AN INNOVATIVE ONTOLOGICAL APPROACH FOR INTRUSION DETECTION SYSTEM

Mukund Katariya[1], Prof. Tejendra Thakur[2]
[1]PG Student, GTU PG School, Gandhinagar, India, [2]Assistant Professor, UCET, Ahmedabad, India

Abstract: In this era of technology Intrusion Detection System (IDS) is one of the fastest developing technology in computer security area Author has projected methodology of using ontology exhibiting to signify IDS knowledge. This model will effectively represent semantic knowledge behind IDS and assistances to concluding high level security policies. This model can also help in recognizing rules and helps in creating effective rule set for IDS. Author makes an innovative approach for above mention domain and implement ontology the system for IDS-SNORT. In information technology, ontology is a prescribed designation and definition of the categories, properties, and interrelationships of the entities which actually or logically happen for a specific domain of dissertation. This proposed work is an engagement of two different things together and that is Snort and Ontology. After engagement with each other it provides to ontological knowledge base which help us to create better rules for snort.

Keywords: Denial of service (DoS), Ontology, Protege, Snort, Security, Knowledge base Ontology (OKB), Community rules.

I. INTRODUCTION

Snort has established great acceptance in the IDS market and has been widely recognized as the reliable open source tool. An IDS examines all incoming and outgoing network movement and find suspicious patterns that might specify a network and system attack from somebody trying to break into or conciliation a system. An IDS is a unique tool because this tool knows interpretation and parsing of network traffic and also detect the host activities[4].

Additionally IDS worked in two parts, first it will check from already recognized attack and/or it also worked using anomaly based detection. IDS compare patterns of activity, traffic, and behavior of data packet[4].

What makes Snort powerful tool? and the answer is supreme feature of it : sniffing the packet, logs the packet and intrusion discovery. Snort has significant mechanism like pre-processor plug-in and alert plug-in, main benefit of these plug-in is that it provides modification facility and snort employment on specific network[10].

Snort mechanism contains four basic mechanisms.

- The sniffer
- The pre-processor
- The detection engine
- The output

In its supreme simple system, Snort is used as a packet sniffer. But, it is deliberate took the packets and process it through the pre-processor, and then checked those packets alongside a chains of rules by the detection engine. Other supreme tool protégé is used to create ontology of snort as well as DoS attack. Protégé tool is an open source tool which helps to create ontology[2][6]. The reason to choose protégé tool for generating ontology is semantic web architecture, extensibility, ontology storage. It also provide good knowledge representation of ontology[8].

A. Denial of Service Attack

DoS is an act that stops the legitimate users from the authorized use of networks, system and/or application by exhausting resources such as disk space, memory bandwidth, and central processing unit[11]. Here author has showed simple DoS attack and that is detected by snort using community rules. N number of simple ping on particular IP address is known as DoS attack. Using that method, attack has been done and detected by predefined rules and after same attack is detected by improved rules which are placed in local rule directory[11].

B. Snort- IDS

Here Snort- IDS is used to identify DoS attack using two different external rules one of them is community rules which is provided by the snort.org and another one is local rules which can be used to generate different users using their own ability and methodology[1]. Author has also generated local rules for DoS attack. Now using these two different scenario author checking for DoS attack. After evaluating the result for both the result, number of packets capture per sec is high and accurate than number of packets capture by the community rule.

C. Ontology

Ontology is an explicit description of a representational terminology for a domain: descriptions of classes, relations, function, constraint and other objects[8][9]. Ontology refers to formal, explicit specification of a shared conceptualization [2][6]. Components of Ontology are shown below:

- Concepts
- Instances, individuals or facts
- Relationships
- Attributes

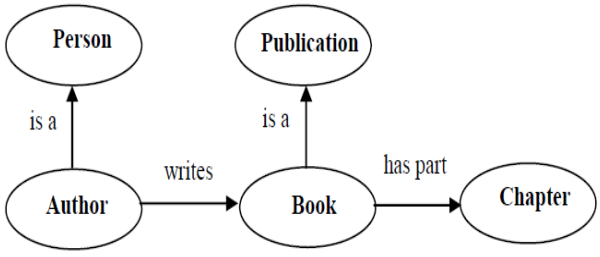

Figure1: Example of small ontology

II. PROPOSED WORK

To Countermeasure the problem in existing system and to generate better result it is required to improve existing system or to improve external rules which is used as plug-in, we have proposed to Ontological knowledge base for snort attacks. As shown in figure 2 proposed architecture takes traffic from the particular source as an input. Now that input is given to snort and snort will check input with predefined rules.

