Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 12 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Performance Metrics Scorecard Based Approach to Intrusion Detection System Evaluation for Wireless Network

By Rupinder Singh & Dr. Jatinder Singh
Khalsa College, Amritsar, Punjab, India

Abstract - Wireless Intrusion Detection System (IDS) performance metrics are used to measure the ability of a wireless IDS to perform a particular task and to fit within the performance constraints. These metrics measure and evaluate the parameters that impact the performance of a wireless IDS. Wireless IDS analyze wireless specific traffic including scanning for external users trying to connect to the network through access points and play important role in security to the wireless network. Design of wireless IDS is a difficult task as wireless technology is advancing every day, performance metrics can play an important role in the design of efficient wireless IDS by measuring the factors concern with the performance of a wireless IDS. In this paper we provide a performance metrics scorecard based approach to evaluate intrusion detection systems that are currently popular for wireless networks in the commercial sector. We provide a set of performance metrics that are relevant to wireless IDS and use a "scorecard" containing the set of values as the centerpiece of testing and evaluating a wireless IDS. Evaluation of a wireless IDS is done by assigning score to various performance metrics concern with wireless IDS. We apply our performance metrics scorecard evaluation based approach to three popular wireless IDS Snort-wireless, AirDefense Guard, and Kismet. Finally we discuss the results and the opportunities for further work in this area.

Keywords : *IDS, Performance metrics, Performance Constraints Access Points, Wireless, Metrics, Scorecard.*

GJCST-E Classification: *C.2.0*

Strictly as per the compliance and regulations of:

A Performance Metrics Scorecard Based Approach to Intrusion Detection System Evaluation for Wireless Network

Rupinder Singh [α] & Dr. Jatinder Singh [σ]

Abstract - Wireless Intrusion Detection System (IDS) performance metrics are used to measure the ability of a wireless IDS to perform a particular task and to fit within the performance constraints. These metrics measure and evaluate the parameters that impact the performance of a wireless IDS. Wireless IDS analyze wireless specific traffic including scanning for external users trying to connect to the network through access points and play important role in security to the wireless network. Design of wireless IDS is a difficult task as wireless technology is advancing every day, performance metrics can play an important role in the design of efficient wireless IDS by measuring the factors concern with the performance of a wireless IDS. In this paper we provide a performance metrics scorecard based approach to evaluate intrusion detection systems that are currently popular for wireless networks in the commercial sector. We provide a set of performance metrics that are relevant to wireless IDS and use a "scorecard" containing the set of values as the centerpiece of testing and evaluating a wireless IDS. Evaluation of a wireless IDS is done by assigning score to various performance metrics concern with wireless IDS. We apply our performance metrics scorecard evaluation based approach to three popular wireless IDS Snort-wireless, AirDefense Guard, and Kismet. Finally we discuss the results and the opportunities for further work in this area.

Keywords : IDS, Performance metrics, Performance Constraints Access Points, Wireless, Metrics, Scorecard.

I. Introduction

Wireless network is a novel technology involving the deployment of hundreds of low-cost, micro-hardware, and resource-limited sensor nodes. Wireless technologies are becoming increasingly ubiquitous in modern networks; however, this new technology comes with its own set of challenges. Wireless networks are inherently 'open' and viewable by all network scanners. There are no physical barriers between data sent through the air. As such, it is relatively easy to intercept data packets in a wireless network.

The biggest concern with wireless network is its security, for some time wireless has had very poor, if any, security on a wide-open medium. Wireless Intrusion Detection System (WIDS) is a new solution to help combat this problem. An Intrusion Detection System (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a management station (Wikipedia, 2012). A wireless IDS performs this exclusively for the wireless network. This system monitors traffic on network looking for and logging threats and alerting personnel to respond.

Lord Kelvin said "If you cannot measure it, you cannot improve it". This fact also applies to wireless network security issues. An activity cannot be managed if it cannot be measured, this is a widely accepted management principle and security falls under this rubric. Metrics can be an effective tool for detecting the capability of a wireless IDS. Metrics can help in raising the level of security awareness within the network. Security metrics that are related to wireless network are hard to generate because the discipline itself is still in the early stages of development. There is not yet a common vocabulary and not many documented best practices to follow [4].

In this paper we provide a performance metrics scorecard based approach to evaluate intrusion detection systems that are currently popular for wireless network in the commercial sector. We describe a testing methodology we developed to evaluate Wireless IDS by assigning score to various performance metrics concern with wireless IDS. The approach followed in this paper do not compare wireless IDS against each other, but against a set of performance metrics concern with wireless IDS.

