NETWORK BASED IDS

IDSs operate as network-based, host-based, or application-based systems. A network-based !OS is focused on protecting network information assets. A host -based version is focused on protecting the server or host's information assets. Figure 7-1 shows an example that monitors both network connection activity and current information states on host servers. The application-based model works on one or more host systems that support a single application and is oriented to defend that specific application from special forms of attack. Regardless of whether they operate at the network, host, or application level, all IDSs use one of two detection methods: signature-based or statistical anomaly-based. Each of these approaches to intrusion detection is examined in detail in the following sections.

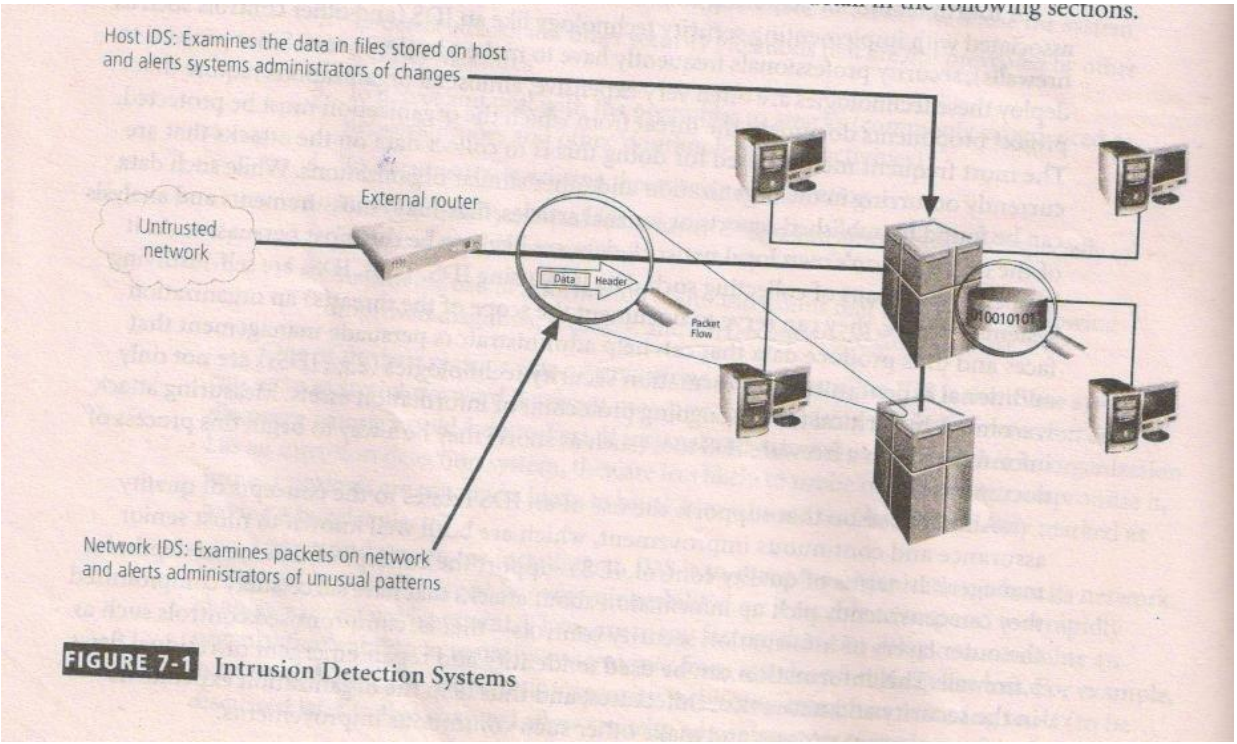

FIGURE 7-1 Intrusion Detection Systems

Network-Based IDS

A **network-based IDS (NIDS)** resides on a computer or appliance connected to a segment of an organization's network and monitors network traffic on that network segment, looking for indications of ongoing or successful attacks. When a situation occurs that the NIDS is programmed to recognize as an attack, it responds by sending notifications to administrators. When examining the packets "transmitted through an organization's networks, a NIDS looks for attack patterns within network traffic such as large collections of related items that are of a

certain type, which could indicate that a denial-of service attack is underway, or the exchange of a series of related packets in a certain pattern, which could indicate that a port scan is in progress. A NIDS can detect many more types of attacks than a host-based IDS, but to do so, it requires a much more complex configuration and maintenance program.

