Honeypots

**Kippo**

Let's begin by installing Kippo (an ssh honeypot)

### Installation and Configuration

I assume you are using a nice ubuntu version

```
`apt-get install honeyd honeyd-common farpd`
```

farpd is a daemon that responds to arp requests if no-one else responds. Need to be very careful about how we use it. An example to listen for a single host (read the man page if you want to listen for more than 1 host):

```
farpd 144.38.200.106 -i eth0
```

Now configure how honeyd will run

- first, edit `/etc/default/honeyd`

```
RUN="yes"
INTERFACE="eth0"
NETWORK=144.38.220.0/27
# Put your network id there or comment the line out
OPTIONS="--disable-webserver"
```

- Note that farpd simply responds to arp requests (layer 2), whereas honeyd will actually process the datagram destined to the above IP (layer 3).

- I would probably change the username and password to something secret. We will use that later (the `-c` flag allows us to collect some statistics)

Create a config machine in `/etc/honeypot/honeyd.conf`, here's mine:

```
create winxp
set winxp personality "Microsoft Windows XP Professional SP1"
set winxp default tcp action reset
set winxp uptime 1728650
set winxp maxfds 35
# For a complex IIS server
add winxp tcp port 80 "sh /usr/share/honeyd/scripts/win32/web.sh"
add winxp tcp port 22 "/usr/share/honeyd/scripts/test.sh $ipsrc $dport"
add winxp tcp port 23 proxy $ipsrc:23
bind 144.38.220.106 winxp
```

### Start honeyd

```
`/etc/init.d/honeyd restart`
```

Look in `/var/log/ honeypot/daemon.log` to make sure it started correctly. One common issue is that when you cut and paste values from above, the quotes are messed up.

Try to connect to those above ports, should be working.

**Finally**

Do some research and make another script work (or write your own) when someone connects to a particular port on the honeypot. These scripts are found in `/usr/share/honeyd/scripts`
To pass off

You will demonstrate this to me.