Vol. 3 No. 1 July 2015 ISSN: 2321 – 788X

A NOVEL ALGORITHM TO MINIMIZE FALSE ALARM IN NETWORK INTRUSION DETECTION SYSTEM

S. Prabavathi
Post Graduate Student, Assistant Professor

M. Rathnasabapathy
School of Information Technology, Madurai Kamaraj University, Madurai

Abstract

Network intrusion detection systems (NIDS) are widely deployed in various network environments. Compared to an anomaly based NIDS, a signature-based NIDS is more popular in real-world applications, because of its relatively lower false alarm rate. In today's era the security of computer system is of great concern. Because the last few years have seen a dramatic increase in the number of attacks, intrusion detection has become the mainstream of information assurance. While firewalls do provide some protection, they do not provide full protection and still need to be complimented by an intrusion detection system (IDS). Data mining techniques are a new approach for Intrusion detection. IDS system can be developed using individual algorithms like classification, neural networks, clustering etc. Such system yields good detection rate and less false alarm rate. Recent studies show that as compared to the single algorithm, cascading of multiple algorithms gives much better performance. False alarm rate was also high in such system. Therefore combination of different algorithms is performed to solve this problem. This paper we uses three hybrid algorithms for developing the intrusion detection system to minimize false alarm rate such as Possible Attack Signature, Known Attack Detection and Possible Attack Detection.

Keywords*: Intrusion Detection, Packet Sniffer, Honey Pot, Data Mining, Signature, Attack Signature.*

Introduction

Due to the expansion of computer networks, the number of hacking and intrusion incidents is increasing year by year as technology rolls out, which has made many researchers focus on building systems called intrusion detection systems (IDSs). These systems are used to protect computer systems from the risk of theft and intruders. IDSs can be categorized as anomaly detection and misuse detection or signature detection systems. In anomaly detection, the system builds a profile of that which can be considered as normal or expected usage patterns over a period of time and triggers alarms for anything that deviates from this behavior. On the other hand, in misuse detection, the system identifies intrusions based on known intrusion techniques and triggers alarms by detecting known exploits or attacks based on their attack signatures. Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility. Intrusion detection is the process analyzing the computer events for,

- Signs of possible incidents

- Violations of Imminent threats & Security policies
- Violations of acceptable use policies

Intruder is an individual who gains or attempts to gain, unauthorized access to a computer system or to gain unauthorized privileges on that system. Generally referred as a hacker or cracker. The three classes of Intruders as follows,

A. Masquerader (Insider)

An individual or an unknown user who don't have access to a computer system, penetrates system and exploits user account.

B. Misfeasor (Outsider)

A known user who accesses data, programs or resources for which such access is not authorized and misuses his or her privileges.

C. Clandestine user (Either insider or outsider)

An individual who seizes supervisory control of the system and uses this control to avoid auditing and access controls or to suppress audit collection.

Intruder attacks range from the benign to the serious. At the least end, people want to explore internets and see the content. At the serious end, individuals may release privileged data, disrupt the system and perform unauthorized modification on data.

Noticed attacks performed by the Intruder

- Attempts to copy the password file once every other day.
- Suspicious remote procedure call once per week.
- Attempts to connect to non-existent 'bait' machines at least every two weeks.
- There are two levels of hackers,
- High level - Sophisticated users with a thorough knowledge of the technology.
- Low level - 'Foot soldiers' who merely used the supplied cracking programs with little understanding of program.

Intrusion Techniques

The main aim of an intruder is to capture privileges against system or increase the range of privileges accessible on a system. A system must maintain a file that associates a password with each authorized user.

The main method of access gaining is through user/password. The password file can be protected in one of two ways as follows,

A. One-way Encryption

The system stores only an encrypted form of the user's password. When the user enters a password, the system encrypts that entered password and compares it with the stored values. The system performs one-way transformation in which the password is used to generate a key for the encryption function and in which a fixed length output is produced.

