IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Special Issue || Dec. 2019 || PP 11-14
International Conference on Management Practices, Innovations & Research 2019

Implementation of Network Intrusion Detection and Prevention using Nidps Technique

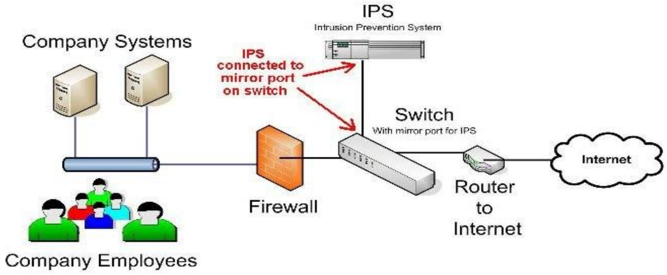
[1]Monali Bodkhe, [2]Gurudev Savarkar
[1]V.M.Institute of Engineering Technology & Management RTMNU, Nagpur,
[2]V.M.Institute of Engineering Technology & Management RTMNU, Nagpur,

Abstract: *This paper presents an investigation, involving experiments, which shows that current network intrusion, detection, and prevention systems (NIDPSs) have several shortcomings in detecting or preventing rising unwanted traffic and have several threats in high-speed environments. It shows that the NIDPS performance can be weak in the face of high-speed and high-load malicious traffic in terms of packet drops, outstanding packets without analysis, and failing to detect/prevent unwanted traffic*

Keywords*: NIDPS, network architecture, network security, open source, quality of service, security, switch Configuration.*

I. Introduction

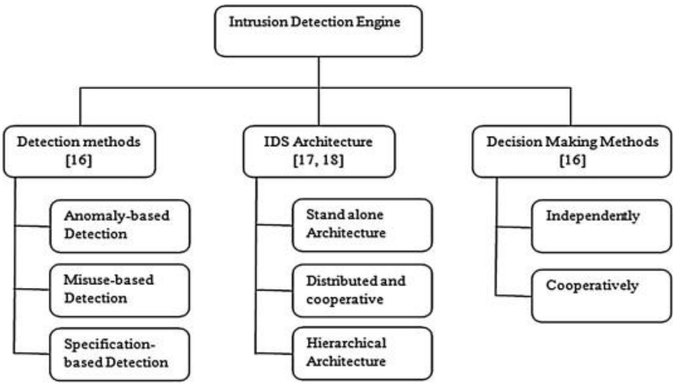
As a result of the technological advances in recent years, we have become increasingly dependent on global networks when engaging in social, business, and educational activities. With the explosive use of computer networks, a number of security issues on the Internet and in computer systems have been raised. Hence, the security of Internet-connected devices from various threats has become considerably important to ensure system availability and integrity [1]. Based on the annual report of 2016 from Asia Pacific Computer Emergency Response Team (CERT) showed a tremendous increment in the amount of intrusions and cyber-attacks over the decade [2]. Similarly, according to a report from the Malaysia CERT published in 2016, 43% of 9986 malicious incidents involve intrusions during system operating hours [3]. An intrusion is a set of actions that violate security policies, the vulnerabilities in the security procedure and the implementation of the system monitored by an IDS [4,5]. By contrast, attacks can be said to be adversarial intrusions against IDS or simply a set of actions that violate the security policies associated with the IDS itself [5,6]. Despite the development of several defensive techniques such as cryptography, firewalls, and access control for secure communication, these anti-threat systems currently possess limitation in detecting intrusion attacks. Therefore, an IDS with appropriate countermeasures, such as an intrusion response system (IRS), is essential for detecting and responding to potential intrusions and attacks [7].



IDSs are the hardware or software systems that autonomously identify and response in-appropriate events (such as intrusion attacks) occur in computer systems [4]. Depending on IDS settings and configurations, IRSs can continuously monitor system health and apply suitable countermeasures to identify and respond to potential incidents and inappropriate activities effectively and hence ensures optimal security in any computing environment [8]. IDS is categorized into three types, namely intrusion tolerance, intrusion prevention system (IPS), and IRS [6,7]. The term “intrusion tolerance” is defined by [6], the capability of a personal computer system to maintain its integrity, confidentiality, and availability even when some of its components are being infected. An intrusion-prevention-system (IPS) is an IDS that generates a proactive response to stop attacks before they occur [8]. In contrast, IRS is always activated after the detection of attacks by IDS and is always generates reactive response. However, existing IDSs only provide a limited response approach and are inadequate to provide optimum response in detected intrusions. Therefore, a response option should be deployed according to the nature of attacks and IDS confidence should be improved in attaining suitable response.

