A Perusal on Intrusion Detection & Deterrence Methodologies

[1]K. Shanthi, [2]R. Maruthi

[1]Research Scholar, PRIST University, Thanjavure; Assistant Professor, Department of Computer Science, Shri Krishnaswamy College for women, Chennai
[2]Associate Professor, Department of Computer Science, Hindustan Institute of Technology, Chennai

Abstract- The increase in the security breach of computer systems and computer networks has led to the increase in the number of security tools that seek to protect these assets. Among these tools are intrusion detection and prevention systems (IDPS). IDPS are security systems that are used to detect and prevent security threats to computer systems and computer networks. These systems are configured to detect and respond to security threats automatically, thereby reducing the risk to monitored computers and networks. Intrusion detection and prevention systems use different methodologies such as signature based, anomaly based, stateful protocol analysis, and a hybrid system that combines some or all of the other systems to detect and respond to security threats. Intrusion detection and prevention system comes as an appliance or a software tool. The combinations of the methodologies, delivery mechanisms, and the technical requirements for properly configuring these systems make it difficult to understand and evaluate these systems. This problem is amplified by the lack of publicly available work and current data sets for use in evaluating the effectiveness of intrusion detection and prevention systems. In this paper we will offer a clear explanation of the detection methodologies used by the IDPSs and offer a way to compare these methodologies.

Keywords: **Intrusion, Anomaly, Signature based**

1. Introduction

Intrusion detection and prevention systems (IDPS) have become a valuable tool in keeping information systems secure. IDPS are security tools that are used to monitor, analyze, and respond to possible security violations against computer and network systems. Although the use and dependency of these systems continue to grow, there are no publicly available ways to evaluate the effectiveness of these systems. The available commercial tools are expensive and are not feasible in some cases.

There is also a lack of current work on this problem and the available work and data sets are dated. IDPSs lack an established testing and evaluating processes such as those that exists in the software development field. Unlike the software testing field that has a number of proven tools that available for testing, the IDPS users does not have the same opportunities or the necessary tools to test the IPDS products once deployed.

IDPS products also work and behave differently using proprietary rules sets and user interfaces which makes it even harder to evaluate them side by side. Most accuracy and performance metrics on IDPS products tend to be available without the raw data on how the results were produced. Also these numbers are based on lab environments which are not identical to the production environment where the IDPS product will protect.

Although these test results are accurate, our research found that most production environments are not identical and that security priorities vary from one organization to the other. We also discovered that a considerable amount of resources are required to properly deploy, run, and maintain an IDPS. IDPS products also use different proprietary detection engines which makes it difficult to evaluate and understand their underlining methodologies.

Most of the research work on this issue tends to focus on improving one methodology or evaluating one methodology against a proposed new one.The objective of this thesis is not to improve any of the IDPS methodologies or propose a new methodology, instead it is to clear the misunderstandings about evaluating IDPS effectiveness by offering a simple but effective way to understand and evaluate IDPS methodologies and products. The first
phase offers a detailed overview of the four commonly used IDPS methodologies and a simple way to evaluate these methodologies. And the second phase explains four ways to setup test environments for evaluating IDPS products using open source utilities and some publicly available evaluation copies of commercial tools. Using the evaluation parameters established during the first phase.

2. Literature Review

2.1 Anomaly based methodology.

Intrusion detection and prevention systems are a combination of intrusion detection systems and intrusion prevention systems. Intrusion prevention came out of research on the short comings of intrusion detection. Intrusion detection evolved out of a report that proposed a threat model [9]. This report laid down the foundation of intrusion detection systems by presenting a model for identifying abnormal behavior in computer systems. This model broke down threats into three groups, external penetrations, internal penetrations, and misuse. The report used these three groups of threats to develop an anomaly based user behavior monitoring system. In 1987, “a model for a real-time intrusion-detection expert system that aims to detect a wide range of security violations ranging from attempted break-ins by outsiders to system penetrations and abuses by insiders” was proposed [10]. This model was based on the idea that security breaches to any system can be identified and monitored by analyzing the system’s audit logs. The model was comprised of profiles, metrics, statistical models, and rules for analyzing the logs. This model provide “a

framework for a general-purpose intrusion-detection system expert system" that is still in use today [11]. Anomaly detection methodologies are plagued with high rates of false positives and a new detection system for anomaly based methodology that strikes a balance between generalizations is proposed [21]. The proposed system balances the generalizations in anomaly detection methodologies and in doing so it achieves both a high accuracy rate and a low false positive rate. In [25] data mining techniques that are used in anomaly based intrusion detection are explored. A further discussion of the statistical based anomaly methodology is covered in [26].

