Science Archives (2023) Vol. 4 (3), 190-194

Science Archives (ISSN:2582-6697)

Journal homepage: www.sciencearchives.org

https://doi.org/10.47587/SA.2023.4302

Review Article

Innovative framework design of an intelligent detection and monitoring system (IDMS) to leverage National Security

Okonta O. Emmanuel[1]✉, Ajani Dele[1] and Okonta I. Love[2]

[1]*Department of Computer Education, FCE(T), Asaba, Nigeria*
[2]*Department of Educational Foundations, FCE(T), Asaba, Nigeria*
Received: May 30, 2023/ Revised: June 30, 2023/Accepted: July 11, 2023
(✉) Corresponding Author: Okey.okonta@fcetasaba-edu.ng

Abstract

Intrusion monitoring is the act of monitoring unwanted traffic on a network or a device, analysing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion detection is the process of detecting a possible compromise or events occurring in a computer system or network. An IDMS can be a piece of installed software or a physical intelligent appliance that monitors network traffic in order to detect and prevent unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable use policies. This innovative design primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, try to inoculate the system to prevent similar attacks using recognisable signature patterns and this will enhance National Security and prevent unwarranted cyber-attacks on organizations and important National resources.

Keywords: Innovative, Intelligent Detection, Monitoring System and National Security.

Introduction

During United States of American national election in 2016 and well as the mid-terms election 2018 it was discovered that Russian Intelligent Unit hack into their Network to influence the outcome of their elections. Back home here in Nigeria, a particular political party boosted it had hacked into the Independent National Election Commission's Server in an attempt to obtain the election results illegally. Come to think of it these are mind bugging incidents that can compromise nation security and throw the country into a deep mess. With this in mind this research work will focus on an Innovative Framework Design of an Intelligent Detection and Monitoring System (IDMS) to leverage National Security.

Intrusion detection

An intrusion detection system (IDS) is software that automates the intrusion detection process. It derives its name from the fact that it monitors the entire network to detect hackers' attempts to compromise system security hence the need for the intrusion narrative.

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analysing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents**.**

Intrusion detection systems (IDSs)

Intrusion detection systems (IDSs) are designed for detecting, blocking, and reporting unauthorized activity in computer networks. If there are attacks on a system, we would like to detect them as soon as possible and take appropriate action.

This is essentially, what an Intrusion Detection System (IDS) does. An Intrusion detection system is a reactive rather than pro–active agent. Wireless networks are susceptible to variety of threats and security issues are ranging from DOS to remote to local and local to root attacks. As we know that wireless network provides less security mechanisms than a wired network.

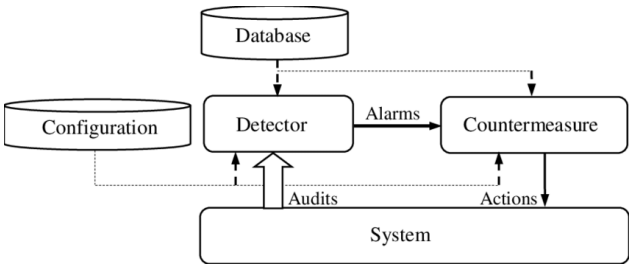

Fig. 1 A simple Intrusion Detection and Monitoring System

Therefore, we need a wireless IDS, which ensure us our network is protected from any kind of attacks. There is no gainsaying that our Wireless Networks are sometimes vulnerable to threats. We felt there is need for an intelligent defence system is that simple, robust and immune from attacks.

Statement of Problem

The idea of designing an effective system is an essential approach for protecting information systems security, and yet it remains an elusive goal and a great challenge to most developing nations even as computer networks are at the core of most nation's operational control. Hackers know that network installations whether monitored by humans or not are susceptible because humans have human failings. Hence, the need to result to soft computing and different artificial intelligence techniques to try to construct new generation computationally intelligent hybrid systems to see if it will ameliorate the human failure.

Objectives of the Research

The fact is that intelligent agents carry out most network-centric cyber-attacks. Such agents as Computer Worms, Viruses, Trojan horse and other supplicated programs. Therefore, our aim is to scan and combat these attacks.

The objectives are

- See if there is any probe or scan before an attack
- To know whether launching defensive attack on hacker's site result in increased attack.
- To understand if these hostile activities occur at specific period of time.
- To know if attack activities vary by geographical location.

