IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 6 (May. - Jun. 2013), PP 27-30
www.iosrjournals.org

A Study on Recent Trends and Developments in Intrusion Detection System

Madura sheetal [1], Manjunath CR [2], Santosh Naik[3]
[1,2] *Department of Computer Science and Engineering, Jain University*
[3] *Departments of Information Science and Engineering, Jain University*

Abstract :*Intrusion detection is the process of detecting unauthorized traffic on a network or a device. Intrusion Detection Systems (IDS) are designed to detect the real-time intrusions and to stop the attack. An IDS is a software or a physical device that monitors traffic on the network and detect unauthorized entry that violates security policy. We present in this paper the various Neural Network approaches adopted by the different Intrusion Detection Systems.*

Artificial Intelligence plays significantly role in intrusion detection. Machine learning can also be applied to intrusion detection systems. Artificial Neural Networks are modelled inline with the learning processes that take place in biological systems. The Neural Networks are basically consists of a set of inputs, some intermediate layers and one output. They are capable of identifying the patterns and its variations. They can be "trained" to produce an accurate output for a given input. Neural Networks are capable of predicting new observations from other observations after executing a process of so called learning from existing data.

Keywords: *Intrusion detection, Neural networks, Prevention system, Security, Technique, Traffic.*

I. Understanding Ids

Due to the variance in Network configuration, a number of IDS technologies have emerged. Each type has its own advantages and disadvantage in terms of detection, configuration, and overall cost.

1.1 Detection Technologies:

The few of the categories of the Detection technologies are, Network Based, Wireless, Network Behavior Anomaly Detection and Host-Based.

Network-Based: A Network Intrusion Detection System (NIDS) analyzes network traffic at every layer of the OSI model for suspicious activity.

Wireless: A wireless local area network (WLAN) IDS analyzes wireless-specific traffic, including scanning for unauthorized users trying to connect to active wireless network components.

Network Behavior Anomaly Detection: Network behavior anomaly detection (NBAD) analyzes network traffic to identify anomalies that exists if any.

Host-Based: Host-based intrusion detection systems (HIDS) analyzes system-specific settings including security policies, log audits and software calls.

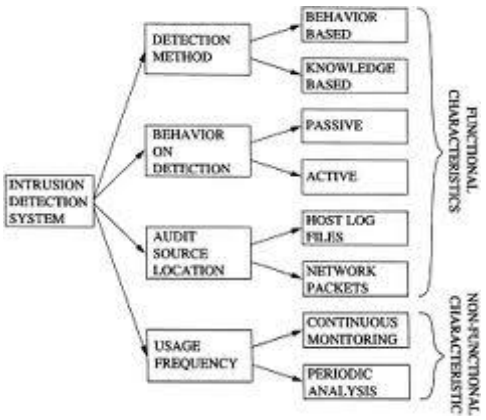

Figure1.Characteristics of intrusion-detection systems.

1.2 Detection Types

Few types of detections include, Signature-Based Detection, Anomaly-Based Detection and Stateful Protocol Inspection Signature -Based Detection: An IDS can use signature-based detection completely relying on known traffic data and analyzes potentially unwanted traffic. It has a limited detection capability, but can be

very accurate.Anomaly-Based Detection: An IDS analyzes the traffic on the network and detects incorrect, invalid and abnormal IP packets.A hybrid or compound detection system combines both approaches. In essence, a hybrid detection system is a signature inspired intrusion detection system that makes a decision using a "hybrid model" that is based on both the normal behavior of the system and the intrusive behavior of the Intruders Stateful Protocol Inspection: An IDS that inspects traffic at the network and transport layer including the vendor-specific traffic in the application layer for any malicious behavior.

II. Application of AI and Allied Techniques in IDS

Artificial Intelligence contributes significantly for intrusion detection in terms of data reduction, analyzing data to identify components and identifying the intruders. Artificial Intelligence could make the use of Intrusion Detection Systems. They could learn the preferences of the security officers and show the kind of alerts first that the officer has previously been most interested. As always, the hardest thing with learning AIs, is to make them learn the right things. AIs could learn the same things as a rule-based system by watching a security officer work. AIs could also link together events that, by themselves, are insignificant but when combined may indicate that an attack is underway.

