# 一种Web攻击变形的自动构造方法*

杨望[1,2] 龚俭[1,2] 吴雄[1,2]

[1]东南大学计算机科学与工程系， 南京 210096

[2]江苏省计算机网络技术重点实验室

**摘要：**随着Web应用的迅速发展，Web攻击成为当前网络攻击的一个主要方面。入侵检测系统对Web攻击的检测能力也成为入侵检测系统能力测试中的一个重要方面。当前的测试方法中，主要采用搜集实际的攻击工具来进行入侵检测系统的测试，该方法受搜集能力的限制，相应测试平台复杂，并且测试中攻击的速度也无法满足目前网络带宽的需要。针对当前Web攻击测试中的不足，以攻击特征为基础构造攻击报文，以分层构造的方式对攻击进行变形，设计一种Web攻击变形生成的新的自动构造方法，该方法经试验证明是有效和完备的。

**关键字：**Web攻击, 网络攻击 攻击变形 IDS测试

# A Method of Web Attack Mutation Auto Construction

Yang Wang[1,2] Gong Jian[1,2] Xiong Wu[1,2]

[1]Department of Computer Science, Southeast Univ, Nanjing 210096

[2]Jiangsu Province Key Laboratory of Computer Networking Technology

**Abstract：** Along with the rapid development of web application, web attacks become an important part of network attacks. The ability of detecting web attacks also becomes an important part for Intrusion detection systems. Most of the IDS testing gather real attack tools to test the ability of intrusion detection systems. This method is limited, the test-bed is complicated, and the traffic volume can't meet the request of the network bandwidth today. The new method uses attack pattern to construct attack packet, and use multi-layer method to construct the mutant of raw attack. The experiments prove that the method is effective.

---

*本文受国家自然科学基金课题（90104031）、国家973计划课题（2003CB314803）和江苏省网络与信息安全重点实验室（BM2003201）资助。作者简介：杨望(1979-)，男，博士生，研究方向为入侵检测系统的测试与评估，EMAIL：wyang@njnet.edu.cn；龚俭(1957-)，教授，博士生导师，研究方向包括网络安全，网络行为学。

**Keyword:** Web attack, network attack, attack mutant, IDS test

# 1 引言

随着 Web 应用的迅速发展，Web 攻击成为当前网络攻击的一个主要方面。当前的入侵检测系统都有大量的 Web 攻击的检测规则，例如使用最广泛的开源入侵检测系统 SNORT[1]，在 2.2.0 版的规则中对应的 Web 攻击共有 8 类 1068 条。另一方面，为了躲避入侵检测系统的检测，各种攻击变形手段也不断被黑客开发出来，使传统的单报文检测手段失效，躲避入侵检测系统的检测。为了测试入侵检测系统对 Web 攻击及其变形的检测能力，必须首先能够构造 Web 攻击及其变形。目前已有的攻击构造手段，大多数采用应用程序模拟攻击，这种方法在扩展性和效率方面都有很大的不足。以攻击特征为基础构造攻击报文，以分层构造的方式对攻击进行变形，实现一种新的自动构造方法。通过对原型的实验，对这种方法的有有效性进行了证明。

本文的组织如下,第二节列举了目前已有的攻击和变体生成的工作；第三节分析了介绍了变形技术的基本原理，分析已有方法的缺点，并提出了新的方法及其实现；第四节是实验与分析；第五节是总结与未来的工作。

# 2 相关工作

MIT 的林肯实验室在 98/99 两年举行了两次大规模的离线 IDS 评估[2][3]，并公布了详细的测试方案与测试数据。在 99 年的实验中，一共设计了 58 种攻击，其中 Web 攻击包括 Apache2、PHF 和 HTTPTUNNEL 等，对于 Web 攻击使用变形手段包括 3 类，分别是将攻击特征分布到多个会话报文、对 URL 进行 UNICODE 编码和替换缓冲区溢出攻击的机器码。林肯实验室采用的攻击设计方法是为每一种攻击设计一个运行脚本，对于攻击的变体，也是专门编写脚本，运行时由系统并发的调用多个脚本来模拟实际的攻击[4]。林肯实验室在攻击变形的实现上并未以一种通用的方法将原始攻击和变形技术分开，也未对原始的攻击和变形技术进行分层。

