International Journal of Research in Advent Technology, Vol.7, No.2, February 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Ensuring the network security using IDS & honeypots

Ayushi.s
1st yr B.Sc computer science, M.O.P Vaishnav College for women
email: ayushikhatod03@gmail.com

Abstract-The primary focus of this paper is to manifest about the rousing trends to ensure the network security.by using network security tools such as honeypots and ids(intrusion detection system) . Honey pots can be called as a software or computer or a file that induces the hacker or the hostile computer activities to commit computer crimes or illegal activities which the hacker feels is concealed but it is being monitored through honey pot. It is basically a defense mechanism. Only the hackers will be caught and the other normal people are not allowed or prevented to connect to it. whereas, an IDS(Intrusion Detection System) is an detection module or a tool used to detect malicious activities.
Keywords- Honeynet;blackhats;firewall;snort;false positives; MySQL database.

1. INTRODUCTION:

On the account of rapidly increasing rate of cybercrimes in today's world it has become eminent to have a preventive measure for it, to reduce these crimes which are done online using a network can be reduced by using honeypots and ids systems.

Honeypots are more and more used to collect data on malicious activities on the Internet and to better understand the strategies and techniques used by attackers to compromise target systems[1]**.** It is basically a technique employed to catch the hostile users who pose a threat to network and security, it also ensures to reduce the security threats such as viruses,worms,crackers or internet attacks which the normal users face. It basically creates intuition for the hackers to attack it as they are closely monitored the network administrator is alerted before a possible trespassing activity. Now a days in this increasing aeon of technology,the restless usage of internet plays a major role in all the activities ranging from education,money transfer and other online banking transactions.If we want all our tasks to undergo in a safe manner then we must ensure security in the network we use or we are connected to for which honey pots are used. Although a honeypot appears and behaves like a real network,it has that capacity to attract hackers and offers easy exploitable flaws to encourage the blackhats to waste their time using this fictional network.There are different types of honeypots used which will be mentioned in this.

Intrusion detection is a complex business. Whether you deploy an intrusion detection system (IDS), or you gather and examine the computer and device logs on your network, identifying malicious traffic in a sea of legitimate activity can be both difficult and time consuming[2].It is an device or an application which monitors intruding activities that tends to hack networks (blackhat community).

The SIEM(security information and event management) system collects the information about any malicious activity or violation that is typically reported to an administrator. Its types ranges from large networks to single computers. As soon as the intrusion activity has been detected it signals an alarm.

2. REVIEW OF LITERATURE:

anon_100036097 [1] defined the IDS and honeypots as the IDS (Intrusion Detection System) gathers information within a LAN/CAN aboutunauthorized access as well as misuse. An IDS isalso referred as packet sniffer. An IDS evaluatesa suspected intrusion once it has taken placeand signals an alarm. And a honeypot is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally, it consists of a computer, data or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers

Tejvir Kaur1, Vimmi Malhotra2, Dr. Dheerendra Singh3 [2] examined the Intrusion as the act of violating the security policy that pertains to an information system. Intrusion detection can be defined as the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource.

F. Pouget, M. Dacier[3]defines"A **honeypot** consists in an environment where vulnerabilities have beendeliberately introduced in order to observe attacks and intrusions."

Lance Spitzner "Honeypots, tracking hackers" [Spit02] (2001) [4] the term 'honeypot' was coined

by him. He defined "A honeypot is security resource whose value lies in being probed, attacked or compromised." [Spit02, page 40]
Reto Baumann [4]"A honeypot is a resource which pretends to be a real target. A honeypot is expected to be attacked or compromised. The main goals are the distraction of an attacker and the gain of information about an attack and the attacker." [BauPla02]
The University of Wisconsin-Platteville) as well as R.C. Barnett[5] mentions the following definition: "An Internet-attached server that acts as a decoy, luring in potential hackers in order to study their activities and monitor how they are able to break into a system. Honeypots are designed to mimic systems that an intruder would like to break into but limit the intruder from having access to an entire network. If a honeypot is successful, the intruder will have no idea that s/he is being tricked and monitored." [Sour03]
Uwe Aickelin,Julie Greensmith,Jamie Twycross (2004) [6] examined that IDSs are software systems designed to identify and prevent the misuse of computer networks and systems.
There are a number of different ways to classify IDSs. Here we focus on two ways: the analysis approach and the placement of the IDS, although there has been recent work on alternative taxonomies. Regarding the former, there are two classes: misuse detection and anomaly detection.
Tejvir Kaur1, Vimmi Malhotra2, Dr. Dheerendra Singh3(2014) [7] analyzed that the Intrusion Detection System (IDS) helps information systems to deal with attacks. This is accomplished by collecting information from a variety of systems and network sources. The information collected is analyzed for possible security problems.