2.2 Signature based methodology.

In [17] a structured approach to intrusion detection systems by defining and classifying the components of an IDS system is offered. This classification offered a clear understanding of all the parts that make up intrusion detection systems and the challenges the systems faces. James and Jay offered survey of where the current research is on the techniques and methodologies used in intrusion detection [18]. Their focus was to summarize the research done in intrusion detection to this point and in so doing offered a starting point for future research to start. A technical overview of intrusion detection systems starting with the fundamentals of how these systems are structured to the techniques they use to detect and identify potential security threats are discussed in [19]. This paper also explains how an intrusion detection system responds to violations of the security policies they are monitoring. In a proposal for a new signature based intrusion detection and prevention system [23], the authors started by presenting the basic organization and implementations of intrusion detection and prevention systems. Then they went on to proposed and design a new signature based intrusion detection and prevention system called HawkEye. The authors also compared it with current intrusion detection and prevention systems on the market. In [27] Snort, the most popular signature based IDS is discussed.

2.3 Stateful protocol analysis based methodology.

Intrusion detection and prevention systems suffer from scalable and efficiency problems, these two problems are addressed by high performance deep packet pre-filtering and memory efficient technique [20]. This technique allows the Intrusion detection and prevention systems to have high accuracy rates and high performance numbers by utilizing a deep packet pre-filter and changing how it handles and processes memory and captured data. In [31] a network based intrusion detection system that is based on dynamic application layer protocol analysis. Protocol analysis is detailed in [32], which combines it with another methodology. In [33] stateful protocol analysis is used as the based for a proposed Web IDS. A new detection engine that is based on understanding the protocols is proposed in [51]

2.4 Hybrid based methodology.

Combining the two most used methodologies in intrusion detection and prevention systems into a system that uses both anomaly and signature based detection methodologies produces a better detection system [22]. This combination of methodologies produces a better system by preprocessing the data with the anomaly detection engine and then passing the results to the signature based engine. This results in a very high accuracy rate and very low false positives. The two main methodologies used in intrusion detection and prevention systems are combined to form a collaborative intelligent intrusion detection system (CIIDS) [16]. This work looked and addressed current challenges to collaborative intrusion detection systems and the algorithms they employ for alert correlation. It also suggested ways to reduce false positives while improving the detection accuracy. Fuzzy logic and data mining is combined in [28] to produce a hybrid methodology that combines anomaly and signature methodologies. In [29] another combination of anomaly and signature based methodologies is covered. In [30] a new hybrid intrusion detection system is proposed for clustered wireless sensor networks. A new hybrid system for mobile adhoc networks is proposed in [52] and this system combines anomaly and the new system that is based on how the system responds to an attack.

3. IDPS Methodologies

There are many different methodologies used by IDPS to detect changes on the systems they monitor. These changes can be external attacks or misuse by internal personnel. Here, we describe the four methodologies in detail. All the methodologies use the same general model and the differences among them is mainly on how they process information gathered from the monitored environment to determine if a violation of the set policy has occurred.

3.1 Anomaly based methodology. Anomaly based methodology works by comparing observed activity against a baseline profile. The baseline profile is the learned normal behavior of the monitored system and is developed during the learning period were the IDPS learns the environment and develops a normal profile of the monitored system. This environment can be networks, users, systems and so on.

The profile can be fixed or dynamic. A fixed profile does not change once established while a dynamic profile changes as the systems been monitored evolves [8]. A dynamic profile adds extra over head to the system as the IDPS continues to update the profile which also opens it to evasion. An attacker can evade the IDPS that uses a dynamic profile by spreading the attack over a long time period. In doing so, her attack becomes part of the profile as the IDPS incorporates her changes into the profile as normal system changes. Once the baseline profile is developed and current profile is also created and compared to the baseline profile. Using a predefined threshold any deviations that fall outside the threshold are reported as violations. A new dynamic anomaly detection technique is proposed that uses hidden Markov model for modeling the normal behavior of program through analyzing system calls [24]. The proposed technique uses a two layer detection scheme to reduce false positives and improve detection rates. A fixed profile is very effective at detecting new attacks since any change from normal behavior is classified as an anomaly.

