MSc. Part-II

INTERNAL EXAM DOCUMENTATION

SUBJECT : CIS

TOPIC: Network Intrusion Detection and Analysis.

Roll Nos: 7 & 14

An **Intrusion Detection System** (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer. Intrusion Prevention Systems (IPS) extended IDS solutions by adding the ability to block threats in addition to detecting them and has become the dominant deployment option for IDS/IPS technologies. This article will elaborate on the configuration and functions that define the IDS deployment.

An IDS needs only to detect threats and as such is placed out-of-band on the network infrastructure, meaning that it is not in the true real-time communication path between the sender and receiver of information. Rather, IDS solutions will often take advantage of a TAP or SPAN port to analyze a copy of the inline traffic stream (and thus ensuring that IDS does not impact inline network performance).

IDS was originally developed this way because at the time the depth of analysis required for intrusion detection could not be performed at a speed that could keep pace with components on the direct communications path of the network infrastructure.

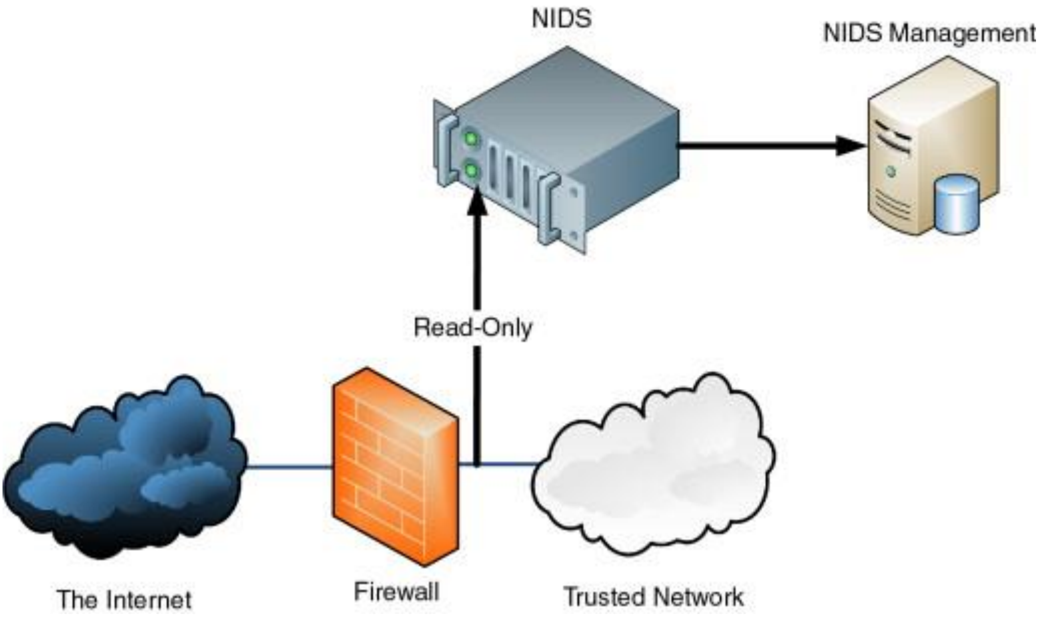
As explained, the IDS is also a listen-only device. The IDS monitors traffic and reports its results to an administrator, but cannot automatically take action to prevent a detected exploit from taking over the system. Attackers are capable of exploiting vulnerabilities very quickly once they enter the network, rendering the IDS an inadequate deployment for prevention device.

