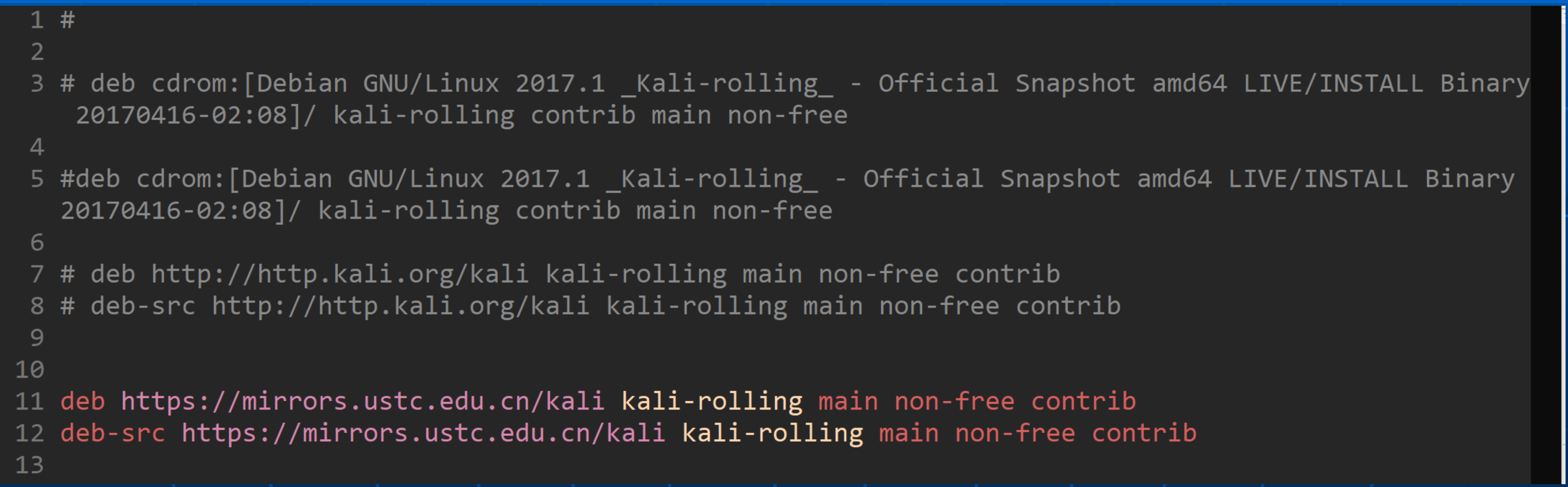
实验 4 SNORT & HoneyD & Metasploitable3 CTF

- 实验目的
  - 通过实验深入理解入侵检测系统与入侵防御系统的原理和工作方式，熟悉入侵检测系统snort的配置和使用
  - 通过实验熟悉利用Honeyd（或WinHoneyd）配置蜜罐。
  - 熟悉Metaspoit-framework和靶机Metaploitable3，综合运用所学针对靶机进行各种攻击

