Honeyd Virtual Honeypot Implementation Guide

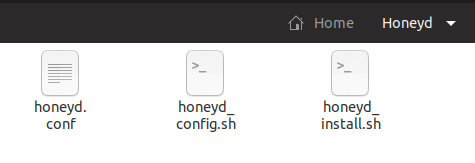
This guide will follow in three parts, the first part is the installation of the honeyd software on any debian operating system. The second part is the configuration of the honeyd config file, this is what creates the virtual honeypot. The third part is to state the location of the log files and how to run honeyd with the configuration file.

Requirements to follow this guide:

* Honeyd Installation Bash Script
* Honeyd Configuration Bash Script
* Virtual Honeypot Config File
* A Debian Operating System

Part 1: Installation Guide

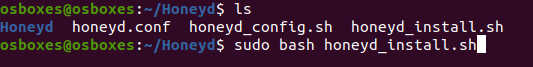
1. The first step is to create a folder in any place you please, then input the scripts and the config file within that file. In Figure 1, we named the folder Honeyd and all the scripts and config file is within that folder.



*Figure 1:* Honeyd folder with config and sh files

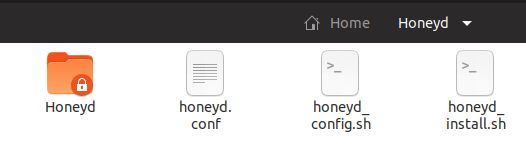
1. The second step is to run the honeyd\_install.sh script, what this script does is that it installs honeyd onto your hardware. It will install all the dependencies first, then proceed to install honeyd. This script will run for a few minutes. To run this script you will need to run this command:

sudo bash honeyd\_install.sh



*Figure 2:* Running honeyd\_install.sh script

After completing the previous step this is how the folder we created in step one should look like Figure 3.



*Figure 3:* Folder after running installation script

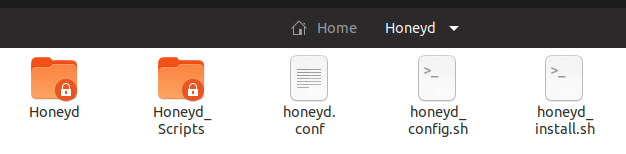
1. The third step is to run the configuration script, this script takes no time at all, so do not worry about it not operating correctly. To run this script use this command:

sudo bash honeyd\_config.sh



*Figure 4:* Running honeyd\_config.sh script

After completing the previous step this is how the folder should look like in Figure 5.

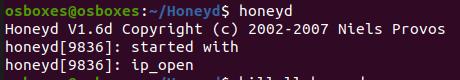


*Figure 5:* Folder after running configuration script

1. To verify that the installation have been successful, just run this command to see if honeyd is functional:

honeyd

The results of the command will be similar to Figure 6.



*Figure 6:* honeyd command

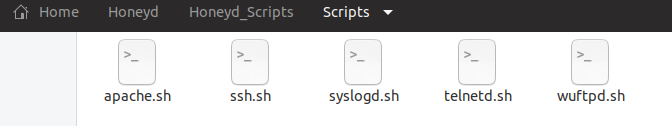
Part 2: Virtual Honeypot Configuration

1. The configuration file is already filled out to represent the Baxter Sigma Infusion Pump, there are minimal changes we will need to make to the configuration file.



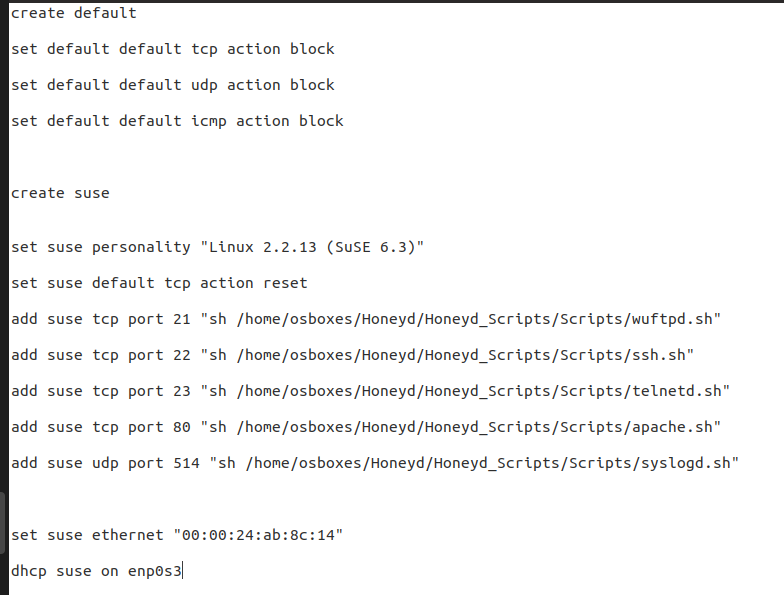
*Figure 7:* Default honeypot configuration file

1. Referring to Figure 7, we will need to change the locations of all the ports, all the .sh files needed will be in the Honeyd\_Scripts/Scripts folder that we installed in the folder we created. Refer to Figure 8 for the location of the sh scripts needed.



