两种基于HTTP的通用IDS躲避技术 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/64/2021_2022__E4_B8_A4_E7_A7_8D_E5_9F_BA_E4_c40_64822.htm I．介绍 自从Rain Forest Puppy（RFP）的网络扫描器whisker首次公布于众以来［1］，HTTP IDS躲避技术已经逐渐流行。原先许多的HTTP IDS技术，都是从whisker的第一个版本出现的，包括简单的使用多个“ / ”的混淆目录技术，也包括更复杂的 — 在URL里插入“ HTTP/1.0 ”以躲避那些搜索URL地址的IDS算法。 除了whisker中出现的躲避技术，还有其他类型的HTTP混淆方法。其中的一个混淆URL的方法就是使用绝对URI与相对URI［2］。虽然这些方法很有趣，但是都不如whisker扫描中使用的方法常见。 下一个流行的躲避方法也是RFP发布的，利用了微软互联网信息服务器（IIS）的UTF-8 unicode解码漏洞［3］。虽然是IIS的一个严重漏洞，它同时也给出了一个IDS未曾实现的URL编码方法。目前为止，大部分IDS仍然只是关注以前whisker的ASCII编码与目录遍历躲避技术，对Unicode的UTF-8编码却没有相应的保护。Eric Hacker对这种类型的HTTP IDS躲避技术，写了一篇非常专业的文章［4］。本文也会对Hacker文中的一些观点分析并解释。我们将继续Hacker的观点并深入了解：这些编码到底意味着什么，怎样才能造出更奇怪的编码。 本文介绍的其他种类的HTTP IDS躲避技术，使用了HTTP协议的属性。其中之一就是请求管道，以及使用内容编码头并将HTTP请求的参数放置到请求负载中的技术。 II．IDS HTTP协议分析 为了能够识别URL攻击，IDS必须检查HTTP的URL字段，看是否有恶意内容。两种

最流行的IDS检测方法 — 模式匹配和协议分析 — 都需要检测URL中是否含有恶意内容（通过某种形式的模式匹配或者HTTP协议分析）。 两种方法的不同之处取决于你的目的，协议分析法只搜索HTTP流URL字段部分的恶意内容，而模式匹配法的搜索范围是整个数据包。 这两种方法在处理恶意URL之前的行为是类似的。之后，协议分析法只需要对URL字段添加合适的解码算法即可（它已经有内建的HTTP协议解码引擎）。而模式匹配算法并不知道需要对包的哪一部分正常化，因此需要与某种形式的协议分析相结合，找到相应的URL字段，才能使用相应的解码算法。某种形式的HTTP协议分析被添加到模式匹配法中，之后两者又行为类似了。 由于这些IDS方法的类似性，本文讨论的HTTP IDS躲避方法适用于各种类型的IDS。 第一种通用的IDS躲避方法是无效协议解析。举个例子，如果HTTP URL没有被正确发现，那么恶意URL就不能被检查出来，原因是：IDS没有发现URL，就不能对URL进行解码。 如果URL是正确的，IDS必须知道正确的解码算法，否则，仍然不能得到正确的URL。这就是第二种IDS躲避技术 — 无效协议字段解码。 A. 无效协议解析 使用无效协议解析IDS躲避技术，在RFP的whisker［1］和Bob Graham的SideStep［5］中给出了很多例子。这两个程序的区别在于：whisker使用了有缺陷的IDS协议解析来躲避检查，而SideStep使用正常的网络层协议来躲避IDS的协议解码器。 这种情况下，无效协议解析的躲避技术，对于HTTP协议的两个字段URL和URL参数是非常有效的。 例如：如果IDS的HTTP解码器假设每个请求包只有一个URL，那么一个包里包含两个URL，IDS就不能对第二个URL正确解析。这

种技术在请求管道躲避技术中还会提到。 B．无效协议段解码 无效协议段解码可以测试IDS是否能够处理特定协议段的各种类型的解码。 如果是HTTP，主要的目标就是URL字段。对于IDS，需要测试它与HTTP RFC编码标准的符合程度，还要看是否能支持特定Web服务器的编码类型（例如IIS）。如果IDS不能对某种URL编码进行正确解码，攻击者就能利用该编码跳过对恶意URL的检测。 另一个HTTP无效协议段编码，是通过目录混淆，操纵目录属性来实现的。例如：对于/cgi-bin/phf，可以使用多个“ / ”而不是一个“ / ”来改变目录的“ 外貌 ”，或者使用目录遍历来混淆目录路径。需要注意的是，只有当IDS共同查找目录和文件时，目录混淆才能隐藏恶意URL。对于“ /cgi-bin/phf ”来说，如果IDS在“ cgi-bin ”目录中寻找“ phf ”文件时，我们的攻击例子才能奏效；如果IDS只寻找“ phf ”文件，目录混淆方法就不管用了。