拒绝服务攻击检测实验指导书

一. 实验目的

拒绝服务攻击检测实验使学生贯通编程技术、计算机网络、网络安全等知识，完成自主设计拒绝服务攻击场景、开发网络攻击程序、使用工具分析和检测网络攻击等实验内容，理解和掌握资源消耗型拒绝服务攻击的原理和过程、攻击流量分析、攻击检测等知识，实现对“网络攻击-安全分析-检测告警”的综合能力培养和实践训练。并使学生能够举一反三，掌握网络攻击检测的通用方法和流程，为后续的网络安全知识学习打下坚实基础。

二. 实验内容

1. 理解拒绝服务攻击导致的资源消耗原理和危害，自主设计构建网络攻击场景。

2. 开发和执行拒绝服务攻击程序，并从网络用户端对比存在和不存在网络攻击两种场景下访问网络应用的情况。

3. 使用网络流量分析工具 Wireshark 等观察、分析和总结拒绝服务攻击流量特征。

4. 使用入侵检测工具 Snort 等，并配置攻击检测特征规则，完成对拒绝服务攻击的检测识别和告警。

三. 实验原理

1. 拒绝服务攻击原理

拒绝服务攻击是针对网络应用有限数量的服务能力，发起大规模的网络服务的请求，耗尽网络应用能够提供的服务计算资源等，使网络应用无法对正常用户的请求进行服务，实现拒绝服务。

2. 拒绝服务攻击流量特征分析

通过网络流量捕获工具捕获与网络应用服务器交互的网络流量，对请求服务和响应的网络应用协议网络流量进行分析，查找网络应用无法为网络用户提供服务的原因。观察每个独立的网络应用请求，都是正常的建立连接、请求网络服务操作过程。但是能够观察到来自于同一个源地址的网络服务请求的数量多、单位时间内的请求频率高，超过了单个网络用户访问网络应用服务的正常表现。这种

异常的大量、高频度访问行为可作为拒绝服务攻击流量的特征。

3．基于流量频率特征的拒绝服务攻击检测

由于拒绝服务攻击具有大量、高频度访问的异常行为特征，将对网络应用的高频请求作为拒绝服务攻击的检测识别特征，配置到入侵检测工具的攻击检测和告警规则中，对网络流量进行检测，实现对拒绝服务攻击的识别和报警。

四． 实验注意事项

1.在编写生成拒绝服务攻击请求的程序时，需要注意配置的并发线程数量等参数，将会影响单位时间内产生的网络攻击流量强度，以及拒绝服务攻击的效果。

2.需要正确配置网络环境以及交换机流量镜像，否则入侵检测系统无法捕获到攻击流量。

3.需要遵循入侵检测规则的格式规范，配置能够反映拒绝服务攻击特征的检测告警规则，否则不会产生告警信息。

五． 实验要求

1. 完成开发拒绝服务攻击程序、攻击流量分析、攻击检测等实验内容。

2. 提交拒绝服务攻击程序代码、可加载运行的相关工程文件。

3. 提交实验报告，包括:拒绝服务攻击环境设计、网络攻击程序概要设计、存在网络攻击时访问网络应用的结果和分析、攻击流量分析和特征说明、配置的攻击检测特征和检测告警结果，以及实验中遇到的问题和原因等。

六． 实验过程

围绕拒绝服务攻击环境构建，以及网络攻击生成、分析、检测告警等实验内容，包括 10 个交互步骤：

步骤 1：构建拒绝服务攻击场景

1）访问 vse.bupt.edu.cn，登陆网络安全虚拟仿真实验系统

图 1 登陆网络安全虚拟仿真实验系统

2）创建拒绝服务攻击网络拓扑

选择“实例管理-创建实例拓扑”，通过拖拽方式在场景中构建 Web 拒绝服务攻击者、网络用户、Web 服务器、交换机、入侵检测等设备，通过绘制连接线完成设备之间的网络互联。

