International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

IMPLEMENTATION OF INTRUSION DETECTION SYSTEM (IDS) IN NETWORK SECURITY SYSTEMS

Luay Abdulwahid Shihab

Assistant Professor in College of Nursing, University of Basrah, Basrah, Iraq.

luaay.abdulwahid@uobasrah.edu.iq

Abstract

Network security faces a wide range of risks including viruses, Trojans, worms, and attacks. A network firewall can only protect against external threats, not attacks from within your own network. The Intrusion Detection System (IDS) is a critical component of network security. and is a tool used to check activities that have occurred. Security in home/office networks is an increasingly worrying problem as the number of devices that connect to them increases and sensitive and personal data is transferred over the network. In most government offices, devices connect to the Internet automatically and we do not usually configure adequate security, which makes the network vulnerable to attacks or intrusions. These devices are also often not designed with security in mind, making them prone to attacks. These attacks are increasingly common on organization networks. Therefore, it is essential that appropriate security measures are implemented to protect office networks. Implementing an intrusion detection system (IDS) on office network can be an effective solution to improve network security. The different information systems used by the main headquarters of the Office of the Trade Commissioner for Al-basrah must be available at all times, given that the systems are used by the users of the entity, and if a failure or intrusion occurs, it must be corrected immediately. to provide continuity to the services provided by the entity. The implementation of this work seeks to benefit the entity's employees, who, through the information assets they manage within the entity .

Keywords: intrusion detection system, snort, software, hardware, Anomaly, computer attacks, intrusion detection, ids, snort, computer security, free software.

1. Introduction

Communication network technology has advanced rapidly in recent years. Businesses and organisations require security technology to ensure the safety of their members. Threats that will affect the company Furthermore, the internet has grown extremely quickly. It's quick and widely used. Because it makes it easier to talk to each other and share information quickly, the following points must be considered: Peace of mind Every day, the attack patterns change. Hackers can come from both inside and outside the network. Those who are experiencing difficulties, such as banks, organisations, or businesses but the threat we face today isn't limited to the Internet. Another approach is to use operating systems or application software, which can make the network or even the protocols used to communicate with one another less secure.

Received: July 20, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Attackers can also enter networks without permission via the internet. Having a firewall in an organisation is insufficient to prevent it [1]. for send any Public confidential and sensitive to face an official must be protected by the local network one way encryption possible transitions simple networks non local communication of email and the insured are [10]. The design of a wireless sensor network involves a number of factors to be considered. Of the most important we have Fault tolerance, Scalability, Production cost, Operating environment,

Hardware restrictions, Network topology, Transmission medium and power consumption [11].

Intrusion Detection System (IDS)

Networks with intrusion detection systems Its purpose is to monitor network traffic. It can search, detect, and analyse attack packets. report to central agencies. In order to conduct an additional survey to determine the type of attack. Are any intrusion detection sensors installed on the network? Types are: 1) It is the detection of abnormal occurrences. (Anomaly-based detection) 2) It is the detection of incorrect usage (misuse-based detection) [2].

Detecting abnormal events. (Anomaly-based detection): Anomaly detection requires separate activities. Normal work or acceptable activities are removed, leaving only abnormal activities. Normal activities observable through user behaviour or network connections, for example. These statistics are derived from usage history [3]. The intrusion detector collects various event data and uses criteria to calculate statistical values. To compare with existing normal activity data, any behaviour that deviates from the existing behaviour is considered "not normal" and is classified as an attack. Advantages and disadvantages. The disadvantages of the Anomaly-Based Detection method are as follows: Advantages

- Detection based on anomalies outperforms signature-based methods. Because it can detect unknown attacks.
- Anomaly-based detection can obtain signature information, which is then used by misuse-based IDS. Disadvantages
- Anomaly-based detection: In general, there will be a large number of false alarms because user and network behaviour cannot be predicted in advance.
- Detecting anomalies requires a large amount of training data. It contains a system event log that allows for a detailed description of normal behaviour.

Misuse-Based Detection: The intrusion detector analyses system activity. Consider the event or set of events that match a pattern. An invasion-level event. It discusses the various types of known invasions. The format for the invasion event. These known invaders are referred to as traces of intrusion (signature).[4] Misused detection is also known as signature-based detection. This approach uses information and knowledge about offensive or unacceptable behaviours to search for and detect these behaviours directly. This is in contrast to anomaly-based detection, which seeks to detect such behaviours.

For the Office of the Trade Commissioner for Al-basrah, security is of vital importance in the correct functioning of its data networks and the information that is transmitted, which is why

Received: July 20, 2025

Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

confidentiality, integrity and availability of data must be guaranteed through the pillars of security. information at all times. Preventing the risk of attacks from being reduced or as minimal as possible, given that in recent years public entities have become targets of hackers or malicious people. If a security breach occurs in the networks, it could cause irreparable damage to the integrity of the information, leaving end users without service, or capturing sensitive information of citizens [5].

The growing use and strategy of information technologies poses to the Trade Commissioner for Al-basrah the need and commitment to improve security tools, since the information managed by the entity must contain the minimum risk of loss and greater control over its access. The opportunity then arises to implement an intrusion detection system to control vulnerabilities for the internal network of the Office of the Trade Commissioner for Al-basrah

2. Research Methodology

The theoretical references consulted for the development of the project allowed the implementation of an intrusion detection system, among which are security, computer security, network security, firewalls, intrusion detection system, architecture of an ids, types of Ids [6], commercial ids and free software. The type of research that will be used in this research work will be empirical, since a hypothesis is proposed, which must be validated through practical work which will be documented [7]. Thus, technical and practical work will be developed to fully achieve the objectives that are intended to be achieved in this project. The empirical methodology is based on the experiment and the direct implementation of the actions, which aim to validate the proposed hypotheses. To achieve the implementation of an intrusion detection system, both technical and theoretical actions are required; these must converge, in practice and experimentation, which will provide information and results that will serve to validate and support the implementation of an intrusion detection system. information on the Commissioner's internal network.

