

A SURVEY ON INTRUSION DETECTION TECHNIQUES AND REAL TIME TRAFFIC ANALYSIS MECHANISM

Prof.Mahendra rai*

Gyanendra Haldkar*

ABSTRACT

Security has become the greatest problem within and outside the organizations. User ID, passwords and firewalls are the common steps that organizations take to secure their computers. However, these are not so effective mediums in current context of unsecure eon. Intruders and attackers are so advanced that they access the computer and manipulate it, so they cannot be traced easily. Through this contribution objective is to find out & present existing intrusion detection system (IDS) with their pros and cons that will be helpful to select the best one and provide the secure environment so that system will be protected from intrusion and attacks.

Keywords

Network Security, Intrusion Detection, Intrusion Prevention, Social Engineering Toolkit.

* SRIT jabalpur

1. INTRODUCTION

Day by day internet is growing and reached to everyone affects on many. People's dependencies are also increased with this. Most of our transaction are now shifted to the internet, thus it is also become a soft area for various types of security threats and attracts various types of attackers whose objective can be data stealing or data diddling, sniffing, password cracking or any other form of misuse of unauthorized data. So IDS can be the best solution for the above problem.

“Intrusion detection system plays a very crucial role in security of organization's information and data. It is a system that checks systems and network traffic and inspects that attacks originating from inside or outside the organization”.[1].

These are the some selecting criteria of IDS

- Objective/Aim Identification (Perform a risk/attack evaluation).
- General Overview of available IDS.
- Define the need of IDS precisely.
- List out the IDS according to need or Purpose.
- Cost Expense (Benefit) Analysis & Selection of IDS.
- Decide Working & Policy (Implementation).

2. EXPLORATORY STUDY ON EXISTING IDS

Based on the study of various research contributions [2] [3] [4] [5], it has been found that around hundred IDS are available. Through this table some popular ones are presented here:

Table 1. Currently Available IDS: At a Glance

AnaDisk	AuditTrack for Netware	Authd
AIDE (Advanced Intrusion Detection Environment)	AppShield	BlackICE Defender
Bro	bv-LifeLine	Check Point RealSecure
Cisco Secure IDS	Clog	CMD5 Computer Misuse Detection System
CRCMD5 Data Validation Tool	CyberCop Monitor NT	CyberCop Monitor Solaris
CyberCop Scanner	CyberCop Sting	DesktopSentry
Detect IT	DiskSearch	Dragon Sensor
eTrust Internet Defense	Extercept	Exodus Cyber Attack Management Service
Firewall Reporting Suite	FireStorm	ForensicToolkit
Gabriel	HP Openview Node Sentry	HP-Tcpdump
ICEcap	ICEpac	iD2 Secure Transport
Ifstatus	Incident Manager	IP-Watcher
ISensor Intrusion Prevention	Kane Security Monitor	KaVaDo InterDo
Klaxon	LSOF	Lucent RealSecure

Each IDS has specific design goals and objectives, thus having some specific/unique as well as some common features. From above listed IDSs, some well-known IDSs used by the organizations and now become de-facto standard as well, described here in brief with their features:

Man Hunt	NetDetector	NetIQ Corp. Security Manager
Netlog	Network Flight Recorder	NetProwler
neuSecure	OSSEC HIDS	OnlineGuardian
Patriot IDS	Prelude Hybrid IDS	Peek & Spy
QRadar	RealSecure	Reactive IDS
Red Sire, 1 st Watch Managed IDS	Review	SafeBack
Samhain	Security Management Pack for MOM 2000	Security Manager
Sentry	Shadow	SilentRunner
SMARTWatch	Snort	Strata Guard
StealthWatch	Suricata	Tcpdump
Tcp_wrappers	Tklogger	Tocsin
Tripwire	T-sight	TTY-Watcher
TurnKey Network Appliance	Vanguard Enforcer	Verizon Federal Network System NetFacade
ViewDisk	Vigient Security Agents	WinSNORT

These well-known IDSs with their conclusive highlights are as follows:

2.1 Bro

It is an anomaly based IDS, provides a real time network or pure traffic analysis that match the captured packets with desired rules applied by the user. It is used to analyze extensive logging functions related to application level details and to recording every connection observed on the wires. [6] model or patterns in N-code for misuse detection. Due to the manual and ad hoc nature of the development process, NFR has low extensibility and adaptability. [10]

Highlights of the NFR are as follows:

- It provides built-in means for customization and extension.
- It is determined language, i.e., flexible and portable language for traffic exploration.
- It doesn't obstruct with network activity
- Having dynamic alerting function.

