

实 验 报 告



课程名称 《网络攻击与防御技术》

学 院 计算机科学技术学院

专 业 信息安全

姓 名 黄 力

学 号 15307130275

开 课 时 间 2018 至 2019 学年第 1 学期

实验项目 名 称	Snort 安装	成绩	
-------------	----------	----	--

一、实验目的

(1) 通过本实验初步了解入侵检测系统的工作原理

二、实验内容

(1) 在虚拟机 (CentOS) 上安装和配置 snort 软件并以 IDS (入侵检测) 模式运行该软件, 在其它主机上使用 X-scan、nmap 等扫描软件对运行了 snort 的虚拟机进行扫描, 分析 snort 给出的报警信息是否与设置的规则相符

(2) 分析实验成功或失败的原因

三、实验环境

(1) PC 机操作系统: macOS Mojave 10.14

(2) 虚拟机操作系统 (Parallels Desktop 13.1.1): 64 位 CentOS、windows10

四、实验原理

snort 有三种用法: 嗅探模式、记录模式和网络入侵检测模式。本实验使用的是网络入侵检测模式, 基本原理是对网卡收发的数据包进行分析, 分析条目包括 IP 地址、协议、端口, 匹配规则集中的报警规则的数据包 snort 将进行报警。

本次实验的原理很简单, 只需按照实验要求中的步骤安装配置 snort、编写规则集, 安装 X-scan 等扫描工具, 然后对目标主机扫描并分析 snort 的报警信息即可。大部分的安装和配置过程参考了网络上资料 (见实验步骤), snort 安装在 CentOS 虚拟机上, X-scan 安装在 windows10 虚拟机上, snort 规则的编写只挑选了较为简单和常见的几条。

五、实验步骤及结果

安装过程参考了参考资料 1, 其中有一些步骤遇到包或库的缺失的错误我通过 google 搜索解决, 此处不赘述此过程。

(1) 安装依赖

安装命令: 1、安装 flex、bison: `yum install flex bison -y;`

2、安装 libpcap、libpcap-devel: `yum install libpcap libpcap-devel -y;`

3、安装 libdnet: `wget https://nchc.dl.sourceforge.net/project/libdnet/libdnet/libdnet-1.11/libdnet-1.11.tar.gz` (获取压缩包)

```
tar -zxvf libdnet-1.11.tar.gz (解压)
cd libdnet-1.11
./configure && make && make install
```

(2) 安装 daq

安装命令: 1、`wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz`

```
tar -zxvf daq-2.0.6.tar.gz
cd daq-2.0.6
./configure && make && make install
```

(3) 安装 snort

安装命令：1、`wget https://www.snort.org/downloads/snort/snort-2.9.12.tar.gz`

`tar -zxf snort-2.9.12.tar.gz`

`cd snort-2.9.12`

`./configure --enable-sourcefire && make && make install`

完成 (1) (2) (3) 步骤后的截图如下：包括了对应的压缩包和解压后的目录

```
[root@CentOS hacker]# ls
LuaJIT-2.0.5          daq-2.0.6          heap.c              log
LuaJIT-2.0.5.tar.gz  daq-2.0.6.tar.gz  libdnet-1.11       snort-2.9.12
community-rules.tar.gz heap               libdnet-1.11.tar.gz snort-2.9.12.tar.gz
```

此时使用 `snort -V` 查看 snort 是否安装成功，结果如下图：可见安装成功

```
[root@CentOS hacker]# snort -V
***
o"  ~-  Version 2.9.12 GRE (Build 325)
****
By Martin Koesch & The Snort team: http://www.snort.org/contact#team
Copyright (C) 2014-2018 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.5.3
Using PCRE version: 8.32 2012-11-30
Using ZLIB version: 1.2.7
```

(4) 安装 snort 规则

安装命令：1、创建 snort 配置及规则目录：`mkdir -p /etc/snort/rules`

2、创建运行目录：`mkdir /usr/local/lib/snort_dynamicrules`

3、将 (3) 中解压出的 etc 下的默认配置文件拷贝到 snort 配置目录下：`cp etc/*.conf* /etc/snort`；`cp etc/*.map /etc/snort`

4、下载社区规则并解压到规则目录：`wget https://www.snort.org/downloads/community/community-rules.tar.gz`；`tar -zxf community-rules.tar.gz -C /etc/snort/rules`

5、注释掉所有默认加载的规则文件：`sudo sed -i 's/include $RULE_PATH/#include $RULE_PATH/' /etc/snort/snort.conf`

