JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Internet Security: Intrusion Detection Systems (IDS)

Vinit Mehta[1], Prabhakar Pal[2]

[1]BE Electronics and Telecommunication Engineering Student, Atharva College of Engineering, Mumbai, India, Mumbai University

[2]BE Electronics and Telecommunication Engineering Student, Atharva College of Engineering, Mumbai, India, Mumbai University

Abstract:
In the modern times with an exponential increase in digitization, the world is reaching new heights in computerization and networking as each and every being is interconnected to each other via some network to increase efficiency and advancements. The digital era has many merits which supports the new technological demands of the world, but with merits there are also obstacles which might hinder the usual workflow of the environment. Many intruders, hackers or unethical users of this digital platform can exploit to harm the system or network of another person. These intruders generally hack the system for a ransom in return. An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies.

Keywords*:*
Intrusion Detection System, Intrusion Prevention System, Security, Intruder. IDPS, Network Security

I. Introduction:

In the past two decades with the rapid progress in the Internet based technology, new application areas for computer network have emerged. At the same time, wide spread application in areas in business, financial, industry, security and healthcare sectors made us more dependent on the computer networks. All of these application areas made the network an attractive target for the abuse and a big vulnerability for the community. In addition to the hacking, new entities like worms, Trojans and viruses introduced more panic into the networked society. As the current situation is a relatively new phenomenon, network defences are weak. However, due to the popularity of the computer networks, their connectivity and our ever-growing dependency on them, realization of the threat can have devastating consequences. Securing such an important infrastructure has become the priority one research area for many researchers. Aim of this paper is to review the current trends in Intrusion Detection Systems (IDS) and to analyse some current problems that exist in this research area. In comparison to some mature and well settled research areas, IDS is a young field of research. However, due to its mission critical nature, it has attracted significant attention towards itself. The Intrusion detection system is about the firewall security. The firewall protects an organization from the malicious attacks from the Internet and the IDS detects if someone tries to access in through the firewall or manages to break in the firewall security and tries to have an access on any system in the organization and alerts the system administrator if there is an undesired activity in the firewall. Therefore, an Intrusion detection system (IDS) is a security system that monitors network traffic and computer systems and works to analyse that traffic for possible hostile attacks originating from outside the organization and also for misuse of system or attacks originating from inside the organization

II. Need:

Now a day’s internet has become part of our daily life infect, the business world is getting connected to Internet. Number of peoples are getting connected to the Internet every day to take advantage of the new business model which is known as e-Business. Connectivity enhancement has therefore become very critical aspect of today's e- business.

There are two phases of business on the Internet. First phase is the Internet brings in outstanding potential to business in terms of reaching the users and at the same time it also

brings a lot of risk to the business. There are both harmless and harmful users on the Internet. Whereas an organization makes its information system accessible to harmless Internet users. Malicious users or hackers can also get an access to organization’s internal systems in various reasons. These are,

- Software bugs called vulnerabilities in a system
- Failure in administration security
- Leaving systems to default configuration

The intruders are use different types of techniques like Password cracking, peer-to-peer attack, sniffing attack, Dos attacks, Eavesdropping attack, Application layer attack etc. to exploit the system vulnerabilities mentioned above and compromise critical systems. Therefore, there required to be some kind of security to the private resources of the organization from the Internet as well as from users inside the organization.

III. Types of Intrusion Detection Systems:

There are four types of Intrusion Detection systems. These are network-based Intrusion Detection System and host-based Intrusion Detection System.

1. Network-based intrusion detection system (NIDS)

NIDS is used to monitor and analyse network traffic to protect a system from network-based threats. A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network.

NIDS works by examining a variety of data points from different sources within the network. Packet headers, statistics, and protocol/application data flows are analysed to determine whether malicious or anomalous activity has taken place. It can be used to identify possible security breaches on a system including sniffers and attacks on services such as HTTP/S, SMB, SSH etc.

2. Host-based intrusion detection system (HIDS)

A host-based IDS is an intrusion detection system that monitors the computer infrastructure on which it is installed, analysing traffic and logging malicious behaviour. An HIDS gives you deep visibility into what's happening on your critical security systems. With it, you can detect and respond to malicious or anomalous activities that are discovered in your environment.

On its own, host intrusion detection does not give you a complete picture of your security posture. You must be able to correlate your HIDS log data with other critical security data and with the latest real-world threat intelligence**.**

3. Protocol-based Intrusion Detection System (PIDS):

Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

4. Application Protocol-based Intrusion Detection System (APIDS):

Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

5. Hybrid Intrusion Detection System:

Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system.

IV. Intrusion Detection Techniques:

1. Signature-based Method:

Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

2. Anomaly-based Method:

Anomaly-based IDS was introduced to detect unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

3.Unauthorized Access Detection:

In this IDS is configured to detect access violations using an access control list. The ACL contains access control policies, and it uses the IP address of users to verify their request.