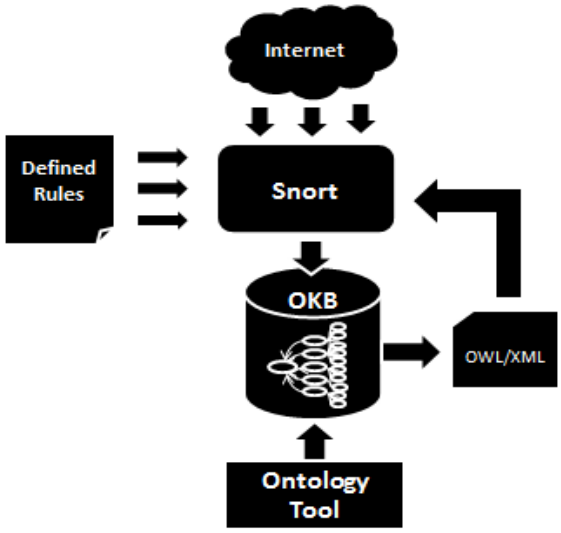

Figure 2: Proposed architecture

On the other hand protégé tool is used for generate Knowledge base of snort. In this way here we merge the two different things together and generate Ontological Knowledge Base. Now the output is saved as XML. We can fetch data from the file and improve rules using ontology. Improved rules are applied in snort as an external local rule[7]. We have created ontological knowledge base for snort. Using this ontological knowledge base we can modify default security policy rule and write our custom security policy rule for Snort.

III. IMPLEMENTATION DETAILS

First of all, Lets start our implementation work with creating different ontology for Snort. We used protégé tool[5] to create ontology. Following fig.3 shows graphical view of protégé while generating ontology for configured snort.

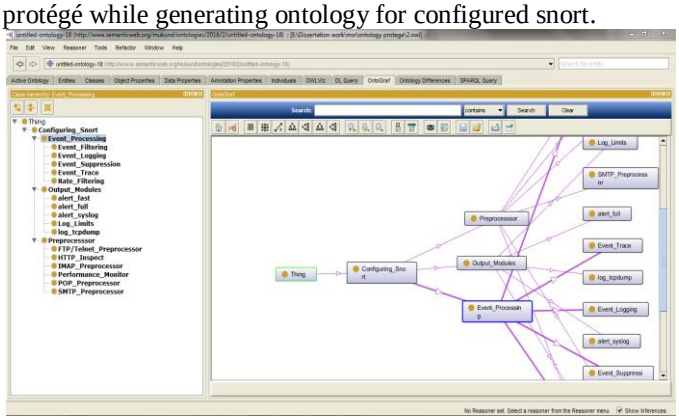

Figure 3: Ontology for Configuration of snort

From the given figure 4 tree base structure we can easily get how the flow is working, it will help users to identify how is the workflow going and working of snort configuration.

While generating ontology of configuring snort we take in to picture main three modules:

- Preprocessor
- Output Module
- Event processing

Each and every module has their own substructure which contains different entities, class, subclass, and relation with each other.

