Twelfth International Conference
Financial and Actuarial Mathematics – FAM-2019

Evaluating Network Intrusion Detection Systems

Pavel Todorov Stoynov
Sofia, Bulgaria

Abstract: This paper considers some approaches for detection of intrusions in on-line transaction systems and some ways for evaluation of the efficiency of the Intrusion Detection Systems (IDS) based on different attack datasets. By confronting IDS to the attack traces in the datasets, it is possible to get a statistical evaluation of IDS, and to rank them according to their detection capabilities.

Key words: Intrusion Detection Systems (IDS), Intrusion Detection methods, Statistical evaluation of IDS, attack traces, attack tools

Introduction

Intrusion Detection Systems (IDS) are IT security systems for detecting hostile activity in IT networks with different use (financial, trade, administration, scientific etc.). When these systems also prevent the hostile activity, they are called Intrusion Detection and Prevention Systems (IDPS). They can be divided into two groups:

1. Host-based – for detecting hostile activity on host systems. They analyze information from operation systems and application files captured by software agents.
2. Network based – for detecting hostile activity on networks. They evaluate information from network communication, analyzing the stream of packets captured by sensors.

The models for intrusion detection can be divided into two groups (Gotseva, Trifonov and Stoynov, 2019):

1. Signature verification. In this case, the system detects previously registered intrusion signature.
2. Anomaly detection. In this case, The system looks for abnormal behavior.

Most IDS commercial tools follow the signature verification detection system. However, they have some drawbacks (false alarms, signature of the attack can't be easily discovered, IDS should be periodically updated with new signatures).

Contemporary IDS usually include both signature verification and anomaly detection modules.

For statistically evaluating Intrusion Dtection Systems IDS in network information security, researchers need a documented attack database which database generally represents the ground truth (Rindberg et al., 2008).

This paper aims at presenting some methods for evaluating anomaly-based Intrusion Detection Systems

Evaluating IDS and Anomaly Detection Algorithms

The statistical IDS evaluation itself counts the number of true positives, true negatives, false positives, and false negatives. The relations between these values can then be exhibited by mean of a ROC curve (Receiver Operating Characteristic). The ROC technique has been used in 1998 for the first time for evaluating IDS in the framework of the DARPA project on the off-line analysis of intrusion detection systems, at the MIT' Lincoln laboratory MIT (2008). Several papers describe this experience as Durst et al. (1999), Lippmann et al. (2000) and Lee et al. (1999).

ROC technique consists in combining detection results with the number of testing sessions to issue two values which summarize IDS performance: the detection ratio (number of detected intrusions divided by the number of intrusion attempts) and the false alarm rate (number of false alarms divided by the total number of network sessions). These summaries of detection results then represent one point on the ROC curve for a given IDS. The ROC space is defined by the false alarms and true positive rates on X and Y axis respectively, what in fact represents the balance between efficiency and cost. The best possible IDS would then theoretically be represented by a single point curve of coordinates $(0,1)$ in the ROC space. Such a point means that all attacks were detected and no false alarm raised. A random detection process would be represented in the ROC space by

a strait line going from the bottom left corner $(0,0)$ to the upper right corner $(1,1)$ (the line with equation $y = x$). Points over this line mean that the detection performance is better than the one of a random process. Under the line, it is worse, and then of no real meaning (Owezarski, 2007).

NADA (Network Anomaly Detection Algorithm) is an anomaly detection tool relying on the use of deltoids for detecting significantly anomalous variations on traffic characteristics. This tool also includes a classification mechanism of anomalies aiming at determining whether detected anomalies are legitimate and their characteristics (Farraposo et al., 2007). NADA has been issued in the framework of the Metrosec project (Metrosec, 2008). NADA uses a threshold k which aims at determining whether a deltoid corresponds to an anomalous variation. Setting the k threshold allows the configuration of the detection tool sensitivity, in particular related to the natural variability of normal traffic.

The Gamma-FARIMA approach (Scherrer et al., 2007) is also one of the achievements of the MetroSec projects.

