Engineering Applications

https://publish.mersin.edu.tr/index.php/enap

e-ISSN 2979-9201

Possibility of protection against unauthorized interference in telecommunication systems

Fatmir Basholli [*1], Adisa Daberdini [2], Armand Basholli [3]

[1]*Albanian University, Department of Engineering, Tirana, Albania, fatmir.basholli@albanianuniversity.edu.al*
[2]*Aleksander Xhuvani University, Informatics Department, Elbasan, adisa.daberdini@uniel.edu.al*
[3]*Vodafone Albania/Safety & Security Lead, Tirana, Albania, armand.basholli@vodafone.com*

Cite this study: Basholli, F., Daberdini, A., & Basholli, A. (2023). Possibility of protection against unauthorized interference in telecommunication systems. Engineering Applications, 2 (3), 265-278

Keywords
Prevention
Interloper
Information
Protocols
Privacy

Research Article
Received: 26.03.2023
Revised: 26.09.2023
Accepted: 01.11.2023
Published:06.11.2023

Abstract

Historically, the concept of ownership has dictated that individuals and groups tend to protect valuable resources. Regardless of how much protection is given to the property, there is always a weak point, where the security provided can fail at certain points. This general notion has guided the concept of systems security and defined the disciplines in cyber security and especially that of computer networks. Computer network security consists of three principles: prevention, detection and response. Although these three are the basic components of security, the main focus is on detection and prevention resources because if we are able to detect and prevent all security threats, then there is no need for reaction and response. Intrusion detection is a technique of detecting unauthorized access to a computer system or a computer network. An intrusion into a system is an attempt by an outsider to gain illegal access to the system. Intrusion prevention, on the other hand, is the art of preventing unauthorized access to a system's resources. The two processes are related in a sense, where intrusion detection passively watches for intrusions into the system, and intrusion prevention actively filters network traffic to prevent intrusion attempts. In the continuation of the treatment, we will focus on these two processes.

1. Introduction

The notion of intrusion detection in computer networks is not a new phenomenon but born around 1980 and addressed by a paper by James Anderson in the paper "Computer security, threat monitoring and surveillance". In his study, Anderson noted that through computer audit trails we gain vital information that can be valuable in tracking misuse and understanding user behavior. The paper introduced the concept of "detection" of abuses and specific user events and encouraged the development of intrusion detection systems.

An intrusion is a deliberate unauthorized attempt, successful or not, to break the security, gain access, manipulate or misuse some valuable information and where the misuse can result in its deformation making it unreliable or unusable. This action could be performed by a person who is often called an intruder.

The process of breaking into a system involves a series of stages that begin with target identification, followed by reconnaissance that provides as much information about the target as possible. Once sufficient information is gathered about the target and vulnerabilities are mapped, the next step is to gain access to the system and finally the actual use of system resources. Let's see below the methods followed in each of these phases [1,2].

2. Material and Method

2.1. Disclosure

Discovery is the process of gathering information about the target system, details of its operation, and weak points. Hackers rarely attack an organization's network before they have gathered enough information about the

target network. They collect information about the type of information used on that network, where it is stored, how it is stored, and the weak point of access to that information. They do detection by scanning the system for vulnerabilities.

Vulnerability assessment is an automated process in which a scanning program sends network traffic to all computers or selected computers on the network and waits for traffic to return that will indicate whether those computers have known vulnerabilities. These vulnerabilities may include vulnerabilities in operating systems, application software, and protocols. Once they have identified the vulnerability of the target system, then they simply log in to perform an intrusion into the system [3].

2.2. Physical interference and denial of service

In addition to scanning the network for information that will eventually enable intruders to illegally access an organization's network, intruders can also access an organization's network masquerading as a legitimate user. They can do this in a number of ways ranging from obtaining special administrative privileges to low-privilege user on system accounts. If the system does not have the latest security patches (updates), it may not be difficult for a hacker to gain these privileges. The intruder could also gain remote access privileges.

Denial-of-service (DoS) attacks are where an intruder tries to crash a service (or machine), overload network connections, overload the CPU, or fill up (block) the hard drive. This intruder is not trying to gain information, but simply act as a vandal to stop you from using your machine (computer) [4].

2.3. Risks of System Interference

The risks of system tampering are numerous, including the following:

• Loss of personal data that can be stored on a computer which means the loss of a lot of personal data for different people depending on the internal interference with the current or accessed data. More alarming in personal data is the way digital information is lost which is not the same as the loss of physical data. In the case of physical data loss, if it is stolen, then someone has it, so you can take precautions. For example, you can report to the police and call your credit card issuer. Physical loss is not the same as digital loss because in digital loss you may never know your data is lost. Hackers can break into your system and copy your data and you'll never know. Therefore, we emphasize that the damage from the loss of personal digital data can be much greater.

• Compromising privacy for many people who keep their personal data online, either through the use of credit or debit cards. In addition, most information about an individual is stored online by companies and government organizations. When a system that stores this type of data is compromised, a lot of individual data is compromised. In any case that the organization's computer network is compromised, the information of individuals is also at risk and their privacy is compromised [5].

• Legal liability where you are potentially liable for damages caused by a hacker breaking into your network or using your computers to break into other systems if your organization's network has personal customer information and it is breached, thereby compromising the information that you have saved. For example, if a hacker does two- or three-level hacking using your network or a computer on your network, you could be held liable. A two-level hack involves a hacker breaking into your network and using it to launch an attack on another network.

2.4. Intrusion Detection Systems (IDS)

An intrusion detection system (IDS) is a system used to detect unauthorized intrusions into computer systems and networks. Intrusion detection as a concept and technology is not new, it has been used for generations to protect valuable resources. Kings, emperors and nobles who had wealth used it in a very interesting way. They built castles and palaces on mountaintops and sharp cliffs with watchtowers to provide them with a clear view of the lands below where they could detect any attempt early and defend themselves. Empires and kingdoms rose and fell based on how well they organized this defense from surrounding enemies and the ability they had in reconnaissance. Over the years, intrusion detection has been used by individuals and companies in a variety of ways, including erecting roads and fences around valuable resources (assets), with watchtowers to watch activities surrounding the asset's premises. Individuals have used dogs, facility lighting, electronic fences, closed-circuit television (cameras) and other surveillance devices to be able to detect intrusions. Security companies are popping up everywhere to provide individual and property security to be a watchful eye so the owner can sleep or take a restful vacation. Intrusion detection mechanisms can be put into three models: anomaly-based detection, signature-based detection, and hybrid detection.

