常见攻击告警分析：

通过安全设配监控，尤其是前两天的信息收集阶段会受到几十万的攻击日志

IPS：时间，源IP，目标ip，事件名称（攻击事件），动作（放行，告警，阻断，丢弃，重置等），报文首行（确定是攻击做排查的时候用），事件返回参数（payload或攻击载荷）

事件返回参数是重点关注对象，是不是误报就是参考这一点

如果从返回参数上没法确定是不是误报，就要结合其他参数，入源ip于目标ip的对应关系，频率等，正常业务应该是多源低频的

SQL注入：

web应用对用户输入的数据合法性没有判断或者判断不严，使得攻击者在web应用程序先定好的SQL语句中插入额外的sql语句

报错函数　floor()函数　　updatexml()函数

延时注入　if()、substr()、ascii() sleep()函数

事件返回参数包含sql语句基本就可以断定是sql注入，乱码的话可以使用一些工具解码，就能看到原来的语句，里面有or，litmit，--等，而且会在很短的时间（1s）执行很多次（几百条），而且IP不太会变化，用wareshark也可以看到很清晰的特征，而正常的sql语句条目，目标都很清晰，而且条件详细，语句规范，同时，执行频率比较低。

有些客户的业务实现机制使用拼接字符的方式，造成存在sql漏洞，这个是需要整改或者加白名单的

（1）所有查询语句都使用数据库提供的参数化查询接口，并且参数化语句使用参数，而不是将用户输入变量嵌入SQL语句中。（2）对进入数据库的特殊字符（'"<>&*;等）进行转义处理，或编码转换。（3）确认每个数据的类型。（4）应严格规定数据长度，以防在一定程度上正确执行较长的SQL注入语句。（5）网站每个数据层的编码是统一的。建议使用UTF-8编码。（6）上下层编码不一致可能会导致某些过滤模型被绕过。（7）严格限制网站用户数据库的操作权限。（8）阻止网站显示SQL错误消息

文件上传漏洞原理：

大部分的网站和应用系统都有上传功能，而程序员在开发任意文件上传功能时，并未考虑文件格式后缀的合法性校验或者是否只在前端通过js进行后缀检验。这时攻击者可以上传一个与网站脚本语言相对应的恶意代码动态脚本，例如(jsp、asp、php、aspx文件后缀)到服务器上，从而访问这些恶意脚本中包含的恶意代码，进行动态解析最终达到执行恶意代码的效果，进一步影响服务器安全。

（1）上传文件的存储目录禁用执行权限。（2）文件的后缀白名单，注意0x00截断攻击。（3）文件上传后修改文件名。（4）不能有本地文件包含漏洞。（5）及时修复web上的代码。升级web server

php代码注入：

在事件返回参数中常会出现：eval，isset，assert，print_r，echo等字符

攻击者一般在数据中植入此类恶意代码，从而生成shell

有时候后台明明是用java编写的，却发现有php的代码发来，一般认为是僵尸网络的扫描器攻击，有些代码是bash64加密的，可以解密后发现真正的样子，同样，一般僵尸网络会对同一个ip做大量的扫描，所以还是利用同源高频原则

xss跨站脚本漏洞

发送恶意的js脚本代码，一般分析xss告警就看事件返回参数有没有js代码，甚至有些会有xss_test字样。

正常的情况，数据虽包含前端代码，但是没有如盗取cookie，弹出框等恶意代码，初步判断是误报，但这也意味着可能存在xss漏洞，可以进一步去判断

strust2命令执行 apache的开源项目

分析此类，需要注意事件返回参数是否有java代码，一般命令执行中包含的命令有：ipconfig，whoami，id，net uer等，一般来说就看返回参数里有没有这些关键字，同样，同源高频也可以作为判断证据。

目录遍历（本地文件包含）

是由于web服务器配置错误，或者web应用程序对用户输入的文件名安全性验证不足导致，是的用户可以使用一些特殊字符（../,返回上一级），绕过服务器安全限制，访问任意文件

