Article Citation Format
Onwodi, G. (2022): Smart Intrusion Prevention System For The Local Area Network Of Nigeria Immigration Special Study Centre, Gwagwalada, FCT, Abuja, Nigeria. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology. Vol. 10, No. 2. Pp 73-78
DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V10N4P10

Smart Intrusion Prevention System for the Local Area Network of Nigeria Immigration Special Study Centre, Gwagwalada, FCT, Abuja, Nigeria

Onwodi, G.
Department of Computer Science,
National Open University of Nigeria
Abuja, FCT, Nigeria
E-mails: gonwodi@noun.edu.ng

ABSTRACT

This study examines the Smart Intrusion Prevention System for the Local Area Network of Nigeria Immigration Special Study Centre, Gwagwalada, Abuja. Different research methodologies for Intrusion Prevention System was analysed and the hybrid based methodology was adopted because of its incorporation of the other methodologies. Configuration of the Intrusion Prevention System was studied and implemented using software known as Mikrotik. The Mikrotik software configuration was analysed properly. Among the major findings of the study was that the Local Area Network of Nigeria Immigration Special Study Centre, Gwagwalada, Abuja was relatively insecure with the sophisticated breed of attackers we have now. The study therefore recommended that Nigeria Immigration Special Study Centre, Gwagwalada, Abuja should integrate a known Intrusion Prevention System software and endeavour to keep it updated at all times. Also, they can work on system design and algorithm design for secure communication over complex networks.

Keywords: Intrusion Prevention System, LAN, Nigeria, Immigration, Special Study Centre, FCT, Abuja,

1. INTRODUCTION

The need to secure data has been a pertinent issue ever since the inception of computers and the advancement in technology has even made this quest more of a necessity in today's world. Intrusion detection was developed to identify and report the attack in the late 1990s, as hacker's attacks and network worms began to affect the internet. It detects hostile traffic and send alerts but does not do anything to stop the attacks. Almost two decades now, Intrusion Detection System (IDS), still cannot detect all malicious programmes and activities most of the time. Also, it is incompatible to integrate with control restriction to stop traffic inbound-outbound from attacking; which means it was only capable to detect attack actions, without prevention actions.

However, due to the inadequacies of an Intrusion Detection System, an intrusion prevention system (IPS) which is a network security tool (which can be a hardware or software), was introduced as an extension of IDS. An Intrusion Prevention System continuously monitors a network for malicious activity and takes action to prevent it, including reporting, blocking, or dropping it, when it does occur. It is more advanced than anintrusion detection system (IDS), which simply detects malicious activities but cannot takeaction against it beyond alerting an administrator.

2. BACKGROUND

2.1 Smart Intrusion Prevention System

Smart technology in offices and homes allow the entire offices to be automated and therefore, the connected smart office devices can be remotely controlled and operated, from any location in the world, through a smartphone app, personal computers or other network devices. However, connecting smart devices such as computers, appliances and other networking devices introduces tremendous cybersecurity risks. All security reports warn that more than 80% of connected smart devices are vulnerable to a wide range of attacks. A recent research by the cybersecurity firm Avast affirms that two out of five smart offices are vulnerable to cyber-attacks.

2.2 Intrusion Prevention System Smart Tools

With the evolution of cyber security solutions from the early days of firewalls, these distinct capabilities merged to offer organizations both intrusion detection and prevention systems solutions. Fast-forward and security tools continue to combine features, including IDPS, into advanced solutions like next-generation firewalls (NGFW) and extended detection and response (XDR). While IDPS comes with a growing number of products and merged services, vendors still offer standalone IDPS, allowing organizations to pick a solution that supports their other security assets and needs. Be it a physical, cloud, or virtual appliance, the next-generation intrusion prevention systems (NGIPS) of today are worth any growing enterprise’s consideration. These are some of the intrusion detection and prevention systems tools to consider in evaluating solutions of network attacks; Check Point Intrusion Prevent System (IPS), Cisco Firepower Next-Generation IPS (NGIPS), Trellix Network Security, Hillstone S-Series Network Intrusion Prevention System (NIPS), and NSFOCUS Next-Generation Intrusion Prevention System (NGIPS).

3.0 RESEARCH METHODOLOGY

3.1 Intrusion Prevention System

There are many different methodologies used by Intrusive Detection and Prevention System to detect changes on the systems they monitor. These changes can be external attacks or misuse by internal personnel. Among the many methodologies, about four methods stand out and are widely used. These are the signature based, anomaly based, stateful protocol analysis based, and hybrid based. Most current IDPS systems use the hybrid methodology with the combination of other methodologies to offer better detection and prevention capabilities.

