INTERNATIONAL BURCH UNIVERSITY

Faculty of Engineering and Natural Sciences

Department of Information Technology

CEN 263: Computer Networks

Research Project

INTRUSION DETECTION

Sarajevo, 24th of December, 2021 *Amira Abdo- 20002450*

TABLE OF CONTENTS

1. Abstract

Intrusion detection can be defined as the ability to monitor and respond to improper use of a computer. Many hardware and software products on the market today offer varying degrees of intrusion detection. Some solutions use signatures to monitor for known attacks. Some solutions offer network monitoring; others are server based systems. Some solutions respond to specific alerts by shutting down services; others use a more passive approach. One should choose their intrusion detection strategy carefully to ensure that the network resources remain safe from unwanted intruders. As well as antivirus protection, many locations and methods are suitable for intrusion detection. The most common use is to install an intrusion detection solution to monitor access points from the Internet or the outside world in one's private network.

As new attacks occur every day, intrusion detection systems (IDSs) play an important role in identifying potential attacks on a system and responding appropriately. IDSs need to adapt and continually improve on these new attacks and attack strategies. How to develop effective, efficient, and adaptable IDSs is a problem that researchers have been tackling for decades. Researchers have investigated the suitability of various technologies for this area of study.

2. Introduction

"The meaning of intrusions in the computer security context has been debated. Many people consider intrusions to include unsuccessful attacks, while others see a distinct difference between attacks and intrusions. We'll work with the definition that an intrusion is an active sequence of related events that deliberately try to cause harm, such as rendering a system unusable, accessing unauthorized information, or manipulating such information. This definition refers to both successful and unsuccessful attempts." *

Security professionals may want the IDS system to record information about successful and unsuccessful attempts so that they more fully understand events taking place on their network. This can be done by placing devices that inspect network traffic, called sensors, both in front of the firewall (unprotected zone) and behind the firewall (protected zone) and compare their recorded information.

2.1. What Is an Intrusion Detection System (IDS)?

Intrusion detection system can be defined as tools, methods, and resources for identifying, assessing, and reporting unauthorized or unapproved network activity. The intrusion detection part of the name is a bit off, because IDS doesn't actually detect

---

*(Endorf, Schultz and Mellander, n.d.)

intrusions - it detects activity in traffic that may or may not be intrusive. Intrusion detection is generally part of an overall protection system installed around a system or device. It is not a stand-alone safeguard.

IDS, either a hardware device or a software application, uses known attack signatures to detect and analyze anomalous activity in incoming and outgoing network traffic.

- This is done in one of the following ways:
- Comparison of system files using malware signatures.
- A scanning process that detects signs of harmful patterns.
- Monitoring user behavior to detect malicious intent.
- Monitoring system settings and configurations.

If IDS detects a security policy violation, virus, or configuration error, IDS can drive the rogue user out of the network and send an alert to security personnel.

Despite its advantages such as detailed analysis of network traffic and attack detection, IDS has its own drawbacks. As previously known attack signatures are used to localize attacks, newly discovered (that is, zero-day) threats may go undetected.

In addition, IDS only recognizes ongoing attacks, not incoming attacks. An intrusion prevention system is required to block these.

2.2. What is an Intrusion Prevention System (IPS)

IPS complements IDS configurations by proactively inspecting incoming traffic on the system to eliminate malicious requests. A typical IPS configuration uses a web application firewall and traffic filtering solution to protect your application.

IPS prevents attacks by dropping malicious packets, blocking offensive IPs, and alerting security personnel to potential threats. Such systems typically use an existing database for signature detection and can be programmed to detect attacks based on traffic and behavioral anomalies.

Some IPS systems effectively block known attack vectors, but with limitations. These are often caused by excessive reliance on predefined rules and are prone to false positives.

As a result, IDS and IPS are used in combination with a firewall to combat unwanted activity on the network. Figure 1 shows an analogy explaining how the combination of the three works to ensure a safe and protected network.

You can loosely compare firewalls to locked doors, intrusion detection to alarm systems, and intrusion prevention to guard dogs. Let's say that you have a warehouse full of secret documents that you want to protect with a fence around the perimeter, an alarm system, locked doors, and security cameras. The locked doors will stop unauthorized individuals from entering the warehouse. By themselves, they do nothing to alert you of an intrusion, but they deter unauthorized access. The alarm system will warn you in case an intruder tries to get into the warehouse. By itself, it does nothing to prevent an intrusion, but it alerts you to the *potential* of an intrusion. The guard dog, in some instances, is able to prevent an intrusion by taking measures to thwart the attack from happening by biting intruders before they can enter the protected perimeter, thereby stopping the intrusion.

