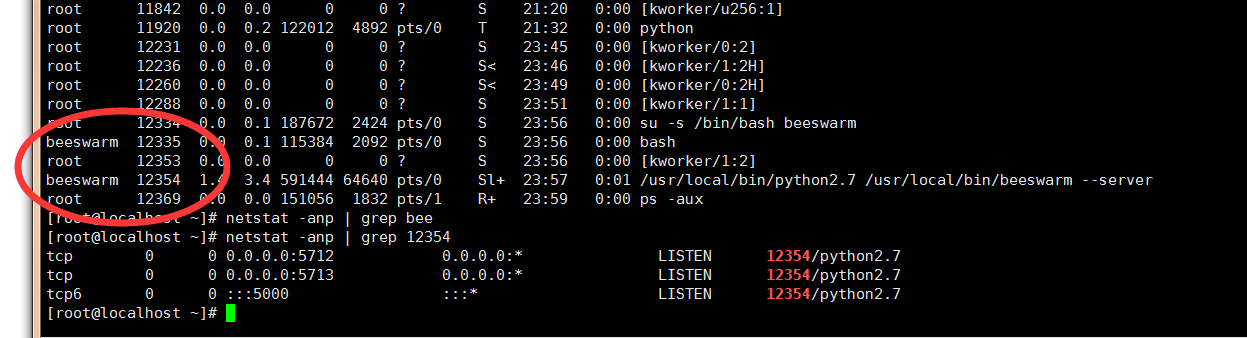
Beeswarm则是一款主动诱骗攻击者的蜜罐，可以模拟客户端与服务器的通信（诱饵通信），诱骗黑客攻击蜜罐，以对付企图通过网络监听获取敏感信息的攻击者。诱饵通信中，包括大量攻击者可能非常感兴趣的信息，如用户名口令、管理后台等。如果有攻击者在网络中进行窃听，获取了诱饵通信的内容，并使用这些敏感信息（如使用诱饵登录凭证）登录系统，Beeswarm就能发现网络攻击。

Server 有界面

使用add特征生产客户端

http://www.beeswarm-ids.org/

<https://github.com/honeynet/beeswarm>



蜜罐服务

telnet ssh pop3 vnc http ftp pop3s smtp

yum search libffi-dev python-dev libssl-dev libxml2-dev libxslt1-dev

sudo yum groupinstall 'Development Tools'

yum install gcc gcc-c++ make openssl-devel python-pip

pip install pydes --allow-external pydes --allow-unverified pydes

pip install beeswarm

cp /usr/lib64/python2.7/lib-dynload/\_curses\* /usr/local/lib/python2.7/lib-dynload

pip uninstall curses-menu

pip install curses-menu

pip install UniCurses

pip install curses-2048

mkdir beeswarm

cd beeswarm

groupadd beeswarm

useradd -g beeswarm -s /usr/sbin/nologin beeswarm

chown -R beeswarm:beeswarm /opt/beeswarm

su beeswarm

su -s /bin/bash beeswarm

beeswarm --server

<https://192.168.161.129:5000/>

客户端安装

同上

**3 BeeswarmDrone Client、BeeswarmDrone Honeypot安装**

在Beeswarm中**Drone Client**和**Drone Honeypot**都是Drone。在第二台虚拟机上重复上述安装步骤，直到Beeswarm安装成功，然后执行如下指令：

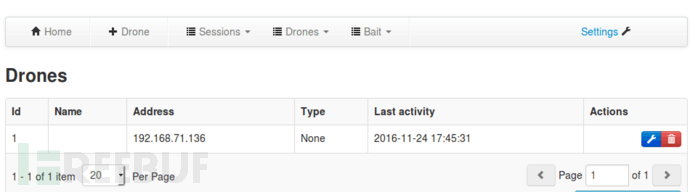
**mkdir drone\_workdir**

**cd drone\_workdir**

使用浏览器访问服务器（https:// 192.168.71.130：5000），输入用户名和密码，选择+Drone菜单项，可以得到启动Drones时需要告诉Drones的Beeswarm服务器的URL，用于让服务器识别Drones：

