Snort调研报告

一、snort的检测范围

1.规则的来源分类

应用检测.规则-该类别包含查找和控制生成网络活动的某些应用程序的流量的规则。此类别将用于控制应用程序行为的各个方面。

黑名单.规则-此类别包含已确定为恶意活动的指标的URI、用户代理、DNS和IP地址规则。这些规则基于来自 Talos 病毒沙盒的活动、恶意 URL 的公开列表和其他数据源。

**浏览器漏洞：**

浏览器-google.规则-此类别包含对Chrome浏览器中存在的漏洞的检测。（这与"浏览器-webkit"类别是分开的，因为Chrome有足够的漏洞可以分解成自己的漏洞，虽然它使用Webkit渲染引擎，但Chrome还有很多其他功能。

浏览器-火狐.规则-此类别包含对Firefox浏览器中存在的漏洞的检测，或具有"壁虎"引擎的产品。（雷鸟电子邮件客户端等）

浏览器-****ie****.规则-此类别包含对IE浏览器浏览器中存在的漏洞的检测

浏览器-webkit-这一类包含对Webkit浏览器引擎（除了Chrome）中存在的漏洞的检测，其中包括苹果的Safari、RIM的移动浏览器、诺基亚、KDE、Webkit本身和Palm。

浏览器-其他-此类别包含对未列出的其他浏览器中的漏洞的检测。

浏览器插件-此类别包含处理浏览器插件的浏览器中的漏洞的检测。（示例：活动-x）

已删除–当规则被弃用或替换时，它将被移动到此类别。规则永远不会完全从规则集中删除，它们被移动到此处。

利用(****exploit****)-这是一个较旧的类别，将很快被弃用。查找软件的通用漏洞。

漏洞利用工具包-此类别包含专门为检测漏洞利用工具包活动而定制的规则。

**文件漏洞：**

文件可执行-此类别包含通过可执行文件（无论平台）发现或交付的漏洞的规则。

文件闪存- 此类别包含通过闪存文件找到或交付的漏洞的规则。无论是压缩还是未压缩。

文件图像-此类别包含图像文件中发现的漏洞规则。无论交付方法、被攻击的软件和图片类型。（示例包括：jpg、png、GIF、bmp等）

文件识别-此类别是通过文件扩展、文件中的内容（文件魔法）或流量中找到的标题来识别文件。此信息通常用于设置流位以用于其他规则。

文件-java - 此类别包含java内存在的漏洞规则（.jar）

文件多媒体-此类别包含多媒体文件中存在的漏洞规则（mp3、电影、wmv）

文件office-此类别包含属于微软office软件套件的文件内存在的漏洞的规则。（Excel, PowerPoint, Word, Visio, Access, Outlook等）

文件-pdf-此类别包含PDF文件中发现的漏洞的规则。无论创建方法、交付方法或哪款软件（例如，Adobe 阅读器和 FoxIt 读卡器）

文件-其他-此类别包含文件中存在的漏洞的规则，这些规则不适合上述其他类别。

**攻击指标检测：**

指标泄露-此类别包含的规则，显然仅用于检测一个积极受损的系统，可能会发生误报。

指标混淆-此类别包含仅用于检测混淆内容的规则。就像编码的JavaScript规则一样。

指示器壳码-此类别包含的规则，只是在流量中查找壳码的简单标识标记。

指示器扫描- 此类别包含的规则，只是在查找网络流量中扫描的迹象。

恶意软件后门-此类别包含用于检测注定要接收后门命令通道的流量的规则。如果打开端口并等待传入命令以获得其控制功能，则此类检测将在这里。一个简单的示例是，在在特定端口上收听，然后执行发送的命令时，会检测 BackOrifice。

恶意软件-cnc-该类别包含已识别僵尸网络流量的已知恶意命令和控制活动。这包括呼叫主页、下载掉落的文件以及数据的过滤。从"大师到僵尸"类型的东西发出的实际命令也将在这里。