The generalized approach of this paper will allow systems with any wireless requirements to tailor evaluation of ID technologies to their specific needs. Since evaluation is against a static set of performance metrics the evaluation may be extended for other metrics like logistical metrics, architectural metrics, quality metrics etc. The standard approach of comparison used in this paper also gives us scientific repeatability.

II. Snort, Airdefense Guard and Kismet Wireless IDS

In order to explain performance metrics scorecard based evaluation approach to wireless IDS,

Author α : Rupinder Singh, Department of Computer Science, Khalsa College, Amritsar, Punjab, India. E-mail : rupi_singh76@yahoo.com
Author σ : Dr. Jatinder Singh, Principal, Golden College of Engg. & Tech., Gurdaspur, Punjab, India. E-mail : bal_jatinder@rediffmail.com

we choose three wireless IDS namely Snort-wireless, Air Defense Guard, and Kismet as these are one of the most popular and works on different technology.

a) Snort Wireless IDS

Snort wireless is an open source network intrusion detection and prevention system (IDS/IPS) that combines the benefits of signature, protocol, and anomaly-based inspection, and is the most widely deployed IDS/IPS technology worldwide. With millions of downloads Snort has become the de facto standard for IDS/IPS [8]. Snort-wireless allows for custom rules to be created based on framing information from a wireless packet. It also contains rules to attempt to find rogue access points, war drivers, and ad hoc networks.

Snort works by implementing a detection engine that allows registering, warning, and responding to attacks previously defined. Snort is available under GPL (General Public License) and runs under Windows and GNU/Linux. It is among the most widely used, has a number of predefined signatures and continuously updated. Snort can be configured in three modes namely sniffer, packet logger, and network intrusion detection. In addition to all of these basic Snort features, Snort can be set up to send real-time alerts. This provides with the ability to receive alerts in real time, rather than having to continuously monitor Snort system. Snort is like a vacuum that takes packets and allows doing different things.

b) Air Defense Guard Wireless IDS

Motorola Air Defense Guard is a wireless IDS based on statistically anomalous behavior, signature analysis and protocol assessment policy deviation. Air Defense Guard is able to respond to attacks with Active Defense technology by disconnecting attacker's connection to the WLAN.

Air Defense can be used to identity theft by tracking the fingerprints of vendor-specified characteristics along with personal trademarks of authorized users in order to identify intruders in the network. Air Defense can be used to detect Denial-of-Service (DoS) attacks. Air Defense is able to quickly recognize DoS attack that jams the network. Air Defense can also detect Man-in-the-Middle attacks and ensures that access points can only operate on specified channels and proper protocols are used.

c) Kismet Wireless IDS

Kismet IDS is an 802.11 layer2 wireless network detector and sniffer. Kismet is able to work with any wireless card that supports raw monitoring mode, and can be used to sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet IDS also supports plugins that allows sniffing other media such as DECT. Kismet uses data traffic to detect presence of nonbeaconing networks. It identifies standard named networks and hidden networks by passively collecting packets [12].

Kismet wireless IDS without sending any loggable packets is able to detect the presence of both wireless access points and wireless clients, and associate them with each other. Unlike most other wireless network detectors, Kismet is able to log all sniffed packets and save them in a tcpdump /Wireshark or Airsnort compatible file format. Kismet also captures PPI headers. Kismet can also detect default or "not configured" networks, can probe requests, and can also determine the levels of wireless encryptions used for a given access point. Kismet is also able to supports logging of the geographical coordinates from inputs provided by a GPS receiver [13].

III. Performance Metrics Scorecard Based Approach

a) Developing Scorecard

Center piece of testing and evaluating wireless IDS will be a "scorecard" containing the set of performance metrics and their definitions. Each metric can have low (+), average (++), or high (+++) score, where higher scores will be interpreted as more favorable ratings.

The performance metrics used are general characteristics that are relevant to the design of wireless IDS. The method used for observing each performance metric value can be either analysis (source code analysis) or open source material (such as specifications, white papers or reviews provided by vendors or users). We use open source material to analyze each performance metrics for wireless IDS. We examine publicly available research papers, reports, product documentation, published conference material (proceedings) and other material available for public review.

b) Performance Metrics for Wireless IDS

Performance metrics are used to measure the ability of a Wireless IDS to perform a particular task and to fit within the performance constraints. These metrics measure and evaluate the parameters that impact the performance of the wireless IDS [15]. The metrics defined in this area are shown in Table 1.

