2012 International Conference on Industrial and Intelligent Information (ICIII 2012)
IPCSIT vol.31 (2012) © (2012) IACSIT Press, Singapore

Using Agent Based SNORT in Intrusion Detection Systems

Kamaruzaman Maskat [1], Mohd Afizi Mohd Shukran [2], Mohammad Adib Khairuddin [3]

[1,2,3] Faculty of Science and Defense Technology,
National Defense University of Malaysia Sungai Besi Camp,
57000 Kuala Lumpur, Malaysia.

Abstract. Intrusion Detection System (IDS) is used to detect intrusion and then alert the system administrator about the intrusion. This is what traditional IDS is all about. It is then up to the system administrator to deal with the intrusion. Human intervention is still needed when it comes to dealing with intrusion. This is because traditional IDS could only detect the intrusion but could not, on its own respond towards the intrusion. IDS is only able to alert the system administrator when it detects an intrusion. How and when the intrusion is dealt with is up to the system administrator. Human intervention when dealing with intrusion is not a problem if the person assigned to that task is always reliable. This perfect scenario is not the case in real life situation. To reduce human intervention when an intrusion is detected, we proposed Agent-Based IDS that has the ability to act autonomously when an intrusion is detected. The component of ABS consists of *Snort* as the IDS and *Aglets* as the mobile agent. *Snort* will log any intrusion it detected in a log file called Alert. The mobile agent platform which is known as *Tahiti* Server will initialize two mobile agents during startup; *abs.ReconAglet* and *abs.RespondAglet*. abs.ReconAglet is to read the Alert log file and if an intrusion occurred, it will inform *abs.RespondAglet* which will clone itself and migrate to drop the attacker's packet at the victim's host through firewall The intrusion or penetration test selected for this project is of DOS attacks types.

Keywords: SNORT, Intrusion Detection Systems, network security

1. Introduction

In today's modern world, more and more people are using the Internet for either personal or business purposes. According to the Internet usage statistics provided by Internetworldstats.com (2006), the latest data on Internet usage as of December 2005, shows that 1,018,057,389 people are using the Internet around the world. In the year 2006 it is expected that this number will increase up to 6,499,697,060 people using the Internet worldwide. The statistics shows that people around the globe are depending on information technology in doing their day-to-day activities such as reading the news, communicating via email, checking stock market prices, playing games, and so on. For organizations this is the opportunity to broaden their marketing area because Internet is not limited by geographical boundaries. More and more online marketing is done which is known as e-commerce. In doing e-commerce customers information is very important. In order to protect this information from falling into the wrong hands, a secure environment is needed during online transactions. One of the methods that could be used to established secure online transaction is by using secure socket layer (SSL).

Hackers and crackers are not always from outside an organization, they could also be from inside an organization. Organizations sometimes too concentrate in building defenses to prevent attacks from the outside forgetting about internal security. The organization's own staffs are also threats to the organization's security because anyone is a potential hacker or cracker once that person is using a computer. A system administrator may crossover his or her job responsibility by introducing malicious program such as worm into the organization's server. In this case the prevention security system implemented by the organization is rendered useless because such a system could only prevent threats that flow through and towards it but not after passing it. Another type of security system is clearly needed. The new security system should not replace the existing security prevention system but complement and work with existing security system in order to enhance security. This type of security system is known as Intrusion Detection System (IDS). As the name implies it will detect outside and inside intrusion and it will alert system administrator of the threats. In this paper, section 2 will describe the basic concept of IDS and section 3 will describe the proposed method which is the Agent Based SNORT (ABS). Finally, section 4 will present the conclusion.

2. Intrusion Detection System (IDS)

Earlier IDS whether it is a host based IDS or network based IDS, is using a central control method of collecting and analyzing data. This type of control raises some security and performance issues such as:

- If an attacker successfully penetrates the central control machine then the attacker will be able to control the entire network without being noticed.
- In a large network the data collected will take some time to reach the control center to be analyzed which will cause a delay in alarming the system administrator about an attack.
- More activities collected and analyzed will cause higher load to the network which leads to degrading of performance.
- If the network is down then the IDS will not be able to detect any suspectable activities.
- Incidents are recorded and alerted to system administrator via IDS, but if the incidents are too many then the system administrator will not be able to deal with or respond to all of those incidents.
- Attackers will try their best to attack IDS in order to stealth their movements.

As e-commerce activities increases so does cyber crime. Organizations are putting a large amount of effort in protecting themselves from threats whether from the outside or inside. An IDS is the type of safeguard which has become increasingly popular among organizations in conjunction with their purpose of enhancing their security system. IDS could detect intrusion from inside out of a network and then trigger an alarm to notify system administrator that an intrusion has occurred. The significance of this study is:

- To avoid single point of failure so that the network will not become easily penetrated without being detected.
- To make it difficult for intruders to sneak inside a network without being detected.
- To give system administrator more time to monitor large network by introducing mobile agent that has autonomous features so that it would not be too dependent on human intervention during an incident.