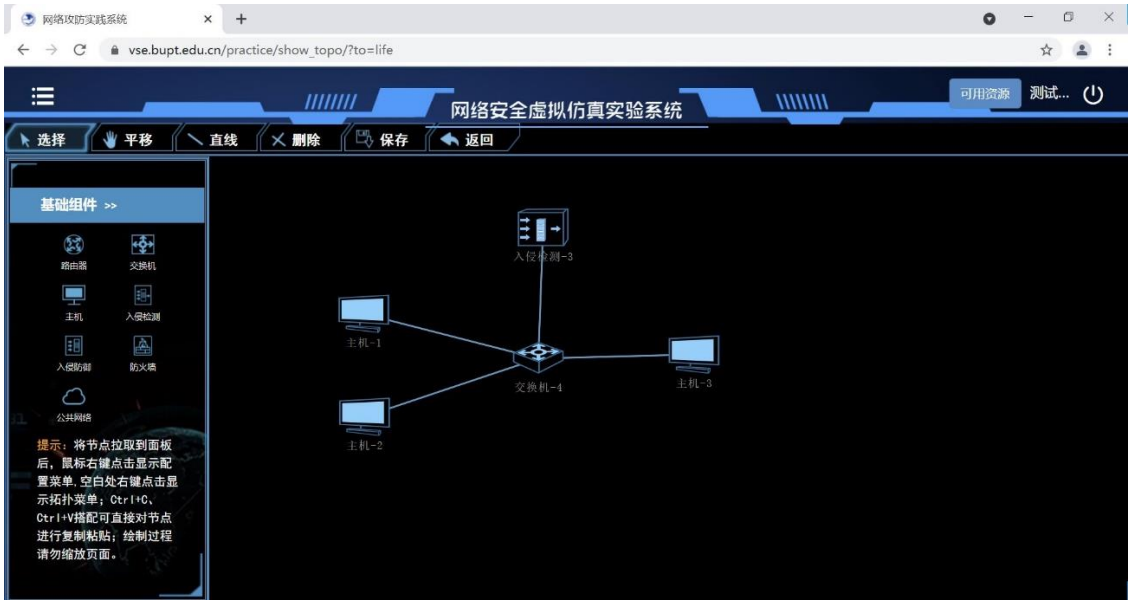

图 2 创建拒绝服务攻击网络拓扑

步骤 2：配置和部署拒绝服务攻击场景的节点

1）通过右键点击 Web 拒绝服务攻击者、网络用户、Web 服务器等设备，配置加载的操作系统模板，以及运行所需的处理器、内存、硬盘等硬件参数。

图 3 配置拒绝服务攻击场景的节点

2）配置入侵检测和交换机镜像，使流经交换机的流量通过镜像口流入入侵检测系统。

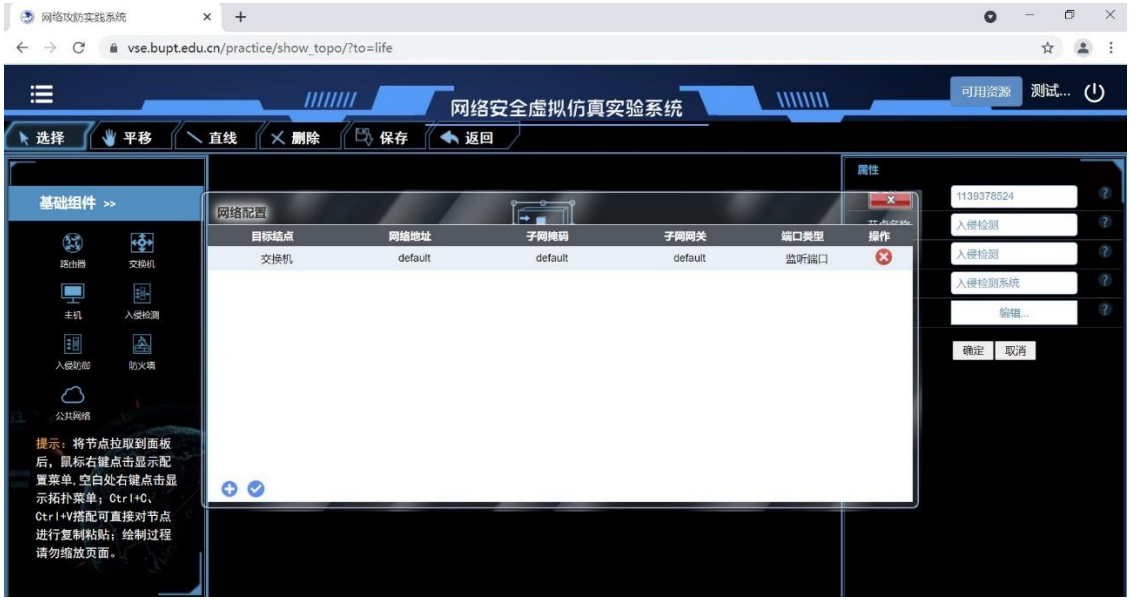

图 4 配置入侵检测和交换机镜像