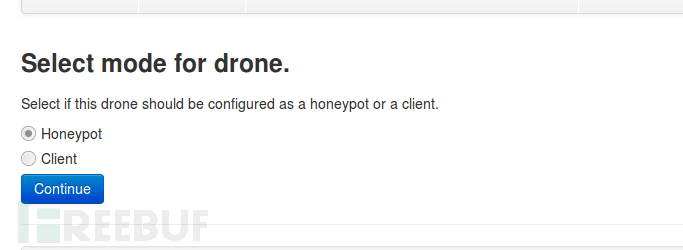
**sudo beeswarm –config** [**https://192.168.71.130：5000/ws/drone/add/82a93121-22dc-4150-a017-976c3ea73f50**](https://192.168.71.130:5000/ws/drone/add/82a93121-22dc-4150-a017-976c3ea73f50)

当Drones和服务器连接后，通过浏览器访问服务器进行配置，配置页面如图3，选择Drone菜单项，然后选Unassigned，此时可以看到待配置的选项，见图6。

[](http://image.3001.net/images/20161207/14810853692231.png)

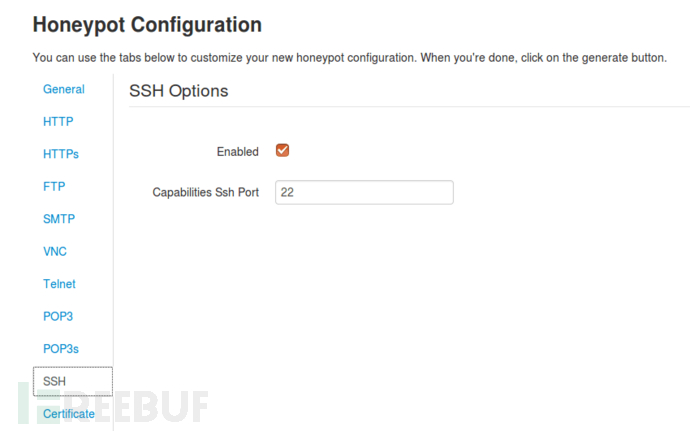
**图 6 待配置的Drone**

选择蓝色的按钮进入模式选择页面，有蜜罐和客户端两种类型，先选择蜜罐类型：

[](http://image.3001.net/images/20161207/14810853891540.png)

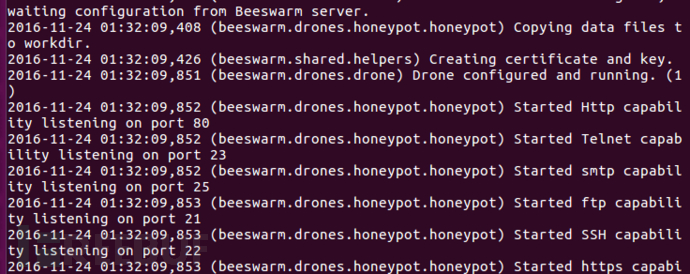
**图 7 Drone类型选择**

选择之后进入蜜罐节点配置页面，需要选择开启哪些服务；

[](http://image.3001.net/images/20161207/14810854043859.png)

