Key Benefits

- Honeypot based intrusion detection
- Real time detection
- Detects unknown threats
- Effective against internal and external threats
- Simple to use
- Highly configurable
- Advanced server emulation
- Detailed logging
- No false positives
- Lower hardware requirements
- Lower total cost of ownership

"A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource" - The Honeypot Maillist Group

Product Overview

KFSensor

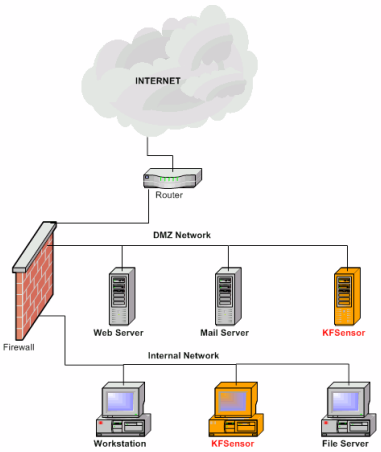
New threats are constantly emerging to the security of organisations' information systems infrastructure. Firewalls and VPNs cannot prevent all intrusions and do little to prevent attacks from within the organisation itself.

Intrusion detection plays a vital role in ensuring the integrity of a network's security. Network intrusion detection systems (NIDS) have long been seen as the most effective means of detecting attacks. However they do have significant weaknesses.

The increasing quantity and diversity of legitimate network traffic has resulted in ever increasing hardware costs and the large number of false positive alerts generated can be too much to analyse effectively.

By relying on the search for known attack signatures NIDS are unable to detect new forms of attacks and the use of encryption prevents them examining traffic altogether.

An additional approach is required to tackle such problems.

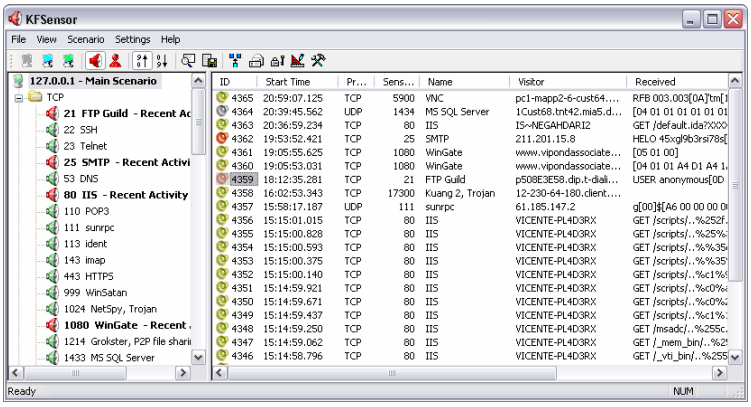


Honeypot technology

A honeypot is a system that is put on a network with the intention that it can be probed and attacked, in order to gain information on an attacker. This concept is a radically different approach to other forms of security and one that is increasingly being recognised to be very effective in detecting security threats.

By allowing intruders to interact with the honeypot, detailed information can be gathered on the techniques and tools that they use. Because there is no legitimate use for the honeypot, all connections it receives are suspect. This results in very few false positive alerts.

KFSensor has been developed from the ground up, as a production honeypot system, dedicated to the task of intrusion detection. Used as part of a comprehensive security strategy, KFSensor adds an additional layer of protection to detect security breaches that may not be picked up by other means.



How KFSensor works

KFSensor is easy to install and configure. It takes just five minutes to set up and become operational. No special hardware is required and its efficient design enables it to run even on low specification Windows machines.

Its straightforward Windows interface controls all functionality. There is no need to edit complex configuration files and it comes pre-configured with all the major systems services required.

KFSensor works by simulating systems services at the highest level of the OSI Network Model - the application layer. This enables it to make full use of Windows security mechanisms and networks libraries, reducing the risk of detection and compromise by not introducing additional drivers and custom IP stacks. A machine running KFSensor can be treated as just another server on the network, without the need to make complex changes to routers and firewalls.

KFSensor provides immediate benefits in revealing the nature and quantity of attacks on a network. By consolidating all the network traffic of an attack into a single alert KFSensor makes it easy to explain a security threat to non-specialist staff.

The information KFSensor generates can be used to refine firewall rules and produce new signatures for network intrusion detection systems.

KFSensor is an extremely cost effective way of enhancing network security infrastructure.

