**Name: Keerthana Satish**

**Student ID: 40036641**

**INSE 6150: Security Evaluation Methodologies (Fall 2016)**

**Assignment 1: IDS TOOLS Evaluation**

Security is one of the key component for any organization. It is known that even today attackers are finding different means to invade numerous homes and organizations across the world via virus, worms, Trojans, DoS/DDoS attacks by inserting bits of malicious code. Intrusion detection system (IDS) was developed to detect actions that attempt to compromise the confidentiality, integrity or availability of a resource. More specifically, the goal of intrusion detection is to identify entities attempting to subvert in-place security controls [1].

Intrusion detection is the act of detecting unwanted traffic on a network or a device. An Intrusion Detection System can be a piece of installed software or a physical appliance(hardware) that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable use policies.

Many IDS tools will also store a detected event in a log to be reviewed at a later date or will combine events with other data to make decisions regarding policies or damage control [2].

The key functionalities of IDS can be pointed out as follows—

• Recording information related to observed events.

• Notifying administrators of important observed events.

• Producing reports.

There are more than hundreds of Intrusion detection systems or tools available in the market at present and this space continues to grow. Free ware or open source tools are known to be very effective and also powerful, if configured and managed properly.

For the purpose of this Assignment, I have chosen three Freeware (open source) and three Commercial tools. Snort, Prelude and Samhain are the open source tools evaluated and Juniper, McAfee – IntruShield, and Internet Security systems- REAL SECURE are the commercial tools evaluated. I have chosen one open source and one commercial tool under [3] [4] -

1. Host based IDS Ex- Samhain and Internet Security systems- REAL SECURE

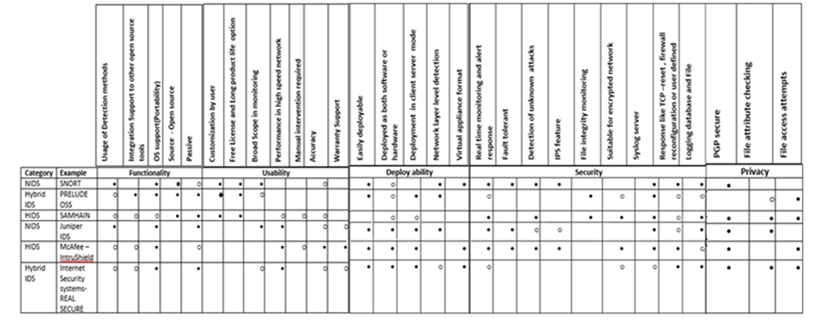
2. Network based IDS - Ex- Snort and Juniper.

3. Hybrid based IDS - Ex- Prelude and Internet Security systems- REAL SECURE

The rows represent the different available alternatives for IDS tools, the column represent the criteria chosen for evaluation and the cells have scores or grades as per my evaluation.

* - This symbol within a cell represents that the alternative fully satisfies the given criteria.
* - This symbol within a cell represents that the alternative partially satisfies the given criteria.

An empty cell represents that alternative does not or fails to satisfy the given criteria.



**FUNCTIONALITY – Criteria 1: Usage of Detection methods**

* - If the tool satisfies all Detection method mentioned here.
* - If the tool satisfies any one or two Detection method mentioned here.

**SNORT** is a network intrusion detection system combining the benefits of signature, protocol, and anomaly-based inspection [5]. **Prelude** – The Prelude LML is a signature-based log analyzer monitoring log files and received syslog messages for suspicious activity [6]. It has signatures for knowledge-based detection [3]. **Samhain** - HIDS will usually remember its attributes and create a checksum for the contents, this information gets stored in a secure database for later comparison [6]. A rule based IDS continuously needs rules or signature updates, predefined set of signatures or rules are provided by vendors [7]. **Juniper** - With MMD, Juniper utilizes eight different detection methods, including protocol anomaly detection, traffic anomaly detection, some advanced techniques, such as Stateful Signature™ and backdoor detection, and others [8]. **McAfee IntruShield** - The IntruShield architecture integrates patented signature, anomaly, and Denial of Service detection on a single purpose-built appliance [9]. **Internet security Systems – Real Secure** - The manager console also allows for alert monitoring and offers an online database of well over 2000 attack signatures [10].

**Criteria 2: Integration support with other open source tools**

• - If the tool supports integration with more than two other open source tools.

* + - If the tool supports integration with only one open source tool.

Blank cell – If the tool doesn’t support integration with any open source tool.