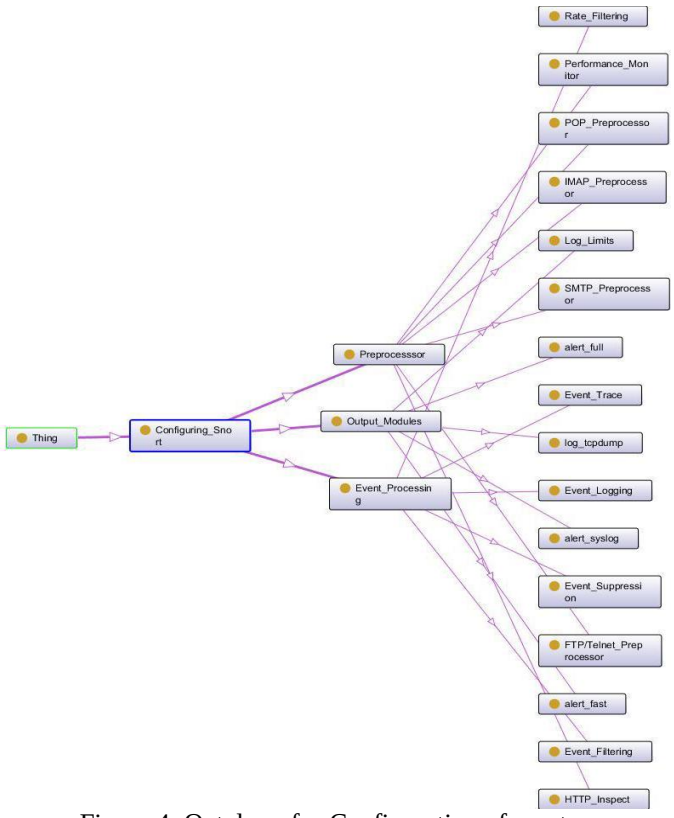

Figure 4: Ontology for Configuration of snort

Here DoS attack is represent the subclasses, all the subclasses are used in generation of improved rule. So improved rule contains rev, msg, metadata, reference, classtype, sid as well.

Figure 5 represents the ontology for DoS

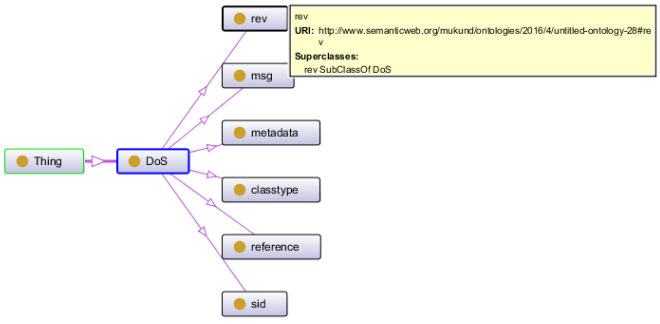

Figure 5: Ontology for DoS

Ontology of writing rules covered rules widely each and every single entities of rule is evaluated. For given example we have take msg, reference, gid, pid, rev, classtype, priority for the general rule option same way we have did it for payload detection rule option and non-payload detection rule option.

For improve rules, it is required to generate separate ontology for writing rule of snort. For that here figure 6 is shown below