- 实验分组
  - 独立完成
- 实验报告：每次实验需提交1份报告
  - 命名：'201530561010-陈梓仪-LAB3

内容一：Snort IDS/IPS

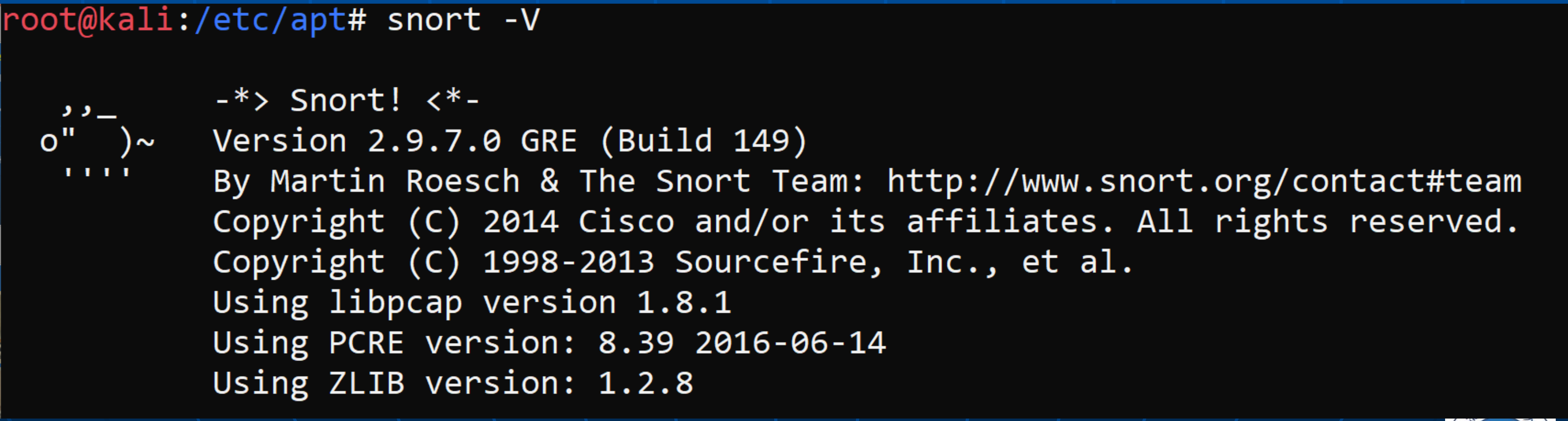
- Installing Snort from the Repositories
  - 编辑 /etc/apt/sources.list
  - 修改为国内源镜像



```
#

# deb cdrom:[Debian GNU/Linux 2017.1 _Kali-rolling_ - Official Snapshot amd64 LIVE/INSTALL Binary 20170416-02:08]/ kali-rolling contrib main non-free

#deb cdrom:[Debian GNU/Linux 2017.1 _Kali-rolling_ - Official Snapshot amd64 LIVE/INSTALL Binary 20170416-02:08]/ kali-rolling contrib main non-free

# deb http://http.kali.org/kali kali-rolling main non-free contrib
# deb-src http://http.kali.org/kali kali-rolling main non-free contrib


deb https://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib
deb-src https://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib

```

内容一：Snort IDS/IPS

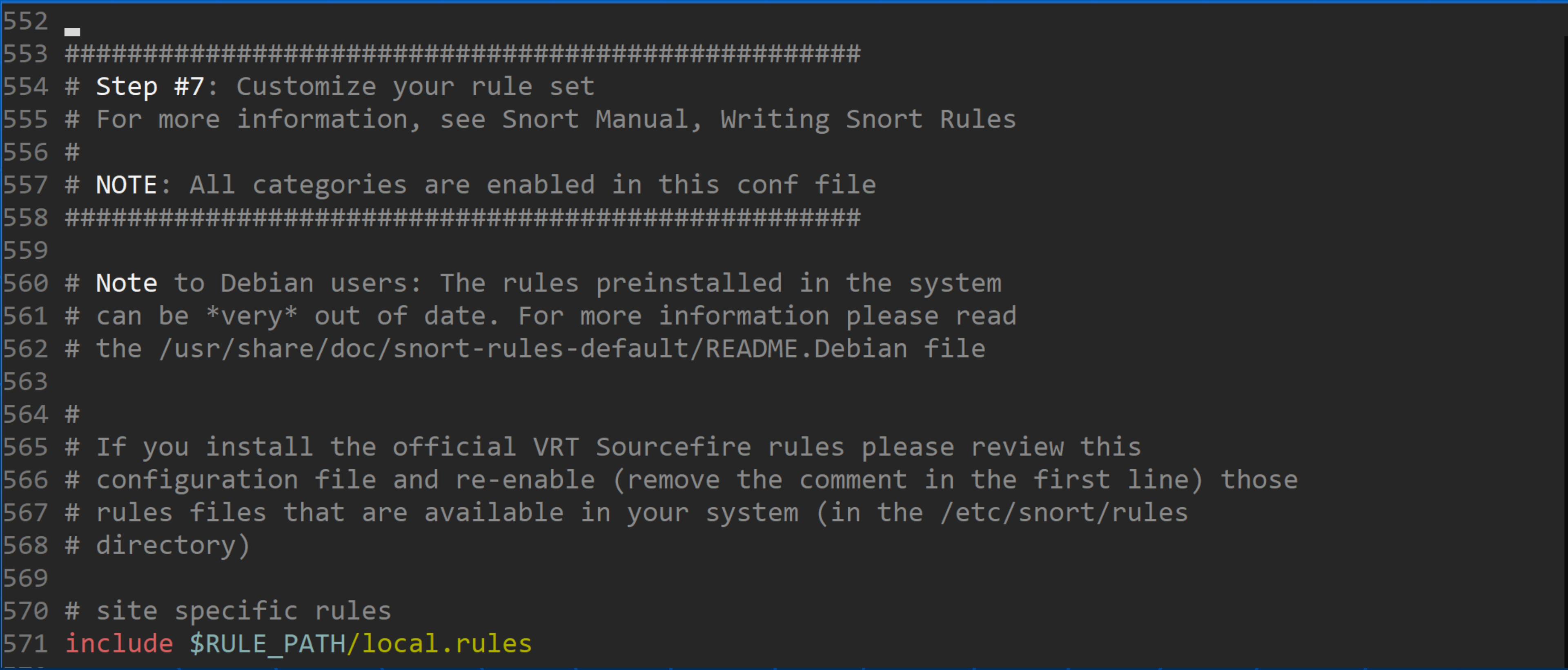
- Installing Snort from the Repositories
  - apt-get update
  - apt-get install snort
- Check installation
  - snort -V



```
root@kali:/etc/apt# snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.8.1
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.8
```