As you can see, the door locks, alarm system, and guard dog play separate but complementary roles in the protection of this warehouse. This is also true of firewalls and IDSs and IPSs. All of these are different technologies that can work together to alert you and can prevent intrusions into a network. In addition, how these technologies are implemented determines whether or not they increase security. For instance, in the warehouse example, the most effective strategy may be to place alarms and locks on all the windows and doors, as well as motion detectors inside the warehouse. You may also want several dogs deployed within the perimeter to watch for possible intruders. Implementing IDSs and IPSs is no different—the placement of the technology makes all the difference between a secure network and an unsecured one.

Figure 1: ISP, IDP, firewall analogy

Intrusion Detection and Prevention- Carl Endorf, Gene Schultz, Jim Mellander

2.3. IDS vs IPS

"IDS and IPS technology each have their own place in a security program because they perform separate functions. Table 1 clarifies some of the differences between them."*

IDS	**IPS**
Installed on network segments (NIDS) and on hosts (HIDS)	Installed on network segments (NIPS) and on hosts (HIPS)
Sits on network passively	Sits inline (not passive)
Cannot parse encrypted traffic	Better at protecting applications
Central management control	Central management control
Better at detecting hacking attacks	Ideal for blocking web defacement
Alerting product (reactive)	Blocking product (proactive)

Table 1: Intrusion-Detection Systems vs. Intrusion-Prevention Systems

Intrusion Detection and Prevention- Carl Endorf, Gene Schultz, Jim Mellander

*(Endorf, Schultz and Mellander, n.d.)

2.4. History of intrusion detection and prevention

Initially, system administrators performed intrusion detection by sitting in front of the console and monitoring user activity. For example, you can detect intrusions by detecting that a user is logged on locally during the holidays or that a printer that is rarely used is abnormally active. Although effective enough at the time, this early intrusion detection was ad hoc, not scalable. The next step in intrusion detection included an audit log that system administrators checked for evidence of anomalous or malicious behavior. From the late 1970s to the early 1980s, managers typically printed audit logs on continuous paper, often stacked to a height of 4-5 feet at the end of the average week. Searching for such a stack was obviously very time consuming. With so much information and manual analysis, administrators primarily used audit logs as a forensic tool to retroactively identify the cause of a particular security incident. There was little chance that the attack would proceed. As storage became cheaper, test reports came online and researchers developed programs to analyze the data. 1 However, due to the slow analysis and often computational complexity, intrusion detection programs were typically run at night when the system was not used by the user. Therefore, most of the intrusions were detected even after they occurred. In the early 1990s, researchers developed a real-time intrusion detection system that validates the audit data created. This allows for immediate detection of attacks and attack attempts, real-time response, and in some cases preemption of attacks. Recent attack detection efforts focus on developing products that users can effectively use in large networks. With growing security concerns, a myriad of new attack techniques, and constant changes in the surrounding computing environment, this is not an easy task.

2.5. Why IDS and IPS are so important

IDSs and IPSs are important for many organizations, from small offices to large multinational companies. Employment of IDSs and IPSs provides many benefits:

- More knowledgeable about intrusion detection than manual execution
- Extensive knowledge base
- Ability to process large amounts of data
- Near real-time alarm function to mitigate potential damage
- Automated responses, such as logging off a user, disabling a user account, or launching automated scripts
- Powerful deterrence
- Built-in forensic and reporting capabilities

All of these are very good reasons to implement these technologies, but there are three main reasons to justify the need for over any other reason.

- Legal Issues- In 1998, US Presidential Decision Directive 63 (PDD 63) increased the use of intrusion detection and prevention to protect the country's infrastructure with steps. British Standard 7799, first published in February 1995, identified comprehensive controls that define "best practices" for information security. Regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Blilly Act of 1999 (GLBA) provide audit control to record and investigate suspicious data access activity. Is required. The above regulations may or may not be required depending on the type and location of the organization.
- Quantifying Attacks- IDS and IPS provide system administrators with the ability to quantify attacks on corporate networks for administrative purposes. Both IDS and IPS can create a profile of the attack type being attempted against the network. This allows for stronger cases of good security measures that are often difficult to justify. IPS and IDS can also provide evidence against an attacker if a proceeding is sought.
- Establishing a Comprehensive Defense-In Depth Strategy**-** IDS and IPS have become an important part of a strong defense-in-depth security program, and their use shows due diligence for organizations as they are expected by the organization. Both of these technologies protect network and application layer vulnerabilities and help correlate and validate information from other devices such as antivirus programs, firewalls, and routers.