**Prelude** benefits from a native support with a number of systems dedicated to enriching information even further (snort, Samhain, ossec, auditd, etc.) [11]. **Samhain** can be compiled against the libprelude library, which will enable it to function as a prelude sensor [12]. **McAfee** is aiming towards bridging the Snort barrier by fully integrating with Snort signatures in order to get better community signatures [13] [14]. **Internet security Systems – Real Secure** -ISS RealSecure has modules that allow you to use Snort rules [15].

**Criteria 3: OS support**

• - If the tool supports integration with Operating systems independently.

O - If the tool does not support integration with Operating systems independently.

**Samhain** - Windows clients require Cygwin [16].

**Criteria 4: Open source tools**

• - If the software is available as open source, Blank cell – commercial ware

**Criteria 5: Passive tool**

• - If the tool is completely passive.

O - If the tool is active in inline mode or acts as IPS in inline mode.

When Snort and IntruShield are in Inline mode, they act as an IPS allowing drop rules to trigger [5] [14].

**USABILITY - Criteria 1: Customization**

• - If source code is released for use or modification by the community. Users can make changes to the code as they please, Blank cell – commercial ware

**Criteria 2: Long product life**

• - Long product life with no signs of going away, Blank cell – commercial ware.

**Criteria 3: Scope of monitoring - Broad**

• - If the tool has broad scope for monitoring.

O - If the tool is a hybrid IDS covering both areas of NIDS and HIDS.

Blank cell - If the tool only monitors specific activities. By definition, All NIDS are Broad in scope and all HIDS are Narrow in scope (monitors specific activities) [17].

**Criteria 4: Performance in high speed network**

• - If the efficiency of performance in high speed network is similar to low or medium speed network.

O - If the efficiency of performance in high speed network is little lesser to low or medium speed network.

Blank cell –if efficiency drops and tool becomes insecure

**Snort** operating with default settings, Snort performs poorly, and is not suited for running in high-speed environments. Even with the modifications done in snort.noflow.conf, Snort still gave an unsatisfactory high drop ratio [18]. Results show that the Snort system imposes noticeably more impacts on network traffic than **Samhain** IDS. It could be a bottleneck on a high speed network. In addition, Snort occupies more system memory than Samhain. However, it generates lower CPU load. The Samhain system imposes the most CPU load among the tested IDSs [19].

**Criteria 5: Manual Intervention required**

O - If partial Manual Intervention is required for analyzing and filtering of logs or to set user defined action, Blank cell – No manual intervention required to analyze or filter logs.

**Criteria 6: Accuracy**

**• -** If the tool has better accuracy than all other tools considered for evaluation.

O - If the tool has average accuracy compared to other tools considered for evaluation.

Blank cell – If the tool has least accuracy compared to other tools considered for evaluation [20] [21].

**Criteria 7: Warranty support**

**• -** Renewable annual as part of support agreement [21]

O - One year with some extension [21]

Blank cell – 0pen source tools does not offer any warranty support [5] [11] [12].

**DEPLOYABILITY - Criteria 1: Ease of deployment**

**• -** Installed and configured easily**,** Blank cell – Harder to install [16]

**Criteria 2: Can be Deployed as both hardware /software**

**• -** Deployed as both hardware /software [21]

O - only be deployed as software

**Criteria 3: Deployment only in Client server mode**

**• -** Deployment only in Client server mode

O - Deployment in Client server mode and stand alone

**Criteria 4: Detection of malware in network layer level**

**• -** Detection possible in network layer level [22]

O - Detection partially possible in network layer level [22]

Blank cell – Detection impossible in network layer level.

**Criteria 5: Virtual appliance format**

**• –** VMware support possible [23]

Blank cell – VMware support not possible.

**PRIVACY - Criteria 1: PGP secure**

• - Tool is PGP secured / Signed [24]

Blank cell – Tool is not PGP secured / Signed

**Criteria 2: File attribute checking**

**• -** This is periodically checking the attributes of important files, such as ownership and permissions, for changes [12] [8] [25].

O - File attribute checking partially possible [11]

Blank cell - File attribute checking feature not available.

**Criteria 3: File access attempt**

**• -** Agent compares those policies to the characteristics of the current attempt, including which user or application is trying to access each file, and what type of access has been requested (read, write, execute) [12] [25] [8] [11].

Blank cell - File access attempt checking feature not available.

**SECURITY - Criteria 1: Real time monitoring and alert response**

**• -** Gives Real time monitoring and alert response [21].

O - Gives near Real time monitoring and alert response [11]

**Criteria 2: Fault tolerance**

**• -** An intrusion-detection system should itself be resistant to attacks, particularly denial of service [3].

Blank cell – Not resistant to denial of service (DOS/DDOS) attack.

**Criteria 3: Detection of zero day and unknown attacks**

**• -** Resistant to Zero-day attack and new attacks [3].

O – Partially Resistant to Zero-day attack and new attacks [3].