事件返回参数中存在多个（../）,并且访问的都是如passwd，shaodow，web.xml等敏感文件，同样，同源高频，时间统一而集中，也是证据之一。

路径扫描（目录扫描）

攻击者在攻击时，一般不知道系统存在那些路径，所以会使用路径扫描工具探测敏感路径，如登陆点（login.jsp），后台，phpinfo.php，svn，mdb等敏感文件

特征是，访问的都是些敏感文件，而且同源高频，时间集中，可判断为使用工具进行扫描攻击，一般阻断了也要封掉

thinkphp5远程代码攻击

非常有特点的payload，一般不想扫描频率那么高，感觉就像在摸奖，测一波，不行就算了的感觉

phpcmsV9 getshell

payload中会添加一个公网的图片，其实是一个木马，需要攻击者自己搭建，可以用情报中心（微步在线这类的）检测一下这个路径，时间上没什么规律，摸奖测试

命令执行漏洞原理：
应用有时需要调用一些执行系统命令的函数，如PHP中的system、exec、shell_exec、passthru、popen、proc_popen等，当用户能控制这些函数的参数时，就可以将恶意系统命令拼接到正常命令中，从而造成命令执行攻击，这就是命令执行漏洞。

命令执行漏洞利用条件：

1. 应用调用执行系统命令的函数
2. 将用户输入作为系统命令的参数拼接到了命令行中
3. 没有对用户输入进行过滤或过滤不严

漏洞分类：

- 代码层过滤不严

商业应用的一些核心代码封装在二进制文件中，在web应用中通过system函数来调用：
system("/bin/program --arg $arg");

- 系统的漏洞造成命令注入

bash破壳漏洞（CVE-2014-6271）

- 调用的第三方组件存在代码执行漏洞

如wordPress中用来处理图片的imageMagick组件
JAVA中的命令执行漏洞（struts2/ElasticsearchGroovy等）
ThinkPHP命令执行