1.1 Types of Intrusion:

At the moment the majority of networks are basically unsecured, which creates opportunities for cybercriminals to access secure data. Attackers are interested in stealing information and also attempt to make digital resources unavailable to users. Numerous defensive techniques such as access control, cryptography, and firewalls can function as the front line of defense against external and internal attacks [6]. Firewalls mainly secure the front access points of a network connected node from a number of threats and attacks [7]. Cryptography allows for secure communication, whereas access control is deployed for authentication purposes. However, these anti-threat applications can only provide external security and are thus inadequate in detecting internal attacks or providing internal security to any computer system and network. IDSs address this problem by monitoring and detecting both internal and external attacks.


Intrusion Detection Engine
Detection methods [16]
IDS Architecture [17, 18]
Decision Making Methods [16]
Anomaly-based Detection
Misuse-based Detection
Specification-based Detection
Stand alone Architecture
Distributed and cooperative
Hierarchical Architecture
Independently
Cooperatively

II. Literature Survey

Generator, Win- Pcap, capture tool, Packets Traceroute, TCP reply and Packets _ooder. The experiments used performance metrics such as number of packets analysed, number of malicious packets detected or prevented, and number of packets dropped. In this section the two experimental setups are described.

2.1 Detecting malicious packets

In this experiment, Win cap, Flooder packet and TCP replay tools were used to send Flood trafficwith signed (known) malicious UDP packets (255 threads per 1mSec) to a physical system at different speeds (see Table 1). The UDP malicious packets were interspersed among other packets transmitted at varying speeds. The following rule has been designed to require Snort to detect (alert and log) any UDP threads or malicious packets that contain the variables `ab.H0..OK..cdef' and time to live (TTL) 132 that comes from any source and port address and goes to any destination address and ports: Alert udp any any -> any any (msg: ``Detect Malicious UDP Packets''; ttl: 132; content:j' 61 62 C2 48 60 AE 97 4F 4B C3 63 64 65 66'j; Sid: 100004;). Flood traffic TCP/IP was sent in different bandwidths (Bps) with 255 malicious UDP packets (threads) in interval packets with a delay of 1 microsecond (1 mSec). The NIDS rule was set up to check the pattern inside the packets and then detect only the malicious UDP threads when the two conditions of (TTL and content) are matched)

2.2 Preventing malicious packets

In this experiment, TCP/IP flood traffic was sent at differing speeds (see Table 2) with 255 malicious UDP packets (threads) also sent at 1 microsecond (1 mSec) intervals. Snort was set to prevent UDP threads by using two rule conditions (TTL and content) as follows: reject udp any any ->any any (msg: ``Prevent Malicious UDP Packets''; ttl: 120; content:j' C2 48 60 AE 97 4F 4B C3 'j; Sid: 100007;). Use of these options will prevent any UDP malicious packet that is matched with the TTL value equal to 120 and a data pattern inside the malicious packet with content ``.H`..OK.''. The hexadecimal number (`C2, 48, 60, AE, 97, 4F, 4B, C3'), which the rule contained, is equal to the ASCII characters (`., H0,,.,., O, K,.').

III. Methodology & Technique

The main feature of intrusion detection system is to provide a view of unusual activity and to issue alerts notifying administrators or blocking a suspected connection. Host Based intrusion Detection System (HIDS) includes software or agent components. It can run on the server, router and switch or network appliance. Network Based Intrusion Detection System (NIDS) collects network traffic packets such as TCP and UDP. NIDS analyzes the content against a set of RULES or SIGNATURES to determine if a POSSSIBLE event took place. HIDS and NIDS are needed in significantly different benefits. For IDS, it is needed to use detection, attack anticipation and prosecution [3] [8].

3.1 Intrusion Prevention System

An IPS sits inline on the network and monitors it, and an event occurs. It takes an action based on prescribed rules. Although it is unlike IDS, which does not sit inline and is passive. However, it is thinking in broader terms and IPS can consider as another tool in the security infrastructure that could help prevent intrusions.IPS has been developed out of IDS but, two systems are really different security products which have different functionality and strengths. In order to detect the intruders the following techniques should be implemented in either HIDS or NIDS [9].

3.2 Anomaly-based IDS

New attack signature is not noticed before it is detected and carefully analyzed. It is difficult to get conclusion based on a small number of packets. Anomaly-based system detects abnormal behaviors and generates alarms based on the abnormal pattern and in network traffic or application behaviors. The main challenges of anomaly based detection system are defining what a normal network behavior is, deciding the threshold to trigger the alarm and preventing false alarms. The network users are hard to predict. If the normal model is not described carefully, there will be lots of false alarms and the detection system can suffer from degraded performance.