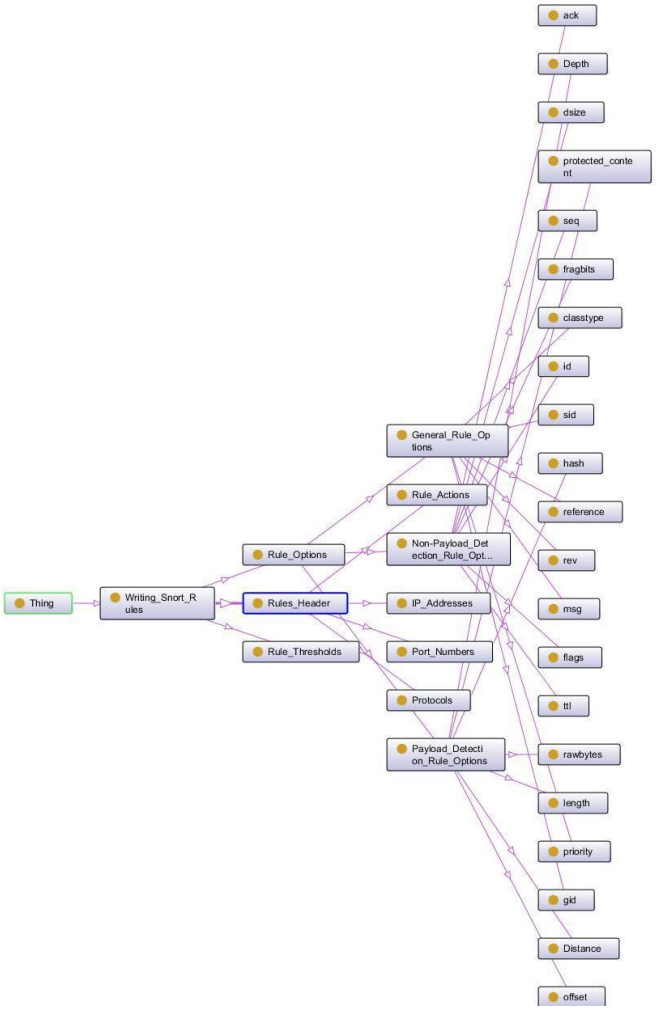

Figure 6: Ontology for writing snort rules

From the ontology generated improved rule is:

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"PROTOCOL-ICMP client check skillz"; icmp_id:666; itype:0; content:"skillz"; metadata:ruleset community; reference:cve,2000-0138; classtype:attempted-dos; sid:229; rev:12;)

Now the improve rules to be included in local rules file which is situated /etc/snort/rules/local.rules

To start snort we have to use given command

@Kali: /etc/init.d/snort start

Initialization of snort is shown in Figure 7:

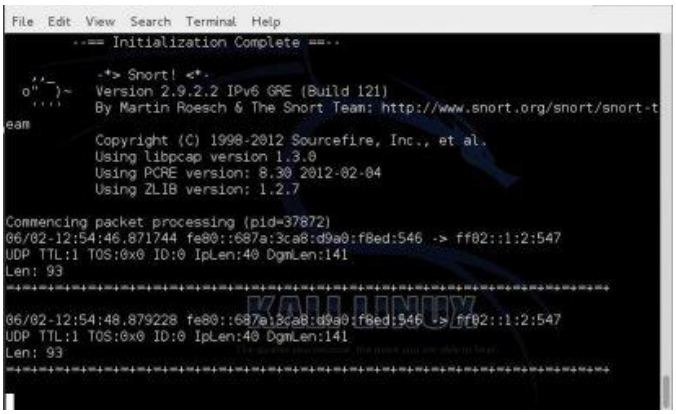

Figure 7: Initialization of snort services

Now detection of snort command is shown in figure 8.

@kali: snort A console -q I eth0 c /etc/snort/snort.conf

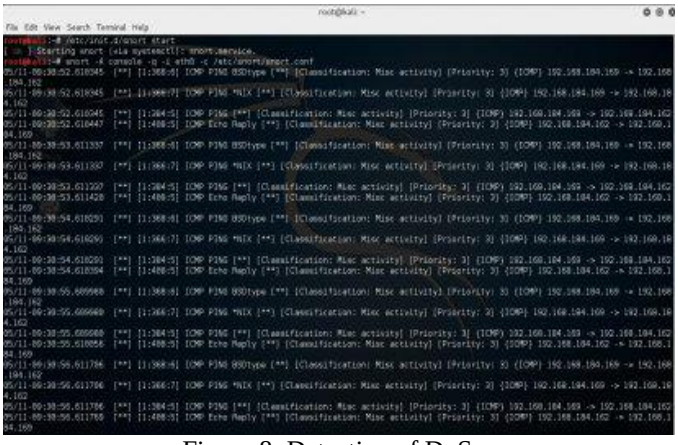

Figure 8: Detection of DoS

IV. TEST OUTCOMES

First of all we are going to implement DoS attack with both of the scenario, for that we have to set up a DoS attack on particular IP address. We can use any DoS attack tool like LOIC. But for our scenario we have used to send N numbers of packet on particular IP address. While we are sending that much packets it means DoS attack is in progress. So let's check the both scenario.