Packet Header Anomaly Detection (PHAD) tool, funded by the American NSF, is said to be the ultimate intrusion and anomaly detection tool (Mahoney et al., 2001). The argumentation of its authors mainly relies on tests lead with KDD'99 traces: on these traces, PHAD gives perfect results.

Attacking tools

There are different attacking tools used to perform attacks which are registered in anomalies databases and used for evaluation of IDS.

The IPERF tool under Linux (IPERF, 1999) aims at generating UDP flows at variable rates, with variable packets rates and payloads.

The HPING2 tool (HPING2, 2019) aims at generating UDP, ICMP and TCP flows, with variable rates (same throughput control parameters as IPERF). With this tool, it is also possible to set TCP flags, and then to generate specific signatures in TCP flows.

TRINOO (Trinoo, 2019) and TFN2K (TFN2K, 2019) are two well known distributed attacking tools. They allow the installation on different machines of a program called zombie, daemon, or bot. This program is in charge of generating the attack towards the target. It is remotely controlled by a master program which commands all the bots. It is possible to constitute an attacking army (or botnet) commanded by one or several masters.

TFN2Kbots can launch several kinds of attacks. In addition of classical flooding attacks using UDP, ICMP and TCP protocols (sending of a large number of UDP, ICMP or TCP packet to the victim), many other attacks are possible. The mixed flooding attack is a mix of UDP flooding, ICMP flooding and TCP SYN flooding. Smurf is an attacking technique based on the concept of amplification: bots use the broadcast address for artificially multiplying the number of attacking packets sent to the target, and then multiplying the power of this attack. TRIN00 bots, on their side, can only perform UDP flooding (Owezarski, 2007).

Comparative evaluation of IDS with different anomalies databases

The statistical evaluation of an IDS based on some Intrusion Dataset is usually performed using the traces with documented anomalies registered in the dataset. Each of the attack traces contain several attacks. In addition, the documented traces can be grouped according to the attacking tools used for generating the attacks/anomalies, and in each group differentiate them according to attack intensities, durations, etc.

The intensity and duration of anomalies are two characteristics which have a significant impact on the capability of anomaly based IDS to detect them. Whereas the detection of strong intensity anomalies is well done by most of detection tools, it is in general not the case when small intensity attacks are considered. Therefore, a suited method for evaluating anomaly detection tools performance must be able to count how many times it succeeds or failed in detecting anomalies contained in the traces, and among which some are of low intensity.

Usualy ROC curve is presented and curve analysis is performed.

An Example. NADA evaluation on KDD'99 database (Owezarski, 2007) uses the 10% KDD database, i.e. only one of the KDD'99 datasets.

During the International Knowledge Discovery and Data Mining Tools contest (UCI KDD Archive, 1999), 10% of the KDD database were used for the learning phase (Hettich and Bay, 1999). This part of the database contains 22 types of attacks and is a concise version of the full KDD database. This later contains a greater number of attack examples than normal connections, and the types of attacks do not appear in a similar way. Because of their nature, DoS attacks represent the huge majority of the database. On the other hand, the

corrected KDD database provides a database with different statistical distributions compared to the databases ”10% KDD” or ”Full KDD”. In addition, it contains 14 new types of attacks.

NADA performance ROC curve obtained with the 10% KDD database shows that NADA got very good results. Applied to the KDD’99 database, NADA exhibits a detection probability close to 90%, and a probability of false alarms around 2%.

Dataset ADFA-IDS

A possible dataset for statistical evaluation of IDS is the Intrusion Dataset (IDS) of Australian Defence Force Academy (ADFA) - ADFA-IDS (Creech and Hu, 2017). It is provided by the University of Arizona Artificial Intelligence Lab and intended as representative of modern attack structure and methodology to replace the older datasets KDD and UNM (Creech and Hu, 2013; Tran et al., 2012).

The version of ADFA-IDS used is released on March 27th, 2017 (Haider et al., 2017) as an update to the original ADFA-IDS made publicly available in 2013 (Creech and Hu, 2013; Creech and Hu, 2014; Haider et al., 2015). ADFA IDS includes independent datasets for Linux and Windows environments.

