Perspectives in Science (2016) 8, 736—738

ScienceDirect
journal homepage: www.elsevier.com/pisc

Performance analysis of DoS LAND attack detection☆

Deepak Kshirsagar[a,*], **Amit Rathod**[b], **Sachin Wathore**[c]

[a] *College of Engineering, Pune (COEP), Pune 411005, India*
[b] *Indian Institute of Management Indore, Indore 453556, India*
[c] *VMware, Software India Pvt. Ltd., Bangalore 560076, India*

Received 20 February 2016; accepted 8 June 2016
Available online 11 July 2016

KEYWORDS
DoS LAND;
IP spoofing;
Memory and CPU usage

Summary Nowadays, e-community business, web servers and organizations, mainly suffered by Denial of Service (DoS) attacks. DoS is a common attack causes significant problems in business operations and 65% organizations are suffering over the Internet. This type of attack is created by sending a high rate malicious traffic towards the server and block genuine users using desired network sources and services. In this way this attack consumes the network resources and services which results into degrades the availability of desired services to the valid users.

This paper proposes the intrusion detection mechanism for DoS detection such as Local Area Network Denial (LAND), which classified into the Network Traffic Analyzer, Traffic Features Identification and Extraction, IP spoofing based attack detection and Intruder Information. This system efficiently detects DoS LAND based on IP spoofing. This system analyzes the network resources consumed by an attacker. The system is implemented and tested using open source tools. The experimental result shows that, the proposed system produces better performance in comparison with state-of-art existing system and result into a low level of memory and CPU usage.

Introduction

The increased number of DoS attacks is threatening the accessibility and reliability of network services for users (Tan et al., 2011). Therefore, there is need of effective mechanisms of denial of service attacks.

Current status of DoS attacks

Prolexic Global Attack Report 2014 (DoS, 2014) shows that DoS attacks has increased in Q1 2014 by 47% and 18%, compared to Q1 2013 and Q4 2013 respectively. It concludes that, 13% DoS attacks are directed towards application level and 87% are directed towards infrastructure level.

☆ This article belongs to the special issue on Engineering and Material Sciences.

* Corresponding author.
E-mail addresses: kdeepak83@gmail.com, ddk.comp@coep.ac.in (D. Kshirsagar).

http://dx.doi.org/10.1016/j.pisc.2016.06.074

DoS attacks and defense techniques

DoS attacks based on weakness are classified (Jain et al., 2011) into vulnerability and flood attacks. LAND, Neptune and ping of death are well unknown vulnerability attacks. Intruder creates this type of vulnerability by sending spoofed packets with SYN Flag to the victim which results into lock up. The packet contains same source and destination address and the victim machine assumes that it is sending itself, resulting into crash the machine.

Filtering, Hybrid approaches and firewall are used to mitigate DoS attacks. State-of-art IDS are able to detect these types of attacks, but shows lower detection rate and performance.

This work has following contributions:

i. This paper proposed intrusion detection mechanism for the effective detection of DoS LAND attack.
ii. The performance measurement metric used in evaluation is memory and CPU usage.

The rest of the paper is organized in sections as follows. ''*Related work*'' section presents related work in the area of intrusion detection for denial of service LAND attack. ''*Proposed intrusion detection mechanism*'' section provides proposed detection mechanism. System implementation deals with various modules involved in detection mechanism. ''Experimental result and analysis'' section deals with experimental results and analysis followed by conclusion and future work.

Related work

Novel ID model (Hussain et al., 2015) detects probing, U2R, R2L and DoS attacks using anomaly and misuse. In the first stage anomaly employed by Support Vector Machine (SVM) and second stage misuse is employed by supervised back propagation ANN algorithm. The accuracy is improved with the help of training dataset.

Feature selection (Chae et al., 2015) is proposed with the help of three standards. This method is evaluated with decision tree classifier and useful for improving the efficiency of data mining algorithms.

