Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 88-97
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.004

Automatic Spotting of Sceptical Activity with Visualization Using Elastic Cluster for Network Traffic in Educational Campus

Dr. Suma V
Dean,
Research and Industry Incubation Center and Department of Information Science and Engineering,
Dayananda Sagar Engineering College,
Bangalore, India
E-mail id: suma-ise@dayanandasagar.edu

Abstract: An automatic sceptical recognition model to identify the suspicious or the malicious activity in the network of the educational institutional campus is laid out in the paper. The carried out work in the paper kindles the network traffic flow in the educational campus and identifies the unwanted activities and stops them. The detected activities are visualized in the real time using a personalized reportage dash board. The design integrates the open source tools to provide an accurate evaluation utilizing the engine for the identifying and preventing the suspicious activities. The suspicious events identified are computed in the elastic cluster to visualize the intimidations. The laid out model computes the events identified and raises alarms. The elastic cluster founded on the No-SQL reports the happenings occurring in real time. The system is initially allowed to learn the various type of network attacks, once trained it the designed model automatically stops the malicious activities in the network traffic. This enhances the security for the campus networks by utilizing the open source libraries as well as minimizes cost imposed by the commercial identification and the prevention system.

Keywords: Sceptical Activity, Elastic Cluster, Automatic Threat Detection, Network Traffic, Educational Campus

1. Introduction

Nowadays the malicious events across the network has heightened due to its security breaches. Almost all the organizations, industries and the institutions affected by such intrusions and the suspicious activity affecting the proper network operation causing malfunctioning and hacking of information or modifying the information's. So there arises a need for finding the measures to safeguard the network as well as the data flowing through it in order to minimize the menace. Few safe guarding measures undertaken are application of "security policies" that regulate the entire system operations as a portion of its "IT policies".

The aspects inspecting the activities of the system confirms the pervious happenings and the way it has occurred with regard to the information gathered from the identification system. The apparatus gathers the details and distinguishes the one that violates the security. The packets transmitted are taken in to

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 88-97
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.004

consideration as the fundamental element for the application of the identification system in the network as well as for carrying out the "security information and event handling along with envisage. All institutions in common has applied the "intrusion detection system" in the network to track the network actions and intimate the violations reports.

The fundamental responsibilities of the "Intrusion identification system" is to identify and as well as intimate the suspicious, annoying action taking place in the network by providing alarms. But the malicious activities taking place today are adaptable to the "intrusion detection system" so the "IDS" prevailing turns out to be ineffective for today's malicious network actions. So the prevailing IDS was enhanced including the prevention system into it. The prevention system is just an enhancement of the IDS including "improved fire wall methodologies" to eliminate the menace in the network. This allows the decision on the access control to be made according to the content of the application instead of the making decisions using the "port and the internet protocol address". The network tracking employing the detection and the protection system is termed as a cost- effective method of discovering the unwanted entries and as well as stopping them to avoid the malfunctioning of the network and the hacking in the network.

For this the proposed model designs a frame work with the centralized network data and activity manager (NDAM) to handle the traffic in the network and evaluate the vulnerability of the network and as well as interpret and envisage the captured information's on the dashboard that could be personalized according demand of the overseer of the network. The key objectives that eh work emphasis on is as follows.

- Configure an "intrusion detection and prevention system" as well as the centralized-NDAM using the open source tools as the salable result existing in the market are very expensive.
- Envisages the detected information into a personalized dash board that is altered according to the requirements of the network overseer.
- Tests the designed model by subjecting it to a real time analysis of the network traffic that flows in the educational campus.

The paper remaining is laid out with the related works in section 2, proposed model designing in section 3, the performance validation in section 4 and conclusion in section 5.

2. Related Works

Waagsnes, et al [1] has performed the "SCADA intrusion detection system evaluation model simulating the SCADA traffic to identify the dangerous actions taking place in the network. the model integrates

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 88-97
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.004

various prevailing components such as the kali, linux, conpot, Qtester104 and the openMUC in virtual machine based frame work to deliver a SCADA traffic in the real time" Khamphakdee, et al [2] proposes an Snort-IDS that uses the rules to identifying the data packets traffic identical to the rules. On identifying the frame work generates the alerts to the network, the proposed model is an improvement of the SNORT-IDS to elude the generation of the incorrect warnings.

