

# Know Your Enemy: Honeywall CDROM Roo

## *3rd Generation Technology*

[Honeynet Project & Research Alliance](#)

<http://www.honeynet.org>

Last Modified: 17 August, 2005

The [Honeywall CDROM](#) is a bootable CDROM that installs all of the tools and functionality necessary to quickly create, easily maintain, and effectively analyze a third generation honeynet. This paper introduces you to the Honeywall CDROM Roo, the second version of our CDROM series, released in May, 2005. The first Honeywall CDROM [Eeyore](#) was released in May, 2003, but is now considered out of date and is no longer maintained. This paper is not an in-depth technical document on how to install or maintain your honeywall, that is the purpose of the [Honeywall CDROM Online User's Manual](#). This paper will instead give you an overview of the capabilities of the new version, and where we hope to take it. It is assumed you have read and understand the concepts covered in [KYE: Honeynets](#) and [KYE: GenII Honeynets](#).

## History

The concept of a honeynet first began in 1999. There was little detailed information on security threats, and few tools to collect data. Back then, honeynets were extremely difficult to deploy and maintain, as they required putting together a variety of different tools (such as firewalls, intrusion detection sensors, packet sniffers, etc). The initial honeynets were crude, having basic data control and capture capabilities. They were limited to layer three routing gateways, counting outbound connections, and could only analyze unencrypted traffic. These initial deployments were considered first generation technology. In 2002/2003 we added additional functionality, including optional layer two bridging, intrusion prevention technology (snort-inline), and [Sebek](#), giving us the ability to analyze encrypted traffic. We considered the enhancements [GenII \(second generation\) Honeynets](#). While this improved the capabilities of honeynets, they were still difficult and time consuming to deploy and maintain.

Over time, attempts were made to make honeynets easier to deploy. This first began with pre-built tools, such as a rc.firewall script, making it easier to build and deploy a honeynet. In May, 2003, the first Honeywall CDROM was released, called *Eeyore*. The intent was to automate GenII honeynet deployments by bringing all the tools and requirements into a single CDROM. This solution was considered a beta concept, and had several weaknesses, ones that we learned from and improved. In September, 2004 team members got together to design, architect and develop a new solution, what we now call *Roo*. This release is considered a GenIII technology, as it has radical new improvements. It contains the core GenII Data Control and Data Capture functionality, but also now has remote GUI administration, Data Analysis integration, support for the Sebek 3.x branch, robust OS base, automated updating, and much more. We wanted a solution that any security professional could easily

use and maintain.

## Overview

In many ways, the original CDROM *Eeyore* was a prototype, to demonstrate the capabilities of a standalone honeynet, and learn from the CDROM. The new CDROM *Roo* is different. This is considered a production solution. Its easier to install and maintain and can be deployed in large numbers. Our intent is for the honeynet to move out of the world of academic research and expand as a real solution for a variety of organisations. Below is an overview of how we intend to achieve that.

Our first key decision was whether to continue to use a LiveCD solution or move to an OS that installed to the local hard drive. Both options have their advantages, however we decided it was best to have everything install to your local hard drive. The entire OS and honeywall functionality is installed to and runs from the system (which destroys any previous data you had on the hard drive). This approach makes it very easy for you to modify the system once installed (such as installing new packages or editing system configuration files), something that could not be done with a LiveCD solution. It also makes it easy for you to update and maintain the OS base (critical for large deployments), allowing you to use automated tools such as *yum* to keep packages current. The only purpose now of the CDROM is to install this functionality to the local hard drive. Once installed, you no longer need it. You can even have the CDROM pre-configured, your honeywall ready to go after installation, learn more at the Online User Manual under the [Installation Section](#). This allows large to quickly and easily deploy large numbers of honeynets.

The second decision was the OS base to use. Our goal is to make the honeywall functionality OS independent. In other words, you choose the OS you want (RedHat, Suse, OpenBSD, Solaris, etc) and simply install the Honeywall packages you need. However, we are not quite there yet. In addition, we had to choose an OS for the CDROM to install. As such, we use a minimized version of Fedora Core 3. We have minimized the system for security reasons (such as no windowing capabilities) but left enough base OS for additional functionality (such as a webserver, database, and international keyboard support). In addition, the package management tools make it easy to add new functionality. For example, if you want additional tools that are not currently installed, you can install them using the same process you would use for any Fedora based operating system. Once you deploy your honeywall, it is your responsibility to maintain the OS and keep it current. Fedora comes with the utility *yum* for this specific purpose. In addition, you use these very same package management tools to maintain the honeywall functionality. When we (the Honeynet Project and Research Alliance) release updated honeywall packages, you do not download and install a new CDROM. Instead, your OS simply downloads the latest packages from our website and installs them. This should make maintaining your honeywall and keeping it current much simpler.

