

**实 验 报 告**

**（ 2021/ 2022 学年 第 1 学期）**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 课程名称 | 网络信息安全 | | | | | |
| 实验名称 | 实验三 入侵检测系统实验 | | | | | |
| 实验时间 | 2021 | 年 | 11 | 月 | 29 | 日 |
| 指导单位 | 计算机学院信息安全系 | | | | | |
| 指导教师 | 吴礼发 | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 学生姓名 | 任远哲 | 班级学号 | 07-B19031614 |
| 学院(系) | 计软网安院 | 专 业 | 信息安全 |

**实 验 报 告**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **实验名称** | | **入侵检测系统实验** | | | | | **指导教师** | | | 吴礼发 |
| **实验类型** | | **验证** | | **实验学时** | | **2** | **实验时间** | | | 2021.11.29 |
| 1. **实验目的和要求**   1. 通过实验掌握轻量级入侵检测系统Snort的安装。  2. 掌握Snort的配置与使用方法，理解基于误用检测的入侵检测系统工作原理。 | | | | | | | | | | |
| 二、**实验环境(实验设备)**  1.安装Windows 操作系统并连接网络的一台PC机。  2.软件：Winpcap, Snort | | | | | | | | | | |
| **三、实验原理及内容**  **实验一．在Windows 环境下安装和使用Snort。要求给出使用的Snort的命令参数。**  **1.使用 snort –W显示网卡接口**  可以看出，我电脑上的无线网卡的编号为5  **2.测试Snort的嗅探器模式**  使用snort -vde在输出包头信息的同时显示包的数据信息，还要显示数据链路层的信息  **3.测试Snort的数据包记录器功能**  如果要把所有的包记录到硬盘上，需要指定一个日志目录，snort就会自动记录数据包：  snort -dev -l ../log  其中./log目录必须存在，否则snort就会报告错误信息并退出。当snort在这种模式 数据链路层、Tcp/IP报头及应用层信息写入当前目录log(log目录已建立)目录下的snort.log.1638321536文件中，而且这是二进制文件。为什么不直接记录成方便阅读的ASCII格式呢？因为系统本生记录的格式就是二进制的，如果再转换成我们能识别的ASCII格式无疑会加重系统负荷，所以Snort在做IDS使用时理应采用二进制格式记录。    **记录的日志文件如下**  **如果想查看二进制日志文件snort.log.1638321536，就得使用“r”参数**  snort –dv -r ../log/snort.log.1638321536    **4.测试Snort作为网络入侵检测系统的功能**  snort –i 5 -dev –c ../etc/snort.conf –l ../log/  其中snort.conf是规则集文件。snort会对每个包和规则集进行匹配，发现这样的包就采取相应的行动。最好不要使用-v选项。因为使用这个选项，使snort向屏幕上输出一些信息，会大大降低snort的处理速度，从而在向显示器输出的过程中丢弃一些包。此外，在绝大多数情况下，也没有必要记录数据链路层的包头，所以-e选项也可以不用  这里-i 5 表示系统里面的第5块网卡，我最开始已经查看过我电脑里无线网卡的编号为5。  snort有6种报警机制：full、fast、socket、syslog、smb(winpopup)和none。其中有4个可以在命令行状态下使用-A选项设置。这4个是：  -A fast：报警信息包括：一个时间戳(timestamp)、报警消息、源/目的IP地址和端口。  -A full：是默认的报警模式。  -A unsock：把报警发送到一个UNIX套接字，需要有一个程序进行监听，这样可以实现实时报警。  -A none：关闭报警机制。    因此，我们使用snort –i 5 -d –c ../etc/snort.conf –l ../log/ -A full    可以看到，网络入侵检测系统已经开启  **实验二：使用另外一台电脑对Snort所在主机发起一次端口扫描攻击，将Snort捕获结果复制到实验报告中。**  **1.实验环境准备**  在物理机Windows10系统上开启Snort网络入侵检测系统，使用虚拟机Kali扫描物理机，观察Snort的捕获结果。  