B. Access Control

Access to the password file is restricted to one or a very few accounts.

C. Techniques used by the Intruder to crack passwords

- Try default password used with standard accounts shipped with the system.
- Try all short passwords.
- Try words in system's online dictionary.
- Collect information about user and try their combination.
- Try user's phone number, SSN etc.,
- Try all legitimate license plate numbers.
- Use Trojan horse.
- Tap the line between a remote user and host system.

The methods from 1 to 6 are ways of guessing password. The counter measure to these attacks are, a system can simply reject any login after three password attempts. It's difficult for an intruder to connect to the host. The 7th method of attack is difficult to counter. The 8th method of attack is a matter of physical security. So it can be countered with link encryption techniques.

Advantages of Intrusion Detection System

- If an intrusion is detected quickly enough, the intruder can be identified and removed from the system before any data are compromised. Even if the detection is not sufficiently timely to preempt the intruder, the sooner that the intrusion is detected, leads to less amount of damage to the system.
- An effective intrusion detection system can serve as deterrent, so acting to prevent intrusions.
- Intrusion detection system enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

Approaches of Intrusion Detection

The Intrusion detection is based on the assumption that the behavior of the intruder differs from that of an original user behavior. Sometimes, the intruder actions or

behaviours overlap with legitimate user behaviours. So, the Intursion detection system creates 'false positives' (Authorized users identified as Intruders) and 'false negatives' (Intruders not identified as Intruders). So, the task of distinguishing between a masquerader and a legitimate user is easier than between misfeasor/ clandestine user and a legitimate user.

A. Statistical Anomaly Detection

Involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.

- Threshold Detection: This approaches involves defining thresholds, independent of user, for the frequency of occurrence of various events. Also it involves counting the number of occurrences of a specific event type over an interval of time. If the count exceeds the threshold value, then intrusion is assumed.
- Profile Based: A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts. It involves characterizing the past behavior of individual user or related groups of users and then detecting significant deviations.

B. Rule-based Detection

Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder. Also it detects intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is intrusion or not.

- Anomaly Detection: Rules are developed to detect deviation from previous usage patterns. It's similar to statistical anomaly detection in terms of its approach and its strength. With this approach, historical audit records are analyzed to identify usage patterns and to generate automatically rules for those patterns. Rules may represent past behavior patterns of users, programs, privileges, time slots, terminals and so on. Then the current behavior is observed and each transaction is matched against the set of rules to determine whether there is an intrusion or not. The advantage is it doesn't require knowledge of security vulnerabilities within the system.
- Penetration Identification: An expert system approach that searches for suspicious behavior. Here the rules are used to identify known penetrations or penetrations that would exploit weaknesses. The rules are specific to the machine and the operating system. The rules in this approach are generated by experts rather than by means of automated analysis of audit records. So the strength of this approach

depends on the skill of setting up the rules. Examples for the rules to detect or to assume intrusions are,

- Users must not write other user's files.
- Users should not read files in other user's personal directories.
- Users do not make copies of system programs.

In a nutshell, statistical approach attempt to define normal, or expected behavior, whereas rule-based approaches attempt to define proper behavior. In terms of the types of attackers listed earlier, statistical anomaly detection is effective against masqueraders, who are unlikely to mimic the behavior patterns of the accounts they appropriate. On the other hand, such techniques may be unable to deal with misfeasors. For such attacks, rule-based approaches may be able to recognize events and sequences that, in context, reveal penetration. In practice, a system may exhibit a combination of both approaches to be effective against a broad range of attacks.

Penetration Schemes

A. IDES Approach:

It's based on examination of audit records and those entries are matched against the rule base. If match is found, intrusion is assumed.

B. State Transition Model Approach:

This model is higher level model independent of specific audit records. It deals with general actions rather than the specific actions. Then the number of different auditable events map into a smaller number of actions, so the rule creation process is very simple.

