

wget <https://pypi.python.org/packages/0f/88/18bb0eddb483033e35b1b84bdf9de4cedb8906ece178e2d921451282b3c8/Twisted-14.0.2.tar.bz2>

pip install PyCrypto

pip install Zope.Interface

git clone <https://github.com/desaster/kippo>

chown -R dionaea:dionaea kippo

su -s /bin/bash dionaea

cp kippo.cfg.dist kippo.cfg

Edit kippo.cfg to your liking and start the honeypot by running:

./start.sh

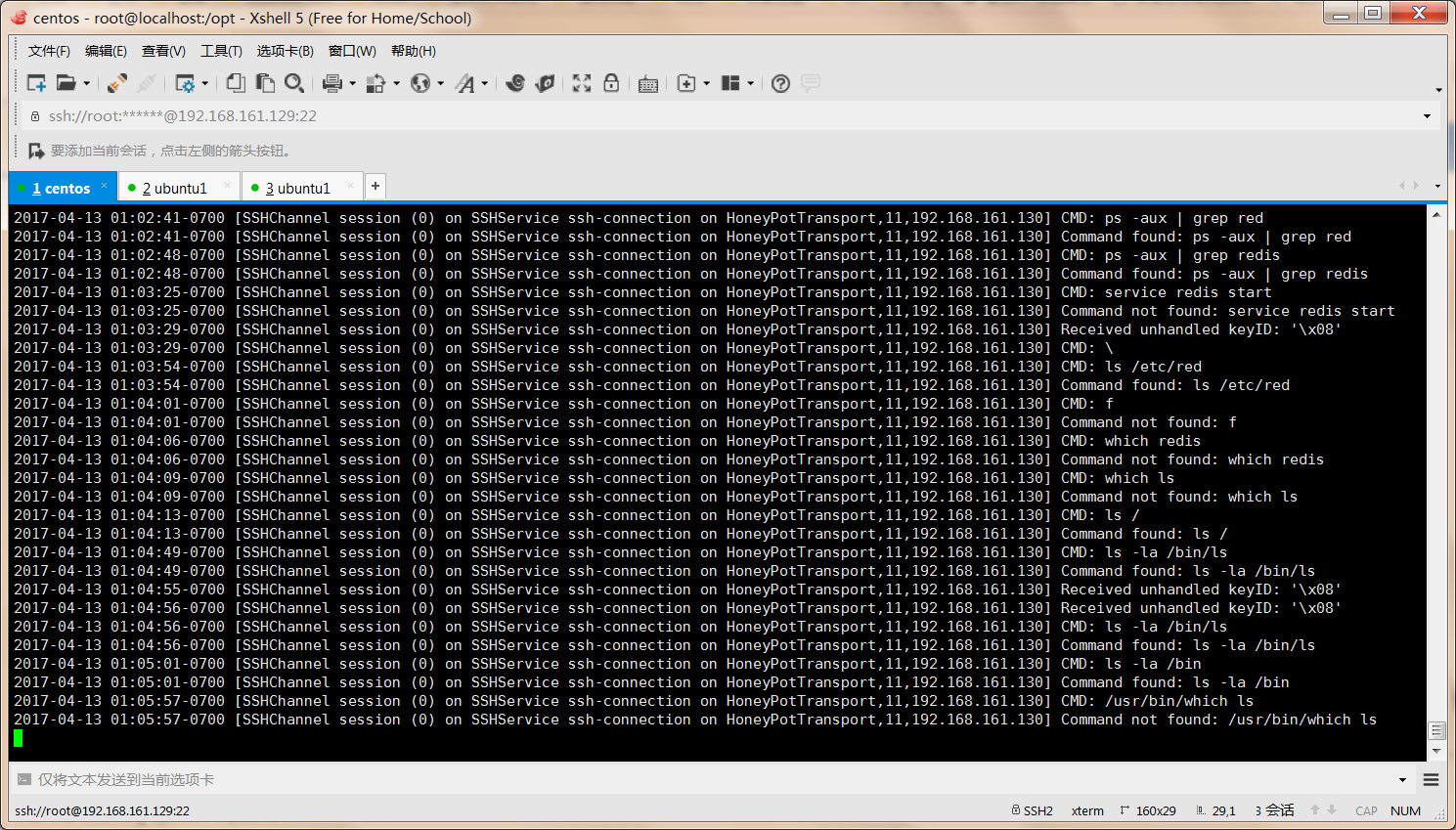
start.sh is a simple shell script that runs Kippo in the background using twistd. Detailed startup options can be given by running twistd manually. For example, to run Kippo in foreground:

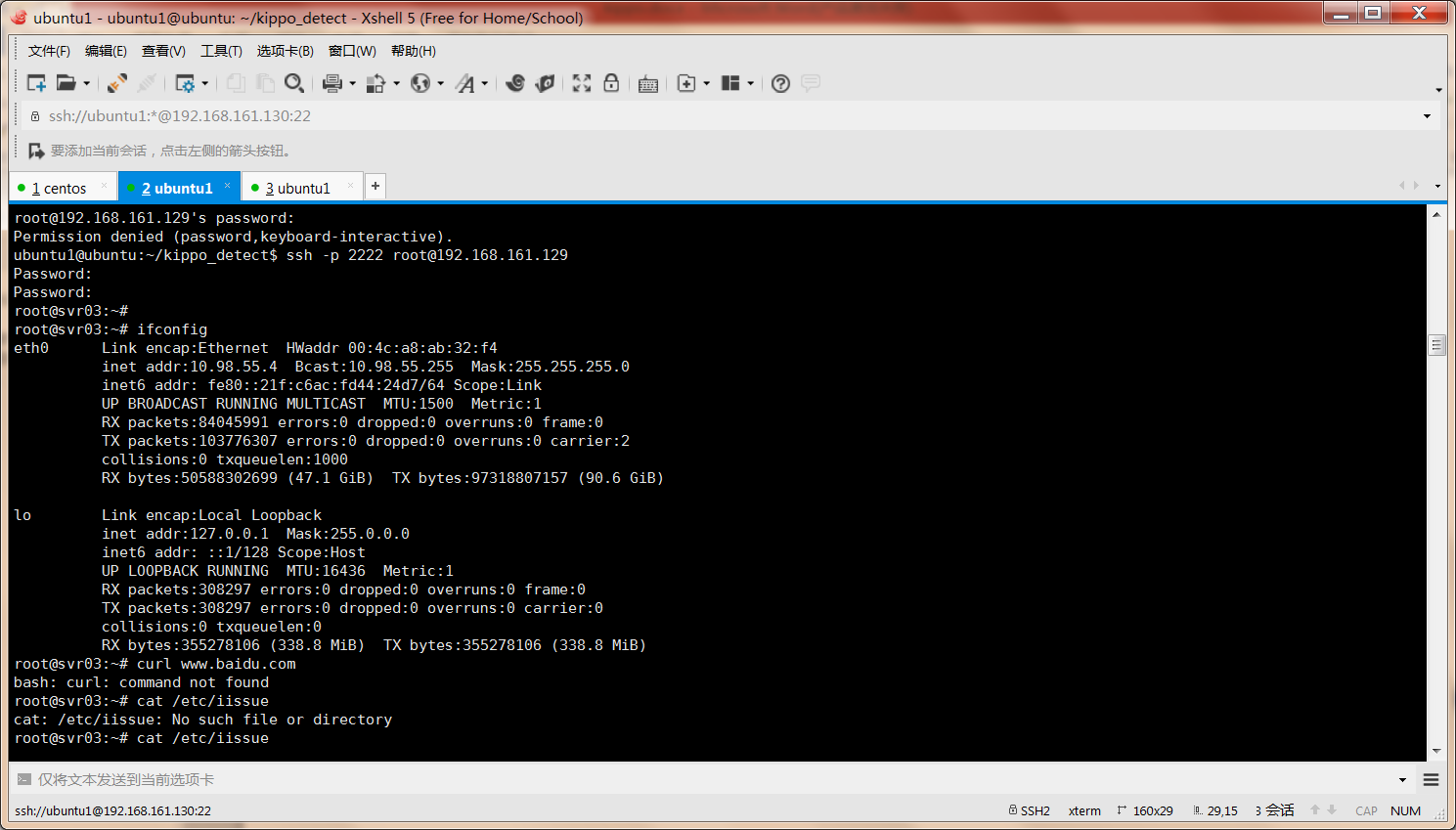
twistd -y kippo.tac -n

By default Kippo listens for ssh connections on port 2222. You can change this, but do not change it to 22 as it requires root privileges. Use port forwarding instead. (More info: [MakingKippoReachable](https://github.com/desaster/kippo/wiki/Making-Kippo-Reachable)).

Files of interest:

* dl/ - files downloaded with wget are stored here
* log/kippo.log - log/debug output
* log/tty/ - session logs
* utils/playlog.py - utility to replay session logs
* utils/createfs.py - used to create fs.pickle
* fs.pickle - fake filesystem
* honeyfs/ - file contents for the fake filesystem - feel free to copy a real system here





展示页面

https://github.com/ikoniaris/kippo-graph