针对林肯实验室的方法在攻击模拟方面的不足，2002 年苏黎世理工学院的 Marty 在他的毕业论文中，提出了一种新的攻击变形系统框架 THOR。THOR 将原始攻击与变形方法分开，分别在两台主机上分别实现攻击的构造与变形的构造。使得不再需要为每一种攻击单独实现变形技术[6]。THOR 只实现了报文分片一种变形技术。没有进行进一步变形技术复合的研究。

另一方面，除了学校的研究，各类商业实验室也进行了大量的 IDS 测试工作。英国的 NSS Group 实验室从 90 年代末开始发布各类安全产品的测试认证方案，目前最新的入侵检测系统测试方案是第三版的千兆入侵检测系统测试方案。在方案中，攻击共有 15 类 100 余种，HTTP 攻击是 15 个类别的一个；变形方法包括三类，分别是报文分片与流分片、URL 编码和杂项[5]。但 NSS Group 在公开的文档中并未提出攻击和变形的实现手段。

# 3 攻击变形构造

本节首先总结现有变形技术的原理，然后分析了现有攻击变形构造方法的不足，针对这些不足，提出了新的构造方法，最后给出了新方法的原型系统的框架。

## 3.1 变形技术

Secure Network 的 Ptacek 和 Newsham 于 1998 年率先研究了欺骗入侵检测系统的各类攻击变形技术，讨论了入侵检测系统的弱点，并从网络层、传输层和应用层三个层次归纳攻击变形手段。随后，Puppy 于 1999 年利用应用层的 URL 编码方法和传输层的流报文分段方法设计了 web 专用的攻击变形测试库 libwhisker[7]；Song 也于 1999 年应用网络层 IP 报文分片的原理设计了网络攻击通用的变形工具 fragroute[8]。综合 98 年以来的变形技术研究成果，变形攻击的方法可归纳如表 1 所示。

表 1 变体攻击分类表

| | 具体技术 | 影响 | 攻击成功可能性 |
|---|---|---|---|
| 网络层变 | TTL 小于到达目标所需的跳数 | 误检 | 成功率高。 |
| 体攻击 | 报文长度大于 MTU 且报文 DF=1 | | |
| | 设置严格源路由选项， | | |
| | IP 报文分段，将特征隐藏于报文的多个分片中 | 漏检 | 成功率高。 |
| | 利用操作系统 IP 碎片重组策略发送重叠报文 | | 成功率低， |
| 传输层变 | 无效的标志位组合 | 误检 | 成功率高。 |
| 体攻击 | 无效的选项 | | |
| | 传输报文长度超过目标窗口，将被丢弃 | | |
| | 利用操作系统报文重组策略发送重叠报文 | | |
| | 流报文分段，将特征隐藏于流的多个分组中 | 漏检 | 成功率高 |
| 应用层变 | URL 编码攻击 | 漏检 | 成功率中等 |
| 体攻击 | 栈溢出攻击机器码替换 | | |
| | 同义服务原语替换 | | |

## 3.2 现有研究方法的不足

当前已有的入侵检测系统的测试，攻击变形构造方法有两种，一是搜集攻击和变形工具构造真实攻击；二是根据攻击的原理编写系统脚本，通过脚本的解释执行来构造真实攻击。这两种方法都存在着以下的不足，使之在入侵检测系统的测试中存在着极大的局限。

（一） 攻击与软件的收集困难

在美国国家标准局与 MIT 在 2003 年联合发布的报告中表明，收集真实攻击是一件非常困难的事情[10]，从目前已有的测试中可以看出，最多的攻击种类不过 100 种左右，如果除去变形方法改变的攻击，实际攻击种类都不足 100 种。另一方面，每一种攻击都对应一定版本的软件，如果需要真实攻击产生效果，则必须在弱点主机商配置对应版本的软件，而搜集和配置相应版本的软件这是一件更加困难的事情[11]。这两个困难使得即使是进行小规模的测试也无法在短时间内配置好。