3）保存拒绝服务攻击场景，等候分钟级的部署时间后，拒绝服务攻击网络环境构建完成，通过节点详情，看到部署完成的所有设备。

图 5 节点详情

步骤 3：网络用户访问网络应用服务

1）在节点详情中，通过远程连接方式登陆网络用户端，根据节点 IP，访问网络应用服务。

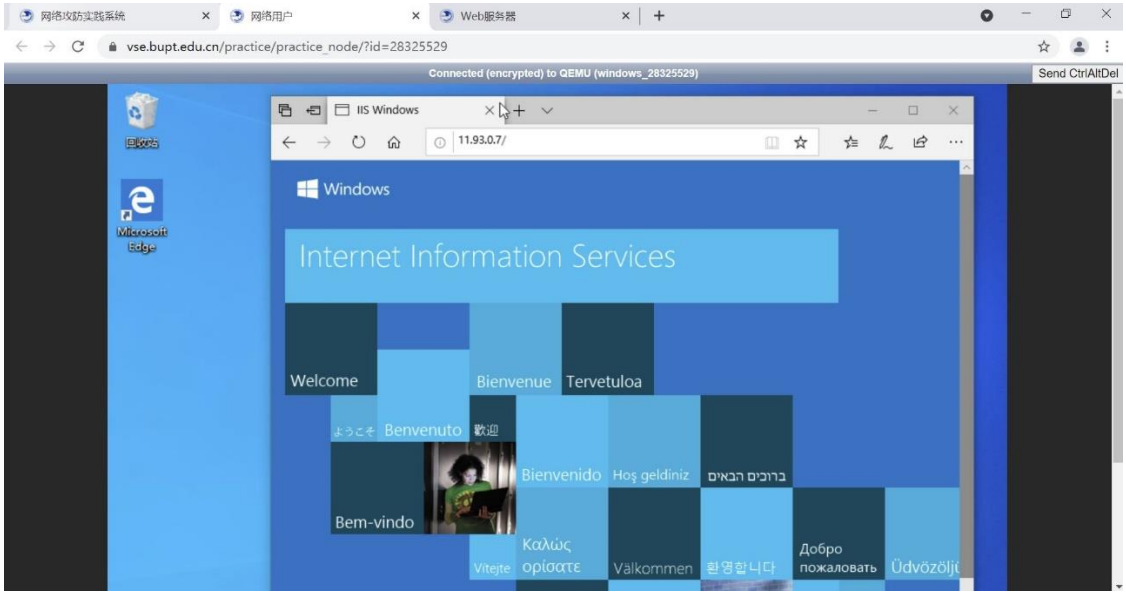

图 6 网络用户成功访问 Web 服务

2）在网络应用服务端查看任务管理器，观察无拒绝服务攻击时 CPU 等资源占用情况。

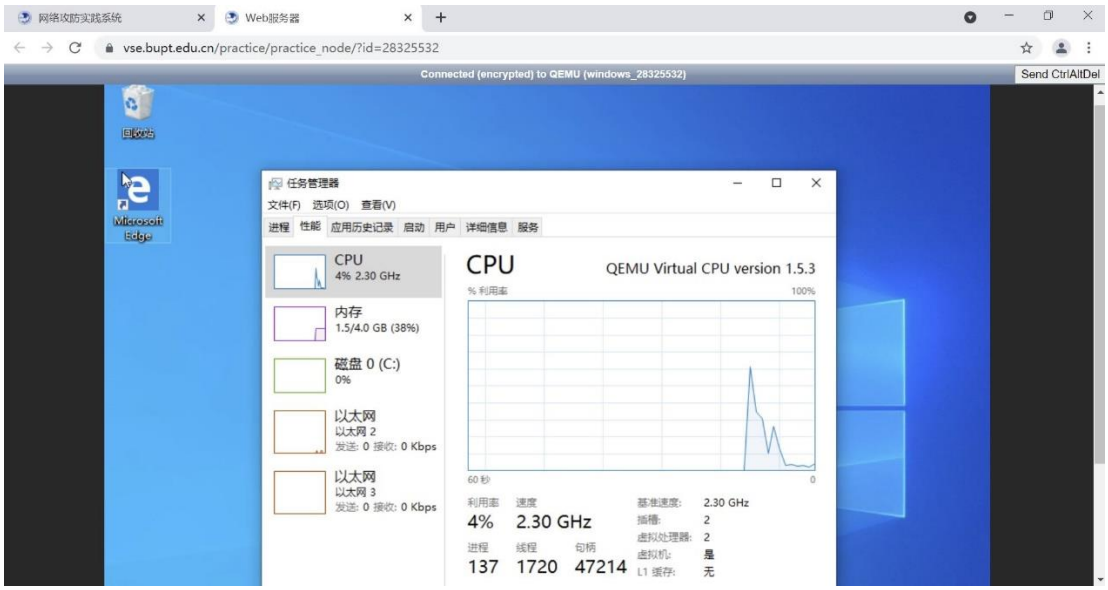