总结以上查找木马程序的方法

第一种、通过生成md5值，查询文件系统的完整性；

第二种、利用find命令查找被入侵当天的所有被修改的文件；

第三种、通过rpm -Va检测生成的文件是否被修改过。

windows日志分析：

系统日志的事件id：

存在大量的登录失败，可能遭受到了爆破

windows日志事件ID：

4624，成功的登录；

4625，失败的尝试；

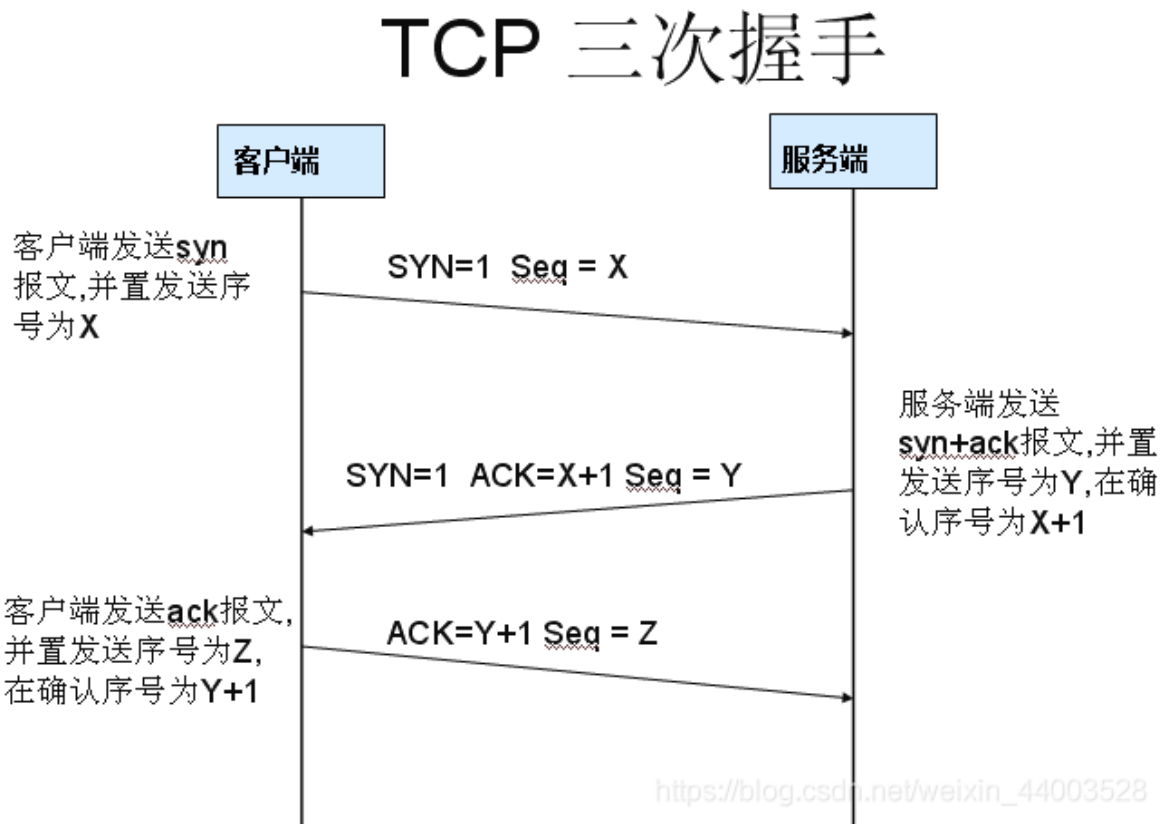
4672，授予特殊权限；

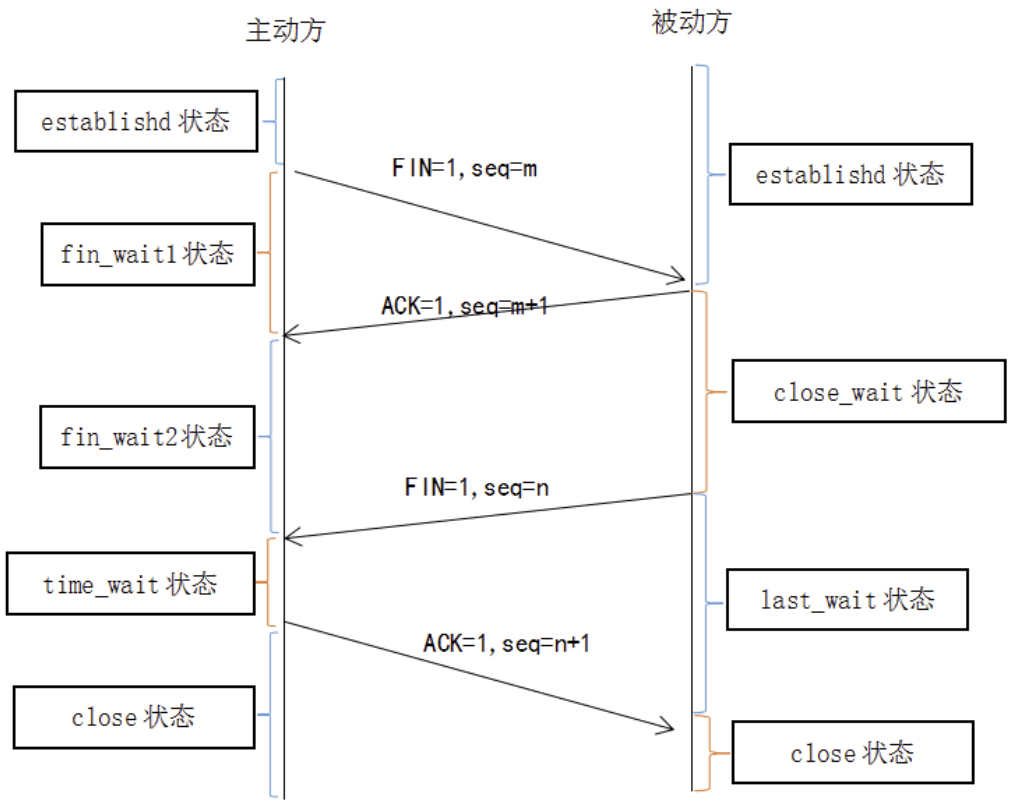
4720，添加用户；

4726，删除用户；

4634，成功的注销；

4672，超级用户登录；





TCP 关闭连接（四次握手）

要封停一个IP，使用下面这条命令：

```
iptables -I INPUT -s ***.***.***.*** -j DROP
```

要解封一个IP，使用下面这条命令：

```
iptables -D INPUT -s ***.***.***.*** -j DROP
```

参数-I是表示Insert（添加），-D表示Delete（删除）。后面跟的是规则，INPUT表示入站，...表示要封停的IP，DROP表示放弃连接。

此外，还可以使用下面的命令来查看当前的IP规则表：

```
iptables -list
```

比如现在要将123.44.55.66这个IP封杀，就输入：

```
iptables -I INPUT -s 123.44.55.66 -j DROP
```

要解封则将-I换成-D即可，前提是iptables已经有这条记录。如果要想清空封掉的IP地址，可以输入：

```
iptables -flush
```

要添加IP段到封停列表中，使用下面的命令：

```
iptables -I INPUT -s 121.0.0.0``/8` `-j DROP
```

其实也就是将单个IP封停的IP部分换成了Linux的IP段表达式。关于IP段表达式网上有很多详细解说的，这里就不提了。

#

IPS入侵防御系统