Table 1 includes only the selected performance metrics. Other performance metrics that can be included are: Analysis of Intruder Intent, Clarity of Reports, Effectiveness of Generated Filters, Evidence Collection, Information Sharing, User alerts, Program interaction, Session recording and Playback, Threat correlation, Trend analysis, Extendibility, Adaptability, Scalability, Overhead, and Latency.

Table 1 : Selected performance metrics for a Wireless IDS

Performance Metrics	Description
False Positive Ratio	This is the ratio of alarms that are wrongly raised by the wireless IDS to the total number of transactions.
False Negative Ratio	This is the ratio of actual attacks that are not detected by the wireless IDS to the total number of transactions.
Cumulative False Alarm Rate	The weighted average of False Positive and False Negative ratios.
Induced Traffic Latency	It measures the delay in the arrival of packets at the target network in the presence and absence of a wireless IDS.
Stress Handling and Point of Breakdown	The point of breakdown is defined as the level of network or host traffic that results in a shutdown or malfunction of IDS.
IDS Throughput	This metric defines the level of traffic up to which the IDS performs without dropping any packet.
Depth of System's Detection Capability	It is defined as the number of attack signature patterns and/or behavior models known to it.
Reliability of Attack Detection	It is defined as the ratio of false positives to total alarms raised.
Possibility of Attack	It is defined as the ratio of false negatives to true negatives.
Consistency	It is defined as the variations in the performance of a wireless IDS.
Error Reporting and Recovery	The ability of a wireless IDS to correctly report and recover.
Firewall Interaction	The ability of a wireless IDS to interact with the Firewall systems.
User Friendliness	The ability of a wireless IDS to configure according to user's environment.
Router Interaction	Degree of interaction of a wireless IDS with the router.
Compromise Analysis	It is the ability to report the extent of damage and compromise due to intrusions.
Simple Network Management Protocol (SNMP) Interaction	Ability of the wireless IDS to send an SNMP trap to one or more network devices in response to a detected attack.
Timeliness	Average/maximal time between an intrusion's occurrence and its being reported.

c) Performance Metrics Scorecard Based Approach

In this section of the paper we will apply above mentioned approach to popular wireless IDS Snort-wireless, AirDefense Guard, and Kismet. We choose these three for evaluation as they are most widely used and have different ways of working. Below with table 2 we describe how scores to performance metrics related to these three wireless IDS are assigned.

Performance metric False Positive Ratio can be assigned score depending on the following criteria:

- Low Score (+): Wireless IDS generate high False Positive Ratio.
- Average Score (++): Wireless IDS generate average False Positive Ratio.
- High Score (+++): Wireless IDS generate low or no False Positive Ratio. False positive rate depends largely on the method used to detect intrusions: an anomaly-based wireless IDS produces more false positives than signature- bases ones [16]. Snort wireless combines the benefits of protocol, signature, and anomaly-based inspection and produces low false positive ratio and gets a high score for this metric [8]. Air Defense guard has ability to detect 200+ attacks and policy violations and therefore produces less false positives. Kismet alert PROBENOJOIN can result excessive false positives while channel hopping is done. False positives are also possible in noisy/lossy situations, it is desirable to disable this alert in some installations [12].

Performance metric False Negative Ratio can be assigned score depending on the following criteria:

- Low Score (+): Wireless IDS generate high False Negative Ratio.
- Average Score (++): Wireless IDS generate average False Negative Ratio.
- High Score (+++): Wireless IDS generate low or no False Negative Ratio.

Table 2 : Scorecard for Snort, AirDefense Guard and Kismet wireless IDS

Performance Metrics	Snort wireless	AirDefense Guard	Kismet
False Positive Ratio	+++	+++	++
False Negative Ratio	+	++	++
Cumulative False Alarm Rate	++	++	++
Induced Traffic Latency	++	+++	++
Stress Handling and Point of Breakdown	++	+++	++
IDS Throughput	+++	+++	++
Depth of System's Detection Capability	+++	+++	++
Reliability of Attack Detection	++	+++	++
Possibility of Attack	+	++	++
Consistency	++	++	++
Error Reporting and Recovery	+++	+++	++
Firewall Interaction	+++	+++	+++
User Friendliness	++	+++	+
Router Interaction	+++	+++	++
Compromise Analysis	++	++	++
SNMP Interaction	+++	+++	++
Timeliness	++	++	++

Snort-Wireless is the most advanced Open Source Wireless IDS. It uses the sequence number analysis technique to detect false frame attacks. In [19] authors tested the effectiveness of the Snort-Wireless with the used data applying the purposed analysis technique. It is not capable of identifying the malicious packets as the threshold-based technique used by Snort-Wireless is prone to false negatives. Table 3 provides the results produced by authors. AirDefense Guard wireless IDS produces very low false negative ratio as it has ability to detect 200+ attacks and policy violations. Kismet has less attack definitions and produces average false negative ratio.