图 7 无拒绝服务攻击时 Web 服务器资源占用情况

步骤 4：开发拒绝服务攻击程序

在拒绝服务攻击者端开发多线程攻击流量生成程序，实现并发产生高强度的网络应用服务请求，并将被攻击的网络应用服务器节点 IP、并发线程数量作为程序的输入参数。

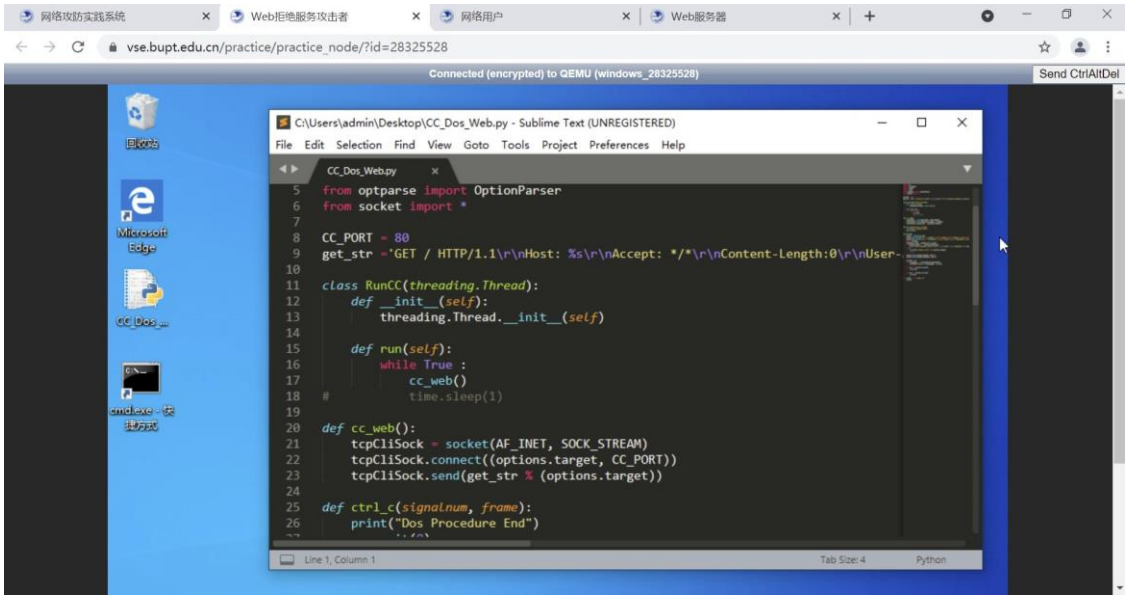

图 8 拒绝服务攻击生成代码

步骤 5：实施拒绝服务攻击

在拒绝服务攻击者端上执行网络攻击程序。通过调节并发线程数量，理解对拒绝服务攻击请求数量强度的影响。

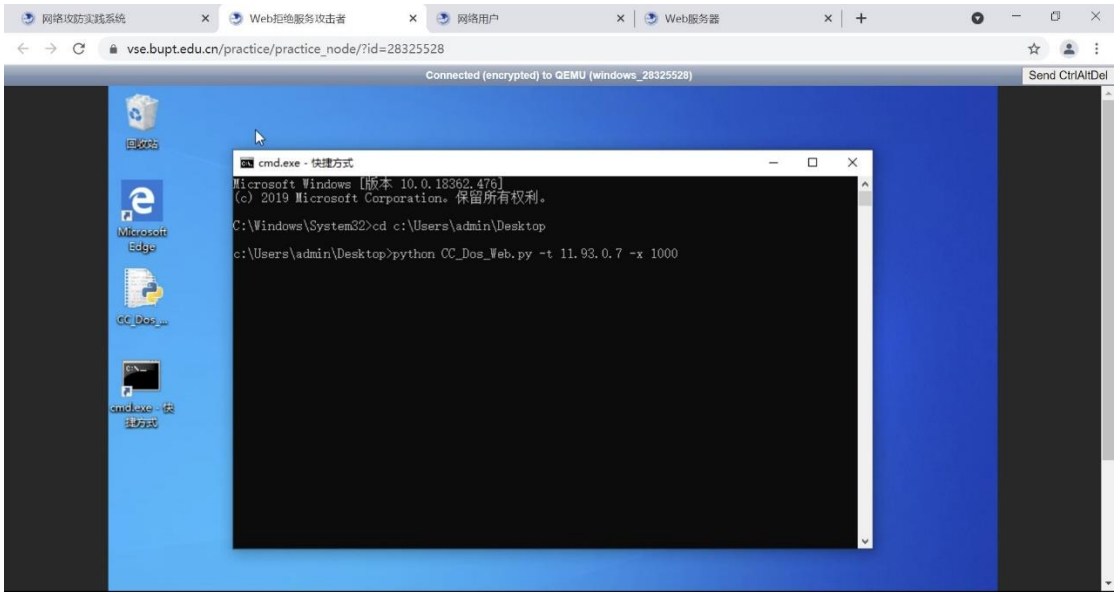