Highlights of Bro are as follows:

- Open-source.
- Specifically timely for scientific environments.
- Very useful in servers with default policies.
- Powerful on traded hardware.

- Intrusion prevention schemes are also supported.

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

2.2 Snort

Snort has become the de-facto accepted for signature-based network IDS. It is based on the Libpcap library to capture packets. Snort is lightweight cross-platform network sniffing tool; it's evolved into a strong and full-featured IDPS. Snort engine allowed a single rule to be applied to any variation of a protocol. [7]

Some features of Snort are as follows:

It works on UNIX based systems and is available in source code form. As it was previously available open source but now under proprietary license.

NFR is a multiuse network monitoring implement, operational for intrusion detection, usage exploration, and troubleshooting by system administrators. The construed N-code language allows a user to write randomly complex scripts for examining incoming packets, in which NFR engine provide timing constrains to limit packets which helps to share system resources properly.

NFR comprises of a sum of modules, all responsible for a specific activity: packet suckers, a decision engine, back ends and a query interface. [11]

2.3 Suricata

An open source, high performance recent signature based network IDPS and Security Monitoring System for UNIX and Window based systems. It use PCAP recorder to log the traffic and provides offline analysis facility of PCAP files.

[7][12]

- Can work on any operating system. - Protocol examining capability. - Supports all operating system.
- Condition examining capability. - Along with the IPS.
- Packet reassembly capability. - Lots of serving GUI's are available for analyzing the results. Automatic detection performance.
- Network Security Monitoring (NSM).
- Filtering of alerts and events.
- Output format support many other tools to analyze data.

Snort is configured using command line switches and optional Berkeley Packet Filter commands. Snort rules can be easily written by normal users, but powerful enough to detect a wide variety of hostile or merely suspicious network traffic. There are three basic actions that Snort can trigger when a packet matches a specified rule pattern: log, alert, or pass. [8]

2.4 NFR

Network Flight Recorder (NFR) gives the users a powerful tool to get the illegal attack in networks. With the efficiency of this tool, network administrator can know better about who is using or accessing their network and what their workers are doing. It is stand-alone configuration; a single NFR station gathers and stores information in a single instance.

Analysis in NFR is developed by script based language known as N-code, it uses web based interface to display the result with the use of java language. By its feature of not to interfere in network activity, this helps to analyze the standard or to free data from unwanted errors. Through the NFR one can store, retrieve, or archived the information to external drives [9] as well. However, this doesn't eliminate the requirement specialist to first analyze and categorize attack situations and system vulnerabilities, and hand-code the analogous rule.

Having functionality of automatic detection of protocols on any port is very useful which helps to

determine the malware and attacks. Another progress in the Suricata engine is to employ native multi-threaded actions, something more necessary as network bandwidth increases. Suricata is planned from the start to take improvement of operating with multiple CPUs. A multi-threaded discovery engine can make intelligent results on how to fragment processing and can match signature detection between these threads all within the same detection engine. [13]

2.5 Dragon Squire

The Dragon IDS products come across the experiments of inspecting over a modern network by providing high speed sensors to sense suspicious activity, allowed data to decide the impact of network attacks and scalability to set up and able to huge numbers of sensors, lacking negatively impacting the task of large networks. [14][15] Dragon Squire is a host-based intrusion detection and firewall monitoring system that express at system logs for proof of malicious or suspicious submission activity, and monitors key system files for proof of damaging in real time. Dragon Squire has been tuned to prevent high load levels and minimize any negative system impact to a server's performance. Besides being an excellent system security tool, it also examines firewall logs, router actions and just about everything that can communicate SNMP or SYSLOG.

