International Journal of Applied Engineering Research Transaction
ISSN Print : xxxx-xxxx | ISSN Online : xxxx-xxxx
Frequency : Quarterly
Language : English
Website:

INTERNATIONAL JOURNAL OF APPLIED ENGINEERING RESEARCH TRANSACTION
Abbreviated Key title: Int. J. Appl. Eng. Res. Trans
(An Open Access Peer Reviewed Multilingual International Journal)
ISSN: XXXX-XXXX (Print)
ISSN: XXXX-XXXX (Online)

Reseach Article

Photodegradation of Olive Mill Wastewaters Using Graphene-Tio$_2$ and Recovery of Graphene-Tio$_2$

Muazu Dalhatu Sifawa, Bello Alhaji Buhari and Lawal Sulaiman

Department of Mathematics Computer Science Unit Usmanu Danfodiyo University Sokoto,Nigeria

***Corresponding Author**
Muazu Dalhatu Sifawa

Article History: | Received: 20.06.2022 | Accepted: 24.07.2022 | Published: 25.08.2022|

Abstract: The increasingly frequent attacks on Internet visible systems are attempts to breach or compromise the security of those systems. Network security issues have been a major challenge on Usmanu Danfodiyo University networks for a long time. Intrusion detection technology allows organizations to protect themselves from losses associated with network security challenges. The aim and objectives of this project is to deploy and evaluate the performance of SNORT-IDS in safeguarding demilitarize zone network segment of Usmanu Danfodiyo University. SNORT-IDS were implemented using some various tools such as Snort Application, Pulledpork, Barnyard, Apache, MySQL, PHP, BASE, and ADODB. The result obtained from the system evaluation indicates that Snort-ids system is able to detect attack at the rate of 96.24%.

Keywords: Intrusion Detection System, Snort-IDS, Demilitarized Zone, Detection Rate.

INTRODUCTION

I. Introduction

Systems and networks are subject to electronic attacks. Today's information systems in government and commercial sectors are distributed and highly interconnected via local area and wide area networks. While indispensable, these networks provide potential avenues of attack by hackers, international competitors, and other adversaries. The increasingly frequent attacks on Internet visible systems are attempts to breach or compromise the security of those systems. Intrusion detection technology allows organizations to protect themselves from losses associated with network security problems (Mohapatra, 2005). Intrusion Detection System (IDS) are Hardware and Software Systems that monitor events which occurred on computers and computer networks in order to analyze security problems. IDS have become a key component in ensuring the safety of systems and networks. Intrusions to computer networks are called ‘‘attacks” and these attacks threaten the security of networks by violating privacy, integrity and accessibility mechanisms (Scarfone & Mell, 2007). Attacks can originate from users who login to the computer using Internet trying to gain administrator rights and other users who misuse the rights they have. IDSs automate monitoring and analyzing the attacks (Bace & Mell, 2001). Intrusion detection systems are classified as either signature-based or anomaly-based. Signature-based schemes (also called as misuse-based) seek to defined patterns, or signatures, within the analyzed data. Anomaly-based IDSs analyses abnormal activities and flag these activities as attacks.

Snort intrusion detection system (IDS) combines both the benefits of signature-based and anomaly-based inspection. Snort is an open source network intrusion detection and prevention system (IDS/IPS) developed by Sourcefire. It is the most widely deployed IDS/IPS technology worldwide because it is free and open source application. With over 4 millions of downloads and over 500,000 registered users; It has become the de facto standard for IDS/IPS. Snort's network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified. Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk.

In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified. With the vast features of Snort and the meager university budget on IT infrastructure and software, Usmanu Danfodiyo University can utilize the benefit of Snort to safeguard their network with minimal cost.

Usmanu Danfodiyo University network is designed using fiber optic based backbone comprising of three rings on the 3 campuses: Permanent Site, City Campus, and College of Health Sciences (UDUTH) all the three campuses are connected. The network runs on Cisco and juniper Devices (Router, Firewall, CORE Switch, DMZ (demilitarize Zone) Switch, Split Switch, and Transparent Switch). The University Network is divided into two segments (LAN & DMZ network). All University client machines are connected to LAN network segment on CORE-Switch. However, all University Servers that hosted their services which are accessible in and outside their network are connected to DMZ (demilitarize Zone) Network segment.