Product Features

KFSensor

Key Features

- Production honeypot
- Monitors multiple ports
- All ports configurable
- Define custom responses
- Supports both TCP and UDP services
- Sophisticated emulation of system services including:
  - FTP
  - HTTP
  - POP3
  - Telnet
  - SMTP
  - VNC
- Sends alerts by email
- DOS attack protection
- All bytes of attack are logged
- System tray indicator
- Colour coded alert warnings
- Filter logs by port or IP address
- Configurable reports
- Export logs in multiple formats

For more information on KFSensor look at our website:

www.keyfocus.net

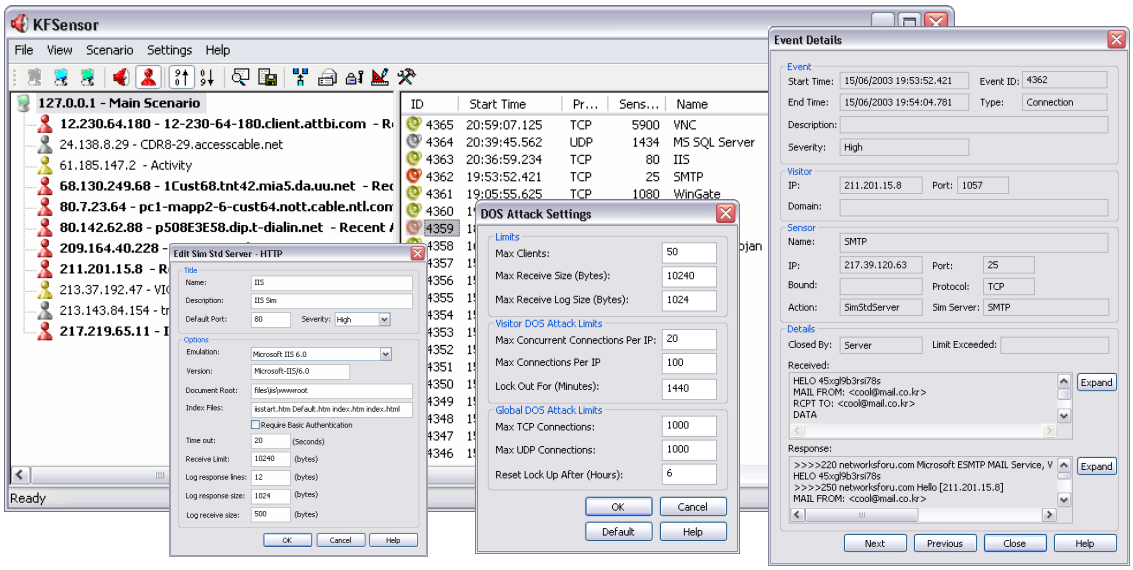
or email us at

contact@keyfocus.net

At the heart of KFSensor sits a powerful internet daemon service that is built to handle multiple ports and IP addresses. It is written to resist denial of service and buffer overflow attacks.

Building on this flexibility KFSensor can respond to connections in a variety of ways, from simple port listening and basic services (such as echo), to complex simulations of standard system services. For the HTTP protocol KFSensor accurately simulates the way Microsoft's web server (IIS) responds to both valid and invalid requests. As well as being able to host a website it also handles complexities such as range requests and client side cache negotiations. This makes it extremely difficult for an attacker to fingerprint, or identify KFSensor as a honeypot.

Every byte of an attack is recorded in KFSensor's logs. Events can be assigned different colour coded severities, making it easy to spot anything unusual or serious. Custom reports can be defined and the log can be filtered to show just those from a certain port, protocol or source IP address.



Example SMTP attack and response

By emulating the behaviour of a vulnerable SMTP server an attacker uses it in an attempt to relay spam. This reveals the source and purpose of the attack with no risk of compromise.

```
>>>>220 networksforu.com Microsoft ESMTP MAIL Service, Version: 6.0.2600.1106 ready at  Mon, 10 Jun 2003
17:26:21 +0000
HELO qqq-6j4vecjhtdb
>>>>250 networksforu.com Hello [61.99.243.194]
MAIL FROM:<SuperMan2173912016@hotmail.com>
>>>>250 2.1.0 SuperMan2173912016@hotmail.com....Sender OK
RCPT TO:<ch69v5@hotmail.com>
>>>>250 2.1.5 ch69v5@hotmail.com
DATA
>>>>354 Start mail input; end with <CRLF>.<CRLF>
From: <SuperMan2173912016@hotmail.com>
To: ch69v5@hotmail.com
Subject: SuperMan - 217.39.120.16
X-Mailer: SuperMail v1.1
Mime-Version: 1.0
Content-Type: text/plain;%09charset=us-ascii

Server Test - 217.39.120.16
.
>>>>250 2.6.0 <NETWORKSFORULvx4efKx00008432@networksforu.com> Queued mail for delivery
QUIT
```

About KeyFocus

Keyfocus is a software company dedicated to developing network and system security software. KeyFocus was one of the first companies to recognise the potential of honeypot technology to move beyond a research tool and become a valuable production system, which could complement and enhance an organisation's existing security infrastructure.

Our goal is to work closely with our customers so we can continue to offer the best product in this exciting and rapidly developing field.

KeyFocus