Anomaly based methodologies can detect zero-day attacks to environment without any updates to the system. Anomaly intrusion detection methodology uses three general techniques for detecting anomalies and these are the statistical anomaly detection, Knowledge/data-mining, and machine learning based [8].

The statistical anomaly techniques are used to build the two required profiles, one during the learning phase which is then used as the baseline profile and the current profile which is compared to the baseline profile and any differences that found a marked as anomalies depending on the threshold settings of the monitored environment [1]. Environments that use high thresholds have a higher rate of false positives and those that uses lower threshold might experience a high rate of false negatives. The threshold must be tuned according to the requirements and behavior of the environment being monitored for the systems to be effective.

The knowledge/data-mining technique is used to automate the way the technique monitor searches for anomalies and this process places a very high overheard on the system. The technique produces the most false positives and false negatives are produced due to the high overhead that result from the complicated task of identifying and correctly categorizing observed events on the system [4]. The machine learning technique works by analyzing the system calls and it is the widely used technique [7, 14]. The monitored environment is monitored by the detector that examines the observed events against the baseline profile. If the observed events match the baseline, no action is taken, but if it does not match the baseline profile is within the acceptable threshold range then the profile is updated.

The anomaly based methodologies have the following advantages and disadvantages:
Advantages

- The ability to detect new attacks/violations without updates.
- Detects insider attacks
- Detects variants of know attacks
- Does not need signature updates to detect new threats
- Can detect threats that utilize multiple but separate attacks

Disadvantages

- High volume of false positives and false negatives
- Needs a training period before use
- Places high overhead on the system
- Difficult to use due to high volume of alerts

3.2 Signature based methodology. Signature based methodology works by comparing observed signatures to the signatures on file. This file can be database or a list of known attack signatures. Any signature observed on the monitored environment that matches the signatures on file is flagged as a violation of the security policy or as an attack. The signature based IDPS has little overhead since it does not inspect every activity or network traffic on the monitored environment. Instead it only searches for known signatures in the database or file. Unlike the anomaly based methodology, the signature based methodology system is easy to deploy since it does not need to learn the environment [4]. This methodology works by simply searching, inspecting, and comparing the contents of captured network packets for known threats signatures. It also compares behavior signatures against allowed behavior signatures. This architecture uses the detector to find and compare activity signatures found in the monitored environment to the known signatures in the signature database. If a match is found, an alert is issued and there is no match the detector does nothing. Signature based methodology also analyzes the systems calls for known threats payload [7]. Signature based methodology is very effective against know attacks/violations but it cannot detect new attacks until it is updated with new signatures. Signature based IDPS are easy to evade since they are based on known attacks and are depended on new signatures to be applied before they can detect new attacks [15]. Signature based detection systems can be easily bypassed by attackers who modify known attacks and target systems that have not been updated with new signatures that detect the modification. Signature based methodology requires significant resources to keep up with the potential infinite number of modifications to known threats. Signature based methodology is simpler to modify and improve since its performance is mainly based on the signatures or rules deployed [19].
The Signature based methodologies have the following advantages and disadvantages:
Advantages

- Has no learning/training period
- Very efficient at detecting known threats
- Low volume of false positives
- Less overhead on the system being monitored

Disadvantages

- Needs signature update to detect new threats
- Cannot detect variants of know attacks
- Cannot detect insider attacks
- Leaves the monitored environment at risk during the time when a new threat is discovered and the time a signature is applied.