In anomaly detection, also known as behavior-based detection, the focus is on detecting behavior that is not normal or behavior that is inconsistent with normal behavior. In theory, this type of detection requires a list of what is normal behavior, however in most environments this is not possible. In real-life models, the list is

determined by historical or empirical data. However, neither historical nor empirical data represent all possible acceptable behaviors. So, a list should be constantly updated as new patterns of behavior emerge that are not on the list classified as acceptable or normal behavior. The danger with this model is that unacceptable behavior is found included in the training data and later accepted as normal behavior. Therefore, detections of behavior-based interventions are also findings as rule-based detection, because they use rules, usually developed by experts, to be able to define unacceptable behavior.

In signature-based detection, also known as exploit-based detection, the focus is on the signature of known activities. This model also requires a list of all actions of unacceptable knowledge or misuse of signatures. Since there are an infinite number of things that can be classified as abuse, it is not possible to list them all and still keep it manageable. So only a limited number of things should be on the list.

To do this and to be able to manage the list, we categorize the list into three broad activities:

- Unauthorized access
- Unauthorized modification
- Denial of service

Using these classifications, it is then possible to have a checklist of abuses whose signatures can be determined. The problem with this model is that it can only detect previously known attacks. Due to difficulties with both anomaly-based and signature-based detections, a hybrid model is being developed. Much research is now focusing on this hybrid model [6].

2.5. Detection of anomalies

Anomaly-based systems are "learning" systems in the sense that they operate by continuously creating "norms" of activities. These rates are later used to detect abnormalities that may indicate an intrusion. Anomaly detection compares observed activity against expected normal usage profiles. Profiles can be developed for users, user groups, applications, or system resource usage.

In anomaly detection, it is assumed that all intrusive activities are necessarily anomalous. This also happens in real life, where most "bad" activities are bad anomalies and we may therefore be able to profile the character of "bad elements" in society. The concept of anomaly detection will create, for everything stored in the system, a corresponding database of "normal" profiles. Every activity in the system is checked against these profiles and considered acceptable or not based on the presence of such activity in the profile database.

Typical areas of interest are threshold monitoring, user job profiling, batch job profiling, resource profiling, executable profiling, static job profiling, and rule-based profiling. Anonymous behaviors are detected when the identification engine takes observed activities and compares them to rule-based profiles to highlight significant deviations. Profiles are typically for individual users, groups of users, system resource usage, and a collection of other values as discussed in [7]:

- The individual profile summarizes a collection of common activities that a user is expected to do and with few deviations from the expected norm.
- The group profile is a profile that covers a group of users who do a common job and use historical resources and activities.
- Resource profiling includes monitoring of system resource patterns such as applications, accounts, storage media, protocols, communication ports, and a list that the system manager may want to include.
- Other profiles include executable profiles that monitor how much system resources and executable programs are used. For example, this can be used to monitor strange deviations of an executable program if it has an embedded Trojan worm or a trapdoor virus.

In addition to executable profiles, there are also profiles that include port monitoring, monitoring the historical usage patterns of all other profiles, and using them to make updates to the rule base.

Anomaly detection systems are also computationally expensive due to the overhead of keeping track of and possibly updating some system profile metrics.

2.6. Disclosure of Misuse

Unlike anomaly detection where we label each intrusive activity as an anomaly, the Malfunction Detection Concept assumes that each intrusive activity is represented by a unique pattern or signature so that small variations of the same activity produce a new signature and for therefore it can be discovered. Malfunction detection systems are commonly known as signature systems. Malfunction pattern analysis is best done by expert systems, pattern-based reasoning, or neural networks.

Two main problems arise from this concept:

• The system cannot detect unknown attacks with unmapped and unarchived signatures.
• The system cannot predict new attacks and therefore will respond after an attack has occurred. This means that the system will never detect a new attack.

Identification of intrusions into the system is supposed to identify three categories of users: legitimate users, legitimate users performing unauthorized activities, and of course intruders who have illegally obtained the required identification and authentication.

3. Results

3.1. Types of intrusion detection systems

Intrusion detection systems are also classified based on their monitoring scope. There are those that monitor only a small area and those that can monitor a wide area. Those that monitor a wide area are known as network-based intrusion detection and those that have a limited scope are known as host-based detections.

3.2. Network-based intrusion detection systems (NIDS)

Network-based intrusion detection systems have the entire network as the monitoring scope. They monitor network traffic to detect intrusions. They are responsible for detecting anomalous, inappropriate or other data that may be considered unauthorized and harmful to what happens on a network. There are fundamental differences between NIDS and firewalls.

Only when the traffic matches an acceptable pattern is it allowed to proceed regardless of what the packet contains. A NIDS also captures and inspects every packet that is destined for the network, regardless of whether it is allowed or not. If the packet signature based on the packet contents is not among the acceptable signatures, then an alert is generated.

There are several ways a NIDS can be run. It can either be run as a stand-alone where it randomly monitors all network traffic or it can simply monitor only the target machine that monitors its own traffic. For example, in this mode, it can watch itself to see if someone is trying to intrude with a SYN (flood) or perform a TCP port scan.

While NIDSs can be very effective at capturing all incoming network traffic, it is possible that an attacker can evade this detection by exploiting ambiguities in the traffic flow seen by the NIDS [8].

• Many NIDS do not have the full analysis capabilities to analyze the full range of behavior that can be exposed by the user and allowed by a given protocol. The attacker can also evade NIDS, even if NIDS performs protocol analysis.
• Since NIDSs are remote from individual hosts, they do not have complete knowledge of each host's protocol implementation. This knowledge is essential for NIDS to be able to determine how the host might handle a particular sequence of packets if different implementations interpret the same packet stream in different ways.
• Again, since NIDSs do not have a complete view of the network topology between the NIDS and the host, the NIDS may not be able to determine whether a given packet will be seen by the hosts.

