CONCEPTUAL RESEARCH PAPER

COMPUTING TRENDZ Vol X No. 1,2 , January - December 2020 Print ISSN : 2230-9152, Online ISSN 2456-138X

A comparative Study of Various Intruder Detection Tools

Anuj Kumar[1], Himanshu Hora[2], Anand Prakash Dube[3]

[1&2] Assistant Professor, SRC, Muzaffarnagar

[3] Associate Professor, School of management Science, Varanasi

ABSTRACT

Today is the era of internet. The vast information is exchange day to day life over the network using internet. The various attacks that is harmful for data such as Denial of Service, Sniffer attacks and Application-Layer attacks. The basic concern is to provide the security to such attacks. A wide variety of algorithm has been developed which can detect and prevents with these security threat. Among all of these, the Intrusion Detection System (IDS) is one of the security technology plays a vital role in detecting and preventing both insider and outsider attack by scanning the traffic in multiple ways and pass reports to the administrator. This paper compares the various features and parameters of existing IDS tools such as Snort, Suricata, Bro, and NFR etc.

Keywords : IDS Tools :(Snort, Suricata, Bro, NFR, ACARM-ng, EMERALD).

Computing Trendz (2020). DOI: 10.21844/cttjetit.v10.i01.17091

Introduction

Today, there are huge amount valuable data transfer over the networks. But one thing that unsecure over mind is security of data. The term intrusion is an activity of unauthorized access of data and compromising network security goals. The Intrusion detection is the system that observe and analyzes the network traffic for the pattern of possible attack. Intrusion Detection structures (IDS), though a new discipline of studies, has attracted sizeable interest towards itself and currently almost each day extra researchers are engaged on this subject of labor. The current trend for the IDS is to make it possible to come across novel community attacks. The primary difficulty is to make certain that in case of an intrusion strive, the system is capable to come across and to file it. Intrusion detection structures (IDSs) are generally deployed alongside with other preventive protection mechanisms, such as get admission to manipulate and authentication, as a 2nd line of protection that protects information structures. There are several reasons that make intrusion detection an essential part of the whole protection of system .First, many traditional systems and applications were developed without security in mind. In other cases, systems and applications were developed to work in a different environment and may become vulnerable when deployed Intrusion detection complements these protective mechanisms to improve the system security. Moreover, even if the preventive security mechanisms can protect information systems successfully, it is still desirable to know what intrusions have happened or are happening, so that we can understand the security threats and risks and thus be better prepared for future

Corresponding Author: Anuj Kumar, Assistant Professor, SRC, Muzaffarnagar, dixit.anuj12008@gmail.com

How to cite this article: Kumar, A., Hora, H., Dube, A.P. (2020). A comparative Study of Various Intruder Detection Tools. Computing Trendz 10(1&2): 1-7

Source of support: Nil

Conflict of interest: None

attacks.

In recent years there are so many commercial and freeware IDS tools (snort , Bro, OSSEC, AIDE, NFR etc.,) were developed to cope with threats(DOS attack, Spoofing, User to Root attck,port scanning, Evasion etc.,) .This paper provides the detailed comparison overview of six IDS tools such as Snort, Bro, Suricata, NFR, Emerald ,ACARM-ng

Intrusion-Detection System (IDS):

An intrusion detection system examines all incoming and outgoing network movement and determines distrustful patterns that may be a sign of a network attack from someone attempting to breakdown a system [JC 2007]. The functionalities of IDS are Observing and examining both user and system activities, Examining system configurations and vulnerabilities., Assessing system and file integrity, Ability to recognize patterns typical of attacks, Analysis of abnormal activity patterns, Tracking user policy violations [7].The IDS is majorly classified into two types such as Host-based intrusion detection systems (HIDS) and Network-based intrusion detection systems (NIDS). HIDS are IDSs that operate on a single workstation. It monitors traffic on its host machine by utilizing the resources of its host to detect attacks [8].NIDS are IDSs that operate as stand-alone devices on a network. NIDS monitors traffic on the network to detect attacks such as denial of service attacks; port scans or even attempts to crack into computers by monitoring network traffic [8].To detect unknown or zero-day attacks by using anomaly based IDS tool [5] even if system is not updated [6]. That can detect occurrence of malicious as compared to the normal system behavior [9]. ANN is similar to work as biological neuron in human mind. ANN made of interconnected group of different layer that produce artificial neuron [3].Artificial neural network can be used for intrusion detection system to generalize data and to be able to categorize data as being normal or intrusive [4]. Support Vector Machines (SVM) can be used for supervised learning with associated learning approach that analysis data patterns that work for classification and regression analysis of both linear and nonlinear data. SVM is useful to finding of intrusions even with the availability of less sample data [9].Fuzzy logic is approach of uncertainty, approximation, probabilistic reasoning rather than precise value [9]. Dickerson and Dickerson [2] introduced a fuzzy logic technique to identify the occurrence of any malicious. Proposed technique is called FIRE (Fuzzy Intrusion Recognition Engine). To find the similarities or relationship between object used association rules. This association rules can be used to discover the variants of well-known attacks, misuse detection and generation of signatures for known attack [9]. Wei Li [1] suggest that used genetic algorithm for categorize the network activities as intrusive or simple for network connection