A hybrid ID (Malik et al., 2015) is proposed for detection of Smurf, land, Neptune, etc. This system uses feature selection and classification steps for intrusion detection. The binary particle swarm optimization is used for finding a suitable set of attributes and random forests are used as a classifier.

Distributed IDS (Li et al., 2010) proposed on cooperative defense, which reduces the impact of DoS attacks in the cloud. IDS is placed in various regions of cloud computing and any IDS communicate with the other using cooperative agent. Snort rules are modified and used for detection.

DoS attacks are detected based on multivariate correlation analysis (Lo et al., 2010). Euclidean distance is used for inner correlation of captured data. Incoming traffic compares to profile generated by normal traffic in the training phase. This system provide high DR but produces high FPR.

Proposed intrusion detection mechanism

The proposed intrusion detection mechanism is classified as follows:

Network traffic analyzer

Open source network traffic analyzer captures the raw data packet in promiscuous mode on Unix and used for

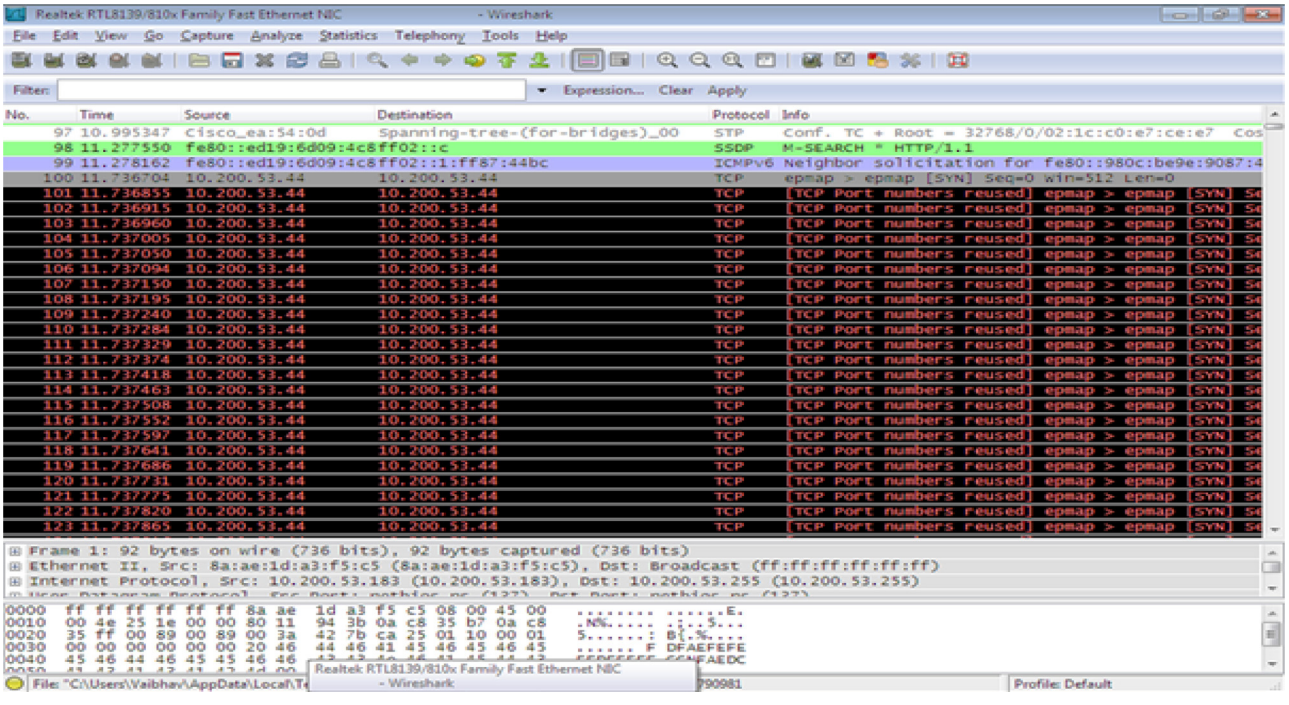

Figure 1 Network traffic analyzer — Wireshark.