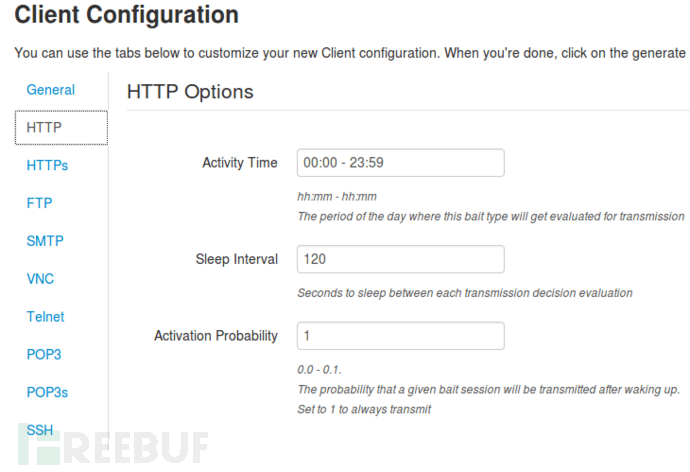
**图 8 蜜罐开启的服务选择**

配置完成后蜜罐主机开始监听端口；

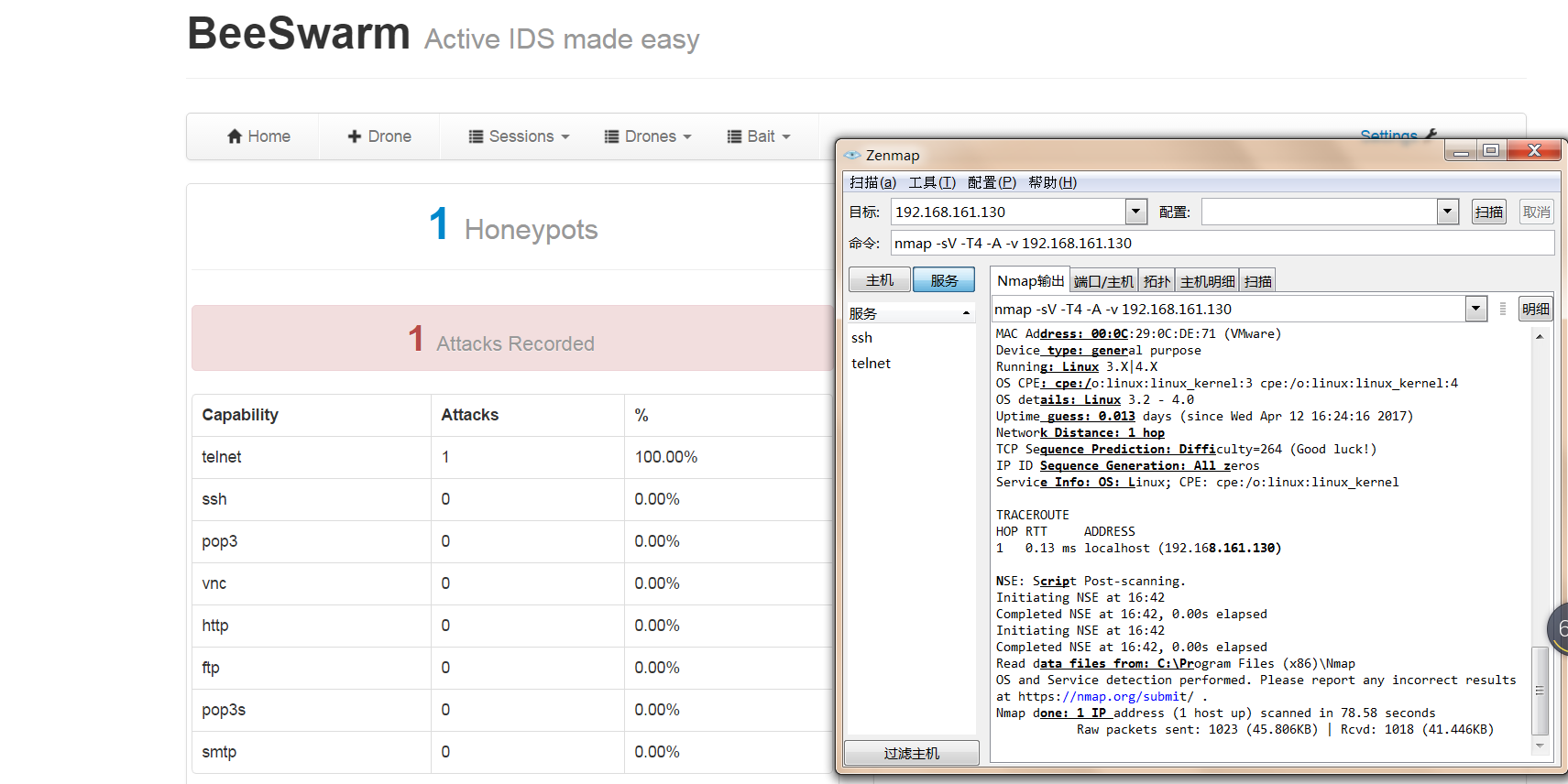
[](http://image.3001.net/images/20161207/14810854147133.png)