Audit Records

A fundamental tool for intrusion detection is the audit record. Some record of ongoing activity by users must be maintained as input to an intrusion detection system. Basically, two plans are used:

A. Native Audit Records:

Virtually all multiuser operating systems include accounting software that collects information on user activity. The advantage of using this information is that no additional collection software is needed. The disadvantage is that the native audit records may not contain the needed information or may not contain it in a convenient form.

B. Detection-specific Audit Records:

A collection facility can be implemented that generates audit records containing only that information required by the intrusion detection system. One advantage of such an approach is that it could be made vender independent and ported to a variety of systems.

The disadvantage is the extra overhead involved in having, in effect, two accounting packages running on a machine.

Hybrid Approaches to Reduce False Alarm Rate

Network-based IDS monitors network traffic using techniques like packet sniffing to collect network traffic raw data. Pass the collected packet data information to Known Attack Detection against Known attack signatures. If the result is negative, Store the packet information in a Feature Data warehouse which can be used to detect intrusion using Data mining.

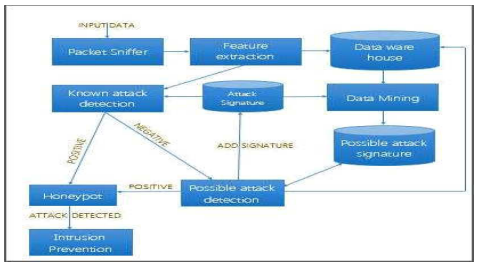

Fig.1. Diagram of the Architecture of Hybrid Approach to reduce false alarm rate

Generate pattern on Feature Data warehouse using Data Mining. Apply the known attack Signature on patterns generated through Data Mining. If there is some level of similarity, store in Possible attack Signature. Possible Attack Detector uses Possible Attack Signature database to detect whether traffic matches with possible attack signature generated by Data Mining. If possible Attack Detection or Known Attack Detection is positive have a closer look using Honey pot technique again to reduce the false alarm. After the Honey pot closer look turns out to be positive then the detected Attack would be raised.

Honeypot is a relatively innovation in Intrusion detection system are trap systems that are designed to attract a potential attacker away from critical systems. The functions of Honeypots are,

- Divert an attacker from accessing critical systems.
- Collect information about the attacker's activity.
- Encourage the attacker to stay on the system long enough for administrators to respond.

Proposed Algorithms

There are three different types of algorithms are derived such as Possible attack signature, Known attack detection and Possible attack detection to reduce the false alarm rate.

A. Possible Attack Signature

Input: Attack Signature Database (ASDB)
Output: Possible Attack Signature Database (PASDB)

Steps:

- Generate Patterns set from the Featured data ware house.
- Utilize Internet protocol address and the corresponding network's Mask IP as signature.
- Set the signature for each network.
    - Compare the similarity of new arrived signature with the existing pattern.
        If (Similarity = 0)
        Add pattern to Possible Attack Signature
    - Stop.

B. Known Attack Detection

Input: Network Traffic Feature, Attack Signature Database
Output: Traffic Classification (Norma/Attack)

Steps:

For each Signature in Known Signature Set

- If (Traffic Feature matches with Signature)
  Forward corresponding Connection to Intrusion Prevention module
  Mark corresponding entry in Feature Data Warehouse for attack
- Else
  Forward Network Traffic Feature to Possible Attack Signature detector

Conclusion

For many years attacks made on networks have risen dramatically. The major reason for this is the unlimited access to and use of software (written and uploaded to websites by technical experts) by inadequately trained people. Network disruptions may be caused intentionally by several types of directed attack. These attacks are made at various layers in the TCP/IP protocol suite, including the application layer. Besides the external body, attacks can be made on the network by the internal body as well. However, an IDPS is considered to be one of the best technologies to detect threats and attacks. NIDPSs have attracted the interest of many organizations and governments, and any Internet user can deploy them. An NIDPS usually features four stages to secure a computer system network: scanning, analyzing, detecting, and correcting. Our paper derived three algorithms such as Possible Attack Signature, Known Attack Detection and Possible Attack Detection to detect intruders and also reduce the false alarm rate. Now, we are implementing the algorithms in real time code with Derba database.

