IDS逃避技术和对策(1) 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_251030.htm 在网络蓬勃发展的几天，网络安全问题日益突出。网络上的黑、白两道在网络安全的各个领域都展开了激烈的竞争。黑帽社团不断推出躲避或者越过网络入侵检测系统（Network Intrusion Detection System,NIDS）的新技术，而NIDS的开发者不断地在自己的产品中加入对这些技术的检测。但是，由于NIDS本身的局限性，胜利的天平正在向 黑帽子倾斜。本文将讨论一些基本的IDS躲避技术，以及如何识破这些技术。 1.字符串匹配的弱点 针对基本字符串匹配弱点的IDS躲避技术是最早被提出和实现的。一些基于特征码的入侵检测设备几乎完全依赖于字符串匹配算法，而对于一个编写很差的特征码，攻击者可以轻松地破坏对其的字符串匹配。虽然不是所有的入侵检测系统都是纯粹基于特征码检测的，但是绝大多数对字符串匹配算法有很大的依赖。这里，我们将使用开放源码工具snort的特征码来进行讨论。 在UNIX系统中，/etc/passwd是一个重要的文件，它包含用户名、组成员关系和为用户分配的shell等信息。我们就从监视对/etc/passwd文件的访问开始，下面是用于检测的snort检测规则： alert tcp $EXTERNAL_NET any -＞ $HTTP_SERVERS 80 （msg:"WEB-MISC /etc/passwd"； flags: A ； content:"/etc/passwd"； nocase ； classtype:attempted-recon ； sid:1122 ；rev:1） snort使用字符串匹配算法对包含特征码（/etc/passwd）的HTTP请求进行检测。但是，这个规则的特征码过于简单了，攻击者修改攻击字 符串可以很轻松地逃过

检测（我们暂时不考虑攻击请求是通过HTTP发出的）。例如，把攻击请求由GET/etc/passwd改为GET /etc//// passwd，或者GET /etc/rc.d/.././passwd，修改方式简直不计其数。这是最基本的娶亲检测逃避技术，对这种技术的检测也相对容易一些，只要在编写特征码时能够仔细考虑一下攻击可能出现的变体。目前大多数流行入侵检测系统都有非常强大的字符串匹配能力，足以检测此类攻击的大多数变体。不过，仍然有些编写不太好的特征码可以给攻击者以可乘之机。 攻击者还可以在此基础上再加以变化，几乎不费吹灰之力就可以加大入侵检测系统的防御难度。例如在telnet之类的交互会话中，攻击者企图读取/etc/passwd文件。通常，入侵检测系统中存在很多特征码一些误用操作和后门等，但是这些特征码一般只包含黑客工具名、文件名和程序名。在获得/etc/passwd文件的内容时，我们不直接输入cat/etc/passwd等命令行，而是通过一个命令解释器（例如：perl）来实现我们的目的：

badguy@host$ perl -e ‘ $foo=pack（“ C11 ”,47,101,116,99,47,112,97,115,115,119,100）； @bam=`/bin/cat/ $foo`； print ”@bam ”； ’ 从这个命令中，入侵检测系统根本就不会重组出/etc/passwd这些字符。显然，防御这种攻击就很困难了，因为这要求入侵检测系统必须能够理解这种解释器如何收到的命令，这恐怕不太现实。当然，入侵检测系统也可以对使用解释器的可疑行为进行报警，但是它很难对攻击行为进行精确的监视。 通过把字符串处理技术和字符替换技术结合到一起，我们可疑实现更复杂的字符串伪装。对于WEB请求，我们不必使用命令解释器，在我们的请求中使用16进制的URL即可，以下的请求可以被目标WEB服务器解

释为/etc/passwd： GET etc/passwd 或者 GET etc/passwd 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