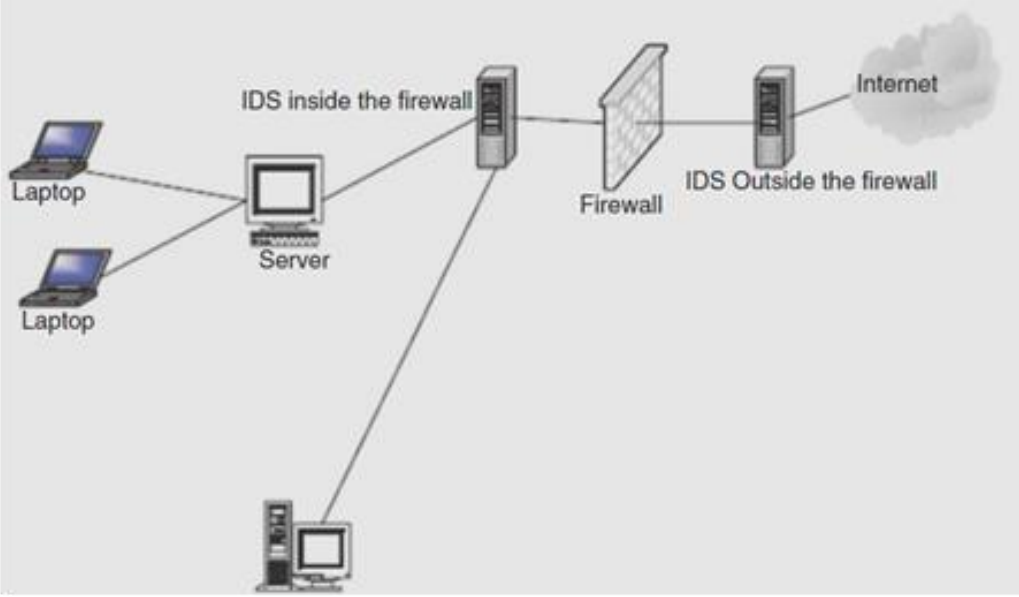

Figure 1. Architecture of a network-based intrusion detection system.

3.2.1 Network-based intrusion detection architecture

An intrusion detection system consists of several parts that must work together to produce an alarm. The operation of these parts can be either sequential or sometimes parallel [9]. The parts are shown in Figure 1.

The network tap/load balancer, or load balancer as it is commonly known, collects data from the network and distributes it to all the network sensors. It can be a software agent running from the sensor or device, such as a router. A load balancer or faucet is an important component of an intrusion detection system because all network traffic passes through it and it also prevents packet loss in high-bandwidth networks. Some types of "taps" have restrictions on the environments they can be chosen to be deployed in, such as switched networks. In networks where there are no load balancers, sensors should be deployed in such a way that they are responsible for the traffic entering the network and their respective subnet.

Network Sensor/Monitoring is a computer program that works to detect machines or network devices in mission critical segments. In networks with a load balancer, sensors receive traffic from the load balancer. In other networks without a load balancer, sensors take traffic directly from the network and separate it between suspicious and normal traffic. A sensor can be implemented as an agent on a mission-critical destination machine in a network. They are either anomaly-based or signature-based.

The analyzer determines the threat level based on its nature and the threat of suspicious traffic. It receives data from sensors. The traffic is then classified as either safe or an attack. Several layers of monitoring can be performed where the primary layer determines the severity of the threat, then the secondary layers determine the extent, scope and frequency of the threat.

The whistleblower contacts the security officer responsible for incident handling whenever a threat is severe enough according to the organization's security policy. Standard capabilities include on-screen alerts, audio alerts, paging, and e-mail. Also, most systems provide SNMP so that an administrator can be notified. Frequent alerts on seemingly trivial threats should be avoided because they result in a high rate of false positives. It should also be noted that non-reporting quite often occurs because sensors are deployed in such a way that they ignore a variety of threats, many of them being real, resulting in false (negative) which results in not detecting system intrusions while providing a sense of security. deceptive.

Because the performance of an intrusion detection system depends on balancing false positives and false negatives, it is important to use damage estimation from intrusions or other investigative tasks. Useful information need not necessarily be indicative of misuse. Behavioral statistics help develop models for the individual and misuse statistics help detect intervention efforts. Detection systems that are adjustable can provide balancing capabilities.

The command panel/manager is to act as a command with central authority to control the entire system. It can be used to manage threats by directing incoming network data either to a firewall or load balancer or directly to routers. It can be accessed remotely so that the system can be controlled from any location. It is usually a dedicated machine (Workstation) with a set of tools for setting policies and processing collected alerts. The response subsystem provides the capabilities to take action based on threats to target systems. These responses may be automatically generated or initiated by the system operator. Common responses include reconfiguring a router or firewall and closing a connection. The database is the repository of knowledge for the entire intrusion detection system that it has observed. This can include both behavioral and abuse statistics. These statistics are necessary to model patterns of historical behavior that may be useful during damage assessment or other investigative tasks. Useful information need not be indicative of misuse. Behavioral statistics help develop the model for the individual and abuse statistics help detect attempts to intervene.

Deployment of IDS sensors. The placement of network IDS sensors actually depends on several factors, including the topology of the internal network to be protected, the type of security, the policies the organization follows, and the types of security practices in place.

For example, you want to place sensors in places where intrusion is most likely and these are the "weak" points of the network. However, it is normal practice to deploy IDS Sensors in the following areas [10]:

• Inside the DMZ is probably the most ideal place to deploy any detection system because almost all attacks enter the protected internal network through the DMZ. Therefore, IDS sensors are usually placed outside the first firewall of the organization's network in the DMZ. IDS sensors in the DMZ can be enhanced by placing them in specific areas. Another good location for IDS sensors is inside any firewall. This placement gives the sensor more protection, making them less vulnerable to coordinated attacks. In cases where the network perimeter does not use a DMZ, then ideal locations can include any entry/exit point such as on both sides of the firewall, dial-up servers and connections to any partner network.

