Snort

The Network intrusion detection systems like snort (2001) typically use **signature detection**, matching patterns in network traffic to the patterns of known attacks. ... Network anomaly detectors look for unusual traffic rather than unusual system calls.

Snort is an Open Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

Snort can be deployed inline to stop these packets, as well. Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger — which is useful for network traffic debugging, or it can be used as a full-blown network intrusion prevention system. Snort can be downloaded and configured for personal and business use alike.

Due to low signal-to noise ratio in the case of a bad choice of rules, and due to Snort missing attacks completely in the case of a Snort system with rules not being updated properly.

Apart from the challenge of choosing/writing good rules for Snort, there is a related disadvantage - since Snort only looks for things defined in its ruleset, it doesn’t have the ability to tell what traffic is considered to be normal from each host on the network, and what traffic seems to be out of place. This way, ’normal’ behaviour but from the ’wrong’ computer on the network isn’t noticed unless rules are setup on a host-by-host basis.

There are a few systems who have started to deal with this problem, called anomaly-based intrusion detection systems

* Bro (Zeek)

 Bro is both a signature and anomaly-based IDS

Zeek is not an active security device, like a firewall or intrusion prevention system. Rather, Zeek sits on a “sensor,” a hardware, software, virtual, or cloud platform that quietly and unobtrusively observes network traffic. Zeek interprets what it sees and creates compact, high-fidelity transaction logs, file content, and fully customized output, suitable for manual review on disk or in a more analyst-friendly tool like a security and information event management (SIEM) system.

“Zeek is an intrusion detection system that works differently from other systems because of its focus on network analysis. While rules-based engines are designed to detect an exception, Zeek looks for specific threats and trigger alerts.

While Zeek IDS can certainly be used as a traditional IDS, users more frequently use Zeek to record detailed network behavior. For example, it can be used to keep long-term records of all HTTP requests and results – or tables correlating MAC and IP addresses.