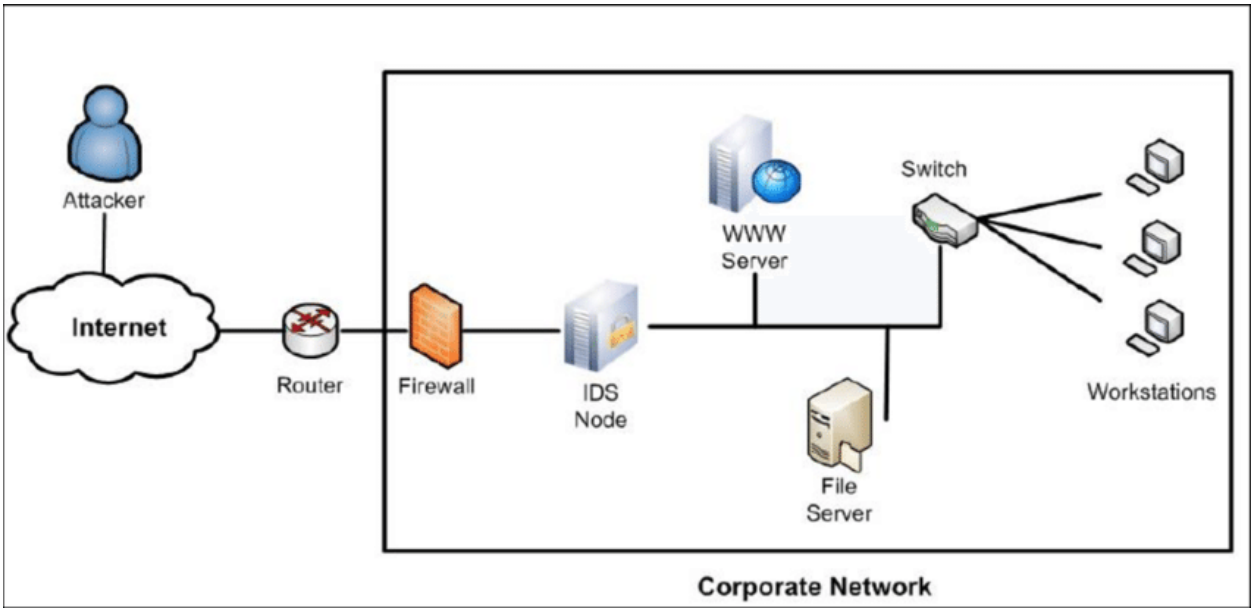
Intrusion Detection System

A system that tries to identify attempts to hack or break into a computer system or to misuse it. IDSs may monitor packets passing over the network, monitor system files, monitor log files, or set up deception systems that attempt to trap hackers.
Computer systems have become more vulnerable to intrusions than ever. Intrusion Detection is a security technology that allows not only the detection of attacks, but also attempts to provide notification of new attacks unforeseen by other components. Intrusion detection is an important component of a security system, and it complements other security technologies.



How does an IDS work?

While there are several types of IDS's, the most common types work the same. They analyze network traffic and log files for certain patterns. What kind of patterns you may ask? While a firewall will continually block a hacker from connecting to a network, most firewalls never alert an administrator.