3. METHODOLOGY

3.1. *Honeypots:*

Tremendous changes have been brought in the way we see the world, by the internet allowing us to communicate at the speed of light but this ability to share details across the enormousness of the internet network is providing the intruders to exploit others personal information and posing a threat to the national security of our entire nation. Honeypots are the decoy systems which uses IDS(intrusion detection systems) tools to detect the intrusions or malicious activities.
Some people prefer the more labor-intensive methodology called honeypot rather than trying to block a hacker (black hat) with a firewall or to find (or) monitor an intruder with an intrusion detection system.
So, for this a proper methodology or a desired algorithm must be used such as explained generally:[5]

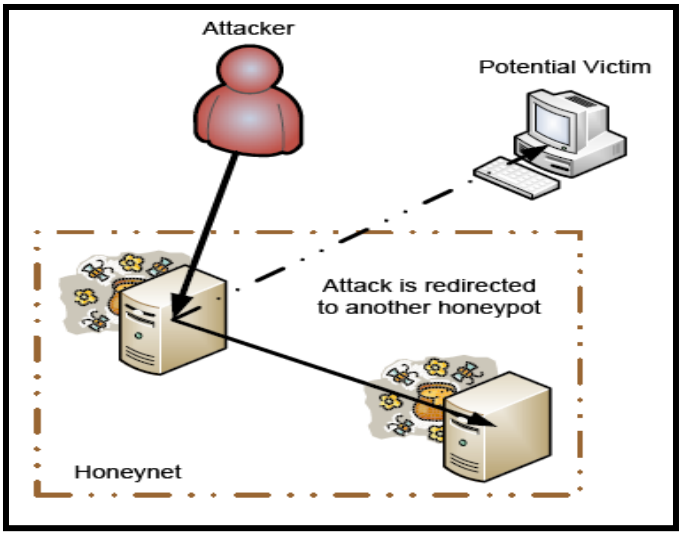

Figure 1 Architecture of honeypots

This forms a basic process in which attacker attacks a computer(potential victim) which is nothing but a trap for hackers (honeypot) when many systems attack together the attack is redirected to another network of honeypot. Likewise, many honeypots combined together forms a honeynet as illustrated in Figure 1.
Another proposed methodology is as follows:[6]
From figure2,it is seen that In our application to monitor enterprise network traffic, analyze it well and to avoid intruding activities a honeypot-based attack detection and prevention design has been developed.The basic components for this developed application can be viewed in three groups respectively,[6]"**the honeypot server application**" that can simulate trap systems, **"the monitor application**" on which the animations are displayed that are detected from honeypot communication server, and by this monitor application honeypot server application many configurations are done, and "**the IDS application**" which is a server application where the packets come to the honeypot server by trapping and are sent to the monitor.It is known that in LAN region as shown in Figure 2, recognizing a honeypot causes significant security risks. So, inthisperformedapplication,theattackattractioncompo nentof honeypot is made as **low-interaction**. for the integrity of the accomplishing application, the honeypot server application is implemented in C #programming language.

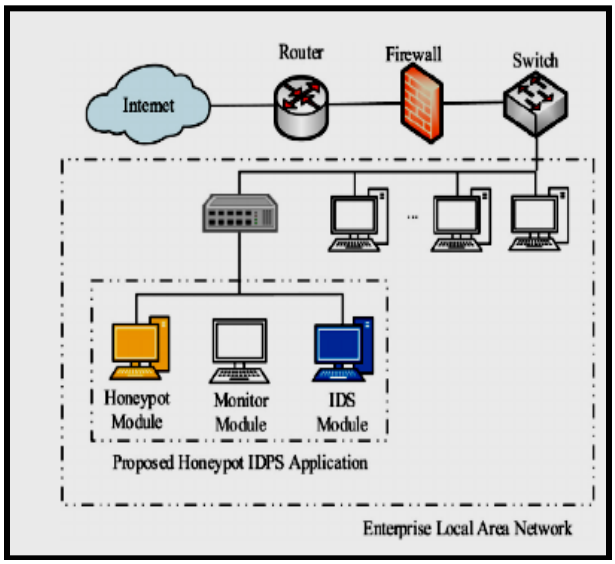

Figure 2 Expanded structure of enterprise LAN

3.1.1. *Honeypot server module:*
Honeypotserver application consists of three components: low-interactionattackattractioncomponent,configurationcomponent and IDS communications component.