Research questions

- Is there any probe or scan before an attack?
- Does launching defensive attack on hacker's site result in increased attack?
- Do these hostile activities occur at specific period of time?
- Do attack activities vary by geographical location?

Literature Review

Denning introduced the technique of detecting intrusion, and since then researchers have worked hard to automatically detect intrusions in network systems (Denning, 1987). Intrusion detection systems have been defined as the technique of using artificial intelligence, machine learning, and database systems to uncover malicious patterns in large datasets (Shaikha & Abduallah, 2017). IDS can be broadly classified into two major categories, anomaly-based IDS and misuse-based IDS. Recently, other methods have emerged through the integration of anomaly and misuse intrusion IDSs to yield more categorizes.

Depending on the approach used to detect suspicious activities, the IDS may be classified in two categories: anomaly-based detection and signature-based detection. The former keeps track of the activities in the network to detect effective deviation from a considered normal behaviour. The latter consist of searching known attack profiles. Comparing these both categories, one can say that a disadvantage of the anomaly-based approach is the high number of false positive alarms, and that the signature-base one demands prior knowledge of the attack profiles. Concerning the advantages, the former approach is able to detect unknown attacks, and the latter is a low computing-intensive method.

Wireless networks are vulnerable to various types of attacks. Because of that, several extensions have been proposed to IEEE 802.11, aiming at reducing or eliminating such deficiencies And distinct approaches have been proposed to IDS (Baig & Kumar, 2011; Mohanabharathi, et al., 2012) Most existing intrusion detection approaches has been developed for wired networks, and these approaches uses several classifying mechanisms such as neural artificial networks (Zhong et al., 2011; Wu & Banzhaf, 2010), clustering and genetic algorithms (Goyal, et al., 2012). A hybrid approach in makes use of information from MAC layer and upper layers to intrusion detection in wireless networks. This approach is used in the feature selection process.

Theoretical framework

A core mathematics of intelligence comprising learning, inference, and neural computation that has emerged in the past few years (Bosman, et al., 2017). That had provided the tools

for the theory platform but Soft Computing techniques are being widely used by the IDS community due to their generalization capabilities that help in detecting know intrusions and unknown intrusions or the attacks that have no previously described patterns (Sun, et al., 2007). Distributed agent technology is being proposed by a few researchers to overcome the inherent limitations of the client-server paradigm and to detect intrusions in real time (Xiao, et al., 2007). They will need to be plausible and testable at all levels. An IDS can be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable use policies (Fu, et al., 2017).

Research methodology

Intrusion detection refers to the process of monitoring the events happening in a computer system or network, examining them for signs of security problems like wrong signatures or other anomalies. Therefore, our novel design called HIDES (Hybrid Intrusion Detection & Elimination System) will gathers and analyses the information within a wireless network to perceive possible security breaches and launches an all-out elimination defensive -attack, which will include a Sniffer, a Scanner, an Attacker, a Defender and Immunizer all cascaded inside HIDES Shell.

IDMS Design

The IDMS first starts by monitoring network packets for signs of reconnaissance, exploits, Denial of Service attacks, and malware. It has the strengths to complement host-based IDSs: IDMS can see traffic for a population of hosts; it can recognize patterns shared by multiple hosts; and it has the potential to see attacks before they reach the hosts.

An IDMS is placed in various locations for different purposes, as shown in Fig. 2. The IDMS outside a firewall is useful for monitoring and learning about malicious activities on the Internet. An IDMS placed in the Demilitarized Zone will see attacks originating from the Internet that are able to get through the outer firewall to public servers. Finally, an IDMS in the private network is necessary to detect any attacks that are able to successfully penetrate perimeter security.

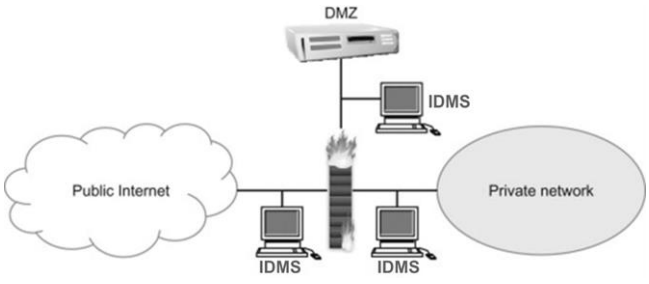

Fig. 2 A simple IDMS deployment diagram
IDMS operation

IDMS is an intelligent and robust network-based intrusion detection system capable of learning and re-learning, they are devices strategically distributed within networks that passively inspect traffic traversing the devices on which they sit. IDMS can be hardware or software-based systems and, depending on the manufacturer of the system, can attach to various network mediums such as Ethernet, FDDI, and others. Oftentimes, IDMS have two network interfaces. One is used for listening to network conversations and the other is used for control and reporting.