6、启用社区规则文件：`echo ">> /etc/snort/snort.conf`

`echo '# enable community rule' >> /etc/snort/snort.conf`

`echo 'include $RULE_PATH/community-rules/community.rules' >> /etc/snort/snort.conf`

7、重设 snort.conf 中的变量值：`sed -i 's/var RULE_PATH ../rules/var RULE_PATH ../rules/' /etc/snort/snort.conf`

`sed -i 's/var WHITE_LIST_PATH ../rules/var WHITE_LIST_PATH ../rules/' /etc/snort/snort.conf`

`sed -i 's/var BLACK_LIST_PATH ../rules/var BLACK_LIST_PATH ../rules/' /etc/snort/snort.conf`

8、创建自己设置的规则文件，稍后我们自己写的规则就是写入到这个文件中：`touch /etc/snort/rules/local.rules`

9、测试配置文件的正确性：`snort -T -c /etc/snort/snort.conf`，测试结果如下图：可见成功

```
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.5.3
Using PCRE version: 8.32 2012-11-30
Using ZLIB version: 1.2.7

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.0 <Build 1>
Preprocessor Object: apid Version 1.1 <Build 5>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_MQDBUS Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDP Version 1.1 <Build 1>
Preprocessor Object: SF_DCEPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 5>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>

Snort successfully validated the configuration
Snort exiting
[root@CentOS hacker]#
```

(5) 编写规则:

根据 snort 的规则编写格式编写了针对虚拟机的 ping、http、https 数据包的报警以及 mysql、ssh、telnet、ftp 等常用服务的入侵报警规则，规则文件为/etc/snort/rules/local.rules，因为扫描的主机（windows10）与（CentOS）在同一局域网下，简便起见，规则中的源 IP 地址都设置为任意 IP 地址（any）；规则集如下图：

```
3. hacker@CentOS:/home/hacker (ssh)
alert icmp any any -> 10.211.55.13 any (msg:"ping attack"; sid:1000001)
alert tcp any any -> 10.211.55.13 80 (msg:"web http attack"; sid:1)
alert tcp any any -> 10.211.55.13 any (msg:"sudo access"; content:"root"; nocase; sid:1000002)
alert tcp any any -> 10.211.55.13 3306 (msg:"mysql attack"; sid:1000003)
alert tcp any any -> 10.211.55.13 22 (msg:"ssh attack"; sid:1000004)
alert tcp any any -> 10.211.55.13 21 (msg:"ftp attack"; sid:1000005)
alert tcp any any -> 10.211.55.13 23 (msg:"telnet attack"; sid:1000006)
alert tcp any any -> 10.211.55.13 443 (msg:"web https attack"; sid:1000007)
```

(6) 以 IDS 模式运行 snort:

为便于查看报警信息，先使用命令 mkdir log 创建目录 log 存放报警信息写入的报警文件 alert；再使用命令：snort -d -l ./log -c /etc/snort/snort.conf 运行 snort，-d 表示解析应用层数据包，-l 表示写入报警信息文件到特定目录，-c 表示使用的配置文件。运行截图如下：

```
3. hacker@CentOS:/home/hacker (ssh)
****
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2018 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.5.3
Using PCRE version: 8.32 2012-11-30
Using ZLIB version: 1.2.7

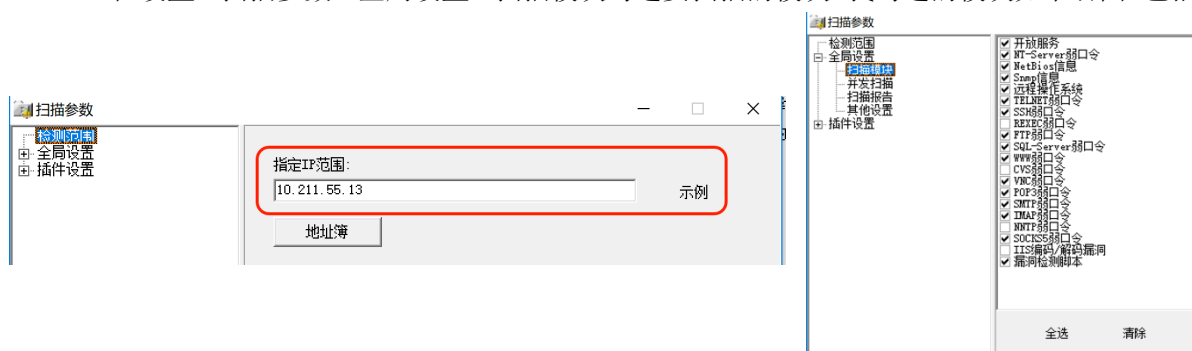
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.0 <Build 1>
Preprocessor Object: apdip Version 1.1 <Build 5>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SOF Version 1.1 <Build 1>
Preprocessor Object: SF_DCEPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Commencing packet processing (pid=2063)
```