The third key decision was how to maintain your honeywall once it was installed. The first CDROM release *Eeyore* was limited to the [Dialog Menu](#), which required either local or terminal access. The new CDROM *Roo* gives users three options for configuring and maintaining their installations. We wanted to make the CDROM as easy as possible to maintain (i.e. a GUI) but also give more advanced users the ability to automate the process, especially for distributed environments. Below is a highlight of those three options.

- **HWCTL**: This is a powerful command line utility that allows you to configure the system variables used by various programs, and the ability to start/start services. The advantage with this tool is you can simply modify the behavior of the system at the command line via local or SSH access. It also allows automated scripts to connect to remote system and change the system configuration, a feature critical for distributed environments.
- **Dialog Menu**: This is the same menu from the previous *Eeyore*. Like the HWCTL utility, it can be used with either local or remote access. Its graphic based, but its capabilities are limited.
- **Walleye**: The third option is a GUI web based interface called *Walleye*. The honeywall runs a webserver that can be remotely connected to over a SSL connection on the management interface. This GUI allows the user to configure and maintain the system using a simple point and click approach. It has an expanding menu making it easy to access and visualize all the information. It also comes with more in-depth explanations of the different options.. It also has different roles, allowing organizations to control who can access what through the GUI depending on the role they have been assigned. The primary advantage of *Walleye* is its much easier to use than the other two options. The disadvantage is it cannot be used locally, but requires a 3rd network interface on the honeywall used for remote connections. The web-based GUI currently supports either Internet Explorer or Firefox browsers.

One of the key lessons learned with the previous release *Eeyore* was the need for a powerful and easy to use data analysis tool. The primary purpose of a honeynet is to collect data, but what good is that data if it cannot be analyzed? The CDROM *Roo* has built in [data analysis capabilities](#), integrated into the *Walleye* interface. This allows you to use the same GUI to not only maintain your honeywall, but to track and analyze all the network and honeypot activity. The GUI starts with an overview of all inbound and outbound traffic, allowing you to focus in and analyze in detail any connection you may be interested in. It even gives you the ability to extract network connections in pcap format, allowing you to use other tools such as Ethereal to do in-depth analysis. Also included is the ability to analyze [Sebek data](#). Sebek is a kernel modification used to capture system activity on honeypots. *Walleye* can be used to analyze all of that system activity, including the ability to draw visual graphs of processes. Sebek is extremely useful, especially in environments where attackers may go encrypted, such as over SSH connections.

## The Future

We are not fully satisfied with the CDROM, and have several areas we hope to address. The first is data analysis. We have many new options and features that are planned to be added, such as the ability to identify suspicious connections, SNMP integration, and report generation. In addition, *Walleye* currently supports only one system, it can only analyze data from one honeynet. We are currently working on the ability to correlate and analyze activity from multiple honeynets. The second area we are developing is distributed capabilities. *Roo* allows you to deploy and maintain multiple honeynets. However, its not as robust as we would like. Work is being done to simplify and centralize remote administration of large, distributed environments. Third, we would eventually like to 'decouple' the honeywall functionality and their respective packages from a specific OS. Our long term goal would be for individuals and organizations to select their own OS base, and then install their respective honeywall packages. If you have any suggestions for new features or capabilities, please submit them as enhancement requests to our [Bug Server](#). The more information you can include in the enhancement request on the value of your suggestion, and how to integrate it into the CDROM, the

more likely your suggestions will be added.

## Conclusion

The Honeywall CDROM *Roo* is designed to be a production solution, to be used by individuals and organizations around the world. Based on lessons learned from the previous *Eeyore*, we have attempted to make this version much easier to install, configure and maintain, with the added capability of data analysis. Before deploying, make sure you have read and understand the risks and issues of using such a technology, and understand the legal considerations local to your organization and country. Expect to see many new features and functionality added in the next twelve months, especially in the areas of data analysis and distributed management. You can find and download the latest version of the CDROM at the [Honeywall CDROM Site](#).

The Honeynet Project