Network Intrusion Detection System operators have to protect computer systems in their care from abuse. To achieve protection, they have to harden the systems and limit access to the resources. How much and what access has to be restricted is defined in a security policy. The security policy of a site can be seen as a set of rules users have to obey. On the network as access medium, system operators can resort to a multitude of active security devices like packet filters (i.e. firewalls) or other access control mechanisms. On the other hand, as no protection plan is perfect, the network administrator wants to monitor that the security policy of the site is obeyed by the users and enforced by the existing security devices. That is where Intrusion Detection Systems (IDS) come into play. Their goal is to work as a “burglar alarm” for a resource: If an attacker is violating a rule (meaning he attacks or misuses a resource) in the environment, the IDS is supposed to alert the system operator. As with access control mechanisms, a fundamental problem is how to implement the security policy in an IDS: Security policies have to be translated into technical rules, the IDS is able to understand and check. Intrusion Detection Systems counter this challenge with complexity: The idea is that offering a large set of features enables the operator to effectively implement his policy. IDS can be separated into two classes: Host based Intrusion Detection Systems (HIDS) and Network Intrusion Detection Systems (NIDS). Host based Intrusion Detection Systems monitor the processes running on a single host for policy violations. In contrast, Network Intrusion Detection Systems monitor network packets going to and from all hosts in the network. Both approaches have advantages and disadvantages. HIDS enable a system operator to detect abuse done by users working locally on the host as well as users logged in remotely over the network. In contrast, NIDS can only detect attacks carried out over the network. On the other hand one NIDS can monitor many hosts at once and correlate attacks targeted at several hosts without implying any instrumentation on the hosts itself. In today’s IDS landscape there are also hybrid systems: Typically NIDS that augment their analysis with input from host sensors. In this thesis our focus is on network intrusion detection systems and the techniques they deploy. 5 2 Background (a) (b) Figure 2.1: Standard deployment of network intrusion detection systems 2.1.1 NIDS Deployment NIDS work by analyzing networks packets that are sent to and from the protected resources. In the most common case a NIDS is used to detect attacks on a local network with a single up-link to the Internet as shown in Figure 2.1. In this case the NIDS either has to be supplied with a copy of all packets traversing that link (see Figure 2.1 (a)) or it has to actively forward the packets (see Figure 2.1 (b)). If it is supplied with copies of the packets, it is considered to be ‘‘passive” or “monitoring only” whereas if it forwards the packets itself it is termed “active” or “in-line”. Today, these active systems are also reffered to as Network Intrusion Prevention System (NIPS). If an inline NIDS is detecting malicious behavior, it is able to block (that means not to forward) the malicious traffic. Deploying active NIDS as access control devices is controversial debated in the security community (e.g., [Bej04]). Such a system is “fail-close” as it in case of a crash or failure does not forward packets any more. This at the first glance may be a great advantage but it also means that an active NIDS does introduce a new singlepointof-failure: Deployment of such a system does only make sense if the system adds significantly to the protection of the resources but on the other hand does not hinder people to use the resources as they are supposed to. In other words: if the system often 6 2.1 Network Intrusion Detection blocks legitimate traffic or does crash regularly it is not suitable for productive network environments. Passive NIDS on the other hand are fail-open. If it triggers an alarm there is by default no automatic reaction. The operator may of course, after interpretation of the alarm, react but for many attacks human reaction times are not short enough to prevent an ongoing attack. Nevertheless, even without automatic reaction, the system may deliver valuable information to the network operator: knowing that a system has been compromised enables the system administrators to avert further damage by e.g., information theft. In technical terms, the actively forwarding systems are easier to implement: The NIDS simply provides two network interfaces and is introduced as an additional router into the network link. However, as discussed above, the challenge is to provide enough throughput and keep the pass-through times low. For the passive approach there are two main options: The most popular technique is to configure a so called monitor- or mirror port on a router which duplicates all packets on the Internet access link. The alternative are so called wire-taps: physical devices which resemble something like a T-shaped pipe for network links. For more information on network tapping techniques and sample topologies refer to [Bej04]. 2.1.2 Network Intrusion Detection Quality The goal of a NIDS is to analyze network data in order to detect behavior that could compromise the network security, short attacks, in a given environment.

