

《计算机网络安全技术》课后作业

2017 秋季 • 40240572 • 主讲：尹霞

姓名： _____ 学号： _____

作业要求：

布置作业时间：2017 年 12 月 08 日（第 12 周）

提交作业期限：[2017 年 12 月 29 日（第 15 周）](#)

提交作业方式：网络学堂（请使用作业模板提交作业）

迟交与未交的作业都按照零分计算

本次作业在课程最终成绩中记 10 分

作业题目：体验入侵检测（10 分）

下面共有 2 个任务，请认真阅读任务说明，并提交详细的实验报告。

《计算机网络安全技术》课后作业

2017 秋季 • 40240572 • 主讲：尹霞

体验入侵检测

实验背景

入侵检测系统 (IDS) 是一种对网络传输进行即时监视, 在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。

Suricata 是一种较为著名的入侵检测系统, 本实验的主要内容是使用 Suricata 对给出的 pcap 文件进行检测, 并对 pcap 文件进行分析。

实验环境

VMware 上的 Ubuntu 虚拟机。已经给出了虚拟机的 ovf 文件, 只需在 VMware 中将 ubuntu.ovf 导入即可。虚拟机中已经对相关实验环境进行了配置。用户名和密码均为 **suricata** (全部小写字母)。

实验数据

进入虚拟机系统后, 在桌面上的 pcapfile 文件夹中有三个标号为 1、2、3 的 pcap 文件, 选择自己学号对 3 取余后的那一个文件进行检测即可。

实验命令

```
cd /home/suricata/Desktop/pcapfile
```

```
sudo su
```

密码输入 suricata

```
suricata -r x.pcap -l ./
```

```
vim fast.log
```

即可得到实验结果

任务 1 分析实验结果 (5 分)

本实验中给出的 pcap 文件内容均为 DoS 攻击的数据包, 请根据 Suricata 的检测结果分析 DoS 攻击的端口以及服务, 并简要描述该服务的内容。

任务 2 分析 pcap 文件内容 (5 分)

使用包分析软件 (如 Wireshark) 对你检测的 pcap 文件进行分析, 找出主要的源 IP、源端口、目的 IP、目的端口、包的内容等。