Snort使用实践报告

姓名：任宇 学号：33920212204567

1. 实践任务

在Linux或Windows攻击机上使用Snort，对给定的pcap文件进行入侵检测，获得报警日志：

➢Snort运行命令提示

• 从离线的pcap文件读取网络日志数据源

• 分析配置规则，并在snort.conf中配置明文输出报警日志文件

• 指定报警日志log目录(或缺省log目录=/var/log/snort)。

1. 实践要求、

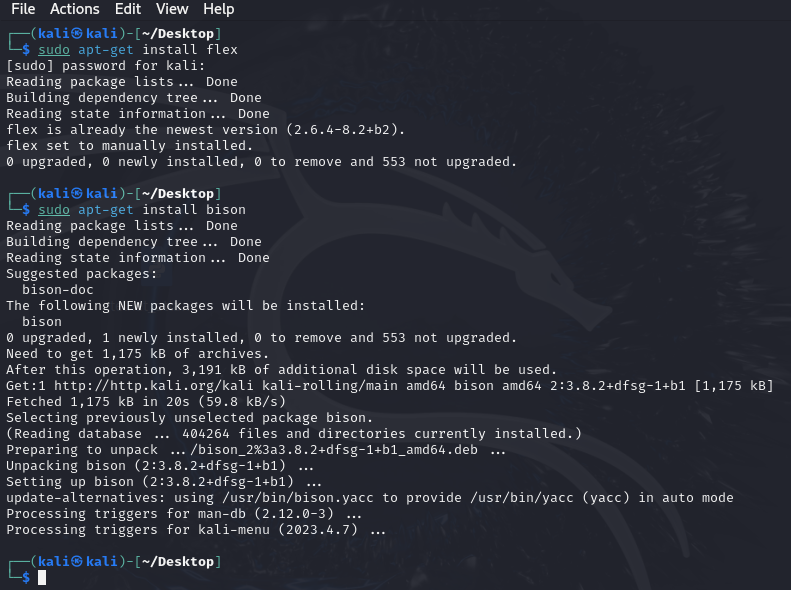
* 安装并使用Snort从离线的pcap文件读取并分析网络日志数据源。

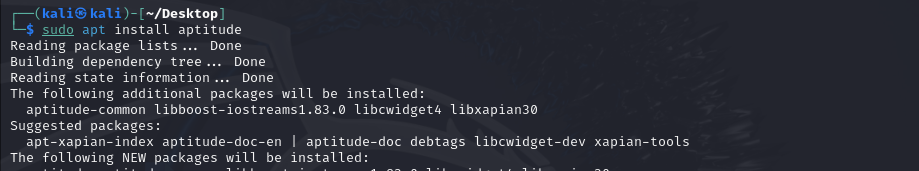
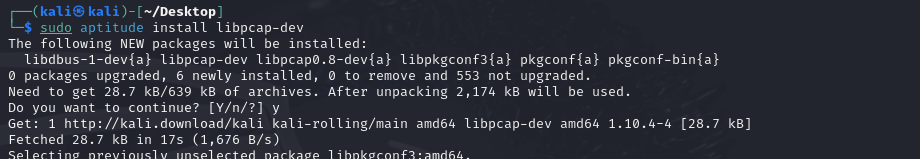
1. 实践环境

虚拟机版本为Kali 2024.1，Snort版本为2.9.17.1。

1. 实践步骤
2. 预装daq所需程序：

* *sudo apt-get install flex*
* *sudo apt-get install bison*
* *sudo apt install aptitude*
* *sudo aptitude install libpcap-dev*

