INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Implementation of Genetic Algorithm on Intrusion Detection System to Enhance Result

Bhumit[1], Kanika Anand[2]

[1]M.Tech. CSE Student
R.N. College of Engineering & Technology
Haryana, India
[1]bhumit.saharan2008@gmail.com

[2]Asst. Professor
R.N. College of Engineering & Technology
Haryana, India

Abstract: *An Intruder is a hacker or cracker which always tries to get access to secure, system Intrusion occurs when an unauthorized person try to gain access or interrupt the normal operations of an information system. Even when such attacks are self-propagating, as in the case of worms, Trojan Horses and denial-of service attacks, they are almost always initiated by an individual whose purpose is to harm an organizational data. Intrusion detection consists of procedures for detection of illegal activity of system that identify the intruders. Some important Intrusion Prevention activities are writing and implementing good activity information security rule, planning and performing effective information security instructions, implementing and testing information security system for counting intruders activities like firewalls and IDS and IPS. In Information security Intrusion Detection Systems (IDS) works like a burglar alarm in that it detects destruction and activates an alarm. Recently new technology for IDS systems is the Intrusion Prevention System (IPS), which can detect an intrusion and also prevent that intrusion from attacking the organization. There is a system called Intrusion Detection/Prevention System (IDPS).Recently SNORT is a very useful tool for Network Based Intrusion Detection. A SNORT is tool which can give alert/alarm to the authentic user or Network Administrator by sending email or giving alarm for illegal network activities.*

Keywords: *Intrusion detection, Genetic algorithm, Data set, Client, Server.*

1. INTRODUCTION

Here we discuss how Genetic Algorithm (GA) can be used to increase performance over existing Network Intrusion Detection System. In existing system SNORT rule cannot be created at run time, expected behavior stored already in rule set. If the behavior of network connection deviates from expected normal behavior which is stored in rule set, it will be considered as intrusion. But motive of this paper is to generate rules at run time i.e. add the rule in rule set with time using genetic algorithm.

1.1 Need of Intrusion Detection System:

When we are working on the Internet it becomes our responsibility make our network more secure by using Network monitoring tools and making security settings and there are several other reasons to use an Intrusion Detection System.

- To detect attacks that are not prevented by other security activities
- To detect and deal with attacks
- To perform as quality organize for security design and administration
- To provide useful information about intrusions that do take place, allowing improved finding, improvement, and correction of contributing factors.

1.2 Types of intrusion detection system (IDS):

1. Network Based Intrusion Detection and Prevention System:- A Network Based IDS (NIDS) present in a computer or device connected to a segment of an organization's network and monitors network traffic on that network segment, looking for ongoing attacks. In network for maintain security to files many various Hashing algorithms are used like MD. When a circumstance occurs that the network-based IDS is planned to know an attack, it responds by sending notifications to administrators. NIDS looks for attack patterns within network traffic, such as wide collections of related variables that are of a certain type that could specify that a denial-of-service attack is ongoing, or it looks for the exchange of a sequence of related packets in a various pattern, which could indicate that a port scan is in progress. NIDSs are installed at a particular place in the network e.g router from where it is possible to watch the traffic going into and out of a particular network segment and it can be used to watch specific host computers on the network, or it can be installed to see all traffic between the computers that make a network. A fundamental problem for network intrusion detection systems (NIDSs) that passively monitor a network link is the ability of a skilled attacker to *evade*

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

detection by exploiting ambiguities in the traffic stream as seen by the NIDS[10].

2. Host Based Intrusion Detection System: - A Host Based Intrusion Detection System (HIDS) is situated on a particular system, known as the host, and check activity only on that system. Host-based intrusion detection systems can be further divided into two categories: signature-based and anomaly detection [11]. HIDS monitor the status of key system files and detect when an intruder creates, modifies, or deletes monitored files. The HIDS then give an alert message when one of the following changes occurs like: file contents change, new files are generated, or modification in the existing files. A HIDS has an advantage over NIDS in that it can usually be installed in such a way that it can get data that is coded when traveling from network to network.