• Between the firewall and the Internet, is a frequent area of unauthorized activity. This position allows NIDS to "see" all Internet traffic as it comes into the network. However, this location needs a good device and sensors that can handle the high traffic volume.

• Behind the front of the network firewall is a good position, where however, most of the bad network traffic is already stopped by the firewall. All bad traffic that manages to pass through the firewall is handled there.

• Within the network, it is usually placed at strategic points and used to "see" network segments. Network segments like these are usually the suspects in weak network areas. The problem with this approach is that the sensors may not be able to cover all the intended targets. It can also cause network performance to degrade. Figure 2, shows the different places where ID sensors can be placed.

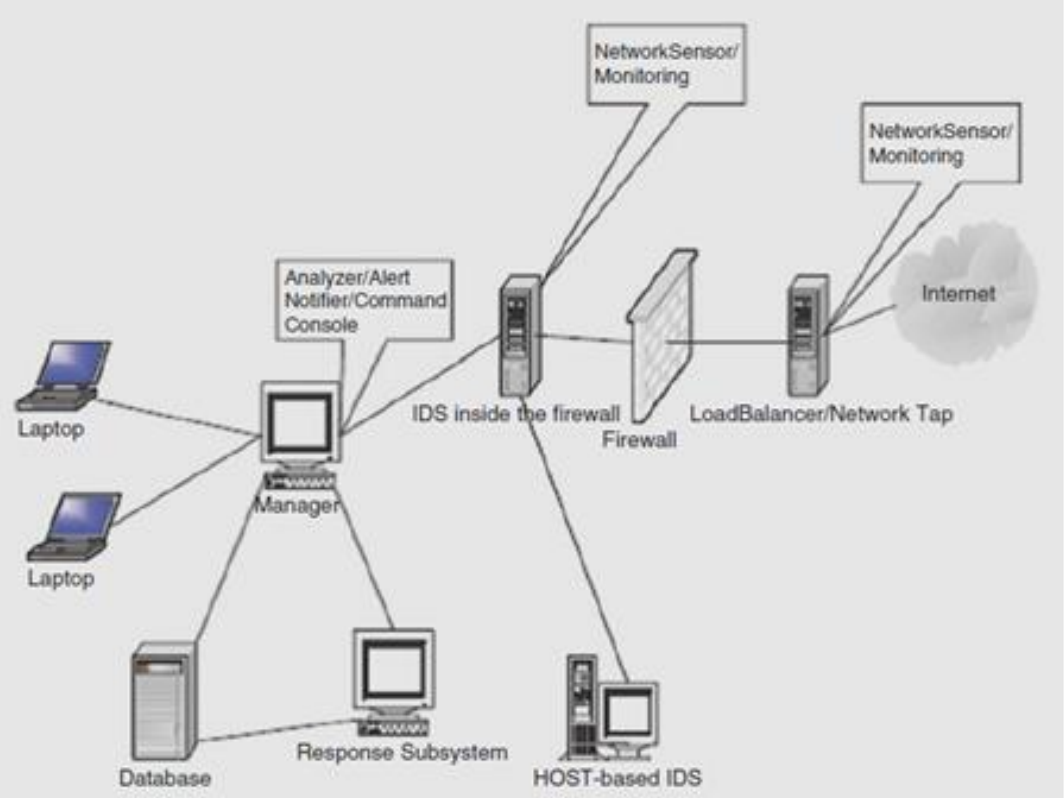

Figure 2. The various places of placing the IDS sensors.

3.2.2. Advantages of network-based intrusion detection systems

Although both NIDS and HIDS have different focuses, the fields, deployment and deployment requirements and the use of NIDS have the advantages as follows [11]:

• The ability to detect attacks that a host-based system would miss, because NIDS are on dedicated machines that are routinely protected, it is more difficult for an attacker to remove evidence that it is with HIDS that are nearby or on the attacker's tables. Also, since NIDSs use live network traffic and it is this traffic that is captured by NIDSs when there is an attack, this also makes it difficult for an attacker to remove evidence.

• Real-time detection and response are best suited to strategic network access points; they are able to detect foreign network intrusions in real time and receive reports as soon as possible from the administrator to provide a quick and convenient response. Real-time notification, which many NIDS now have, allows for a quick and appropriate response and enables administrators not to leave intruders too much time for targeted surveillance.

• The ability to detect unsuccessful attacks and malicious intent because HIDSs are inside the protected internal network, which many types of attacks never come into contact with since such attacks are often stopped from outside the firewall. NIDSs, especially those in the DMZ, encounter these attacks (those escaping the first firewall) that are later rejected by the internal firewall, and those targeting DMZ services that have been allowed by the external firewall. In addition to indicating these attacks, NIDS can also record the frequency of these attacks.

3.2.3. Disadvantages of NIDS

Although NIDS are very suitable for monitoring all data entering the network, they have limitations [12]:

• Located at the boundaries of an organizational network, NIDS is blind to the entire internal network. Since sensors are placed at specific points, especially and mainly in switched networks, NIDSs have blind spots that sometimes-entire network segments cannot see.

• One of the main weaknesses of NIDS is in encrypted data. They have no ability to decrypt encrypted data. Although they can scan unencrypted parts of the packet such as headers, they are useless for the rest of the packet.

3.3. Host-based intrusion detection systems (HIDS)

Recent studies have shown that the problem of misuse of organizational information is not limited to "bad" outsiders, but the problem is more rampant within organizations. To address this problem, security experts have turned to inspecting systems within an organizational network. This local inspection of systems is called Host Based Intrusion Detection Systems (HIDS).

Host-based intrusion detection is the technique of detecting malicious activities on a single computer. Therefore, a host-based intrusion detection system resides on a single computer and uses software that monitors the operation of specific system logs, including the system, event, and security logs on Windows systems. When a change is detected in any of these files, HIDS compares the record with its configured signatures to see if there is a match. If a match is detected, then this signals the presence of illegal activity.

Although HIDS can be placed on a single computer, they can also be placed on a remote host, or they can be placed on a segment of a network to monitor a section of the segment. The data collected, which can sometimes be overwhelming, is compared to the rules in the organization's security policy. The biggest problem with HIDS is that given the amount of data logs generated, such raw data analysis can impose a large overhead not only on the processing power required to analyze this data but also on security personnel needed to review data.