3.3 Stateful protocol analysis based methodology.
The Stateful protocol analysis methodology works by comparing established profiles of how protocols should behave against the observed behavior. The established protocol profiles are designed and established by vendors. Unlike the signature based

methodology which only compares observed behavior against a list, Stateful protocol analysis explores in detail how the protocols and applications should interact/work. This deep understanding/analysis places a very high overhead on the systems [30]. Stateful protocol analysis blends and compliments other IDPS methodologies well which has led to rise of hybrid methodologies [32]. Stateful protocol analysis's deep understanding of how protocol should behave is used as a base for developing IDPS that understand web traffic behavior and are effective at protecting websites [33]. Although the Stateful protocol analysis has a deep understanding of the monitored protocols, it can be easily evaded by attacks that follow and stay within the acceptable behavior of protocols. Stateful protocol analysis methodologies and techniques have slowly been adapted and integrated into other methodologies over the past decade. This has led to the decline of IDPS that utilize just Stateful protocol analysis methodology. The majority of the research on IDPS methodologies mainly concentrates on anomaly, signature, and hybrid methodologies which further reduce the viability of Stateful protocol analysis as a standalone IDPS methodology.
The Stateful protocol analysis architecture is identical to that of the signature based methodology with one exception, instead of the signature database the Stateful protocol analysis has database of acceptable protocol behavior.
The Stateful protocol analysis methodologies have the following advantages and disadvantages:
Advantages

- Has no learning/training period
- Very efficient at detecting known threats
- Low volume of false positives
- Can detect specialized threats

Disadvantages

- Needs signature/rule update to detect new threats
- Cannot detect variants of know attacks
- Cannot detect insider attacks
- Can place high overhead on the processing system
- Leaves the monitored environment at risk during the time when a new threat is discovered and the time a signature/rule is applied

3.4 Hybrid based methodology. The hybrid based methodology works by combining two or more of the other methodologies. The result is a better methodology that takes advantage of the strengths of the combined methodologies. Prelude is one of the first hybrid IDS that offered a framework based on the Intrusion Detection Message Exchange Format (IDMEF) an IETF standard that allows different sensors to communicate[26]. In [27], Snort is modified by adding an anomaly based engine to its signature based engine to create a better detection and then the new hybrid systems is tested against the regular Snort using same test data. The hybrid system detected more intrusions than the regular one. A hybrid intrusion detection system of cluster-based wireless sensors networks was proposed that worked by breaking the detection into two, first it used anomaly based model to filter the data and then it used signature based model to detect intrusion attempts. Another model for a hybrid methodology was proposed based on how the human immune system works [28]. The proposed system is "based on the framework of the human immune system, that uses a hybrid architecture which applies both anomaly and misuse detection approaches" [7]. In hrbrid, three popular methodologies are combined to produce a better system that capitalizes on the strengths of the combined methodologies. The monitored environment is analyzed by the first methodology which sanitizes the monitored environment and then sanitized passed environment is then analyzed by the second methodology which repeats the sanitizing process. After the second sanitizing, the final methodology is engaged to performs the final cleanse. This produces a better system.
The Hybrid based methodologies have the following advantages and disadvantages:
Advantages

- Has a shorter or no learning/training period
- Very efficient at detecting both known and unknown threats
- Can detect variants of know attacks
- Low volume of false positives
- Accurate alerts
- Can detect insider attacks
- May protect the monitored environment during the time when a new threat is discovered and the time when a signature/rule is applied

Disadvantages

- Needs signature/rule update to detect new threats
- Cannot detect variants of know attacks
- Cannot detect insider attacks
- May leave the monitored environment at risk during the time when a new threat is discovered and the time when a signature/rule is applied.

4.Advantages and Disadvantages of IDPS Detection Methodologies Features

The four main methodologies have advantages and disadvantages over one another. The current systems are combining these methodologies in effort to have intrusion detection and prevention system takes advantage of the advantages of each methodology while reducing the short comings of each methodology. This section details the advantages and disadvantages of each methodology.

After going through research papers, commercial products, we selected the following parameters to compare the four methodologies. The advantages and drawbacks of the four main intrusion detection and prevention system (IDPS) methodologies are described below and shown in Table 1.1.

4.1 Detects new attacks. This is the ability of a methodology to automatically detect new attacks to the protected environment. This should happen without any changes or updates to the monitoring system. A system that uses the anomaly or the hybrid based methodologies can detect new attacks without any updates, while the signature based and the Stateful protocol analysis based systems needs their signatures or rules to be modified and updated with new attacks signatures.