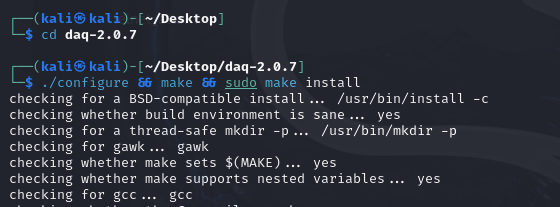


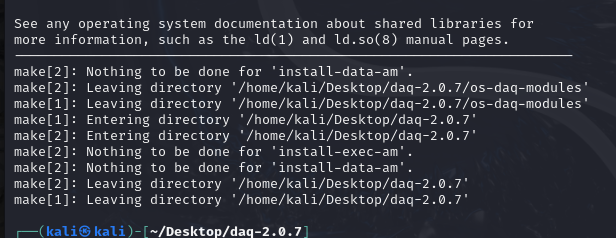
 

1. 安装daq：
   * + *wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz*
     + *tar xvfz daq-2.0.7.tar.gz*
     + *cd daq-2.0.7*
     + *./configure && make && sudo make install*
     + *cd ..*



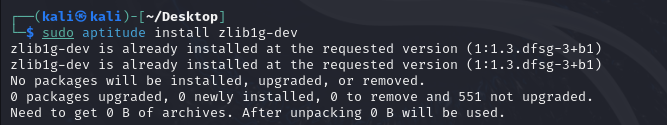
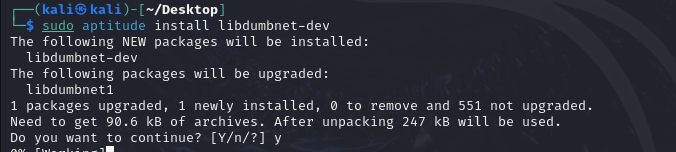
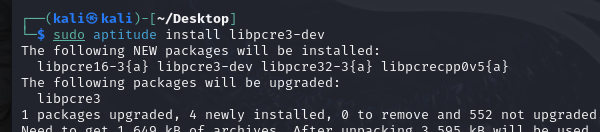
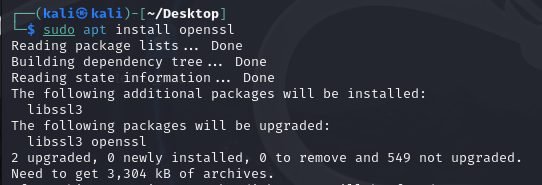
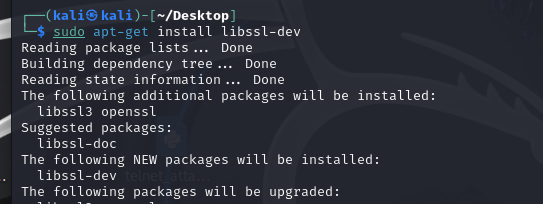