Host sensors can also use user-level processes to check the main system files and executables to periodically calculate their checksum and report multiple changes during the check.

3.3.1. Advantages of host-based intrusion detection systems

HIDS are new intrusion detection methods for a large number of illegal activities in organizations' networks that actually originate from within employees. Over the following years where advanced technology is applied, HIDS technology has also advanced a lot. Many organizations are discovering the benefits of HIDS for security in general. In addition to being faster than the options offered by NIDS, they offer additional advantages including the following [13]:

• The ability to quickly verify the success or failure of an attack, because they record continuous events that actually happened, they have information that is more accurate and are less prone to false positives than the options that NIDS provides. - of. This information can accurately infer whether an attack was successful or not and a response can be initiated early. In this role, they complement NIDS, not as an early warning, but as a verification system.

• Level monitoring on a local host, where they are able to do so on low-level local activities such as file accesses, file permission changes, attempts to install new executables or attempts to access services privileged access, changes to key system files and executables, and attempts to overwrite vital system files or install Trojan horses or hack back doors. These low-level activities can be detected very quickly and reporting is quick and timely to enable the administrator for an appropriate response. Some of these low-level attacks are so small and far less intense that no NIDS can detect them.

• Near real-time detection and response, HIDSs have the ability to detect activities on target hosts and report them very quickly to the administrator at near real-time speeds. This is possible because the operating system can recognize the event before any IDS, in which case, an intruder can be detected and stopped before substantial damage is done.

• Ability to deal with coded environments. In a congested network, it can be difficult to determine where to place a network-based IDS to achieve sufficient network coverage. This problem can be solved by using traffic mirroring on switches and administrative ports, but not as effectively. HIDS provides the greater visibility needed in these environments by deploying to as many critical hosts as needed. In addition, because operating systems see incoming traffic after the encryption has already been decrypted, HIDSs that monitor operating systems can deal better with these encryptions than NIDSs, which may sometimes not deal with them at all. them.

• Cost effectiveness because no additional equipment is needed to install HIDS, it can provide huge savings to the organization. This compares favorably with the huge installation costs of NIDS that require dedicated and expensive servers. In fact, in large discontinuous networks that require a large number of NIDS per segment, this cost can increase.

Disadvantages of HIDS. Like detection by NIDS, HIDS have limitations in what they can do. These limitations include the following [14]:

• Myopic view, since they are located on a host, they have many limitations in the network view.

• Since they are close to the users, they are more susceptible to illegal intrusions.

3.4 Hybrid Intrusion Detection System

We have concluded that there is a need for both NIDS and HIDS, each patrolling its own area of the network to check for unwanted and illegal network traffic. We also note the advantages of not using one over the other and of

using one to complement the other. In fact, we come up with an assessment of how complementary these two intrusion detection systems are. Both bring network security to their strengths and weaknesses that best complement and add to network security. However, we also know and have observed that NIDS have historically been unable to work successfully on switched and encrypted networks, and as we have discussed above, both HIDS and NIDS have not been successful on networks with high speed whose speed exceeds 100 Mbps. This raises the question of a hybrid system that contains all the things each system has and the things each system lacks, a system with both components. Having both components provides greater flexibility in their deployment options. Hybrids are new options and need a lot of support to gain from the two distinct options. However, their success will depend to a large extent on how well the interface receives and distributes incidents and integrates the reporting structure between different types of sensors in the HIDS and NIDS realms. Also the interface must be able to intelligently and intelligently collect and report data from the network or systems being monitored. The interface is so important and critical because it receives data, collects analysis from the relevant component, coordinates and correlates the interpretation of this data and reports it. It represents a complex and unified event tracking, reporting and review environment.

3.4.1. The changing nature of IDS tools

Although ID systems are assumed by the networking community to protect network systems from outside intruders, recent studies have shown that most system intrusions come from insider attacks. So newer IDS tools are focusing on this issue. Also, we must know that the human mind is the most complicated and unpredictable machine ever, as new IDS tools are being created to counter intrusion into the system, new attack models are being developed to be considered. This human behavior must take into account unpredictability. To keep up with all these changes, ID systems must constantly change.

While all these changes are happening, the main focus of ID systems has been on a network as a unit where they collect network packet data by looking at the packet traffic on the network and then analyzing it based on patterns. of network protocol "norms", "normal" signatures and network traffic anomalies built into ground rules. But as networks grow larger, traffic becomes heavier, and local networks become more fragmented, it becomes increasingly difficult for an ID system to "see" all the traffic on a switched network such as it is an ethernet.

So, in general, ID systems fall into two categories, host-based and network-based.

3.4.2. Other types of intrusion detection systems

Although NIDS and HIDS and their hybrids are the most widely used tools in network intrusion detection, there are others that are less used but more targeted and therefore more specialized. Because many of these tools are so specialized, many of these are not yet considered intrusion detection systems, but instead are identified as add-ons or intrusion detection tools such as:

System integrity verifiers (SIVs), which monitor critical files in a system, such as a file system, to find out if an intruder has changed them. They can also detect other data and system components, for example they detect when a normal user somehow obtains root/administrator level privileges. In addition, they also monitor system logs to find known signatures [15].

Log file monitors (LFMs) first create a record of log files generated by network services. Then they monitor this record and just like NIDS, looking for system trends, trends and patterns in log files that would suggest an intruder is attacking.

3.4.3. Honeypot

A honeypot is a system designed to look like something an intruder can hack. They are built for many purposes, but the main one is to deceive attackers and learn about their tools and methods. They are good cheat systems that protect the network in the same way as HIDS and NIDS. Since the purpose of a honeypot is to deceive intruders and learn from them without compromising the security of the network, then it is important to find a strategic location for the honeypot.

For many professionals, the best location to achieve this goal is in the DMZ for those networks with a DMZ or behind the network firewall if the private network does not have a DMZ. The location of the firewall is ideal because of the following [16]:

• Most firewalls log all traffic that passes through it, so this becomes a good way to track all intruder activities. By reviewing the firewall logs, we can determine how intruders are probing the honeypot and what they are looking for.