Performance metric Cumulative False Alarm Rate can be assigned score depending on the following criteria:

Table 3 : Snort-wireless alert results (a) during attack with low traffic. (b) during an attack with high traffic [19]

(a)

Attack frames	499
Alerts	121
True Positives	90
False Positives	31
False Negatives	378

(b)

Attack frames	472
Alerts	110
True Positives	83
False Positives	27
False Negatives	362

- Low Score (+): Wireless IDS generate high Cumulative False Alarm Rate.
- Average Score (++): Wireless IDS generate average Cumulative False Alarm Rate.
- High Score (+++): Wireless IDS generate low or no As discussed above Snort-wireless and AirDefense Guard produces low false positive rate and high false negative rate, therefore they get average score for the metric Cumulative False Alarm Rate. Kismet produces average false positive and false negative ratios and therefore generates average score for Cumulative False Alarm Rate.

Performance metric Induced Traffic Latency can be assigned score depending on the following criteria:

- Low Score (+): Wireless IDS presence highly delays the arrival of packets at the target network.
- Average Score (++): Wireless IDS presence delays the arrival of packets at the target network.
- High Score (+++): Wireless IDS presence has no or little delay in the arrival of packets at the target network.

Inside the packet processing function, Snort performs several tasks. First, it calls into libpcap using the *pcap_dispatch* function to process any waiting packets. For each packet that is available, libpcap calls the *Pcap Process Packet* function, which handles the actual packet processing. This function resets several per-packet counters, collects some statistics about the packet, and calls *Process Packet*. The *Process Packet* function handles all of the details of decoding the packet, printing the packet to the screen and either directly calling the packet logging functions or calling into the pre-processors. If no packets are available, Snort performs basic housekeeping chores such as checking for pending signals. In order to perform all this functions, Snort-Wireless IDS delays the arrival of packets at the target network. Air Defense has the most detailed available wireless forensic database in the industry. It has more than 300 wireless statistics per device per minute logged and has instant analysis using the forensic wizard [20]. The point of breakdown is defined as the level of network or host traffic that results in a shutdown or malfunction of IDS. Air Defense. Kismet IDS identifies networks by collecting passively packets

and detecting standard named networks, detecting hidden networks, and inferring to the presence of networks (non-beaconing) via data traffic.

Performance metric Stress Handling and Point of Breakdown can be assigned score depending on the following criteria:

- Low Score (+): Wireless IDS cannot handle stress and easily breakdowns.
- Average Score (++): Wireless IDS can handle stress up to some extent before it breakdowns.
- High Score (+++): Wireless IDS can handle stress at the maximum and can avoid breakdown.

The detection engine is the time-critical part of Snort wireless. Depending upon how powerful user machine is and how many rules have been defined, it may take different amounts of time to respond to different packets. If traffic on the network is too high when Snort wireless is working in NIDS mode, it may drop some packets and may not get a true real-time response. The load on the detection engine of snort wireless depends upon the following factors:

- Number of rules
- Power of the machine on which Snort is running
- Speed of internal bus used in the Snort machine
- Load on the network

Motorola Air Defense utilizes its 24x7, real-time monitoring of the 802.11a/b/g networks for most accurate intrusion detection of known as well as unknown attacks and does not easily breaks down. Kismet is able to handle stress up to some extent.

Performance metric IDS Throughput can be assigned score depending on the following criteria:

- Low Score (+): Wireless IDS regularly drops packets.
- Average Score (++): Wireless IDS rarely drops packets.
- High Score (+++): Wireless IDS can perform without dropping any packet.

When Snort wireless is working in Inline mode, it works like an Ethernet bridge, that is, in order to monitor a network segment, it has to be inserted transparently with two bridged NICs. With this setup, any packet can flow through the bridge from a network card to the other, unless it matches the drop rules; in that case, the switch opens and blocks the packet. So, Snort wireless drops packet only when it matches the drop rule specified by the user. Studies have shown that Air Defense rarely drops packets. Kismet processes data rate as supported by access point and drops more packets than others.

