Development of a Hybrid Intrusion Detection System for Security Analysis at the IP Layer

Arphaxad Kioko Muia

Department of computing and IT, Jomo Kenyatta University of Agriculture and Technology, Box 62000-00200-Nairobi-Kenya

Abstract: ***Around us are Computer networks that necessitate effective communication, sharing of knowledge, research and development, education modernization, e-commerce and entertainment just to mention a few. The present days' network systems are increasingly getting exposed to many security threats and vulnerabilities including: denial of service (DoS), scanning, password cracking, spoofing, eavesdropping, spamming, phishing, worms among others. These security threats and vulnerabilities have seen organizations and companies implement security policies for their networks. However, most of these security policies only inspect the network traffic passing through them denying or permitting packets passage based on their active set of rules. This ideally leaves the network exposed to attacks from outside and within. This paper presents technical evaluation methods for network security at the IP layer. This will be done through experiments on network traffic data. This will involve Network analyzers for collecting data from 15 entry points having a population of about 160 computers that will be processed by the various methods. To demonstrate the results, Network traffic graphs and figures will be used. Through Observations, analysis of the effects of certain behaviors will be done. This results will help in designing a method that's would simplify network security analysis at the IP Layer, in this case a hybrid method. The technical evaluation mainly focuses on deployment in real high speed networks. The method designed shall then be tested in a government ICT department network***.

Keywords: Netflow data, Computer Networks, Intrusion Detection, Visualization, Collectors, Anomaly detection, Agents, Security analysis

1. Introduction

The most important issue that is to be given greatest consideration is the security of an environment. Be it a single host or a LAN or any complex environment like Grid or Cloud attacks are always there. It can be attacks on a single host, port scans to check vulnerabilities, flooding attacks, denial of service etc. All these attacks have severe consequences in an environment. Therefore it is good to identify these attacks at any early stage itself, so that the attacker can be blocked and avoid further effects. This is possible by an intrusion detection system (ids), which can identify the intrusions before attack can take place and can give a notification that it is possible to have an attack Most of the ids identify attacks at an early stage itself. There are several open source ids present. Some of them are Snort, Bro, and Suricata etc. They are very strong and efficient in identifying attacks. Most of them identify pre-defined attacks. These kind of intrusion detection systems are called as Signature based Intrusion Detection Systems. Signature based ids have a set of rules. The incoming packets are compared with the set of rules. If any of the packets matches with the set of rules, actions specified in the corresponding rules are performed. Therefore by writing a wide variety of rules one can detect any attack with these kind of intrusion detection systems.The evaluation of each technique used in detection is done considering the its coverage, effectiveness, performance, applicability for different types of data acquisition and ability of intrusion detection in encrypted traffic. TCP/IP as the foundation of the internet and it's a collection of various communication protocols operating over the internet supporting most of the services running over the network. The Protocol provides an end to end connectivity by establishing, maintaining and releasing connections between the two communicating sides [1].The paper is sturctured in the following manner; section 2 describes the literature review, section 3 brings forth Methodology of the proposed system, section 4 presents the results from our method and section 5 is the conclusion and future work.

2. Literature Review

Techniques for network traffic acquisition-a key area in network security analysis will also be highlighted. Thereafter, a review on intrusion prevention, detection and the techniques thereof in network security analysis will be done highlighting on their strengths and weaknesses. The description and evaluation of each technique shall be according to coverage, effectiveness, performance, applicability for different types of data acquisition and ability of intrusion detection in encrypted traffic.TCP/IP as the foundation of the internet and it's a collection of various communication protocols operating over the internet supporting most of the services running over the network. The Protocol provides an end to end connectivity by establishing, maintaining and releasing connections between the two communicating sides [1].

a) Flow-Based Traffic- Many Intrusion Detection Systems (IDSs) or Intrusion Prevention Systems (IPSs) have classic approach to data collection, where they capture all network packets that pass through the system. This function however is performed by many routers and monitoring probes which still perform a flow-based data collection, using the Net-Flow format: Net Flow - A flow is a unidirectional sequence of packets with some common properties that pass through a network device. These flows can be collected and exported to an external device called a NetFlow collector. IPFIX - unified protocols and applications that require flow-based IP traffic measurements. For instance RFC 3917 defines the requirements for exporting traffic flow information out of routers, firewalls, proxies, load balancers and NATs.