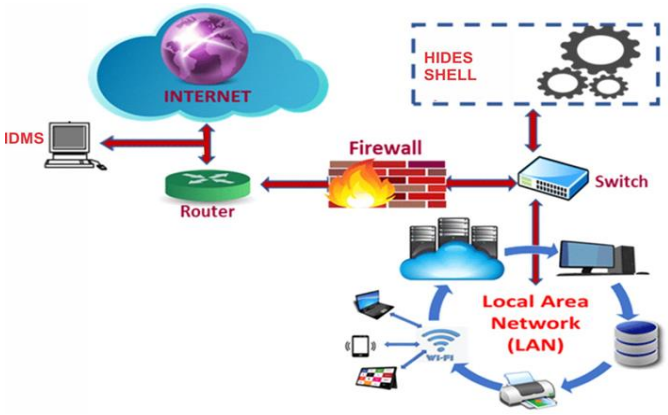

Fig. 3 Hybrid Design

Expected results

Our approach to computer security is to attempt to create a completely secure system. Unfortunately, in many environments, it may not be feasible to render the computer system.

Immune to intrusions, for several reasons. First, system software is becoming more complex. A major challenge programmers face in software design is the difficulty in anticipating all conditions that may occur during program execution and understanding precisely the implications of even small deviations from usual designs and software upgrades come with their own variety of new problems. Second, the increasing demand for network connectivity makes it difficult, if not impossible, to isolate and thereby protect a system from external penetration. Finally, a central component of computer systems, the computer network itself, may not be secure. For instance, there are a number of securities lapses inherent in the widely used Transmission Control Protocol/Internet Protocol (TCP/IP) suite, regardless of its particular implementation. With the advent of our HIDES design:

- We are able to measure the attack-resistance of our wireless networks every microsecond.
- We can know within minutes if we are being probed, hacked, infected, or misused.
- And we can be alerted with a prompt of an e-mail.

Findings

Deploying this innovative detection and monitoring system code name HIDES, it was observed that there were usually no probe or scan before any attacks. That these attacks just occur spontaneously. Nevertheless, it was also observed that when you activate your preventive mechanism, these hackers adopt evasive techniques and relaunch the attack that sometimes leads to increased attack.

These hostile activities do not occur at any specific period, these attacks are done randomly and there were no indication that these attacks also vary by geographical locations**.**

The Evasion Techniques deployed by Hackers

There are some observed techniques, intruders used; to try avoiding detection by our innovative design. These methods created some challenges for IDMS, as they are meant to circumvent our deployment.

Fragmentation

Fragmentation divides a packet into smaller, fragmented packets. This allows an intruder to remain hidden, as there will be no attack signature to detect. The recipient node at the IP layer later reconstructs fragmented packets. They are then, forwarded to the application layer. Fragmentation attacks generate malicious packets by replacing data in constituent fragmented packets with new data.

Flooding

This attack is designed to overwhelm the detector, triggering a failure of control mechanism. When a detector fails, all traffic will then be allowed. The IDMS sniffer mode had difficulty detecting these malicious packets trying to overwhelm it.

Obfuscation

The hackers in order to avoid being detected send obfuscating malware to evade IDMS. The objective is to reduce detectability to reverse engineering or static analysis process by obscuring it and compromising readability by making a message difficult to understand, thereby hiding an attack.

Encryption

Hackers and malware creators use encryption security attributes to conceal attacks and evade detection. IDMS had a tough time blocking encrypted protocol.

Innovation: How different it is from other or earlier projects?

Too often, people design and install software with all kinds of the features that "can" be used and forget to configure tools to meet their own requirements for what "must" be done.

Our HIDES design is intended to help Network use decide what "must" be done in order to select tools that meet those requirements.