Blank cell - Not Resistant to Zero-day attack and new attacks [11] [25].

**Criteria 4: IPS feature**

**• -** If the tool acts as IPS in inline mode. When Snort and IntruShield are in Inline mode, they act as an IPS [5] [14].

O – If the tool acts partially as IPS [8].

Blank cell – IPS feature is not present.

**Criteria 5: File Integrity Monitoring**

**• -** Presence of FIM feature [11] [12].

Blank cell – FIM feature is not present.

**Criteria 6: Suitable for Encrypted network**

**• -** BetterPerformance in Encrypted network.

O – AveragePerformance in Encrypted network.

Blank cell – Least performance in Encrypted network.

All Host based IDS Suitable for encrypted network and Network based IDS Not suitable for encrypted network.

**Criteria 7: Syslog server**

**• -** Presence of Syslog server [8] [9] [11] [12] [5].

O – Partial Presence of Syslog server [25].

**Criteria 8: Response**

**• -** ActiveResponse to TCP reset, firewall, Reconfiguration or other user defined response [5] [9] [25]

O – Response to, firewall and other user defined response [11] [12] [8]

**Criteria 9: Logging Database and file**

**• -** Logging Database [12] [8] [5] [25]

O – partial Logging Database [11] [9].

**REFERENCES**

[1] <https://www.sans.org/security-resources/idfaq/what-is-intrusion-detection/1/1>

[2] Nilotpal Chakraborty, INTRUSION DETECTION SYSTEM AND INTRUSION PREVENTION SYSTEM: A COMPARATIVE STUDY; International Journal of Computing and Business Research (IJCBR), ISSN (Online): 2229-6166, Volume 4 Issue 2 May 2013

[3] <http://www.ccs-labs.org/teaching/netsec/2012s/>

[4] Asmaa Shaker Ashoor, Prof. Sharad Gore, Importance of Intrusion Detection System (IDS); International Journal of Scientific Engineering Research, I061227

[5] SNORT website, http://www.snort.org, 30 Oct 2013

[6] Jack TIMOFTE, Intrusion Detection using Open Source Tools; Revista Informatica Economică nr.2(46)/2008

[7] Al-Sakib Khan Pathan, The State of the Art in Intrusion Prevention and Detection

[8] White Paper - Intrusion Detection and Prevention, Protecting Your Network from Attacks; 2006, Juniper Networks, Inc.

[9] White Paper- McAfee® IntruShield® IPS User-Defined Signature Creation version 4.1; 2007

[10] SANS Institute InfoSec Reading Room, Intrusion Detection Systems: An Overview of RealSecure; SANS Institute 2001,

[11] prelude website, <https://www.prelude-siem.org/projects/prelude>

[12] Samhain website, <http://www.la-samhna.de/samhain>

[13] <https://playingwithothers.com/2014/08/13/mcafee-now-highlighting-snort-signature-integration/>

[14] <https://community.mcafee.com/docs/DOC-6086>

[15] <http://searchsecurity.techtarget.com/tip/Why-Snort-makes-IDS-worth-the-time-and-effort>

[16]<https://www.alienvault.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview>

[17] Sailesh Kumar, “Survey of Current Network Intrusion Detection Techniques”, available at <http://www.cse.wustl.edu/~jain/cse571-07/ftp/ids.pdf>

[18] Martin Riegel, Claes Lyth Walsø, Intrusion Detection in High-Speed Networks; <https://brage.bibsys.no/xmlui/bitstream/handle/11250/250528/347522_FULLTEXT01.pdf?sequence=1&isAllowed=y>

[19] Xinli Wang, Alex Kordas, Lihui Hu, Matt Gaedke, Derrick Smith; Administrative Evaluation of Intrusion Detection System[20] C. A. P. Boyce, A. N. Zincir-Heywood, A Comparison of Four Intrusion Detection Systems for Secure E-Business

[21] <http://www.zdnet.com/article/detection-and-prevention-6-intrusion-detection-systems-tested/>

[22] <http://wiki.cas.mcmaster.ca/index.php/Systems_for_Detecting_Network_Intrusion>

[23] <http://searchsecurity.techtarget.com/tip/Security-in-virtualization-IDS-IPS-implementation-strategy>

[24] 1SURYA BHAGAVAN AMBATI, 2DEEPTI VIDYARTHI, A BRIEF STUDY AND COMPARISON OF, OPEN SOURCE INTRUSION DETECTION SYSTEM TOOLS; International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-1, Issue-10, Dec-2013

[25] <ftp://public.dhe.ibm.com/software/security/products/infrastructure_protection/RealSecureServerSensor/IBM_RealSecure_Server_Sensor_System_Requirements.pdf>