3. IDS and IPS Analysis Schemes

IDS and IPS perform analyses. It is important to understand the analytical process. What are the contents of the analysis, the types of analyses available, and what are the strengths and weaknesses of the various analysis schemes?

3.1. What is analysis?

Analysis in the context of intrusion detection and prevention is to organize the components of your data and their interrelationships to identify anomalous activity of interest. Real-time analysis is an in-flight analysis while the data is moving to the network or host. However, this can be a bit misleading, as the analysis can only be performed retroactively in near real time.

3.2. The anatomy of intrusion analysis

The analysis engine has many possible data analysis schemes, and to understand them, the intrusion analysis process can be divided into four phases.

1. Preprocessing

2. Analysis
3. Response
4. Improved

Preprocessing Data from IDS or IPS sensor is a key function which takes place after data is collected by the sensors. In this step, the data is organized in some way for classification. Preprocessing helps determine the format in which the data is entered. This can usually be legitimate or a structured database. Once the data is formatted, it is further classified into categories. These classifications may vary depending on the analysis scheme used.

For example, if rule-based discovery is used, the classification contains rules and pattern descriptors. Typically, anomaly detection creates statistical profiles based on various algorithms to baseline user behavior over time and flag user behavior as anomalous.

When the classification process is complete, the data is concatenated and inserted into the predefined version of the object or the recognition template by replacing the variable with a value. These discovery templates are populated in the Knowledge Base stored in the Core Analysis Engine:

- Detection of system log file changes
- Detection of unexpected privilege elevation
- Detection of Netbus backdoor
- Detection of backdoor subseven
- ORACLE authorization attempt
- RPC mountd UDP export request

After completion, prepossessing begins the analysis phase. The data record is compared to the knowledge database and the data record is logged or discarded as an intrusion event. Next, the following data records are analyzed.

The next step, the reaction, is one of the differentiators between IDS and IPS. IDS usually limits proactive features. The information is received passively, so alerts are received after the fact. As soon as the information is recorded as an intrusion, the reaction is started. In IPS, the sensor is inline and can provide real-time protection through an automated response. This is the main difference between reactive security and proactive security.

In each case, the answer is specific to the type of intrusion or the various analytical schemes used. The response can be set to run automatically, or it can be run manually after someone has manually analyzed the situation.

The final stage is the improvement stage. IDS or IPS system can be fine-tuned here based on previous usage and detected attacks. This will allow security professionals to reduce the number of false positives and use more accurate security tools. This is a very important phase for the to get the most out of its IDS or IPS system. For them to provide

service appropriately, the system needs to be tailored to the environment. There are tools like Cisco Threat Response (CTR) that help the refinement phase by checking for vulnerabilities to this attack and actually verifying that alerts are valid.

4. Types of detection

4.1. Rule-Based Detection (Misuse Detection)

Rule-based detection, also known as signature detection, pattern matching, and fraud detection, is the first scheme used in early intrusion detection systems. Rule-based detection uses pattern matching to identify known attack patterns.

The four phases of the analysis process when applied in a rule-based detection system are described by Carl Endorf, Gene Schultz, Jim Mellander in "Intrusion Detection and Prevention" as following:

1. Preprocessing- The first step is to collect data about intrusions, vulnerabilities, and attacks, and put them into a classification scheme or pattern descriptor. From the classification scheme, a behavioral model is built, and then put into a common format:

- Signature Name- the given name of a signature
- Signature ID- a unique ID for the signature
- Signature Description- description of the signature and what it does
- Possible False Positive Description- an explanation of any “false positives” that may appear to be an exploit but are actually normal network activity.
- Related Vulnerability Information- this field has any related vulnerability information
- User Notes- this field allows a security professional to add specific notes related to their network

The pattern descriptors are typically either content-based signatures, which examine the payload and header of a packet, or context-based signatures that evaluate only the packet headers to identify an alert. Note that pattern descriptors can be atomic (single) or composite (multiple) descriptors. An atomic descriptor requires only one packet to be inspected to identify an alert, while a composite descriptor requires multiple packets to be inspected to identify an alert. The pattern descriptors are then put into a knowledge base that contains the criteria for analysis.