2.1 Methodology Development

For the development of this project, multiple parameters must be taken into account that directly influence the operation and actions carried out within the entity, which have specific aspects for information processing, which must be safeguarded in some cases. cases and in others become public by fulfilling a number of particular characteristics, allowing improvement within the processes.

Therefore, for the development of the project, the PDCA (Plan, Do, Check and Act) methodology [8] was used, which proposes continuous improvement, in this case in the model for the implementation of the intrusion detection tool through its cycles.

To plan: In this first cycle, all the project activities were determined, the delimitation of the project, the necessary resources, the time necessary for the correct execution of the activities, definition of objectives, as well as the identification of a contextual framework, project

Received: July 20, 2025

Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

background and a theoretical framework. For this initial phase of the project, the activities listed below were carried out.

- Analysis of information from related projects
- Identification of the current status of the Trade Commissioner's network.
- Analysis of the tools available for the execution of the project
- Schedule of activities

Do: For this cycle of the methodology, the Doing activities were carried out that allowed the project objectives to be executed, as well as the product to be delivered, and the implementation model of an intrusion detection system in the internal network of the Commissioner's office. hunting using free software, for which the following activities were executed in the Do Phase of the PDCA cycle:

- Verification of the characteristics and specifications of the server or computer equipment where the operating system was installed.
- Analysis of the areas or schemes in which it is possible to install the intrusion detection system.
- Installation of the necessary libraries for the correct functioning of the intrusion detection system.
- Installation and configuration of the database engine for storing detection system alerts, as well as the Php language, and the Apache application server.
- Installation and configuration of the intrusion detection system with the Snort tool, in addition to the barnyard tool.

Verify: In this third phase, reviews and monitoring of the development of the project were carried out, allowing us to verify that each of the selected tools worked correctly and thus met the objectives. Likewise, the required adjustments were made to the document. For this phase, the following activities of the verify phase were carried out, taking into account the schedule of activities.

- Review of each of the tools and applications, carrying out tests that allowed us to verify their correct operation.
- Required adjustments to the project document verifying its alignment with the project objectives.

Act: For the act phase of said methodology, the result was the continuous improvement of the network devices of the systems office, through the implementation of an intrusion detection system in the network of the Office of the Trade Commissioner for Al-basrah.

2.2 Current Network Design of The Trade Commissioner for Al-basrah

The main headquarters of the Office of the Trade Commissioner for Al-basrah currently has in its infrastructure data backup servers, application servers, client stations that connect to local servers, as well as database servers, where data is managed and stored. of great relevance. The

Received: July 20, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

following figure 1 shows more accurately the status of the network, with the devices that make it up.

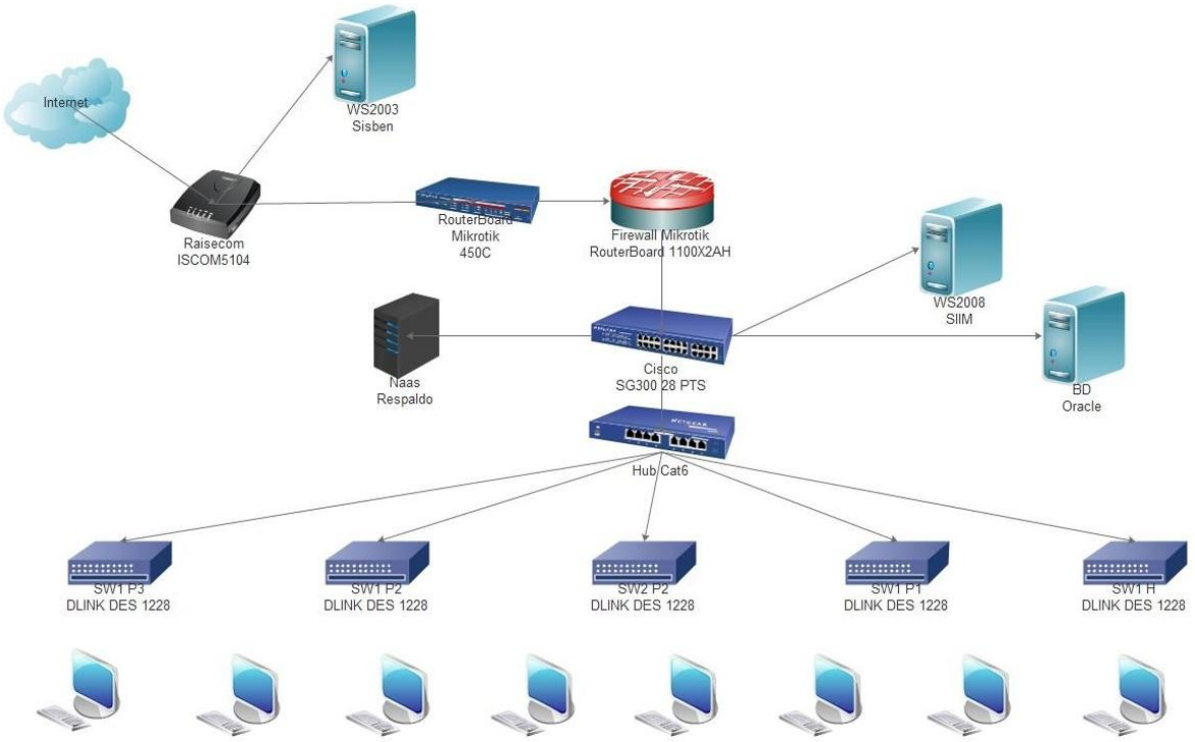


Figure 1. Main headquarters network

The devices that make up the network are protected in a machine room, which provides them with physical security. In addition, they are under refrigeration to prevent overheating. It also has a 15kva power supply system that provides power supply, in cases of external power failure. The equipment shown in the previous figure is described below.

- Mikrotik 1100X2AH Firewall: Device used in blocking ports, redirecting services, denying services, blocking connections, as well as publishing services to the web.
- Naas Lenovo Px 300: 4Tb network storage, used to backup information in different offices.
- Naas Segate: 4Tb network storage, used to backup information in different offices.
- Hp Proliant ML150 G3: Web application server, which has the Windows 2016 operating system.
- Hp Proliant ML150 G6: Web application server with Centos 8 operating system, with Apache server and MySQL database.
- Cisco SG300 Switch: Switch that interconnects external devices, as well as connects internal LAN equipment, like other switches, and distributes connections to servers.
- Hub: Device that interconnects the d-link switches of the infrastructure.
- Switch Dlink Des 1228 (5): Network equipment that connects the computer equipment of all offices.