b) **Intrusion Prevention System**(IPS) - software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. An intrusion prevention system (IPS) is a reactive system in which the IDSs are tightly coupled with firewalls. The IPS mainly forms part of the communication link and their main task is to mitigate the detected attack. IPS can be divided into three classes: host-based (HIPS), network-based and distributed IPS [2].
c) **Intrusion Detection System**–Intrusion detection is the process of monitoring and analyzing data and events occurring in a computer and/or in a network system in order to detect attacks, vulnerabilities and other security problems [3]. Typically, IDS happens to be used as a security control or countermeasure to monitor, identify, and inform any unauthorized use, abuse, or misuse of knowledge systems or network assets [16].
d) **Signature-based Detection** - is very effective in detecting known threats, but largely ineffective in detecting threats unknown previously, threats disguised by the use of evasion techniques, and many variants of unknown threats [4].
e) **Deep Packet Inspection**: This is also called Stateful Protocol Analysis approach in intrusion detection and it is the analysis that operates mainly on the higher layers of the TCP/IP network model. For the sake of our completeness and comparison, this method is considered it for this discussion. The method compares predetermined profiles of generally accepted definition of benign protocol activity for each protocol state against observed events to identify deviations. It relies on vendor-developed universal profiles that specify how particular protocols should and should not be used. That means that the IDS is capable of understanding and tracking the state of network, transport, and application protocols that have a notion of state [2].
f) **Anomaly-based Detection**: [5] defines Anomaly-based Detection as the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations.Cooperative Adaptive Mechanism for Network Protection (CAMNEP). CAMNEP is an agent-based network IDS [6]. It is a combination of a few methods that are described above, it then creates a whole system.

3. Methodology

The NIDSs being deployed in this approach are passive, hence "invisible" to attackers. On the contrary, HIDSs rely on processes that are running in the operating system of the host. The deployment, testing and possible upgrade of IDS are greatly considered.

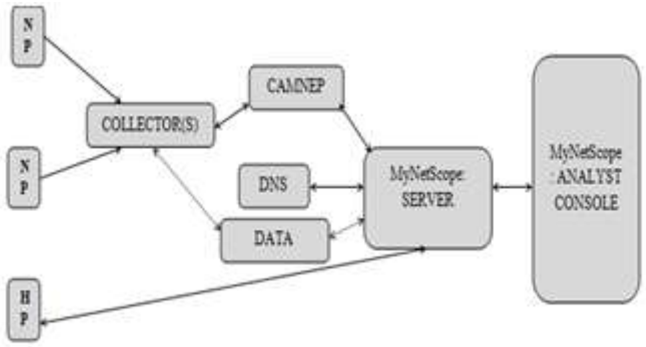


Figure 1: Conceptual framework

In a general sense, it is easier to update one component of NIDS than many components of HIDS on hosts. The proposed solution consists of several components and layers including as shown in Figure 1 above:-

Network Probes - The bottom layer of our system is created by probes. The network traffic is acquired by the probes which then serves the collectors with the captured data.

Collectors- NetFlow Collectors receive, and store NetFlow data that are exported by the network probes. We use the existing tools and wide-spread software that are well tested to carry out the deployment and NetFlow analysis. We shall mainly rely on *nfdump*and *NfSen* toolsets. Our collectors not only receive and store NetFlow records but also perform some preprocessing tasks such as periodic executions of scripts that monitor policy violation. **MyNetScope and Data Sources** - This layer requires data from collectors and other sources for its operation. However, we shall describe the core of our intrusion detection system. MyNetScope platform shall be employed. **MyNetScope Server -** This server reads NetFlow records from collectors, performs some preprocessing tasks on the flows and replies to the analyst's queries that are submitted by client application (analyst console). Again, the entire communication between all parts is encrypted. We shall apply SSH tunnels.

CAMNEP - Part of the CAMNEP principle is deployed as the "brain" of our intrusion detection system. This principle is as well integrated with the DNS. MyNetScope itself does not perform intrusion detection. However, it is a very useful visualization tool that meets our requirements including Accuracy, Detection of novel threats, operating in high-speed Networks, early detection and anomaly detection in encrypted traffic. Its power is in integration of external data sources.

Analyst console - This is responsible for querying through client application on the NetFlow and communication amongst various clients or network nodes.

Deployment and analysis of the Proposed IDS

The system is deployed and tested in a large network of an ICT unit connected to the Government of Kenya's Common Core Network. The detailed system deployment status shall be described. The description is structured accordingly and commensurate to our objectives. Eventually a use case shall be outlined and compared with the security analysis performed by the classic approach with the help of the designed system.

The key considerations in the IDS design includes;accuracy, detection of novel threats, operating in high-speed networks, early detection, long-term data storage, ipv6 support, scalability, easy to maintain, transparency, security robustness, anomaly detection in encrypted traffic, user-friendly interfaces and well-arranged visualization

a) Network Probes

Probing is a class of attacks where an attacker scans a network to gather information or find known vulnerabilities. An attacker with a map of machines and services that are available on a network can use the information to look for exploits. There are different types of probes: some of them abuse the computer's legitimate features; some of them use social engineering techniques. This class of attacks is the most commonly heard and requires very little technical expertise. Different types of probe attacks that were deployed are as illustrated in Table 1 below.