AI and machine learning could be applied to intrusion detection systems by using concept learning, Clustering, Predictive learning and ability to extract relevant features from irrelevant data and the possibility of combining relevant features into functions that identify intrusive events.

There are several different soft computing techniques and algorithms that can be successfully used to detect intrusions. These techniques include: Fuzzy logic, Probabilistic reasoning, neural networks, Genetic algorithms and combinations of these can also be used. For example, genetic algorithms can be used to build neural networks and probabilistic reasoning can be built on fuzzy logic.

Neural Networks provides a value addition to IDS because of its flexible pattern recognition capability and effectively handle intrusive events. Neural Networks are useful in identifying gradual changes to the system. Application of AI, machine learning techniques, and neural networks could result in the development of a comprehensive intrusion detection system.

III. Off The Shelf Ids Tools

The several typical features were usually given due importance the study of different products. They are : **flexibility** of adaptation for any network which needs to be monitored, **suitability** for IDS architecture, **protection** against malicious attacks, **interoperability** with various network management tools, **comprehensiveness** to extend the intrusion detection mechanism to block program plug-ins viz. Java applets or Active-X controls, **event management** to manage and report the event traces and update the existing attack database, **active response** during occurrences of attacks, such as reconfiguration of router or a firewall and **support** for the product.

The IPS market is composed of stand-alone appliances that inspect all network traffic that has passed through frontline security devices, such as firewalls, Web security gateways and email security gateways. IPS devices are deployed in line and perform full-stream reassembly of network traffic. They provide detection via several methods — signatures, protocol anomaly detection, behavioral or heuristics. By being in-line, IPSs can also use various techniques to block attacks that are identified with high confidence. The capabilities of IPS products need to adapt to changing threats, and next-generation IPSs have evolved in response to advanced targeted threats evading first-generation IPSs.

Gartner is an information technology research and advisory company providing technology related insight. Research provided by Gartner is targeted at CIOs and senior IT leaders in industries that include government agencies, high-tech and telecom enterprises, professional services firms, and technology investors. The Following figure shows Gartner's report on IT Security leaders.

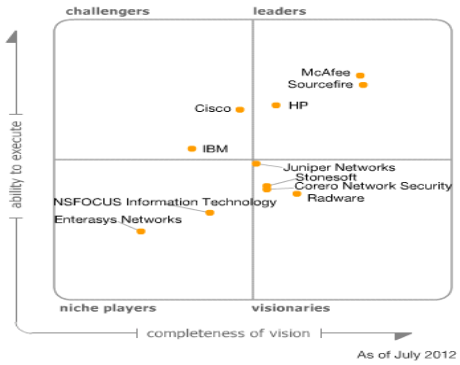

Figure 2 Gartner's Magic Quadrant

IV. Open Source Tools

The Open Source tools include Snort, another freely-available vulnerability-assessment tool is Nessus, a Linux-based vulnerability scanner (http://www.nessus.org)

Some commercial IDS providers use Snort and/or Snort signatures for their appliances, which gives Snort credibility in this direction. But different organizations have different needs. While for big enterprises open source IDS systems might not be enough, since they are the target of the most sophisticated attacks, the smaller and medium-sized businesses can protect their intranet for free or at a fraction of the price of a commercial system. However, even for the companies choosing commercial IDS, tools like Snort, OSSEC or Prelude can be used for 'a second opinion'.

V. Intrusion Prevention Systems

IPS contains all features of IDS with two more improvements

- IPS moves beyond simple attack signature detection to add vulnerability based signatures and non-signature detection capabilities
- Network IPS sensors operate in line at wire speeds to enable automated blocking and mitigation of attacks.

The new and enhanced automated techniques have improved detection abilities. These vulnerabilities facilitate attacks on computer systems by reducing the amount of effort required by an intruder to gain access. The structured software engineering techniques eliminates numerous potential sources of insecurity. The available development techniques would eliminate the three types of flaws.