3.3 Signature-based IDS

The system can use signature-based detection for detecting known attacks. There are different explanations of attack signatures. In this paper, the main feature base on content International signatures that represent a string of characters which appear in the payload of attack packets. It is not required normal traffic knowledge and signature database is required for this type of detection systems.

IV. Attack Detection & Prevention

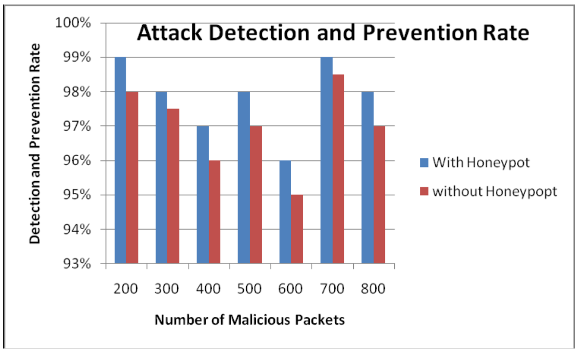


Fig 4.1 Attack Prevention & Detection Rate

The result for the attack detection rate for the two cases. Finally, we test for the performance analysis of attack detection on the number of 800 malicious packets. As proved the result, our proposed framework can perform detection and prevention system.

V. Conclusion

This research study provides a comprehensive explanation of intrusions in terms of their detection and corresponding responses. A few decades back, emphasis was placed on the development of automatic IRSs to overcome the effects of different intrusions. However, IRSs still require extensive research, especially with regard to the selection of proper response options through an automatic response selection process based on intrusion types. Different response options must be activated and executed for each intrusion type to mitigate and overcome the effects of such intrusions.

VI. Summary & Future Work

In this paper, we have discussed the need for building high-speed NIDS that can reliably generate alerts as intrusions occur and have the intrinsic ability to scale as network infrastructure and attack sophistication evolves. We have analyzed the key design principles and have argued that network intrusion detection functions should be carried out by distributed and collaborative NNIDS at the end-hosts. We have shown that an NNIDS running on the network interface instead of the host operating system can provide increased protection, reduced vulnerability to circumvention, and much lower overhead. We have also described our experience in implementing a prototype NNIDS.

References

[1]. R. Lippmann, D. Fried, I. Graf, J. Haines, K. Kendall, D. McClung, D. Weber, S. Webster, D. Wyschogrod, R. Cunninghan, and M. Zissman, "Evaluating Intrusion Detection Systems: The 1998 DARPA Off-line Intrusion Detection Evaluation," DARPA Information Survivability Conference and Exposition, Jan 2000.

[2]. R. Lippmann, J. Haines, D. Fried, J. Korba, and K. Das., "Analysis and Results of the 1999 DARPA Off-line Intrusion Detection Evaluation," Recent Advances in Intrusion Detection (RAID 2000), Oct 2000.

[3]. J. Allen, A. Christie, W. Fithen, J. McHugh, J. Pickel, and E. Stoner, "State of the Practice of Intrusion Detection Technologies," Technical Report CMU/SEI-99-TR-028, CMU/SEI, 2000.

[4]. T. H. Ptacek and T. N. Newsham, "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection," Technical report, Secure Networks Inc., Jan 1998.

[5]. V. Paxson, "Bro: A System for Detecting Network Intruders in Real-time," Computer Networks, 31(23-24), Dec 1999.

[6]. L.G. Roberts, "Beyond Moore's Law: Internet Growth Trends," IEEE Computer, pp. 117-119, Jan 2000.

[7]. P. A. Porras and P. G. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," National Information Systems Security Conference, Oct 1997.

[8]. G. Vigna, R. A. Kemmerer, and P. Blix, "Designing a Web of Highly-configurable Intrusion Detection Sensors," Recent Advances in Intrusion Detection (RAID 2001), Oct 2001.

[9]. J. Balasubramaniyan, J. Garcia-Fernandez, D. Isacoff, E. Spafford, and D. Zamboni, "An Architecture for Intrusion Detection using Autonomous Agents," 14th IEEE Computer Security Applications Conference, pp. 13-24, Dec 1998.

[10]. R. Gopalakrishna and E. H. Spafford, "A Framework for Distributed Intrusion Detection Using Interest-driven Cooperating Agents," Recent Advances in Intrusion Detection (RAID 2001), Oct 2001.