规则说明

Snort规则是基于IDS入侵检测系统，主要针对流量中数据包内容编写的扫描规则。

Snort已发展成为一个具有多平台、实时流量分析、网络IP数据包记录等特性的强大的网络入侵检测/防御系统，即NIDS/NIPS。当Snort作为NIDS模式运行时，可以分析网络传输的数据包，它发现可疑流量时就会根据事先定义好的规则发出报警。

规则定义

Snort规则被分成两个逻辑部分：规则头和规则选项。

a. 规则头包含规则的动作，协议，源和目标ip地址与网络掩码，以及源和目标端口信息；

b. 规则选项部分包含报警消息内容和要检查的包的具体部分。

规则头部	规则选项

括号之前的部分叫做规则头部，括号中的部分叫做规则选项。

```
alert icmp any any -> any any (msg: "Ping with TTL=100"; ttl:100;)
```

规则头部

动作	协议	地址	端口	方向	地址	端口

在snort中有五种动作：alert、log、pass、activate和dynamic.

1、Alert-使用选择的报警方法生成一个警报，然后记录（log）这个包。

2、Log-记录这个包。

3、Pass-丢弃（忽略）这个包。

4、activate-报警并且激活另一条dynamic规则。

5、dynamic-保持空闲直到被一条activate规则激活，被激活后就作为一条log规则执行。

Snort当前分析可疑包的ip协议有四种：

1、tcp

2、udp

3、icmp

4、ip

地址：（地址部分定义源或目的地址）

a. 关键字"any"可以被用来定义任何地址。地址就是由直接的数字型ip地址和一个cidr块组成的。cidr块指示作

用在规则地址和需要检查的进入的任何包的网络掩码。/24表示c类网络， /16表示b类网络，/32表示一个特定的机器的地址。

b. 否定操作符用"！"表示。

c. 只有两个方向"->" "<>"

规则选项

规则选项构成了 Snort 入侵检测引擎的核心，将易用性与强大功能和灵活性结合在一起。

所有 Snort 规则选项均使用分号 (;) 字符相互分隔。规则选项关键字与其参数之间用冒号 (:) 字符分隔。

有4类规则选项：general/payload/non-payload/post-detection

general: 只提供信息；

payload: 在payload中查找数据，且能相互关联；

non-pyalod: 在非payload中查找；

post-detection: 在规则命中后触发；

gid关键字（生成器 id）用于标识 Snort 的哪一部分在触发特定规则时生成事件。

sid关键字用于唯一标识 Snort 规则。

rev关键字用于唯一标识 Snort 规则的修订版本。

classtype关键字用于将规则分类为检测属于更一般类型的攻击类别的一部分的攻击。

参考链接

参考连接：Snort规则 - 鱼儿叁 - 博客园 (cnblogs.com)

语法手册：Writing Snort Rules (up.pt)

官方手册：http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node1.html（第三章）