（二） 网络发送速率的不足

目前所有的方法，在性能上都很难满足目前高速发展的网络带宽的需求，如 MIT 在 98/99 离线测试基础上开发的实时测试系统 LARIAT 中，一直未能突破 100Mbps 的流量速率的瓶颈。

随着千兆网的不断普及，千兆的入侵检测系统逐渐成为主流。而试图从应用层构造真实攻击的方法，受到主机资源包括 CPU 和内存方面的限制，攻击测试的报文速率无法达到千兆网络下入侵检测系统测试的需求。而专用的高速网络测试设备，如 Smartbits、WebAvalance 等，不但代价高昂，而且无法构造复杂的攻击，也不能应用各类变形技术，无法满足入侵检测系统功能测试的需求。

## 3.3 新的攻击变形的自动构造方法

由于现有系统存在上述不足，新的方法采用从攻击的检测特征直接构造攻击报文文件，然后离线播放的方法。主要方法包括 3 点，从攻击特征构造攻击报文，分层构造变形攻击，离线播放。

（一） 从攻击的检测特征构造攻击报文

虽然攻击工具与应用软件难于搜集和安装，但是攻击的报文特征是易于寻找的。当新的攻击出现，一般 IDS 开发者会对新攻击进行研究，并发布攻击的检测特征定义出新的攻击检测规则，如 SNORT，会不断推出新的规则库。根据规则库的报文特征反向的构造出攻击报文，来测试 IDS 系统，这个方法在已经在一些简单的 IDS 测试软件中使用，如 STICK、SNOT 从 SNORT 的检测特征构造攻击报文测试 SNORT 系统，但这些工具只能构造简单的单报文攻击，无法加入变形手段，无法测试入侵检测系统在单报文上层的检测能力。

（二） 分层构造变形攻击

从 3.1 节中的变形技术的列表中我们可以看到，变形技术在不同的层次有不同的方法。所以我们设计三层的变形功能对原始的攻击报文进行处理，以产生攻击变体。并且可以将不同的变形功能进行组合。产生复合变形的攻击变体。

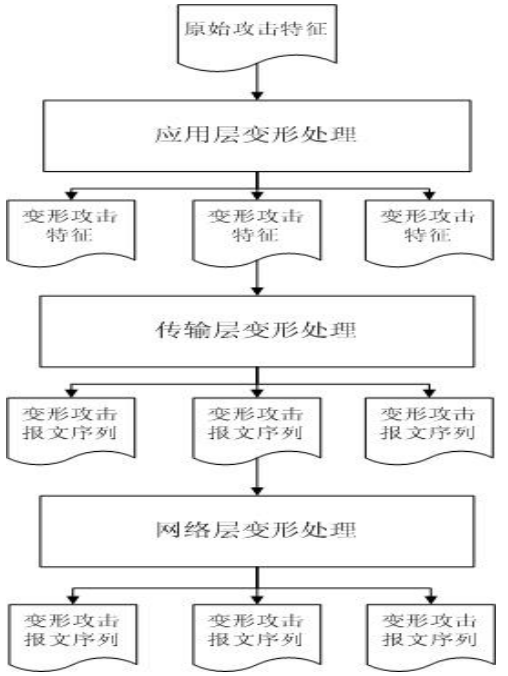

图 1 变形处理层次图

如上图所示，我们将变形处理分为应用层、传输层、网络层。每一层次定义了若干种变形技术。不同层次的变形功能可以复合使用；而在同一层次的变形功能则由处理的内容而定，对于处理报文不同部分的变形功能，彼此间不互斥，可以复合使用；如果处理的是报文的同一部分，则彼此间互斥，不能复合使用。应用层变形处理为原始的攻击特征生成一个或一组新的变形攻击特征，每个变形攻击特征，经过传输层变形处理后，扩展为一个会话的报文序列，该序列再经过网络层的变形处理生成最终的会话序列。