2. Analysis- The event data are formatted and compared against the knowledge base by using a pattern-matching analysis engine. The analysis engine looks for defined patterns that are known as attacks.

3. Response If the event matches the pattern of an attack, the analysis engine sends an alert. If the event is a partial match, the next event is examined. Note that partial matches can only be analyzed with a stateful detector, which has the ability to maintain state, as

many IDS systems do. Different responses can be returned depending on the specific event records.

4. Refinement- refinement of pattern-matching analysis comes down to updating signatures, because an IDS is only as good as its latest signature update. This is one of the drawbacks of pattern matching analysis. Most IDSs allow automatic and manual updating of attack signatures.

4.2. Profile-Based Detection (Anomaly Detection)

Anomalies are those that deviate from the norm or cannot be easily classified. Anomaly detection, also known as profile-based detection, creates a profile system that identifies all events that deviate from the normal pattern and passes this information to the output routine. The main difference between anomaly detection and other analysis schemes is that the anomaly-based scheme defines not only prohibited activities, but also allowed activities. In addition, anomaly detection is typically used for the ability to capture statistical and characteristic behavior. The statistics are quantitative and the characteristics are more qualitative. For example, "UDP traffic on this server does not exceed 23% of capacity" shows statistical behavior, and "User John672 does not normally use FTP files outside the company" shows characteristic behavior. Anomaly-based schemes can be divided into three main categories: behavior, traffic patterns, and protocols. Behavior Analysis looks for anomalies in the type of behavior based on statistics, such as relationships in packets or those being sent over the network. Traffic pattern analysis looks for specific patterns of network traffic. Protocol analysis looks for network protocol violations or misuse based on RFC-based behavior. Log analysis has the advantage of being able to identify attacks that may not have been published yet, or whose signature or solution for may not be known.

Again, the four phases of the analysis process when applied in a profile-based detection system are described by Carl Endorf, Gene Schultz, Jim Mellander in "Intrusion Detection and Prevention" as following:

1. Preprocessing- the first step in the analysis process is collecting the data in which behavior considered normal on the network is baselined over a period of time. The data are put into a numeric form and is then formatted. Then the information is classified into a statistical profile that is based on different algorithms in the knowledge base.
2. Analysis- the event data are typically reduced to a profile vector, which is then compared to the knowledge base. The contents of the profile vector are compared to a historical record for that particular user, and any data that fall outside of the baseline normal activity is labeled a deviation.
3. Response- at this point, a response can be triggered either automatically or manually.

5. Refinement- the data records must be kept updated. The profile vector history will typically be deleted after a specific number of days. In addition, different weighting systems can be used to add more weight to recent behaviors than past behaviors.

5. More on detection

5.1. Target monitoring

The target monitoring system reports whether a particular target object has changed or changed. This is typically done using a cryptographic algorithm that calculates the cryptographic checksum for each target file. IDS reports all changes including file changes or program logons that result in changes to the crypto checksum. Tripwire software provides immediate notification of changes to the configuration file and targets using the crypto checksum by enabling automatic recovery. Perform monitoring. The main advantage of doing this is that the target files don't have to be monitored constantly.

5.2. Stealth probes

Stealth probes correlate data to detect long-running attacks. This is often referred to as the "low and slow" attack. Data is collected from various sources, characterized and scanned with to discover correlated attacks. This technique, also known as widespread correlation, is typically a composite or hybrid approach that attempts to detect malicious behavior using other detection methods.

5.3. Heuristics

The term heuristic refers to artificial intelligence (AI). In theory, IDS detects anomalies, detects intrusions, and learns what can be considered normal over time. To use heuristics, the AI scripting language can apply analysis to incoming data. Heuristics currently leave a lot to be desired, but development is underway. What is needed is a pattern matching language that can more accurately learn and identify malicious activities using programming structures.

5.4. Hybrid approach

We considered a fundamental analysis scheme. You can see that there is a lot of debate about which is considered the best approach. In fact, they all have their strengths and weaknesses, but when used together, they can provide a more robust security system. Products that use a hybrid approach usually perform better, especially against complex attacks.