Performance metric Depth of System's Detection Capability can be assigned score depending on the following criteria:

- Low Score (+): Wireless IDS has low number of attack signature patterns and/or behavior models known to it.
- Average Score (++): Wireless IDS has average number of attack signature patterns and/or behavior models known to it.
- High Score (+++): Wireless IDS has high number of attack signature patterns and/or behavior models known to it.

Snort wireless maintains a rule set in order to have the latest detection capabilities. Sourcefire Vulnerability Research Team (VRT) Rules are the official rules of snort wireless. One of the best features of Snort is its rule engine and language. Snort's rule engine provides an extensive language that enables user to write their own rules, allowing them to extend it to meet the needs of their own network. Motorola Air Defense wireless IDS utilizes 24x7, real-time monitoring of the 802.11a/b/g networks for producing most accurate intrusion detection of known and unknown attacks. It has ability to detect 200+ attacks and policy violations [20]. Kismet has less number of attacks detections as compare to snort wireless and Air Defense guard.

Performance metric Reliability of Attack Detection can be assigned score depending on the following criteria:

- Low Score (+): Wireless IDS generates high ratio of false positives to total alarms raised.
- Average Score (++): Wireless IDS generates average false positives to total alarms raised.
- High Score (+++): Wireless IDS generates low ratio of false positives to total alarms raised.

As shown in table 3, during attack with low traffic Snort wireless produces 31 false positives out of total 121 alerts. During attack with high traffic it produces 27 false positives out of total 110 alerts. So, snort wireless generates nearly average false positives to total alarms raised. Air Defense guard has ability to detect 200+ attacks and policy violations and therefore produces less false positives and is very reliable. Reliability of Attack Detection is average in kismet as it has average false positive ratio.

Performance metric Possibility of Attack can be assigned score depending on the following criteria:

- Low Score (+): Wireless IDS generates high ratio of false negatives to true negatives.
- Average Score (++): Wireless IDS generates average ratio of false negatives to true negatives.
- High Score (+++): Wireless IDS generates low ratio of false negatives to true negatives.

As shown in table 3, during attack with low traffic Snort wireless produces 378 false negatives and 121 true negatives corresponding to 499 attack frames. During attack with high traffic it produces 362 false negatives and 110 true negatives out of total 472 attack

frames. So, Wireless IDS snort generates high ratio of false negatives to true negatives. Air Defense guard has ability to detect 200+ attacks and policy violations and therefore produces less false positives and it generates low ratio of false negatives to true negatives. Kismet has average Possibility of Attack as it has average false negative ratio.

Performance metric Consistency can be assigned score depending on the following criteria:

- Low Score (+): Wireless IDS has high variations in the performance.
- Average Score (++): Wireless IDS has average variations inthe performance.
- High Score (+++): Wireless IDS has low or no variations in the performance.

In [20] author evaluated two open source network based intrusion detection systems. Snort wireless performed well during tests, but did produce false positives and false negatives. Snort is very lightweight and fast but is limited in its ability to scale in bandwidth per instance. Studies show that Air Defense and kismet has average variations in the performance.

Performance metric Error Reporting and Recovery can be assigned score depending on the following criteria:

- Low Score (+): Wireless IDS has low or no ability to correctly report and recover.
- Average Score (++): Wireless IDS has average ability to correctly report and recover.
- High Score (+++): Wireless IDS has high ability to correctly report and recover.

Snort wireless generates reports that show what happened during the last day, week or month. - T option of snort wireless is very useful for testing and reporting on the Snort configuration. This option can be used to find any errors in the configuration files. Snort wireless provides tool that gives user a detailed report of actions taken during the update process. SPADE module keeps a record of history data and uses threshold values to report the anomalies. Air Defense guard has flexible alerting and reporting options with integration capabilities into the various Security Information Management (SIM) systems [20]. Error Reporting and Recovery of kismet is poor as compare to snort wireless and Air Defense.

Performance metric Firewall Interaction can be assigned score depending on the following criteria:

- Low Score (+): Wireless IDS has poor interaction with the Firewall systems.
- Average Score (++): Wireless IDS has average interaction with the Firewall systems.
- High Score (+++): Wireless IDS has excellent interaction with the Firewall systems.

