IDS逃避技术和对策(2) PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/251/2021_2022_IDS_E9_80_83_E9_81_BF_E6_c101_251028.htm 通过这种方式，每次只投递几个字节的数据，就可能避开字符串匹配入侵检测系统的监视。要监视这种攻击，需要入侵检测系统或者 能够理解、监视网络会话（即使IDS有这种能力，攻击者也可以通过其它的凡是避开监视），或者采用其它的技术监视这种攻击。snort使 用以下规则来监视会话拼接： alert tcp $EXTERNAL_NET any -＞ $HTTP_SERVERS 80 （msg:"WEB-MISC whisker space splice attack"； content:"|20|"； flags:A ； dsize:1； reference:arachnids,296； classtype:attempted-recon； reference）这条规则使snort检测目标为$HTTP_SERVERS 80端口的ACK报文的负载长度是否等于1以及是否包含空格（16进制的20）。使用这条规则可以精确地检测出whisker，但是攻击者只要稍加修改就可以避开这个检测。为了能够检测可能出现的会话拼接攻击，可以对上面这条 snort规则进行扩展，使其检查负载很短的HTTP请求。但是，这样做的副作用是提高了误报警数量，而且在某些情况下攻击者还是能 够避开监视。为了真正有效地检测这种攻击，需要入侵检测系统能够完整地理解网络会话，不过这是非常困难的。应该注意的是目前 大多数系统能够重组会话，在所有的会话数据到达之前，它们会等待一些时间。而等待时间的长短与程序有关。例如，Apache/RedHat 的会话超时时间是6分钟，IIS/Win2K等待的时间非常长。因此，攻击者完全可以每15分钟发送一个字节的会话数据，而IIS还会认为是有效的会话。最新版本的snort

能够监视长期的会话和网络层欺骗，例如：小TTL值。 4.碎片攻击 碎片攻击和会话拼接（session splicing）有点类似。直到最近，很多入侵检测系统在进行字符串匹配之前不能准确地重组碎片。现在这种 情况有了改观，所有的入侵检测系统都能够进行某些重组。不过，还是有很多方法可以避开入侵检测系统的监视。碎片重组的问题是 在进行字符串匹配以前，入侵检测系统必须在内存中缓存所有的碎片，然后进行重组。而且，他还需要直到、碎片在目的主机会如何 重组。Thomas Ptacek and Timoth Newsham于1998年写的Insertion,Evasion and Denial of Service: Eluding Network Intrusion Detection描述了许多基于网络的碎片躲避和其它类型的躲避技术。碎片攻击包括：碎片覆盖、碎片重写、碎片超时和针对网络拓扑的碎片技术（例如使用小的 TTL）等。下面，我们将详细讨论。 4.1.碎片覆盖 所谓碎片覆盖就是发送碎片覆盖先前碎片中的数据。例如： 碎片1 GET x.idd 碎片2 a.?（缓冲区溢出数据） 第二个碎片的第一个字符覆盖第一个碎片最后一个字符，这两个碎片被重组之后就变成了GET x.ida?（缓冲区溢出数据）。实际情况远非这么简单。 4.2.碎片数据覆盖 这种方法和上面的碎片覆盖有些类似，只不过是覆盖全部的碎片数据，例如： 碎片1 GET x.id 碎片2 一些随机的字符 碎片3 a.?（缓冲区溢出数据） 这些碎片在经过目标系统的重组之后，碎片3将完全覆盖碎片2，重组之后的数据变成GET x.ida?（缓冲区溢出数据）。如果入侵检测系统的重组方式和目标系统不同，就无法重组出“ GET x.ida?（缓冲区溢出数据）”，因此就检测不出这个攻击。 4.3.碎片超时 这种攻击依赖于入侵检测系统在丢弃碎片之前会保存多少时

间。大多数系统会在60秒之后将丢弃不完整的碎片流（从收到第一个碎片开 始计时）。如果入侵检测系统保存碎片的时间小于60秒，就会漏掉某些攻击。例如： 碎片1（设置了MF位） GET foo.id 碎片2（59秒之后发出） a?（缓冲区溢出数据） 如果IDS保存起始碎片的时间不到60秒，就会漏过攻击。幸运的是，如果配置没有错误，现在的网络入侵检测系统能够检测此类攻击。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com