6. IDS/IPS Pros and Cons

As mentioned earlier, IDS and IPS are two separate technologies that can complement each other. Table 2 lists the strengths and weaknesses of both technologies.

	DETECTION	PREVENTION
PROS	• Can detect external hackers as well as internal network-based attacks • Scales easily to provide protection for the entire network • Offers centralized management for correlation of distributed attacks • Provides defense in depth • Gives system administrators the ability to quantify attacks • Provides an additional layer of protection	• Protects at the application layer • Prevents attacks rather than simply reacting to them • Can use a behavioral approach • Provides defense in depth • Permits real-time event correlation
CONS	• Generates false positives and negatives • Reacts to attacks rather than preventing them • Requires full-time monitoring • Requires a complex incident-response process • Cannot monitor traffic at higher transmission rates • Generates an enormous amount of data to be analyzed • Requires highly skilled staff dedicated to interpreting the data • Susceptible to “low and slow” attacks • Cannot deal with encrypted network traffic	• Generates false positives that can create serious problems if automated responses are used • Creates network bottlenecks • It is a new technology • It is expensive

Table 2: Pros and cons of IDS and IPS

Intrusion Detection and Prevention- Carl Endorf, Gene Schultz, Jim Mellander

7. IDS and IPS architectures

The term architecture refers to the features and relationships between supported machines, network devices, programs, processes, and the communication between them. Three major types of architecture- single-tier, multi-tier, and peer-to-peer are commonly used for intrusion detection and intrusion prevention.

A single-tiered architecture consists of one component that performs all its functions.

The multi-tiered architecture has multiple components, each of which communicates with some or all of the others. The components are hierarchical, with sensors (usually at the bottom), agents (more complex but usually aimed at one type of analysis), and manager components, which usually embodies many centralized functions. increase.

Peer-to-peer architecture is an architecture with multiple components, such as firewalls, each of them being a peer (not a subordinate or superordinate).

Of the three major types of architecture, multitier architectures are used more than any other architecture. The sensor collects data, and the agent gets the information it receives from the sensor and, in some cases, gets them from other agents for analysis. The Manager component also provides centralized and advanced functionality, including data aggregation, data correlation, policy creation and distribution and alerts. Operators and analysts typically interact with the management console. The management console is the part of the manager component user interface for controlling the entire IDS or IPS. Many deployment and security decisions need to be made for each component.

In general, the higher the level of a component, the greater the need for a higher level of security. Sensors, for example can usually be used anywhere on the network without causing undo issues, but the agent requires a higher level of protection and needs to be placed in the most efficient and safest appropriate location. Manager components require the highest level of security and must provide the same protection as the agent, as well as additional controls such as physical security measures, strong authentication, and strong encryption.

8. IDS and IPS Internals

IDS and IPS can be simple or complex as needed. At the simplest level, you can use a package-capturing program to save the package to a file and use commands such as egrep and fgrep in your script to find the desired string in the file. However, this approach is not practical given the amount of traffic that needs to be collected, processed, and stored for a simple, feasible analysis. But even at this rudimentary level, much more happens than we can imagine. Packets are collected and then decoded. Some of these packets are fragmented and must be reassembled before they can be parsed. TCP streams also often need to be reassembled. For more complex IDS or IPS, excluding unwanted inputs, applying firewall rules, geting certain types of incoming data in an easy-to-process format, executing discovery routines on the data and any additional advanced operations may be performed. In this latter case, even more complex internal events and processes occur. To better explain this, we will deal with the internals of IDS and IPS, including information flow within these systems, exploit detection, malicious code handling and output routine functionality.

8.1. Information flow in IDSs and IPSs

Khondker Ishtiaq described the information flow in IDS and IPS in an article titled "Overview of an IDS & an IPS" at https://www.linkedin.com/pulse/overview-ids-ips-khondker-ishtiaq-murshid (published Nov 13, 2016) as follows:

"We find the flow of information behaving similarly in both IDS and IPS. This flow of information can follow eight different ways as described below:

1. Information flow begins from Raw Packet Capture in both the IDS and IPS. It captures the packets and transfers data as well to the next component of the system in two modes such as Promiscuous Mode and Non-Promiscuous Mode.
2. Filtering is a procedure of controlling the captured packets using network interface cards or configured packet filters.
3. Packet Decoding is used to define structures collected through promiscuous monitoring and we use Decoder to determine if the packet is IPV4, in the IP header with no options, or in IPV6.
4. Storage of decoded and saved data to a file or placed in a data structure is needed.
5. Packet fragmentation of stored data can be done differently such as overlapping packets through fragment reassembly in sequential order and removing wasted space in a window-like disk fragment.
6. The Stream Assembly method is a bit complicated storage mechanism and it has to handle more conditions.
7. Stateful inspection of TCP Session: Stateful inspection helps both the IDS and IPS to perform signature matching as well as the matches to be performed on the contents of the session.
9. Firewalling is alike to firewalls. The main objective of firewalling is to protect both the IDS and IPS from external attacks such as worm, Trojan horses, viruses etc."

8.2. Exploit detection

Next, we will look at how IDS and IPS identify exploits, which is done by using some matching methods such as signature matching, rule matching, and profiling.

8.2.1. How signature matching works

As mentioned earlier, the signature is part of the string that the attacking host sends to the intended victim host that uniquely identifies a particular attack. Signature matching means that the input string passed to the recognition routine matches the pattern in the IDS / IPS signature file. The exact way IDS or IPS performs signature matching varies from system to system. The simplest but most inefficient way is to use fgrep or a similar string search command to compare each part of input passed by the kernel to the recognizer with the list of signatures. Each time the string search command finds a match, a positive identification of the attack occurs.

8.2.2. How rule matching works

Rule-based IDS and IPS, as the name implies, are based on rules. These types of IDSs are generally based on a combination of possible attack indicators and are very promising as they aggregate them to determine if the rule conditions are met. The signature itself can be a clue. In some cases (unusually), the signature, which always indicates an attack, may be the only indicator of an attack required for a rule-based IDS or IPS to issue an alert. However, in most cases you will need a specific combination of indicators.

A very good example is given by Carl Endorf, Gene Schultz, Jim Mellander in "Intrusion Detection and Prevention" as following:

"For example, an anonymous FTP connection attempt from an outside IP address may not cause the system to be suspicious at all. But, if the FTP connection attempt is within, say, 24 hours of a scan from the same IP, a rule-based IDS should become more suspicious. If the FTP connection attempt succeeds and someone goes to the /pub directory and starts entering cd .., cd .., cd .., a good rule-based IDS or IPS should go crazy. This is because what we have here is most likely a dot-dot attack (in which the intention is to get to the root directory itself) with the major antecedent conditions having been present. This example is simple, yet it is powerful. Real rule-based systems generally have much more sophisticated (and thus even more powerful) rules."

8.2.3. How profile-based matching works

Information about the user's session characteristics is recorded in the system log and process list. The profiling routine extracts each user's information and writes it to the data structure they store. Other routines generate statistical criteria based on measurable usage patterns. If a user action occurs that deviates significantly from the normal pattern, the profiling system marks this event and forwards the required information to the output routine. For example, if a user normally signs in from 8am. Until 5:30 pm, but if logs in one day at 2:00 am, a profile-based system could flag this event.

8.3. Malicious code detection

Malicious code is so widespread that there are many different types of malicious code, so antivirus software alone cannot explain the whole problem. Therefore, another important function of intrusion detection and prevention is to detect the presence of malicious code in the system.

IDSs and IPSs generally detect the presence of malicious code in much the same manner as these systems detect attacks in general.

8.3.1. Types of malicious code

According to Edward Skoudis in Malware: Fight Malicious Code (Addison Wesley, 2003), major types of malicious code include the following:

- "Viruses- self-replicating programs that infect files and normally need human intervention to spread
- Worms- self-replicating programs that spread over the network and can spread independently of humans
- Malicious mobile code- programs downloaded from remote hosts, usually (but not always) written in a language designed for interaction with web servers
- Backdoors programs that circumvent security mechanisms (especially authentication mechanisms)
- Trojan horses- programs that have a hidden purpose; usually, they appear to do something useful, but instead they perform some malicious function
- User level rootkits- programs that replace or change programs run by system managers and users
- Kernel level rootkits- programs that modify the operating system itself without indication that this has occurred
- Combination malware- malicious code that crosses across category boundaries"

8.4. Output routines

As soon as the IDS or IPS detection routine detects a potentially unwanted event, the system must at least do something to warn the operator that something is wrong. Therefore, calls within recognition routines typically activate output routines, and most current IDSs and IPSs write events to easily inspectable logs. However, evasive operations are usually much more difficult to perform.