Snort Sam is a tool used to make Snort work with most commonly used firewalls. It is used to create a Firewall/IDS combined solution. Firewall can be configured to automatically block offending data and addresses from entering system when intruder activity is detected. It is available from http://www.snortsam.net/ where one can find the latest information. The tool consists of two parts:

1. A Snort output plug-in that is installed on the Snort sensor.
2. An agent that is installed on a machine close to Firewall or Firewall itself. Snort communicates to the agent using the output plug-in in a secure way. Air Defense Guard supports stateful Layer 2 and role-based firewalls and base security policy on the user, group, location, encryption strength, etc. studies show that kismet also has good Firewall Interaction.

Performance metric User Friendliness can be assigned score depending on the following criteria:

- Low Score (+): It is difficult to configure wireless IDS according to user's environment.
- Average Score (++): Wireless IDS can be configured up to some extent according to user's environment.
- High Score (+++): Wireless IDS can be easily configured according to user's environment.

In snort wireless a thorough understanding of what snort. conf file is and how to configure it is essential to a successful deployment of Snort wireless as an IDS in user environment. Snort configuration consists of Global configuration (snort. conf), Optional **.rules* file(s), and Additional files. Air Defense Guard is very user friendly as it provides location tracking of the devices on a map, and provides minute by minute granular forensic information for any of the device. Kismet only runs under LINUX and does not have easy to use graphical interface.

Performance metric Router Interaction can be assigned score depending on the following criteria:

- Low Score (+): Wireless IDS has a poor interaction with the router.
- Average Score (++): Wireless IDS has an average interaction with the router.
- High Score (+++): Wireless IDS has excellent interaction with the router.

Depending upon the type of router used, snort wireless can be used on a port. Some routers, like Cisco, allow to replicate all ports traffic on one port where snort machine can be attached. These ports are usually referred to as spanning ports. The best place to install Snort wireless is right behind the firewall or router so that all of the Internet traffic is visible to Snort before it enters any router or hub. Air Defense Guard provides nice router interaction. Kismet does not have good interaction with some of the routers like belking54g.

Performance metric Compromise Analysis can be assigned score depending on the following criteria:

- Low Score (+): Wireless IDS has a poor ability to report the extent of damage and compromise due to intrusions.
- Average Score (++): Wireless IDS has average ability to report the extent of damage and compromise due to intrusions.
- High Score (+++): Wireless IDS has excellent ability to report the extent of damage and compromise due to intrusions.

Snort wireless IDS captures intrusion data and stores it in My SQL database using output plug-in that can be viewed by administrator, but it cannot properly report the extent of damage caused by intruder. Air Defense Guard IDS utilizes it's the 24x7, real-time monitoring of the 802.11a/b/g networks for the most accurate detection of intrusion of known and unknown attacks and therefore has very less compromise due to intrusions. Kismet does not have Compromise Analysis reporting as in snort wireless and Air Defese.

Performance metric SNMP Interaction can be assigned score depending on the following criteria:

- Low Score (+): Wireless IDS has poor ability to send an SNMP trap to one or more network devices in response to a detected attack.
- Average Score (++): Wireless IDS has average ability to Send an SNMP trap to one or more network devices in response to a detected attack.
- High Score (+++): Wireless IDS has high ability to send an SNMP trap to one or more network devices in response to a detected attack.

In snort wireless snort SnmpPlugin is used to send snmp alerts to network management systems (NMS). The alerts can be traps or informs. This adds to significant power of the NMS by allowing it to monitor security of the network. It also allows snort wireless sensor to exploit the features that are built into the existing network management systems. Air Defense Guard eliminates many of vulnerabilities impacting the security of the wireless network by providing good interaction with SNMP. Kismet provides various utilities for configuring and monitoring of wireless Access Points under Linux using SNMP protocol.

Performance metric Timeliness can be assigned score depending on the following criteria:

- Low Score (+): Wireless IDS takes a lot of time to report the occurrence of an intrusion.
- Average Score (++): Wireless IDS takes average time to report the occurrence of an intrusion.
- High Score (+++): Wireless IDS takes a minimal time to report the occurrence of an intrusion.

Snort wireless is a packet-based system. The basic life of a packet inside snort starts with packet acquisition. Once the packet is inside snort it is passed into the packet decoder. After decoding, the packet is passed on to the pre-processors for normalization, statistical analysis, and some nonrule-based detection. Once the pre-processors are done with the packet it goes into the detection engine, where it is evaluated against all of the rules that were loaded from the configuration file. Finally, the packet is sent off into the output plug-ins for logging and alerting. So, it takes lot of time for snort wireless to detect an attack. Air Defense Guard takes average time for reporting of intrusion as it has 200+ attacks and policy violations detection capability. Studies show that kismet is slow in detection as compare to snort wireless and Air Defense.