Received: July 20, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2.3 Verification of IDS to implement

Intrusion detection systems are programs that scan system or network activity, with the aim of detecting unauthorized access or actions to a machine or network [9].

When implementing an intrusion detection system, it must be taken into account which of the two types, Hids (host) or Nids (network), will be developed. The option of choosing to implement some of these lies in the objective that you want to monitor or analyze; In this case, scan the network of the Trade Commissioner's office in search of intrusions.

There are different types of software ids tools on the market for configuration and commissioning, within the Hids type there is Ossec and on the Nids side, Snort.

- **Ossec**: This intrusion detection system is of the host type, that is, it analysis everything related to the events and records of the operating system of the computer where it is installed, it also checks its integrity, and performs audits of the records of Windows computers.

  It is also an open-source application and free to implement, it has a wide range of options in its configuration, which makes it a software adaptable to security needs; allows the customization of alert rules, as well as the definition of action rules in response to previously established security alerts.

  This system is comprised of three components, a main application, a Windows agent, and a web interface. The main application is used in distributed networks, where it can support various operating systems such as Linux, BSD, and Mac.

  The Windows agent is used in Windows environments, configuring the main application in server mode, and verifying support for the agent in Windows. Finally, the web interface allows graphical visualization of alerts and operation to the administrator user.

- **Snort.** NIDS type intrusion detection system (scans the network unlike ossec, which has computer-level behavior) therefore works by scanning and analyzing the packets circulating in the network, identifying possible attacks based on their behavior. The most basic way to install snort allows the activation of system logs, saving those logs in a database and viewing them from a web administrator. It has a GPL license, is free and works under Linux and Windows platforms, in addition to having a large number of plugins developed by independent organizations, making it one of the most used detection systems, as well as the integration of applications that allow great adaptability to the needs of the users. In its structure it is defined by a packet decoder, preprocessors, detection engine, alarm and reporting system. Packet decoder is responsible for capturing packets. The preprocessor performs analysis of the packets that have passed through the decoder. The detection engine detects whether a captured packet contains any attack patterns, based on snort signatures. Finally, the alarm and reporting system allows you to define what and how the generated alarms are saved.

Received: July 20, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Similarly, the fact that it is an Open-Source application, Snort has the advantage of being a system that is configurable and adaptable to specific needs, so it can be a good solution if you are looking for a personalized system for the development of the project. This is one of the reasons why it was decided to select Snort as an intrusion detection system instead of other applications, which in many cases do not achieve the same performance or features.

2.4 Where to Install The IDS

Prior to installing the selected Snort tool, the possibilities where the intrusion detection system can be located must be verified. For this location, the traffic to be scanned or detected must be taken into account, incoming or outgoing packets, in front of the firewall or behind it. Wherever the IDS is located, its operation must be guaranteed in conjunction with the other elements of the network, capturing and sharing information from switches, routers and firewalls. This is how the locations where the ids can be installed are shown below.

2.4.1 In front of the Firewall

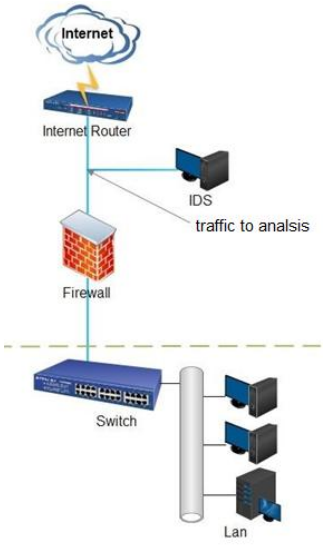


Figure 2: Ids in front of the Firewall

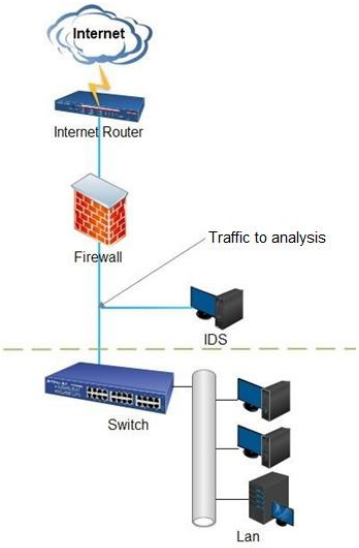


Figure 3: Ids behind the Firewall

With this location, many false positives of attacks are generated, in addition to the large amount of information that is saved in the logs, which is why it analysis all the traffic that enters and leaves the network.

2.4.2 Behind the Firewall: Configuring the ids behind the firewall is the most used location, because its analysis the traffic that passes through the firewall, becoming another filter for the network. Here the traffic actually entering the network that the firewall could not block is scanned, so there are fewer cases of false alarms than in the previous location.

2.4.3 Combination of the two cases: By configuring the ids in front of the firewall and behind the firewall, you have greater control of the attacks that actually cross the firewall, having the opportunity to detect them if they occur. This model presents a difficulty, and that is that it requires two teams to launch it.

Received: July 20, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

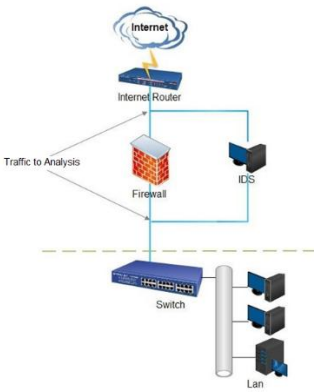


Figure 4: Combined IDS

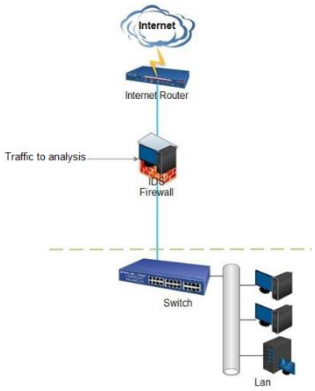


Figure 5: Firewall/NIDS

2.4.4 Firewall/NIDS: With this location the objective is for a single computer to perform the task of firewall and IDs at the same time. Carrying out this configuration requires robust equipment and is usually an expensive solution.

