Monitoring and Evaluating Open Wireless LAN using Hybrid IDS

Mohd Mirza Abdul Malik [1*], Mohd Nizam Osman [2], Mushahadah Maghribi [3]
[1,2,3]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Perlis, 02600 Arau, Perlis, Malaysia
[3] Politeknik Tuanku Syed Sirajuddin, 026000 Arau, Perlis, Malaysia

*Corresponding author: *mohdnizam@uitm.edu.my*
Received Date: 6 October 2019
Accepted Date: 11 November 2019

ABSTRACT

In this ever-growing wireless technology era, the number of Open Wireless Local Area Network (WLAN) are on the rise. From cafes to shopping areas, most of them offer users with a free-to-use WLAN which popularly known as Open Wi-Fi or Wi-Fi Hotspots. Although it is a convenient for them to access the Internet at these places, later they know it also makes them a vulnerable target for attackers that might be lurking in the same network they are connected. Therefore, a Hybrid IDS that combines both SNORT, a network-based IDS (NIDS) and OSSEC, a host-based IDS (HIDS) was developed to curb the problem. NIDS was used to monitor network traffics while HIDS monitor user's system for any suspicious activities. Then, a system that can control and manage both IDS in the much easier and simpler way was developed using Python programming language. The system then can generate alerts with the help of both IDS to notify users for any suspicious activities that might occur in the network or user's system. Several attacks were launched from the attacker's laptop to test whether Hybrid IDS can generate alerts to notify the victim. As a result, the system breeze through the testing phase by showing necessary output. All the results were taken and then compared with other scenarios to determine whether they can give the same results as Hybrid IDS. From the comparison results, it can be said that Hybrid IDS can give the extra protection layer towards Open Wi-Fi users. Therefore, the Hybrid IDS was proven to provide vast tracking detection for suspicious activity in the network environments by monitor and alert the users about malicious activities.

Keywords: *WLAN, IDS, hybrid IDS, SNORT, OSSEC*

INTRODUCTION

Wireless Local Area Network (WLAN) allows devices such as computers and mobile phones to communicate over a wireless signal. One of the most known types of WLAN is Wi-Fi (short for "wireless fidelity"). It has become a popular technology and even close to become a basic need for humans today. Based on the statistic given by(Cisco, 2017), 94.0 million public hotspots in 2016 will increase to 541.6 million by the year 2021.

At this moment, many enterprises are offering wireless Internet-services to customers which can be seen mostly at the airports, cafes, restaurants and shopping areas. This free-to-use service may seem attractive for some people to use without thinking twice, but chances are the security levels on these networks can be arguably weak and lead to cyber-attacks.

For business owners, they might believe that they are providing a valuable service to their customers, but it can also lead them to man-in-the-middle attacks, malware distribution, snooping and sniffing attacks.

This is where Intrusion-Detection System (IDS) takes place to help people who are connected to the open Wi-Fi stay in the safe zone.

Intrusion-detection system or commonly known as IDS is a system that monitors packets entering and leaving in a network. The purpose of intrusion detection is to monitor network devices while detecting malicious activities in the network (Ashoor & Gore, 2011). IDS can give greater understanding of what really happened in a network by monitoring the packets. There are two different types of IDS; host-based IDS(HIDS) and network-based IDS(NIDS).

Protection against network-based threats using monitoring and analyzing network traffic is called Network-based Intrusion-Detection System or NIDS. Utilizing the network adapter running in the system, NIDS reads all raw inbound packets as data source and searches for any suspicious patterns in real-time as it travels across the network which typically referred to as "packet sniffers" (Am & Chezian, 2017).

Meanwhile, Host-Based Intrusion-Detection System (HIDS) is a very useful tool for understanding previous attacks and determining effective methods to defeat them in any networks or systems. The ability to monitor and respond to specific user actions and file accesses on the host makes the HIDS the best option to combat internal threats and malicious behaviors in networks. HIDS usually monitors the system, event, and security logs on Windows NT and syslog in Unix environments.

