International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 8 Ver V || Aug 2018 || PP 01-05

A Cross Encroachment detection system design for computer network security

Dr. Amamer Khalil Masoud Ahmidat, Muhamad Abdulla Muhamad Abdussalam
Higher Institute of Medical Technology in Baniwaleed, Libya
Higher Institute of Medical Technology ,Baniwalid, Libya
Corresponding author : Dr. Amamer Khalil Masoud Ahmidat

Abstract:*Encroachments detection systems (EDSs) are systems that try to detect attacks as they occur or after the attacks took place. EDSs collect network traffic information from some point on the network or computer system and then use this information to secure the network. Encroachment detection systems can be misuse-detection or anomaly detection based. Misuse-detection based EDSs can only detect known attacks whereas anomaly detection based EDSs can also detect new attacks by using heuristic methods. In this paper we propose a cross EDS by combining the two approaches in one system. The cross EDS is obtained by combining packet header anomaly detection and network traffic anomaly detection (NETAD) which are anomaly-based EDSs with the misuse-based EDS Snort which is an open-source project. The cross EDS obtained is evaluated using the MIT Lincoln Laboratories network traffic data (IDEVAL) as a test bed. Evaluation compares the number of attacks detected by misuse based EDS on its own, with the cross EDS obtained combining anomaly-based and misuse based EDSs and shows that the cross EDS is a more powerful system.*

Date of Submission: 17-08-2018 Date of acceptance: 31-08-2018

I. Introduction

Nowadays with the spreading of the Internet and online procedures requesting a secure channel, it has become an inevitable requirement to provide the network security. There are various threat sources including software bugs mostly as the operating systems and software used becomes more functional and larger in size. Intruders who do not have rights to access these data can steal valuable and private information belonging to network users. Firewalls are hardware or software systems placed in between two or more computer networks to stop the committed attacks, by isolating these networks using the rules and policies determined for them.

It is very clear that firewalls are not enough to secure a network completely because the attacks committed from outside of the network are stopped whereas inside attacks are not. This is the situation where Encroachments detection systems (EDSs) are in charge. EDSs are used in order to stop attacks, recover from them with the minimum loss or analyze the security problems so that they are not repeated.

EDSs collect information from a computer or a computer network in order to detect attacks and misuses of the system. Many EDSs only analyze the attacks and some of them try stopping the attack at the time of the Encroachment. Three types of data are used by EDSs. These are network traffic data, system level test data and system status files.

In ‘‘2003CSI/FBI Computer Crime and Security Survey” it has been stated that the EDS usage in 1999 had been 43% and this ratio has become 74% in year 2003. This great improvement shows that EDSs are very important as security technologies.

II. Encroachment detection systems

Encroachment detection systems are hardware and software systems that monitor events occurred on computers and computer networks in order to analyze security problems. The number and severity of these attacks has been increasing continuously. Consequently EDSs have become an integral part of the security infrastructure of organizations. Encroachments to computer networks are called as ‘‘attacks” and these attacks threaten the security of networks by violating privacy, integrity and accessibility mechanisms. Attacks can be originated from users who login to the computer using the Internet trying to gain super user or administrator rights and other users who misuse the rights they have. EDSs automate monitoring and analyzing the attacks.

EDS types

There are two approaches to analyzing of events using EDSs. These are misuse-based and anomaly-based approaches. Misuse- based EDSs aim to distinguish events that violate system policy. Anomaly-based EDSs try analyzing abnormal activities and flag these activities as attacks. Both approaches have advantages and disadvantages when compared to each other.

Snort is the most commonly used signature-based Encroachment detection system. Snort is a network Encroachment detection system that runs over IP networks analyzing real-time traffic for detection of misuses. Snort depends on a template-matching scheme and makes content analysis. It has the ability to flag alerts depending on pre-defined misuse rules and saves packets in TCP dump files or in plain text files. Snort is preferred to be used in academic research projects as it is an open source tool and for this reason we have also chosen Snort as the signature-based Encroachment detection system in our work.