2.5 Network Diagram Design With IDS

Once the different possibilities of installing an ID in the network have been verified, a diagram is made that allows identifying the location of the system in the internal network of the Office of the Trade Commissioner for Al-basrah.

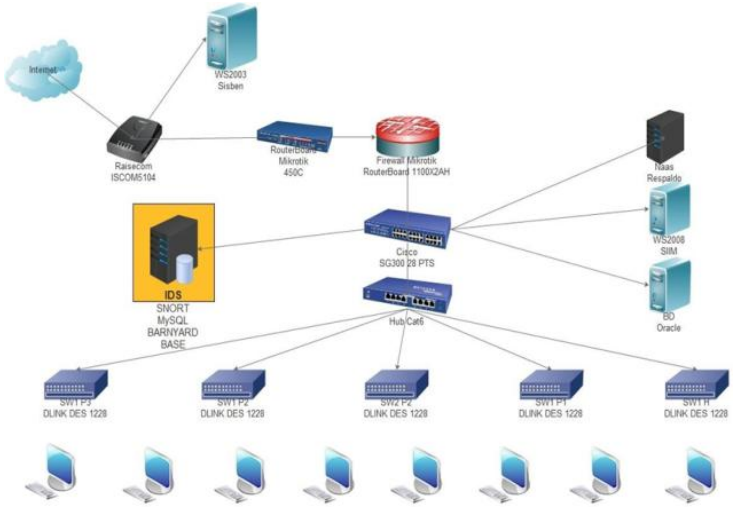


Figure 6. Network diagram with IDS

Within the options analysed above, the configuration of the Ids behind the Firewall was selected. In addition to being another filter behind the firewall, it is also presented as the configuration where all the alerts generated will be hostile or of greater importance, given that the first barrier (firewall) has been overcome, which results in fewer of false alarms for the system. In addition, it also results in the least expensive configuration for implementation, since only one server computer is required unlike the other possibilities.

Received: July 20, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2.6 implementation of the IDS in the data network of the trade commissioner for Al-basrah

To install Snort, it is necessary to disable the Linux security module, so that it does not block any type of installation or configuration. To do this, modify the config file located in the /etc/selinux/config path and make the following changes, as seen in the following figure 7,

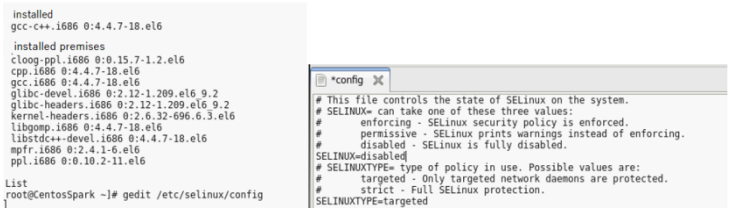


Figure 7. Deactivating Selinux

Likewise, it is necessary to deactivate the iptables firewall by executing the $\#iptables\ -F$ command in the terminal, then saving the changes.

The configuration is then saved with $iptables - save\ > /etc/sysconfig/iptables$

It is also necessary to install Libcap, which is a TCP/IP packet programming library. Initially, the libpcap-1.8.1.tar.gz package is downloaded from the website www.tcpdump.org. After downloading, it is decompressed and compiled by executing the terminal commands.

Snort uses regular expressions for its rules so it is necessary to install the Pcre library that performs this function.

Download the pcre-8.41.tar.gz package from the website (www.pcre.org). Unzip the package: tar xvfz pcre-8.41.tar.gz. Finally, it is compiled and installed by executing the commands.

2.6.1 Snort installation. To start the installation of snort, you must initially download the snort-2.9.9.0.tar.gz package from the website, then unzip it. Finally, it is compiled and installed by executing the commands in the terminal. This process can be seen in the following figure 8.

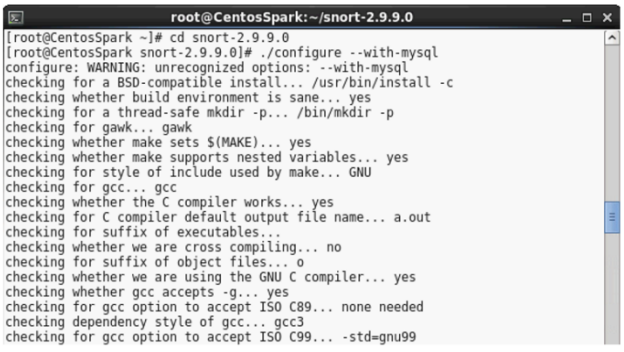


Figure 8. Snort installation

2.6.2 Snort Configuration. As a first step, you must create the folders where snort will work. For this, commands will be used in the Linux terminal. Therefore, the commands used in each step will be shown in figure 9.

Received: July 20, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Now within the created snort folder, another folder is added where the signatures that will be downloaded from the application page are stored.
- Then in the path where the Centos logs are saved, a snort folder is created to store the snort system activity logs.
- It is also required to create a snort user, and give that user permissions to the previously created folder.
- The local configuration file is created in the sysconfig folder in the etc. folder.
- Now the executable is copied to your working directory

The following figure shows the execution of these commands.

```
[root@CentosSpark snort-2.9.9.0]# cd
[root@CentosSpark ~]# mkdir /etc/snort
[root@CentosSpark ~]# mkdir /etc/snort/rules
[root@CentosSpark ~]# mkdir /var/log/snort
[root@CentosSpark ~]# adduser snort
[root@CentosSpark ~]# chown snort /var/log/snort
[root@CentosSpark ~]# touch /etc/sysconfig/snort
[root@CentosSpark ~]# cp /usr/local/bin/snort /usr/sbin
```

Figure 9. Creating snort folders

In addition, it is also necessary to copy certain files extracted from the snort folder to the path of the snort system folder.