Nowadays, there are a lot of Intrusion-Detection Systems (IDS) that people as users can choose from in order to stay protected when connecting to Open WLANs. Open WLANs are easily exposed to cyber-criminal attacks than Private or Wired WLANs because they sometimes do not have any security protections. A cybercriminal can be defined as a real-world entity that tries to get unauthorized access and cause harmful activities in the system. Cyber-attacks have become more complicated and unpredictable as attackers are trying any possible way to successfully launch an attack towards the users without being detected(Wang & Zhu, 2017).

At the current moment, most of the host-based IDS or network-bases IDS that can be installed and used by users are flawed (Wang & Zhu, 2017). These flaws can be used by cyber-criminals to attack the system and with many IDS to choose from, users may face problems when choosing the right IDS to be installed on their computers or laptops.

IDS is a process used for monitoring and analyzing networks(K S, Kumar, & T S, 2014). It helps users to detect any malicious activity and alerts them to take actions that will protect their data from unwanted attacks. IDS can be installed as the both host-based and network-based intrusion-detection systems whereby each has its own strengths and weaknesses. Therefore, a hybrid intrusion-detection system with the strengths of both host-based and network-based can hopefully complement each other's weaknesses.

In this paper, the main sections are organized as follows: section 2 discusses the related work. In section 3, provides the methodology of the proposed work. Then, section 4 analyzes the results, and finally section 5 concludes the paper.

RELATED WORKS

Network Traffic Monitoring

Monitoring network traffic is a combination of several tasks such as process reviewing, analyzing and managing network traffic. These tasks are required to detect any abnormality or suspicious process that can affect network security, availability and performance.

One of the benefits from monitoring network traffic is detecting any malicious activity in the network. For example, network monitoring can be used to track attacker activities in a WLAN (Shum & Ng, 2010). Based on their findings, it is possible to detect hacking activities and location of a mobile user by monitoring the network traffics thus enhancing the information security. Meanwhile, the use of visualization techniques in network monitoring not only can reduce the time to observe network traffics but also gives essential information in a single picture(Safdar, Durad, & Alam, 2018). By using visualization in network monitoring, users can see clearly what actually happens in the network.

Intrusion Detection System (IDS)

Intrusion-Detection System (IDS) can be a host-based or a network-based ID. For many years, researchers have used either or maybe both types of IDS in their research in many related fields, including network monitoring. From a survey by (Am & Chezian, 2017), they have reviewed and studied different types of IDS and its corresponding tools. They come out with some notable points from their survey. For example, configuring the rules properly can lead to a higher detection rate, and several tools can only support small types of security threats and problems.

The packet losses issue has been identified by (Al-Dalky, Salah, Otrok, & Al-Qutayri, 2014) and they have proposed SNORT and NetFPGA combination to increase SNORT performance to analyses and filter packets. As a result, from their experiment combining both tools, SNORT has increased its performance and yields less packet losses even though there is an increase with traffic loads.

Meanwhile, (Wang & Zhu, 2017) have proposed a centralized Host-Based IDS (HIDS) framework for private cloud as it is becoming more efficient and convenient for the users. They want to overcome the problem of HIDS for cloud computing whereby it uses a high number of system resources. On the other hand, (Ghorbanian, Shanmugam, Narayansamy, & Idris, 2013) used HIDS to create an intrusion-detection app and active defense mechanism as a substitute for available passive antivirus in Android platform. They were able to develop a HIDS app that can alert users if there is a matched attack pattern trying to sneak in the system.

Hybrid IDS can be a way to solve both NIDS and HIDS disadvantages by combining them in a system that can complement each other's weaknesses. For instance, (Gupta, 2015; Zekrifa, 2014) both have implemented Hybrid IDS in their research. They combined misuse detection system and anomaly detection system to increase detection rate and reduce false positives and negatives. Both studies have shown some positive results where the detection rate has increased and the number of false positives and negatives has reduced slightly.