Some features of Dragon Squire are as follows:

- Ease of use because of single interface.
- Host & network based versions.
- Clever to work over high-speed networks without dropping packets.
- Able to replay stored attacks for post-mortem and forensic analysis.
- Strong reporting capabilities.
- It has the ability to detect evasive IDS Techniques.

- GUI / command line alternative if preferred.
- Capability of secure remote administration.

The Dragon Squire's signature archive contains suspicious events from a comprehensive range of operating systems.

These actions check for guarding file transfers, failed login attempts, physical messages and system reboots. The library contains security messages such as Secure Shell, Qmail, Send mail and Apache Web servers.

It is used to observe network packets for proof of hacker and malicious worker activity by monitoring their system logs and firewall logs. It analyzes the system logs for proof of malicious or suspicious application programs in real time. It also observes main system records for evidence of tampering. Being a tremendous system security tool, it can examine firewall logs, router events and reasonable about everything that can start SNMP or SYSLOG.

Dragon Squire has been engineered to have a slight influence on the servers it is protecting. It is also a superb supplement to the Dragon Sensor Network IDS.

3. ANALYSIS OF EXPERIMENTAL SCENARIO

For experimental purpose a popular IDS, SNORT tool has been selected. Two hosts primarily connected to a LAN has been used, one become a victim machine and another becomes an attacker machine. SNORT, is installed on victim machine having Windows 8 and Intel's X86-based PC (64-bits i5-2430M CPU@2.4GHz Processor with 2 GB RAM) configuration. Dummy attacker's machine having the same hardware configuration with BackTrack 5 R2 (a flavor of Linux) operating system [16]. All recorded data is contained in a local snort log file. The experiment was done to identify particular attacks and some packets. The traffic speed was low. With the use of Wireshark Packet Analyzer [17] the packets has been analyzed.

The three types of intrusions has been evaluated an examined for experimental purposes at here:

- Attempt by a program to access the network resources.
- Denial-of-service (e.g., Ping-of-death).
- Unauthorized access from a remote machine (using Social Engineer Toolkit-SET [18]).

4. EXPERIMENT RESULTS

The generated log files are used to save the captured packets.

The snort log file should be converted to “.csv” format for analysis in Wireshark. The log file of snort contains the following information, No., time, Source, Destination, Protocol, length, & Info. Wireshark uses color coding to differentiate the packets received.

4.1 Unauthorized Access by a Program to the Network Resources

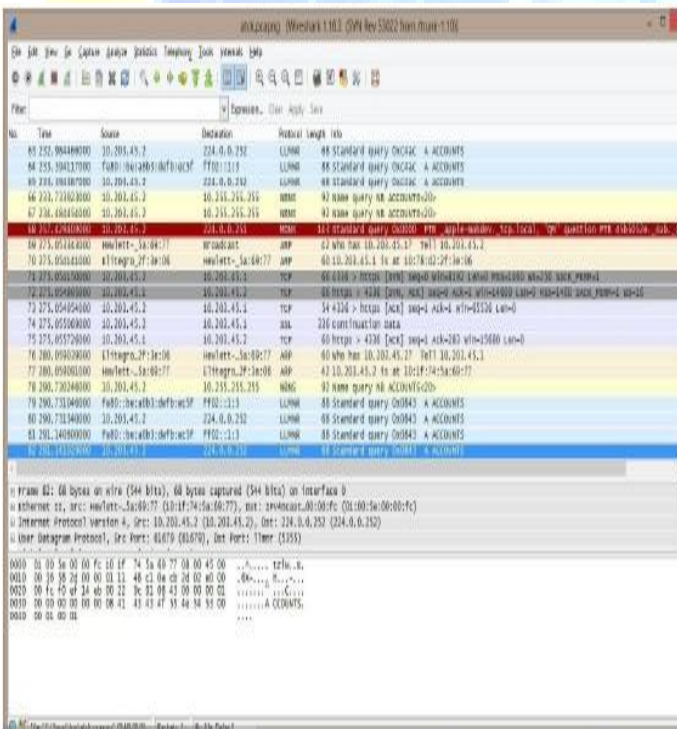


Fig 1: Attempt by a program to access the network resources

Figure 1 shows the detail view of packets that are not trusted by the machine as the valid traffic in the network. Here a packet from the machine having IP address 10.203.45.2 from an unknown location in the network to the machine having IP address 224.0.0.251 is an illegal traffic.