4.2. Detects insider attacks. Insider attacks happen when trusted personal who have access and knowledge of the intrusion detection and prevention system takes advantage of their access and knowledge and use it to bypass and attack the system. Only systems that employ the anomaly methodologies can detect the diversion from the normal behavior of a user and alert on it. Other methodologies cannot detect this change in behavior as they are only looking for known signatures or behavior.

4.3 Detects attacks from day one of installation. This is the ability of an IDPS to work from the moment of initial installation without needing a period of time for the methodology to learn the environment and create profiles. The signature and the Stateful protocol analysis based methodologies have the advantage here when compared to the anomaly based methodology. The hybrid based methodology can have an advantage depending on the characteristics of the combined methodologies.

4.4 Detects all known attacks. This is the ability of the methodology to successfully detect all know threat attempts. This is an area were the signature and the Stateful protocol analysis based IDPS has an advantage over the anomaly based systems. The hybrid based methodology can have an advantage or disadvantage based on the methodologies that are combined.

4.5 Detects variants of known attacks. This is the capacity of the methodology to recognize any modifications and variants of all known attacks. The anomaly based methodologies have the advantage over other methodologies due to the way the anomaly works. Signature and Stateful protocol analysis based methodologies cannot detect any changes to know attacks without first updating their signatures or rules. The hybrid based methodologies can have an advantage if one of their combined methodologies is anomaly based.

4.6 Training period. A training period is the amount of time required by an IDPS methodology after installation to learn the monitored environment and build its profiles. These profiles are then used by the methodology as a base. This is a disadvantage for the anomaly based methodology as it prevents it from working from day one of installation. This can also be a disadvantage for the hybrid methodology based if anomaly based methodology is one of the combined methodologies, but the disadvantage is not as high as for the anomaly based methodology.

4.7 Easy to understand alerts. An IDPS methodology has to produce threat alerts that are easy to understand. The anomaly based methodology is plagued with a very high number of alerts due to the way it works and this makes it difficult to interpret and understand all the alerts it produces. The signature based and Stateful protocol analysis based methodologies tend to generate few and more specific alerts which gives them an advantage over the anomaly based and hybrid based methodologies.

5. Conclusion and Future Work

This paper discussed IDPS methodologies by explaining the four popular IDPS methodologies which are anomaly based, signature based, stateful protocol analysis based, and hybrid based detection methodologies. A method for evaluating and comparing these methodologies was developed and presented thereby simplifying the evaluation of IDPS methodologies and products that use these methodologies.

This paper was not focused on developing a new IDPS methodology or improving the ones that exit, instead it was focused on three things. It is currently very difficult to evaluate and select an IDPS product and we offered a solution to this problem through our experiments. The parameters used to evaluate our test IDPS products can be used as a guide to help evaluate and understand what an IDPS offers and also validate its claims. For example most popular IDPS products claim to have a very high accuracy without explaining what they mean by high accuracy. The parameters that have to be understood before selecting an IDPS are cost, usability and scalability, most vendors tend to separate these parameters and present them in way that does not present the whole picture.

Future work includes fine tuning and explaining our evaluation parameters and making them and our setups available to the public. We are looking at setting up a presence on the web for running more evaluations of both commercial and open source IDPS products and making our results public. The focus will be on evasion techniques, accuracy rates, and validating vendor claims and helping users better understand IDPS products and trends.

REFERENCES:

[1] Patcha, A., & Park, J. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends, Computer Networks. *The International Journal of Computer and Telecommunications Networking, 51(12),* 3448-3470.

[2] Bace, R. (1999). An introduction to intrusion detection and assessment for system and network security management. ICSA Intrusion Detection Systems Consortium Technical Report, 1999.

[3] Anderson, J.P. (1980). *Technical Report James P Anderson Co Fort Washington Pa*. Technical report, James P. Anderson Company, Fort Washington, Pennsylvania. Retrieved from http://www.citeulike.org/user/animeshp/article/592588.

[4] Sobh, S. T. (2006). Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art. *Computer Standards & Interfaces,* 28, 670– 694.

[5] Valeur, F., Vigna, G., Kruegel, C., & Kemmerer, A. R. (2004). A comprehensive approach to intrusion detection alert correlation. *IEEE Transactions on Dependable and Secure Computing,* 1, (3), 146-169.