• Most firewalls have some alerting capabilities, which means that with some additions to the firewall's rule base, we can receive timely alerts. The honeypot is built in such a way that no one is supposed to connect to it, any packets sent are most likely from intruders probing the system. And if there is any outgoing traffic coming from the honeypot, then the honeypot is most likely compromised.

• Firewall can control incoming and outgoing traffic. This means that intruders can find, probe and exploit our honeypot, but they cannot compromise other systems.

So, any dedicated firewall as a honeypot can do as long as it can control and record the traffic passing through it. If no firewall is used, then dedicate a machine either inside the DMZ or behind a firewall for the purpose of logging all attempted accesses. Figure 3, shows the positioning of a honey pot.

Honeypots come in a variety of capabilities from the simplest to monitor two intrusive activities to the most powerful that monitor multiple intrusive activities.

The simplest honeypot is a monitor port which is a simple socket-based program that opens a listening port. The program can listen on any designed port. For example, NukeNabbe, for Windows, listens on ports that are commonly scanned by hackers. It then alerts the administrator whenever such specific ports are being requested to be scanned. The second type of honeypot is the spoof system, which instead of quietly listening on a port, interacts with the intruder, responding to him or her as if it were a real server with that port number. Most spoofing systems implement as many protocols on the machine as necessary to block 90% of attacks against the protocol [17]. The other type of honeypot is the multi-protocol cheat system which provides most of the commonly hacked protocols in a single toolkit. Finally, there is a complete system that goes beyond what cheat systems do to include the ability to notify the system administrator of any exceptional conditions. Other more complex Honeypots combine a full system with NIDS to complement internal interventions.

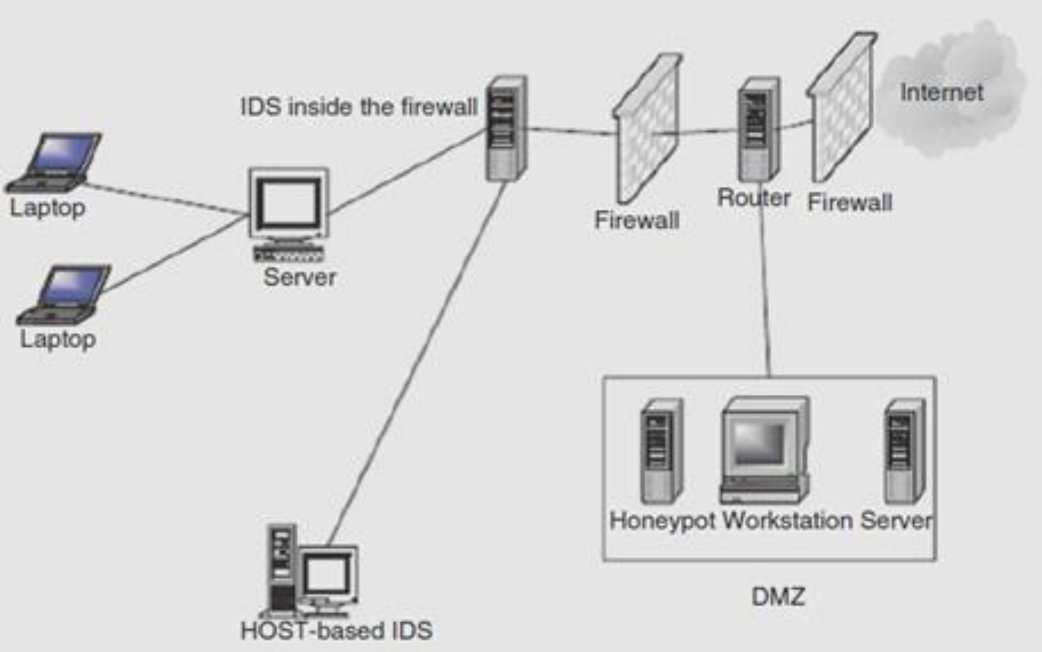

Figure 3. The positioning of a honeypot.

Advantages of Honeypots One might wonder why a system administrator would go through the trouble of setting up, maintaining and providing day-to-day response to honeypots. The advantages of having honeypots in a network include the following [18]:

• Since NIDS have difficulty distinguishing between hostile and non-hostile activities, honeypots are better suited for digging up hostile intrusions because isolated honeypots do not normally need to be accessed. So if they are accessed at all, such accesses are unwanted intrusions and should be reported.

• A honeypot can lure would-be hackers into a trap by providing a banner that looks like an easily hackable system.

4. Discussion

4.1. Response to intervention in the system

A good intrusion detection system alarm should produce an appropriate response. The type of response is related to the type of attack. Some attacks require no response, others require a preliminary response. Still others need a quick and powerful response. For the most part, a good response should consist of pre-planning and safeguards that include an incident response team and ways to collect IDS logs for future use and legal evidence when needed.

4.2. Incident Response Team

An incident response team (IRT) is a primary, centralized and dedicated group of people charged with the responsibility of being the first team of contact whenever an incident occurs. We suggest that an IRT should have the following responsibilities:

- Keeping up to date with the latest threats and incidents.
- Being the main point of contact for incident reporting.
- Notifying others whenever an incident occurs.
- Assessing the damage and impact of each incident.
- Finding how to avoid exploiting the same vulnerability.
- Eliminating the effects (healing) from the incident

In handling an incident, the team should carefully prioritize actions based on the organization's security policy, but taking into account the following order:

– Human life and people's safety.
– More sensitive or classified data.
– Expensive data and files.
– Preventing damage to systems.
– Minimizing the destruction of systems.

• The assessment of the damage from the incident is done by performing a complete check on all the following steps, such as system log statistics, infrastructure and control of the entire operating system, system configuration changes, changes in classified data and sensitive, traffic logs and password files.

• Alerting and reporting the incident to relevant parties, which may include informing law enforcement agencies, incident reporting centers, company executives, employees and sometimes the public.

• Incident recovery involves conducting a post-lethal analysis with the entire team. This post-attack report should include steps to be taken in the event of similar incidents in the future.