Table 1: Types of probe attacks

Attack Type	Service	Mechanism	Effect of the attack
Ipsweep	Icmp	Abuse of feature	Identifies active machines
Mscan	Many	Abuse of feature	Looks for known vulnerabilities
Nmap	Many	Abuse of feature	Identifies active ports on a machine
Saint	Many	Abuse of feature	Looks for known vulnerabilities
Satan	Many	Abuse of feature	Looks for known vulnerabilities

Network Probes create the bottom layer of our system. They acquire network traffic and serve collectors with captured data. In this section we discuss probe features and probe deployment in our administered network.

Data acquisition:Network probes monitor the link and export captured data in the Net-Flow format. In our proposed system, we decided that the Net-Flow format meets the requirement on operating in multi-gigabit networks. However, we rejected the use of SNMP counters and packet traces. The reason for our decision was that the Net-Flow format gives coarse-grained data whilst SNMP is a bit difficult to deal with at least for our system. It is practically infeasible to capture and store packet at wire speed even with specialized hardware.

Our emphasis was that we did not want to entirely rely on NetFlow data that was exported by some Cisco routers that may have existed in the network that we were presently investigating. Actually, our measurements revealed that Cisco's routers did not export NetFlow correctly in all circumstances. Ideally, [7] explains that the main task of the router is to route network traffic and nothing else. As a matter of fact therefore, we must take into account that NetFlow export is an additional feature. Consequently, the NetFlow data from the routers were used as supplemental data source for our system.

Pointedly, our concern was the possibility of distortion of the acquired data. It was then decided that for this reason we rather avoided the packet sampling. This study's decision was supported by [10] – "Impact of Packet Sampling on Anomaly Detection Metrics",).

For the purpose of this research, the use of probes based on COST (commercial off-the-shelf) was deployed for the computers because of their cost recommended. In fact, there existed two alternatives of network interface cards (NIC) that are usually used in the probes. The earlier ones utilize common NIC (such as Intel) and the latter rely on the COMBO technology developed in the Liberouter project. The software probes that capture network traffic by NIC (such as nprobe) is not sufficiently efficient.

We had to desirably consider the "One-way Throughput Test - 20070715-F-0001 by [11]. In this, deployment of Flow-Mon was made, this actually a hardware-accelerated passive network monitoring probe. Generally, the software probes are satisfactory for small networks, the hardware-accelerated probes for large, multi-gigabit networks. Both types of probes meet the requirement on transparency since they are "invisible" at the IP layer. There is no IP address assigned to the interface performing packet capturing. Thanks to the use of NetFlow version 9, it supports IPv6.

Location: the main function of a network probe is to monitor traffic passing through a certain node of the network being investigated. For this reason therefore, the location of the network probe determines what is monitored. This is of great importance because the proposed system is based on data provided by network probes. Preferably, each packet that ingresses or egresses the administered network should pass through the place where the probe is located. Discussions with network administrators of the ICT department of government network were carried. Identification was then reached that the probes should be located "in the neighborhood" of the edge router considering the network traffic from/to the Internet. Figure...shows the location of the main probe. Actually, a choice was made between the two alternatives. Supposedly, the assumption was that the edge router acts as a firewall too. In case the probe was to be placed in front of the router/firewall, then the traffic that would not enter the administered network would also be monitored. However, the second alternative was chosen. The main probe was located in the administered network, behind the router/firewall. This ensured that the probe "see" only the traffic that passed through the firewall. The firewall usually implements (a part of) the security policy of the organization.

From the informed discussions above, the probe will not be inserted into the network link, but only a network tap. This was because it was a hardware device which provides a way to access the data flowing across a computer network. As a consequence, delegation of the responsibility for the continuous operating to the tap was actually made. If a consideration to use the tap that requires power supply was to be realized, then it had to be connected to the uninterruptible power supply (UPS) so that there is a continuous power supply to the probe and related devices. At the same time our consideration was that we had/should choose tap with dual power supply unit in case of failure. The main probe is capable to capture only the attacks that originate from or are destined for outside the network. In cases of attacks emanating from insiders, we propose that other probes inside our network to be deployed, especially in front of/behind the firewalls that protect particular network segments. From this, we can then reveal possible malicious activities of hosts in the administered investigation network.

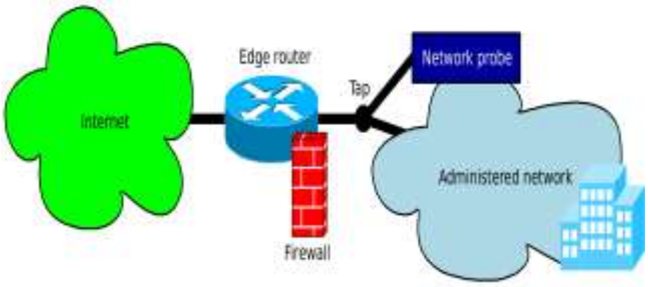


Figure 2: Domain view of VisFlowConnect-IP

For instance, the Figure below depicts deployment of one main probe and three other probes inside the administered network. This is an essential demand in an organization or corporate networks. There is one segment consisting of more sensitive servers than the others or the organization is large enough to monitor network traffic inside the organization.