4. Protocol Anomaly Detection:

The anomaly detector detects the traffic that does not match the existing protocol standards.

V. Tools for IDS

The wide array of intrusion detection products available today (freely available of commercial) addresses a range of organizational security goals and considerations.

SNORT -

This lightweight network intrusion detection and prevention system excels at traffic analysis and packet logging on IP networks. It detects threats, such as buffer overflows, stealth port scans, CGI attacks, SMB probes and NetBIOS queries, NMAP and other port scanners and DDoS clients, and alerts the user about them. It develops a new signature to find vulnerabilities. It records packets in their human-readable form from the IP address.

OSSEC – HIDS –

It is scalable, multi-platform, open source Host-based Intrusion Detection System (HIDS). It has a powerful correlation and analysis engine, integrating log analysis; file integrity checking; Windows registry monitoring; centralized policy enforcement; rootkit detection; real-time alerting and active response.

FRAGROUTE –

It is a one-way fragmenting router - IP packets get sent from the attacker to the Fragrouter, which transforms them into a fragmented data stream to forward to the victim. Fragrouter helps an attacker launch IP-based attacks while avoiding detection.

METASPLOIT - It is an advanced open-source platform for developing, testing, and using exploit code. It ships with hundreds of exploits, as you can see in their online exploit building demo. This makes writing your own exploits easier, and it certainly beats scouring the darkest corners of the Internet for illicit shell code of dubious quality.

TRIPWIRE –

It Detects Improper Change, including additions to, deletions from and modifications of file systems
and identifies the source. It Simplifies and Eases Management of Change Monitoring Policies.

VI. Principles and Assumptions in Intrusion Detection

Denning defines the principle for characterizing a system under attack. The principle states that for a system which is not under attack, the following three conditions hold true:

1. Actions of users conform to statistically predictable patterns.

2. Actions of users do not include sequences which violate the security policy.

3. Actions of every process correspond to a set of specifications which describe what the process is allowed to do.

Systems under attack do not meet at least one of the three conditions. Further, intrusion detection is based upon some assumptions which are true regardless of the approach adopted by the intrusion detection system. These assumptions are:

1. There exists a security policy which defines the normal and (or) the abnormal usage of every resource.

2. The patterns generated during the abnormal system usage are different from the patterns generated during the normal usage of the system; i.e., the abnormal and normal usage of a system results in different system behaviour. This difference in behaviour can be used to detect intrusions.

VII. Drawbacks of IDS

With the increasing amounts of traffic through our networks, performance is an important factor in any decision that is made regarding an organization's network. As explained in the discussion of anomaly-based intrusion detection above, modern IDSs generate a lot of false alarms. When deviations from the norm are detected, alerts are triggered. This gives rise to so many alarms, most of which tend to be baseless, that network administrators are wont to skim over the warnings and thereby miss the signals of a lethal attack. One way of dealing with this is to specify stricter rules as to what constitutes an attack. With more comparisons that need to be made in order to trigger off an alarm, there are network performance hits, which is a very niggling worry for today's administrators. Besides the performance issue, more specific patterns for intrusion detection mean that in order to be detected, future attacks on the system must match every aspect of the new, stricter rules. This means that penetration attempts that are slight variations of attacks that occurred in the past, but don't match them exactly, have a high likelihood of entering undetected.

VIII. Conclusion

IDS tools are becoming the need for the day and for security not only in the corporate world but also for network users. Security incidents are becoming more and more common and measures have to be taken to curb such incidents. IDS are becoming the main part for many organizations after deploying firewall technology at the network perimeter. IDS can offer protection from external users and internal attackers, where traffic doesn't go past the firewall at all. there are still many challenges to overcome.

Improving, mining, and reducing intrusion detection data are critical to dealing with multisensory architectures of the future. Fast and flexible detection techniques are necessary to identify the vast variety of clever and unusual attacks we will undoubtedly encounter. Finally, cooperation with not only other IDS but also other network security components is mandatory to achieving a holistic network security posture for organizations of the future.

IX. References

1. M. Tanase, "The Future of IDS", *SecurityFocus*, 2001.

2. Peyman Kabiri and Ali A. Ghorbani. Research on Intrusion Detection and Response: A Survey. International Journal of Network Security, 1(2):84–102, 2005.

3. Intrusion Detection Tools and Techniques –A Survey Karthikeyan. K.R1 and A. Indra2 International Journal of Computer Theory and Engineering, Vol.2, No.6, December, 20101793-8201

4. A Research Paper on Hybrid Intrusion Detection System Amit Kumar, Harish Chandra Maurya, Rahul Misra International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.

5. Intrusion Detection and Prevention Response based on Signature-Based and Anomaly-Based: Investigation Study (IJCSIS) International Journal of Computer Science and Information Security, Vol. 10, No. 6, June 2012.

6. INTRUSION DETECTION SYSTEM International Journal of Technical Research and Applications 5(2):2320-8163 April 2017