In this Paper, Snort Intrusion Detection System (Snort-IDS) will be deploy on demilitarize Zone (DMZ) network segment of Usmanu Danfodiyo University to help in detecting any suspicious traffic thereby safeguarding their servers.

II. Related works

Several researchers have proposed different approaches and models to address the various types of security breaches of computer network and computer systems. Some previous works reviewed are presented as follows:

Yi & Zhang(2010)proposed an implementation of a campus network security system based on distributed network intrusion detection technology. The system is designed using Protocol Analysis and Pattern Matching detection methods to improve the accuracy of intrusion detection and efficiency. It integrated a variety of attack detection technologies (such as data capture module, the data server module, secure communications module and the response module) which effectively detect different type of attacks. The system is able to detect and analyzed malicious behavior through data capture module from the packet capture, protocol analysis, and pattern matching. The weakness of this work is that it only detects remote attacks. The work can be improved to detect both remote attacks and local attacks within the network. Many local hackers hide their identity and compromise the security of the organizational network resources.

Xiong & Peng (2012) proposed a distributed Snort Intrusion detection system model applying protocol analysis and pattern matching detecting method in order to improve the speed and accuracy of Snort intrusion detection system. It consists of three-layer structure: the sensor, data management Centre and the management decision center. Sensor collects data from the network, while the data management Centre collects the alarm information for storage and classification of the alarm. The data management Centre collects and analyze alarm information. the result of the system test shows clearly that the applications of campus network security have been improved effectively through the implementation of distributed Snort Intrusion detection system model, and also speed and accuracy of detecting attacks have been improved through the use of protocol analysis and pattern matching intrusion detecting methods. Protocol analysis use the network communication protocol of specific rules and analyzed the protocol information. Pattern machine compared protocol information with known network intrusion and system misused mode to find the violated behavior of the security policy. The weakness of the work is that the system collects and reacts to only intrusive packets with protocols on the network, any other intrusion that is not protocol wise will not be detected by the system.

Suman & Vikram (2013) proposed a security tool for intrusion detection in campus network environment using Snort. The system was configured in four modes; packet sniffer mode, packet logger mode, detection mode, and prevention mode. In this system, raw packets are captured using libcap and then decode forwarded to the detection engine. The detection engine then checks the header of this packets as well as payloads against multiple thousands of rules stored in the database of pre-defined attack signatures. The system is able to detect several attacks in system rule file such attacks are denial of service attack, ping attempt, and identity spoofing attack. Every type of attack contains multiple alerts related to a particular signature. It detects the number of sources that generate the attacks and the number of destinations that received the attacks. Every signature of attack has a unique Id and from that Id full detail about signature is known. However, analysis indicates that the system has detected 12 signatures among which ICMP ping attack signature has the maximum number of alerts. The weakness of the work is that, the system performance becomes down during heavy network traffic which can be improved by adding new algorithm called pre-processor to the snort detection engine to avoid packet dropping.

Garg (2014) proposed a hybrid intrusion detection system using SNORT in a Campus environment. In this system a new algorithm called pre-processor is added to the Snort detection engine to find the detection anomalies. This engine filters all the files and loads the attacked or infected files into its loader by .conf file command. The system is design using some tools (i.e. SNORT IDS, SNORT Rules, and Windows Operating System). The proposed System is called H-Snort (Hybrid Snort). The system is implemented by website that displays the system status (such as network traffic, detected anomalies, e.t.c) which allowed it to be configuring easily. the result of the system test indicates that several attacks on LAN network segment have been detected through detection engine which filters all the files and loads them into its loader by configuration (.conf) file. The limitation of the work is that the system is implemented only on LAN network segment which can be improved by implementing on DMZ network segment.

Considering the reviewed of the Garg (2014) work which focuses only on LAN network segment, our work will be focusing on deploying Snort intrusion detection system on demilitarized zone (DMZ) network segment of Usmanu Danfodiyo University Network.

III. RESEARCH METHODOLOGY

Quantitative research method was adopted to evaluate the performance of the Snort Intrusion Detection System (IDS) on demilitarized zone (DMZ) network segment of Usmanu Danfodiyo University. Two Network traffics will be captured, one from the system that initiated the attack, and another traffic from snort-ids system on DMZ network segment. Traffic to be capture on Snort-ids system will be comparing against suspicious traffic detected by Snort-Ids System. Detection rate metric will be used to evaluate the performance of Snort-Ids system to know the rate at which it is able to suspicious traffic.