1.3 Usefulness of HIDS:

- Logs. A HIDS can detect local events on host systems and also detect attacks that may avoid network-based IDS.
- HIDS encrypted traffic will have been decrypted and is available for processing.
- The use of switched network protocols does not affect a HIDS.
- A HIDS can find incompleteness in how applications and systems programs were used by checking the records stored in audit

1.4 Drawbacks of HIDSs:

- A HIDS is vulnerable to some denial-of-service attacks.
- A HIDS can use large amounts of disk space to retain the host OS audit logs, and, to role properly, it may require disk capacity to be added to the system.
- A HIDS can inflict a performance overhead on its host computer systems & in some cases may Reduce system performance below acceptable level

1.5 An IDS is composed of several composed Components:-

- Sensor: it is crucial to protecting your network..
- Console: provides various views & controls of the IDS.
- Engine: it store the events logged by sensors in a database.

2. RELATED WORK

We have concluded from the past research [5] that there are three factor of genetic algorithm:
1) Fitness function
2) Representation of individual
3) GA parameters.

Genetic Algorithm based IDS divided into two parts: Pre-calculation Phase & Intrusion Detection Phase. In Pre-calculation Phase different set of chromosomes is generated using training data in offline environment.[2] In Intrusion Detection phase generated rules are used to classify incoming network connections in real time environment using evaluation process i.e. selection, crossover and mutation .[2] After generating rule it is easy to detect intrusion. Pre-calculated data is used in this phase to find out fitness of each chromosome. In the real world the types of intrusion change and become complicated very rapidly. So, proposed detection system can upload and update new rules to the system. It is cost effective-[2] and adaptive.GA can be used to generate the rule for detecting normal and anomalous connections. These rules are stored in rule set in the form of if {condition} then {act}. Condition part check for matching the current network connection and rules in the rule set if any connection having same source & destination IP address, destination port number and connection time then this connection will be stop because it matches with the blacklisted IP address. Final goal of applying Genetic Algorithm is to create rule that match only anomalous connection. These rules are tested on historical connection and used to filter the new connection. This paper presents that implementation of GA is unique as it consider both temporal and spatial information of network connection during encoding the problem. If any function produces more and more new rule then add them to the existing rules. Functional advantage is that every time new rules generate, the number of rules overall doubles. So administrator has no need to keep account of all these rules.

3. INTRUSION DETECTION PREVENTION SYSTEM METHODS

IDPS provides multiplicity of detection methods to check and calculate approximately N/W traffic.

1. Signature Based Intrusion Detection System: - Signature-based detection is normally used for detecting known attacks. A signature-based ID is useful in data traffic which search patterns that match known signatures that is, predefined attack patterns. Signature-based IDS technology is mostly used because many attacks have clear and distinct signatures. In signature-based IDS is that every signature requires an entry in the database, and so a complete database contain many entries. Each packet is to be compared with all the entries in the database. [6]
2. Statistical Anomaly Based Intrusion Detection System: - In statistical-based techniques, the network traffic activity is checked and a profile

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

representing its stochastic behavior is created. This profile is based on metrics such as the traffic rate, no of packets for each protocol [7]. Anomaly-based intrusion detection fires an alarm on the IDS when some type of unusual behavior occurs on your network. This would include any activity, state, or behavior that is considered to be harmful by a pre-defined standard [8]. The Statistical Anomaly based IDS collects statistical summaries by observing traffic that is known to be normal. This normal period of examination establishes a performance baseline. The data that is measured from the normal traffic and is used to prepare the baseline can include variables such as host memory, network packet types, and no of packets. The advantage of this approach is that the Intrusion Detection System can detect new types of attacks because it is looking for unusual activities of any type.

3. Stateful Protocol Analysis Intrusion Detection Prevention System: - Stateful inspection improves on the functions of packet filters by tracking the state of connections and blocking packets that deviate from the expected state. As with packet filtering, Stateful inspection intercepts packets at the network layer and inspects them to see if they are permitted by an existing firewall rule, but unlike packet filtering, Stateful inspection keeps track of each connection in a state table. While the details of state table entries differ by firewall product, they typically include source and destination IP address, different port numbers, and connection state information [9]. Stateful protocol analysis (SPA) is a process of comparing predetermined profiles of generally usual definitions of benign activity for each protocol state against observed events to identify deviations. By storing relevant data detected in a session and then using that data to identify intrusions that involve multiple requests and responses.

3.1 How to Protect IDS Itself:

One major subject is how to protect the system on which your intrusion detection software is running. If security of the IDS is compromised, you may start getting false alarms or no alarms at all. The intruder may disable IDS before actually performing any attack. There are different ways to protect your system, starting from exceptionally wide-ranging recommendations to some sophisticated methods. Some of these are mentioned below.