Mugunthan, S. R et al [3] and et al [4] has devised a "Security and Privacy Preserving of Sensor Data Localization Based on Internet of Things" and "Soft Computing Based Autonomous Low Rate Ddos Attack Detection and Security for Cloud Computing." Suma, V. et al [5] has proposed a "Security and Privacy Mechanism Using Blockchain." Anguraj et al [6] has performed the Trust-based intrusion detection and clustering approach for wireless body area networks."

Haoxiang, Wang et al [7] has conducted a "Trust Management of Communication Architectures of Internet of Things." Bhalaji, N.et al [8] has proposed the "Efficient and Secure Data Utilization in Mobile Edge Computing by Data Replication." Smys, S et al [9] has performed the "DDOS Attack Detection in Telecommunication Network Using Machine Learning."

Sathesh, A.et al [10] has devised an "Enhanced Soft Computing Approaches for Intrusion Detection Schemes in Social Media Networks." Bashar, et al [11] has proposed a "Secure and Cost Efficient Implementation of the Mobile Computing Using Offloading Technique." Francisquelo et al [12] has put forth the "ELK stack Big Data visualitzation using D3 library." The guide for the elastic cluster is presented in [13] Gormley et al [14] has proposed the "Elastic search: the definitive guide: a distributed real-time search and analytics engine. "And the tutorial of the elastic cluster is presented in [15]

3. Technology Applied

The configurations starts by initializing the intrusion identifying and stopping system (IIDSS) along with the centralized-NDAM. The tracker in the IIDSS gathers the actions in all the network traffic that flows across the network in the educational institution campus. The unwanted traffic in the network are detected by utilizing the rules along with the signatures. For this the traffic in the network that is equal or matches the malicious activity are detected based on the rules and the signatures and the intimation is sent. The model for the IIDSS is designed with the capability to assist the multi-threaded processor and the hardware operations in order to identify the network traffic evaluation with the heightened swiftness and the efficacy.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 88-97
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.004

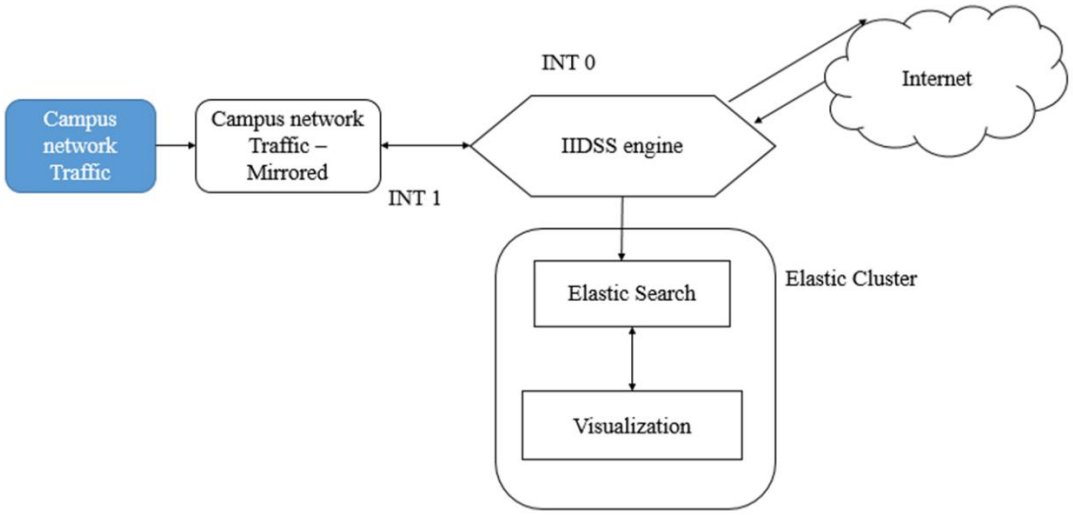


Figure.1 Flow Diagram for Threat detection

As shown in figure.1 the inlet and the outlet network traffic of an educational campus from its main switch is replicated to the interface (INT 1) of the IDSS engine. The replicated information's are computed in the IIDSS to activate warnings if identified with the malicious packet in the network. The packets captivated are compared with the rules clubbed with signatures and then the warning is initiated. These warnings are preserved as "log file". As the Logs stored are very important attribute for all the security devices. The designed structure must be competent of preserving the logs in diverse formats. The proposed design is set up with the capacity to preserve logs in the "java script object notation" format. The JSON is preferred due to its features such as "light weight data-interchangeable format and the preservation of the data doesn't demand and relational database.