Detection quality basically is defined along two metrics: false negatives and false positives: The former are missed attacks, meaning there was an actual attack but the IDS did not detect it e.g., due to inappropriate analysis of the data. The latter are false alarms. In this case the IDS issues an alert, but there was no security relevant threat. False positives are often caused by imprecise detection algorithms of the NIDS. On the other hand, unintentionally inappropriate but benign usage of network resources can also trigger false positives. The problem that false negatives cause is apparent. The NIDS is “blind” to certain attacks, drastically reducing the value of a system that should protect resources against misuse. False positives on the other hand imply a different problem: Each alarm triggers some reaction: In the worst case an operator has to check whether the alarm makes sense or not. Like someone who is shouting warnings all the time about a fire that does not exist, the alarms of the NIDS are ignored by the IDS operator at some point. In the case the IDS discovers a real attack, it is likely that the alarm is ignored too. In the case that there is some kind of automatic reaction, e.g., blocking of the corresponding traffic, triggered by an alarm, false positives are fatal too: Alarms now turn to annoyed and complaining end-users which again may render the NIDS to be unusable for the network operators. NIDS operators and developers obviously aim at reducing false negatives and false positives to a minimum. An ideal NIDS would detect every attack (no false negatives) and would never notify the administrator unnecessarily (no false positives). Unfortunately, reducing false negatives and false positives is extremely hard in reality. Bejtlich 7 2 Background reasons in [Bej04] that intrusion detection will never be 100% accurate since they lack context. He defines context to be “the ability to understand the nature of an event with respect to all other aspects of an organizations environment”. More technically, Ptacek et. al. show in [PTN98], how NIDS analysis techniques can be deceived by manipulating network traffic so that the NIDS interprets it different than the actual end system. Modern NIDS come with techniques to counter these attacks e.g, traffic normalization [HKP01] or actively collecting information on the hosts to be protected [SP03a]. In [Axe99] Axelsson points out a more fundamental problem of IDS: They analyze huge amounts of data of which only a quite small fraction is actually malicious. In the paper Bayesian statistics are applied on a typical ratio of malicious and benign “input-events”. The conclusion is, that even a system that has no false negatives at all needs to have a very low false alarm rate (i.e. 1 × 10−5) in order to achieve substantial values of the Bayesian detection rate (that is the probability of an intrusion under the condition that there is an alarm). 2.1.3 Network Intrusion Detection Techniques Network Intrusion Detection Systems can be classified into three categories each using a different approach of detecting attacks. The two traditional approaches are called misuse detection and anomaly detection. A rather new approach is the so called specificationbased detection. We now take a closer look at each technique and it advantages and disadvantages. Misuse detection is based on a definition of misuse. That means the behavior that is considered to be dangerous or compromising has to be described to the NIDS. The NIDS then compares the current usage of the resources with the misuse usage patterns and alerts on matches. Most NIDS incorporate misuse detection by implementing signature matching. A signature, in this context, is a characteristic byte pattern of a known attack. What attacks can be detected by signatures and how good the detection quality is, depends among others on how exact the characteristic attack patterns can be described. Most NIDS nowadays allow signatures to use regular expressions for describing the byte patterns. This technique adds significantly to detection quality [SP03b]. On the other hand, powerful matching capabilities are no guarantee for high signature quality. To our experience, for the open source NIDS snort [Roe99] many signatures have poor quality, resulting in a lot of apparent false positives. Nevertheless, given signatures of good quality, meaning signatures that tightly describe a characteristic misuse pattern, the resulting low rate of false positives is the huge advantage of misuse detection. The most significant disadvantage of misuse detection is the conceptual inability to detect unknown attacks. The second traditional approach to intrusion detection is anomaly detection. As is apparent from the name this technique works by distinguishing normal behavior from non-normal behavior. For anomaly based NIDS the idea is, that traffic containing an attack looks different than normal traffic. Having a knowledge base of normal behavior patterns, the IDS compares certain characteristics of the current behavior with the corresponding characteristics of the normal behavior from the knowledge base. If the 8 2.2 Bro deviation between the normal and the current behavior exceeds some threshold, the IDS issues an alarm. In practice there is a wealth of heuristics that implement anomaly detection for NIDS. Usually statistic methods are used to gain an abstract view on the network traffic that in turn can be compared to the same statistic view on normal network traffic. A popular example for a statistic metric is “transferred volume per time interval”. For every time interval of size t the transmitted traffic volume v is measured and compared against what is considered the normal transmission volume vnorm. The fundamental problem of anomaly detection can also be seen in this example: How to get an appropriate value for vnorm; or more generally: How to define normal behavior? For the example outlined before one could compare v against the volume v ′ measured at the same time of day exactly one week before. In this case one would assume that the volume v ′ resembled normal behavior. The advantage of anomaly detection is clearly the ability to detect unknown attacks. On the other hand the extreme variability of regular network traffic makes it very hard to come up with statistical metrics that are stable as long as everything behaves normal but show significant deviation as attacks take place. This usually results in a high false positive rate since regular traffic variability often causes significant deviation in typical statistical traffic metrics. The third approach, specification based detection, aims at combining the advantages of misuse detection and anomaly detection. The idea is that the operator specifies the allowed behavior manually. Everything that occurs and is not specified violates the security policy and is therefore considered an attack. The advantage of the approach is that detection quality is high. By doing a specification derived from the security policy false negatives as well as false positives can be minimized. The disadvantage is, that it is a very labor-intensive process to (i) map out a comprehensive security policy and (ii) generate a tight specification for that policy. Furthermore, generating the specification once is not enough. Especially in large network environments the policy and the specification have to be continuously adapted to the network usage profile.

An **intrusion detection system** (**IDS**) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.[1]

IDS types range in scope from single computers to large networks.[2] The most common classifications are **network intrusion detection systems** (**NIDS**) and **host-based intrusion detection systems** (**HIDS**). A system that monitors important operating system files is an example of an HIDS, while a system that analyzes incoming network traffic is an example of an NIDS. It is also possible to classify IDS by detection approach. The most well-known variants are signature-based detection (recognizing bad patterns, such as malware) and anomaly-based detection (detecting deviations from a model of "good" traffic, which often relies on machine learning). Another common variant is reputation-based detection (recognizing the potential threat according to the reputation scores). Some IDS products have the ability to respond to detected intrusions. Systems with response capabilities are typically referred to as an **intrusion prevention system**.[3] Intrusion detection systems can also serve specific purposes by augmenting them with custom tools, such as using a honeypot to attract and characterize malicious traffic.[4]



Comparison with firewalls[edit]

Although they both relate to network security, an IDS differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS describes a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. This is traditionally achieved by examining network communications, identifying heuristics and patterns (often known as signatures) of common computer attacks, and taking action to alert operators. A system that terminates connections is called an intrusion prevention system, and performs access control like an application layer firewall.[5]

Intrusion prevention

Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPS for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPS have become a necessary addition to the security infrastructure of nearly every organization.[18]

IDPS typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPS can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.[18]

Intrusion prevention systems (**IPS**), also known as **intrusion detection and prevention systems** (**IDPS**), are network security appliances that monitor network or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, report it and attempt to block or stop it.[19].