注：虚拟机需要使用桥接模式，以使物理机虚拟机处于同一局域网内。  物理机的IP地址    Kali的IP地址  关闭物理机的防火墙    **2.在物理机中开启网络入侵检测系统**  snort –i 5 -d –c ../etc/snort.conf –l ../log/ -A full  **3.在Kali中使用Nmap扫描物理机端口**  nmap 192.168.43.138  **4.查看alert日志，可以看到udp端口扫描已经被检测到**  **实验三：查看Snort的代码结构**    snort使用一种简单的，轻量级的规则描述语言，这种语言灵活而强大。Snort规则写在.rule文件中。Snort规则分为两个部分：规则的头部和规则选项。  首先，规则头部包含着规则、动作、协议、源地址和目标地址、源端口、目标端口。第二部分是规则选项，它包含着一个警告消息和某数据包有关部分的信息（如果要采取某个动作的话，就应当看一些这种信息）。  例如：alert tcp any any -> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg: "mountd access";)  上例中，圆括号之前的部分属于规则的头部，圆括号内部的属于规则选项部分。  基本格式：  动作 协议 源IP地址 源端口 方向 目标地址 目标端口 ( 规则选项)  动作：规则动作描述一个数据包的“谁，在何处，什么”的问题，并指明规则被激发后，在事件中应当做什么。在编写规则时，你可以从下面的关键字中选择：alert –用选择的警告方法生成一个警告，然后记录这个数据包。log -记录这个数据包。pass – 忽略此数据包。  协议：规则的下一部分是协议。一些比较流行的协议包括TCP、UDP、ICMP等，不过Snort支持许多其它的协议，并继续增加新的协议。  源IP地址：紧跟着协议的部分是IP地址。它定义了数据包来自何处。你可以用“any”这个关键字来定义所有的IP地址。你甚至可以编写一个能够匹配除你指定的IP地址之外任何地址的规则。这是通过使用“！”这个否定操作符实现的。  源端口：它说的是数据包来自哪个端口。端口号也可以使用“any”关键字。你还可以通过使用“：”定义一个范围内的端口。例如，1:1000定义了从1到1000范围内的所有端口。  方向操作符：方向操作符“->”用于定义规则所适用的通信方向。换句话说，即指明通信进入或出自你计算机的什么地方。  目标地址：下一部分是目标地址。它定义了数据包要到何方。与源地址类似，你也可以使用“any”关键字或定义一个不会引起规则被激发的地址。  目标端口：紧随目标IP地址的部分是目标端口号，即数据包设法连接的端口号。这儿的选项与源端口相同。  规则选项：圆括号内的所有内容称为规则选项。一个比较常用的关键字是“content”，不过你还可以用其它许多关键字。关键字“content”允许用户设定规则，搜索数据包有效负荷内的特定内容，并激发一个响应。 | | | | | | | | | | |
| **四、实验小结（包括问题和解决方法、心得体会、意见与建议等）**  **问题和解决方法**  问题1：一开始我把Snort安装在D:\Program Files(x86)下，但发现这个软件好像要求安装路径中不能有空格  解决方法：直接安装在C盘  问题2：实验指导中的一些命令路径存在问题  解决方法：./log代表当前目录下的log文件夹，改成../log，即上层目录下的log文件夹  问题3：实验指导中的一些解释存在问题，这个版本的snort日志应该默认是二进制格式的  解决方法：使用snort –dv -r ../log/snort.log.1638321536 可查看二进制文件  **心得体会**  通过这次实验，我掌握轻量级入侵检测系统Snort的安装，以及Snort的配置与使用方法，理解基于误用检测的入侵检测系统工作原理。Snort的这个软件感觉还是比较小众，网络查到的教程基本全是互相复制的，中间也存在很多错误，踩了很多坑，所以还是最好去官网查看英文的使用文档。Snort入侵检测系统适应多种平台，源代码开放，使用免费，受众多用户喜爱，但也有不少缺点，比如界面简陋，安装复杂，各软件插件有时会因版本等问题影响程序运行。Snort从原理上来看还是静态的入侵检测系统，它能力的强弱还是主要取决于rule规则编写者的经验，因此在当下机器学习技术蓬勃发展的今天，显得稍微有些过时。  **意见与建议**  无 | | | | | | | | | | |
| **五、指导教师评语** | | | | | | | | | | |
| **成 绩** |  | | **批阅人** | |  | | | **日 期** |  | |