[6] Wu, X. S., & Banzhaf, W. (2010). The use of computational intelligence in intrusion detection systems: A review. *Applied Soft Computing Journal,* 10, 1-35.

[7] Hoang, X. D., Hu, J., & Bertok, P. (2009). A program-based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference. *Journal of Network and Computer Applications*, 32(6), 1219-1228.
[8] Elshoush, H. T., & Osman, I. M. (2011) Alert correlation in collaborative intelligent intrusion detection systems—A survey. *Applied Soft Computing* 11, 4349-4365
[9] Shanbhag, S.; Wolf, T. (2009). Accurate anomaly detection through parallelism. *IEEE Network*, 23 (1), 22-28.
[10] Cannady, J., & Harrell, J. (1996). A Comparative Analysis of Current Intrusion Detection Technologies. *Pattern Recognition*, 96, 212-218.
[11] Bejtlich, R. (2004). The Tao of network security monitoring: beyond intrusion detection. Addison Wesley (p. 832). Addison-Wesley Professional.
[12] Brugger, T. (2007). KDD Cup '99 dataset (Network Intrusion) considered harmful. *KDnuggets News*, 18(4), 1-2.
[13] Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). *Nist Special Publication.* NIST.
[14] Pedro Garcı´a-Teodoroa, P., Dı´az-Verdejoa, E.J., Macia-Ferna´ndeza, G., & Va´zquezb, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenge. *Computers Security*, 28 (1-2), 2009, 18-28.
[15] Tsai, C.-F., Hsu, Y.-F., Lin, C.-Y., & Lin, W.-Y. (2009). Intrusion detection by machine learning: A review. *Expert Systems with Applications*, 36(10), 11994-12000.
[16] Denning, D. E. (1987). An Intrusion-Detection Model. *IEEE Transactions on Software Engineering*, SE-13(2), 222–232.
[17] Valdes, A., & Skinner, K. (2001). Probabilistic Alert Correlation. Recent Advances in Intrusion Detection, 54-68.
[18] Mukhopadhyay, I., Chakraborty, M., & Chakrabarti, S. (2011). A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems. *Journal of Information Security*, 2, 28-38.
[19] Patel, A., Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention systems. *Information Management Computer Security*, 18(4), 277-290.
[20] Weng, N., Vespa, L., & Soewito, B. (2011). Deep packet pre-filtering and finite state encoding for adaptive intrusion detection system. *Computer Networks*, 55(8), 1648-1661.
[21] Aydın, M. A., Zaim, H. A., & Ceylan, K. G. (2009). A hybrid intrusion detection system design for computer network security. *Computers and Electrical Engineering*, 35, 517–526.
[22] Ingham, K. L., & Somayaji, A. (2007). A methodology for designing accurate anomaly detection systems. *Proceedings of the 4th international IFIPACM Latin American conference on Networking LANC 07*, 139. ACM Press.
[23] Kruegel, C., Valeur, F., & Vigna, G. (2005). Intrusion Detection and Correlation: Challenges and Solutions. Evaluation, *Advances in Information Security*, 14, 122-136.
[24] Verwoerd, T. (2002). Intrusion detection techniques and approaches. *Computer Communications*, 25(15), 1356-1365.
[25] Noel, S., Wijesekera, D., & Youman, C. (2002). Modern Intrusion Detection, Data Mining, and Degrees of Attack Guilt. *Information Systems Journal*, 1-29.
[26] Javitz, H. S., & Valdes, A. (1991). The SRI IDES statistical anomaly detector. *Proceedings 1991 IEEE Computer Society Symposium on Research in Security and Privacy*. IEEE Comput. Soc. Press.
[27] Roesch, M., & Telecommunications, S. (1999). Snort – Lightweight Intrusion Detection for Networks. *Proceedings of the 13th USENIX conference on System administration*, 229–238. Seattle, Washington.
[28] Bashah, N., Shanmugam, I. B., & Ahmed, A. M. (2005). Hybrid Intelligent Intrusion Detection System. *Neural Networks*, 6, 23-26. Retrieved from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1297598
[29] Depren, O., Topallar, M., Anarim, E., & Ciliz, M. K. (2005). An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. *Expert Systems with Applications*, 29(4), 713-722.
[30] Wang, S.-S., Yan, K.-Q., Wang, S.-C., & Liu, C.-W. (2011). A Hybrid Intrusion Detection System of Cluster-based Wireless Sensor Networks. Expert Systems with Applications, 38(12), 15234-15243.
[31] Dreger, H., Feldmann, A., Mai, M., Paxson, V., & Sommer, R. (2006). Dynamic Application-Layer Protocol Analysis for Network Intrusion Detection. *15th USENIX Security Symposium*,
[32] Mai, M., & Sommer, D. (2005). Dynamic Protocol Analysis for Network Intrusion Detection Systems. *informatikmaide*, 9. Retrieved from http://informatik-mai.de/files/Mai_DA.pdf
[33] Sourour, M., Adel, B., & Tarek, A. (2007). A Stateful Real Time Intrusion Detection System for high-speed network. *21st International Conference on Advanced Networking and Applications AINA 07*, 404-411.
[34] Haines, J., Lippmann, R., Fried, D., & Zissman, M. (2001). 1999 DARPA intrusion detection evaluation: Design and procedures. Lexington MA MIT, (February).
[35] McHugh, J. (2000). 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.
[36] Mahoney, M. V. & Chan, P. K. (2003). An Analysis of the 1999 DARPA/Lincoln Laboratory Evaluation Data for Network Anomaly Detection. *In Proceedings of the Sixth International Symposium on Recent Advances in Intrusion Detection*, 6, 220-237.
[37] Brugger, S. T. (2007). An Assessment of the DARPA IDS Evaluation Dataset Using Snort. *Electrical Engineering*, *1*, 1-19. doi : 10.1.1.94.674&rep=rep1&type=pdf
[38] Cardenas, A. A., Baras, J. S., & Seamon, K. (2006). A Framework for the Evaluation of Intrusion Detection Systems. *2006 IEEE Symposium on Security and Privacy SP06*, 0, 63-77). Retrieved from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1624001
[39] Sommers, J., & Yegneswaran, V. (2005). Toward Comprehensive Traffic Generation for Online IDS Evaluation. *Development*, 12.