ADFA-LD (Linux dataset) was generated on a Ubuntu Linux 11.04 host OS with Apache 2.2.17 running PHP 5.3.5. FTP, SSH, MySQL 14.14, and TikiWiki were started (Xie and Hu, 2013; Xie et al., 2014).

Table 1 below shows the payloads and vectors used to attack the Ubuntu OS and generate the dataset.

Table 1. The payloads and vectors used to attack the Ubuntu OS and generate the dataset

PAYLOAD/EFFECT	VECTOR
password bruteforce	FTP by Hydra
password bruteforce	SSH by Hydra
add new superuser	Client side poisoned executable
Java based meterpreter	Tiki Wiki vulnerability exploit
Linux meterpreter payload	Client side poisoned executable
C100 Webshell	PHP remote file inclusion vulnerability

ADFA-WD (Windows dataset) was genearted on a Windows XP Service Pack 2 host OS with the XP default firewall enabled for all attacks, and file sharing enabled, a network printer configured, wireless and Ethernet networking (Haider et al., 2016a; Haider et al., 2016b). Norton AV 2013 was used to scan certain payloads. FTP server, web server and management tool, and streaming audio digital radio package were activated.

A target ratio of 1:10:1=normal:validation:attack data was used to guide collection and structuring activities.

The vectors used here are: TCP ports, web based vectors, browser attacks, and malware attachments

The effects are: Bind shell, reverse shell, exploitation payload, remote operation, staging, system manipulation, privilege escalation, data exfiltration, and back-door insertion.

Conclusion

The statistical evaluation of IDS and Anomaly Detection Algorithm is based on the number of true positives, true negatives, false positives, and false negatives. It is presented by ROC curves based on specified Intrusion Datasets where specific attacking tools generate intrusion attacks.

References

Creech, G. and J. Hu (2013) Generation of a new IDS test dataset: Time to retire the KDD collection, 2013 IEEE Wireless Communications and Networking Conference, WCNC 2013, pp.4487-4492.

Creech, G. and J. Hu (2014) A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns, IEEE Transactions on Computers, vol. 63, issue 4, April 2014, pp. 807-819.

Creech, G. and J. Hu (2017) ADFA IDS Dataset, University of Arizona Artificial Intelligence Lab, AZSecure-data, Director Hsinchun Chen.

Available: http://www.azsecure-data.org/ [November 2016]

Durst, R., T. Champion, B. Witten, E. Miller anf L. Spagnuolo (1999) Testing and evaluating computer intrusion detection system. Communications of the ACM, 42(7), 1999.

Gotseva, D., R. Trifonov, P. Stoynov (2019) Neural Networks for Intrusion Detection – Proceedings of the International conference HiTtech-2019, 10-12 October, Sofia, Bulgaria.

Farraposo, S., P. Owezarski, E. Monteiro (2007) Nada - network anomaly detection algorithm. In Proceedings of the 18th IFIP/IEEE Distributed Systems: Operations and Management (DSOM'2007), October 2007.

Haider, W., J. Hu, and M. Xie (2015) Towards reliable data feature retrieval and decision engine in hostbased anomaly detection systems, Proc. Of the 2015 10th IEEE Conference on Industrial Electronics and Applications, ICIEA 2015, pp. 513-517.

Haider, W., J. Hu, X. Yu, and Y. Xie (2016a) Integer data zero-watermark assisted system calls abstraction and normalization for host based anomaly detection systems, Proc. Of the 2nd IEEE International Conference on Cyber Security and Cloud Computing, 2016, pp. 349-355.

Haider, W., G. Creech, Y. Xie, and J. Hu (2016b) Windows Based Data Sets for Evaluation of Robustness of Host Based Intrusion Detection Systems (IDS) to Zero-Day and Stealth Attacks. Future Internet 8.3 (2016): 29.