In first scenario i.e. In Existing system, we have performed DoS attack and detect it through the Snort community rules which is provided by the snort.org and it detect wide number of packets i.e. 1045 packets/sec. Which also have some burger alarm also so the accuracy is lower.

In second scenario i.e. In Proposed architecture, to overcome different issues regarding to security policy rule we have created Ontological Knowledgebase of DoS. We have performed same attack as performed in scenario 2 DoS attack using same method. We have also created one specific DoS attack ontology. Using DoS Ontological Knowledgebase and DoS attack ontology we have created custom security policy rule of DoS. We have written our

custom security policy rule in local.rules file. As a result we came to know that our custom security policy rule works and detects DoS attack based on signature matched data. DoS ICMP request is also collected as log file. Packet capturing is fast for this result is fast as compare to the existing system. Here we have capture 958 packets/sec. False-positive rate decrease. So proposed method is more accurate than existing system.

V. CONCLUSION AND FUTURE WORK

We have proposed an approach of using ontology modeling to represent snort configuration knowledge for the administrator. Our ontological knowledgebase of Snort and DoS effectively represents the semantic knowledge behind Snort configurations for the administrator in writing, editing and updating Snort configuration and helps him in inferring high level security policies from firewall configurations. Our ontological knowledgebase can also help administrator in identifying redundant, partially overlapping rules and helps in generating efficient rule sets for Snort. We have create specific attack ontology for DoS attack. Using DoS Snort IDS ontological knowledgebase and specific ontology for DoS, we have modify default rule of snort and made one custom security policy rule for snort rule to prevent from attack i.e. DoS. On the basis of our proposed work we conclude that ontology is kind of new concept and by using ontological knowledge base administrator can be easily write security policy rules to protect server from different attacks. Our custom security policy rule is work and it can be easily understand.

In future, we can create lots of rules for each and every attack but its take wide area in consideration. To overcome this problem user can create a tool which takes input from the ontology and give an output in the form of rule. Which help us for generating more rules.

Acknowledgment
I am highly take immense pleasure in thanking to Prof. Tejendra Thakur, for constantly guiding me and showing me the correct path to reach my desired goal. I would like to express my gratitude towards Mr. Nareshkumar Gardas and Mr. Bhadreshsinh Gohil for their kind co-operation and encouragement.

REFERENCES

[1] Zahraa Al-Mousa and Qassim Nasir, "A Cloud Computing Based Cooperative Intrusion Detection and Prevention System Framework", 2015 Springer International Publishing Switzerland, 2015.
[2] Emhimed Alatrish, "Comparision Some of Ontology Editors", 2013 Management Information system 2013.
[3] The Definition of Intrusion Detection System. http://www.authorbopedia.com/TERM/I/intrusion detection system.htmlin Web Applications".
[4] Benjamin, Perakath C.; Menzel, Christopher P.; Mayer, Richard J.; Fillion, Florence; Futrell, Michael T.; deWitte, Paula S.; Lingineni, Madhavi (September 21, 1994). "IDEF5 Method Report" (PDF). Knowledge Based Systems, Inc.
[5] James Stanger "How to cheat at Securing Linux": Book, Member of Comp TIA's Linux+.
[6] Nattawat Khamphkdee, Nunnapus Benjamas, Saiyan Saiyod "Improving Intrusion Detection System Based on Snort Rules for Network Probe Attack Detection" 2014 2nd International Conference on Information and Communication Technology (ICoICT).
[7] Emhimed Alatrash "Using Web Tools for Constructing an Ontology of Different Natural Languages", Mathematics University of Belgrade.
[8] Gruber, T. (2001) "What is an Ontology?", Stanford University Retrieved 2009-11-09.
[9] Snort Intrusion Detection, http://www.techrepublic.com/article/using-snort-for-intrusion-detection
[10] https://nsfocusblog.com/2015/08/05/evolution-of-ddos-attack-tools/