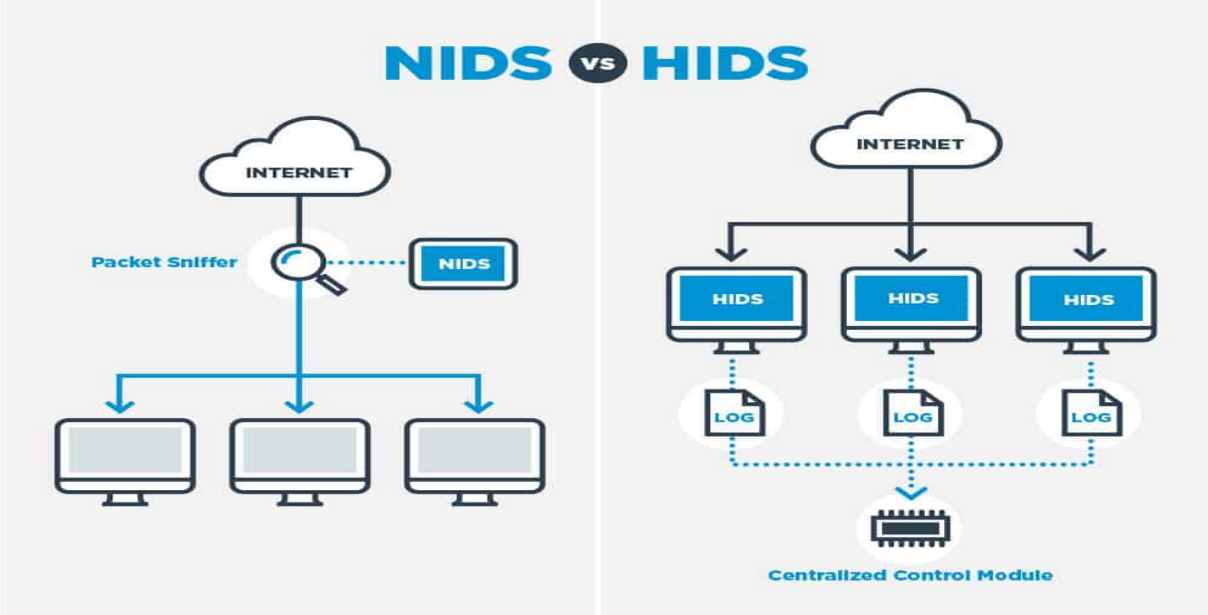
The administrator may notice if he/she checks the access log of the firewall, but that could be weeks or even months after the attack. This is where an IDS comes into play. The attempts to pass through the firewall are logged, and IDS will analyze its log. At some point in the log there will be a large number of request-reject entries. An IDS will flag the events and alert an administrator. The administrator can then see what is happening right after or

even while the attacks are still taking place. This gives an administrator the advantage of being able to analyze the techniques being used, source of attacks, and methods used by the hacker.

Following are the types of intrusion detection systems :-

1) **Host-Based Intrusion Detection System (HIDS)**: Host-based intrusion detection systems or HIDS are installed as agents on a host. These intrusion detection systems can look into system and application log files to detect any intruder activity.

2) **Network-Based Intrusion Detection System (NIDS)**: These IDSs detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment, thereby protecting those hosts. Network-based IDSs often consist of a set of single-purpose sensors or hosts placed at various points in a network. These units monitor network traffic, performing local analysis of that traffic and reporting attacks to a central management console.



intrusion detection are as follows :-

1) **Signatures:** Signature is the pattern that you look for inside a data packet. A signature is used to detect one or multiple types of attacks. For example, the presence of "scripts/iisadmin" in a packet going to your web server may indicate an intruder activity. Signatures may be present in different parts of a data packet depending upon the nature of the attack.

2) **Alerts:** Alerts are any sort of user notification of an intruder activity. When an IDS detects an intruder, it has to inform security administrator about this using alerts. Alerts

may be in the form of pop-up windows, logging to a console, sending e-mail and so on. Alerts are also stored in log files or databases where they can be viewed later on by security experts.

3) **Logs:** The log messages are usually saved in file.Log messages can be saved either in text or binary format.

4) **False Alarms:** False alarms are alerts generated due to an indication that is not an intruder activity. For example, misconfigured internal hosts may sometimes broadcast messages that trigger a rule resulting in generation of a false alert. Some routers, like Linksys home routers, generate lots of UPnP related alerts. To avoid false alarms, you have to modify and tune different default rules. In some cases you may need to disable some of the rules to avoid false alarms.

5) **Sensor:** The machine on which an intrusion detection system is running is also called the sensor in the literature because it is used to "sense" the network.