The information stored in the form of logs are "parsed, indexed and stored" by the elastic cluster encompassed with the Kibana, log-stash, file-beat and elastic-search. These tools develop and envisage the captured information of the packets in the personalized dash board. The depiction of the network activities in the dash board enables one to swiftly gain knowledge about the vulnerabilities in the potential network. Thus assisting in describing the various networks actions that are to be stooped from further propagation into the network.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 88-97
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.004

3.1. Practical Configuration

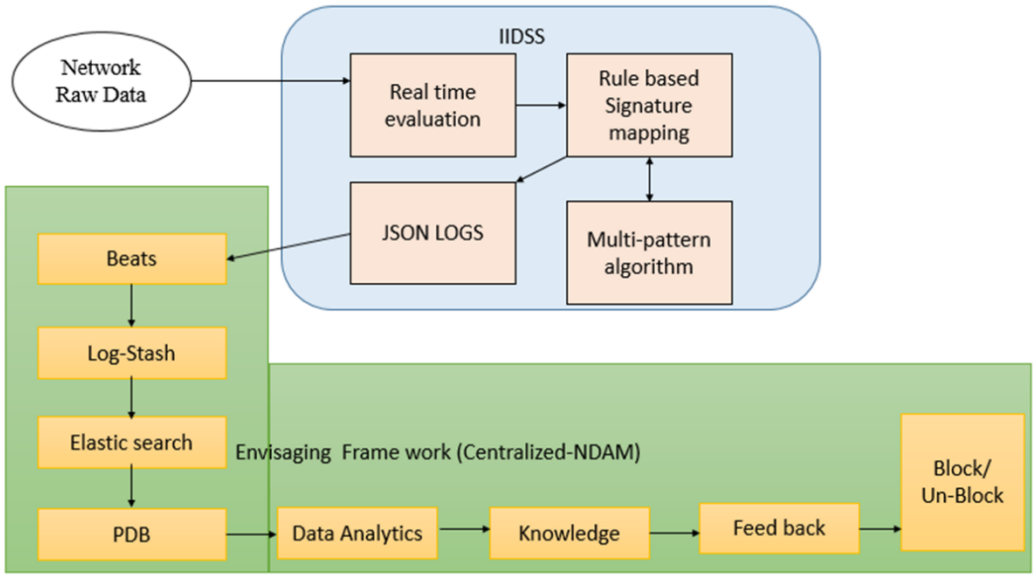


Figure.2 Configuration of IIDSS and Centralized-NDAM

The local area networks main switch of the in the institutional area is set up with the replication port to IIDSS in order to capture the packets flowing in the network. The complete set up of the IIDSS is shown in figure. 2. The hardware necessary for the set up and the tools used in the design are elaborated in the table.1 below.

Hardware and Software Used	Description
Processor	Intel (R), Xeon (R), E5-1620@ 3.60 GHz
Core	16
RAM	64
HDD	2 TB
Storage	64 bits
Open software's	Ubuntu, Suricata, Snort, beats , Log-stash, Elastic search , Kibana

Table .1 Hardware and software Used

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 88-97
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.004

The setup done is capable of gathering the network traffic in online and in offline. Thus enabling the overseer to evaluate the traffic in the network and also refine or calibrate the configurations of the network according to the institutional demands. The significant parts in the configuration is the data packet accumulator, IIDSS and the centralized-NDAM

The main switch which is a “cisco catalyst” directs the packets for identifying as well as stopping the unwanted events taking place to the IIDSS, which is created by the “open information security foundation” it is the core part of the designed system, this is a “rule- centered IDS” that is transformed into ISS that utilizes the outwardly framed set of rules with the warning signature to track the traffic in the network. The warning is triggered only on identifying a suspicious activity. Complicated menace are identified swiftly by the “warning signature relied set of rules” by employing the “multi-pattern matching algorithm” that heightens the rate of identification. The computing system for the packet integrates the procedures while obtaining the networks packets. The distinguished decoder enables the inspection of the data sequence in the application layer and later applies it to the identification strings. The inlet as well as the outlet packets are filtered and preserved in form of logs. To further enhance the process the elastic clustering with the tools that are open source are used in the system. Information is transformed into a human understandable form using the elastic cluster that are used in envisaging the details gathered into dash board representations