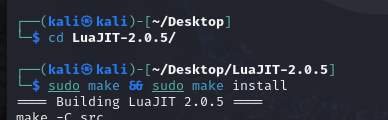




1. 安装Snort依赖程序：

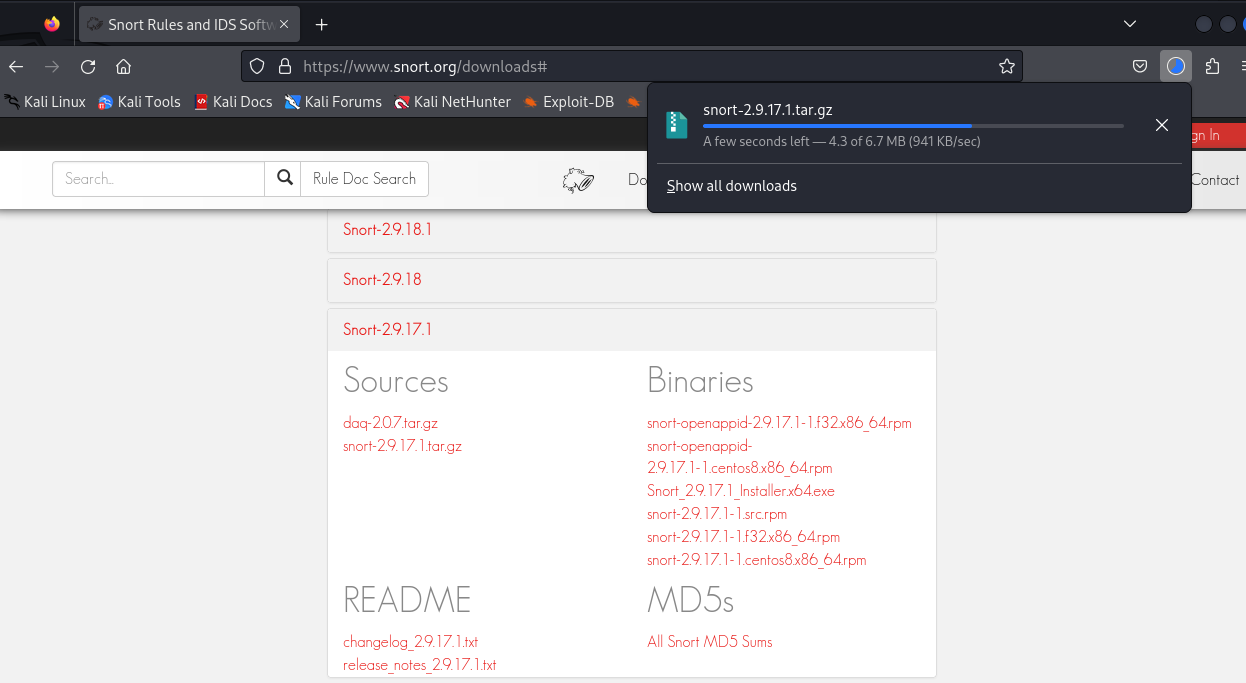
* *aptitude install libpcre3-dev*
* *aptitude install libdumbnet-dev*
* *aptitude install zlib1g-dev*
* *apt install openssl*
* *apt-get install libssl-dev*
* *sudo wget http://luajit.org/download/LuaJIT-2.0.5.tar.gz*
* *sudo tar -zxvf LuaJIT-2.0.5.tar.gz*
* *cd LuaJIT-2.0.5/*
* *sudo make && sudo make install*

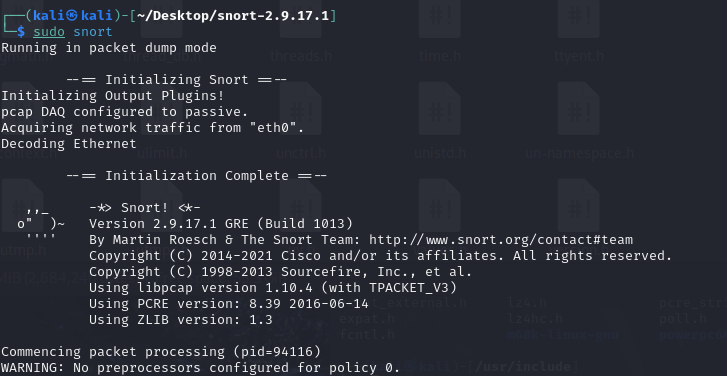
 

1. 安装Snort：

* *tar xvfz snort-2.9.17.1.tar.gz*
* *cd snort-2.9.17.1*
* *./configure --enable-sourcefire && make && sudo make install*

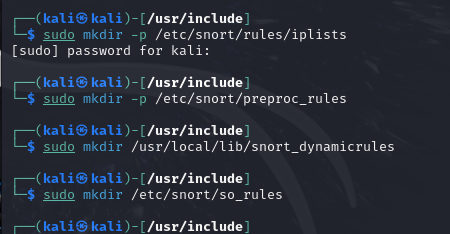




1. 配置Snort，创建配置必要的文件夹：

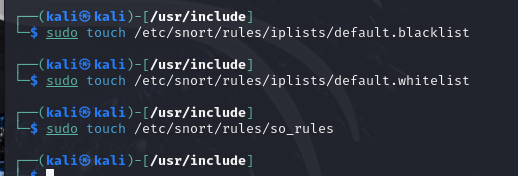
Snort的安装目录

* *sudo mkdir -p /etc/snort/rules/iplists*
* *sudo mkdir -p /etc/snort/preproc\_rules*
* *sudo mkdir /usr/local/lib/snort\_dynamicrules*
* *sudo mkdir /etc/snort/so\_rules*