图 9 实施拒绝服务攻击

步骤 6：对比查看拒绝服务攻击效果

1）拒绝服务攻击发生时，在网络用户端访问网络应用，并与无拒绝服务攻击时能够成功访问网络应用的情况进行对比。

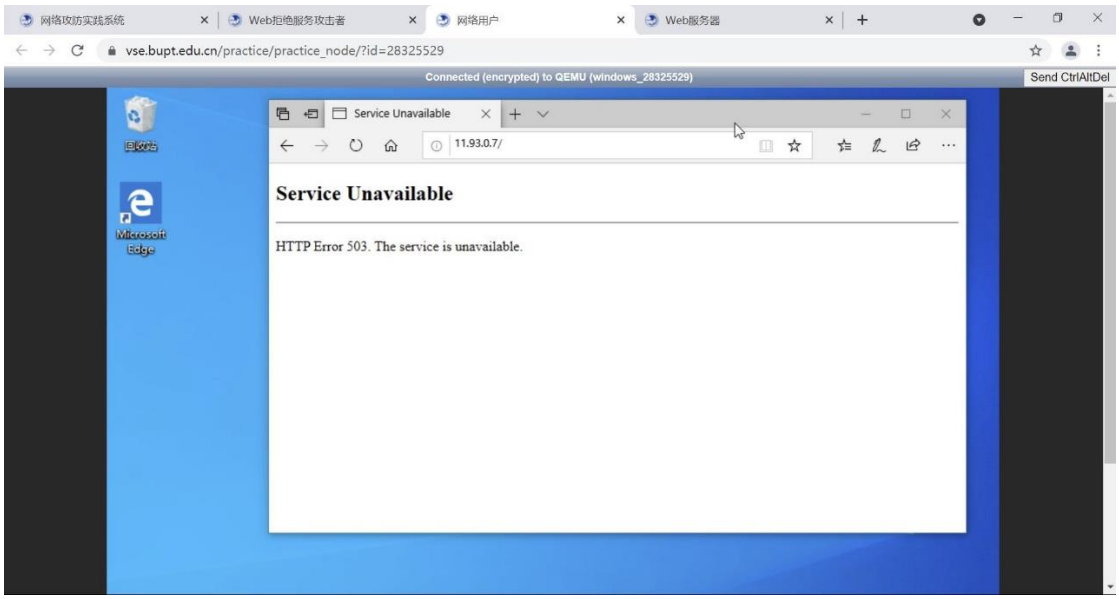

图 10 拒绝服务攻击发生时 Web 访问失败

2）在网络应用端，观察计算等资源占用率情况，并与无拒绝服务攻击时的情况进行对比，理解拒绝服务攻击对资源的消耗影响。

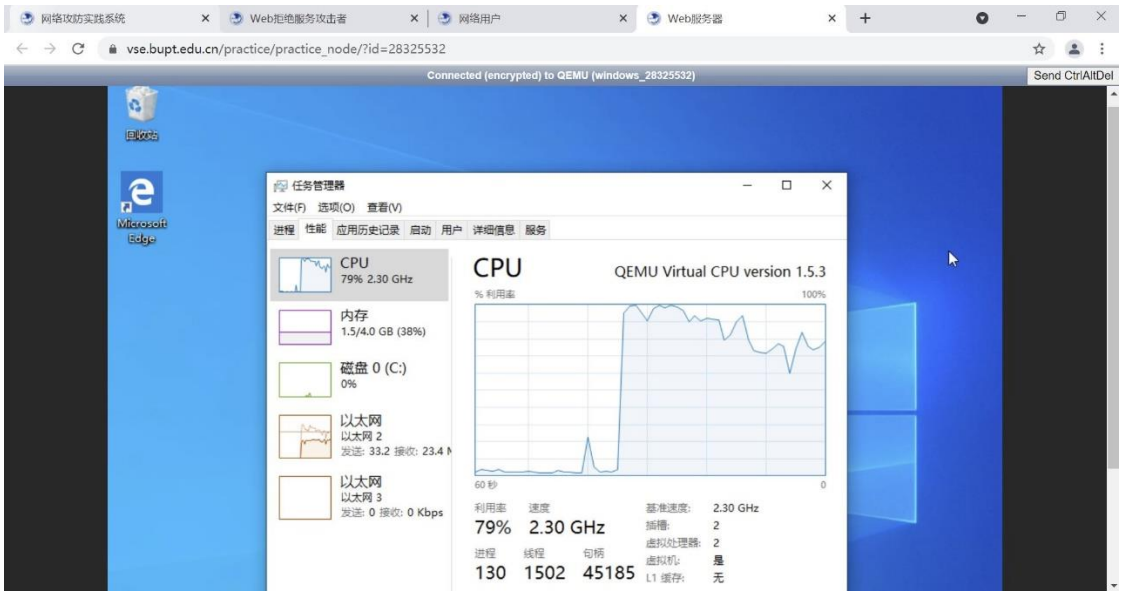