- The first obsession that you can do is not to run any service on your IDS sensor itself. Network servers are the most common method of exploiting a system.
- New threats are discovered and patches are released by vendors. This is almost a continuous and non-stop process. The platform on which you are running IDS should be patched with the latest releases. For example, if Snort is running on a Microsoft Windows machine, you should have all the latest security patches from Microsoft installed.
- Configure the IDS machine so that it does not respond to ping (ICMP Echo-type) packets.
  If you are running Snort on a Linux machine, use net filter / iptable to block any unwanted data. Snort will still be able to see all of the data.

4. SNORT

SNORT is an open source ID that is used on Window or Linux operating system. Snort is rule based detection engine which is freely available. Snort is able to perform real time traffic, analysis, packet logging on Internet Protocol network. It can be detect different type of attacks [3]. By protocol analysis and content searching, snort find out many of worms, vulnerability exploit attempts, port scan and other behavior. Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify harmful activity, log information about such activity, try to block or stop such activities, and report activities. Intrusion prevention systems are considered extensions of intrusion detection systems because they both check network traffic and/or system activities for harmful activities. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected [1].Snort is divided in three modes:
Sniffer mode,
Packet logger mode,
Network Intrusion Detection System (NIDS) mode.

In sniffer mode it simply reads the packets of network and displays them on monitor screen.
Packet Logger mode it logs the packets to disk.
Network Intrusion Detection System Mode it allow snort to analyze network traffic for matches against user defined rule set.

4.1 PROBLEM IN EXISTING SYSTEM :

Snort performance evaluation:- F.Alserhana at el.[4] evaluated the performance of snort in high speed network. They were having two cases:-
1) Snort and attacker on different operating system platforms.
2) Snort and attacker on same operating system platform.
In the first case snort only find twenty percent (20) of

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

attack at 1.0 gbps speed of network traffic, when snort installed on Window XP and was generated from Linux 2.6. In second case snort detect 100% attack up to 400 mbps but only capture 30% of attack at 1.0 gbps. CPU utilization by snort is 80% at 500 mbps input traffic but only 30% at 1.0 gbps. So in this way performance of snort degrade as we increase network traffic. Different problem occur [5] in existing system. These problems are: Fidelity problem is caused when data packets traverse through long path and it can be modified by an attacker. Resource usage problem caused because component of IDS has to be run whole time while there is no intrusion occurred. Reliability problem raise because the component of intrusion detection system is implemented as separated programs, they are susceptible to tempering and an intruder can disable or modify them. So to overcome these problems we are using Genetic Algorithm [5].

5. GENETIC ALGORITHM

It is not technically feasible to build a system which is having no vulnerabilities. So, intrusion detection has become an important area of research. If an intrusion slightly deviates from the already defined pattern then it will consider as normal and if normal behavior slightly changes it may be treated as intrusion. Intrusion detection system offers various techniques which recognize and differentiate between normal and intrusion data. Genetic algorithm can be used to tune the membership function of IDS. Genetic Algorithm is a family of computational model based on principles of evolution and natural selection. Genetic Algorithm convert the problem into a model by using chromosomes like data structure and evolve the chromosomes using selection, recombination and mutation operator. GA begins with randomly selected population of chromosomes which represents the problem to be solved. An evaluation function is used to examine the "goodness" of each chromosome. The operation start from an initial population of randomly generated chromosomes population evolved for a number of generation and every time quality of an individual gradually increased. Three basic GA operators are applied to each individual i.e.

Selection,
Crossover,
Mutation.

Firstly a number of individual are selected based on user defined fitness function, the remaining are discarded. Next, a number of individual are selected and paired with each other. Each pair produces one offspring by applying crossover operator. At the end a certain number of individual are selected and mutation operator applied i.e. a randomly selected gene of individual abruptly changes its value [2].

5.1 Crossover Operator**:-** The parents' chromosomes are recombined by one of the crossover methods. It produces one or more new chromosome(s) called offspring(s). Such methods are: Single Point Crossover, Multipoint Crossover, Uniform Crossover and Arithmetic Crossover. Here is the example of single point crossover.

Document 1=100 | 110
Document 2=111 | 000

After applying crossover operator

Doc 1=100000
Doc2=111110

5.2 Mutation Operator:- New genetic material could be introduced into the new population through mutation process. Mutation in a way is the process of randomly disturbing genetic information. For each offspring mutation randomly alters some gene(s). Some encoding schemas: binary encoding and real-number encoding.