[40] Corsini, J. (2009). *Analysis and Evaluation of Network Intrusion Detection Methods to Uncover Data Theft*, Master's thesis. Edinburgh Napier University, Edinburgh, U[41] Athanasiades, N., Abler, R., Levine, J., Owen, H. & Riley, G. (2003). Intrusion detection testing and benchmarking methodologies. *First IEEE International Workshop on Information Assurance 2003 IWIAS 2003*, 63-72.

[42] Sannella, M. J. 1994. *Constraint Satisfaction and Debugging for Interactive User Interfaces*. Doctoral Thesis. University of Washington, Seattle, WA.

[43] Wireshark. (2012), Wireshark, Retrieved from http://www.wireshark.org/docs/wsug.html

[44] Tomahawk. (2012), Tomahawk, Retrieved from http://tomahawk.sourceforge.net/

[45] Kayacik, H., Zincir-Heywood, A. N., & Heywood, M. I. (2005). Selecting Features for Intrusion Detection : A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets. *Proceedings of the Third Annual Conference on Privacy Security and Trust PST2005*, 3-8. doi : 10.1.166.7574

[46] Mudzingwa, D & Agrawal, R. (2012). A Study of Methodologies used in Intrusion Detection and Prevention Systems. *Proceedings of the IEEE SouthernCon 2012*.

[47] Backtrack. (2012), Backtrack, Retrieved from http://www.backtrack-linux.org/

[48] LOIC. (2012), LOIC, Retrieved from http://sourceforge.net/projects/loic/

[49] Shahriar, M., Vahid, A., & Mojtaba, K. (2012). Effect of Network Traffic on IPS Performance. *Journal of Information Security*, 162-168.

[50] Antonelli, J.C. (2012). *Hands-On Network Security: Practical Tools & Methods, Security Training Course* [PowerPoint slides].
297.

[53] Zanero, S. (2007). Flaws and frauds in the evaluation of IDS/IPS technologies. *First'07 Proc 19th Annual FIRST conference*. Retrieved from http://www.first.org/conference/2007/papers/zanero-stefano-paper.pdf