

# [Bro: a system for dectecting network intruders in real-time](https://assignbuster.com/bro-a-system-for-dectecting-network-intruders-in-real-time/)

[Technology](https://assignbuster.com/essay-subjects/technology/), [Information Technology](https://assignbuster.com/essay-subjects/technology/information-technology/)

Bro: A System for Detecting Network Intruders in Real-Time Overview Bro, a standalone system detector is described by passively monitoring a network that links over the intruder’s traffic transit. The system has system designs that are meant to emphasize high speed monitoring, clear separation between the policy and mechanism, and real time notifications (Paxson, 1998). The policy has various advantages that enable event handlers to synthesize new events, update state information, record the information to disks, as well as generate real time notifications through the syslog. Most importantly, it enables the reduction of kernel-filtered network traffic stream into series of high level events.
Body
The growing internet connectivity has created growing opportunities for attackers to unlawfully get their way in computers over the networks. The setback of detecting such attacks is referred to as network intrusion detection, which is a relatively new area of security research. These systems can be divided into two types; those that operate alone by observing network traffic directly and passively using a packet filter, and those that depend on audit information that is gathered by the host in the network that they are trying to protect (Paxson, 1998).
There is an increasing interest on building hybrid systems that will combine these two approaches. Bro is abstractly divided into an event engine that enables the reduction of stream of filtered packets to the stream of high level network events, and an interpreter specialized for language used in expressing site security policy (Paxson, 1998). Structurally, it is set in layers, with the lower layer processing the greatest volume of data. As one goes high through the layers, the data system diminishes giving room for processing of data per item.
This system has various advantages that makes anyone who uses it recognize its reliability. It has high speed and large mechanisms for monitoring the environment. It enables us view the supreme source of threats as external hosts when connecting to the host over the internet. It also offers real time notifications, as well as enables full recording of every attacker’s network activity (Paxson, 1998). It has also separated mechanism from policy; this buys flexibility and simplicity. This is advantageous since it helps handle the high volume of traffic.
Lastly, I loved this system because it can access the monitor code; thus, enabling the detection of the attacker’s break-in activity. Additionally, this system has the most impressive record in the way it is able to avoid simple mistakes; that is to say it is reliable. It is free, simple and capable of avoiding defiance of the security policy by being both clear and error free.
This system enables us understand the security and management by having a clear overview of its structures and the language used in expressing security policy. The system is implemented with specialized analysis; thus, it uses regular expression matching records, rather than reusing existing ones (Paxson, 1998). There are hopes that the system is going to benefit the community in the ongoing operations without incurring any packet drops. Security management might be a hard task due to problems such as overload attacks, crash attacks, and subterfuge attacks. Unless we are careful keeping track on these contiguous data, the obvious attack will keep reoccurring.
References
Paxson, V. (1998). Bro: A System for Detecting Network Intruders in Real-Time. Computer Networks, 1-22.