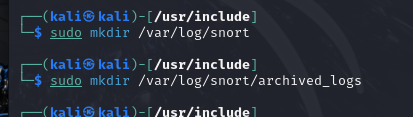
存储过滤规则和服务器黑白名单

* *sudo touch /etc/snort/rules/iplists/default.blacklist*
* *sudo touch /etc/snort/rules/iplists/default.whitelist*
* *sudo touch /etc/snort/rules/so\_rules*



创建日志目录

* *sudo mkdir /var/log/snort*
* *sudo mkdir /var/log/snort/archived\_logs*

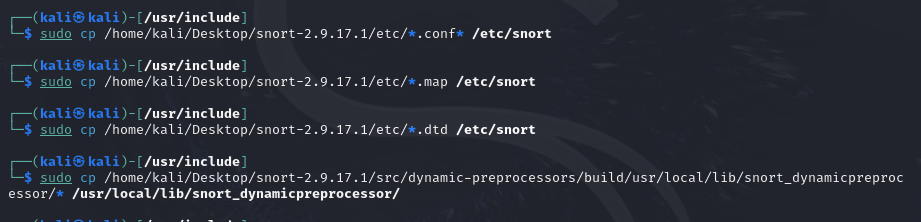


调整权限

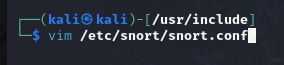
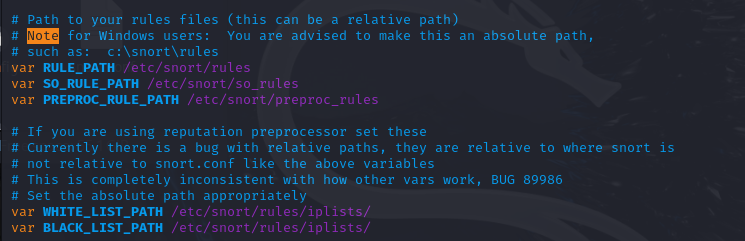
* *sudo chmod -R 5775 /etc/snort*
* *sudo chmod -R 5775 /var/log/snort*
* *sudo chmod -R 5775 /var/log/snort/archived\_logs*
* *sudo chmod -R 5775 /etc/snort/rules/so\_rules*
* *sudo chmod -R 5775 /usr/local/lib/snort\_dynamicrules*



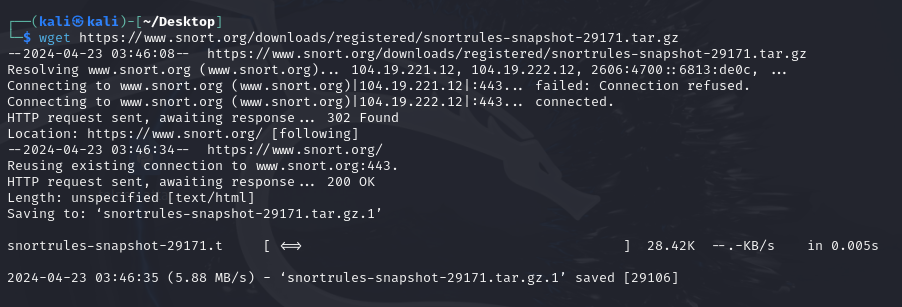
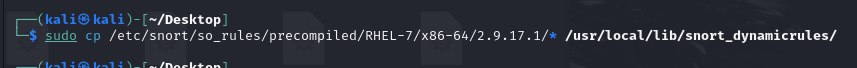
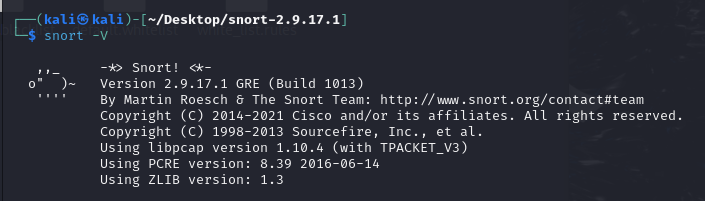
1. 复制文件到 /etc/snort：