A NIDS is installed at a specific place in the network (such as on the inside of an edge router) from where it is possible to watch the traffic going into and out of a particular network segment. The NIDS can be deployed to watch a specific grouping of host computers on a specific network segment, or it may be installed to monitor all traffic between the systems that make up an entire network. When placed next to a hub, switch, or other key networking device, the NIDS may use that device's monitoring port. The monitoring port, also known as a switched port analysis (SPAN) port or mirror port, is a specially configured connection on a network device that is capable of viewing all of the traffic that moves through the entire device. In the early '90s, before switches became the popular choice for connecting networks in a shared-collision domain, hubs were used. Hubs received traffic from one node, and retransmitted it to all other nodes. This configuration allowed any device connected to the hub to monitor all traffic passing through the hub. Unfortunately, it also represented a security risk, since anyone connected to the hub could monitor all the traffic that moved through that network segment. More recently, switches have been deployed on most networks, and they, unlike hubs, create dedicated point-to-point links between their ports. These links create a higher level of transmission security and privacy, and effectively prevent anyone from being able to capture, and thus eavesdrop on, the traffic passing through the switch. Unfortunately, however, this ability to capture the traffic is necessary for the use of an IDS. Thus, monitoring ports are required. These connections enable network administrators to collect traffic from across the network for analysis by the IDS as well as for occasional use in diagnosing network faults and measuring network performance.

Figure 7-2 shows a sample screen from Demark Pure Secure (see www.demarc.com) displaying events generated by the Snort Network IDS Engine (see www.snort.org