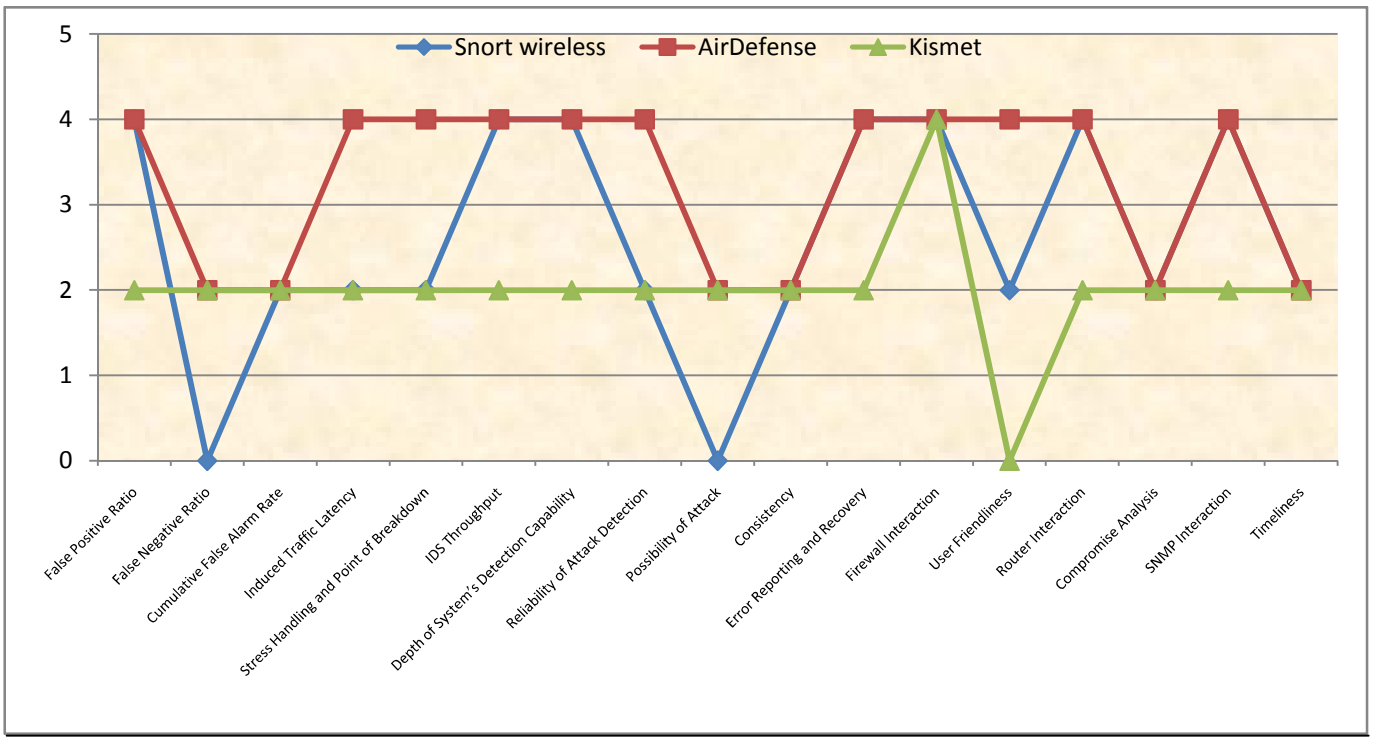

Figure : Graph showing score of Snort, Air Defense and Kismet wireless IDS. Scores are converted to numeric i.e. +: 0, ++: 2, and +++: 4

IV. Conclusion and Future Work

Wireless IDS are used in detecting unwanted activities on a wireless network. Performance metrics can be used to measure the performance of a wireless IDS within the performance constraints. These metrics measure and evaluate the parameters that impact the performance of the wireless IDS. This paper provides a performance metrics scorecard based approach that can be used for evaluating a wireless IDS in order to find out how it behaves within performance constraints.