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected.[20]:273[21]:289 IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.[22] An IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues, and clean up unwanted transport and network layer options.

What is the function of an intrusion detection system on a network?

Intrusion detection is a passive technology; it detects and acknowledges a problem but interrupt the flow of network traffic, Novak said. “As mentioned, the purpose is to find and alert on noteworthy traffic. An alert informs the IDS analyst that some interesting traffic has been observed. But it is after-the-fact because the traffic is not blocked or stopped in any way from reaching its destination.”

Compare that to firewalls that block out known malware and intrusion prevention system (IPS) technology, which as the name describes, also blocks malicious traffic.

Although an IDS doesn’t stop malware, cybersecurity experts said the technology still has a place in the modern enterprise.

“The functionality of what it does is still critically important,” said Eric Hanselman, chief analyst with 451 Research. “The IDS piece itself is still relevant because at its core it’s detecting an active attack.”

However, cybersecurity experts said organizations usually don’t buy and implement IDS as a standalone solution as they once did. Rather, they buy a suite of security capabilities or a security platform that has intrusion detection as one of many built-in capabilities.

Rob Clyde, board of directors vice chair ISACA, an association for IT governance professionals, and executive chair for the board at White Cloud Security Inc., agreed that intrusion detection is still a critical capability. But he said companies need to understand that an intrusion detection system requires maintenance and consider whether, and how, they’ll support an IDS if they opt for it.

“Once you’ve gone down the path to say we’re going to keep track of what’s going on in our environment, you need someone to respond to alerts and incidents. Otherwise, why bother?” he said.

Given the work an IDS takes, he said smaller companies should have the capability but only as part of a larger suite of functions so they’re not managing the IDS in addition to other standalone solutions. They should also consider working with a managed security service provider for their overall security requirements, as the provider due to scale can more efficiently respond to alerts. “They’ll use machine learning or maybe AI and human effort to alert your staff to an incident or intrusion you truly have to worry about,” he said.

“And at mid-size and larger companies, where you really need to know if someone is inside the network, you do want to have the additional layer, or additional layers, than just what’s built into your firewall,” he said.

3 challenges of managing an IDS

Intrusion detection systems do have several recognized management challenges that may be more work than an organization is willing or able to take on.

1. **False positives** (i.e., generating alerts when there is no real problem). “IDSs are notorious for generating false positives,” Rexroad said, adding that alerts are generally are sent to a secondary analysis platform to help contend with this challenge.

This challenge also puts pressure on IT teams to continually update their IDSs with the right information to detect legitimate threats and to distinguish those real threats from allowable traffic.

It’s no small task, experts said.

“IDS systems must be tuned by IT administrators to analyze the proper context and reduce false-positives. For example, there is little benefit to analyzing and providing alerts on internet activity for a server that is protected against known attacks. This would generate thousands of irrelevant alarms at the expense of raising meaningful alarms. Similarly, there are circumstances where perfectly valid activities may generate false alarms simply as a matter of probability,” Rexroad said, noting that organizations often opt for a secondary analysis platform, such as a Security Incident & Event Management (SIEM) platform, to help with investigating alerts.

2. **Staffing.** Given the requirement for understanding context, an enterprise has to be ready to make any IDS fit its own unique needs, experts advised.

   “What this means is that an IDS cannot be a one-size-fits all configuration to operate accurately and effectively. And, this requires a savvy IDS analyst to tailor the IDS for the interests and needs of a given site. And, knowledgeable trained system analysts are scarce,” Novak added.

3. **Missing a legitimate risk.** “The trick with IDS is that you have to know what the attack is to be able to identify it. The IDS has always had the patient zero problem: You have to have found someone who got sick and died before you can identify it,” Hanselman said.

   IDS technology can also have trouble detecting malware with encrypted traffic, experts said. Additionally, the speed and distributed nature of incoming traffic can limit the effectiveness of an intrusion detection system in an enterprise.

   “You might have an IDS that can handle 100 megabits of traffic but you might have 200 megabits coming at it or traffic gets distributed, so your IDS only sees one out of every three or four packets,” Hanselman said.