In a research conducted by (Day, Flores, & Lallie, 2012), they combined both detection systems to improve and harden the process of detecting intrusion. From the research, they discovered that the combination of both IDS improved protection against attacks and maximized the chances of intrusion detection.

To further support the idea of Hybrid IDS,(K S et al., 2014) have analyzed data mining techniques used in Hybrid IDS. Data mining or knowledge discovery is the process of finding patterns from a large quantity of datasets that can be useful in detecting intrusions. This paper analyzed the random forest classification algorithm and weighted k-means algorithm used in Hybrid IDS. The result showed that their technique achieves a higher detection rate and low false-positive rate, compared to other approaches.

METHODOLOGY

The method used in developing this system was System Development Life Cycle (SDLC) based on the waterfall model. It consists of five phases, starting with system planning, system analysis, system design and development, system testing and evaluation as well as documentation.

System Planning

The feasibility study was conducted to identify the problem statement, objectives, scope and significance of the project. All information was gathered by read articles, journals and thesis from previous research.

System Analysis

During system analysis, all required hardware and software for the project were determined. Table 1 and Table 2 show details of the hardware and software requirements.

Table 1: Hardware Requirements

No.	Item	Description
1	Personal Laptop	This laptop acted as the user's laptop and was installed with the Hybrid IDS. Specifications: • Brand: HP • CPU: Intel® Core™ i5-8250U • RAM: 8 GB • Operating System: Ubuntu
2	Attacker Laptop	This laptop acted as the attacker's laptop and tried to execute some malicious activities.

Table 2: Software Requirements

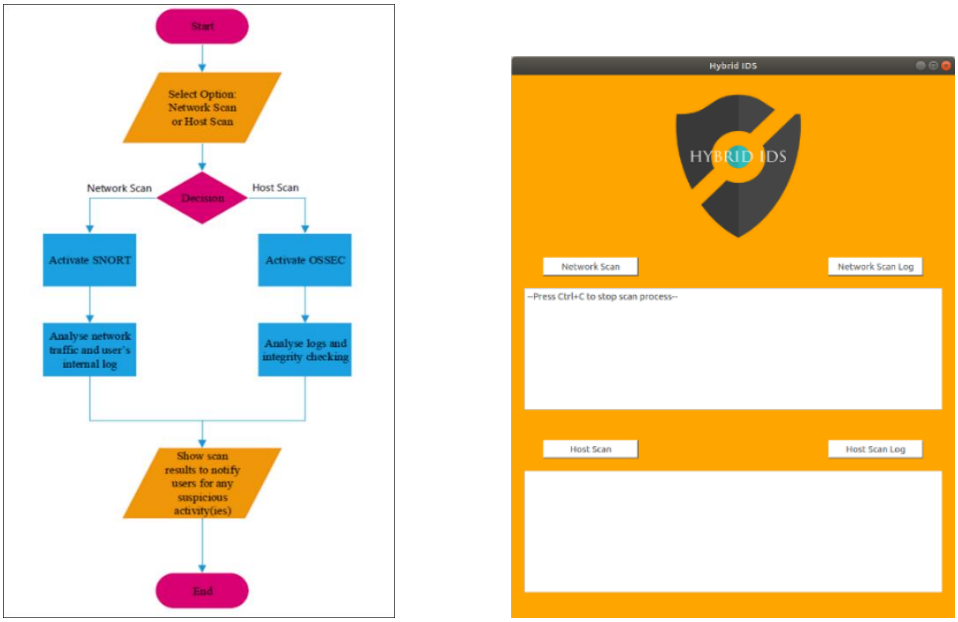
No.	Item	Description
1	Ubuntu Operating System	Ubuntu is used to develop the Hybrid IDS because of its compatibility with both IDS.
2	SNORT	A NIDS software that was installed on the user's laptop for network monitoring.
3	OSSEC	A HIDS software that was installed on the user's laptop for host monitoring.
4	SUBLIME	A coding software that was used to code the Hybrid IDS using Python Language.

