# 实 验 报 告 三

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **课 程** | 网络攻击与防御 | **实验项目** | 攻防综合实验 | |
| **专业班级** | 网络空间安全 | | **实验日期** | 3/31 |
| **学 号** | **201831082313** | | **姓 名** | 牟垠川 |

提醒：实验报告撰写完毕后进行保存，取名为类似**201831025678\_张三\_网络攻防实验3.docx**，并上传到超星系统课程作业“第二次实验报告”。

本次实验所使用到的主要软件包括：Wireshark, Suricata, 虚拟机等，。

**每个题目给出主要操作步骤、截图和分析。**

**实验报告正文**

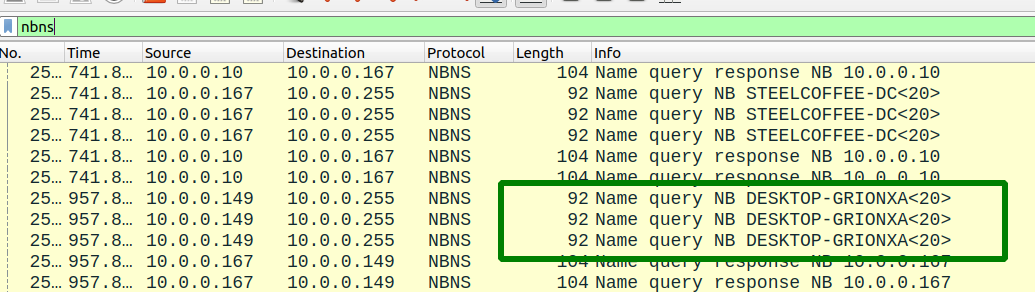
|  |  |  |  |
| --- | --- | --- | --- |
|  | **题号** | **分数** | **自评分** |
| **分数自评** | **1** | **30** | **30** |
| **2** | **20** | **20** |
| **3** | **20** | **20** |
| **4** | **20** | **20** |
| **5(实验报告编写)** | **10** | **10** |
| **自评总得分** | **100** | | |

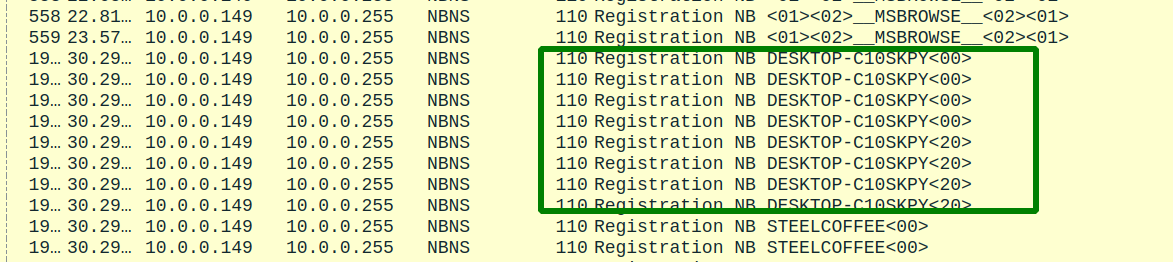
1. **使用流量分析技术分析真实恶意代码(30分)**

使用Wireshark对pcap文件进行分析，结合安全告警提示，回答以下问题：

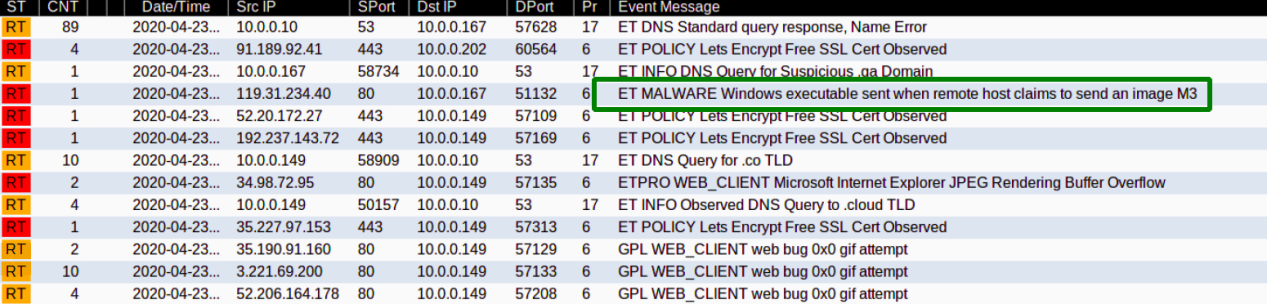
1) 两台Windows操作系统的IP和主机名是什么？(提示：结合netbios协议信息)

DESKTOP-GRIONXA<20> 10.0.0.149  
DESKTOP-C10SKPY<20>10.0.0.167

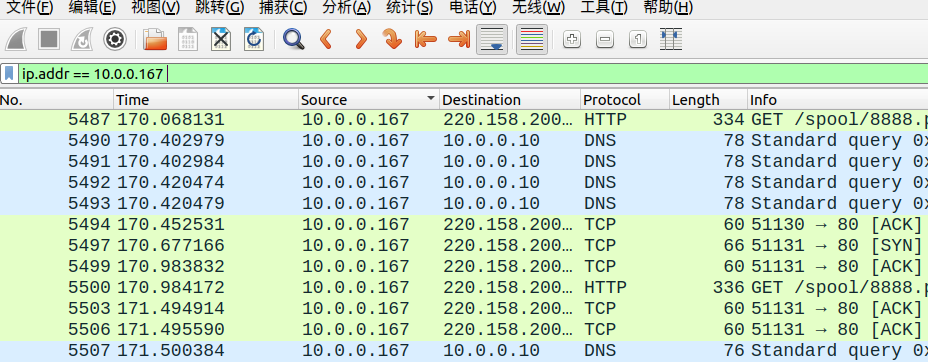
直接过滤nbns在info字段查看  


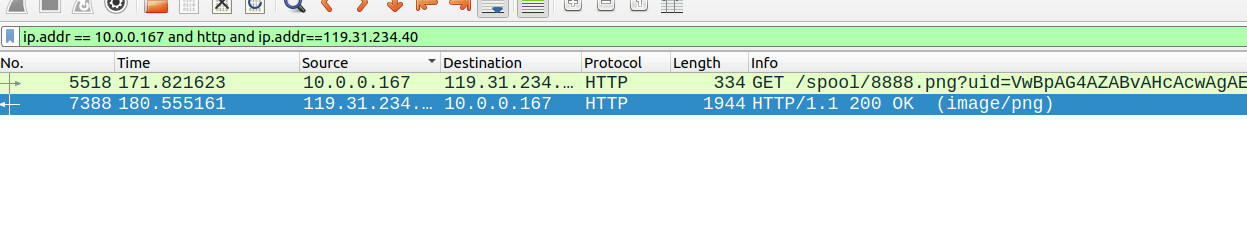


2) 哪台Windows主机被恶意代码感染？

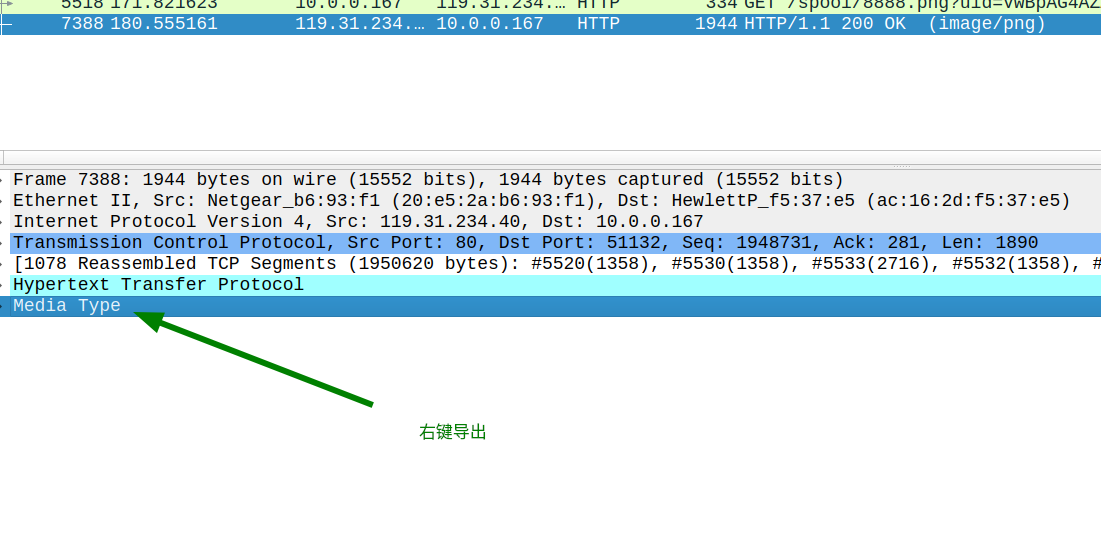
1.根据告警信息可以判断指导 在10.0.0.167 有一个恶意文件传入,可以判断其被恶意感染  


1. 在wiresahek中过滤找到这个ip与主机的交互信息

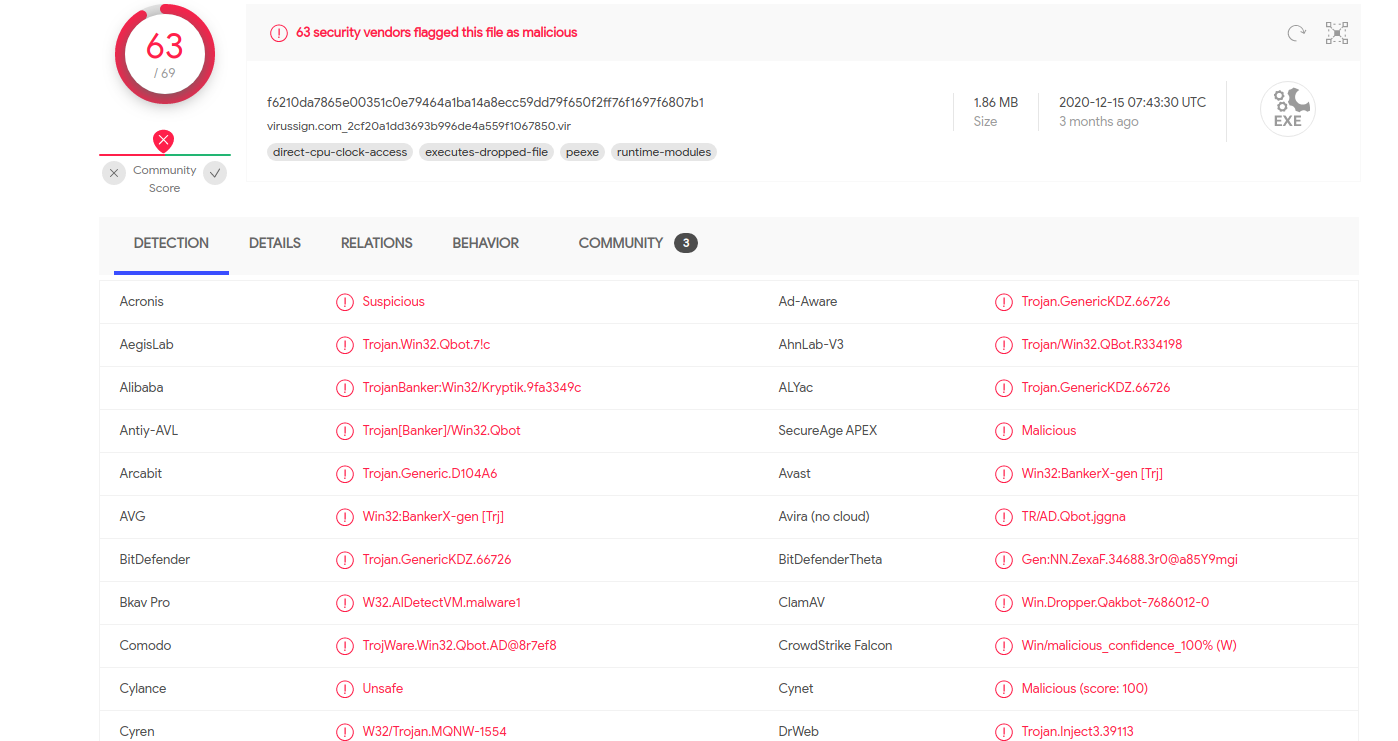
  
3.过滤119.237.143.72与http可以找到这个主机发起请求



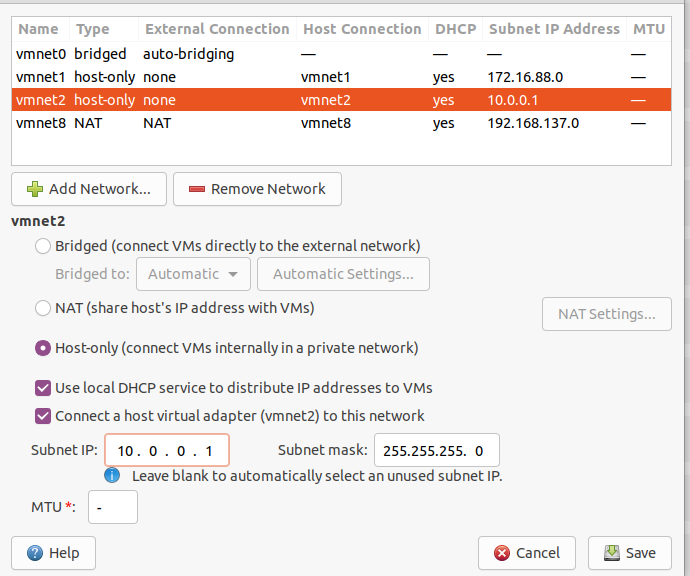
4.导出文件  
发现导出文件为exe可执行文件

  
导出的exe

  
3) 使用VirusTotal对该恶意代码进行分析，解释分析结果。  


  
出现多处Trojan  
说明是妥妥的木马  
2.**恶意代码分析环境搭建(20分)**

1) 使用虚拟机和inetsim搭建恶意代码分析环境，见参考资料；(10分)



2) 将第1题分析得到的恶意代码在上述环境执行，inetsim产生了什么信息提示？(10分)

$ sudo su

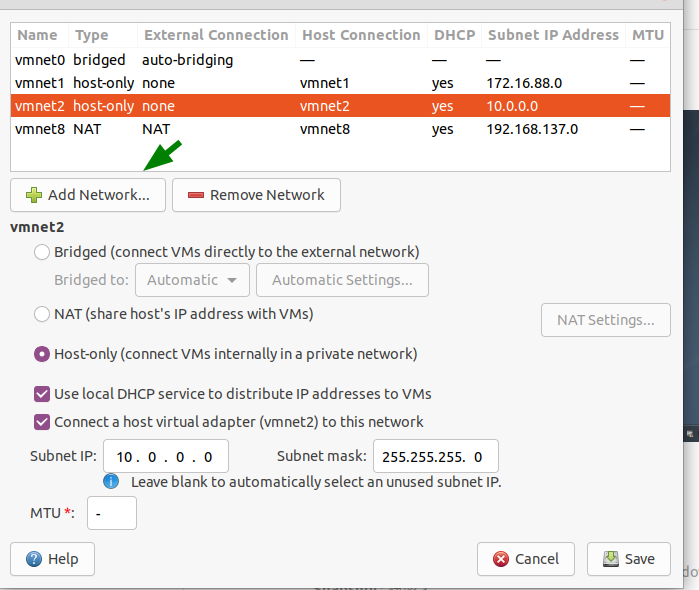
$ echo "deb http://www.inetsim.org/debian/ binary/" > /etc/apt/sources.list.d/inetsim.list

$ wget -O - http://www.inetsim.org/inetsim-archive-signing-key.asc | apt-key add -

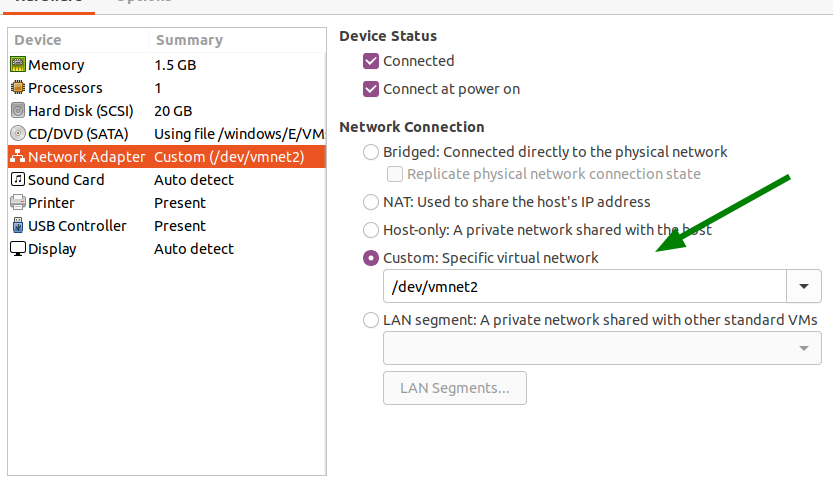
$ apt update

$ apt install inetsim

添加一个host only网络环境

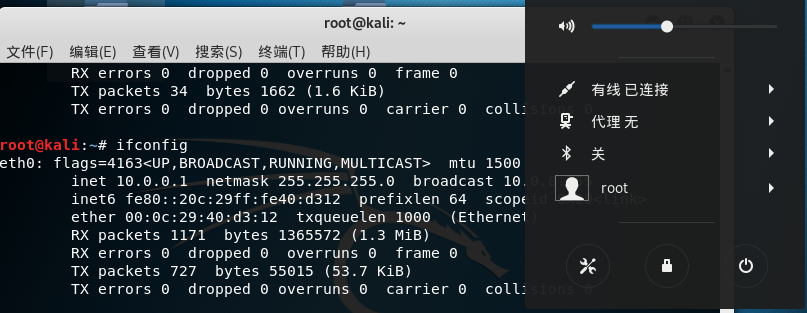


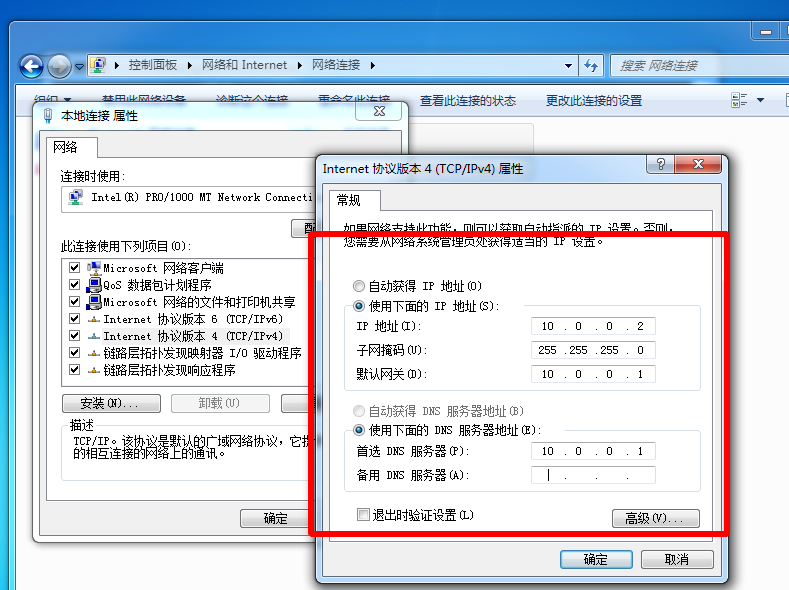
选择网络

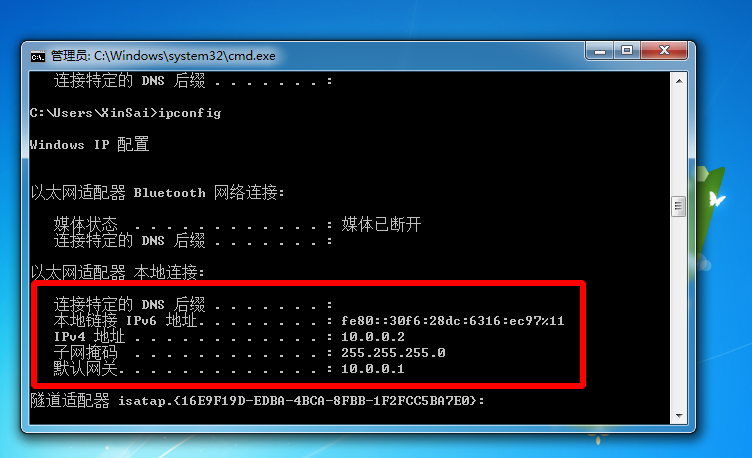
修改网卡



重启一下网卡  
ifconfig eth0 down   
 ifconfig eth0 up



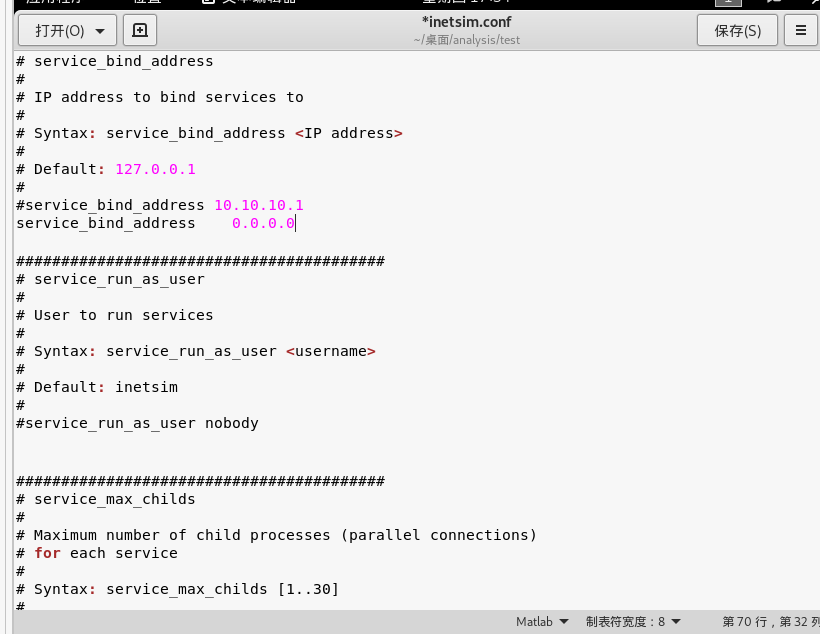




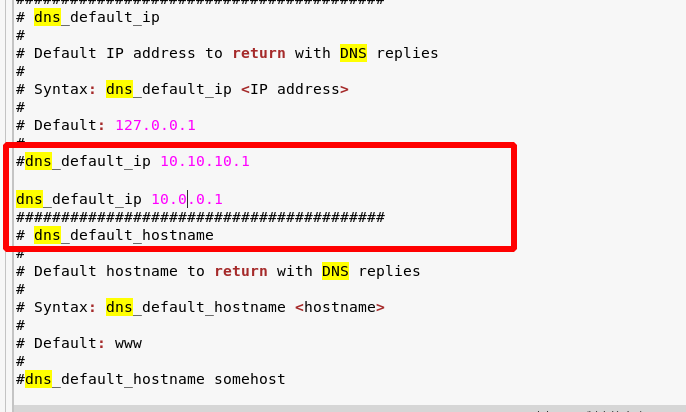


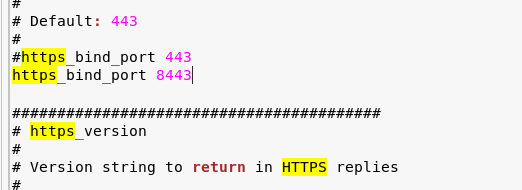
4.创建和还原快照

**$ mkdir analysis/test-analysis  
$ cp /etc/inetsim/inetsim.conf analysis/test-analysis  
$ sudo cp -r /var/lib/inetsim analysis/test-analysis/data  
$ sudo chmod -R 777 data  
$ cd analysis/test-analysis**

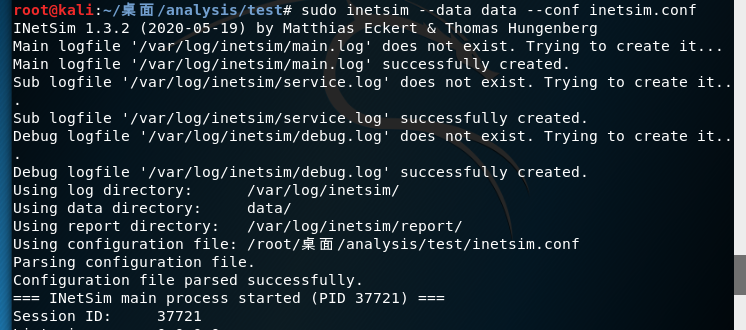


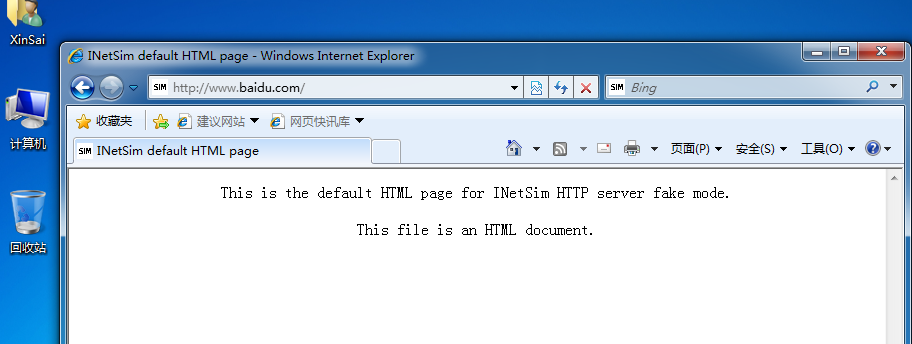
**$ sudo systemctl disable systemd-resolved.service  
$ sudo service systemd-resolved stop**



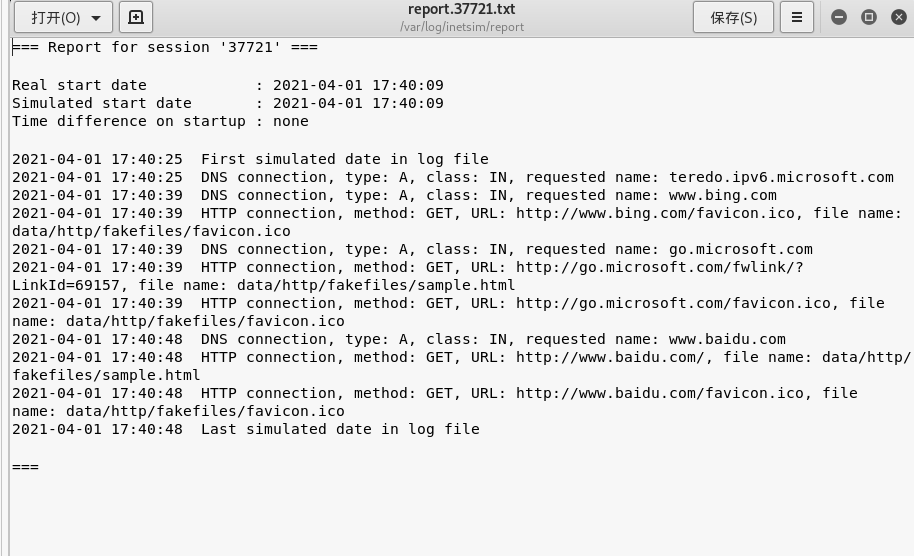


启动**sudo inetsim --data data --conf inetsim.conf**





ctrl+c结束并查看摘要报告  
**gedit /var/log/inetsim/report/report.37721.txt**

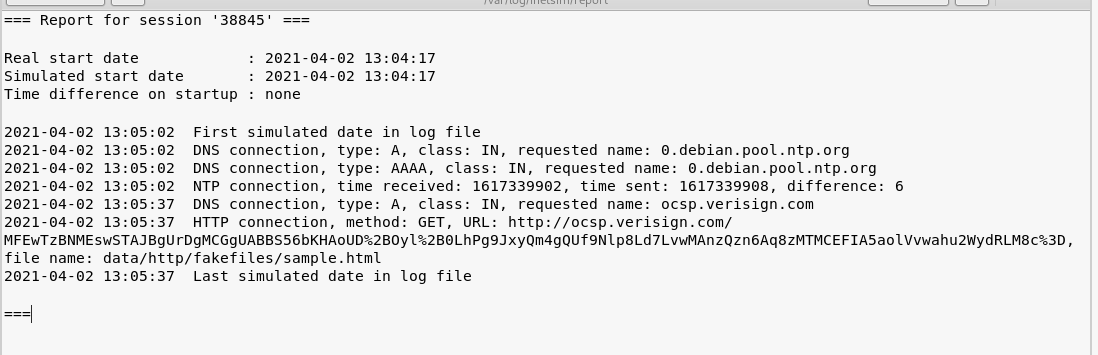


点击运行





查看生成的报告



1. **Cuckoo使用(20分)**
2. 在Linux搭建cuckoo沙箱；(10分)

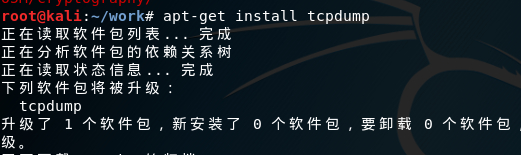
1.安装依赖



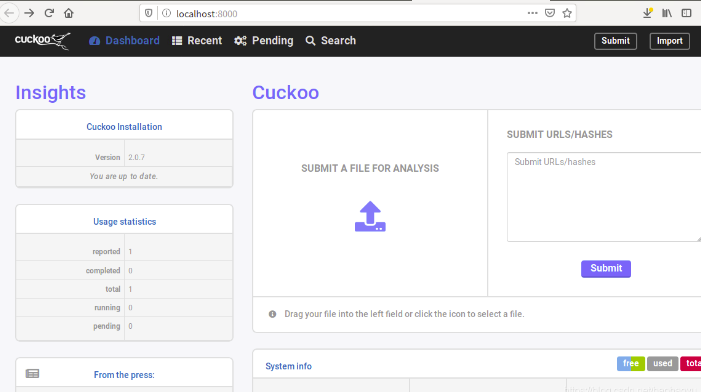
2.安装mongodb



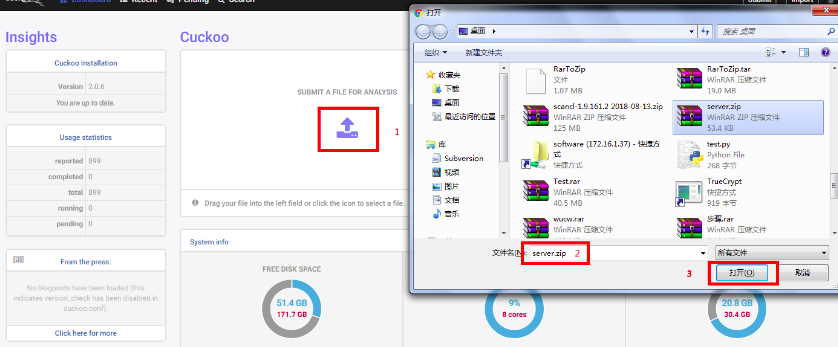
3.安装python依赖与tcpdump



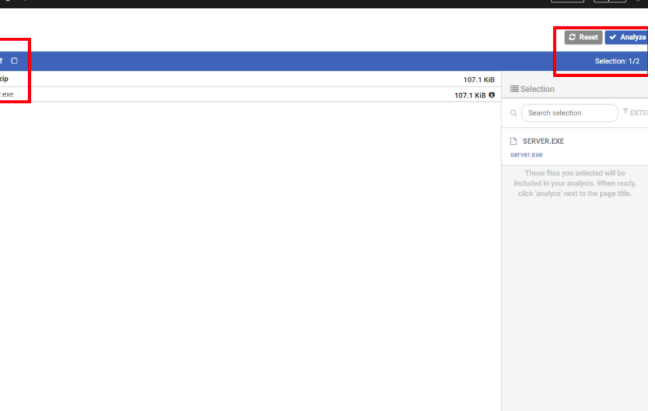


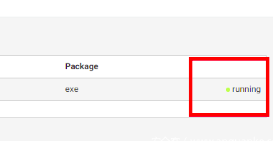


1. 使用python或手动上传第1题分析得的恶意软件，阅读分析报告，分析其在进程、注册表、网络等方面的行为，解释分析结果。(10分)

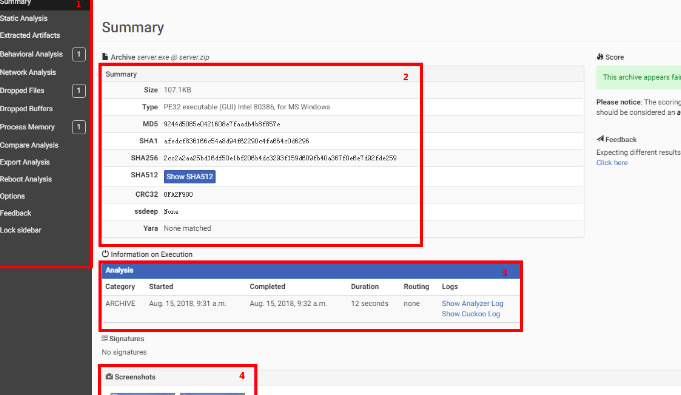


分析





查看分析结果

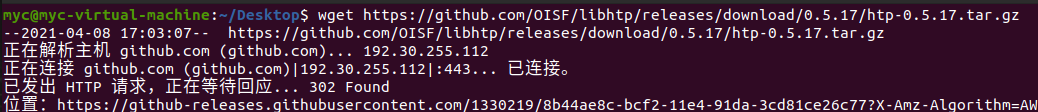


**4. Suricata使用(20分)**

1) 在Linux使用**源码**安装流量分析系统Suricata；(10分)

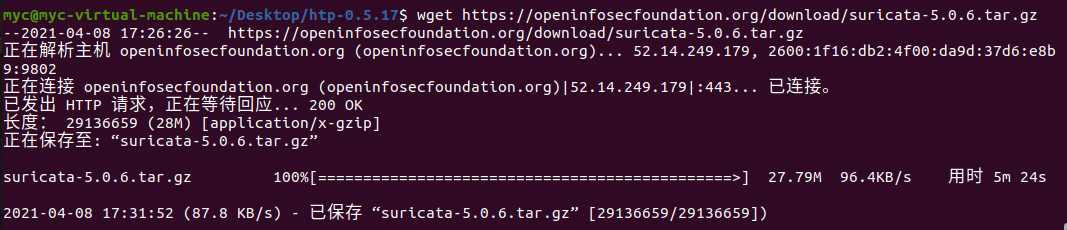
1.下载

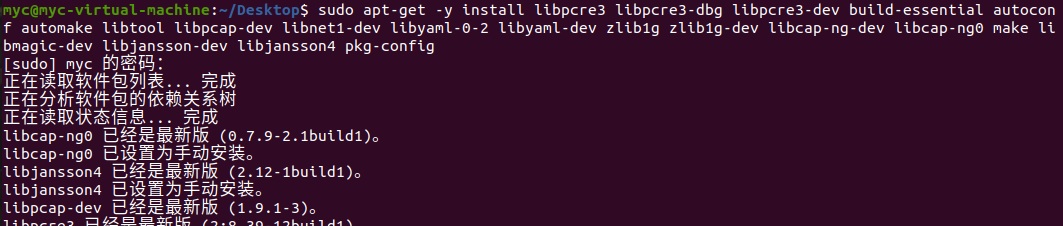
htp下载  
wget https://github.com/OISF/libhtp/releases/download/0.5.17/htp-0.5.17.tar.gz



suricata 源码安装

<https://openinfosecfoundation.org/download/> 中选个自己喜欢的版本下载



1. 安装依赖  
   sudo apt-get -y install libpcre3 libpcre3-dbg libpcre3-dev build-essential autoconf automake libtool libpcap-dev libnet1-dev libyaml-0-2 libyaml-dev zlib1g zlib1g-dev libcap-ng-dev libcap-ng0 make libmagic-dev libjansson-dev libjansson4 pkg-config   
   

安装ntp

tar -xzvf libhtp-0.5.17.tar.gz   
cd libhtp-0.5.17   
./configure   
make&& make install

安装suricata

tar -xzvf suricata

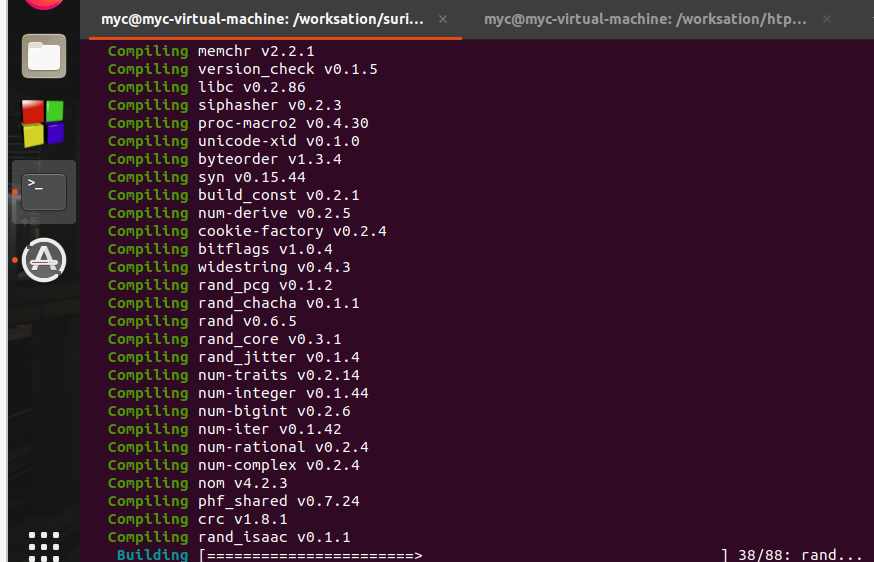
cd suricata

./configure --enable-nfqueue --prefix=/usr --sysconfdir=/etc --localstatedir=/var

中间报缺失软件

sudo apt install rustc cargo

make

  
  
make sudo make install sudo make install-conf # 安装默认配置  
 sudo make install-rules # 安装默认规则  
 sudo ldconfig # 让系统共享动态链接库

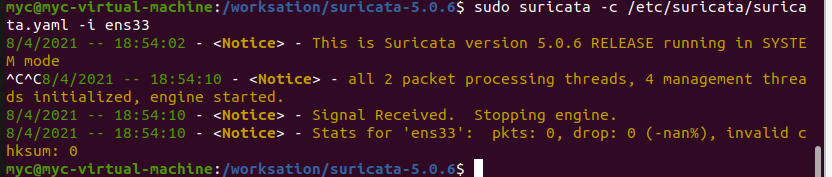
sudo ethtool -K ens33 gro off lro off

关闭 Suricata 监听网卡上的包卸载例如 LRO/GRO）功能，会干扰包捕获

如果提示 Cannot change large-receive-offload，那就不用管他了，这说明你的网卡本来就不支持 LRO 功能。

sudo iptables -I INPUT -p tcp -j NFQUEUE   
sudo iptables -I OUTPUT -p tcp -j NFQUEUE

让 Suricata 以 IDS 模式启动:  
sudo suricata -c /etc/suricata/suricata.yaml -i ens33

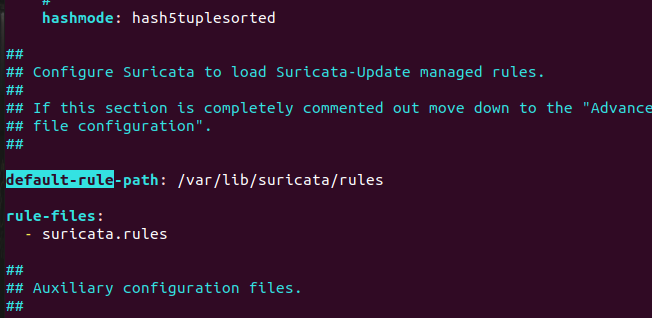


2) 编写Suricata规则，用于检测第1题的攻击(可针对IP、域名或恶意代码的规则)，并进行验证。(10分)  
**规则编写**

alert tcp any any ->any any (msg:”MALWARE Windows executable sent when host clamis to send an image”;flow:to\_server,established;content:"PE";sid:2021040801; rev:1;)

**验证过程**

1. 准备好恶意代码  
    <http://101.200.46.43/1.png>   
   2.修改规则，软件自带有规则 ,打开配置文件查看



3.修改/var/lib/suricata/rules/suricata.rules

直接自己传建一个，把自带的备份  
mv /var/lib/suricata/rules/suricata.rules /var/lib/suricata/rules/suricata.rules.bak

vim /var/lib/suricata/rules/suricata.rules  
写入规则

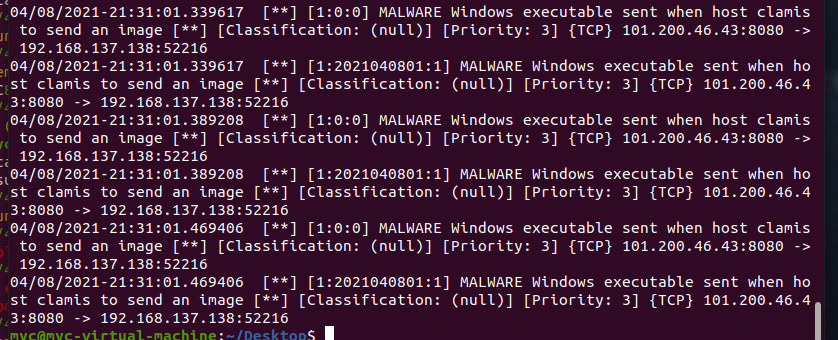
4.重启服务

5.下载



6.查看

cat /var/log/suricata/fast.log



**5. 编写实验报告文档，包括实验过程、分析和截图**(10分)。