The experiment shows how to configure SNORT and WireShark on Windows 8 machines. It is better to install Win Snort in place of Snort because it provides a GUI for better user interaction. The ReverseTCP successfully led the attacker to gain access to

the system. It should have shown an alarm like a warning message on cmdmad-line, with the details like the port number and type of protocol that is used to access the system, the destination and source IP addresses, with a particular color coding.

5. CONCLUSION

There are many Open source IDS available for use, but Snort is the best alternative system to ensure network security. It is non GUI interface, takes time to get familiar. Through this paper we are analysing, a detailed study on IDS has been performed and a popular IDS Snort has been implemented and configured on Windows-based environment. Snort was only used to capture the packets and WireShark analysis showed the illegal packets. Only detecting the attacks will not work, Snort should trigger some action that alerts the user about the attack. The GUI available for Snort should be comfortable for native users for configuration and running.

6. REFERENCES

- [1] Fagg, C.R. 2001. Intrusion Detection Systems: Definition, Need and Challenges. White Paper. SANS Institute InfoSec Reading Room.
- [2] Axelsson, S. March 2000. Intrusion Detection Systems: A Survey and Taxonomy. Technical Report. Chalmers University, Sweden. IJCA TM : www.ijcaonline.org
- [3] Sobirey, M. November 1999. Michael Sobirey's Intrusion Detection Systems page. <http://www-rnks.informatik.tu-cottbus.de/~sobirey/ids.html>.
- [4] Timberline Technologies LLC. Alphabetical List of Intrusion Detection Products. <http://www.timberlinetechnologies.com/products/intrusiondtct.html>, [Last Updated 2009].
- [5] Boyce, C.A.P. and Zincir-Heywood, A.N. October 2003. A Comparison of Four Intrusion Detection Systems for Secure E-Business. In Proceedings of the 6th International Conference on Electronic Commerce Research (ICECR03), ATSM, IFIP, Dallas, USA.
- [6] Varadarajan, G.K. October 2012. Web application attack analysis using bro ids. White Paper. SANS Institute InfoSec Reading Room.
- [7] White, J.S. Fitzsimmons, T. and Matthews J. Quantitative Analysis of Intrusion Detection Systems: Snort and Suricata. In Proceedings of the SPIE, Cyber Sensing 2012

[8] Roesch, M. 1997. Snort – Lightweight Intrusion Detection for Networks. In Proceedings of the USENIX LISA'99 USA. November 1999.

[9] Inc. Network Flight Recorder. <http://www.nfr.com>, 1997

[10] Lee, W. Park, C. and Stolfo, S. 1999. Automated Intrusion Detection using NFR: Methods and Experiences. USENIX Intrusion Detection Workshop. California, USA.

[11] Undy, M. and Antonelli, C.J. 1998. Sifting the Network: Performing Packet Triage with NFR. CITI Technical Report 98-6. Center for Information Technology Integration, University of Michigan, USA.

[12] <http://suricata-ids.org/features/all-features> [last visited: 02/12/2013]

[13] Albin, E. 2011. A Comparative analysis of the Snort and Suricata Intrusion Detection Systems. Master's Thesis, Naval Postgraduate School, Monterey, California, USA.

[14] Neumann, P. G. 1990. A Comparative Anatomy of Computer System/Network Anomaly Detection Systems, CSL, SRI BN-168, Menlo Park, CA, USA.

[15] Enterasys Networks. http://www.voxtechnologies.com/enterasys_files/pdf/overview-datasheet.pdf [last visited: 04/12/2013]

[16] BackTrack Linux. Available at: <http://www.backtrack-linux.org>

[17] Wire Shark Packet Analyzer. Available at: <http://www.wireshark.org>

[18] Social-Engineer Toolkit (SET).
<https://www.trustedsec.com/> Available at: