IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. IX (Mar-Apr. 2014), PP 82-84
www.iosrjournals.org

lntrusion Detection System Using GA

Ms.Lata Jadhav[1,] Prof.C.M.Gaikwad[2]
Dept. of Comp. Science & Engg. Govt. College of Engg. Aurangabad, India.
Dept.of Information Technology Govt. College of Engg. Aurangabad, India.

Abstract: *Intrusion detection has become an essential component of computer security in recent years so many technologies have been developed to protect our system or network from intruders such as antivirus, firewalls etc. so this paper describes the brief overview of Intrusion detection, genetic algorithm and related detection techniques.*

Keywords:*Information assurance, misuse intrusion detection, genetic algorithms, support-confidence framework, software development.*

I. Introduction

Intrusion detection systems (IDSs) are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyze them for security problems. As network attacks have increased and severity until now, so intrusion detection systems is essential to the security infrastructure of most organizations. Nowadays, many organizations and companies use Internet services as their communication and marketplace to do business such as at EBay and Amazon.com website. Together with the growth of computer network activities, the growing rate of network attacks has been advancing, impacting to make available, critical, and data integrity of information. Therefore a network system must use more than one security tools such as firewall, antivirus, IDS and Honey Pot to prevent important data from criminal enterprises.

A network system using a firewall only is not enough to prevent networks from all attack types. The firewall cannot defense the network against intrusion attempts during the opening port. Therefore IDSs have gained acceptance as a necessary addition to every organization's security infrastructure. There are several compelling There are several compelling reasons to acquire and use IDSs:

[1] To detect attacks and other security violations that is not prevented by other security measures.
[2] To document the existing threat to an organization.
[3] To act as quality control for security design and administration for huge enterprise.
[4] To provide useful information about intrusions that takes place, allows being improved diagnosis, recover, and corrective measures of causative factors.

II. Literature Survey

There are several types of intrusion detection system which are as follow:

1.1. Host-based system:

As stated earlier Host-based approaches detect intrusions utilizing audit data that are collected from the host machine [4]. As per the information of the review data can be tremendously inclusive and complicated, host based approaches can acquire high discovery rates and low false alarm rates. Host-based approaches cannot easily prevent attacks because when an intrusion is detected, the attack is partially occurred.

1.2. Network-Based system

Network-based approaches detect intrusions using the IP package information collected by the network hardware such as switches and routers. Such information is not as plentiful as the review data of the objective host machine[4][5].

1.3. Protocol based intrusion detection system (PIDS)

A protocol based intrusion detection system mainly operates with web server. Protocol based intrusion detection system usually installed on a web server in order to monitor and examine the number of protocols associated with the existing computer system. The protocol based intrusion detection system examines the run time or dynamic performance of the protocols as well as it keeps aye on the current status of the protocol. Protocol based intrusion detection typically work as agent in the system that always stands at front end of the server. It strictly verifies and examines the communication between the connected devices on network and the system on what it installed.

2.4 An Anomaly Based IDS (ABIDS)

An Anomaly Based Intrusion Detection System (ABIDS) is an intrusion detection system which is useful for verifying computer attacks as well as any type of error in monitoring or examining the system activity and mistakes in distinguish between normal and irregular. In this type of intrusion detection system the classification is mostly depends on the heuristics or rules instead on patterns or the signatures. An Anomaly Based Intrusion Detection System clever to identify any type of exploitation during normal system operation.

III. Proposed System

This system basically uses the genetic Algorithm. Genetic Algorithms is an optimization technique using an evolutionary process. A solution to a problem is represented as a data structure known as chromosome. The "goodness" of a solution is evaluated by an algorithm which is called as fitness function. A series of initial solutions is initially generated (random population) and through a combination of algorithms similar to an evolutionary process (often a combination