- **Attackattractioncomponent**:Thiscomponentisa lowinteractionhoneypotthathastheskillofattackattractionandit hasbeenprovidedbythehoneyapplication.Thiscomponent is the part which includes a mechanism that can attract the intruders.
- **Configurationcomponent**:Bythiscomponent,theIDSandthe honeyapplications'attackattractioncomponentthatcanbe configured.
- **IDScommunicationscomponent**:Thiscomponentprovidesthe honeypot server module tobe able to communicate with IDS module.

3.1.2. *Simple algorithm's flow chart is as follows:[4]*
From figure 3, it can be seen that whenever the given conditions are satisfied the control is transferred for honeypot to honeycentre and then followed by to the additional server. Then the data that is gathered about the hackers is processed and then honeycentre sends the information to the web server and all the instructions are executed, Where as, if the given conditions are not satisfied the honey Centre sends an error report to the network administrator of related web server or incrementation takes place.

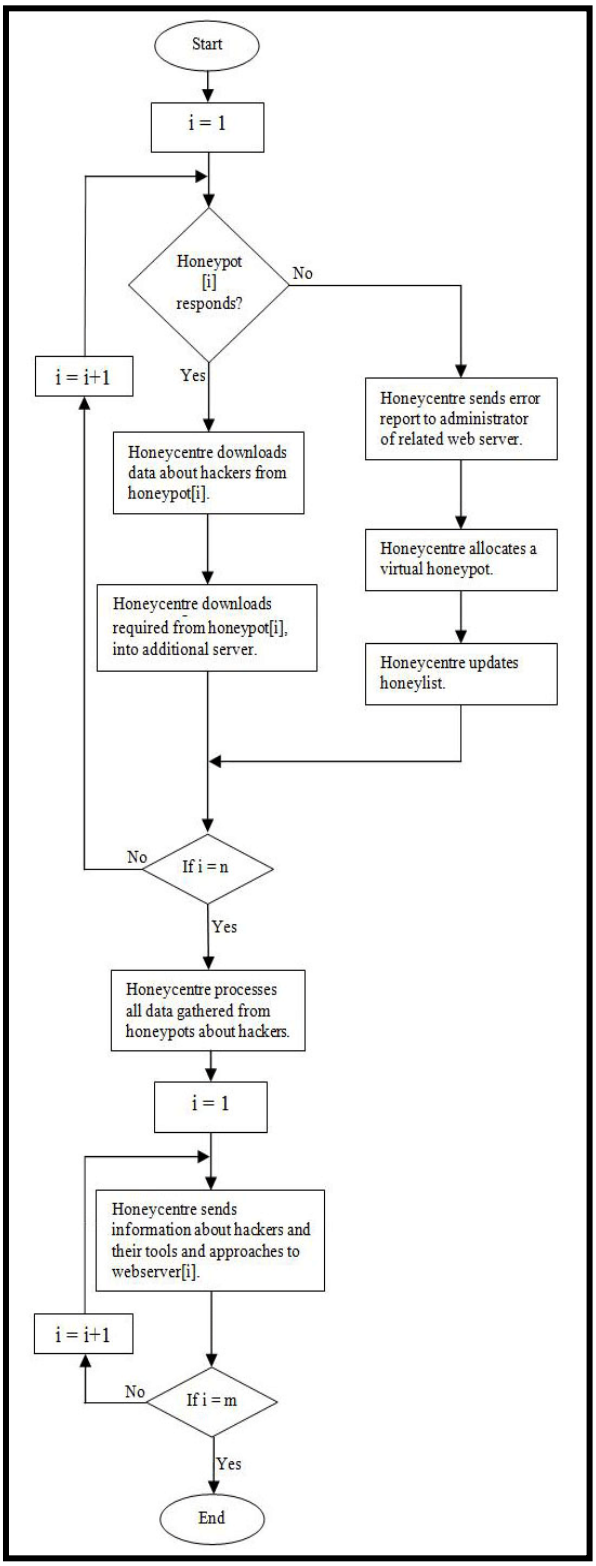

Figure 3 A basic algorithm used in honeypot

3.2 ***Types of honeypots:***

There are different varieties of honeypots: they can be classified on the basis of their level of involvement(design) and based on their deployment.