3.2 Configuration of Intrusion Prevention System

The intrusion prevention system of a network can be configured by:

1. Securing Router: The main idea to secure the router is by minimizing the intrusion.
2. Security means complexity of network intrusion types. Network intrusion is a serious
3. Security risk that could result in not only the temporal denial, but also in total refusal of network service.
4. Port Scan: This is a method of intrusion where the outsider will scan the router's port to find one or more open port that they can use to penetrate the router.
5. DOS Attack: Main target for dos attacks is consumption of resources, such as CPU time or bandwidth, so the standard services will get denial of service (dos).
6. DOS Attack Protection
7. DOS Attack Suppression
8. Connection Limit

3.3 Hybrid Based Methodology

The hybrid based methodology works by combining two or more of the other methodologies. The result is a better methodology that takes advantage of the strengths of the combined methodologies. Prelude is one of the first hybrid IDS that offered a framework based on the Intrusion Detection Message Exchange Format (IDMEF) an IETF standard that allows different sensors to communicate.

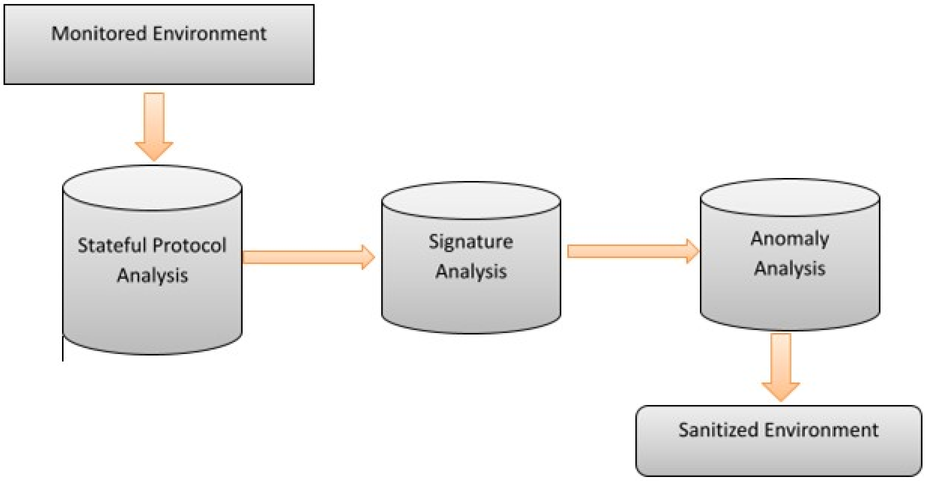

Fig. 5- Hybrid based methodology architecture

4.0 NETWORK SECURITY

In the present era, there is an enormous growth of the Internet in terms of its usage and resources. Almost all major commercial organizations, educational institutes, governments and individuals are dependent upon the Internet for providing their services.

Most of the commercial organizations exchange information with their collaborators and clients through the Internet. Educational institutes are uploading study materials and research findings over the Internet for the speedy propagation of the information. Governments provide information to the citizens through the Internet. Individuals use the Internet for accessing the information, online shopping and communicating with others through emails and social networking, etc. Thus, the Internet provides a platform to run the services and to store sensitive information of commercial organizations, educational institutes and governments.

However, presence of configuration errors and vulnerabilities in the most popular softwares provide numerous chances for malicious users to mount a variety of attacks to disrupt services and integrity of sensitive information over the Internet called cyber-attacks. A cyber-attack is a deliberate exploitation of computer systems, technology-dependent networks and enterprises. The cyber-attacks use malicious code to alter computer code, logic or data resulting in destructive consequences that can compromise information security. Zero-day (unknown) vulnerabilities are potentially more harmful, associated with newly published program or web services. Such vulnerabilities may be visible for days or weeks until patched and offers more chances for attackers to exploit them.

4.1 Security Threats

The dependence of the information-based organizations and individuals over the Internet is increasing day by day. However, most of the popular software contains vulnerabilities and configuration errors, which are not only technically difficult, but also economically costly to be solved. The intruders to misuse the Internet resources and launch influential attacks against them such as the Denial of Service (DoS) and Information attacks exploit these vulnerabilities and easy access to Internet resources. The sheer volume of vulnerabilities revealed every year is overwhelming, as more than 5000 new ways for hackers to cause, damage and access systems were discovered in 2012 alone. The most popular products used by organizations were also the most susceptible to cyber-attacks. For example, Oracle, Apple and Microsoft are the most vulnerable system vendors. Research at Checkpoint software technologies; show that 75% of hosts in organizations were not using the latest software versions (e.g. Acrobat Reader, Flash Player, Internet Explorer, Java Runtime Environment, etc.). This means that these hosts were exposed to a wide range of vulnerabilities that could have been exploited by hackers. Their research also shows that 44% of hosts in organizations were not running the latest Microsoft Windows Service Packs. Service packs usually include security updates for the operating system. Not running the latest versions increases security risk.