Intrusion Detection Tools:

I) Snort

Snort is open source network intrusion prevention and detection system (IDS/IPS).It combines the benefits of signature, protocol, and anomaly-based inspection. It is used Libpcap library to capture packets. Snort is lightweight cross-platform network sniffing. Snort engine allowed a single rule to be applied to any variation of a protocol.

Snort is capable of performing real-time traffic analysis, packet logging, alerting and blocking on IP networks. It performs protocol analysis, content searching, and content matching. Snort can also be used to detect probes or attacks, operating system

fingerprinting attempts, common gateway interface (CGI) attacks, buffer overflows, server message block (SMB) probes, and stealth port scans.

ii). Bro:

Bro is an anomaly based IDS, provides a real time network or clean traffic analysis that match the taken packets with desired rules applied by the user. It is a passive, open-source and UNIX based Network Intrusion Detection System (NIDS) that monitors network traffic looking for doubtful activity. Bro has gained its reputation due to its Stateful Protocol Analysis capabilities. Bro has its own specialized policy language and it can be instructed to either generate a log entry, alert the operator in real-time, execute an operating system command. The main goal of Bro is to target high speed, high- volume intrusion detection.

The Key benefits of Bro IDS are permitting it to measures from the desires of smaller institutions to those of the biggest research universities. Bro is employed as a cluster set of conditions that uses three kinds of methods: Manager, Worker, and Proxy.

iii). NFR (Network Flight Recorder):

NFR is an IDS (Intrusion Detection System) that gives the users a powerful tool for the war against illegal access to your network. With the flexibility of this tool, network managers can feel a little better about who is accessing their network and where their employees are going. Through the NFR you will store, retrieve, or archived the records to outside drives [11] as well. However, this doesn't take away the requirement expert to first analyze and categorize assault situations and system vulnerabilities, and hand-code the analogous rules. NFR uses N-Code that was released to allow the users the flexibility to configure the IDA for their configuration. NFR is a program able traffic Analysis/intrusion detection engine that can be instantly updated when a new attack is discovered. Prowler requires that the vendor send out either an executable from ISS or a signature from Axent. With NFR a user can write their own request order and install it. NFR gives the users a chance to customize the IDA to their needs.

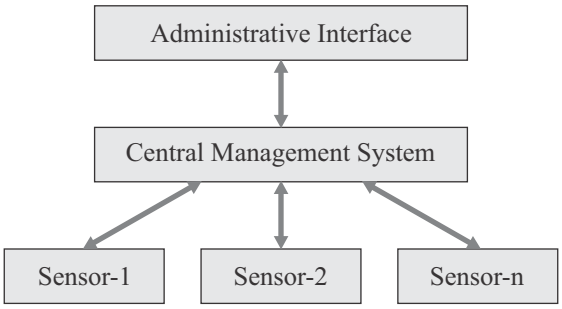

Figure: NFR 3- Tier Architecture [10]

The NFR Sentivist product operates in a three-tier environment, consisting of the sensors, a Central Management System (CMS), and an Administrative Interface (AI). The Sentivist sensors are passive devices that collect data on the wire. The collection point