SNORT:

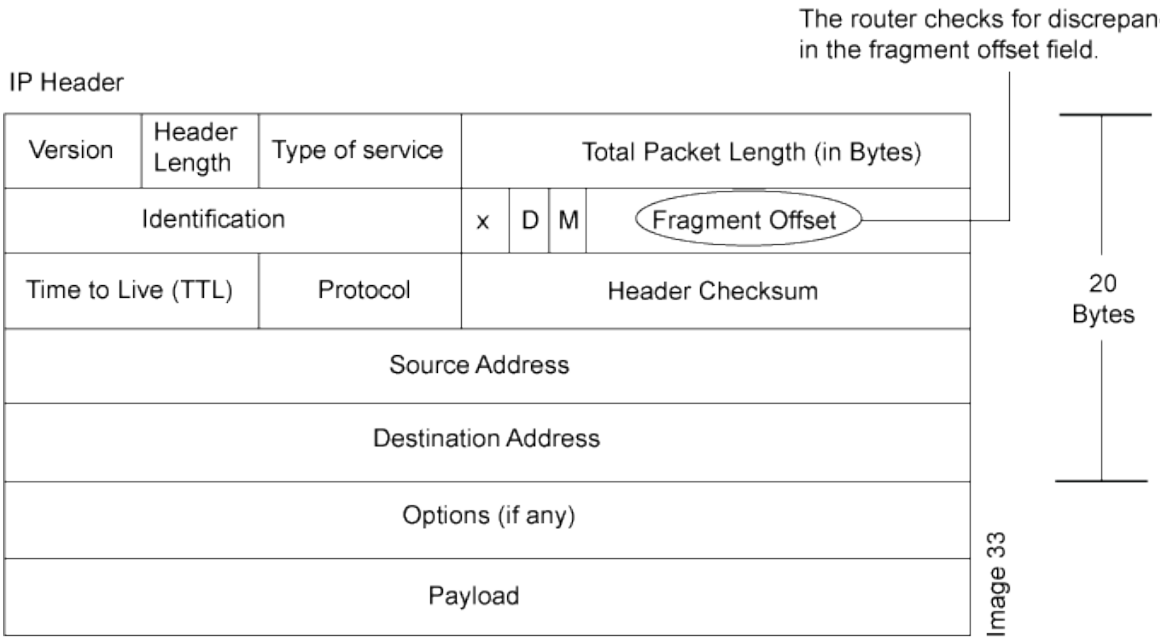
Snort is a very flexible network intrusion detection system that has a large set of pre-configured rules. Snort also allows you to write your own rule set. There are several mailing lists on the internet where people share new snort rules that can counter the latest attacks.
Snort is a modern security application that can perform the following three functions :
* It can serve as a packet sniffer.
* It can work as a packet logger.
* It can work as a Network-Based Intrusion Detection System (NIDS).

In Teardrop Attack, fragmented packets that are sent in the to the target machine, are buggy in nature and the victim's machine is unable to reassemble those packets due to the bug in the TCP/IP fragmentation.

In this way, the packets keep on getting accumulated over the victim's machine and finally due to the buffer overflow, the target machine crashes down.

How Teardrop Attack works?

Here, I am taking a reference from the Juniper's technical publication to illustrate how does it work —



As you can see in the above figure of IP header, which operates at the network layer, there is a field called fragment offset field.

Teardrop Attack and Fragment Offset:

Understand it like this — When a large amount of data is sent across the internet, the data is broken into the smaller fragments. Each of these fragments is assigned a number. When they reach the receiving end, these fragments are rearranged to reproduce the original data or message.

To identify the sequencing of the fragments, **the fragment offset field** holds the necessary information using which the target machine rearranges the sequence.

However, in the Teardrop Attack, the fragment offset field is made buggy by the hacker so the victim's machine is unable to find the relative fragments.

So, as the name suggests, the buggy packets keep on accumulating at the victim's side like teardrops and ultimately it leads to the machine crash.

However, modern networking devices can detect this discrepancy in a fragmented packet. Once they detect the problem, they simply drop the packet.