3. Proposed IDS method

The proposed method is called Agent Based SNORT or so called ABS. ABS architecture will be discussed in later section. There are three basics components, the intrusion detection, the mobile agent platform and the mobile agents. Briefly, ABS will rely on the intrusion detection component to detect intrusion using the misuse analysis method. Once an intrusion is detected the mobile agent will gather information about the attack and then respond to it autonomously. The mobile agent platform is where the mobile agents are initiated and used for mobile agent's mobility.

3.1 ABS Architecture

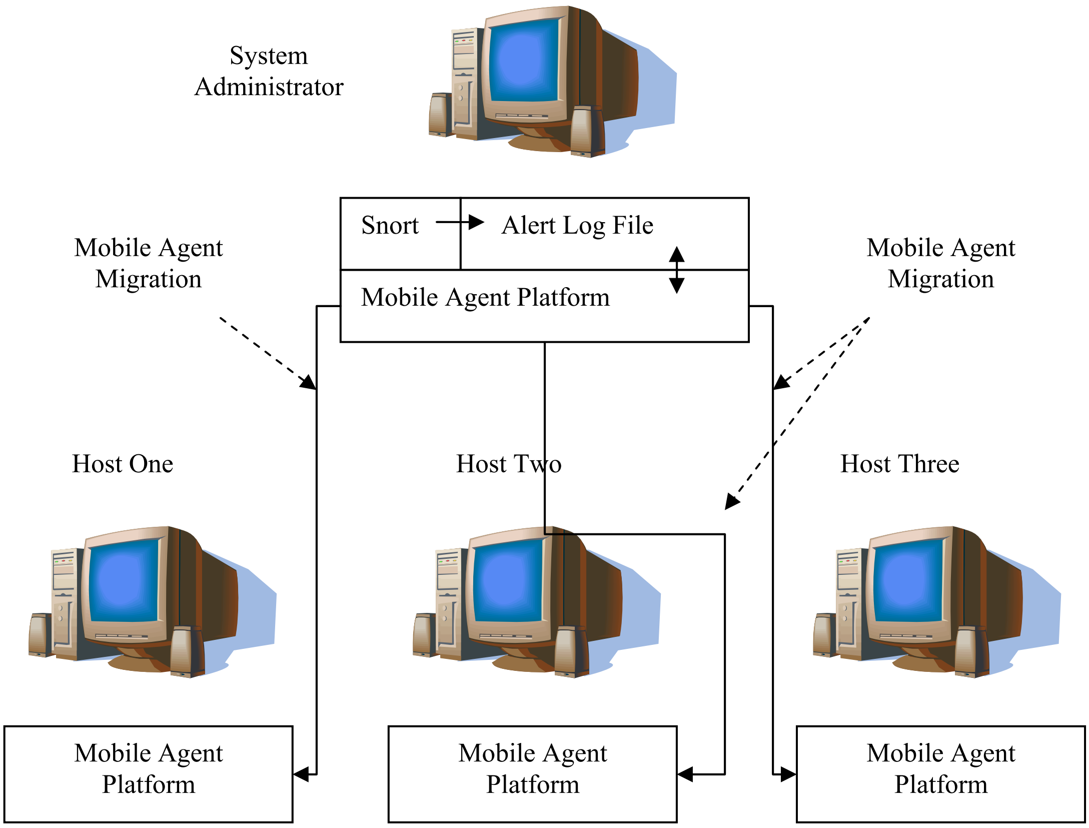

Figure 1: ABS Architecture

The ABS Architecture is as shown in Figure 1. At the system administrator host, Snort must be up and running before the Mobile Agent Platform is initiated. On startup the Mobile Agent Platform will initialize mobile agents. Other hosts must also have the Mobile Agent Platform started in order for the mobile agents to move from one host to another. If an intrusion is detected by Snort, the intrusion will be recorded or logged in the Alert Log File which is continuously read by a mobile agent. The mobile agent reading the Alert Log File will then inform another mobile agent that will clone itself first and then the cloned mobile agent will migrate to the targeted host and try to stop the intrusion. If the cloned mobile agent successfully stops the intrusion, it will inform the Mobile Agent Platform.