Haider, W., J. Hu, S. Slay, B. P. Turnbull and Y. Xie (2017) Generating Realistic Intrusion Detection System Dataset based on Fuzzy Qualitative Modeling," Journal of Network and Computer Applications (JNCA), 2017, DOI: 10.1016/j.jnca.2017.03.018.

Hettich, S. and S. Bay (1999) The uci kdd archive, Irvine - University of California, Department of Information and Computer science. http://kdd.ics.uci.edu, 1999.

HPING2 (2019) http://sourceforge.net/projects/hping2.

IPERF (1999) The TCP/UDP bandwith Measurement Tool. http://dast.nlanr .net/Projects/Iperf/.

Lee, W., K. Stolfo, K. Mok (1999) Mining in a data-flow environment: Experience in network intrusion detection. In Proceedings of the ACM International Conference on Knowledge Discovery & Data Mining (KDD'99), pages 114–124, 1999.

Lippman, R., D. Fried, I. Graf, J. Haines, K. Kendal, D. McClung, D. Weber, S. Webster, D. Wyschogrod, R. Cunningham, Y. Zissman (2000) Evaluating intrusion detection systems: The 1998 darpa off-line intrusion detection evaluation. In DARPA Information Survivability Conference and Exposition, pages 12–26, 2000.

Mahoney, M., P. Chan (2001) Phad: Packet header anomaly detection for identifying hostile network traffic. In Technical Report CS-2001-04. Department of Computer Sciences - Florida Institute of Technology, 2001.

Mahoney, M., P. Chan (2003) An analysis of the 1999 darpa/lincoln laboratory evaluation data for network anomaly detection. In Recent Advances in Intrusion Detection (RAID 20003), pages 220–237, September 2003.

McHugh, J. (2001) Testing intrusion detection systems: A critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory. ACM Transactions on Information and System Security, 3(4):262–294, 2001.

Metrosec (2008) http://www.laas.fr/METROSEC.

MIT (2008) Lincoln Laboratory. http://www.ll.mit.edu/mission/communications /ist/corpora/ideval, 2008.

Rindberg, H., M. Roughan and J. Rexford (2008) The need for simulation in evaluating anomaly detectors. Computer Communication Review, 38(1):55–59, January 2008.

Owezarski, P. (2007) Contribution of the French METROSEC project to traffic anomalies detection, Colloque STIC, Paris, France, 5-7 November 2007.

Scherrer, A., N. Larrieu, P. Owezarski, P. Borgnat, P. Abri (2007) Non-gaussian and long memory statistical characterisations for internet traffic with anomalies. IEEE Transaction on Dependable and Secure Computing, 4(1), January 2007.

TFN2K (2019) An analysis.
http://packetstormsecurity.org/distributed/TFN2k Analysis-1.3.txt.

Tran, Q., F. Jiang, and J. Hu (2012) A real-time NetFlow-based intrusion detection system with improved BBNN and high-frequency field programmable gate arrays, Proc. Of the 11th IEEE International Conference on trust, Security and Privacy in Computing and Communications, TurstCom 2012, 2012, pp. 201-208.

Trifonov, R., G. Tsochev, R. Yoshinov, S. Manolov, G. Pavlova (2017) Conceptual model for cyber intelligence network security system. International Journal of Computers. Vol. 11, 2017.

Trinoo (2019) The DoS Project's "trinoo" distributed denial of service attack tool http://staff.washington.edu/dittrich/misc/trinoo.analysis.

UCI KDD Archive (1999) KDD'99 datasets. http://kdd.ics.uci.edu/databases/ kddcup99/kddcup99.html.

Xie, M. and J. Hu (2013) Evaluating host-based anomaly detection systems: A preliminary analysis of ADFA-LD, Proc. Of the 6th International Congress on Image and Signal Processing, CISP 2013, pp. 1711-1716.

Xie, M., J. Hu, X. Yu, and E. Chang (2014) Evaluating host-based anomaly detection systems: Applications of the frequency-based algorithms to ADFA-LD," LNCS, vol. 8792, 2014, pp.542-549.