(7) 安装 X-scan 扫描软件:

在另一台虚拟机 windows10 上安装 X-scan 扫描软件，下载地址为：<https://x-scan.apponic.com/download/>，下载后解压运行 xscan-gui.exe 即可，运行过程中遇到了缺失 npptools.dll 的报错，于是我在<http://filediag.com/>上下载了缺失的 npptools.dll 文件并将它放在与 xscan-gui.exe 同一路径下，再次运行 xscan-gui.exe 即可成功

(8) 简单设置 X-scan 扫描选项

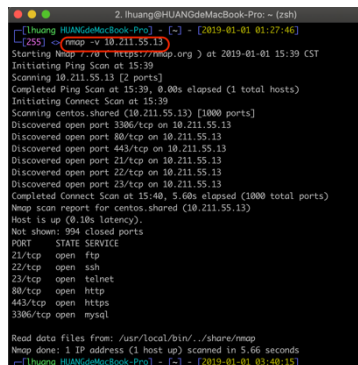
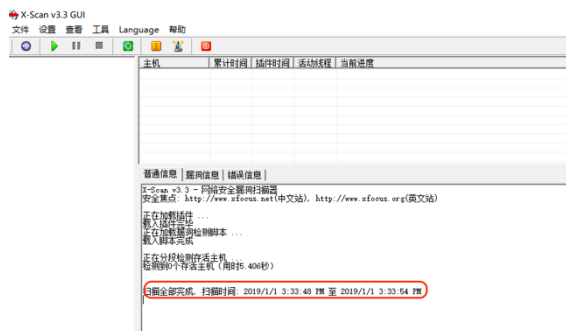
- 1、先在 language 选项中设置语言为简体中文，
- 2、在设置->扫描参数->检测范围->指定 IP 范围中填入 snort 运行的虚拟机 ip 地址（10.211.55.13），如下左图：
- 3、在设置->扫描参数->全局设置->扫描模块勾选要扫描的模块，我勾选的模块如下右图：包括 ssh、



ftp 等之前设置过的 snort 规则选项。

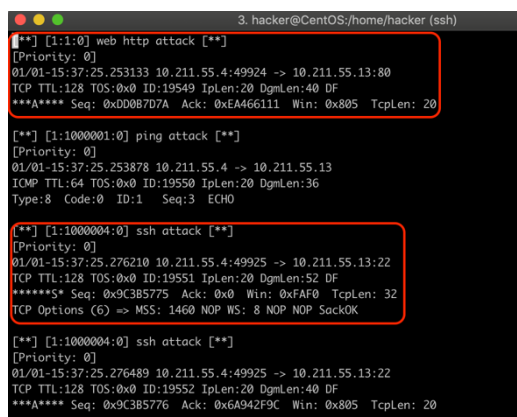
(9)开始扫描:

点击开始按钮开始扫描: 如下左图: 此外我还在主机 (MAC) 上使用 nmap 进行了扫描, 命令为 nmap -v 10.211.55.13, 如下右图: 此外我还进行了 ping 测试。



(10)查看报警文件中的信息:

在 CentOS 上使用 Ctrl-C 结束 snort 的运行, 并使用 vi log/alert 查看报警文件 (该文件已经随本报告一同提交); 下图为节选的一段报警信息: 从图中可以看出, snort 针对 80 端口的 http 数据包、22 端口的 ssh 数据包和 ping 数据包都按照我们之前编写的规则进行了报警。实验成功。



六、实验总结

通过本次实验, 我初步了解了入侵检测软件的工作原理, 也成功在 CentOS 上安装和配置了 snort、编写了简单的入侵检测规则, 并最终使用 X-scan、nmap 等扫描工具对 snort 进行了扫描, 成功得到 snort 的报警信息。本次实验的主要难点在于 snort、X-scan 等软件的安装和配置, 由于是初次使用这些软件, 所以过程中遇到了不少的麻烦, 但我最后都根据参考资料的帮助和 google 解决了这些报错问题。

七、参考资料

- 1、<https://www.cnblogs.com/lstdb/p/8023884.html>
- 2、<https://www.jianshu.com/p/113345bbf2f7>