1. 修改默认配置：

1. 安装rules包：

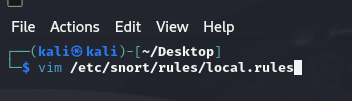
  

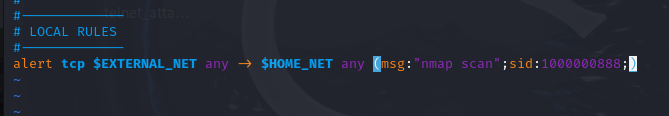
1. 利用Snort检测nmap扫描，在 /etc/snort/rules/local.rules下进行tcp规则配置：

Snort的规则配置是它的核心功能之一，用于定义如何监控网络流量并对潜在的威胁进行响应。规则文件通常包含在Snort安装目录下的rules文件夹中。每条规则定义了一组条件，用来匹配数据包中的特定模式。当匹配发生时，Snort 会执行规定的动作，如记录日志、发送警告等。每条规则由以下几部分组成：

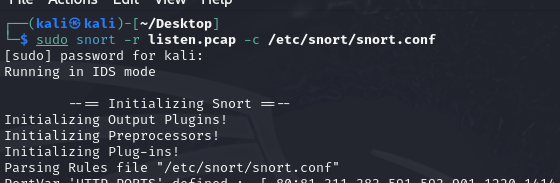
* 动作：例如 alert, log, pass等，指定当规则匹配时Snort应采取的动作。
* 协议：指定规则适用的网络协议，如ip,tcp,udp,icmp等。
* 源IP和端口：定义数据包源的IP地址和端口号。可以是具体值或通配符。
* 方向运算符：通常是->(从源到目标)或<>(双向)。
* 目标IP和端口：定义数据包目的地的IP地址和端口号。
* 规则选项：包含在括号内，提供了规则的详细条件，如内容、SID、修订号、消息等。

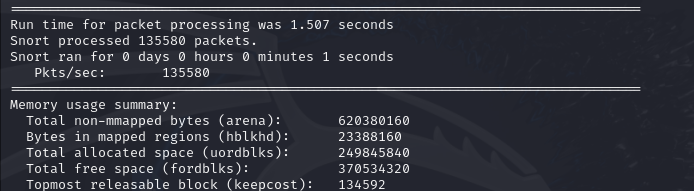
根据以上几部分，可以构建一条用于记录nmap命令的警告规则，如下所示：

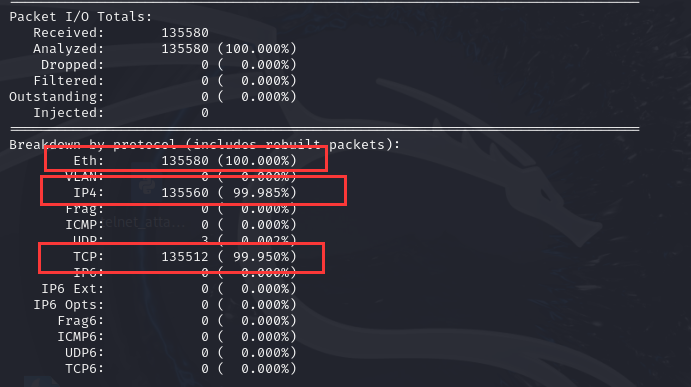
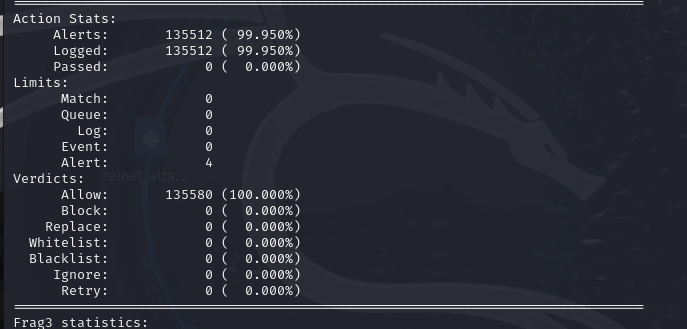