"The following types of evasive actions are currently often found in IDSs and IPSs:

- Output routines can dynamically kill established connections. If a connection appears to be hostile, there is no reason to allow it to continue.
- Systems that appear to have hostile intentions can be blocked (shunned) from further access to a network.
- “A central host that detects attack patterns can recognize a new attack and its manifestations within a successfully attacked system."*

---

*(Endorf, Schultz and Mellander, n.d.)

9. Defending IDS and IPS

Most of the IDS and IPS currently available have little or no ability to monitor their own integrity. Given the importance of intrusion detection and intrusion prevention in so many organizations, this is a very serious problem. An attacker that we wouldn't want to be overlooked could break into a host running IDS or IPS, alter the system, and prevent the attacker's (and possibly others') actions from being recorded. Alternatively, if an attacker sends the input, the IDS or IPS may not handle it properly or a DoS may occur.

Countermeasures against this type of threat include:

- Filtering inputs that can make IDS / IPS inoperable. Stateful firewall is often ideal for this purpose.
- If a particular input can lead to partial or complete destruction of the IDS or IPS, stop further processing of the input. This is an extreme measure, as intrusion detection and prevention features are temporarily suspended while this option is enabled.
- Shunning apparently hostile IP addresses, as discussed previously
- Installation of the internal watchdog feature on the system. This function can determine if the IDS / IPS is working as expected. This feature sends an alert to the operator if the system determines that it is not performing its function properly.

10. Future of intrusion detection and prevention

First, given the significant pitfalls in the signature-based approach, there will continue to be less reliance on signatures in intrusion detection and intrusion prevention.Protocol analysis, target recognition (using cryptographic algorithm output to detect unauthorized changes in files and directories), rule-based intrusion detection (using monitoring-based logic) all are viable alternatives to signature-based intrusion detection, which are likely to become more prevalent. Intrusion prevention continues to grow rapidly due to its ability to shut down attacks, which can completely prevent damage and disruption. Active defense approach assesses system and network conditions and respond appropriately

Corrective actions are still new, but they are already rapidly gaining popularity. Advances can also be expected in the method of data correlation and warning fusion. Tracking the origin of the network connection may also see significant increase is popularity.

Finally, it is reasonable to expect improved forensic capabilities to be incorporated into IDS and IPS.

In the future, honeypots will be used more and more in connection with intrusion detection and prevention. "A honeypot is a decoy server that looks and acts like a normal server, but that does not run or support normal server functions. The main purpose of deploying honeypots is to observe the behavior of attackers in a safe environment, one in which there is (at least in theory) no threat to normal, operational systems."*

11. Conclusion

Intrusion detection systems are a technology that has been used for decades, but some of the basics of the first systems still exist in some respects in today's more modern solutions. Although IDSs are flawed in detection methods and functionality, they continue to be an important part of cybersecurity architecture. Like many security solutions and technologies, IDS is not a simple "install and run" proposition, but is fine-tuned and properly configured to distinguish between normal and potentially malicious traffic, through the installation of different types of architectures which support its flow of information, exploit detection, malware identification, etc. It is not a standalone solution to cybersecurity, but is used in combination with intrusion prevention systems (IPSs) as well as firewalls. It needs to be updated and monitored continuously in order to keep up with today's ever-evolving security threats, and advances in some of the intrusion detection methods are expected more than in other methods.

---

*Source: https://cdn.ttgtmedia.com/searchSecurity/downloads/IDP_Ch17.pdf

References:

1. Endorf, C., Schultz, E. and Mellander, J., n.d. Intrusion detection & prevention. New York.
2. Skoudis, E. and Zeltser, L., 2004. Malware. Upper Saddle River, NJ: Prentice Hall PTR.

3. https://www.sciencedirect.com/topics/computer-science/intrusion-detection (website accessed on 18th of December, 2021)
4. https://www.imperva.com/learn/application-security/intrusion-detection-prevention/ (website accessed on 18th of December, 2021)
5. https://www.computer.org/csdl/magazine/co/2002/04/r4s27/13rRUIJcWgL (website accessed on 18th of December, 2021)
6. https://www.linkedin.com/pulse/overview-ids-ips-khondker-ishtiaq-murshid (website accessed on 18th of December, 2021)
7. https://securitytrails.com/blog/intrusion-detection-systems (website accessed on 18th of December, 2021)