Table 1 Analytical comparison with state-of-art existing IDS.

Sr. no.	Systems	Detection mechanism	Performance metrics
1	Cooperative IDS (Lo et al., 2010)	Signature	DR and computation time
2	DoS detection (Tan et al., 2011)	Anomaly	DR and FPR
3	Hybrid IDS (Malik et al., 2015)	DM and ML	IDR and FAR
4	Two stage hybrid IDS (Hussain et al., 2015)	Signature and anomaly	TPR and FPR
5	Proposed system	Signature	Memory and CPU usage

Table 2 Memory and CPU usage for DoS LAND attack.

Sr. no.	Before attack		During attack		After attack detection	
	Memory usage in MB	CPU usage in %	Memory usage in MB	CPU usage in %	Memory usage in MB	CPU usage in %
1	671	9	684	100	673	10
2	689	10	711	100	692	10
3	721	7	733	99	724	8

analysis. The captured raw data records contain information regarding packets.

Traffic features identification and extraction

The important features are identified, extracted and stored in database for generation of rules.

IP spoofing based attack detection

IP spoofing is used for attack detection. The intruder is detected and information regarding intruder is stored in database.

System implementation

The open source Wireshark captures TCP packets and necessary features extract from the records of packets as shown in Fig. 1. The extracted features are stored in Oracle database 10 g. Netbeans IDE is used for implementation of the system and the hping tool is used for creation of LAND attack. The DoS LAND attack is detected based on IP spoofing.

Experimental result and analysis

This section describes experimental results and analysis for the detection of denial of service attacks such as LAND attack. Table 1 shows a comparative study of existing IDS and performance for DoS LAND attack.

The system performance is measured in terms of memory and CPU usage before attack, during attack and after attack detection. Table 2 shows memory and CPU usage during an attack is increased. This system is efficiently detected DoS LAND attack which minimizes memory and CPU usage after attack detection and is approximately similar to memory and CPU usage before attack.

Conclusion

This paper has proposed and implemented detection mechanism for efficient detection of denial of service LAND attack. The proposed detection mechanism architecture consists of network traffic analyzer, feature identification and extraction, IP spoofing based attack detection and intrusion information module. The efficient detection of DoS LAND attack is based on IP spoofing. The results show that memory and CPU usage is increased during the occurrence of attack and minimized efficiently after detection of DoS LAND attack.

However, this detection system detects only denial of service attacks such as LAND. The further task is to test the system for different denial of service attacks in distributed architectures and cloud computing environment.

References

Chae, H.-s., Jo, B.-o., Choi, S.-H., Park, T., 2015. Feature selection for intrusion detection using NSL-KDD. Recent Adv. Comput. Sci., ISBN: 978-960-474-354-4.

2014. Analysis of an Intrusion: Dos Attack.

Hussain, J., Lalmuanawma, S., Chhakchhuak, L., 2015. A novel network intrusion detection system using two-stage hybrid classification technique. IJCCER 3 (2), 16—27.

Jain, P., Jain, J., Gupta, Z., 2011. Mitigation of denial of service (DoS) attack. Int. J. Comput. Eng. Manage. 11, 38—44.

Li, J., Liu, Y., Gu, L., 2010. DDoS attack detection based on neural network. In: 2nd International Symposium on Aware Computing (ISAC), IEEE, pp. 196—199.

Lo, C.-C., Huang, C.-C., Ku, J., 2010. A cooperative intrusion detection system framework for cloud computing networks. In: 39th International Conference on Parallel Processing Workshops (ICPPW), IEEE, pp. 280—284.

Malik, A.J., Shahzad, W., Khan, F.A., 2015. Network intrusion detection using hybrid binary PSO and random forests algorithm. Security Commun. Netw. 8 (16), 2646—2660.

Tan, Z., Jamdagni, A., He, X., Nanda, P., Liu, R.P., 2011. Denial-of-service attack detection based on multivariate correlation analysis. In: Neural Information Processing, Springer, Berlin, Heidelberg, pp. 756—765.