Firstly a number of individual are selected based on user defined fitness function, the remaining are discarded. Next, a number of individual are selected and paired with each other. Each pair produces one offspring by applying crossover operator. At the end a certain number of individual are selected and mutation operator applied i.e. a randomly selected gene of individual abruptly changes its value [2].

Data1=1 1 1 0 **1** 1 0

After applying mutation operator

Data 1=1 1 1 0 **0** 1 0

The result of mutation operator increases the diversity in the population.

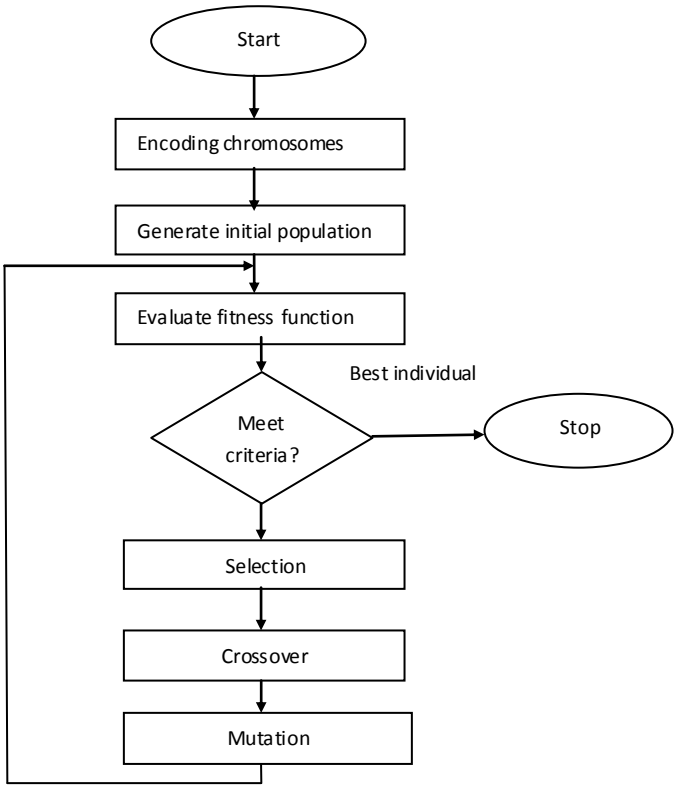

Figure1: Genetic algorithm process

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

REFERENCES

[1] NIST – Guide to Intrusion Detection and Prevention Systems (IDPS). 2007-02. Retrieved 2010-06-2.

[2] R. H. Gong, M. Zulkernine, and Purang, A software Implementation of a Genetic Algorithm Based Approach to Network Intrusion Detection‖, SNPD/SAWN'05, IEEE, 2005.

[3] K. Scarfone, and P. Mell, —Guide to Intusion Detection and Prevention Systems‖, National Institute of Standards and Technology NIST. Computer Security, 2007.

[4] F. Alserhani, Monis Akhlaq, I. U. Awan, A. J. Cullen, J. Mellor ,Pravin Mirchandani "Snort Performance Evaluation" Informatics Research Institute, University of Bradford,

[5] Bradford, BD7 1DP, United Kingdom. M.S. Hoque, M.A. Mukit, M.A.N. Bikas "An implementation of intrusion detection system using Genetic Algorithm" International Journal of Network Security & its Application (IJNSA),Vol.4,no.2,march 2012.

[6] Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents by Mueen Uddin1, Kamran Khowaja2 and Azizah Abdul Rehman in International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010 PP.129-141.

[7] Anomaly-based network intrusion detection: Techniques, systems and challenges by P. Garcı´a- Teodoro , J. Dı´az-Verdejo, G. Macia´-Ferna´ndez & E. Va´zquez in computers & security28 (2009) Elsevier PP.18-28

[8] Deciphering Detection Techniques: Part II Anomaly-Based Intrusion Detection By Dr. Fengmin Gong, Chief Scientist, McAfee Network Security Technologies Group Network Associates Your Netwok, our business March 2003.

[9] Guidelines on Firewalls and Firewall Policy by Karen Scarfone Paul Hoffman National Institute of standards and Technology sep-2009

[10] T. H. Ptacek and T. N. Newsham, "Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection", Secure Networks, Inc., Jan. 1998. http://www.aciri.org/vern/Ptacek-Newsham- Evasion-98.ps

[11] Mimicry Attacks on HostBased Intrusion Detection Systems by David Wagner & Paolo Soto *CCS'02,* November 18–22, 2002, Washington, DC, USA.