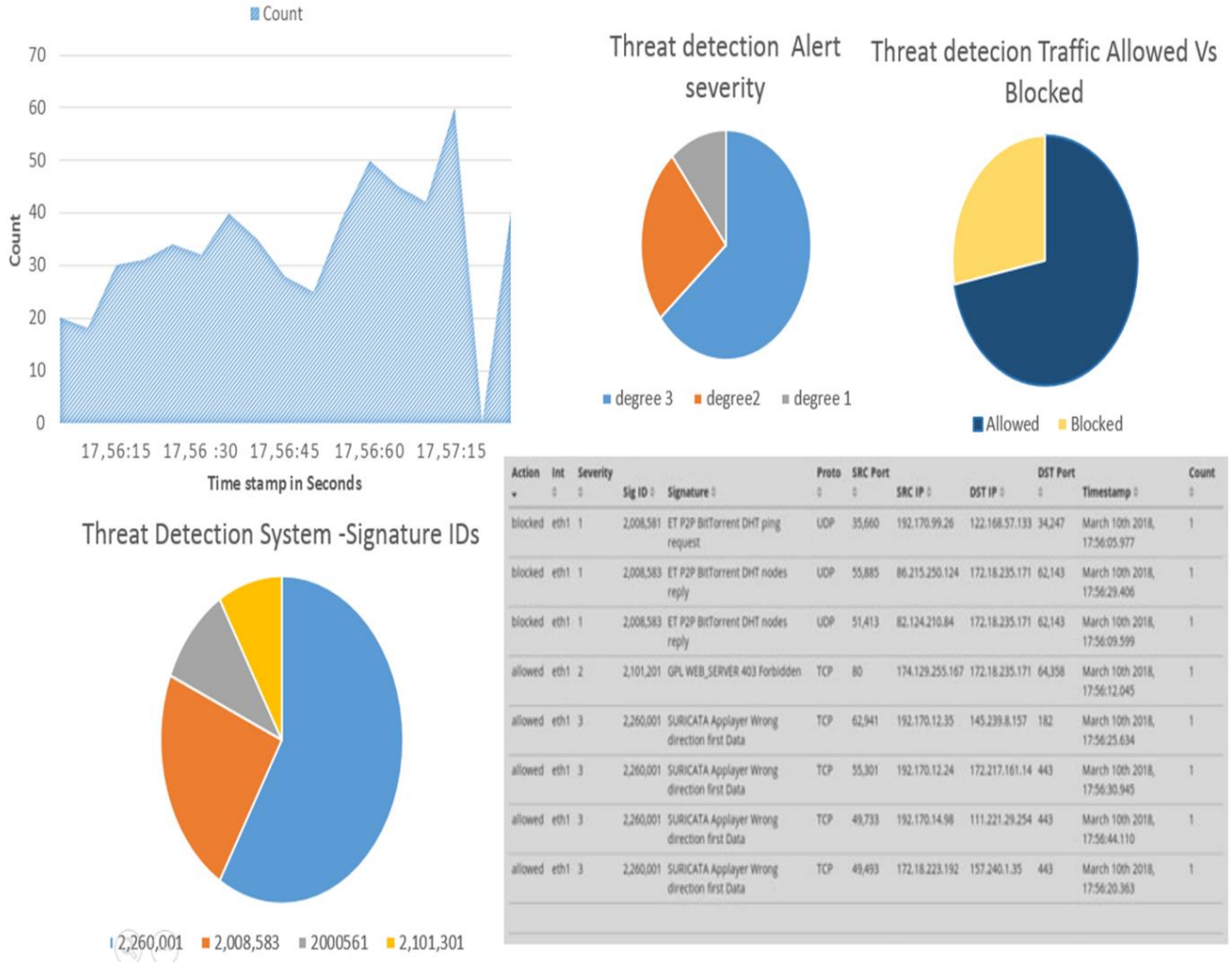
4. Performance Evaluation

The system designed is evaluated in real time with the educational institution holding more than 5500 LAN and wireless network clients. The competency of the designed system is comprehended by the identification of the menace across the networks and it envisage in the personalized dash board.