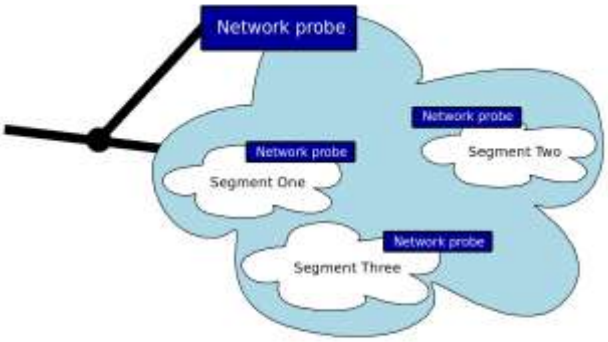


Figure 3: Probes inside the network

Honeypots: Beside the NetFlow probes, the deployment of Honeypots to complement the probes functionality were used. In fact, this is an information system resource whose value lies in unauthorized or illicit use of that resource. Accordingly, a low-interaction honeypot was chosen because passive performance rather than active detectionwas to be realized [12]. The output of a honey pot should be a list of hosts (from outside and even inside the network) that try to communicate with imaginary hosts in the administered network. Typically, reserved for this were several unassigned IP addresses (almost the whole subnet) for the Honeypot. The major objective for this was that, if it was to observe a connection attempt to such address, it logs the host that originated the connection. However, premature conclusions ought to be avoided. For example, by considering a user who types an incorrect IP address, misconfigured host and so on.

Security: Security robustness is extremely significant for such devices as network probes. The probe itself is controlled via management interface. A secure channel (namely SSH) was used. In this case the access is granted only from specified IP addresses. In case study, deployment of identity management system called a Remote Authentication Dial In User Service (RADIUS) was employed [13]. RADIUS is advantageous to distributed systems in that it eliminates synchronization issues. Last, but not least, NTP was used to synchronize the clocks of computers over a network. Since the probes timestamp flows using the host time it was necessary to set the precise time.

Maintenance and Management: Generally, the probes are easy to maintain devices. If they are in fact placed in the network and set up, they will work and fulfill their task. However, if they do not send any data to the collector, determination cannot be made whether the monitored link or the probe fails. Hence, NETCONF Configuration Protocol is employed over SSH to monitor a probe status [14].

b) Collectors

A NetFlow collector is responsible for correct reception and storing NetFlow data that are exported by network probes. To prevent reinventing the wheel, the existing tools were used as well as software that is well tested and wide-spread. In the case of NetFlow collectors, nfdump and NfSen toolsets were relied upon [15]. Our collectors receive and store NetFlow records but also perform some preprocessing tasks such as periodically execution of scripts that monitor policy violation. Collectors comply with requirements described above as well as other parts of the proposed IDS.

Security: To meet security requirements, IP addresses specification of probes that are authorized to send the NetFlow data to the particular collector were made. Notice that the collector itself does not restrict the reception of NetFlow records. It can be considered to be a security threat since the NetFlow records are transmitted in UDP packets that can be easily forged. In cases where NetFlow records via the same network cannot be transmited, the collectors can be connected directly to the probes through local network and thus considerably intensify the security. In addition, this could lighten the loaded network links.

Long-term data storage: while NetFlow records are already aggregated (in terms of network flows), they occupy relatively a lot of disk space. For example, the records that cover one month of network traffic of large government ICT department network occupy about 240GB of disk space. If more probes cannot be deployed, then only one collector could be utilized. Nevertheless, long-term data storage requires enough space on disk drives.

NFDUMP Collectors - a group of cooperating independent programs (according to "do one thing and do it well" philosophy) to collect and process IP flow data received from exporting devices. NFDUMP tools currently support sFlow and NetFlow version 5, 7 and 9 protocols.Figure 4.3 below represents a Scheme of collecting and processing flow data by NFDUMP tools