Registration was then carried out on the snort website, in order to download the official signatures and unzip them in the $/etc/snort/rules$ folder created previously. Additionally, the folder where the snort preprocessors will be saved is created by executing the command. The preprocessors from the extracted folder were copied to the folder path created earlier, inside the snort folder. The precompiled objects for CentOS version 6.9 are copied to the respective folder.

The snort configuration file, located in the path $/etc/snort/snort.conf$, allows you to configure the system to assign the network address range, library path, and configure the rules, among other functions. As evidenced in the following figures.

The range of IP addresses of the Commissioner's internal network is specified by modifying the HOME_NET variable: var HOME_NET or ANY. To edit said file, it is opened through the Gedit editor, so the console command is executed. Modifying the HOME_NET variable by the network address range.

```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.88.1/24
```

Figure 10. Configuring the network in snort

Next, the directory where the rules are stored is edited, modifying the variable as in figure 11 directory that was created in previous steps.

```
var RULE_PATH /etc/snort/rules
```

Figure 11. Rule configuration

The directory where the preprocessors are located is specified as below,

Received: July 20, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

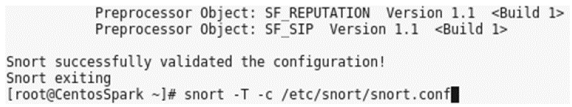
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

```
var PREPROC_RULE_PATH /etc/snort/preproc_rules
```

Figure 12. Configuring preprocessors

After editing the snort.conf file, save the changes and test it with the command $\#snort\ -T\ -c\ /etc/snort/snort.conf$

When performing the test, view the following figure, which shows its correct operation.



2.6.3 MySql installation.

- The Mysql database manager will be used to store the alert data generated by snort, and will also be used by web applications that will display the data from said alerts. To install the MySql server, the following commands must be executed:
  - $\#yum\ install\ mysql-server\ \#yum\ install\ mysql-devel$
- To start the MySQL server run
  - $\#service\ mysqld\ start$
- Connects to MySQL server through terminal.
  - #mysql –u root –p

A test is then carried out to verify that the database engine is installed, and the snort user, the database and the necessary permissions for its operation are created.

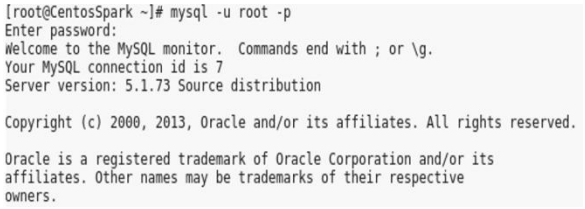


Figure 13. Connecting to Mysql server

Next, all privileges are given to the root user, indicating an access password.

- The snort database is created
- create database snort

Next, the tables for the snort database are created, importing them from the $create\_mysql\ file$, extracted from the /schemas subdirectory of the barnyard application, which was installed earlier. To do this, execute the required command. Then you enter the Mysql server, and enter the password, in this case test, to verify that the tables have been created correctly, for this the following steps were carried out.

- The password is entered. The snort database is selected
- To see the tables that have been created for our snort database, run:

The execution of these commands can be seen in the figure below.

Received: July 20, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

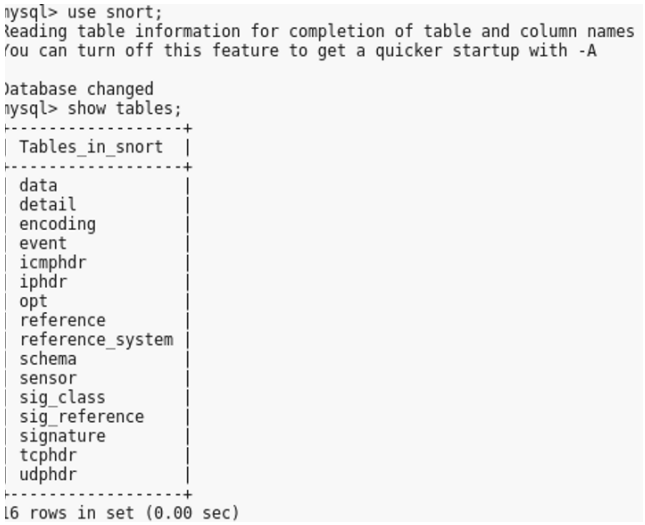


Figure 14. Snort database tables

2.6.4 Barnyard Installation. This is an application that takes the Snort log files and processes them and then saves the data to the snort database that was created earlier in mysql.

To install it, download the compressed package from the web page. Once downloaded, it is decompressed with the command in the console.

$$\#tar\ -xzvf\ v2-1.13.tar.gz$$

Next, enter the extracted folder with the command, inside the folder it is compiled, configured with the mysql library, and installed with the following steps.

- $\#./autogen.sh$
- $\#./configure\ -with-mysql\ -libraries=/usr/lib/mysql/\ \#make$
- $\#make\ install$

- Next the barnyard configuration file is required to be copied to the snort path.
  - $\#\ cp\ etc/barnyard2.conf\ /etc/snort$
- A folder is also created within the log folder, where a Waldo file (blank file) will be stored.
  - $\#mkdir\ /var/log/barnyard2$
- This folder is given permissions to make it modifiable.
  - $\#chmod\ 666\ /var/log/barnyard2$
- The blank file required for barnyard2 is created in the snort folder within the log directory.
  - $\#\ touch\ /var/log/snort/barnyard2.waldo$
- It is also necessary to copy the barnyard2 configuration file to the snort installation path.
  - # cp etc/barnyard2.conf /etc/snort

To finish, it is necessary to configure the barnyard2 configuration file, copied to the snort path. First it is located in the file path, and then the file is opened with the gedit editor. To do this, execute the following lines in the console.

- $\#cd\ /etc/snort/$

Received: July 20, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- $\#gedit\ barnyard2.conf$

This configuration file $barnyard2.conf$ consists of three configuration blocks, where the first part declares the variables, followed by the input configuration, and finally the data output configuration.