恶意软件工具-此类别包含处理可被视为恶意的工具的规则。例如，loic。

恶意软件-其他-此类别包含与恶意软件相关的规则，但不属于其他"恶意软件"类别之一。

**系统漏洞：**

os-linux-该类别包含在基于Linux的OS中查找漏洞的规则。不是用于浏览器或上面的任何其他软件，而只是针对操作系统本身。

os-****solaris****-这一类包含的规则，正在寻找在solaris漏洞。不用于操作系统顶部的任何浏览器或任何其他软件。

Os-Windows-此类别包含基于Windows的操作系统中查找漏洞的规则。不用于操作系统顶部的任何浏览器或任何其他软件。

Os -moblie- 此类别包含基于移动的操作系统中查找漏洞的规则。不用于操作系统顶部的任何浏览器或任何其他软件。

os-其他-此类别包含在未列出的操作系统中查找漏洞的规则。

**Policy:**

政策多媒体-该类别包含检测多媒体政策的潜在违规行为的规则。例如在网络上检测使用 iTunes。这不是针对多媒体文件中发现的漏洞，因为这将在文件多媒体中。

政策社会-这一类包含检测公司网络上使用社交媒体可能违反政策行为的规则。（p2p、聊天等）

政策垃圾邮件-此类别是用于可能表示网络上存在垃圾邮件的规则。

政策-其他-这一类是针对可能违反最终用户的公司政策芽的规则不属于任何其他政策类别第一。

**协议：**

协议 dns - 此类别用于可能表示网络上 dns 协议中存在漏洞的规则。

协议****finger****-此类别用于可能表示手指协议中****finger****协议存在漏洞的规则。

协议-ftp-此类别用于可能表示网络上ftp协议中存在漏洞的规则。

协议-icmp-此类别用于可能表示网络上icmp流量漏洞存在的规则。

协议-imap-此类别用于可能表示网络上的imap协议存在漏洞的规则。

协议-nntp - 此类别用于可能表示网络上的 nntp 协议中存在漏洞的规则。

协议****pop****-此类别是用于可能表示网络上****pop****协议中存在漏洞的规则。

协议-rpc - 此类别用于可能表示网络上 rpc 协议中 rpc 协议中存在的 rpc 协议或漏洞的规则。

协议-****scada****- 此类别用于可能表示网络上的 scada 协议中存在漏洞的规则。

协议****services****-此类别用于可能表示网络上rservices协议中存在漏洞的规则。

协议-snmp - 此类别用于可能表示网络上 snmp 协议中存在 snmp 协议或漏洞的规则。

协议-telnet- 此类别用于可能表示网络上telnet协议中存在漏洞的规则。

协议-tftp - 此类别用于可能表示 tftp 协议存在漏洞的规则。

协议-voip-这一类是用于可能表示网络上的voip协议存在漏洞的规则。

协议-其他- 此类别用于在协议中查找协议或外向的规则，但不属于其他"协议"规则文件之一。

pua-adware-此类别涉及处理广告软件或间谍软件的"pua"或可能不需要的应用程序。

pua-p2p-此类别涉及处理p2p的"pua"或可能不需要的应用程序。

pua工具栏-此类别涉及处理客户端系统上安装的工具栏的"pua"或可能不需要的应用程序。（谷歌工具栏、雅虎工具栏、热吧等）

pua-其他-此类别涉及"pua"或可能不需要的应用程序，这些应用程序不适合上述类别之一。、

**服务器：**

服务器-****apache****-这一类处理对****apache****网络服务器的漏洞或攻击。

服务器-iis-这一类处理对微软 IIS Web 服务器中的漏洞或攻击。

服务器-mssql-这一类处理微软SQL服务器中的漏洞或攻击。

服务器-mysql-这一类处理甲骨文MySQL服务器中的漏洞或攻击。

服务器****oracle****-这一类处理甲骨文的****oracle****数据库服务器中的漏洞或攻击。