IDS TOOL Features	SNORT	SURICATA	BRO	NFR	EMERALD	ACARM-ng
DEVELOPER	Sourcefire, Inc.	Open information security Foundation	Centrax corporation	Check point ,Inc.	SRI International	Wrocław Centre for Networking and Supercomputing
AUTHOR	Martin Roesch	OSIF community and supporting vendors	Vern Paxson	Marcus J.Ranum	Dr. Peter Neumann & Phillip Porras.	Bartłomiej Balcerek, Bartosz Szurgot, Wojciech Waga,Mariusz Uchroński
AVAILABILITY	Since 1998	Since 2009	Since 1998	Since 1999	Since 1997	Since 2011
FREEWARE / COMMERCIAL	Freeware	Freeware	Freeware	Commercial	Commercial	Freeware
LANGUAGE	C	C	C++	N-code	D.3.3	C++ and Python
LICENSE	GPLv2+ and commercial	GNU General Public License	GNU General Public License	NFR license	SRI International License	GPLv2
DETECTION TECHNIQUES	NIDS	NIDS	NIDS	HIDS/NIDS	HIDS	HIDS/NIDS
PLATFORMS	Signature	Signature	Signature and Anomaly	Signature and Anomaly	Signature and Anomaly	Signature and Anomaly
PROTOCOLS	Cross-platform	Cross-platform	FreeBSD, Linux, Mac OS X,Solaris	Redhat,Linux	MS windows , Unix	linux
ARCHITECTURE	TCP/IP			TCP/IP	TCP/IP	
THREADING	Single Layer	Multi Layer	Layered	Multi Layer and Distributed	distributed and hierarchically layered	Multi core and plug-in based
PACKET INCSPEC TION	Single thread	Multithread	Single thread	Single thread	Single thread	Multithread
DETECTION ENGIENE	COMPLETE PACKET	COMPLETE PACKET	COMPLETE PACKET	COMPLETE PACKET	COMPLETE PACKET	COMPLETE PACKET
SCALABILTY	Rule-based	Rule-based	Event -based	Rule-based	Rule-based	correlation-based
FLEXIBILTY	Yes (not much)	yes	Yes (not much)	yes	yes	yes
THROUGHPUT	Yes (not much)	yes	Yes (not much)	yes	yes	yes
SPEED	moderate	maximum	maximum	moderate	moderate	maximum
INSTALLATION/ DEPLOYMENT	moderate	maximum	maximum	moderate	moderate	moderate
IPS CAPABILITY	Easy	Intermediate	difficult	Easy	Easy	Easy
ALERT GENERATION	yes	yes	no	no	no	yes
TRAFFIC ANALYSIS	Real time	Real time	Real time	Real time	Real time	Real time

or Central Management System provides a single collection/aggregation point for data collected by the sensors. The data spooled on the sensors are pushed into a proprietary data file store located on the CMS. The AI is a Windows 32 program that provides a GUI interface to the alerts, forensics, and controls of the Sentivist environment. All management of the IDS environment can be done via the AI.

iv). Emerald

Emerald provides a rare example of distributed IDS offering both signature and anomaly based detection, and also real-time response. A research project, Emerald was targeted for a large enterprise network with thousands of users connected in an association of independent administrative realms. Each realm offers local and network services that provide an interface for requests from individuals internal and external to the realm. But defining a single security policy over such an enterprise, let alone a single point of authority, is often not practical [11,14]. Most of current security approaches are difficult to be applied to large networks. A fully distributed architecture could be applied to a large network with some tradeoffs
.
The objective of the EMERALD work is to bring a collection of research and prototype development efforts into the practical world, in such a way that the analysis tools for detecting and interpreting anomalies and misuses can be applied and integrated into realistic network computing environments [12, 13].

EMERALD introduces service monitors, which are dynamically deployable and highly distributed. Monitors may interact with other monitors using a subscription based scheme. These monitors can also be deployed to provide domain wide and enterprise wide analysis. EMERALD'S ability to perform inter domain analysis is vital for global attacks again an enterprise.
EMERALD's principal focus is its resource objects, attached to targets, routers or gateways, and services such as FTP or HTTP, which are frequently the subject of malicious attacks.
Its architecture consists of three main components profiler engines, signature engines, and resolver as shown in the figure 4 and is designed to permit communication with external data sources and alternative analysis platforms. Independently configurable monitors watch over the resource objects, working in conjunction when a coordinated attack is suspected.

v). ACARM-ng:

ACARM-ng is an open source IDS/IPS system. ACARM-ng is an alert correlation software which can facilitate analyses of traffic in computer networks. ACARM-ng has a modular structure you are free to implement user-specific input module to collect alerts from any possible sensor ascribed to two main categories called HIDS (Host-based Intrusion Detection System) and NIDS (Network-based Intrusion Detection system).. Correlation process aims to reduce the total number of messages that need to be viewed by a system administrator to as few as possible by merging similar events into groups representing logical pieces of malicious activity. ACARM-ng was to bring the alert correlation to a new dimension thank to its scalability and plug-in-based architecture. ACARM-ng provides core system functionalities, like logging, alerts and correlated meta-alerts passing between system parts, error recovery, multi-threading, etc..

vii).Suricata:

The Suricata Engine is an Open Source Next Generation Intrusion Detection and Prevention

Engine. This engine is not intended to just replace or emulate the existing tools in the industry, but will bring new ideas and technologies to the field. Suricata is a rule-based ID/PS engine that utilises externally developed rule sets to monitor network traffic and provide alerts to the system administrator when suspicious events occur. Designed to be compatible with existing network security components, Suricata features unified output functionality and pluggable library options to accept calls from other applications. The initial release of Suricata runs on a Linux 2.6 platform that supports inline and passive traffic monitoring configuration capable of handling multiple gigabit traffic levels. Linux 2.4 is supported with reduced configuration functionality, such as no inline option.

Available under Version 2 of the General Public License, Suricata eliminates the ID/PS engine cost concerns while providing a scalable option for the most complex network security architectures. As a multi-threaded engine, Suricata offers increased speed and efficiency in network traffic analysis. In addition to hardware acceleration (with hardware and network card limitations), the engine is built to utilize the increased processing power offered by the latest multi-core CPU chip sets. Suricata is developed for ease of implementation and accompanied by a step-by-step getting started documentation and user [1].

Conclusion:

This paper shows the various tools of intrusion detection system. Intrusion detection system is software tools that provide security and maintain flag when someone is try to capture your system on the network. In this paper, there are many parameters (show in above table) of various tools and gives the comparison among them.

References:

Wei Li 2004, ―Using Genetic Algorithm for Network Intrusion Detection‖, In Proceedings of the United States Department of Energy Cyber Security Group Training Conference, pp. 24-2

Dickerson, J.E., Dickerson, J.A. 2000, ―Fuzzy network profiling for intrusion detection‖, 19th International Conference of the North American Fuzzy Information Processing Society, pp. 301-306.

Carlos Gershenson 2003, ―Artificial Neural Networks for Beginners‖. http://arxiv.org/ftp/cs/papers/0308/0308031.pdf (Accessed 30 April 2013)

Ibrahim LM. 2010, ―Anomaly network intrusion detection system based on distributed time-delay neural network‖, Journal of Engineering Science and Technology, Vo. 5, Issue: 4, Start page: 457

[JC 2007] Jupiter media Corporation. Intrusion Detection System (2007). Available from http://www.webopedia.com/TERM/I/intrusion_detection_system.html (visitedAug. 26, 2007).

Dotan Cohen 2007, ―What is a Zero-Day Exploit?‖ http://what-is-what.com/what_is/zero_day_exploit.html (Accessed 29 April 2013)

Mudzingwa, D.; Agrawal, R. 2012, ―A study of methodologies used in intrusion detection and prevention systems (IDPS)‖, Proceedings of IEEE South east con, pp. 1-6.

What is intrusion detection? - Midmarket IT Security Definitions – Intrusion detection, http://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci295031,00.html Accessed on: 23/02/2012.

Micheal E. Whitman and Herbert J. Mattord, "Principles of Information Security" page 289-294.

International Journal of Computer Applications (0975 – 8887) Volume 109 – No. 1, January 2015 6 A Survey on Intrusion Detection Systems for Cloud Computing Environment Uttam Kumar ,Bhavesh N. Gohil

Carl Endorf, Eugene Schultz, Jim Mellander, "Intrusion detection & prevention" McGraw-Hill/Osborne, c2004.

Adaptive, Model-based Monitoring for Cyber Attack Detection Alfonso Valdes and Keith Skinner. October, 2000.

Detecting Computer and Network Misuse through the Production-Based Expert System Toolset (P-BEST) Ulf Lindqvist and Phillip A Porras. May, 1999.

Experience with EMERALD to Date Peter G. Neumann and Phillip A. Porras. April, 1999.

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances Phillip A. Porras and Peter G. Neumann. October, 1997.

The types IDS are 'signature-based IDS vs. anomaly-based IDS', 'misuse detection vs. anomaly detection', and 'passive system vs. reactive system' [JC 2007].