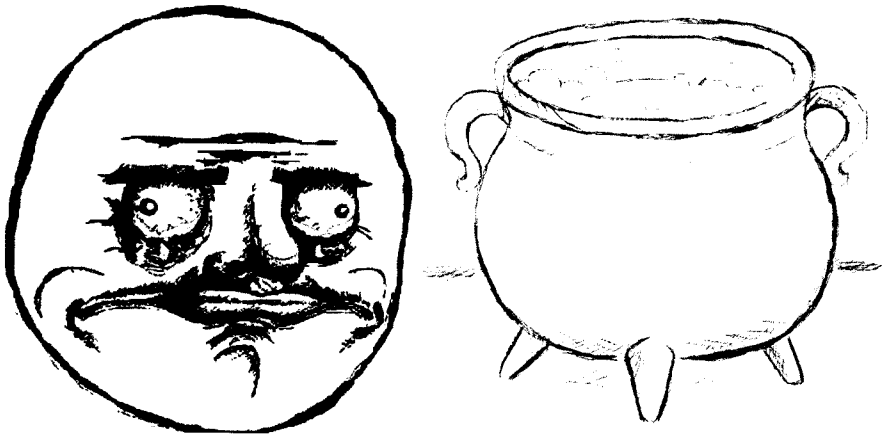

Derpypot 1.0 Instructions

Blue Teams

2015

Acknowledgements: A big thank you goes out to my (former) co-worker Tom Liston who provided the excellent Python honeypot script, as well as some very detailed install instructions for it and the web based honeypot, Glastopf.

About this document: This is the usage instructions for Derpypot a custom honeypot. Because we have two different platforms for the install (Ubuntu 14.04 for the Virtual Machine and Raspian for the Raspberry Pi), we will note subtle differences where needed. In most cases, operation of the honeypot are identical to both platforms.

Getting started: Derpypot is a Linux based system that listens on a bunch of ports and provides simulated services, while logging connections. These ports are:

1. 1433 – MS-SQL (TCP and UDP)
2. 3389 – RDP (TCP)
3. 5900 – VNC (TCP)
4. 5060 - sip (UDP)
5. 22292 – random (TCP)
6. 80 – via Glastopf (TCP)

You have two ways to access the system:

1. SSH to the system IP address on port 2222.
2. Use the VM console, or HDMI video connection on the Raspberry Pi.

What is the IP address you ask? The system is enabled for DHCP, so you'll have to flex your mental muscles to figure that out.

Your default username is "derpypot" (without the quotes), and is fully enabled for sudo access. The password is a bit more of a challenge: You need to figure that out as part of a small puzzle. Take a look at your badge for the first clue. Once you have that figured out, move to the next. There are 3 steps to find the password, which should take you no longer than 15-30 minutes to solve. The correct password IS case sensitive and includes spaces and punctuation.

Once logged into the system, you will note that the appropriate honeypot services are started automatically via "screen". Screen allows for multiple virtual sessions that can be sent to the background, and derpypot uses 4 screen sessions. The commands that are run to start derpypot can be found in the system wide screen configuration file, /etc/screenrc.

The 4 screen sessions contain the two console screens for the python port listener, and XXX web honepot, as well as two console screens for log output for the two services. These will be your friend.

A bit on screen: Because the screen session has already been started, you'll need to reconnect to the existing session with "screen -r", where you will be presented with the default screen interface. To switch between virtual sessions "CTRL-A, <session #>" , where the session number is 1-4 for the session. As an example "CTRL-A, 3" will switch you to the derpypot log file.

All of the derpypot executables can be found in /opt/derpypot and /opt/glastopf, and the services should be started in these directories. The log files can be found in the "log" directories in each respective service directory, EG. /opt/derpypot/log