服务器-****samba****- 这一类处理对****samba****服务器中的漏洞或攻击。

服务器-Webapp-这一类处理服务器上基于Web的应用程序中的漏洞或攻击。

服务器邮件–此类别包含检测邮件服务器漏洞的规则。

服务器-其他-此类别包含检测上述列表中未详细说明的服务器中的漏洞或攻击的规则。

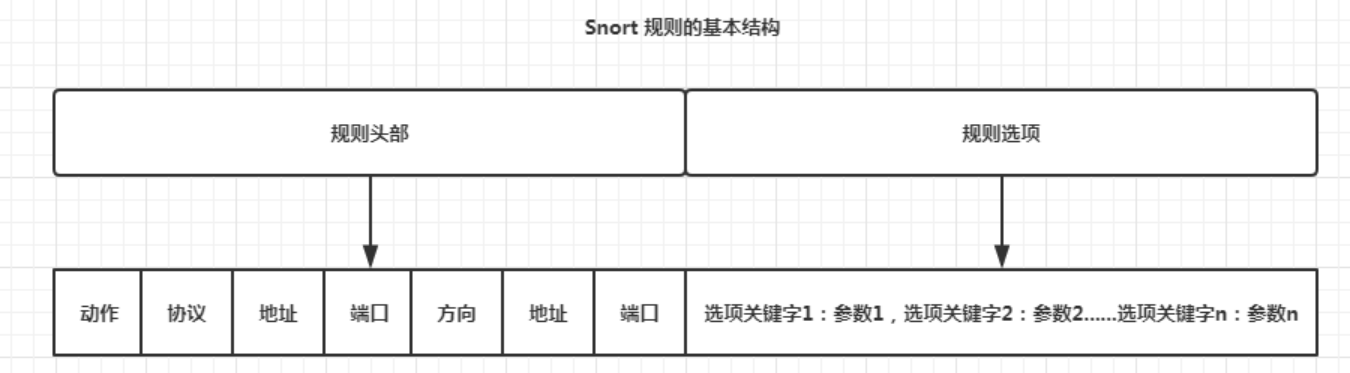
sql - 此类别包含检测sql注入或者是sql相关攻击。

x11 - 此类别包含检测 x11 使用情况或对 x11（如服务器）存在其他漏洞的规则。

2.规则对应的攻击类型

|  |  |  |
| --- | --- | --- |
| 类型 | 描述 | 优先权 |
| attempted-admin | 尝试管理员权限 | 高 |
| attempted-user | 尝试用户权限 | 高 |
| inappropriate-content | 检测到不适当的内容 | 高 |
| policy-violation | 潜在的公司隐私侵犯 | 高 |
| shellcode-detect | 检测到可执行代码 | 高 |
| successful-admin | 成功的管理员权限 | 高 |
| successful-user | 成功的用户权限 | 高 |
| trojan-activity | 检测到网络特洛伊木马程序 | 高 |
| unsuccessful-user | 不成功的用户权限 | 高 |
| web-application-attack | 网络应用攻击 | 高 |
| attempted-dos | 试图拒绝服务 | 中等 |
| attempted-recon | 尝试信息泄露 | 中等 |
| bad-unknown | 潜在的不良流量 | 中等 |
| default-login-attempt | 尝试按默认用户名和密码登录 | 中等 |
| denial-of-service | 检测拒绝服务攻击 | 中等 |
| misc-attack | 误击攻击 | 中等 |
| non-standard-protocol | 检测非标准协议或事件 | 中等 |
| rpc-portmap-decode | RPC 查询的解码 | 中等 |
| successful-dos | 成功的拒绝服务攻击 | 中等 |
| successful-recon-largescale | 大规模信息泄露 | 中等 |
| successful-recon-limited | 信息泄漏 | 中等 |
| suspicious-filename-detect | 检测到可疑文件名 | 中等 |
| suspicious-login | 检测到使用可疑用户名的尝试登录 | 中等 |
| system-call-detect | 检测到系统呼叫 | 中等 |
| unusual-client-port-connection | 客户端正在使用一个不寻常的端口 | 中等 |
| web-application-activity | 访问可能易受攻击的 Web 应用程序 | 中等 |
| icmp-event | 通用ICMP事件 | 低 |
| misc-activity | 混杂活动 | 低 |
| network-scan | 网络扫描检测 | 低 |
| not-suspicious | 不可疑流量 | 低 |
| protocol-command-decode | 通用协议命令解码 | 低 |
| string-detect | 检测到可疑字符串 | 低 |
| unknown | 未知流量 | 低 |
| tcp-connection | 检测到 TCP 连接 | 非常低 |

二、snort规则的编写规范



alert tcp any any -> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg: "mountd access";)