4.2.1. IDS logs as evidence and challenges to intrusion detection systems

First of all, IDS logs can be kept as a way to protect the organization in case of legal proceedings. Some people tend to view IDS as a form of eavesdropping. If sensors to monitor the internal network are to be deployed, verify that there is a policy to publish network usage and consent for monitoring is obtained. While IDS technology has come a long way and has an exciting future for it as a marriage between itself and artificial intelligence, it continues to face many challenges.

4.2.2. Deploying IDS in Switched Environments

There is a particularly difficult challenge facing organizations trying to deploy IDS on their networks. Network-based IDS sensors should be placed in areas where they can "see" network traffic packets. However, in switched networks, this is not possible because by their very nature, sensors in switched networks are shielded from most network traffic. Sensors are only allowed to "see" traffic from specified network components.

One way to handle this situation has traditionally been to attach a network sensor to a mirror port on the switch. But port mirroring, in addition to putting an overhead on the port, becomes impractical when there is an increase in traffic on that port because overloading a port with traffic from other ports can cause the port to grow and slow us down. the traffic.

Among other issues that still limit IDS technology are [19]:

• False alarms where, although the tools have come a long way and are slowly gaining acceptance as they gain widespread use, they still produce a significant number of both false positive and negative alerts.

• The technology is not yet ready to handle a large-scale attack. By its very nature, it must scan literally every packet, every touchpoint, and every traffic pattern on the network. For larger networks and in a large-scale attack, it is not possible that the technology can be relied upon to continue working with acceptable quality.

• Unless there is a breakthrough today, the technology in its current state cannot handle large amounts of traffic very quickly and efficiently.

• Perhaps the biggest challenge is the perceived and sometimes overpowered IDS. Technology, while good, is not a panacea for all Computer Networks, it is like any other good security tool.

4.3. Implementation of an intrusion detection system

An effective IDS does not stand alone. It must be supported by a number of other systems. Among the things that should be considered, in addition to the IDS, in setting up a good IDS for the company's network, the following measures should be taken [20]:

• Operating systems, where a good operating system that has logging and auditing features. Most modern operating systems including Windows, Unix and other Unix Variants have these features. These features can be used to monitor security critical resources.
• Services, where all applications on servers such as web servers, email servers and databases must also include logging/auditing features.
• Firewalls, a good firewall should have some ability to detect network intrusions.
• Network management platform, make sure they have tools to help set up alerts for suspicious activity.

4.3.1. Intrusion Prevention Systems (IPS)

Although IDSs have been one of the cornerstones of network security, they have only been a cover for one component of the total network security picture. They have been and are a passive component that detects and reports only by preventing. A promising new intervention model is developing and growing rapidly. It is the intrusion prevention system (IPS), which is to prevent attacks. Like their IDS counterparts, IPS fall into two categories: network-based and host-based.

4.3.2. Network-based intrusion prevention systems (NIPS)

Because NIDSs are passively detecting network intrusions without preventing them from entering networks, many organizations in recent times have combined IDSs and firewalls to create a model that can detect and then prevent.

The package works as follows. The IDS faces the network with a firewall behind it. Upon detection of an attack, the IDS then goes into prevention mode by changing the firewall's access control rules. The action may result in an attack being blocked based on all access control regimes administered by the firewall.

But this type of prevention is expensive and complex, especially for an untrained security team. The model suffers from the delay time it takes for IDS to modify firewall rules or issue a TCP reset command. This period of time is critical to the success of an attacker.

To answer this need, a new technology, IPS, is making its way into the network security arena to address this latent issue. It does this by the cooperation of the two systems, that of detecting intrusions in line with the firewall. As with NIDS, the NIPS architecture naturally varies from product to product, but there is a basic underlying structure for all.

These include the traffic normalizer, system service scanner, detection engine, and traffic shaper.

4.3.3. Traffic Normalizer

The normalizer is in line with network traffic to intercept traffic, troubleshooting traffic that has anomalies before sending it. While normalizing the traffic, it may come to a point where it will drop the packet that does not match the set of security policy criteria such as if the package has a bad check. It also furthers the firewall's activities, thus blocking traffic based on criteria that would normally be set in a firewall. The normalizer can also take packet fragments and reassemble them into a packet based on its knowledge of the target system. Target system knowledge is provided by a reference table built by the system service scanner.

The detection engine handles all pattern matches that are not handled by the normalizer. These are models that are not based on protocol states.

Traffic Shaper, where before traffic leaves the NIPS, it must pass through the traffic shaper for classification and flow management. The shaper classifies protocol traffic, although this may change in the future to include classification based on users and applications.

The benefits of NIPS for Network Interventions will be:

• Zero Latency Prevention Without the NIDS packet and firewall, NIPS reduce this latency drastically by providing notification within one network circuit instead of two.
• Effective network hygiene, since many attacks are recycling attacks, whose signatures are known, NIPS drops these packets quickly, even though you do a lot of the effective anomaly analysis that NIDS does.
• Simplified management, since the potential package of a NIDS and firewall are all packaged in one hardware, which reduces storage space and of course overall management.

Despite having all these advantages, NIPS suffer from a number of problems including the following:

• Production readiness, because the technology is new it has not yet received the field testing it needs to prove effectiveness in any test.

• High availability, because it is online and in first contact with network traffic, it may not be able to handle the high traffic availability and tolerance required for all the first and direct network equipment.

• Detection effectiveness has not yet been tested for detection effectiveness, and it never stops everything.

4.4. Host-based Intrusion Prevention Systems (HIPS)

Like protection with NIDS, NIPS also have corresponding HIPS based on a host. Most HIPS work with sandboxing, a process of limiting the definition of acceptance to the rules of competent behavior used in HIPS. HIPS prevention occurs on the agent that resides on the system. The agent intercepts system calls or system messages using dynamic replacement of linked libraries (dll). The replacement is done by injecting the existing system dlls with stub dlls of the vendors that perform the interception. So, it works calls made to the system dlls that actually make a pass to the vendor's stub code where the bad calls are then processed, evaluated and handled. Most vendor stubs are kernel drivers that provide kernel-level system interception due to processes, in which case system calls can be easily intercepted.