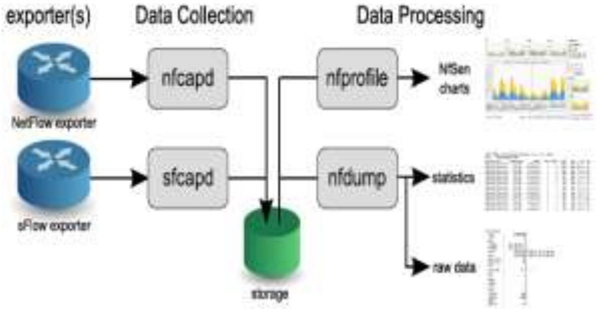


Figure 4: Scheme of collecting and processing flow data by NFDUMP tools

nfcapd (1) - The nfcapd is one of two main backend programs. nfcapd(1) is used to capture incoming NetFlow data, process them and store flow information to the NFDUMP files. These files are automatically rotated and renamed after specified amount of time (typically after 5 minutes) to enable better and faster further work with the stored data. nfcapd(1) serves as a typical network server daemon listening on specified port (by default on port number 9995). Daemon is used for listening on not only unicast addresses attached to a host interfaces, but it is also able to join multicast group for listening. On the other hand, it can also be used as a packet repeater resending incoming packets to another host. NetFlow data are stored in the proprietary NFDUMP extensible file format.

sfcapd(1) - sfcapd(1) is an analogy of the nfcapd(1) for processing IP flow information exported in sFlow format. Received sFlow data are also stored in NFDUMP binary file format, which is independent of the source format of the flow data.

nfdump(1) - Together with nfcapd(1), nfdump(1) makes up a base of the NFDUMP tool set. It is used to display and analyze stored IP flow information. Stored flow records are processed according to given filtering options based on the Berkeley Packet Filter (BPF) syntax, which is used also by tcpdump (1).

NfSen collectors - NfSen is a graphical web based frontend for the NFDUMP tools. The NfSen interface is what used in most cases see and work with while using Nf-Sen/NFDUMP collector. It preserves advantages of command line based tools using directly nfdump (1) program but in addition it gives easy to understand graphical overview of the network utilization.

c) MyNetScope and Data Sources

This layer requires data from collectors and other sources for its operation. The MyNetScope is a platform for advanced network traffic processing, analysis and visualization. MyNetScope overcomes the barrier of traffic content by focusing on traffic characteristics and behavior patterns and targets the intrusion detection and prevention systems (IDS/IPS) segment of recent times. The MyNetScope platform is a reaction to the current tendency to analyze or process network traffic using statistical methods. While traffic content processing is inapplicable in encrypted traffic, statistical methods are unable to detect precisely targeted or sophisticated attacks. The MyNetScope platform overcomes these limits by performing behavior-based analysis. It moves down from the application layer to the network and transport layer, reducing the amount of data to be processed but still focusing on individual data flows. Typical tasks for behavior analysis include dictionary attacks against network services or the misuse of secured hypertext transport protocol (HTTPS), where signatures can't be specified and a statistical approach may detect only massive attacks or HTTPS protocol misuse.

MyNetScope focuses on data flow characteristics and statistics - NetFlow data - and doesn't work with traffic content. NetFlow is an open industry standard defined by Cisco and designed to monitor large-scale and high-speed networks. MyNetScope provides an interactive insight into network traffic. It combines various visualization methods (dynamic mind maps, tables, forms and statistical graphs) in a single workspace and guides the user through visualization showing a greater or lesser level of detail according to the user's preference.

d) CAMNEP Data Sources

CAMNEP MyNetScope itself does not perform intrusion detection. However, it is very useful visualization tool that meets the requirements of “User-friendly Interface and Well-arranged Visualization”. Its power is in integration of external data sources. We decided to deploy of of the CAMNEP project. The description and evaluation for it as the “brain” of the intrusion detection system of the investigation was made. Reasonably this was made because the following requirements needed to be met:

- Accuracy,
- Detection of Novel Threats,
- Operation in a High-speed Networks,
- Early Detection,
- Anomaly Detection in Encrypted Traffic.

The CAMNEP Cooperative Threat Detection Layer was mainly used as shown in the figure 4.4 below. This layer combines modern intrusion detection methods. Precisely, this provides us with better accuracy than if particular anomaly detection methods could separately be deployed. The methods that were applied are able to detect novel threats and anomalies in case of the security anomaly. At the same time, they are captured as network traffic anomaly too.