Table 1 shows the hardware requirements for this project used two different laptops where both have their own tasks in this project while Table 2 represents the software requirements which Ubuntu operating system was installed in the user's laptop. Python programming language was used to develop the Hybrid Intrusion Detection System.

System Design and Development

Figure 1(a) and Figure 1(b) show the flowchart and the main page of the proposed hybrid IDS. After the system started, the user needs to choose one from two options available. First option, Network Scan, is for throughout scanning of network while the other scan option is for system's log file and integrity. From there, the Hybrid IDS created a sub-process based on the user's chosen option.

During the process, the monitoring software(s) analyzed and detected any malicious activities that might be occurred during the scanning process. A notification result was alerted to the user if the system successfully detects any malicious activities.



(a) (b)

Figure 1: (a) Flowchart of the Hybrid IDS and (b) Main page of the Hybrid IDS

System Testing and Evaluation

Figure 2 shows the test bed that was conducted for the proposed Hybrid IDS. A Wireless Router provides the wireless LAN to the Internet while both laptops were connected to the same network.

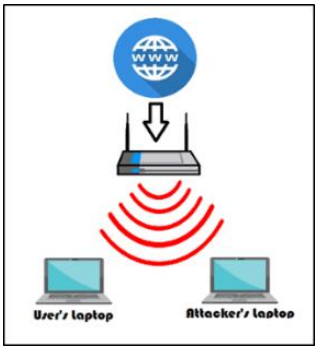


Figure 2: Test bed for the Hybrid IDS

After conducting the test bed, testing phase of Hybrid IDS began where all required hardware and software must work exactly as they should. During the testing, Hybrid IDS monitors and evaluates packets that went through the wireless network while the attacker laptop tried to execute some malicious activities.

The results from the testing were analyzed and discussed based on the system's ability to detect malicious activities that were carried out during this phase.

Documentation

The final phase was a process of documenting all related information and results from the previous phases.

RESULTS AND ANALYSIS

Several attacks were launched from the attacker's laptop targeting the user's laptop to evaluate the degree of security level using the proposed Hybrid IDS. In this case, both laptops were connected with the same network. The system launched SNORT IDS as a Network IDS was responsible to alert the user if any suspicious activities occur through the network, while OSSEC IDS focusses on any signs of intrusion or problems related with the user's system. The proposed Hybrid IDS was able to generate alerts if the malicious activities occurred. Some examples of alert that can be generated by the systems were bad traffic, TCP DOS, ICMP Ping, Port Scan, Access Unsecure Website, SNMP DOS, Integrity Checksum, Root Check, New Installation Detection and Disk Space Utilization.

Then, the proposed Hybrid IDS was analyzed with other scenarios such as the system installed with NIDS only, HIDS only, and Antivirus only. The Windows Defender was chosen as the antivirus.

Table 3: Comparison of Hybrid IDS with other scenarios

User installed with Type of alerts	Hybrid IDS	Network IDS only	Host IDS only	Antivirus only
Bad Traffic	✓	✓		
TCP DOS	✓	✓		
ICMP Ping	✓	✓		
Port Scan	✓	✓		
Access Unsecure Website	✓	✓		
SNMP DOS	✓	✓		
Integrity Checksum	✓		✓	
Root Check	✓		✓	✓
New Installation Detection	✓		✓	✓
Disk Space Utilization	✓		✓	✓

Table 3 shows the Hybrid IDS clearly had the advantage from the other scenarios. A computer system can take the full advantage of using Hybrid IDS where both SNORT and OSSEC can act together to build a secondary layer of security when connecting to an Open Wi-Fi. Hybrid IDS produced a better result than the rest because it can generate alerts for both network and system activities such as TCP DOS, ICMP Ping and Integrity Checksum.

On the other hand, although antivirus had the ability to replicate some of the functions as OSSEC does, unfortunately it does not have the ability to monitor the network thus it can't detect or alert the user if any malicious activities occur in the network such as TCP DOS and Port Scan attacks.