图 11 拒绝服务攻击发生时 CPU 资源占用率高

步骤 7：捕获网络流量

在入侵检测端使用网络流量捕获工具 Wireshark 等，捕获交换机镜像的包含拒绝服务攻击的网络流量。

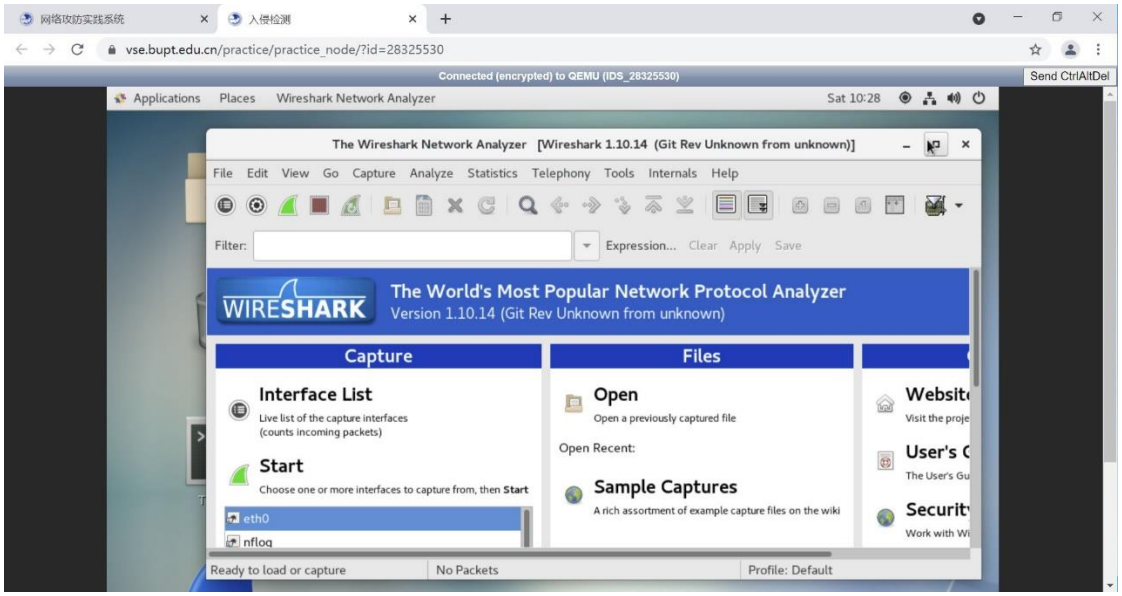

图 12 Wireshark 捕获网络流量

步骤 8：分析拒绝服务攻击流量

在入侵检测端结合 TCP/IP、网络应用协议等知识，使用网络流量分析工具 Wireshark 等观察、分析和总结拒绝服务攻击流量特征。发现在短时间内，网络流量中含有大量来自同一个源地址的网络请求，具有显著的拒绝服务攻击的高频特征。