Based on deployment honeypots are classified as:

(1) Production honeypots

And

(2) research honeypots

3.2.1**.** *Production honeypots:*

Production honeypots are placed by an organization inside the production network with other production servers to improve their overall state of security. Generally, production honeypots are low-interaction honeypots, which are easier to establish. They provide somewhat less information about the attacks or attackers than research honeypots do. These are easy to use, they capture only limited information, and are used primarily by companies or corporations. [3]

3.2.2. *Research honeypots:*

They capture extensive information, and are used primarily by research, military, or government organizations. Research honeypots are complex to maintain as well as establish , They are used most often to gather information about the tactics and motives of the intruders community targeting different networks. Research honeypots as they do not add any direct value to a specific organization so they are used to research about the threats organizers and helps us to learn how to be better protective against those threats.[3]

Based on involvement(design) honeypots are classified as:

(1) Low-interaction honeypots.
(2) Medium-interaction honeypots.
(3) High-interaction honeypots.

3.2.3. *Low-interaction honeypots:*

Low-interaction honeypots represent the intruders imitated services with a limited subset of the functionality they would expect from a server, with the intent of detecting sources from an unauthorized activity. For example, the HTTP service provided on low-interaction honeypots would only support the commands needed to identify that a known exploit is being attempted. Further more, they replicate the services frequently requested by attackers .Since, they consume relatively few resources, multiple virtual machines can easily be hosted on one physical system. Because , the virtual systems have a short response time, and less code is required it theryby reduces the complexity of the security of the virtual systems.[3]

3.2.4. *Medium-interaction honeypots:*

Some authors classify a third categoryof honeypot called medium-interaction honeypots, as they provide an expanded interaction over low-interaction honeypots but less than high-interaction systems. They only provide partial implementation of services and do not allow typical, full interaction with the system as of high-interaction honeypots.They, might more fully implement the HTTP protocol to emulate(establish) a well-known vendor's implementation, such as Apache.[3]

3.2.5. *High-interaction honeypots:*

In accordance to the recent researchers, the technology using high interaction honeypots , with the help of utilizing virtual machines, multiple honeypots can be hosted on a single physical machine. Incase even if one of the honeypot is compromised, it can be re-imposed more quickly. These honeypots imitate the activities of the real systems that host a variety of services.(no emulation) .It lets the intruder interact with the system as they would do on any regular operating system, with the goal of capturing the maximum amount of information on the attacker's techniques.Although high interaction honeypots provide more security by being difficult to detect, but it has the main drawback that it is very costly to maintain.[3]

3. 3. ***Intrusion Detection System (IDS):***

For any security network,intrusion detection and prevention are necessary.Priory,firewalls were eminently used for network security but now IDS(intrusion detection systems) are used to detect any kind of malicious activity.For this detection purposes many types of software are used such as snort(software). **Snort** is a free open source network intrusion detection system (IDS) and intrusion prevention system (IPS) created in 1998 by Martin Roesch, former founder and CTO of Sourcefire. Snort is now developed by Cisco , The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprintingattempts, semantic URL attacks, buffer overflows, server message block probes [7] .A proposed algorithm(flowchart) is as follows:

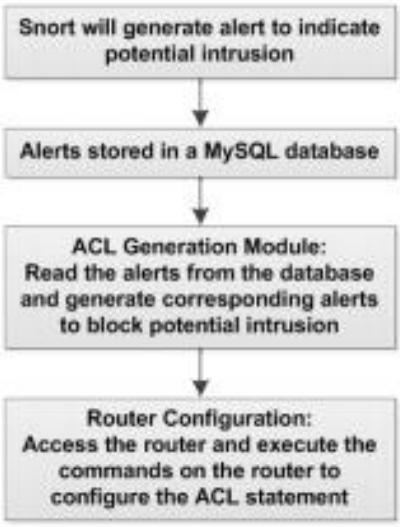

Figure 4 Algorithm used by IDS

IDS(intrusion detection system) uses this algorithm to detect intruding activities where Snort is used as an intrusion detection system to provide alerts for the potential intrusions. The alerts generated by IDS are instinctually logged by Snort to MySQL database from where they are read by the proposed software and are used to prevent the potential intrusion [8]. IDS uses only the first two sections from above model: snort(software) and MYSQL database where alerts are stored.