1. The structured software validation and verification methods will reduce errors due Design flaws which result from inaccurate interpretation of software requirements and the improper analysis of the intended design of the system.
2. Faults within the application occur from the development of computer code which does not follow the defined specifications of the intended application. The complete eradication of all coding errors is extremely difficult, if not impossible, to achieve. However, the investment in the reduction of software faults offers the return of increasingly secure systems.
3. Operational and administrative flaws are those which result from the improper configuration of applications, operating systems, and security systems. These flaws are also difficult to eliminate completely, but the removal of configuration errors which are commonly known greatly enhances the security of the system.

VI. Intrusion Verification Systems

Recently, intrusion detection systems (IDSs) have been increasingly brought to task for failing to meet the expectations of researchers and vendors. Promises that IDSs would be capable of reliably identifying malicious activity never turned into reality. While virus scanners and firewalls have visible benefits and remain virtually unnoticed during normal operation, intrusion detection systems are known for producing a large number of alerts that are either not related to malicious activity or not representative of a successful attack. Although tuning and proper configuration may eliminate the most obvious spurious alerts, the problem of the vast imbalance between actual and false or non-relevant alerts remains.

The problem is that the concept of network-awareness is not broad enough to completely capture the complexity that is at the core of excessive amounts of false alarms. When a sensor outputs an alert, there are three possibilities. Alert verification is a term that we use for all mechanisms that can help to determine whether an attack was successful or not. This information is passed to the intrusion detection system to help differentiate between type-1 (The sensor has correctly identified a successful attack. This alert is most likely relevant) alerts on one hand and type-2 (The sensor has correctly identified an attack, but the attack failed to meet its objectives) and type-3 (The sensor incorrectly identified an event as an attack. The alert represents incorrect information) alerts on the other hand. When the success of an attack is a priori impossible (e.g., no vulnerable service is running) or cannot be verified (e.g., the attack failed because incorrect offsets were used), the IDS can react accordingly and suppress the alert or reduce its priority.

VII. Conclusion

The study indicates that intrusion detection system will be replaced by intrusion prevention systems. With the advent of IPS and IVS the Organizations will have cutting edge technological solutions in providing a stronger defense against attacks.

Security is an utmost priority of any organization, but this costs the exchequer of the organization. So, more and more organizations are leaning towards cost effective solutions like open source IDS tools which are equally efficient in providing defense.

References

[1] Zhang Wei, Wang Hao-yu, 2010, Intrusive Detection Systems Design based on BP Neural Network, IEEE.
[2] Paulo M. Mafra, Vinicius Moll, Joni da Silva Fraga, 2010, Octopus-IIDS: An Anomaly Based Intelligent Intrusion Detection System, IEEE.
[3] Milan Tuba, Dusan Bulatovic, 2010, Design of an Intrusion Detection System Based on Bayesian Networks, ACM.
[4] Naeeam Seilya, Taghi M. Khoshgoftaar, "Active Learning with Neural Networks for Intrusion Detection" Knowledge Discovery and Data Mining, 2010.WKDD '10. 3rd International Conference on, Jan. 2010, pp. 601–604.
[5] Iftikhar Ahmad, Azween B Abdullah, Abdullah S Alghamdi "Comparative Analysis of Intrusion Detection Approaches", 2010 12th International Conference on Computer.
[6] G. Liu, Z. Yi, and S. Yang, "A hierarchical intrusion detection model based on the pca neural networks," Journal of Information Science and Technology, pp. 1561–1568, 2006.
[7] G. Giacinto, F. Roli, and L. Didaci, Fusion of multiple classifiers for intrusion detection in computer networks, 2003.
[8] R. Mukkamala, J. Gagnon, and S. Jajodia, "Integrating data mining techniques with intrusion detection methods," in Advances in Database and Information Systems Security, 2000.
[9] T. Lunt, "Detecting intruders in computer systems," in Conference on Auditing and Computer Technology, 1993.