3.2 Architecture Components

3.2.1. Network Intrusion Detection System

Snort is an open source network intrusion detection system that has been chosen for this study. Snort comprises of multiple components that communicate with each other in order to detect intrusion according to its signature database, Snort basic components are as shown below while Figure 2 shows how these components work together:

- Packet Decoder
- Preprocessors
- Detection Engine
- Logging and Alerting System
- Output Modules

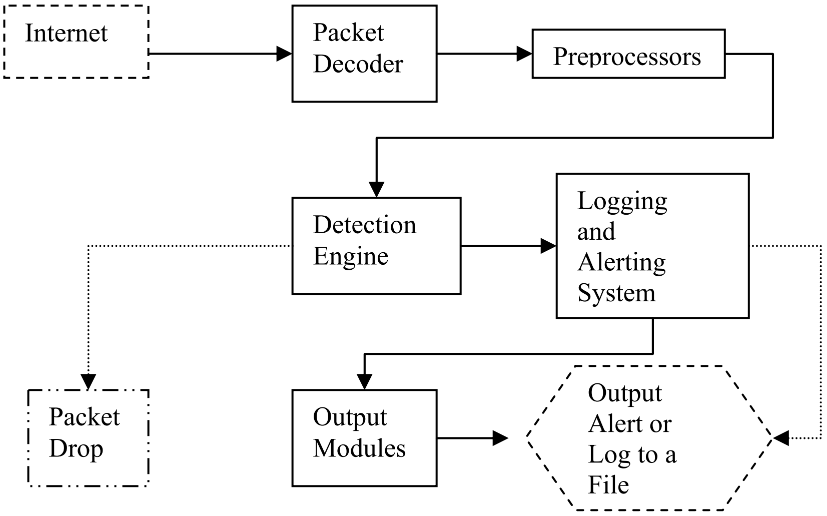

Figure 2: Snort Components Architecture

Snort produces two types of log files; Alert log file and Snort log file. Alert log file is used to log intrusions detected by the detection engine component using the signature based data stored in a file called Rules. Snort log file is where all packets activities are recorded. For all three types of DOS Attack chosen for this projects, the packets are captured by using Ethereal a network tools and analyze the attacks to come up with unique signatures of each attacks. After the signatures are ready, it will be stored in a rule file, for this study the rule file is named dos_attack.rule. The reason for not using snort's default rule files is because, when snort reads the DARPA 1999 evaluation data set, there are lots of other intrusions being detected which cause confusion and difficulties in identifying the attacks chosen for this study. Moreover the rule used to detect certain attacks is not under the appropriate name, for example, the Ping of Death attack rule is under Bad-Traffic.rule file not under DOS.rule file. How to write Snort rule is not going to be discussed here because it's quite a large topic, therefore to better understand about writing Snort rule, the Snort manual is the best document to refer to. It is available at http://www.snort.org/docs/.

3.2.2. Mobile Agent

Aglet is the mobile agent chosen for this study. Two mobile agents involved in the ABS system are *abs.ReconAglet* and *abs.RespondAglet*. *abs.ReconAglet* will be initiated when Tahiti server is activated. Once initiated, *abs.ReconAglet* will then initialized *abs.RespondAglet*. These mobile agents will autonomously execute their given tasks. *abs.ReconAglet* is responsible in reading snort's alert log file from time to time to search for any intrusion detected by snort. Because intrusion could happen anytime, *abs.ReconAglet* could be instructed to read the Alert log file in milliseconds. If there's an intrusion, *abs.ReconAglet* will gather information about the attack, which is the attacker and victim IP address, protocol and port. This information will then be passed to *abs.RespondAglet* using Aglet's message passing method. *abs.RespondAglet* as the name implies will respond to intrusion after receiving message from *abs.ReconAglet* by instructing the host's firewall to drop the attackers packets or closing ports where the intrusion is generated. *abs.RespondAglet* will move from host to host by cloning itself first at the system administrator host. The cloned *abs.RespondAglet* will then migrate to the targeted host. After successfully executing its task, *abs.RespongAglet* will pop up a window at the system administrator host before disposing itself in order not to congest the network or hosts with mobile agents. The changes made to the host firewall by *abs.RespondAglet* is not permanent, the firewall settings will go back to its default settings when the host is restarted. The intention of doing this is not to change the default settings that the system administrator has made to all hosts. Otherwise system administrator has to check each host in order to change the firewall settings back to its default settings.

3.2.3. Tahiti Server

Tahiti server is the platform for mobile agent Aglets and it has Graphical User Interface (GUI). Tahiti server is responsible for creating, disposing, cloning, kill, dispatching, retracting and so forth. In order for Aglets to move from host to host, *Tahiti* server must be installed at each host. *Tahiti* server at the system administrator host will initialize *abs.ReconAglet* as soon as it is executed. Then it will prompt the system administrator to select the location of the snort Alert log file. After that the system administrator is asked to key in the time interval for *abs.ReconAglet* to read the snort Alert log file in milliseconds.