内容一：Snort IDS/IPS

- vim /etc/snort/snort.conf
  - 注释除 local.rules 以外的其他规则



```
 
###################################################
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
###################################################

# Note to Debian users: The rules preinstalled in the system
# can be *very* out of date. For more information please read
# the /usr/share/doc/snort-rules-default/README.Debian file

#
# If you install the official VRT Sourcefire rules please review this
# configuration file and re-enable (remove the comment in the first line) those
# rules files that are available in your system (in the /etc/snort/rules
# directory)

# site specific rules
include $RULE_PATH/local.rules
```

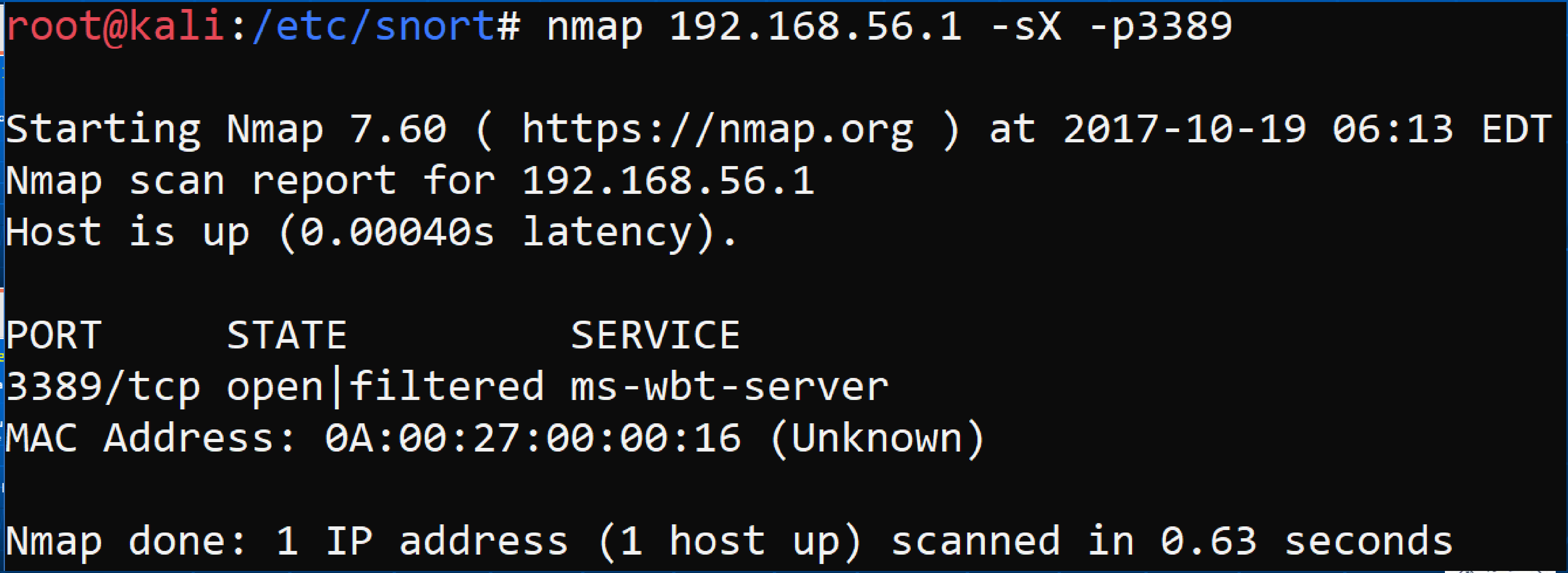