Initially, the snort configuration files are located, verifying that they are in the snort directory. The figure where these steps are displayed is presented below.

```
config reference_file:      /etc/snort/reference.config
config classification_file: /etc/snort/classification.config
config gen_file:            /etc/snort/gen-msg.map
config sid_file:            /etc/snort/sid-msg.map
```

Figure 15. Setting up the barnyard file

The next line is then uncommented to locate the barnyard output directory.

$$config\ logdir: /var/log/barnyard2$$

In the lines where the equipment and network interface variables are declared, they are uncommented and edited, giving the corresponding data, as shown below.

$$config\ hostname: localhost\ config\ interface: eth0$$

The path where the waldo file is located is declared, in the log folder.

$$config\ waldo\_file: /var/log/snort/barnyard2.waldo$$

In the second configuration block of the barnyard file, no changes are made, since there is only one entry type for that file, so it is set to default.

Finally, in the last block of the file, the snort database variables are declared, a new line is created, giving the database parameters, as seen in the following figure.

```
output database: log, mysql, user=root password=test dbname=snort host=localhost
```

Figure 16. Database parameters in barnyard

Completing the barnyard configuration saves the changes made to the barnyard2.conf configuration file.

2.6.5 Apache installation. To install Apache, execute the following line from the command line.

$$\#yum\ install\ httpd$$

Next start the server in the terminal with the command shown below.

$$\#service\ httpd\ start$$

Next, write the address $http://localhost$ in the browser and you can see that the Apache server is working correctly, as shown in figure 17.

Received: July 20, 2025

International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

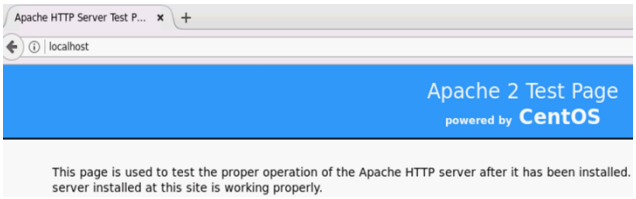


Figure 17. Apache installation

Likewise, the php-mysql library is also needed to make connections to the mysql database. Just as the php language is needed to support the previously installed Apache web server.

2.6.6 Base Installation. The installation of php and apache was carried out, which are required for the base to function, which is nothing more than a graphical interface that allows you to view and analyze the intrusions detected and stored by snort, it processes them to display them comfortably through its Interface. Below are the steps that were followed for its installation.

First, download the base-1.4.5.tar.gz package from the website: $http://base.secureideas.net/$.

Next, unzip the package into the $/var/www/html\ directory$:

$$\#cp\ base-1.4.5.tar.gz\ /var/www/html\ \#cd\ /var/www/html$$

$$\#tar\ xvfz\ base-1.4.5.tar.gz\ \#mv\ base-1.4.5\ base$$

The base folder has been copied to the www folder of the apache server. But this is not enough for it to work, it was also required to have the Adodb and Image_Graph packages installed.

To install Adodb you must perform the following steps:

Download the adodb5.20.9 package from the web page

Unzip the package and copy it into the $/var/www/$ folder:

It is also necessary to install the following elements, so that Base can graph.

- #yum install php - pear
- #pear install Image_Canvas - alpha #pear install Image_Color
- #pear install Numbers_Roman #pear install Image_Graph - 0.8.0

The web server is started through the console command, in which the apache service is httpd.

$$\#service\ httpd\ start$$

The BASE Web page is accessed through a web browser, indicating the local IP of the server or localhost, followed by the Base folder. It shows the following screen when starting, where it is configured through the Setup Page option.

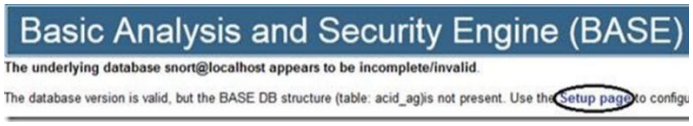


Figure 18: Base Screen

Received: July 20, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Next, the path to adodb hosted in the Apache www folder was configured, as shown below.

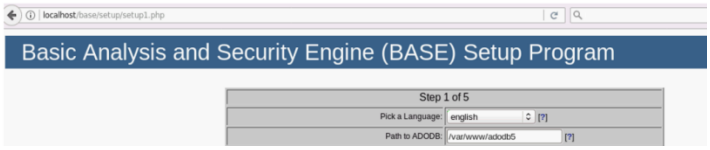


Figure 19: Configuring Base

In the next configuration step, the database data such as database name, host, user, password is configured and then the query is submitted.

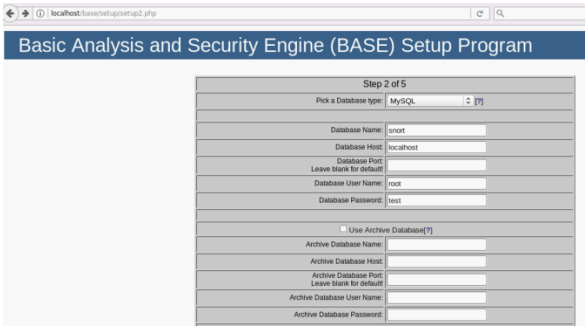


Figure 20. Configuring the database

The following screen is presented below where user data is requested to log in and connect to the database created in Mysql.

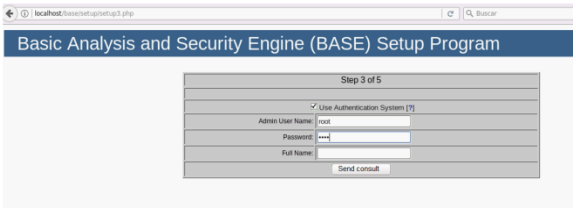


Figure 21. Finishing the Base configuration

The following figure is shown where Create Base AG is pressed to add tables to the Snort database.

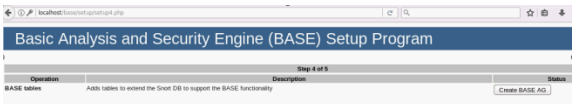


Figure 21. Adding tables to Snort

At the end of the process that began in the previous step, the following figure is displayed, where it can be seen that the process ended and that it was successful.

Received: July 20, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 22. Base finished process

Once the process is finished, it requests to log in with the previously established data such as the username and password, as presented in the following figure.