规则头 规则选项

1.规则头

第一个括号前的部分是规则头（rule header），包含的括号内的部分是规则选项（rule options）。规则选项部分中冒号前的单词称为选项关键字（option keywords）。注意，不是所有规则都必须包含规则选项部分，选项部分只是为了使对要收集或报警，或丢弃的包的定义更加严格。规则的头包含了定义一个包的who，where和what信息，以及当满足规则定义的所有属性的包出现时要采取的行动。

1.1规则动作

规则的第一项是"规则动作"（rule action），"规则动作"告诉snort在发现匹配规则的包时要干什么。

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。

1.2 协议、ip地址、端口号

1）协议

规则的下一部分是协议。Snort当前分析可疑包的ip协议有四种：tcp 、udp、icmp和ip。将来可能会更多，例如ARP、IGRP、GRE、OSPF、RIP、IPX等。

2）Ip地址

规则头的下一个部分处理一个给定规则的ip地址和端口号信息。关键字"any"可以被用来定义任何地址。Snort没有提供根据ip地址查询域名的机制。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。例如，

有一个操作符可以应用在ip地址上，它是否定运算符。这个操作符告诉snort匹配除了列出的ip地址以外的所有ip地址。否定操作符用"！"表示。下面这条规则对任何来自本地网络以外的流都进行报警。

alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111 (content: "|00 01 86 a5|"; msg: "external mountd access";)

这个规则的ip地址代表"任何源ip地址不是来自内部网络而目标地址是内部网络的tcp包"。也可以指定ip地址列表，一个ip地址列表由逗号分割的ip地址和CIDR块组成，并且要放在方括号内“[”，“]”。此时，ip列表可以不包含空格在ip地址之间。下面是一个包含ip地址列表的规则的例子。

alert tcp ![192.168.1.0/24,10.1.1.0/24] any -> [192.168.1.0/24,10.1.1.0/24] 111 (content: "|00 01 86 a5|"; msg: "external mountd access";)

3）端口号

端口号可以用几种方法表示，包括"any"端口、静态端口定义、范围、以及通过否定操作符。"any"端口是一个通配符，表示任何端口。静态端口定 义表示一个单个端口号，例如

111表示portmapper，23表示telnet，80表示http等等。端口范围用范围操作符"："表示。范围操作符 可以有数种使用方法，如下所示：

log udp any any -> 192.168.1.0/24 1:1024

记录来自任何端口的，目标端口范围在1到1024的udp流

log tcp any any -> 192.168.1.0/24 :6000

记录来自任何端口，目标端口小于等于6000的tcp流

log tcp any :1024 -> 192.168.1.0/24 500:

记录来自任何小于等于1024的特权端口，目标端口大于等于500的tcp流

4）方向操作符

方向操作符"->"表示规则所施加的流的方向。方向操作符左边的ip地址和端口号被认为是流来自的源主机，方向操作符右边的ip地址和端口信 息是目标主机，还有一个双向操作符

"<>"。它告诉snort把地址/端口号对既作为源，又作为目标来考虑。这对于记录/分析双向对话很方 便，例如telnet或者pop3会话。用来记录一个telnet会话的两侧的流的范例如下：

log !192.168.1.0/24 any <> 192.168.1.0/24 23

2.规则选项

规则选项组成了snort入侵检测引擎的核心，既易用又强大还灵活。所有的snort规则选项用分号"；"隔开。规则选项关键字和它们的参数用冒号"："分开。按照这种写法，snort中有42个规则选项关键字。

2.1 ‎一般规则选项‎

msg - 在报警和包日志中打印一个消息。

reference - 外部攻击参考ids，帮助生成警告信息。

sid - snort规则id。

rev - 规则版本号。

classtype - 规则类别标识。

priority - 规则优先级标识号。

Metedata -元数据关键字允许规则编写者嵌入有关该规则的其他信息，通常以关键值格式。

2.2有效载荷选项

content - 在包的净荷中搜索指定的样式。可以包含混合文本和二进制数据。

alert tcp any any -> any 139 (content:"|5c 00|P|00|I|00|P|00|E|00 5c|";)

alert tcp any any -> any 80 (content:!"GET";)