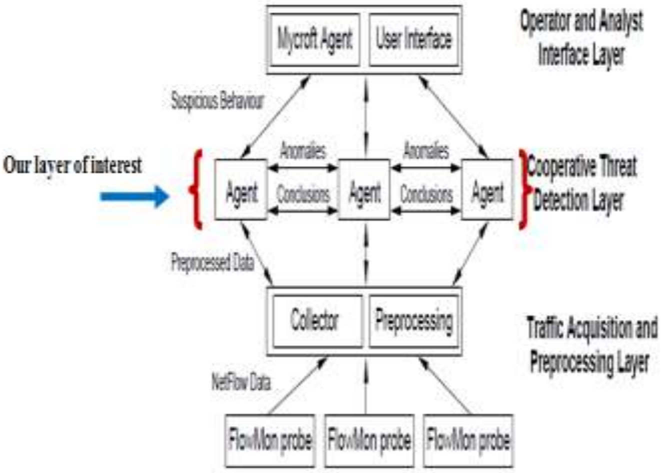


Figure5: CAMNEP architecture

For instance, a worm spreading or denial of service attack is “visible” in network flows. On the contrary, single packet that causes buffer overflow on a host computer does not represent the network traffic anomaly. Next, the methods were designed for high-speed networks from the very beginning or they were modified to meet this requirement. The detection is performed in 5-minute time windows. This is a reasonable interval due to flow aggregation, commonly used in connection with NetFlow. Finally, since the methods work purely with packet headers, the anomaly detection is possible even in case of the encrypted payload.

CAMNEP Detection Layer computes for each network flow and its trustfulness. This value is then imparted to MyNetScope and the user can view the suspicious flows and query the MyNetScope for other relevant information.

Other data sources: Apart from CAMNEP, other data sources such as DNS server were also utilized. The specific service or specific scripts for this data sources were to periodically check for policy violation. Their output is then included in MyNetScope too.

e. IDS Use Case Diagram

IDS system consists of use cases, actors and their relationships and a single use case diagram describes a particular functionality of a system.

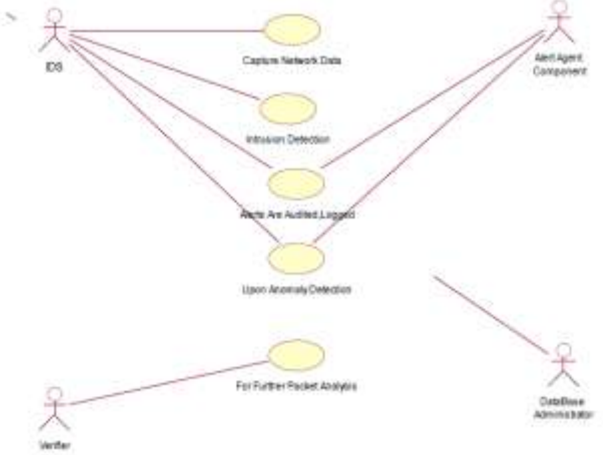


Figure 6: Use Case Diagram for the proposed IDS

The use case diagram basically shows different actors, use cases and the relationships between the use cases. This diagram is prepared in UML language using rational rose tool. The actors involved in our system are Intrusion Detection System, The alert agent, Verifier and finally the Database administrator. The use cases are to capture network data, Intrusion Detection, Audited and logged alerts, anomaly detection and further packet analysis. Now function of Intrusion detection system is to capture network data and detect intrusion in it and corresponding database administrator will maintain information about the same in its database. If intrusions are detected then corresponding alerts will be generated for it by another actor that is alert agent and if abnormal behavior is detected it will get updated into database. Verifier will do further analysis of the packet.

4. Discussion and Results

The question is where the Intrusion detection system fit in the design. To put it in simpler terms, an Intrusion detection system can be compared with a burglar alarm. For example, the lock system in a car protects the car from theft. But if somebody breaks the lock system and tries to steal the car, it is the burglar alarm that detects that the lock has been broken and alerts the owner by raising an alarm.

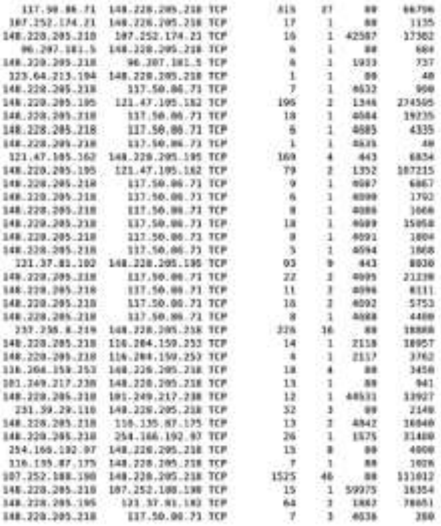
The Intrusion detection system in a similar way complements the firewall security. The firewall protects an organization from malicious attacks from the Internet and the Intrusion detection system detects if someone tries to break in through the firewall or manages to break in the firewall security and tries to have access on any system in the trusted side and alerts the system administrator in case there is a breach in security**.**

Moreover, Firewalls do a very good job of filtering incoming traffic from the Internet; however, there are ways to circumvent the firewall. For example, external users can connect to the Intranet by dialing in through a modem installed in the private network of the organization. This kind of access would not be seen by the firewall.

Therefore, an Intrusion detection system (IDS) is a security system that monitors computer systems and network traffic and analyzes that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization.An Intrusion Detection system comprises of Management console and sensors.