4. Conclusion

In conclusion, Intrusion Detection System (IDS) in its traditional form is doing intrusion detection all by itself. Its function is to alert system administrator once an intrusion is detected. The system administrator then will take appropriate action to deal with the intrusion. Agent Based Snort (ABS) is proposed to discover whether the integration of IDS and Mobile Agent would lessen the human intervention when an intrusion is detected having the Mobile Agent autonomously respond towards the intrusion.

5. References

[1] Abraham, A. and Thomas, J. (2005). *Distributed Intrusion Detection Systems: A Computational Intelligence Approach.* Chung-Ang University.

[2] Abraham, A., Grosan, C., and Yuehui, Chen. (2005). *Cyber Security and the Evolution of Intrusion Detection Systems*. Chung-Ang University.

[3] Albag, H. (2001). *Network & Agent Based Intrusion Detection Systems*. Istanbul Technical University.

[4] Amal El Fallah-Seghrouchni and Alexandru Suna (2000). *An Unified Framework for Programming Autonomous, Intelligent and Mobile Agents*. University of Paris 6.

[5] Aslam, J., Cremonini, M., Kotz, D., and Rus, D. (2001). Using Mobile Agents for Analyzing Intrusion in Computer Networks. *In Proceedings of the Workshop on Mobile Object Systems at ECOOP 2001*. July. Hanover, NH. http://www.cs.dartmouth.edu/~dfk/papers/aslam:position.pdf

[6] Bace, R., and Mell, P. (2001). Intrusion Detection Systems. *Infidel, Inc., Scotts Valley, CA and National Institute of Standards and Technology.*

[7] Balasubramaniam, J. S., Garcia-Fernandez, J. O., Isaoof, D., Spafford, E., and Zamboni, D. (1998). An Architecture for Intrusion Detection Using Autonomous Agents. *COAST Technical Report 98/05*. June 11. Purdue University.

[8] Barrus, J. (1998). A Distributed Autonomous-Agent Network-Intrusion Detection and Response System. *Procedings of the 1998 Command and Control Research and Technology Symposium*. June-July. Monterey, CA. http://www.cs.nps.navy.mil/people/faculty/rowe/barruspap.html

[9] Basicevic, I., Popovic, M., and Kovacevic, V. (2005). The Use Of Distributed Network-Based IDS Systems In Detection Of Evasion Attacks. *Proceedings of the Advanced Industrial Conference on Telecommunications/Service Assurance with Partial and Intermittent Resources Conference/ELearning on Telecommunications Workshop*. Montenegro: IEEE.

[10] Bigus, P. J and Bigus, J. (2001). *Constructing Intelligent Agents Using Java*. Canada: John Wiley & Sons, Inc.

[11] Botha, M., Solms, R. V., Perry, K., Loubser, E., and Yamoyany, G. (2002). The Utilization of Artificial Intelligence in a Hybrid Intrusion Detection System. *Proceedings of SAICSIT 2002.* Port Elizabeth Technikon, 149 – 155.

[12] Brennan, M. P. (2002*). Using Snort For a Distributed Intrusion Detection System Version 1*. SANS Institute.

[13] Cardoso, R. C. and Freire, M. M. (2004). *Intelligent Assessment of Distributed Security in TCP/IP Networks*. University of Beira Interior.

[14] Columbia University DNAD Team. (2005). On The Feasibility of Distributed Intrusion Detection. Columbia University.

[15] Crosbie, M. J. and Kuperman, B. A. (2001). *A Building Block Approach to Intrusion Detection*. Hewlett-Packard Company,Purdue University.

[16] Curtis A. Carver, Jr., John M.D. Hill, John R. Surdu Member, IEEE, and Udo W. Pooch, Senior Member, IEEE. (2000). A Methodology for Using Intelligent Agents to provide Automated Intrusion Response. *Proceedings of the*

2000 IEEE Workshop on Information Assurance and Security. June 6-7. West Point, NY: IEEE, 110 – 116.

[17] Deeter, K., Singh, K., Wilson, S., Filipozzi, L., and Vuong, Son. (2005). *APHIDS: A Mobile Agent-Based Programmable Hybrid Intrusion Detection System*. University of British Columbia.

[18] Duda, R., Hart, P.E., nillson, J.J., Reboh, R., Slocum, j;, and Sutherland, G. (1997). Development of A Computer-based *Consultant for Mineral Exploration. In SRI Report*. Menlo Park, CA:Stanford Research Institute.

[19] Eanes, M. (2003). *Wanted Dead or Alive: Snort Intrusion Detection System*. SANS Institute.