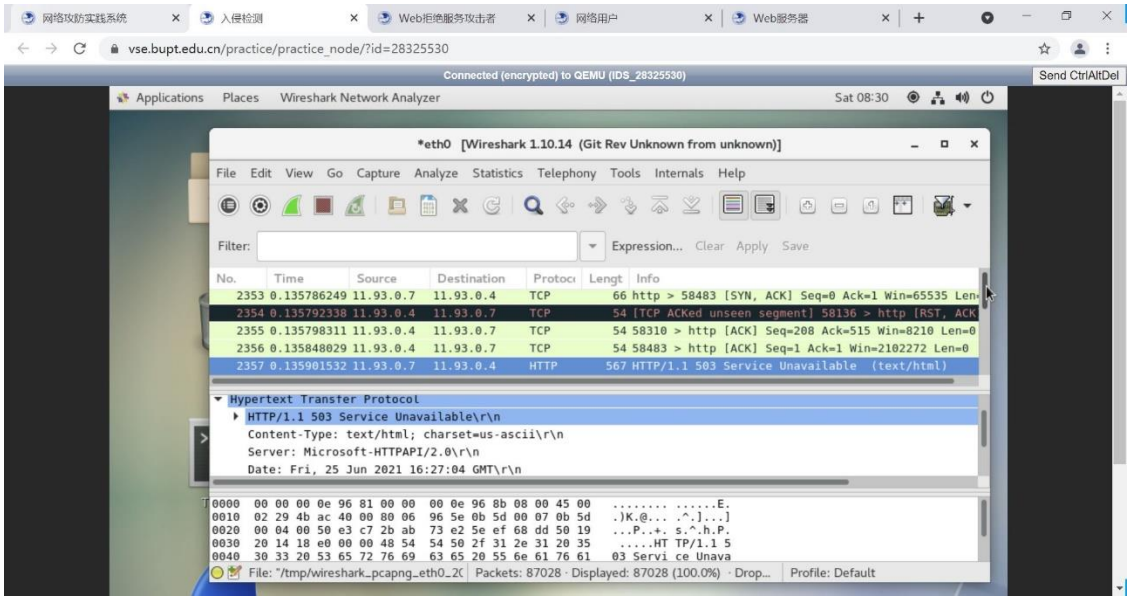

图 13 分析拒绝服务攻击流量

步骤 9：配置拒绝服务攻击检测规则

在入侵检测端，将对网络应用的高频请求作为拒绝服务攻击特征，配置到入侵检测工具 Snort 的检测和告警规则中。

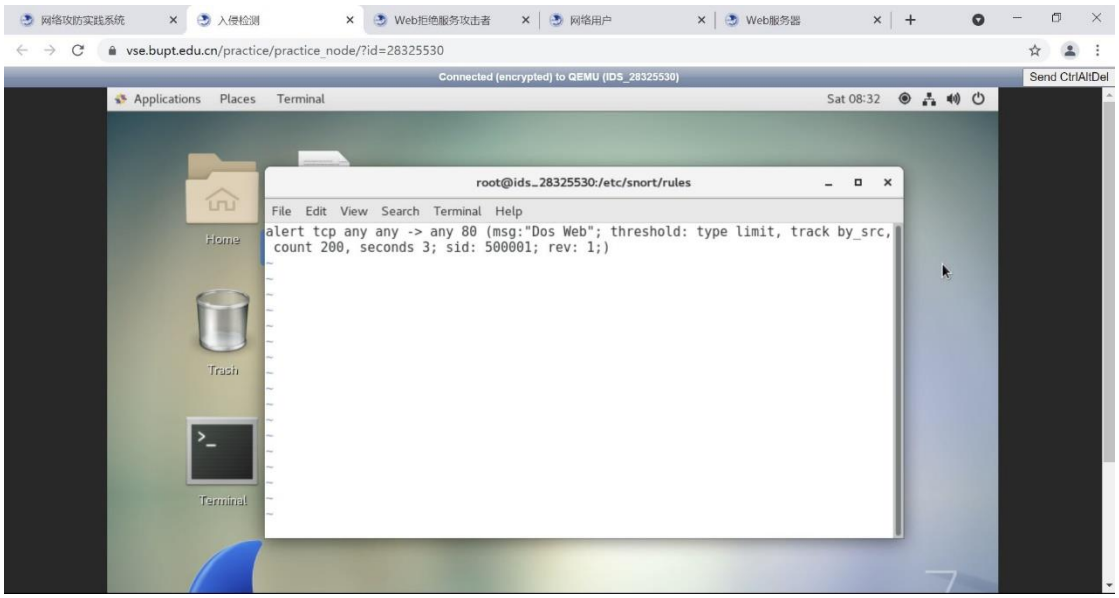

图 14 编写拒绝服务攻击检测规则

步骤 10：检测拒绝服务攻击