Management console is the management and reporting console. Sensors are agents that monitor hosts or networks on a real time basis. An Intrusion Detection System has a database of attack signatures. The attack signatures are patterns of different types of previously detected attacks.

If the sensors detect any malicious activity, it matches the malicious packet against the attack signature database. In case it finds a match, the sensor reports the malicious activity to the management console. The sensor can take different actions based on how they are configured. For example, the sensor can reset the TCP connection by sending a TCP FIN, modify the access control list on the gateway router or the firewall or send an email notification to the administrator for appropriate action.



```
   117.50.86.71  148.228.205.218 TCP     815   27     80   66796
 107.252.174.21  148.228.205.218 TCP      17    1     80    1135
148.228.205.218   107.252.174.21 TCP      16    1  42587   17302
   96.207.181.5  148.228.205.218 TCP       6    1     80     664
148.228.205.218     96.207.181.5 TCP       6    1   1933     737
 123.64.213.194  148.228.205.218 TCP       1    1     80      40
148.228.205.218     117.50.86.71 TCP       7    1   4632     960
148.228.205.195   121.47.105.182 TCP     196    2   1346  274505
148.228.205.218     117.50.86.71 TCP      18    1   4084   19235
148.228.205.218     117.50.86.71 TCP       6    1   4085    4335
148.228.205.218     117.50.86.71 TCP       1    1   4635      40
 121.47.105.162  148.228.205.195 TCP     169    4    443    6854
148.228.205.195   121.47.105.182 TCP      79    2   1352  187215
148.228.205.218     117.50.86.71 TCP       9    1   4087    6867
148.228.205.218     117.50.86.71 TCP       6    1   4090    1792
148.228.205.218     117.50.86.71 TCP       8    1   4086    1066
148.228.205.218     117.50.86.71 TCP      18    1   4089   15058
148.228.205.218     117.50.86.71 TCP       8    1   4091    1804
148.228.205.218     117.50.86.71 TCP       5    1   4094    1868
  121.37.81.182  148.228.205.195 TCP      93    9    443    8830
148.228.205.218     117.50.86.71 TCP      22    2   4095   21238
148.228.205.218     117.50.86.71 TCP      11    2   4096    8111
148.228.205.218     117.50.86.71 TCP      16    2   4092    5753
148.228.205.218     117.50.86.71 TCP       8    1   4088    4480
  237.238.8.219  148.228.205.258 TCP     226   16     80   18888
148.228.205.218  116.204.159.253 TCP      14    1   2118   18957
148.228.205.218  116.204.159.253 TCP       4    1   2117    3762
116.204.159.253  148.228.205.218 TCP      18    4     80    3458
101.249.217.238  148.228.205.218 TCP      13    1     80     941
148.228.205.218  101.249.217.238 TCP      12    1  48531   13927
  231.39.29.110  148.228.205.218 TCP      32    3     80    2148
148.228.205.218   110.135.87.175 TCP      13    2   4842   16840
148.228.205.218   254.166.192.97 TCP      26    1   1575   31480
 254.166.192.97  148.228.205.218 TCP      15    8     80    4008
 110.135.87.175  148.228.205.218 TCP       7    1     80    1026
107.252.188.198  148.228.205.218 TCP    1525   46     80  111812
148.228.205.218  107.252.188.198 TCP      15    1  59975   16354
148.228.205.195    121.37.81.182 TCP      64    2   1887   78651
148.228.205.218     117.50.86.71 TCP       7    1   4636     280
```