Anomaly detection based Encroachment detection systems are separated into many sub-categories in the literature including statistical methodologies, data mining, artificial neural networks, genetic algorithms and immune systems. Among these sub-categories, statistical methods are the most commonly used ones in order to detect Encroachments by analyzing abnormal activities occurring in the network and NETAD statistical methods are chosen as the anomaly-based Encroachment detection systems in this paper. We have implemented a cross EDS by mounting anomaly based EDSs and NETAD to Snort as a preprocessor is different than the other conventional network-based anomaly detection systems for two reasons. First, it models protocols rather than user behaviors. Second, it uses a time-based model depending on the rapid change of network statistics in short term. Flags only the first anomaly it detected as an alert even if there is a series of the same anomaly recurring. This feature of helps reducing the number of false alerts. NETAD, models single packets like, uses dynamic-conditioned rules like ALAD, and rule verification like LERAD. Its greatest contribution is modeling values that are not new.

Misuse-based EDSs

Misuse detectors analyze system activities and try to find a match between these activities and known attacks having definitions or signatures introduced to the system beforehand.

Advantages:

- Misuse detectors are very efficient in detecting attacks without signaling false alarms (FA).
- Misuse detectors can quickly detect specially designed Encroachment tools and techniques.
- Misuse detectors provide systems administrators an easy to use tool to monitor their systems even if they are not security experts.

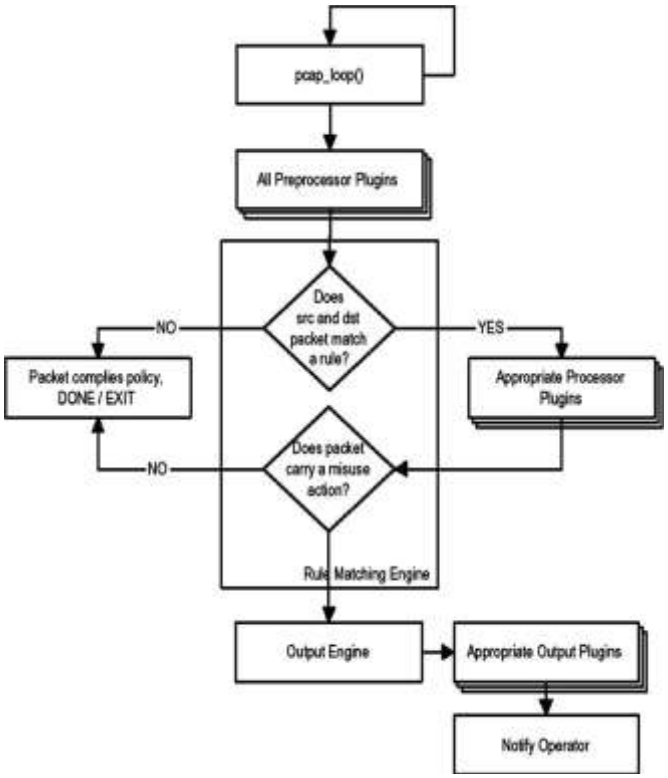
Disadvantages:

- Misuse detectors can only detect attacks known beforehand. For this reason the systems must be updated with newly discovered attack signatures.
- Misuse detectors are designed to detect attacks that have signatures introduced to the system only. When a well-known attack is changed slightly and a variant of that attack is obtained, the detector is unable to detect this variant of the same attack. Misuse-based EDS used in our cross EDS is the open-source project Snort.

Snort

A software engineer working on the computer security topics, has developed Snort in 1990 in order to detect attacks targeting his home network. Snort is a fast, signature-based and open-source EDS. It produces alarms using misuse rules defined previously. It uses binary TCP dump-formatted files or plain text files to capture network packets. TCP dump is a software program that captures network packets from computer networks and stores them in TCP dump-formatted files.

Snort is rule-based and it has a language to define new rules. Snort is an open-source project and it has an architecture making it possible to integrate new functionalities at the time of compilation.



Anomaly-based Encroachment detection systems

Anomaly detectors detect behaviors on a computer or computer network that are not normal. According to this approach, behaviors deviating from behaviors assumed as ‘‘normal” are thought to be attacks and anomaly detectors compute the deviation in order to detect these attacks. Anomaly detectors construct profiles of users, servers and network connections using their normal behaviors. These profiles are produced using the data that is accepted as normal. After the profile construction, detectors monitor new event data, compare the new data with obtained profile and try to detect deviations. These deviations from normal behaviors are flagged as attacks.

Advantages:

- Anomaly-based EDSs, superior to signature-based ones, are able to detect attacks even when detailed information of the attack does not exist.
- Anomaly-based detectors can be used to obtain signature information used by misuse-based EDS.

Disadvantages:

- Anomaly-based EDSs generally flag many false alarms (FA) just because user and network behavior are not always known beforehand.
- Anomaly-based approach requires a large set of training data that consist of system event log in order to construct normal behavior profile.

III. Evaluation of the cross EDS

Scientific advances rely on reproducibility of results so that they can be independently validated and compared. Much of the evaluation in Encroachment detection has been based on proprietary data and results are generally not reproducible. One of the main problems of releasing data stems from privacy concerns. To reduce this problem, Lincoln Laboratory (LL), under sponsorship of DARPA, created the IDEVAL datasets that serves as an evaluation benchmark.

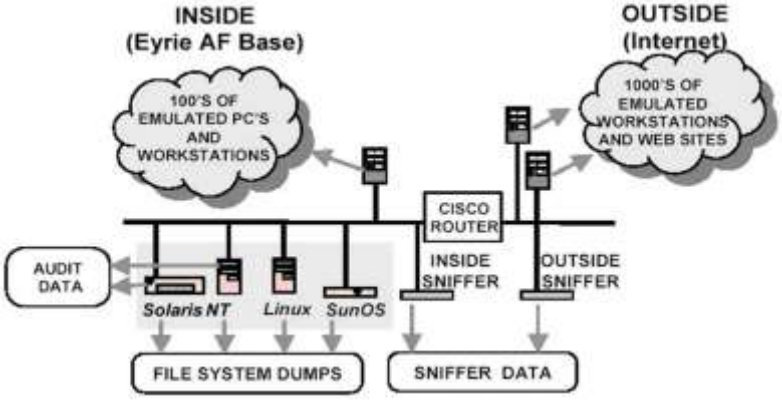
The goal of the 1998 DARPA Encroachment detection system evaluation was to collect and distribute the first standard corpus for evaluation of Encroachment detection systems. 1998 DARPA Encroachment detection system evaluation was generated and recorded on a network which simulated an operational network connected to the Internet. Automatically generated traffic

used more than 20 network services, including dns, finger, ftp, http, ident, ping, pop, smtp, snmp, telnet, time, and X. A Windows NT host is added to three UNIX based target hosts and twelve new Windows NT attacks were added in 1999 along with stealthy versions of many 1998 attacks, new inside console-based attacks and six new UNIX attacks. Fifty-six different attack types were used in the evaluation. Block diagram of the network from which Encroachment data is captured is illustrated in.

There are four main ‘‘victim” machines, running SunOS, Solaris, Linux, and Windows NT. Traffic generators simulate hundreds of other hosts and users running various applications and Internet. The evaluation data set is collected from the four victim machines and from two network sniffers, an ‘‘inside” sniffer between the router and the victims, and an ‘‘outside” sniffer between the router and the Internet. The 1999 evaluation had two phases separated by about three months. During the first phase, participants were provided with three weeks of data. The first and third weeks contained no attacks, and could be used to train anomaly detection systems. During the second phase, participants were provided with two weeks of test data (weeks 4 and 5) containing 201 unlabeled instances of 58 attacks, 40 of which were not in the training data. Attacks are classified by category (probe, DOS, R2L, U2R), the type of data examined (inside sniffer, outside sniffer, BSM, audit logs, file system dumps, or directory listings), victim operating system (SunOS, Solaris, Linux, or NT), and whether the attack is new.

Performance of Snort on IDEVAL data

Snort is tested on IDEVAL dataset (fourth and fifth weeks including attack) and the detected attacks are listed day by day. IDEVAL dataset files used for the test and the days each file belongs. These files have been downloaded from. Attacks detected on a daily bases are shown in Snort has detected 27 attacks out of 201 attacks available in IDEVAL data.



IV. Conclusion

Signature-based systems can only detect attacks that are known before whereas anomaly-based systems are able to detect unknown attacks. Anomaly-based EDSs make it possible to detect attacks whose signatures are not included in rule files.

NETAD are added one by one to signature-based EDS namely Snort as a preprocessor in this study. IDEVAL test bed which was created in MIT Lincoln Laboratories is used to evaluate the performance of new constructed cross EDS.

Firstly, Snort is tested on IDEVAL data and the number of attacks it detects is found. Secondly, anomaly detection system, , is added to Snort as a preprocessor and this new version of Snort (Snort +) is tested on the same data. There is an increase in the number of attacks detected in this case. Finally another anomaly detection system, NETAD, is added to version of Snort as a second preprocessor. This final system is called the cross EDS (Snort + + NETAD) and it is also tested on IDEVAL data. It is observed that number of attacks detected increases much more with the cross EDS.

As seen from, Snort, on its own, is able to detect 27 attacks. After is added as a preprocessor, this number increases to 51 and finally after NETAD is added as a preprocessor the number of attacks detected increases up to 146.

As a result it can be mentioned that combining and NETAD as a preprocessor which are anomaly-based systems with the signature-based EDS Snort, contributes to Encroachment detection positively. The cross EDS is said to be more powerful than the signature-based on its own because it uses the advantages of anomaly-based approach for detecting unknown attacks.

References

[1]. Noel S, Wijesekera D, Youman C. Modern Encroachment detection, data mining, and degrees of attack guilt, in applications of data mining in computer security. Kluwer Academic Publisher; 2002.
[2]. Bace R. Encroachment detection. Indianapolis, USA: Macmillan Technical Publishing; 2000.
[3]. Bace R, Mell P. Encroachment detection systems. NIST Special Publication on Encroachment Detection Systems; 2001, SP 800-31.
[4]. Mahoney MV, Chan PK. Learning nonstationary models of normal network traffic for detecting novel attacks. In Proceedings of eighth international
[5]. Dayiog˘lu B. Use of passive network mapping to enhance network Encroachment detection. Thesis (Master), The Graduate School of Natural and Applied Sciences of the Middle East Technical University; 2001.
[6]. Mahoney MV, Chan PK. Learning models of network traffic for detecting novel attacks, Florida Institute of Technology Technical Report, CS-2002-08;2003.
[7]. Debar H, Becker M, Siboni, D. A neural network component for an Encroachment detection systems. In Proceedings of the 1992 IEEE symposium on security
[8]. Lee W, Stolfo S. Data mining approaches for Encroachment detection. In Proceedings of the seventh USENIX security symposium (SECURITY'98), San Antonio, TX; 26–29 January 1998. and privacy, Oakland, CA; 4–6 May 1992. p. 240–50
[9]. Warrender C, Forrest S, Pearlmutter B. Detecting Encroachments using systems call: alternative data models. In Proceedings of the 25th IEEE symposium on
[10]. Mahoney MV. Network traffic anomaly detection based on packet bytes. In Proceedings of ACM-SAC; 2003.

Amamer Khalil Masoud Ahmidat PhD in the computer and information Faculaty of electrical Engand information technical University of Kosice Slovaki (2003-2008) . BSc electronic .Eng Computer Dept (1987-1991).MSc in Computer engineering and information Faculaty of electrical Eng.and information technical University of Kosice Slovaki (1995-1998) . **Head of Higher Institute of Medical Technology in Baniwaleed-Libya,** Assistant Professor from (01-10-2013.)

Muhamad Abdulla Muhamad Abdussalam M.Sc. in Computer Engineering Technical University of Kosice ,Slovak Republic. Bachelor of Science B.Sc. in Electronic Engineering, College of Electronic Technology Baniwalid. **Head of Study And Examinations Department, Higher Institute of Medical Technology ,Baniwalid, Libya**.

Dr. Amamer Khalil Masoud Ahmidat"A Cross Encroachment detection system design for computer network security "International Journal of Engineering Science Invention(IJESI), vol. 7, no. 8, 2018, pp. 01-05