**图 9 蜜罐主机监听端口**

在第三台虚拟机上重复上述步骤，但是在图7的模式选择中选Client；Client模式配置页面如图10；

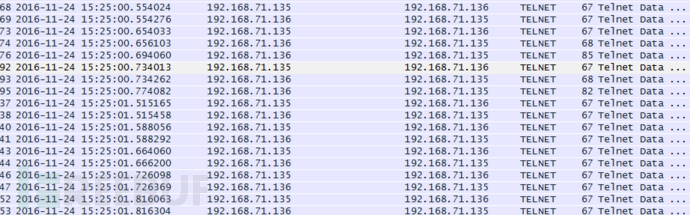
[](http://image.3001.net/images/20161207/14810854242306.png)

**图 10 client配置页面**

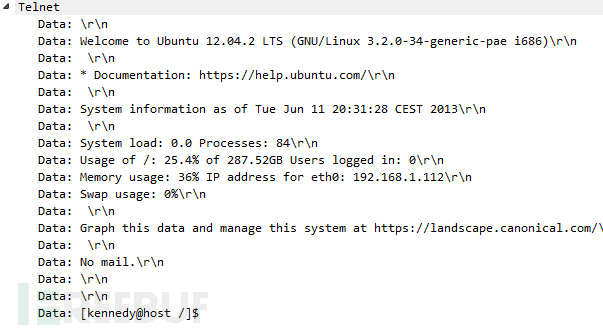


## ****三、使用方法****

在Beeswarm蜜罐系统中，Beeswarm Drone Client需要部署在想要进行检测的网段，一旦完成部署，Beeswarm Drone Client将会不断访问系统（图11是Beeswarm Drone Client 与Honeypot 交互示例）。当BeeswarmDrone Client所在网段有攻击者进行窃听并使用窃听得到的登录凭证访问蜜罐系统时，Beeswarm就能发现攻击者的存在。

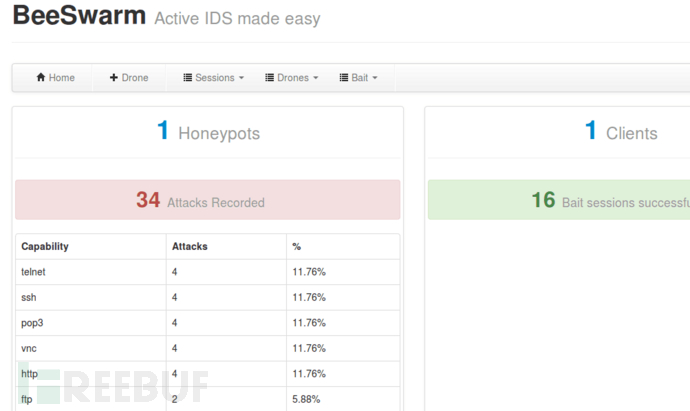
[](http://image.3001.net/images/20161207/14810854338326.png)

**图 11 Beeswarm Drone Client 与Honeypot 交互示例**

[](http://image.3001.net/images/20161207/14810854443919.png)

**图 12 通过wireshark抓包获取的telnet会话内容**

Beeswarm Drone Client 和BeeswarmDrone Honeypot会将信息报告给服务器，访问服务器可以看到Honeypot、Clients、产生的诱饵会话和攻击信息。

[](http://image.3001.net/images/20161207/14810854538327.png)