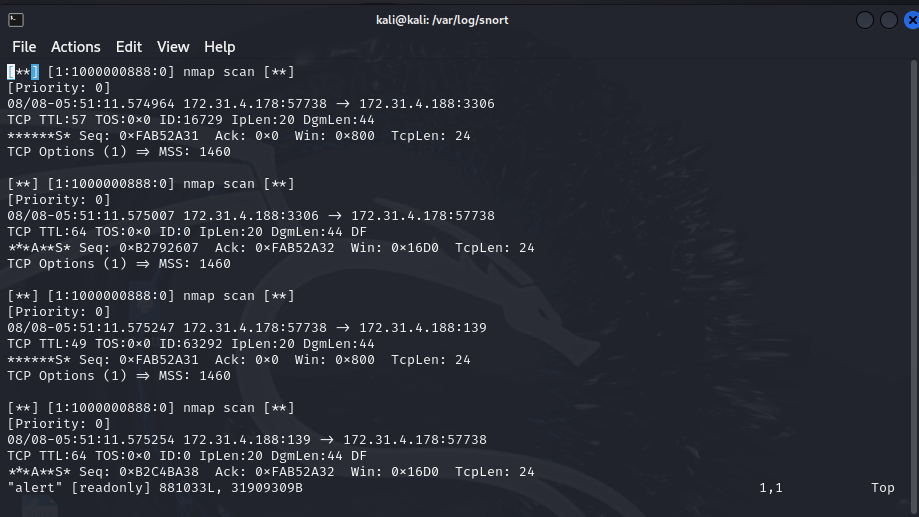
1. 启动snort扫描检测离线的网络数据包：





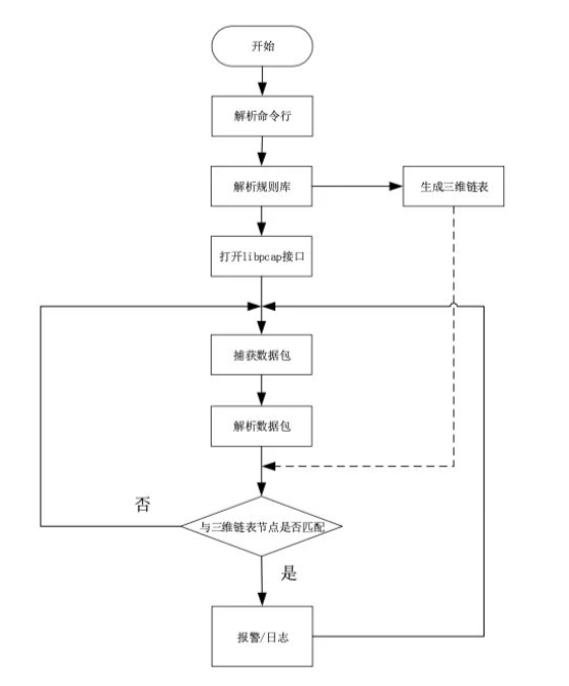
 

1. 在var/log/snort中查看检测结果：



1. 实践总结

Snort是一个非常流行的开源网络入侵检测系统，它能够进行实时的流量分析和数据包记录。Snort利用强大的规则引擎，通过网络接口来检测潜在的恶意活动或策略违规行为。Snort的规则库被设计来检测各种攻击和漏洞，如隐蔽扫描、CGI攻击、OS指纹识别等。其结构如下所示：



在本次实践中，我通过在Kali Linux环境下安装和配置Snort，成功地对包含nmap命令生成的数据包的pcap文件进行了入侵检测分析。通过本次实践，我深入理解 Snort的基本工作原理和配置方法。利用Snort检测nmap扫描只是展示了它能力的一小部分。Snort的真正力量在于其灵活的规则配置和广泛的社区支持，这使它成为网络安全领域中不可或缺的工具之一。