内容修饰符：

offset - content选项的修饰符，设定开始搜索的位置 。

depth - content选项的修饰符，设定搜索的最大深度。

nocase - 指定对content字符串大小写不敏感。

distence- 在开始搜索下一个之前忽略上一个多远。

uricontent - 在数据包的URI部分搜索一个内容。

http\_client\_body -将搜索限制在 HTTP 客户端请求的主体。

http\_cookie -将搜索限制在 HTTP cookie里。

within -模式1和模式2距离必须小于within 。

pkt\_data -表示适应于原始的TCP/UDP 有效载荷。

byte\_test - 数字模式匹配。

byte\_jump - 数字模式测试和偏移量调整。

2.3非有效载荷选项

ttl - 检查ip头的ttl的值。

tos 检查IP头中TOS字段的值。

id - 检查ip头的分片id值。

ipoption 查看IP选项字段的特定编码。

fragbits 检查IP头的分段位。

dsize - 检查包的净荷尺寸的值 。

flags -检查tcp flags的值。

seq - 检查tcp顺序号的值。

ack - 检查tcp应答（acknowledgement）的值。

window 测试TCP窗口域的特殊值。

itype - 检查icmp type的值。

icode - 检查icmp code的值。

icmp\_id - 检查ICMP ECHO ID的值。

icmp\_seq - 检查ICMP ECHO 顺序号的值。

ip\_proto - IP头的协议字段值。

sameip - 判定源IP和目的IP是否相等.

rpc - 监视特定应用/进程调用的RPC服务。

flow -这个选项要和TCP流重建联合使用。它允许规则只应用到流量流的某个方向上。这将允许规则只应用到客户端或者服务器端

2.4检测后规则选项

logto - 把包记录到用户指定的文件中而不是记录到标准输出。

session - 记录指定会话的应用层信息的内容。

resp - 主动反应（切断连接等）。

react - 响应动作（阻塞web站点）。

tag - 规则的高级记录行为。

Replace-将先前匹配的内容替换为相同长度的给定字符串。仅在内联模式下提供。

detection\_filter-按源或目的地 IP 地址进行跟踪，如果规则与配置速率匹配，则会进行响应。

例子1：

alert tcp any any -> any 3306

(msg:"MySQL Server Geometry Query Integer溢出攻击"; flow:to\_server,established; dsize:<300; flags:A; content:"|03|"; nocase; offset:4; depth:1; content:"select|20|geometryn|28|0x00000000000700000001"; distance:10; within:50; reference:cve,2013-1861; reference:bugtraq,58511; classtype-danger:medium; tid:14999; rev:1;)

msg:"MySQL Server Geometry Query Integer溢出攻击"; //在报警和包日志中打印的消息内容。

flow:to\_server,established; 　　　　　　　　　　　　 //检测向服务器发送方向的报文。

dsize:<300; 　　　　　　　　　　　　　　　　　　　　　　 //应用层负载包长度小于300

flags:A; 　　　　　　　　　　　　　　　　　　　　　　　　//TCP flags值为10

content:"|03|"; nocase; offset:4; depth:1; 　　　　 //负载偏移4取1的值为03,不区分大小写，这块写的应该是有问题字符串有不区分大小写，16进制不涉及。  
 //相对于上面的03特征向后偏移10个字节之后再取50个字节，  
 //50个字节里边包含select|20|geometryn|28|0x00000000000700000001

content:"select|20|geometryn|28|0x00000000000700000001"; distance:10; within:50;