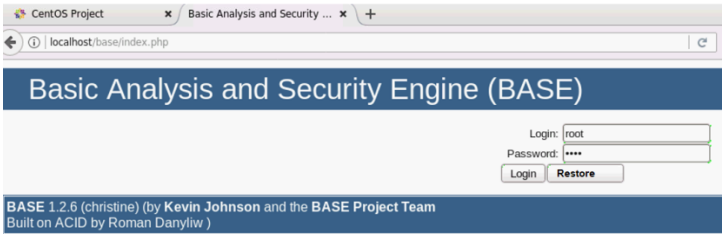


Figure 23. Logging into Base

Once logged in to Base, you can access the snort information stored in the database, as well as view the alerts that are generated.

3. Results and discussion

4.1 IDS tests in the data network of the trade commissioner for Al-basrah.

The installations and configurations of the tools and applications necessary for the correct functioning of the intrusion detection system with Snort were carried out, as well as the network configuration. For the system to work, application services need to be started, such as $mysql, apache$ and finally snort.

But before starting the application services, Snort specifically allows you to perform a test that it is installed correctly, also specifying the path of the .conf file that was configured previously. The figure below shows the command used for said test.

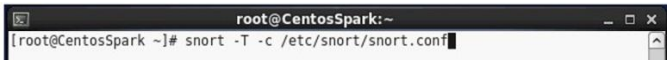


Figure 24. Testing Snort

Once the command has been executed in the console, the testing process begins by verifying each of the elements detailed in the configuration file, as seen in the following figures.

Received: July 20, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

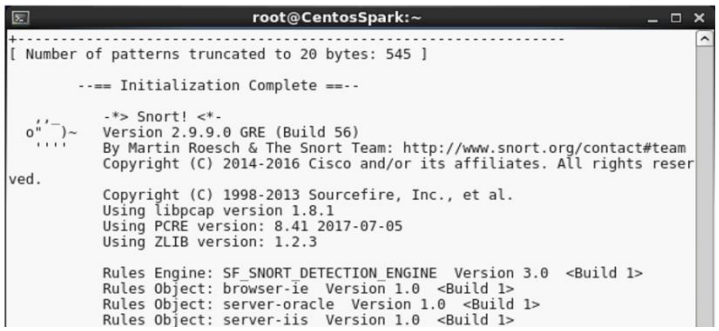


Figure 25. Snort testing process

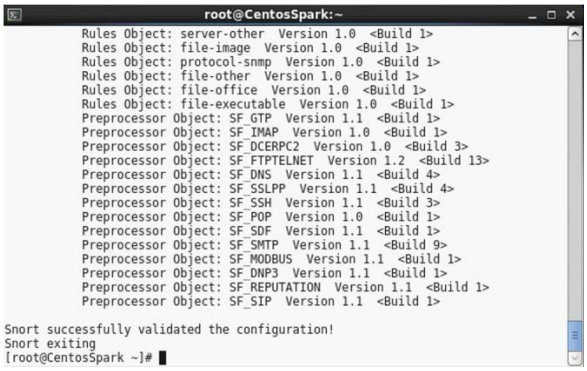


Figure 26. Successful Snort tests

Once the snort verification test is complete, it shows that the configuration was successfully validated. Once these services were started, they have remained in operation for several days, to collect data, and then analyse the data obtained.

At the first start of the Base application, you can verify the analysis of the information based on the snort database. Allowing you to view in the first instance the traffic analysis by Tcp (1%), Udp (98%), and $Icmp$ (1%).

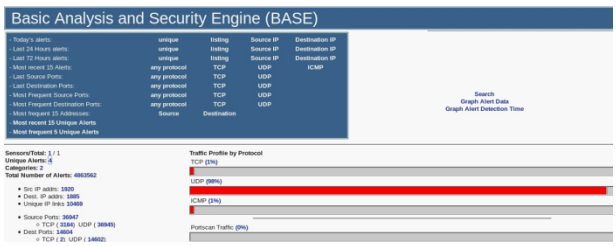


Figure 27. Baseline Analysis

On the left side appears a panel that details in summary by elements, the number of sensors working, alerts detected, total alerts, as well as the IP addresses involved, whether source or destination.

Another important data that it details is the number of unique alerts, four in this analysis, grouping them into 2 categories. Likewise, the total number of alerts (4863562), total number of port scans, among other data. By selecting each of the options shown in the menu, you can

Received: July 20, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

view detailed information about each of these, allowing for a more exhaustive analysis of the captured data.

For an alert to be established through captured packets, it is necessary for the detection engine to act through the information captured by the libcap packet decoder. The detection engine is responsible for detecting if any intrusion activity exists in a packet, using the rules that have been defined for this purpose. The rules are checked against all packets. If a package meets the definition of the rule, the alert system will generate a log or an alert stored in the mysql database.

The visualization of the data obtained is provided by the Graph Alert Data option, which allows the data to be graphed according to the options that the user needs. An example of these is the graph obtained from the number of alerts that were generated in a day. This example can be seen in the following figure.

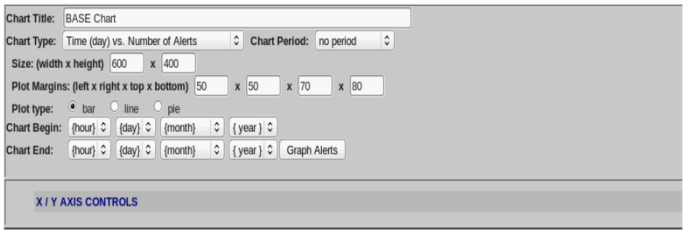


Figure 28. Number of alerts presented per day

Among the alerts that were generated when executing the intrusion detection system, the following alerts could be seen, as shown in the following figure.

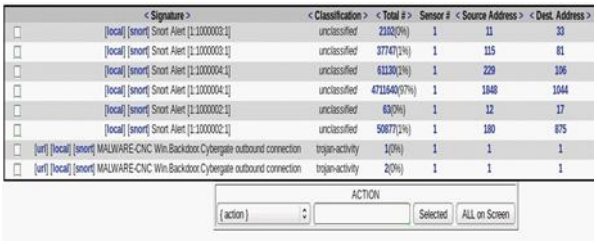


Figure 29. Alerts generated

It can be seen that one of the alerts generated corresponds to the classification of “Trojan activity”, that is, the activity of a Trojan of the Backdoor type or that was infected through a backdoor; The following figure shows in detail the IP from where the alert was generated, the sensor that detected it, and the times it occurred.