1）在入侵检测端运行入侵检测工具 Snort 等。

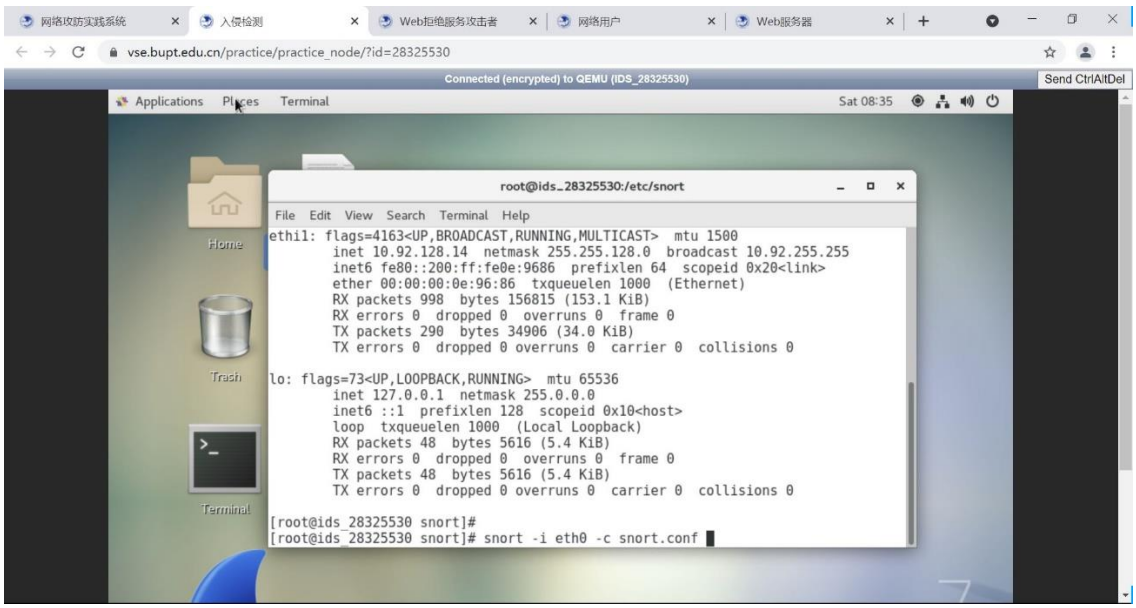

图 15 运行入侵检测工具 Snort

2）验证日志文件中触发网络攻击告警信息的检测规则的编号是否与之前配置的检测规则的编号相同。

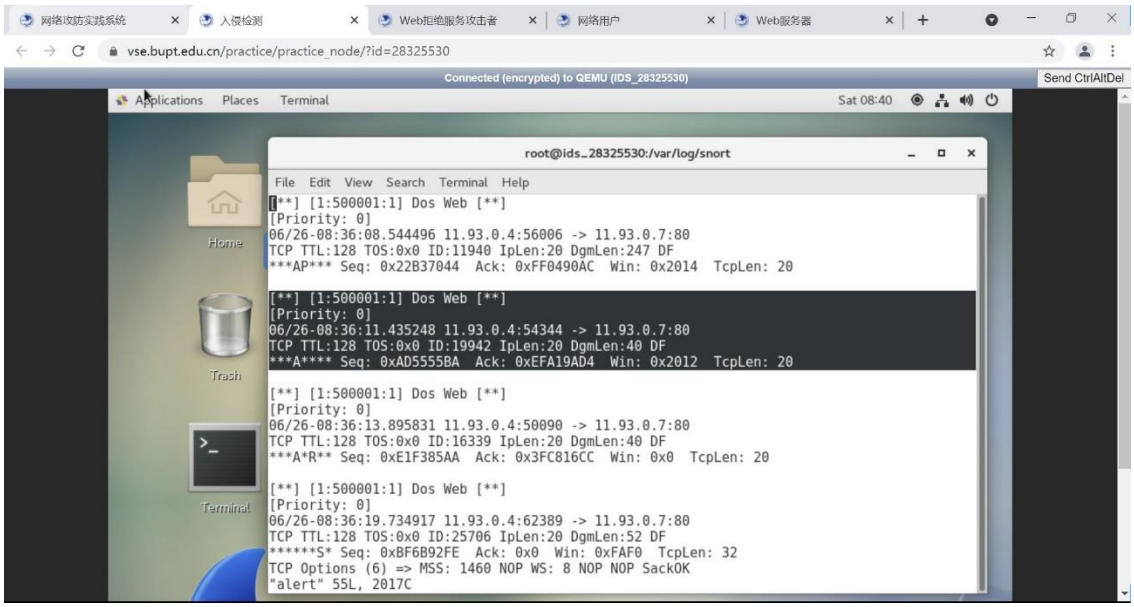

图 16 检测到拒绝服务攻击的告警日志