4.5. Benefits of HIPS

Again, like the application and discovery from HIDS, HIPS have benefits that include the following:

• Effective context-based prevention, where HIPS are the only solution for preventing attacks that require simulation context. HIPS agents reside on the protected host, they have full context of the environment and are therefore better able to deal with such attacks.

• Effective against zero-day attacks, since HIPS uses the sandboxing method to deal with attacks, they can define the application or operation of acceptable parameters in the behavior of the system service to enable the agent to prevent any attack in order to bad.

Although they have good benefits, HIPS also have disadvantages based on limitations that prevent their rapid adoption. Among these restrictions are:

• Deployment challenge as we discussed in HIDS, there is difficulty in deploying remote agents on each host. These hosts need updating and are susceptible to tampering.

• Difficulty of effective sandbox configuration, it can be a challenge to define effective and non-restrictive parameters on hosts.

• Lack of effective prevention due to the use of sandboxing, HIPS cannot be used in any standard prevention such as signature prevention.

5. Conclusions

In the process of computer network security, intrusion detection system research and design are a very important task. A good intrusion detection system can effectively compensate for the shortcomings of the firewall, can provide a reliable guarantee for the security of the computer network, and is the most effective protection technology in modern network security measures. Intrusion detection tools work best when used after vulnerability scans are performed.

All network-based intrusion detection systems and tools that can provide probes (detectors) in addition to port and host scans, as monitoring tools will provide us with information on:

• Hundreds of thousands of network connections.; • Attempts at external penetration.; • Internal scans.;
• Misuse of confidential data models.; • Unencrypted remote logins or web sessions.

All this information collected by these tools, which monitor network components and services included in cyber systems, should be based on prevention, detection and response to any possible intervention.

Acknowledgement

This study was partly presented at the 6th Advanced Engineering Days [21].

Funding

This research received no external funding.

Author contributions

Fatmir Basholli: Conceptualization, Methodology, Software, validation, Writing-original draft. **Adisa Daberdini:** Data curation, Visualization, Investigation, Software. **Armand Basholli:** Validation, Experimentation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

1. Chand, N., Mishra, P., Krishna, C. R., Pilli, E. S., & Govil, M. C. (2016, April). A comparative analysis of SVM and its stacking with other classification algorithm for intrusion detection. In 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA)(Spring), 1-6. IEEE. https://doi.org/10.1109/ICACCA.2016.7578859
2. Kizza, J. M. (2017). Guide to Computer Network Security. https://doi.org/10.1007/978-3-319-55606-2
3. Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. Alexandria Engineering Journal, 61(12), 9395-9409. https://doi.org/10.1016/j.aej.2022.02.063
4. SANS Institute (2016). The History and Evolution of Intrusion Detection. https://www.sans.org/reading-room/whitepapers/detection/history-evolution-intrusion-detection-344
5. Sharma, R. K., & Pippal, R. S. (2020, September). Malicious Attack and Intrusion Prevention in IoT Network Using Blockchain Based Security Analysis. In 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), 380-385. IEEE. https://doi.org/10.1109/CICN49253.2020.9242610
6. Mitchell, R., & Chen, I. R. (2014). A survey of intrusion detection techniques for cyber-physical systems. ACM Computing Surveys (CSUR), 46(4), 1-29. https://doi.org/10.1145/2542049
7. Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Garg, S., & Hassan, M. M. (2022). A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. Journal of Parallel and Distributed Computing, 164, 55-68. https://doi.org/10.1016/j.jpdc.2022.01.030
8. http://resources.infosecinstitute.com/internet-things-much-exposed-cyber-threats
9. Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access, 9, 59353-59377. https://doi.org/10.1109/ACCESS.2021.3073408
10. Liu, Y. S., Lai, Y. K., Wang, Z. H., & Yan, H. B. (2019). A new learning approach to malware classification using discriminative feature extraction. IEEE Access, 7, 13015-13023. https://doi.org/10.1109/ACCESS.2019.2892500
11. Masduki, B. W., Ramli, K., Saputra, F. A., & Sugiarto, D. (2015, August). Study on implementation of machine learning methods combination for improving attacks detection accuracy on Intrusion Detection System (IDS). In 2015 International Conference on Quality in Research (QiR), 56-64. IEEE. https://doi.org/10.1109/QiR.2015.7374895
12. Basati, A., & Faghih, M. M. (2022). PDAE: Efficient network intrusion detection in IoT using parallel deep auto-encoders. Information Sciences, 598, 57-74. https://doi.org/10.1016/j.ins.2022.03.065
13. McHugh, J. (2000). Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory. ACM Transactions on Information and System Security (TISSEC), 3(4), 262-294. https://doi.org/10.1145/382912.382923
14. Al-Taleb, N., & Saqib, N. A. (2020, September). Attacks detection and prevention systems for IoT networks: a survey. In 2020 International Conference on Computing and Information Technology (ICCIT-1441) 1-5. IEEE. https://doi.org/10.1109/ICCIT-144147971.2020.9213770
15. http://www.combofix.org/what-it-is-network-intrusion-detection-system.php.Dec-2015
16. Axelsson, S. (2005). Intrusion detection systems: a survey and taxonomy. 2000. Chalmers University of Technology: Goteborg, Sweden.
17. Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16-24. https://doi.org/10.1016/j.jnca.2012.09.004
18. Sans Penetration Testing (2001). Host-vs. Network-Based Intrusion Detection Systems. https://cyber-defense.sans.org/resources/papers/gsec/host-vs-network-based-intrusion-detection-systems.

19. SANS Institute InfoSec Reading Room (2001). Application of Neural Networks to Intrusion Detection. https://www.sans.org/reading-room/whitepapers/detection/application-neural-networks-intrusion-detection.
20. Soniya, S. S., & Vigila, S. M. C. (2016, March). Intrusion detection system: Classification and techniques. In 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT) (pp. 1-7). IEEE. https://doi.org/10.1109/ICCPCT.2016.7530231
21. Basholli, F., Daberdinİ, A., & Basholli, A. (2023). Detection and prevention of intrusions into computer systems. Advanced Engineering Days (AED), 6, 138-141.