IPS(Intrusion Prevention System)：入侵防御系统。随着网络攻击技术的不断提高和网络安全漏洞的不断发现，传统防火墙技术加传统IDS的技术，已经无法应对一些安全威胁。在这种情况下，IPS技术应运而生，IPS技术可以深度感知并检测流经的数据流量，对恶意报文进行丢弃以阻断攻击，对滥用报文进行限流以保护网络带宽资源。对于部署在数据转发路径上的IPS，可以根据预先设定的安全策略，对流经的每个报文进行深度检测(协议分析跟踪、特征匹配、流量统计分析、事件关联分析等)，如果一旦发现隐藏于其中的网络攻击，可以根据该攻击的威胁级别立即采取抵御措施，这些措施包括(按照处理力度)向管理中心告警、丢弃该报文、切断此次应用会话、切断此次TCP连接。

IDS入侵检测系统

IDS（intrusion detection system）入侵检测系统是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。它与其他网络安全设备的不同之处便在于，IDS是一种积极主动的安全防护技术。在很多中大型企业，政府机构，都会布有IDS。我们做一个比喻——假如防火墙是一幢大厦的门锁，那么IDS就是这幢大厦里的监视系统。一旦小偷进入了大厦，或内部人员有越界行为，只有实时监视系统才能发现情况并发出警告。

专业上讲IDS就是依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。与防火墙不同的是，IDS入侵检测系统是一个旁路监听设备，没有也不需要跨接在任何链路上，无须网络流量流经它便可以工作。因此，对IDS的部署的唯一要求就是：IDS应当挂接在所有所关注流量都必须流经的链路上。

IDS的接入方式：并行接入(并联)
IDS在交换式网络中的位置一般选择为：尽可能靠近攻击源，尽可能靠近受保护资源

这些位置通常是：

服务器区域的交换机上
边界路由器的相邻交换机上
重点保护网段的局域网交换机上
入侵检测系统的作用
防火墙的重要补充
构建网络安全防御体系重要环节
克服传统防御机制的限制
入侵检测系统功能
监测并分析用户和系统的活动
核查系统配置和漏洞
对操作系统进行日志管理，并识别违反安全策略的用户活动
针对已发现的攻击行为作出适当的反应，如告警、中止进程等

ClamAV实战

Windows登录类型及安全日志解析

Windows下计划任务的使用

Linux查看隐藏进程工具

windows入侵排查思路

常见web 容器比较

Linux下手动查杀木马