5. FUTURE TRENDS

We have seen what has happened in the recent past: Malware creation records the highestnumber of Trojans ever, attacks in social networks, cyber-crime and cyber war everywhere. What do we have to expect for the near future? Nowadays, cyber threat is no longer a threat, it is a daily reality. These threats continue togrow. They must be understood for addressing them so that tenets of information securityare adhered. The important tenet of information security includes confidentially, integrity and availability. By understating the motivation behind various cyber-attacks, we can moreclearly present the future trends of cyber-attacks. The cyber-attacks can be broadly classified into four categories described as below (depicted in Figure 5).

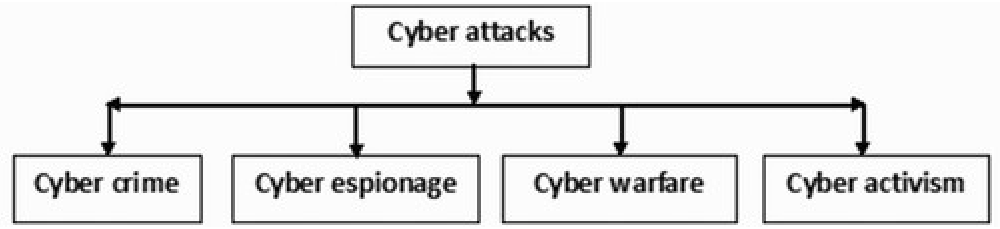

Figure 5. Cyber-Attacks Classification.

5.1 Cyber Crime

The cyber-crimes in the near future are enriched with the terms like cyber fraud, stealing, phishing and other malicious behaviors. Generally, cyber-crimes refer to the malicious activities to block, read or interfere with cyber services. Multiple information security tenets including confidentially, integrity and availability may be compromised during this type of cyber-attack. Here, the motivations of cyber criminals include gaining economic benefit, compromising cyber infrastructure (e.g. in cyber warfare) and self-satisfaction. The cyber criminals use stolen identity of victims; perform online extortion, spamming, phishing, etc. as attack vectors to commit cyber-crimes. Most of cyber-crimes committed in the real world are committed through online computers. Generally, the aim of cyber criminals is to gain access of victims' computers, online resources and credentials. Once they gain access to victims' resources by any means, then compromised resources can be used to perform any malicious activity. For example, booming e-commerce or online business lures cyber criminals. Cyber criminals can use Malware tools to commit economic crimes, such as stealing credit cards and social security numbers, and electronic money. Flaws in the software used for e-commerce or online services provide numerous chances for cyber-crimes in the economy. Cyber-crimes go on daily in the real world and will continue to take place because of huge profits behind them and the availability of cyber tools to commit these crimes.

6. CONCLUSION

Cybercriminals use sophisticated techniques and social engineering tactics to target computer users. Some cybercriminals are becoming more sophisticated and ambitious. Cybercriminals have demonstrated their ability to disguise identities, hide communications, separate identities from illicit gains, and leverage breach-resistant infrastructure. Therefore, it is becoming increasingly important to protect computer systems with advanced intrusion prevention systems that can detect and prevent the latest malware. Designing and buildingsuch an IPS system requires a thorough understanding of the strengths and weaknesses of his current IPS research. A survey of Intrusion Prevention System methodologies, types, and technologies with their advantages and limitations were presented in this research. Several machine learning techniques that have been proposed to detect zero-day attacks are reviewed. However, such an approach has problems generating and updating information about new attacks, which can lead to many false positives and low accuracy. In today's cybersecurity environment, malware detection and prevention technologiesmust be employed. Stand-alone IDS is not enough to protect your system from cybercriminals. However, combining IDS and IPS together with a firewall can better detect and prevent threats.

REFERENCES

1. J. Armstrong Joseph and Korah Reeba "Efficient String Matching FPGA for speed up Network Intrusion Detection", 2018
2. Pradeepa Wijuntunga "Local Area Networks (LANs) and Their Application in Libraries", 2002
3. Computer Security Institute. The Fifteenth Annual CSI Computer Crime and Security Survey. Monroe, WA: Computer Security Institute, 2010
4. Computer Economics. Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and Other Malicious Code. Irvine, CA: Computer Economics, 2007.
5. Symantec. The 2012 Norton Cybercrime Report. Mountain View, CA: Symantec. 2012 Economist. A thing of threads and patches. Economist, August 25, 2012.
6. Chi, M. Reducing the Risks of Social Media to Your Organization. Bethesda, MD: SANS Institute, 2011.
7. Merrill, T.; Latham, K.; Santalesa, R.; and Navetta, D. Social Media: The Business Benefits May Be Enormous, but Can the Risks—Reputational, Legal, Operational—Be Mitigated? Zurich, Switzerland: ACE Group, 2011.
8. Consumer Reports. Social insecurity: What millions of online users don't know can hurt them. Consumer Reports, 2010.
9. Mansfield-Devine, S. Anti-social networking: Exploiting the trusting environment of web 2.0. Network Security, 11 (2008), 4–7.