C. Possible Attack Detection

Input: Network Traffic Feature, Possible Attack Signature Database

Output: Traffic Classification (Norma/Attack)

Steps:

- For each Signature in Possible Signature Set
  - If (Traffic Feature matches with
  - Signature)
  - Forward corresponding Connection to Honey pot module to detect Intrusion.
- If (Result from Honeypot is Positive)
  - Remove Corresponding Signature entry from Possible Attack Signature Database.
  - Add removed Signature to Known Attack Signature Database.
- else
  - Remove Corresponding Signature entry from Possible Attack Signature Database.
- Mark corresponding Network Traffic Feature entry in
- Feature Data Warehouse for attack.

References

1. Abadeha, M.S, Habibia J, and Lucas C, 2007, "Intrusion detection using a fuzzy genetics-based learning algorithm", Journal of Network and Computer Applications, Science Direct, Vol.30, pp. 414-428.
2. Adam N, Atluri V, Bertino E, and Ferrari E,2002, "A content-based authorization model for digital libraries", IEEE Transactions on Knowledge and Data Engineering, Vol. 14, No.2, pp. 269-315.
3. Anderson, J.P,1980, "Computer security threat monitoring and surveillance" ,Technical Report, Fort Washington.
4. Ashfaq M.S, Farooq U and Karim A,2006, "Efficient rule generation for cost-sensitive misuse detection using genetic algorithms," in Proceedings of IEEE International Conference on Computational Intelligence and Security, Vol.1, pp. 282-285.
5. Bellovin S.M, 1994, "Network firewalls", IEEE Communications Magazine, Vol.32, pp. 50-57.
6. Bloedorn E, Christiansen AD, William Hill, Clement Skorupka, Talbot, LM., Jonathan Tivel (2001), "Data Mining for Network Intrusion Detection: How to Get Started", Technical paper.
7. Bridges S.M. and Vaughn R.B, 2000 "Fuzzy data mining and genetic algorithms applied to intrusion detection", in Proceedings of 12th Annual Canadian Information Technology Security Symposium, pp.109-122.

8. Crosbie M. and Spafford E, 1995 "Applying genetic programming to intrusion detection," in Proceedings of the AAAI Fall Symposium, pp. 1-8.
9. Dartigue C., Jang H.I. and Zeng W, 2009 "A new data-mining based approach for network intrusion detection," Proceedings of Seventh Annual Communication Networks and Services Research Conference, IEEE Computer Society, pp.372-377.
10. Debar H, Becker M, and Siboni D, 1992, "A neural network component for an intrusion detection system," in IEEE Symposium on Research in Computer Security and Privacy, pp. 240-250.
11. Denning, D.E , 1983, "Security model for the statistical database problem," in Proceedings of the Second International Workshop on Statistical Database Management, California, pp. 368-390.
12. Denning D.E. and Neumann P. G, 1985, "Requirements and model for IDES - A real-time intrusion detection system" , Computer Science Laboratory, SRI International, Menlo Park, California.
13. Denning, D.E, 1987, "An intrusion-detection model", IEEE Transaction on Software Engineering, Vol.13, pp. 222-232.
14. Esponda F, Forrest S, and Helman P,2004, "A formal framework for positive and negative detection schemes", IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics, Vol. 34, No. 1, pp. 357-373.
15. Fayyad UM, Piatetsky - Shapiro G, and Smyth P. (1996), "The KDD Process for Extracting useful Knowledge from Volumes of Data", Communications of the ACM, Pp. 273-276.
16. Gal A, and Atluri V,2000, "An Authorization model for temporal data," in Proceedings of the Seventh ACM Conference on Computer and Communication Security, Athens, Greece, pp. 144-153.