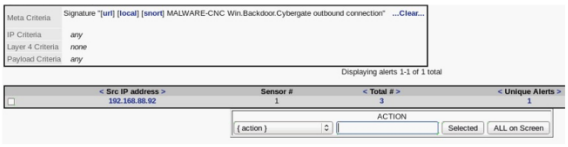


Figure 30. Detail of generated alert

Received: July 20, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Another of the alerts generated also corresponds to the same type of Trojan, where the activity of malware is evident that affects a machine on the Commissioner's network and that can affect several computers and put user information at risk. Below is the detail of the alert generated in figure 31.

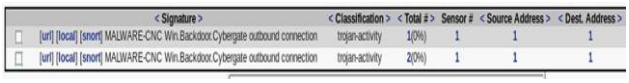


Figure 31. Alert detail

For this type of alerts generated by the system, an immediate action plan must be made to eliminate these threats from the network. Verifying the total elimination of said Malware on each of the infected computers.

After the malware is eliminated, these system alerts are deactivated, and the network is scanned again in search of new intrusions or anomalies in the network.

With this analysis of the network, it was evident that the installed solutions such as a firewall or physical firewall and antivirus are not enough to avoid computer attacks with malware, which put information security at high risk. With the implementation of the intrusion detection system, an additional layer of security is provided to the networks, allowing system administrators to quickly act on the alerts generated by the system.

4.2 Result to Deliver

An intrusion detection system launched in the internal network of the Trade Commissioner's office will be delivered, for which the free software Snort will be used, which runs on Linux platforms, so it is necessary to have a server computer.

Thanks to Snort, which is a network-based intrusion detection system, which provides alerts and notifications against unauthorized access to the internal computer infrastructure, the objectives set out in this project would be achieved.

4. Conclusions

With the review of the current network of the Trade Commissioner's office, the need to add another level of security was evident, through a tool that would detect intrusions that have surpassed the first security barrier, in this case the firewall. After an analysis of the types of ids, within which host and network types were found, as well as paid and other open source; the type of ids to be implemented could initially be determined; which for the Office of the Trade Commissioner for Al-basrah required a network type that would carry out analysis and monitoring of the entire organization. In addition, a great variety of open-source tools were found, which met the demands and requirements of the implementation, adapting and configuring themselves to the development of the project. With the implementation of the intrusion detection system through free software tools, there is a server that monitors the network traffic of the Office of the Trade Commissioner for Al-basrah. This traffic is stored in the mysql database, providing a historical record of everything that has happened since its

Received: July 20, 2025

Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

implementation, providing an auditing tool, identifying the source and destination IP addresses, as well as the ports and protocols scanned in the traffic. The intrusion detection system requires continuous monitoring by network administrators to notify machine users, given that the system alone is not capable of giving warning or identifying whether the intrusion was successful or not. It is of great importance to have developed the project through free software tools, from the operating system through databases, to other complementary tools that integrate the detection system, providing multiple adaptation and configuration possibilities, greatly reducing the costs. implementation costs of said system.

Competing interests

The authors have declared that no competing interests exist

References

[1]. Abrahams, Temitayo & Ewuga, Sarah & Dawodu, Samuel & Adegbite, Abimbola & Hassan, Azeez. (2024). A REVIEW OF CYBERSECURITY STRATEGIES IN MODERN ORGANIZATIONS: EXAMINING THE EVOLUTION AND EFFECTIVENESS OF CYBERSECURITY MEASURES FOR DATA PROTECTION. Computer Science & IT Research Journal. 5. 1-25. 10.51594/csitrj.v5i1.699.

[2]. Rao, U.H., Nayak, U. (2014). Intrusion Detection and Prevention Systems. In: The InfoSec Handbook. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4302-6383-8_11

[3]. Li, Xiaowei & Xue, Yuan & Malin, Bradley. (2012). Detecting Anomalous User Behaviors in Workflow-Driven Web Applications. Proceedings of the IEEE Symposium on Reliable Distributed Systems. 1-10. 10.1109/SRDS.2012.19.

[4]. Ibor, Ayei & Epiphaniou, Gregory. (2015). A Hybrid Mitigation Technique for Malicious Network Traffic based on Active Response. International Journal of Security and its Applications. 9. 63-80. 10.14257/ijsia.2015.9.4.08.

[5]. Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R. *et al.* Review and insight on the behavioral aspects of cybersecurity. *Cybersecur* **3**, 10 (2020). https://doi.org/10.1186/s42400-020-00050-w

[6]. Khraisat, A., Gondal, I., Vamplew, P. *et al.* Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecur* **2**, 20 (2019). https://doi.org/10.1186/s42400-019-0038-7

[7]. Ozkan Okay, Merve & Samet, Refik & Aslan, Ömer & Gupta, Deepti. (2021). A Comprehensive Systematic Literature Review on Intrusion Detection Systems. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3129336.

[8]. Lodgaard, Eirin & Gamme, Inger & Aasland, Knut. (2013). Success Factors for PDCA as Continuous Improvement Method in Product Development. IFIP Advances in Information and Communication Technology. 397. 645-652. 10.1007/978-3-642-40352-1_81.

[9]. Dini P, Elhanashi A, Begni A, Saponara S, Zheng Q, Gasmi K. Overview on Intrusion Detection Systems Design Exploiting Machine Learning for Networking

Received: July 20, 2025

Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Cybersecurity. *Applied Sciences*. 2023; 13(13):7507. https://doi.org/10.3390/app13137507.

[10]. Luaay Abdul Wahed Shihab, Wireless LAN Security and Management, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-1, October 2012.

[11]. Luay Abdulwahid Shihab, Study and Evaluation of Wireless Sensor Networks Performance, Webology, Volume 19, Number 1, January, 2022.

Received: July 20, 2025