The complete system is validated by subjecting it to monitor the network for about 5 months day and night without any interruption in between. The information gathered were depicted in the form of personalized dash board (PDB) the degree of security was segregated into three stages with the as degree 1 2 and 3 each stage reported different amount of malicious activities such as 6,00,000,5,00,0000, and 4,00,000 respectively. The dash board depicted the attacks the link courts are displayed in 40s chart and the heightened count is understood as the unwanted action in the network. ie if the UDP goes high then it is intimated as unwanted activity taking place in network and if the TCP is high it is considered to be normal. The dash board in the figure. 3 depicts the IIDSS.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 88-97
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.004



Action	Int	Severity	Sig ID	Signature	Proto	SRC Port	SRC IP	DST IP	DST Port	Timestamp	Count
blocked	eth1	1	2,008,581	ET P2P BitTorrent DHT ping request	UDP	35,660	192.170.99.26	122.168.57.133	34,247	March 10th 2018, 17:56:05.977	1
blocked	eth1	1	2,008,583	ET P2P BitTorrent DHT nodes reply	UDP	55,885	86.215.250.124	172.18.235.171	62,143	March 10th 2018, 17:56:29.406	1
blocked	eth1	1	2,008,583	ET P2P BitTorrent DHT nodes reply	UDP	51,413	82.124.210.84	172.18.235.171	62,143	March 10th 2018, 17:56:09.599	1
allowed	eth1	2	2,101,201	GPL WEB_SERVER 403 Forbidden	TCP	80	174.129.255.167	172.18.235.171	64,358	March 10th 2018, 17:56:12.045	1
allowed	eth1	3	2,260,001	SURICATA Applayer Wrong direction first Data	TCP	62,941	192.170.12.35	145.239.8.157	182	March 10th 2018, 17:56:25.634	1
allowed	eth1	3	2,260,001	SURICATA Applayer Wrong direction first Data	TCP	55,301	192.170.12.24	172.217.161.14	443	March 10th 2018, 17:56:30.945	1
allowed	eth1	3	2,260,001	SURICATA Applayer Wrong direction first Data	TCP	49,733	192.170.14.98	111.221.29.254	443	March 10th 2018, 17:56:44.110	1
allowed	eth1	3	2,260,001	SURICATA Applayer Wrong direction first Data	TCP	49,493	172.18.223.192	157.240.1.35	443	March 10th 2018, 17:56:20.363	1

Figure.3 IIDSS Visualization

The CPU utilization and the for the system designed in identifying the threats at regular intervals displayed below in figure.4 this enables to note down the hardware consumption of the system designed while subjected to real time network traffic tracking.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 88-97
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.004