In this paper we provide various performance metrics concern with wireless IDS and a scorecard method for evaluation. Evaluation of a wireless IDS is done by assigning scores to various performance metrics. We use our evaluation methodology to test popular wireless IDS Snort, Air Defense Guard, and Kismet. We define commonly used performance metrics that are important to a wireless IDS, but a lot is required to be done to find out more ones like analysis of intruder intent, clarity of reports, effectiveness of generated filters, evidence collection, information sharing, user alerts, program interaction, session recording and playback, threat correlation, trend analysis, extendibility, adaptability, scalability, overhead, and latency. More performance metrics and their definitions can be defined as lessons are learned while evaluating a wireless network. Future work also includes applying the evaluation methodology to other metrics concern with wireless IDS like logistical metrics, architectural metrics, quality metrics etc.

References Références Referencias

1. Rupinder Singh, Dr. Jatinder Singh, "A Metrics Based Approach to Intrusion Detection System Evaluation for Wireless Network,"International Journal of Education and Applied Research (IJEAR) Vol.1, Issue 1, Ver. 1:Jul.-Dec, 2011, ISSN: 2249-4944.
2. G. A. Fink, B. L. Chappell, T. G. Turner, and K. F. O'Donoghue, "A Metrics - Based Approach to Intrusion Detection System Evaluation for Distributed Real-Time Systems," WPDRTS, 15 - 17 April 2002, Ft. Lauderdale, Florida.
3. Harrykar Freelance, "HARRYKAR'S TECHIES BLOG Snort, IDS, IPS, NSM, hacking and.... beyond, " 31 May 2009
4. Eugene Albin, "A comparative analysis of the snort and suricata intrusion-detection systems, "September 2011.
5. SNORT Users Manual 2.9.0, The Snort Project, March 25, 2011
6. J. Gómez, C. Gil, N. Padilla1, R. Baños, and C. Jiménez, "Design of a Snort-Based Hybrid Intrusion Detection System," S. Omatu et al. (Eds.) : IWANN 2009, Part II, LNCS 5518, pp. 515–522, 2009.
7. Rafeeq Ur Rehman, " Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID," Prentice Hall, ISBN 0-13-1407 33-3
8. http://www.snort.org/

9. Reijo Savola, "On The Feasibility of Utilizing Security Metrics in Software Intensive Systems, " IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.1, January 2010.
10. Snehal Boob and Priyanka Jadhav, "Wireless Intrusion Detection System," International Journal of Computer Applications (0975–8887) Volume 5 No.8, August 2010.
11. David, J., and Benjamin, M., 2011, "A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engines," ICDS 2011 : The Fifth International Conference on Digital Society, ISBN: 978-1-61208-116-8.
12. http://www.kismetwireless.net/
13. http://en.wikipedia.org/wiki/Kismet
14. Fayssal, Samer, " Performance analysis Toolset for wireless intrusion detection systems," 2010 International Conference on High Performance Computing and Simulation (HPCS),Caen, France, ISBN: 978-1-4244-68 27-0
15. Gautam Singaraju, Lawrence Teo, and Yuliang Zheng1, "A Testbed for Quantitative Assesment of Intrusion Detection Systems Using Fuzzy Logic," Proceedings of The Second IEEE International Information Assurance Workshop (IWIA'04) 0-7695-2117-7/04.
16. Fatbardh Veseli, "Wireless Intrusion Detection Systems,"
17. http://www.securityworm.com/software/ wireless sec urity /intrusiondetectionsystems/airdefense-guard. Html
18. http://www.cysols.com/contrib/snortsnmp/README. SN MP
19. Asier Mart´ınez_, Urko Zurutuzayz, Roberto Uribeetxeberriay, Miguel Fern´andezy, Jesus lizarragay, Ainhoa Sernay and I˜naki V´elezy, "Beacon Frame Spoofing Attack Detection in IEEE 802.11 Networks"
20. PCI Wireless Compliance Demystified Best Practices for Retail, White paper. http:// www. airdefense.net/PCIpaper. Pdf
21. Rupinder Singh, Dr. Jatinder Singh, "A Logistic Metrics Scorecard Based Approach to Intrusion Detection System Evaluation for Wireless Network," International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol. 2 No.3 June 2012. ISSN: 2250 – 3501 (Online), 2277 - 5307 (Print).
22. Rupinder Singh, Dr. Jatinder Singh "An Architectural Metrics Scorecard Based Approach to Intrusion BDetection System Evaluation for Wireless Network," Global Journal of Computer Science and Technology (GJCST) Volume 12 Issue 11 Version 1.0 June 2012

This page is intentionally left blank