3.3.1 *The proposed methodology is as follows*: [8]

From figure 5, To detect the distrustful activity both at the network & host level IDS using various methods and techniques.Intruders have signatures that can be detected[8] and on the basis of it is able to find the malicious activities running on computer and generate alerts using alarm network. In the above model multiple server systems are connected to a firewall that is again used to protect (a network or system) from unauthorized access with a firewall. And then the whole thing is connected to alarm network through IDS.

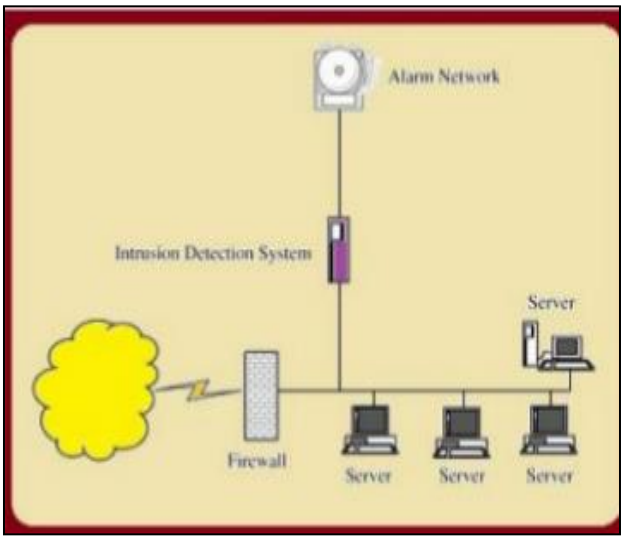

Figure 5 Methodology used in IDS systems

3.4. ***Types of IDS (intrusion detection systems):***

The most common classifications are:

(1) Network intrusion detection system (NIDS)- That is, it is a system that analyzes incoming network traffic.

(2) Host-based intrusion detection system (HIDS) That is, it is a system that monitors important operating system files.

By detection approach, we can classify IDS as:

(1) Signature-based detection (used for recognizing bad patterns (malware))

(2) Anomaly-based detection (detecting deviations from a model of "good" traffic, which often relies on machine learning)

3.4.1. *Network intrusion detection systems:*

NIDS can be also combined with other technologies to increase detection, and prediction rates**.** It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Network intrusion detection systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator. OPNET and NETSIM are commonly used tools for simulating network intrusion detection systems [10].

3.4.2 *Host intrusion detection systems:*

The systems that runs on individual hosts or devices on a network are called as Host intrusion detection systems (HIDS). It will alert the user or administrator

only if suspicious activity is detected as HIDS monitors the inbound and outbound packets from the device only. It takes a snapshot of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their configurations [10].

Detection methods:

3.4.3. *signature -based:*

This terminology originates from anti-virus software, which refers to these detected patterns as signatures.. On-time updation of the IDS with the signature is a key aspect .Signature-based IDS refers to the detection of attacks by looking for specific patterns, such as byte sequences in network traffic, or known intruding instruction sequences used by malware. Although signature-based IDS can easily detect known attacks, it is difficult to detect new attacks, for which no pattern is available [10].

3.4.4. *Anomaly -based:*

In contrast with signature based detection ,Anomaly-based intrusion detection systems were primarily introduced to detect unknown attacks, in part due to the rapid development of malware. The basic approach is to use machine learning to create a model of trustworthy activity, and then compare new behavior against this model. Although this approach enables the detection of previously unknown attacks, it may suffer from **false positives**: previously unknown legitimate activity may also be classified as malicious [10].

3.5. ***Pros and cons:***

Table 1. Advantages and Disadvantages

Honeypots	**Intrusion detection systems(IDS)**
Advantages:	**Advantages:**
1. Honeypots are designed to apprehend anything thrown at them, including tools or tactics that have never been seen before.	1. IDS are easier to utilize as it does not affect existing systems or infrastructure[10]
2. Honeypots can collect small amounts of information.. Instead of generating 10,000 alerts a day, they can generate only 10 alerts a day. Instead of logging a two GB of data a day, they can log only two MB of data a day	2. NIDS(network-based IDS) sensors can detect many attacks by inspecting the packet headers for any intruding attack like TCP SYN attack fragmented packet attack etc. [10]
3. Any kind of interaction with a honeypot is most likely an unauthorized access or malicious activity.	3. IDS can monitor traffic on a real time. So, network-based IDS can detect malicious activity as they occur [10]
4. Honeypots require minimal resources, as they only record the bad(illegal) activity. It uses a defense mechanism.	4. IDS sensor deployed outside the firewall can detect malicious attacks on resources behind the firewall [10]
5. Honeypots work in encrypted or IPv6 environments unlike most security technologies (such as IDS systems). It does not matter what the intruder guys throw at a honeypot, the honeypot will detect and record it.	5. It is a detection mechanism [10]
6. Simplicity: Finally, honeypots are conceptually very simple.	
Dis-advantages:	**Dis –advantages:**
1. If they honeypots are used by hackers then it can be used to attack other system making it a bane for us.	1. IDS is not an alternative to strong user identification and authentication mechanism [10]
2. It can only track and record the activity that directly interacts with them. It will not capture	2. IDS is not a solution to all security concerns andHuman intervention is required to