IV. Experimental design

To evaluate the performance of the Snort Intrusion Detection System (IDS) on demilitarized zone (DMZ) network segment of Usmanu Danfodiyo University, A Snort Server will be configure and deploy on DMZ network segment. This Server will be connected to the DMZ Switch on interface (ether1), and a Console Monitoring port. The Console monitoring port will be used by network administrator for monitoring Intrusion activities detected by Snort through web browser. A comprehensive working Snort System utilizes these tools to provide a web-based user interface with a backend database.

- MySQL is used with Snort to log alert data.
- Apache acts as a web server.
- PHP is used as an interface between the web server and MySQL database.
- BASE (Basic Analysis and Security Engine) is a PHP package that is used to view and analyze Snort data using a web browser.
- Barnyard2-2-1.13 is a dedicated spooler that generates alerts from snort and send to MYSQL database that reduce load on the snort.
- Pulledpork-0.7.0 this will automatically download the latest rulesets from snort website.
- Image_Graph is used by BASE to create graph.
- ADODB is used by BASE to connect to MySQL database

V. system evaluation

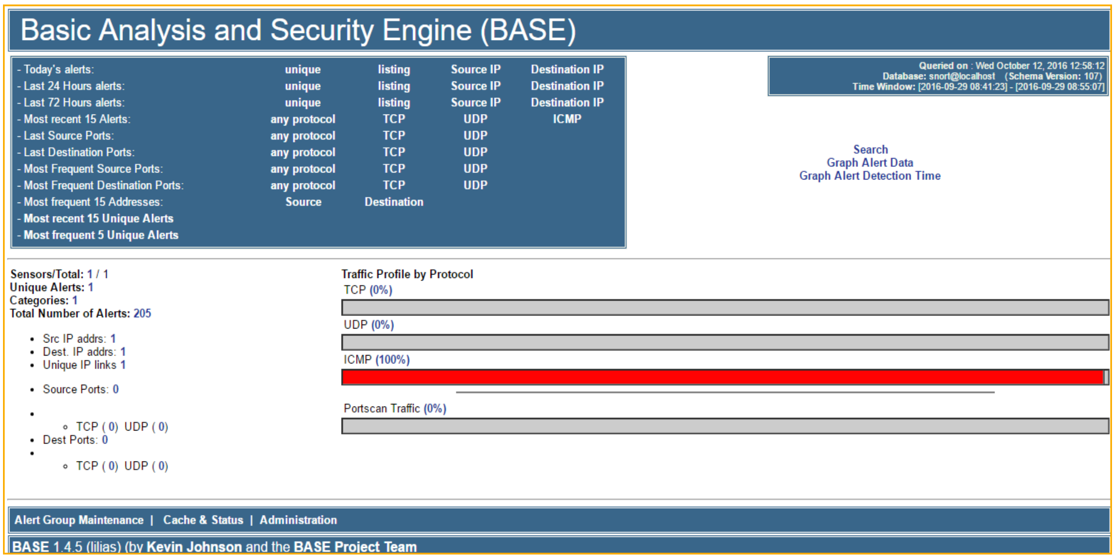
We initiated ping attack from System with 82.101.148.64 IP address to the Server with 41.78.224.44 IP address on DMZ network segment. These traffics were compared against the traffics captured on Snort-ids system using wireshark. However, Traffic captured from Snort-ids System is compared against suspicious traffics detected by Snort-ids. These traffics are shown in **Table4.1** and **Figure 4.1**.

Table 4.1: Summary of ICMP (Ping) Traffic captured on initiating system and traffic captured on Snort-ids system.

Application	**Initiating System**	**SNORT-IDS**	**% of Total Traffic**
ICMP (Ping)	213	213	100%
Total no. of Traffic	**213**	**213**	**100%**

From Table 4.1, 213 ICMP (Ping) traffic on Snort-ids system were captured out of 213 ICMP (Ping) traffics captured from initiating system for a period of 15 minutes. However, ICMP (Ping) traffic captured from Snort-ids system is 100% of total number of ICMP (Ping) traffic captured from the system that initiate the ping attack.