HIDES Shell has

- Probe Sniffer
- Scanner for File Integrity Checker and detect Network Vulnerability
- Attacker to Eliminate Intrusion
- Defender to Stabilize the Network
- Immunizer to Protect the Network from further Attacks

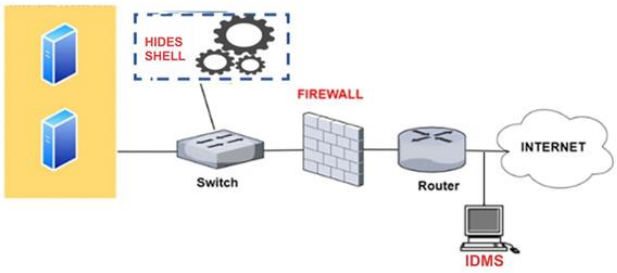

Fig. 4 HIDES shell deployment

Conclusion

In this work, we designed an innovative framework to detect, monitor, and prevent Cyberattacks. These attacks are always increasing in complexity and sophistication, as witnessed in just concluded national elections some few weeks back. Zero Day Attacks are common; as a result, network protection deployment like our design tried to keep pace with new threats, because nations must maintain high levels of security.

The aim to combat cyberattacks with intelligent semi-autonomous agents to assure secure, trusted network was achieved in our IDMS framework design. Therefore, IDMS is important to the security ecosystem of this nation. It operates as a defence for our network systems security when other technologies fail.

Recommendation

We recommend that government and private entities should sponsor more research in our institutions of higher learning to identify serious security incidents and compromises in our national networks and proffer practical solution on how to combat them.

Research centres should be set up to analyse the quantity, types of attacks and help identify bugs or problems with device configurations and enforce regulatory compliance.

Conflict of Interest

The author hereby declares no conflict of interest.

Consent for publication

The author declares that the work has consent for publication.

References

Bao, F, Chen I-R, Chang M, Cho J-H (2012). Hierarchical Trust Management for Wireless Sensor Networks and its applications to trust-based routing and intrusion detection. *IEEE Trans Network Server Management 9*(2):169–183

Baig, M. &. Kumar. K (2011). "Intrusion Detection in Wireless Networks Using Selected Features," Int. J. Computing. Sci. *Inf. Technol.,2*, pp. 1887–1893, 2011.

Bosman, H., Iacca, G., Tejada, A., Wörtche, H. J. and Liotta, A. (2017). Spatial anomaly detection in sensor networks using neighbourhood information. *Information Fusion 33*:41–56.

Corchado, E. & Herrero, A. (2011). "Neural visualization of network traffic data for intrusion detection," *Appl. Soft Computing*., *11*(2), 2042–2056.

Denning, D. E (1987). "An intrusion-detection model," IEEE Transactions on Software Engineering, *13*(2), 222–232.

Fu, Y, Yan Z, Cao J, Kone O, Cao X (2017). An automata based intrusion detection method for internet of things. Mob Inf Syst 2017(1750637):13. https://doi.org/10.1155/2017/1750637

Goyal, M. K., Aggarwal, A. & Jain, N. (2012). "Effect of change in rate of genetic algorithm operator on composition of signatures for misuse intrusion detection system," in 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 12, 669–672. http://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow /54945561.cms. Accessed 26 Dec 2017.

Krimmling, J. and Peter, S. (2014) Integration and evaluation of intrusion detection for CoAP in smart city applications. In: IEEE Conference on Communications and Network Security (CNS'14), pp 73–78.

Mohanabharathi, M., Kalaikumaran, T. & Karthi, S. (2012), "Feature Selection for Wireless Intrusion Detection System Using Filter and Wrapper Model," *Int. J. Mod. Eng. Res., 2*(4), 1552–1556, 2012.

Sun, B., Wu, K., Xiao, Y. and Wang, R. (2007). Integration of mobility and intrusion detection for wireless ad hoc networks. *Wiley's International Journal of Communication Systems 20*(6), 695–721

Shaikha, H. K. & Abduallah, W. M. (2017) "Review of intrusion detection systems," Academic Journal of Nawroz University, vol. 6, no. 3, pp. 106–111.

Wu, S. X. & Banzhaf, W. (2010), "The use of computational intelligence in intrusion detection systems: A review," Appl. Soft Computing., vol. 10, no. 1, pp. 1–35, Jan. 2010.

Xiao, Y., Shen, X. S. and Du, D. Z. (2007). Wireless Network Security, Springer Science+Business Media, LLC, USA. E-ISBN-10 0-387-33112-3.

How to cite this article

Okonta, O. E., Ajani, D. and Okonta, L. I. (2023). Innovative framework design of an Intelligent Detection and Monitoring System (IDMS) to leverage national security. *Science Archives, Vol. 4*(3), 190-194. **https://doi.org/10.47587/SA.2023.4302**