attacks against other systems unless the attacker or threat interacts with the honeypots.	investigate the attack once it is detected and reported [10]
3. If a hacker is too smart then he can potentially detect the honeypot's trap.	3. False positives occur when IDS incorrectly identify normal activity as being malicious. Whereas, False negatives occur when IDS fail to detect the malicious activity [10]

4. CONCLUSION:

Honeypots and IDS both acts as an eminent tool for observing the hacker's movements as well as preparing the system for future attacks. If one provides a detection system the other provides us with a defense system thereby ensuring network's security.

Honey pots as well as IDS acts as flexible tools with wide variety of applications for security purposes. Their main purpose is detection of malicious activities and to gather that information.Honeypots are a new and interesting field in the sector of network security,while IDS is an old field in comparison to it but has a wide variety of fields in it than honeypots.Currently, there is a lot of ongoing research and discussions about them all around the world. No other method or technique is comparable in the efficiency of a honeypot if gathering information is a primary goal, especially if the tools an attacker uses are of interest. As honeypots are getting more advanced, hackers will also develop methods to detect such systems,but before the hackers detect it, we should also improvise the network security techniques then, A regular arms race could start between the good people and the Blackhat community(hackers).

REFERENCES:

[1] M. Kaâniche1, E. Alata1, V. Nicomette1, Y. Deswarte1, M. Dacier2 1LAAS-CNRS, "Empirical Analysis and Statistical Modeling of Attack Processes based on Honeypots",Université de Toulouse 7 Avenue du Colonel Roche, 31077 Toulouse Cedex 4, France https://arxiv.org/pdf/0704.0861

[2] Roger A.Grimes" Intrusion detection honeypots simplify network security" https://www.networkworld.com/article/2194777/security/intrusion-detection-honeypots-simplify-network-security.html Columnist, InfoWorld | NOV 17, 2010

[3] Mohit Arora"Various Types Of HoneyPots"September 17, 2015 https://catchupdates.com/honeypots/

[4] Bahman Nikkhahan, Sahar Sohrabi, and ShahriarMohammadi "Using Honeypots to Secure E-Government Networks" © Springer-Verlag Berlin Heidelberg2009https://link.springer.com/chapter/10.1007%2F978-3-642-10240-0_7

[5] Eric Peter "A Practical Guide to Honeypots" https://www.cse.wustl.edu/~jain/cse571-09/ftp/honey/

[6] MuhammetBaykara, ResulDas"A novel honeypot based security approach for real-time intrusion detection and prevention systems" https://www.researchgate.net/publication/326746050_A_novel_honeypot_based_security_approach_for_real-time_intrusion_detection_and_prevention_systems August 2018

[7] snort(software) https://en.wikipedia.org/wiki/Snort_(software)

[8] Muhammad Naveed1 , Shams un Nihar2 , Mohammad Inayatullah Babar3 "Network Intrusion Prevention by Configuring ACLs on the Routers, based on Snort IDS alerts " https://www.researchgate.net/profile/Muhammad_Naveed23/publication/224196023_Network_intrusion_prevention_by_configuring_ACLs_on_the_routers_based_on_Snort_IDS_alerts/links/0f31753ba67dd73266000000.pdf

[9] Tejvir Kaur1 ,Vimmi Malhotra2 , Dr. Dheerendra Singh "Comparison of network security tools-Firewall, Intrusion Detection System and Honeypot" February-2014 https://pdfs.semanticscholar.org/c437/2e695acd7636367c106d6c347544ed131b98.pdf

[10] "Intrusion Detection System" Wikipedia https://en.wikipedia.org/wiki/Intrusion_detection_system