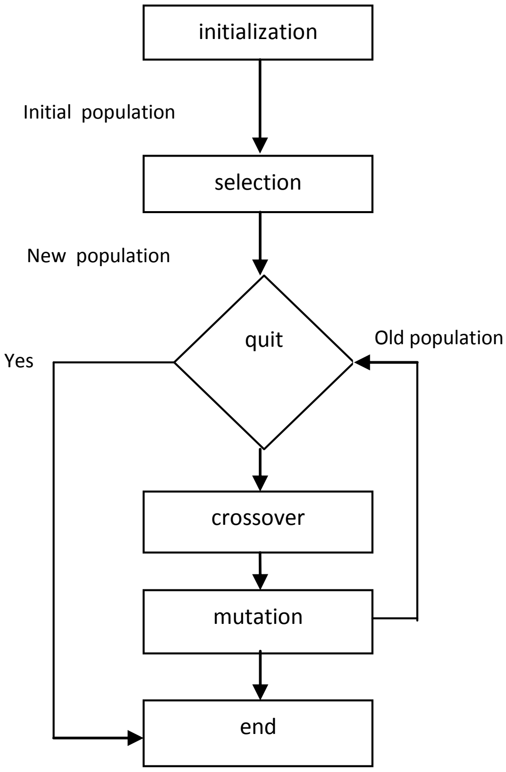

Figure1.Operation of GA

1.4. DARPA Data Sets

A key dependency of the work done by Gong and Li and as will be shown with netGA is the usage of DARPA data sets for training data[1]. Creating this training data is not a trivial task and is considered beyond the scope of this project. The MIT Lincoln laboratory provides an excellent description of the process followed for creating the data[3]. This DARPA training data is actually a result of test network traffic data, a Sun Microsystems Solaris and the use of Sun's Basic Security Module[Sun]. The data sets used in both papers were created in 1998. Today's attacks have changed with regard to rule based systems, but the training data still works well for developing Genetic Algorithms.

1.5. Detection Algorithm Overview

Listing 1 shows the major steps of the employed detection algorithm as well as the training process. It first generates the initial population, sets the defaults parameters, and loads the network audit data. Then the initial population is evolved for a number of generations.

Algorithm: Rule set generation using genetic algorithm.
Input: Network audit data, number of generations,and population size.
Output : A set of classification rules.

```
1. Initialize the population
2. $W1 = 0.2$, $W2 = 0.8$, $T = 0.5$
3. $N$ = total number of records in the training set
4. For each chromosome in the population
    5. $A = 0$, $AB = 0$
    6. For each record in the training set
        7. If the record matches the chromosome
            8. $AB = AB + 1$
        9. End if
        10. If the record matches only the “condition” part
            11. $A = A + 1$
        12. End if
    13. End for
    14. Fitness = $W1 * AB / N + W2 * AB / A$
    15. If Fitness > $T$
        16. Select the chromosome into new population
    17. End if
18. End for
19. For each chromosome in the new population
    20. Apply crossover operator to the chromosome
    21. Apply mutation operator to the chromosome
22. End for
23. If number of generations is not reached, then goto line 4
```

Listing 1. Major steps of the detection algorithm.

In each of the the qualities rules are firstly calculated, then a number of best-fit rules are selected, and finally the GA operators are applied to the selected rules. The training process starts by randomly generating an initial population of rules (line 1). The weights and fitness threshold values are initialized in line 2. Line 3. calculates the total number of records in the audit data. Lines 4-18 calculate the fitness of each rule and select the best-fit rules into new population. Lines 19-22 apply the crossover and mutation operators to each rule in the new population. Finally, line 23 checks and decides whether to terminate the training process or to enter the next generation to continue the evolution process.

IV. Conclusion

In this paper, a method of applying genetic algorithms for network intrusion detection is presented. In this study, we will propose the system for using genetic algorithm to derive a set of classification rules from network audit data and the support-confidence framework is utilized as fitness function to judge the quality of each rule. For dataset collection, we use DARPA dataset.

Acknowledgment

We would like to thank Prof.C.M.Gaikwad for valuable guidance at every step in making this paper. She motivated us and boosted our confidence and we must admit that the work would not have been accomplished with her guidance and encouragement.

References

[1] W. Li, “A Genetic Algorithm Approach to Network Intrusion Detection”, SANS Institute, USA, 2004.
[2] Li, Wei. 2002. “The integration of security sensors into the Intelligent Intrusion Detection System (IIDS) in a cluster environment.” Master’s Project Report. Department of Computer Science, Mississippi State University.
[3] MIT Lincoln Laboratory, DARPA datasets, MIT,USA, in November r 2004). http://www.ll.mit.edu/IST/ideval/data/data_index.html(accessed
[4] Base ,Rebecca:An introduction to Intrusion Detection & Assessment.Infidel Inc.prepared for ICAS Inc.Copyright 1998.
[5] Base ,Rebecca Gurley:IntroductionDetection Copyright 2000 by Macmillan Tchnical Publishing ISBN 1-57870-185-6.