the message that will be displayed oncea packet matching the rule isdetected.

• The***Sid***field is the ID number of the ruleand must be different from the ID number of

every other rule.

Once saved thelocal.rules file, type the following command on a terminal to start Snort:

sudo snort -i eth1 -c /etc/snort/snort.conf -A console

If a ping is sent from theattacker to the victim machine using the command:

ping192.168.136.102

Fig 5: Screenshot of PING attack

an alert should be displayed by Snort on the terminal running in the router machine.

Once this steps are correctly performed, Snort is now running on the virtual net.

X. CONCLUSION

This paper is to provide an overview of the application and uses of RaspberryPi as intrusion detection system . This paper gives gives an overview about IDS, and its attacks (PING). IDS are essential for day today security in corporate world and for network users.Still, thereare more challenges to overcome. Future works are based on improving security and performance of detecting PING attack and other TCP/UDP attacks.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9414 - 9420

REFERENCES

[1] R. Chandran, S. Pakala, Simulating Network with Honeyd, Technical Paper, Paladion Networks.
[2] http://www.snort.org
[3] https://www.zeltser.com/mpdernhoneynetwork experime nts/
[4] http://bob.k6rtm.net/kippo.html
[5] http://www.edgissecurity.org/honeypot/dionae a
[6] Kareem Sumner ,Honey pots Security on Offense, Security Architecture 774.716.
[7] S. Boseand A. Kannan. Detecting denial of serviceattacks using cross layer based intrusion detection system in wireless ad hoc networks. In International Conference on Signal Processing Communications and Networking, pages 182–188, Chennai, India.
[8] Mike Fisk and GeorgeVarghese. Fast Content-Based Packet Handling for Intrusion Detection. Technical Report CS2001-0670, La Jolla, CA.
[9] Guy Helmer, Johnny S. K. Wong, Vasant G. Honavar, Les Miller, and Yanxin Wang. Lightweight Agents for Intrusion Detection. Journal of Systems and Software, 67(2):109–122

Published by: The Mattingley Publishing Co., Inc.