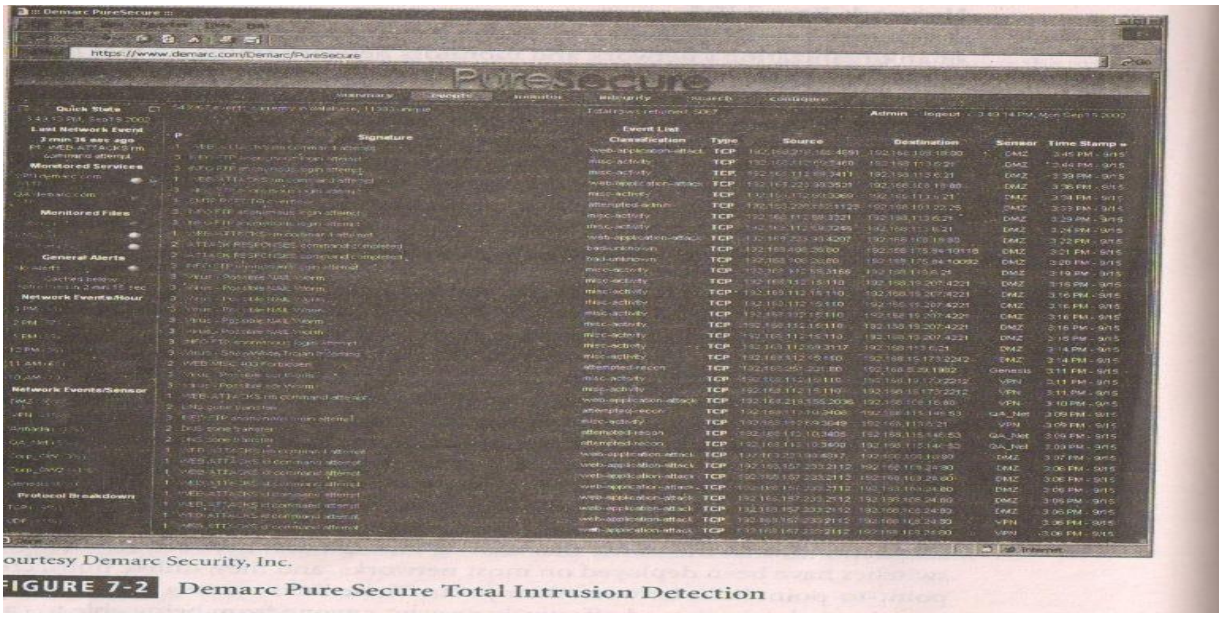

FIGURE 7-2 Demarc Pure Secure Total Intrusion Detection

NIDS Signature Matching: To determine whether or not an attack has occurred or may be underway, NIDSs must look for attack patterns by comparing measured activity to known signatures in their knowledge base. This is accomplished by the comparison of cap turned network traffic using a special implementation of the TCP/IP stack that reassembles the packets and applies protocol stack verification, application protocol verification, and/or other verification and comparison techniques.

In the process of protocol stack verification, the NIDSs look for invalid data packets i.e., packets that are malformed under the rules of the TCPIIP protocol A data packet is verified when its configuration matches that defined by the various Internet protocols (e.g., TCP, UDP, IP). The elements of the protocols in use (IP, TCP, UDP, and application layers such as HTTP) are combined in a complete set called the protocol stack when the software is implemented in an operating system or application. Many types of intrusions, especially DoS and DDoS attacks, rely on the creation of improperly formed packets to take advantage of weaknesses in the protocol stack in certain operating systems or applications.

In application protocol verification, the higher-order protocols (e.g., HTTP, FTP, Telnet) are examined for unexpected packet behavior, or improper use. Sometimes an intrusion involves the arrival of valid protocol packets but in excessive quantities (in the case of the Tiny Fragment Packet attack, the packets are also excessively fragmented).

While the protocol stack verification looks for violations in the protocol packet structure, the application protocol verification looks for violations in the protocol packet use. One example of this kind of attack is DNS cache poisoning, in which valid packets exploit poorly configured DNS servers to inject false information to corrupt the servers' answers to routine DNS queries from other systems on the network. Unfortunately, however, this higher-order examination of traffic can have the same effect on an IDS as it can on a firewall-that is, it slows the throughput of the system. As such, it may be necessary to have more than one NIDS installed, with one of them performing protocol stack verification and one performing application protocol verification.

Advantages and Disadvantages of NIDSs: The following is a summary, taken from Bace and Mell, of the advantages and disadvantages of NIDSs:

Advantages:

1. Good network design and placement of NIDS devices can enable an organization to use a few devices to monitor a large network.
2. NIDSs are usually passive devices and can be deployed into existing networks with little or no disruption to normal network operations.
3. NIDSs are not usually susceptible to direct attack and, in fact, may not be detectable by attackers.

Disadvantages:

1. A NIDS can become overwhelmed by network volume and fail to recognize attacks it might otherwise have detected. Some IDS vendors are accommodating the need for ever faster network performance by improving the processing of detection algorithms in dedicated hardware circuits to gain a performance advantage. Additional efforts to optimize rule set processing may also reduce overall effectiveness in detecting attacks.
2. NIDSs require access to all traffic to be monitored. The broad use of switched Ethernet

networks has replaced the ubiquity of shared collision domain hubs. Since many switches have limited or no monitoring port capability, some networks are not capable of providing aggregate data for analysis by a NIDS. Even when switches do provide monitoring ports, they may not be able to mirror aJl activity with a consistent and reliable time sequence.

3. NIDSs cannot analyze encrypted packets, making some of the network traffic invisible to the process. The increasing use of encryption that hides the contents of some or all of the packet by some network services (such as SSL, SSH, and VPN) limits the effectiveness of NIDSs.

4. NIDSs cannot reliably ascertain if an attack was successful or not. This requires the network administrator to be engaged in an ongoing effort to evaluate the results of the lugs of suspicious network activity.

5. Some forms of attack are not easily discerned by NIDSs, specifically those involving fragmented packets. In fact, some NIDSs are particularly susceptible to malformed packets and may become unstable and stop functioning.4