ICMP (Ping) traffic captured on Snort-Ids system initiated by System with 82.101.148.64 IP address to the Server with 41.78.224.44 IP address on DMZ network segment are compared against the number of ICMP (Ping) suspicious traffic detected by Snort-Ids system. This enable us to know how many traffic out of the total number of ICMP (Ping) traffic captured on Snort-Ids system were detected by itself. Figure 4.1 shows ICMP (Ping) attack traffic detected by Snort-Ids System:



Basic Analysis and Security Engine (BASE)

- Today's alerts:	unique	listing	Source IP	Destination IP
- Last 24 Hours alerts:	unique	listing	Source IP	Destination IP
- Last 72 Hours alerts:	unique	listing	Source IP	Destination IP
- Most recent 15 Alerts:	any protocol	TCP	UDP	ICMP
- Last Source Ports:	any protocol	TCP	UDP	
- Last Destination Ports:	any protocol	TCP	UDP	
- Most Frequent Source Ports:	any protocol	TCP	UDP	
- Most Frequent Destination Ports:	any protocol	TCP	UDP	
- Most frequent 15 Addresses:	Source	Destination		
- Most recent 15 Unique Alerts				
- Most frequent 5 Unique Alerts				

Queried on : Wed October 12, 2016 12:58:12
Database: snort@localhost (Schema Version: 107)
Time Window: [2016-09-29 08:41:23] - [2016-09-29 08:55:07]

Sensors/Total: 1 / 1
Unique Alerts: 1
Categories: 1
Total Number of Alerts: 205

- Src IP addrs: 1
- Dest. IP addrs: 1
- Unique IP links 1
- Source Ports: 0
-
  - TCP (0) UDP (0)
- Dest Ports: 0
-
  - TCP (0) UDP (0)

Traffic Profile by Protocol
TCP (0%)
UDP (0%)
ICMP (100%)
Portscan Traffic (0%)

BASE 1.4.5 (lilias) (by Kevin Johnson and the BASE Project Team

Figure 4.1: ICMP (Ping) suspicious traffic detected by Snort-ids

From Figure 4.1 above, 205 ICMP (Ping) suspicious traffic were detected by Snort-ids system within the period of 15 minutes.

Table 4.2: Comparison of Snort-ids suspicious traffics detected against the total no. of traffic captured passing through it.

Application	Traffic Captured from Snort-ids System	Suspicious Traffic Detected by Snort-ids System
ICMP (Ping)	213	205
Total no. of Traffic	**213**	**205**

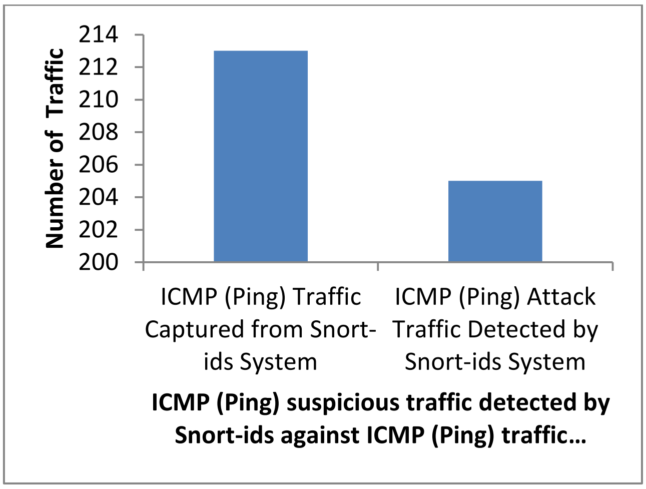


Figure 4.2: Comparison of Snort-ids suspicious traffics against the total no. of traffic captured from it.

As shown in Figure 4.2 and Table 4.2, based on the Rule specified in snort-ids system Rules File to detect remote Ping attack from initiating host with 82.101.148.64 IP address to server with 41.78.224.44 IP address on DMZ network segment, we ping 41.78.224.44 IP address for the period of 15 minutes. Snort-id system detects 205 ICMP (Ping) suspicious traffic out of 213 total numbers of ICMP (Ping) traffic captured from snort-ids system. To ensure the rate at which Snort-ids detected these suspicious traffics, we used Detection Rate Metric as follows:

$$DR=\frac{correctlydetectedattacks}{totalnumberoftraffics}*100$$

$$=\frac{205}{213}*100=96.24\%$$

From the detection rate (DR) computation, the rate at which Snort-ids correctly detect attack is 96.24% which shows that it is capable of detecting attacks by 96.24%.