Based on the results, it can be said that Hybrid IDS was better as it can detect and alerts more suspicious activities than the other scenarios hence it can provide the users with a better protection when connecting to Open Wi-Fi.

CONCLUSION

The Hybrid IDS was used by combining SNORT and OSSEC which aimed to monitor and evaluate Open Wireless LAN (WLAN). For that, a system was developed to control and manage both IDS to help users use the Hybrid IDS easily and efficiently. The whole idea of creating a Hybrid IDS was based on the need to help users to stay protected when connecting to an Open WLAN.

This type of network often targeted by the attackers to launch attack through the network itself. If this situation occurs, the system generates alert(s) to notify the user about the possible attack that might be happened. In addition, the system also provides a function that user can check previous scan results without having to search the log file in the computer system which surely cost some time to find it.

Furthermore, the system was developed with a user-friendly interface that can help users to navigate and control both IDS. In the main page of the system, there were several buttons and textbox where each of them has their own function. If one of the IDS in the system detects any suspicious activities, the system then shows responding alerts in the textbox given in the main page so user can take further action.

In conclusion, the proposed Hybrid IDS was shown positive results during testing and analysis phases. The combination of SNORT and OSSEC produced better security than other scenarios that had been tested. Besides, the Hybrid IDS also provided a wide range of tracking detection for suspicious activities in the network environments. Based on these results, it could be said with certainty that the system can monitor and evaluate Open WLAN to find and alert the users about malicious activities.

REFERENCES

Al-Dalky, R., Salah, K., Otrok, H., & Al-Qutayri, M. (2014). Accelerating snort NIDS using NetFPGA-Based Bloom Filter. *2014 International Wireless Communications and Mobile Computing Conference (IWCMC)*, 869–874.

Am, R., & Chezian, R. M. (2017). Intrusion Detection System Techniques and Tools: A Survey. *Scholar Journal of Engineering and Technology (SJET)*, *5*(3), 122–130.

Ashoor, A. S., & Gore, S. (2011). Intrusion Detection System (IDS): Case Study. *2011 International Conference on Advance Materials Engineering*, *15*, 4.

Cisco. (2017). *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021* (pp. 1–35) [Whitepaper]. Cisco.

Day, D. J., Flores, D. A., & Lallie, H. S. (2012). CONDOR: A Hybrid IDS to Offer Improved Intrusion Detection. *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 931–936.

Ghorbanian, M., Shanmugam, B., Narayansamy, G., & Idris, N. B. (2013). Signature-based hybrid Intrusion Detection System (HIDS) for Android Devices. *2013 IEEE Business Engineering and Industrial Applications Colloquium (BEIAC)*, 827–831.

Gupta, M. (2015). Hybrid Intrusion Detection System: Technology and Development. *International Journal of Computer Applications*, *115*(9), 5–8.

K S, P., Kumar, P., & T S, S. (2014). Analysis of Hybrid Intrusion Detection System Based on Data Mining Techniques. *International Journal of Engineering Trends and Technology*, *15*(9), 448–452.

Safdar, A., Durad, H., & Alam, M. (2018). Design and Implementation of Real-Time Visualization Tool for Network Security Monitoring. *2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, 477–483.

Shum, K. C., & Ng, J. K. (2010). Detecting, Locating, and Tracking Hacker Activities within a WLAN Network. *2010 IEEE 16th International Conference on Embedded and Real-Time Computing Systems and Applications*, 53–58.

Siregar, B., Manik, M. S., Rahmat, R., Andayani, U., & Fahmi, F. (2017). Implementation of Network Monitoring and Packets Capturing using Random Early Detection (RED) Method. *2017 IEEE International Conference on Communication, Networks and Satellite (Comnetsat)*, 42–47.

Wang, Z., & Zhu, Y. (2017). A centralized HIDS framework for private cloud. *2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 115–120.

Zekrifa, D. M. S. (2014). *Hybrid Intrusion Detection System*. Computer Science, School of Information Technology & Mathematical Sciences.