Web link for install

http://www.keyfocus.net/kfsensor/

Honey Pot is a device placed on Computer Network specifically designed to capture malicious network traffic. KF Sensor is the tool to setup as honeypot when KF Sensor is running it places a siren icon in the windows system tray in the bottom right of the screen. If there are no alerts then green icon is displayed.

INTRODUCTION: HONEY POT:

A honeypot is a computer system that is set up to act as a decoy to lure cyber attackers, and to detect, deflect or study attempts to gain unauthorized access to information systems.

Generally, it consists of a computer, applications, and data that simulate the behavior of a real system that appears to be part of a network but is actually isolated and closely monitored. All communications with a honeypot are considered hostile, as there's no reason for legitimate users to access a honeypot. Viewing and logging this activity can provide an insight into the level and types of threat a network infrastructure faces while distracting attackers away from assets of real value.

Honeypots can be classified based on their deployment (use/action) and based on their level of involvement. Based on deployment, honeypots may be classified as:

1. Production honeypots
2. Research honeypots

Production honeypots are easy to use, capture only limited information, and are used primarily by companies or corporations. Production honeypots are placed inside the production network with other production servers by an organization to improve their overall state of security. Normally, production honeypots are low-interaction honeypots, which are easier to deploy. They give less information about the attacks or attackers than research honeypots.

Research honeypots are run to gather information about the motives and tactics of the Black hat community targeting different networks. These honeypots do not add direct value to a specific organization; instead, they are used to research the threats that organizations face and to learn how to better protect against those threats.

KF SENSOR:

KFSensor is a Windows based honeypot Intrusion Detection System (IDS). It acts as a honeypot to attract and detect hackers and worms by simulating vulnerable system services and trojans. By acting as a decoy server it can divert attacks from critical systems and provide a higher level of information than can be achieved by using firewalls and NIDS alone. KFSensor is a system installed in a network in order to divert and study an attacker's behavior. This is a new technique that is very effective in detecting attacks.

The main feature of KFSensor is that every connection it receives is a suspect hence it results in very few false alerts. 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.

KFSensor installs a new system tray (systray) icon in the shape of a siren on the desktop. You click the siren icon to launch the KFSensor monitor, and it is used liberally throughout the program to indicate KFSensor's current status. On the desktop, it will usually be gray, but it will flash red or yellow, based on event activity. The systray icon will flash until you view the KFSensor monitor, although its behavior can be customized. Low-priority events are just logged, and no alert is generated. Medium-priority events alert and make the systray icon flash yellow and orange. High-priority events alert and make the systray icon flash red and orange.

Emulating Services with KFSensor

Each port in the Port view represents a listener. Listeners are attached to actions. Actions can be close, close and read, or call up a simulated server. The close action will immediately close the connection and log the event. Read and close will wait for the visitor to send a request, and then close the connection without sending a response. A listener can also be attached to a server action.

KFSensor calls emulated services *sim servers*, short for simulated servers. A single instance of KFSensor can have an unlimited number of sim servers defined, although only 256 can be active at once. KFSensor has two types of sim servers: *sim banner* and *sim* *standard*. Some services, like FTP and SMTP, exist as both sim banner servers and sim standard servers, and listen on TCP or UDP ports, depending on the requirements of the environment.

Sim Banner Servers

Sim banner servers are simple port listeners with the ability to serve up text or encoded data as a banner in response to a visitor request. Each sim banner server can be edited, and new banner sim servers can be added.

The default sim banner servers include Echo (7), Daytime (13), Quote of the Day (17), Chargen (19), MyDoom worm (3127), Dameware (6129), and the SubSeven trojan (54283).

Sim Standard Servers

Sim standard servers entail a higher level of interaction than a mere one-time banner response. KFSensor currently comes with the following emulated services:

- FTP (Guild, not Microsoft, on port 21)
- Telnet (port 23)

- SMTP (Microsoft Exchange Server 2003 on port 25)
- HTTP (IIS 6.0 and Apache on ports 80, 81, 82, and 83)
- POP3 (Exchange Server on port 110)
- NetBIOS (ports 137, 138, 139, and 445)
- SOCKS Proxy (port 1080)
- Microsoft SQL Server (ports 1433 and 1434)
- SubSeven trojan (ports 2794, 7215, and 27374)
- Hogle SMTP trojan (port 3355)
- Terminal Server (port 3389)
- HTTP Proxy (port 8080)
- VNC (port 5900)

honeypot should be set up just like the real server so that data can appear to be authentic by showing fake files, fake ports, fake directories, etc. As the honeypot creates the illusion of being legitimate; the attacker tends to believe that they have gained accessed of the real deal.

KFSensor is a honeypot for a windows system. it also acts as an IDS. Its job is to attract and detect all the attackers in the network, hence the name ‘Honeypot’. It does so by imitating a vulnerable environment and disguising itself as a server and it way, it succeeds to not only catch the attacker but also helps to know their motive

KFSensor’s role is to be a decoy server for the attackers in order to protect the real thing.

It does its job perfectly by opening fake ports on the system where it’s installed and gathering the information when a connection is made. It does this in precisely the same way as a routine server program, such as a web server or an SMTP server. By doing this it sets up a target, or a honeypot server, that will record the activities of an attacker.