reference:cve,2013-1861; reference:bugtraq,58511; //可参考cve和bugtraq

classtype-danger:medium; 　　　　　　　　　　　　　　 //危险等级中等

sid:20141107; 　　　　　　　　　　　　　　　　　　　　 //规则ID

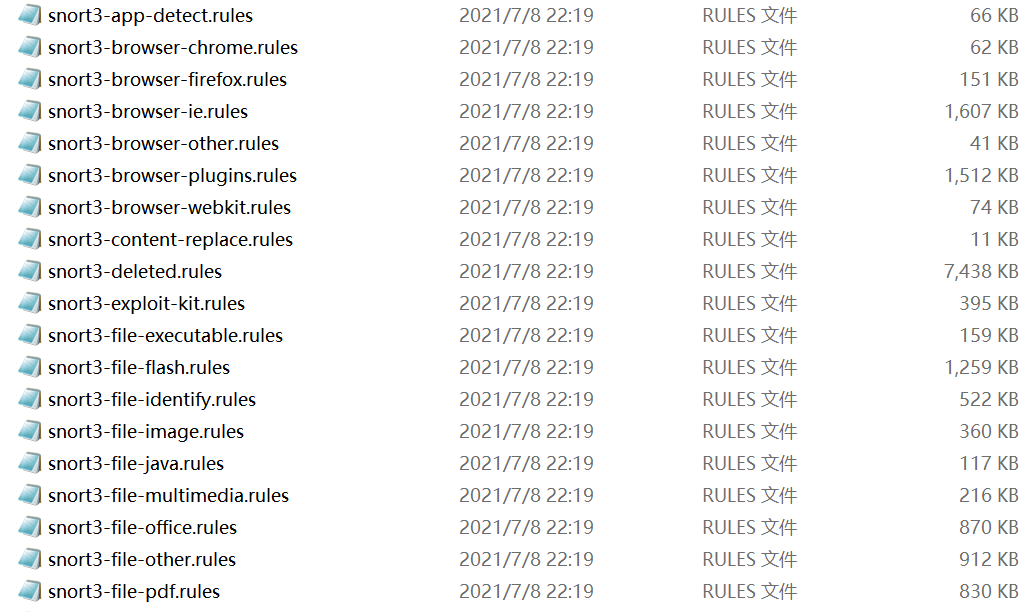
rev:1 　　　　　　　　　　　　　　　　　　　　　　　　//版本信息，第一个版本

三、规则库

官方规则库（未废弃规则20000+，加上已废弃规则30000+）

<https://www.snort.org/downloads>

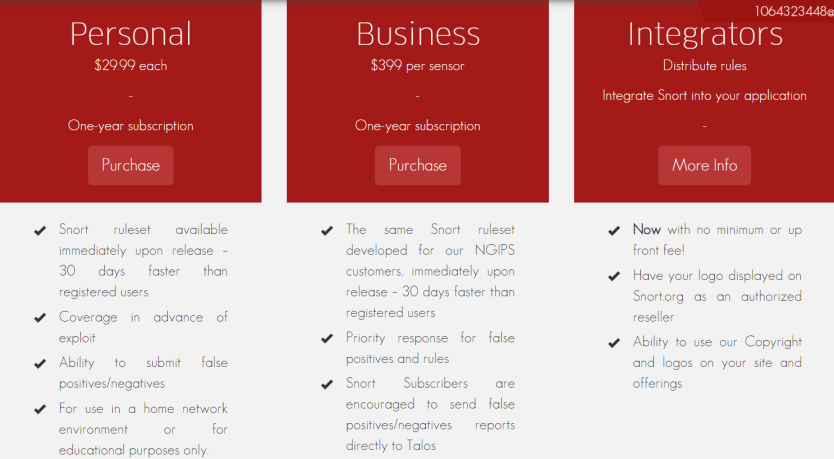
规则按类别排列好



官方还提供了一个黑名单列表

https://snort-org-site.s3.amazonaws.com/production/document\_files/files/000/007/631/original/ip\_filter.blf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20210714%2Fus-east-1%2Fs3%2Faws4\_request&X-Amz-Date=20210714T081121Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=2d201c0f06e7d08059069fbeb3acdf4bf44a69f1aad6624b055ea3979f34a3f8

收费版仅比免费规则提前30天以上提供，收费详情如下：



非官方数据集

1. ET open规则集（包括30000+规则）



收费版规则集

购买途径：

1）Proofpoint客户经理

2）认证合作伙伴

3）授权零售商：OPNSense（税后1191.61美元)

2.github上其他规则集

1）https://github.com/dnlongen/Snort-DNS（通过检查 OpenDNS 的 DNS 响应来检测本地恶意软件、网络钓鱼和成人内容的 Snort 规则）

2）https://github.com/ptresearch/AttackDetection（700+，Suricata 规则）

3）<https://github.com/bhdresh/SnortRules/tree/master/Exploit>

4）<https://github.com/MrAnde7son/Snort/blob/master/local.rules>

5）https://github.com/amonzark/Snort\_DDoS\_NMAPScan\_Rules

6）https://github.com/mbujes/snort-ddos-syn-flood-rule/blob/master/ddos-syn-flood-rule.rules