*Figure 8:* Location of sh script files for ports

Now knowing the location of the script files we can input them into the configuration file, reference Figure 9 for the configuration file change.



*Figure 9:* Updated port file location in configuration file

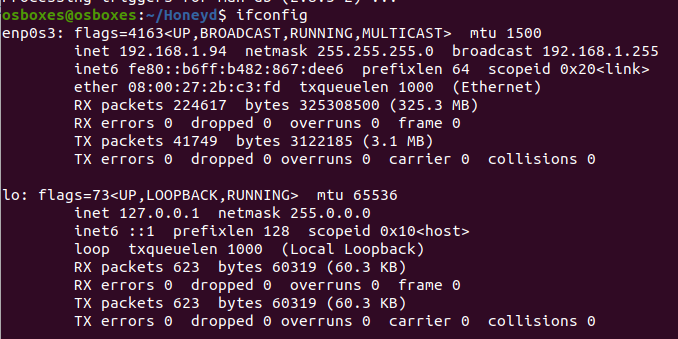
1. The mac address on the configuration file is set to 00:00:24:ab:8c:14, if you would like to change the mac address just change these numbers to the chosen mac address. Therefore on the line that states “set suse ethernet” input this:

set suse ethernet “XX:XX:XX:XX:XX:XX”

The X’s represents the mac address.

1. The final change needed to be done to the configuration file is to change the dhcp suse command at the bottom of the file. To change this file we need to determine the network it will be on.

To determine the network perform the command ifconfig to see the networks the device is connected to. Reference Figure 10, there are two types of networks the enp0s3 and the lo, always ignore lo. Therefore the network we will add to the configuration file is enp0s3.

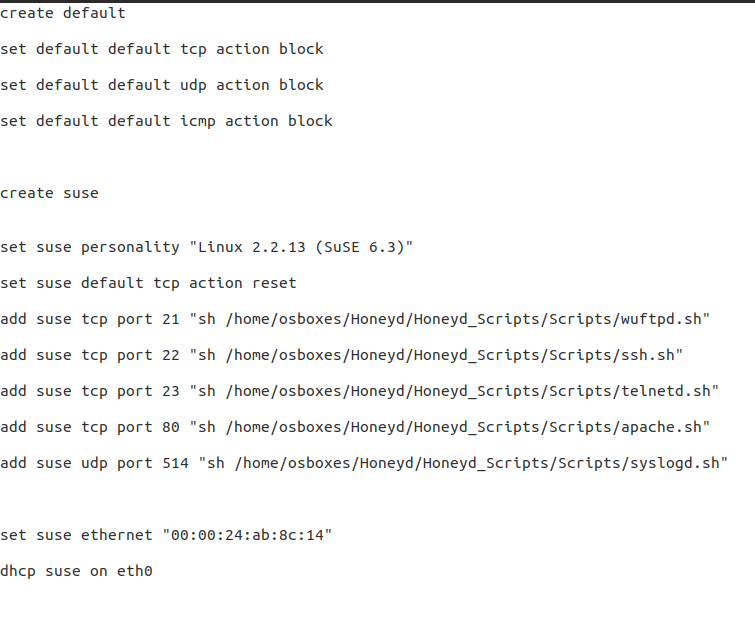


*Figure 10:* ifconfig command results

Since that is already in the configuration file, let's say we had the network eth0 instead. We will change the statement in the bottom to this instead:

dhcp suse on eth0

Reference Figure 11, for an updated honeypot configuration file with the eth0 as the network.



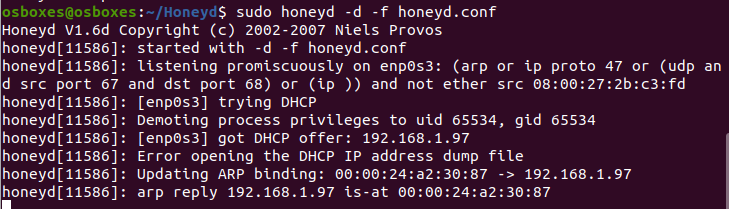
*Figure 11:* Network update configuration file

Part 3: Log File Locations and Honeyd Implementation

1. To deploy and implement the virtual honeypot it is just one command.

sudo honeyd -d -f honeyd.conf

The results should match what is in Figure 12.



*Figure 12:* Honeypot implementation command

1. Now that the honeypot is operational these are the location of the logs and what services will point to which log.

Port 21 - ftp service : /var/log/honeyd/msg.log

Port 22 - ssh service : /var/log/honeyd/msg.log

Port 23 - telnet service: /var/log/honeyd/msg.log

Port 80 - HTTP service: /var/log/hoenyd/web.log

Refer to Figure 13 for location of log files.



*Figure 13:* Log files location in /var/log/honeyd

If you would like further references on honeyd itself please go to this page for more details:

<http://www.honeyd.org/>