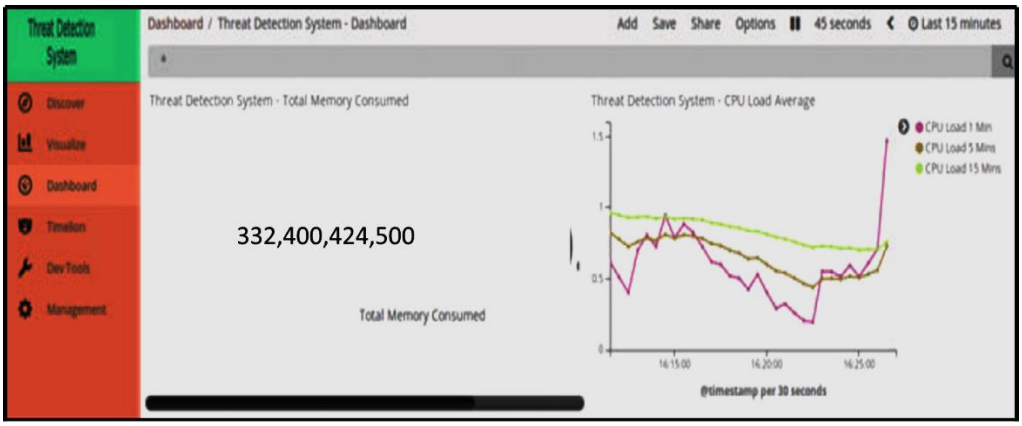
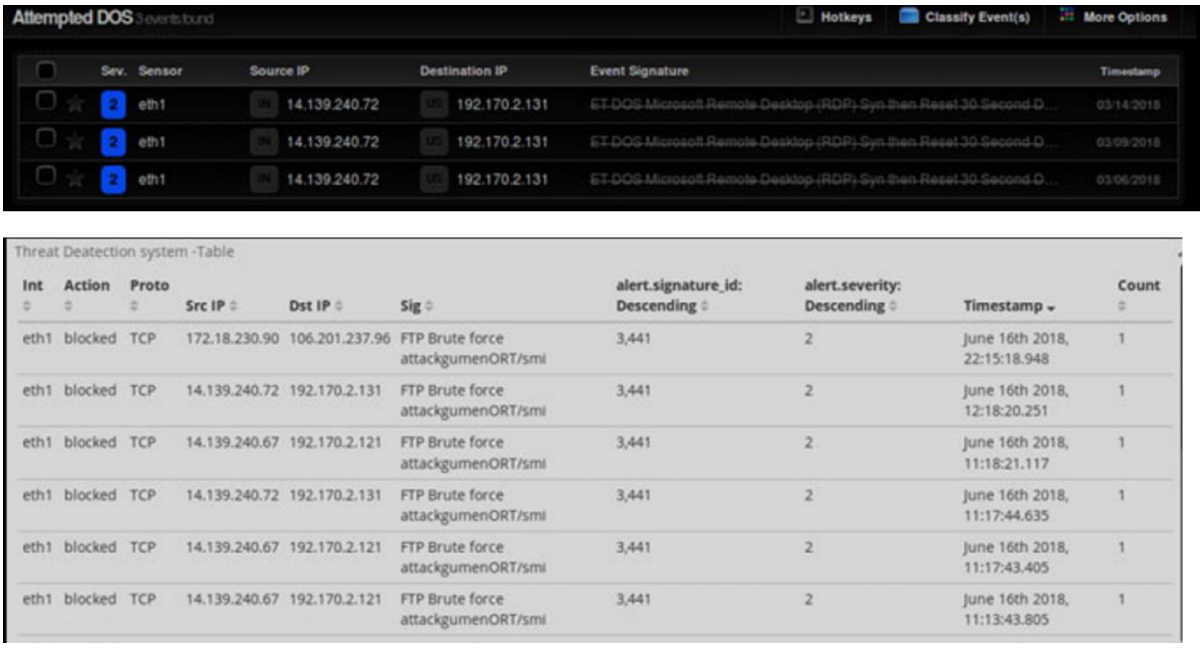


Figure.4 CPU load and Memory Utilization.

The particulars of the other attack that were identified was also visualized as shown in the figure.5, some of the other attacks observed were DDOS, Brute force, etc. the remedies taken by the IIDSS shows that the attacks are blocked from further propagation into the network.



Int	Action	Proto	Src IP	Dst IP	Sig	alert.signature_id: Descending	alert.severity: Descending	Timestamp	Count
eth1	blocked	TCP	172.18.230.90	106.201.237.96	FTP Brute force attackgumenORT/smi	3,441	2	June 16th 2018, 22:15:18.948	1
eth1	blocked	TCP	14.139.240.72	192.170.2.131	FTP Brute force attackgumenORT/smi	3,441	2	June 16th 2018, 12:18:20.251	1
eth1	blocked	TCP	14.139.240.67	192.170.2.121	FTP Brute force attackgumenORT/smi	3,441	2	June 16th 2018, 11:18:21.117	1
eth1	blocked	TCP	14.139.240.72	192.170.2.131	FTP Brute force attackgumenORT/smi	3,441	2	June 16th 2018, 11:17:44.635	1
eth1	blocked	TCP	14.139.240.67	192.170.2.121	FTP Brute force attackgumenORT/smi	3,441	2	June 16th 2018, 11:17:43.405	1
eth1	blocked	TCP	14.139.240.67	192.170.2.121	FTP Brute force attackgumenORT/smi	3,441	2	June 16th 2018, 11:13:43.805	1

Figure. 5 Other Attacks Observed

ISSN: 2582-337X (online)