内容一：Snort IDS/IPS

- vim /etc/snort/rules/local.rules
  - 添加关于Xmas扫描规则（源IP/目的IP、源端口和目的端口可以自己修改)

```
alert tcp any any -> any any (msg:"SCAN nmap
XMAS"; flow:stateless; flags:FPU,12;
reference:arachnids,30; classtype:attempted-recon;
sid:1228; rev:7;)
```

内容一：Snort IDS/IPS

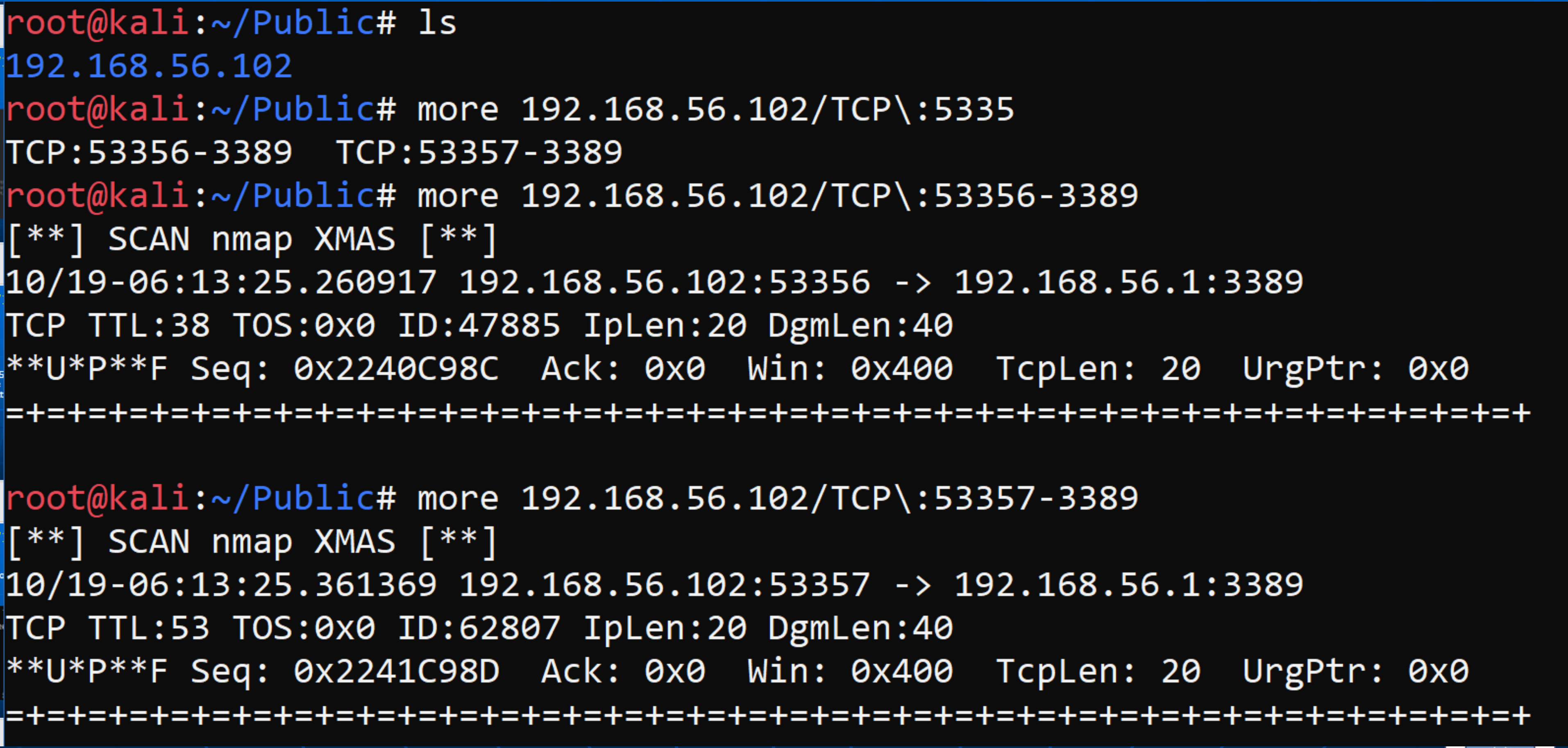
- 运行snort
  - snort -l ~/Public -K ascii -c /etc/snort/snort.conf
- Xmas扫描目标IP



```
root@kali:/etc/snort# nmap 192.168.56.1 -sX -p3389

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-19 06:13 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00040s latency).

PORT     STATE         SERVICE
3389/tcp open|filtered ms-wbt-server
MAC Address: 0A:00:27:00:00:16 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds
```

内容一：Snort IDS/IPS

- 查看日志
  - 扫描行为已被记录



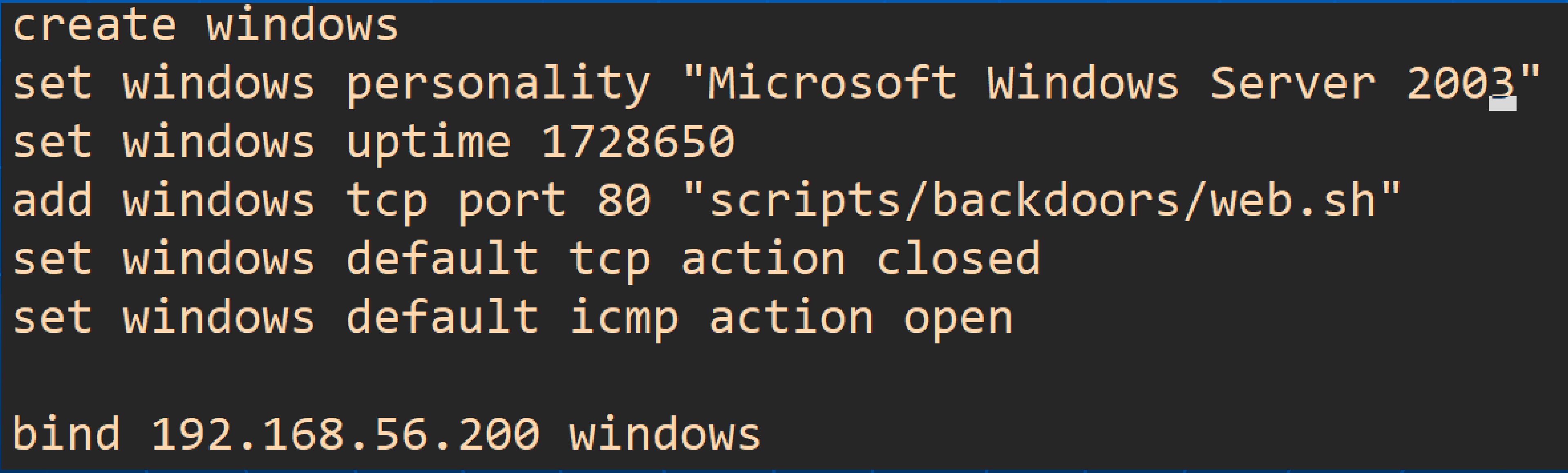
```
root@kali:~/Public# ls
192.168.56.102
root@kali:~/Public# more 192.168.56.102/TCP\:5335
TCP:53356-3389  TCP:53357-3389
root@kali:~/Public# more 192.168.56.102/TCP\:53356-3389
[**] SCAN nmap XMAS [**]
10/19-06:13:25.260917 192.168.56.102:53356 -> 192.168.56.1:3389
TCP TTL:38 TOS:0x0 ID:47885 IpLen:20 DgmLen:40
**U*P**F Seq: 0x2240C98C  Ack: 0x0  Win: 0x400  TcpLen: 20  UrgPtr: 0x0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

root@kali:~/Public# more 192.168.56.102/TCP\:53357-3389
[**] SCAN nmap XMAS [**]
10/19-06:13:25.361369 192.168.56.102:53357 -> 192.168.56.1:3389
TCP TTL:53 TOS:0x0 ID:62807 IpLen:20 DgmLen:40
**U*P**F Seq: 0x2241C98D  Ack: 0x0  Win: 0x400  TcpLen: 20  UrgPtr: 0x0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

内容二：Honeyd

- Install Honeyd under Kali Linux
  - apt-get install libevent-dev libdumbnet-dev libpcap-dev libpcre3-dev libedit-dev bison flex libtool automake zlib1g zlib1g-dbg zlib1g-dev
  - cd ~/Downloads
  - git clone https://github.com/DataSoft/Honeyd.git
  - cd ~/Downloads/Honeyd
  - ./autogen.sh
  - ./configure
  - make
  - sudo make install

内容二：Honeyd

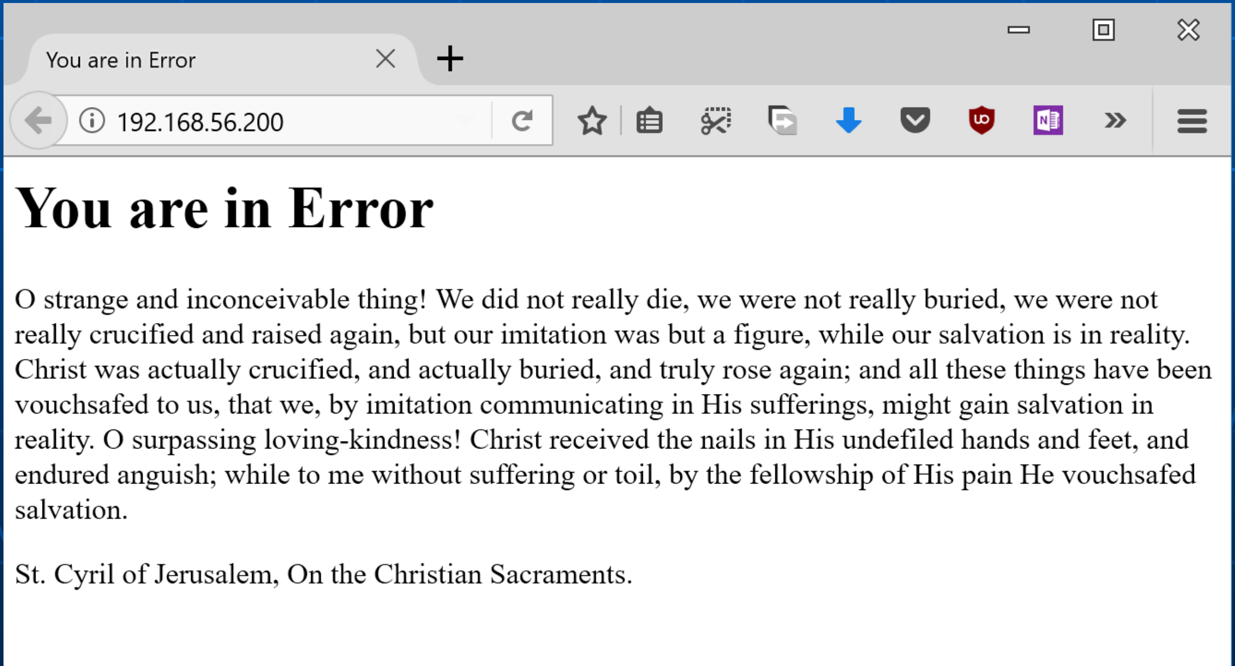
- Configure Honeyd
  - cd /usr/share/honeyd
  - vim honeyd.conf



```
create windows
set windows personality "Microsoft Windows Server 2003"
set windows uptime 1728650
add windows tcp port 80 "scripts/backdoors/web.sh"
set windows default tcp action closed
set windows default icmp action open

bind 192.168.56.200 windows
```

内容二：Honeyd

- Run farpd and honeyd
  - chown -R nobody /usr/share/honeyd/scripts/logs
  - farpd -i eth0 -d
  - honeyd -d -f /usr/share/honeyd/honeyd.conf
- Browser virtualpot under host machine



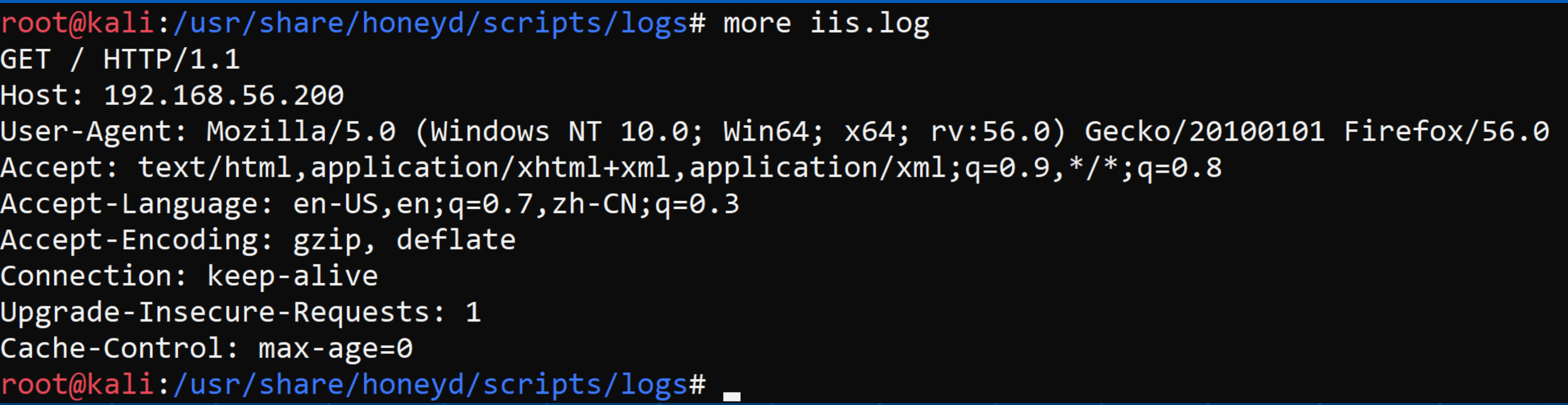
You are in Error

O strange and inconceivable thing! We did not really die, we were not really buried, we were not really crucified and raised again, but our imitation was but a figure, while our salvation is in reality. Christ was actually crucified, and actually buried, and truly rose again; and all these things have been vouchsafed to us, that we, by imitation communicating in His sufferings, might gain salvation in reality. O surpassing loving-kindness! Christ received the nails in His undefiled hands and feet, and endured anguish; while to me without suffering or toil, by the fellowship of His pain He vouchsafed salvation.

St. Cyril of Jerusalem, On the Christian Sacraments.

内容二：Honeyd

- Check logs
  - cd /usr/share/honeyd/scripts/logs



```
root@kali:/usr/share/honeyd/scripts/logs# more iis.log
GET / HTTP/1.1
Host: 192.168.56.200
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.7,zh-CN;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
root@kali:/usr/share/honeyd/scripts/logs# _
```

内容三：Metasploitable 3 CTF

- Download and install Metasploitable 3.
- Dig in! Find those flags!
- Complete a simple write-up including the procedures and the proof you've found one
  - 描述和图解夺旗步骤
- BTW, there are at least 15 flags hidden in Metasploitable 3.

Sample Flags

Thank You!