VI. Conclusions

Usmanu Danfodiyo University DMZ network without Snort-IDS provide room for malicious traffics to pass through without been detected. Based on the traffics we captured using wireshark from DMZ network, it has clearly indicates that the security of Usmanu Danfodiyo University DMZ network can easily be compromise without Snort-ids system. SNORT IDS was implemented together with various tools such as

Snort Application, Pulledpork, Barnyard, Apache, MySQL, PHP, BASE, and ADODB to achieve web base intrusion detection system for analyzing intrusive attacks. The result obtained from the system evaluation indicates that Snort-ids systemis able to detect attack atthe rate of 96.24%. However, with Snort-ids on DMZ network segment of Usmanu Danfodiyo University, Suspicious traffic can easily be detected. Snort-ids serve as security mechanisms for Usmanu Danfodiyo University to safeguard their DMZ network segment to detect suspicious traffics with minimal cost.

REFERENCES

1. Deborah Estrin, Lewis Girod, Greg Pottie, and Mani Srivastava. Instrumenting the world with wireless sensor networks. In International Conference on Acoustics, Speech, and SignalProcessing, 2001.
2. Alberto Cerpa, Jeremy Elson, Deborah Estrin, Lewis Girod, Michael Hamilton, and Jerry Zhao. Habitat monitoring: Application driver for wireless communications technology. In ACM SIGCOMM Workshop on Data Communications in Latin America and the Caribbean, April 2001.
3. Jiagen Ding, Sing Yiu Cheung, Chin-Woo Tan, and Pravin Varaiya. Signal processing of sensor node data for vehicle detection. In International IEEE Conference on Intelligent Transportation Systems, October 2004.
4. Kredo, K. and P. Mohapatra, Medium access control in wireless sensor networks. Computer Networks, 2007. 51(4): p. 961-994.
5. W. Ye, J. Heidemann, and D. Estrin. An energy efficient mac protocol for wireless sensor networks.In 21st International Annual Joint Conference of theIEEE Computer and Communications Societies (INFOCOM’02), New York, NY, USA 2002.
6. T. van Dam and K. Langendoen. An adaptive energy efficient mac protocol for wireless sensor networks. In1st ACM Conference on Embedded Networked Sensor Systems (SenSys), pages 171–180, 2003.
7. Mao, J.L., et al., A novel energy-aware TDMA scheduling algorithm for wireless sensor networks. Wireless Algorithms, Systems, and Applications, Proceedings, 2006. 4138: p. 319-328.
8. Egea-Lopez, E., et al., A real-time MAC protocol for wireless sensor networks: Virtual TDMA for sensors (VTS). Architecture of Computing Systems - Arcs 2006, Proceedings, 2006. 3894: p. 382-396.
9. J.P. Sheu, C.H. Liu, S.L.Wu, and Y.C. Tseng, A PriorityMAC protocol to support real-time traffic in ad hoc networks, Wireless networks 10(January 2004) 61–69.
10. Paek, K.J., et al., Priority-based medium access control protocol for providing QoS in wireless sensor networks. Ieice Transactions on Information and Systems, 2007. E90d(9): p. 1448-1451.
11. Chen, J.M. and Y.X. Sun, Experiments study on a dynamic priority scheduling for wireless sensor networks. Mobile Ad-Hoc and Sensor Networks, Proceedings, 2005. 3794: p. 613-622.
12. Kwon, Y., Energy-efficient, traffic-adaptive, fast collision resolution MAC for WSNs. Ubiquitous Intelligence and Computing, Proceedings, 2006. 4159: p. 586-594.
13. Ren, B., et al., An energy-conserving and collision-free MAC protocol based on TDMA for wireless sensor networks. Mobile Ad-Hoc and Sensor Networks, Proceedings, 2005. 3794: p. 603-612.
14. Mao, J.L., Z.M. Wu, and X. Wu, A TDMA scheduling scheme for many-to-one communications in wireless sensor networks. Computer Communications, 2007. 30(4): p. 863-872.

Li Hongjun , born in 1979. Ph. D. candidate in National University of Defense Technology from China.

In recent years, networked control systems have been actively researched. MAC protocol is the elementary problem in the applications. His main research interests include wireless sensor networks and networked control system.

Li Xun, born in 1972. Ph. D. and associate professor in National University of Defense Technology. His main research interests include wireless network.

Ma Hongxu, born in 1966. Professor and Ph. D. supervisor in National University of Defense Technology. His main research interests include robot control and networked control system.