Ubiquitous Computing & Communication Technologies

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 88-97
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.004

5. Conclusion

The designed system is competent enough to track and identify the various sorts of endangered actions of the networks from a real time observation performed over a network that is compromised. The system was capable enough to classify the more than 40 lakhs attacks over a duration of 5months according to the severity degree. While validation it was found that the system stopped certain attacks from propagating into network automatically. Although those attacks did not have high frequencies. The Centralized-NDAM envisaged the endangered identified menace over the PDB, initially the system is trained and after training tit is subjected to block the attacks based on its degree of severity. The developed frame work was tested over an educational campus that had more than 5500 local area network and wireless connection. To secure the network and cut down the expenses on employing a commercial-identification and stopping system.

References

[1] Waagsnes, Henrik, and Nils Ulltveit-Moe. "Intrusion Detection System Test Framework for SCADA Systems." In *ICISSP*, pp. 275-285. 2018.

[2] Khamphakdee, Nattawat, Nunnapus Benjamas, and Saiyan Saiyod. "Improving intrusion detection system based on snort rules for network probe attacks detection with association rules technique of data mining." *Journal of ICT Research and Applications* 8, no. 3 (2015): 234-250.

[3] Mugunthan, S. R. "Security and Privacy Preserving Of Sensor Data Localization Based On Internet of Things." *Journal of ISMAC* 1, no. 02 (2019): 81-91.

[4] Mugunthan, S. R. "Soft Computing Based Autonomous Low Rate Ddos Attack Detection and Security For Cloud Computing." *Journal of Soft Computing Paradigm (JSCP)* 1, no. 02 (2019): 80-90.

[5] Suma, V. "Security and Privacy Mechanism Using Blockchain." Journal of Ubiquitous Computing and Communication Technologies (UCCT) 1, no. 01 (2019): 45-54.

[6] Anguraj, Dinesh Kumar, and S. Smys. "Trust-based intrusion detection and clustering approach for wireless body area networks." *Wireless Personal Communications* 104, no. 1 (2019): 1-20.

[7] Haoxiang, Wang. "Trust Management of Communication Architectures of Internet of Things." *Journal of trends in Computer Science and Smart technology (TCSST)* 1, no. 02 (2019): 121-130.

[8] Bhalaji, N. "Efficient and Secure Data Utilization in Mobile Edge Computing By Data Replication." Journal of ISMAC 2, no. 01 (2020): 205-216.

[9] Smys, S. "DDOS Attack Detection In Telecommunication Network Using Machine Learning." *Journal of Ubiquitous Computing and Communication Technologies (UCCT)* 1, no. 01 (2019): 33-44.

ISSN: 2582-337X (online)

[10] Sathesh, A. "Enhanced Soft Computing Approaches for Intrusion Detection Schemes in Social Media Networks." *Journal of Soft Computing Paradigm (JSCP)* 1, no. 02 (2019): 69-79.
[11] Bashar, Abul. "Secure And Cost Efficient Implementation Of The Mobile Computing Using Offloading Technique." *Journal of Information Technology* 1, no. 01 (2019): 48-57.
[12] Francisquelo Tacca, Nicolas Ernesto. "ELK stack Big Data visualitzation using D3 library." Bachelor's thesis, Universitat Politècnica de Catalunya, 2019.
[13] https://www.elastic.co/guide/en/elasticsearch/reference/current/add-elasticsearch-nodes.html
[14] Gormley, Clinton, and Zachary Tong. *Elasticsearch: the definitive guide: a distributed real-time search and analytics engine*. " O'Reilly Media, Inc.", 2015.
[15] https://dzone.com/articles/elasticsearch-tutorial-creating-an-elasticsearch-c

Authors Biography

Dr. Suma V. holds a B.E. in Information Science and Technology, M.S. in Software Systems and Ph.D. in Computer Science and Engineering. Currently, she is working as Dean of the Research and Industry Incubation Centre, and a Professor at the Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, India. She has more than 17 years of teaching experience and has published over 180 papers, including research articles published in leading international journals, such as ACM, ASQ, Crosstalk, IET Software, and journals published by MIT and Dartmouth College in the USA. Her research has also been published on NASA, UNI Trier, Microsoft, CERN, IEEE, ACM and Springer portals.

ISSN: 2582-337X (online)