Figure 7: Network traffic as a listing of flows

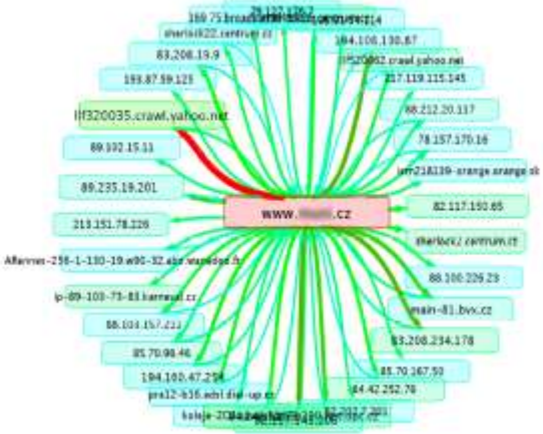


Figure 8: Network traffic as a graph

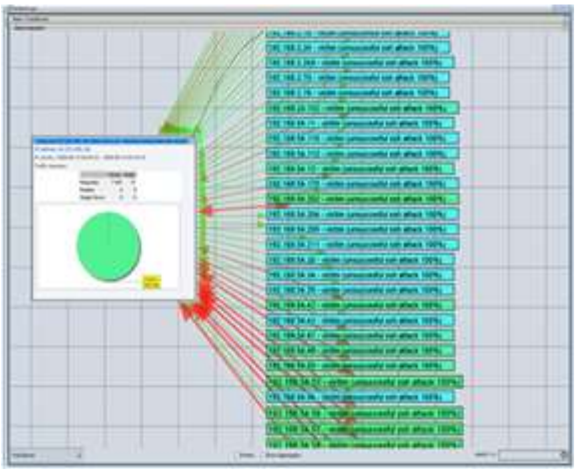


Figure 9: The results of SSH dictionary attack detection

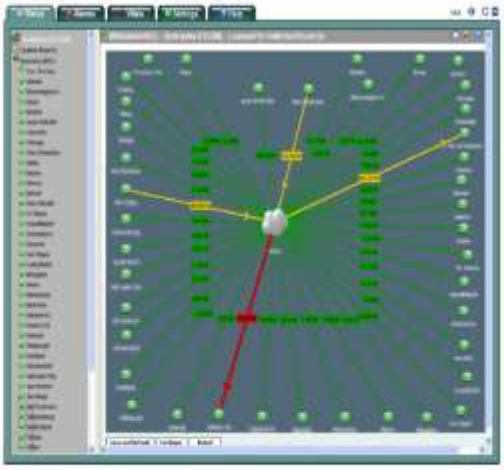


Figure 10: Network map

5. Conclusions and Future Work

It remains a challenge still today to detect and classify known and unknown malicious network activities through identification of intrusive behavioral patterns (anomaly detection) or pattern matching (misuse or signature-based detection). In fact, the number of network attack incidents continues to grow.

The new reality in IT security is that network breaches are inevitable, and the ability to monitor and control access and behavior patterns and misuse relies upon intrusion detection and prevention methods to be more quickly identified and more effectively addressed. In fact, An IDS/IPS is a must-have device; The focus will be on the application of Artificial Neural Networks (ANN) to be incoporated in Intrusion systems.

An ANN model will be based on learning patterns and classifying intrusion data packets in an effective manner. In comparison to traditional IDSs, ANNs have the ability to learn, classify, process information faster, as well as ability of self-organization. For these reasons, Neural Networks can increase the accuracy and efficiency of IDSs and Artificial Intelligency techniques that ANN will come with can improve IDS/IPS effectiveness.

6. Acknowledgement

I wish to express my profound sense of deepest gratitude to my classmates, friends and workmates for their valuable guidance and advice during the entire period of the project. I am also very grateful to my supervisors; Dr. George Okeyo and Dr. Wilson Cheruiyot for their invaluable and continuous guidance during the entire period of research. Without their support, this research would not fully been realized.

References

[1] Avaya Aura. : *Administering Network Connectivity*, 2014.

[2] Karen, S. et al : *Guide to Intrusion Detection and Prevention Systems* (IDPS), 2007

[3] Jiawei Han and. MichelineKamber, *Data Mining: Concepts and Techniques*, Morgan Kufmann, 2nd edition, 3rd edition 2011.

[4] Mueen, U. et al: *Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents*, 2010.

[5] Cho S. and Cha. S. SAD: *Web Session Anomaly Detection Based On Parameter Estimation*. Computers & Security 23(4):312–319, 2003.

[6] Rehak, M et al.: *CAMNEP: An Intrusion Detection System for high speed network*, 2008.

[7] Summer, R. and Feldmann, A.: NetFlow: Information loss or win?, 2002.

[8] Hong Yaling: *Research on Computer Network Security Analysis model*. 2013.

[9] Huang Zhilong: *Research on computer network security analysis model* 2014

[10] Brauckhoff, D. and Tellenbach, B. and Wagner, A. and Lakhina, A. and May, M.: Impact of Packet Sampling on Anomaly Detection Metrics, 2006, <http: //cs-people.bu.edu/anukool/pubs/anomalymetrics-sampling-imc06.pdf>

[11] Ivanko, J.: One-way Throughput Test - 20070715-F-0001, 2007, http://www. liberouter.org/flowmon/reports/report-20070715-F-0001.pdf

[12] Spitzner, L.: Honeypots, 2003, http://www.tracking-hackers.com/papers/ honeypots.html

[13] Rigney, C. and Willens, S. and Rubens, A. and Simpson, W.: RFC 2865: Remote Authentication Dial in User Service (RADIUS), 2000, http://www.ietf.org/rfc/ rfc2865.txt.

[14] Enns, R.: RFC 4741: NETCONF Configuration Protocol, 2006, <http://www.ietf. org/rfc/rfc4741.txt>.

[15] Haag, P.: NfSen, 2007, http://nfsen.sourceforge.net/

[16] David Burns, OdunayoAdesina, Keith Barker. (November 4, 2011). CCNP Security IPS 642-627 (Vol. 1). Indianapolis, IN 46240 USA: Cisco Press.