表 2 变形功能

| | |
|---|---|
| 应用层变形功能 | URL 编码、 |
| | SHELLCODE 替换 |
| | 同义原语替换 |
| 传输层变形功能 | 会话流分片 |
| | 会话流乱序 |
| 网络层变形功能 | IP 报文分片 |
| | 分片报文覆盖 |

（三） 离线播放

在线测试的最大问题在于受限系统资源，流量的速率无法突破。采用离线的流量播放，可以不受生成报文的资源限制，不仅可以实现高速的流量播放，而且对于同一攻击报文数据，可以在峰值以内自由的调节播放速率，以测试不同负载下的入侵检测系统的检测能力。

## 3.4 实现框架

攻击变形程序的框架如图。报文的格式我们选择了 libpcap 的报文格式，这是目前最常用的报文格式，可为 tcpdump 和 ethereal 等程序读取分析；攻击特征我们选择了 SNORT 的规则库，因为 SNORT 是目前开源软件内使用最广泛的入侵检测系统。输入的攻击序列传递给变形引擎，变形引擎为序列中的每个攻击生成多个攻击报文序列。由于这些攻击是并发发生的，根据每个序列提供的报文时戳，报文归并模块负责将报文按时间先后顺序排列，生成一个完整的报文序列文件。最后播放引擎按照速度要求来播放报文序列文件。开始我们采用了 tcpreplay 作为播放程序，在实际使用中，我们发现 tcpreplay 的性能在平均报文长度较大时可以达到千兆网络的流量要求，而在短报文长度如 500 字节时则无法达到这个要求。所以我们构造了自己的播放引擎。

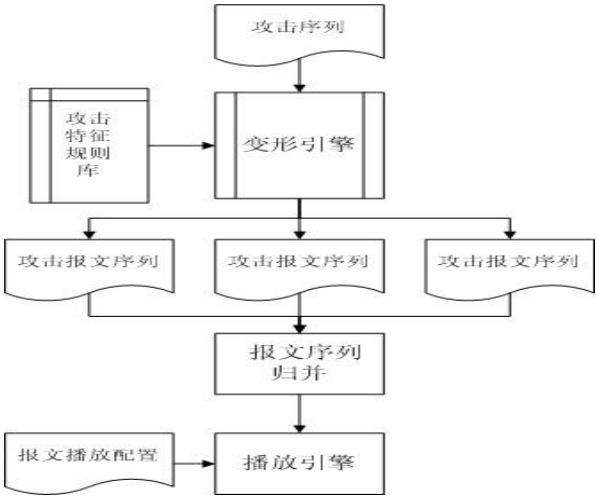


图2 系统框架

# 4 实验与评估

为了测试系统的效果，我们分别作了变形攻击生成的实验与报文播放速率的实验。实验环境为两台主机通过光纤互连，一台主机配置攻击生成程序，并进行离线的播放；另一台主机配置入侵检测系统 SNORT，版本为 2.2.0。两台实验主机均为双 Xeron2.4G 处理器，1G 内存和 Intel Pro1000 千兆光网卡。

我们从 SNORT 的规则库中选取了 10 种 Web 攻击。先用传输层报文分段的方法生成 100 个攻击案例，再采用 URL 编码和报文乱序两种变形手段生成复合变形攻击，编码方案包括 UTF-8 的 6 种编码和%U 的 2 种编码共有 8 种，一共产生 800 个攻击实例。测试分两次进行，第一次不打开 stream4 和 http 的预处理器（分别进行组流和 URL 的解码处理），第二次不打开预处理器。两次 SNORT 仅配置选取得规则，以防止其他规则的警报产生干扰。测试结果如下：

表3 变形功能测试结果

| 系统配置 | 变形方法 | 攻击个数 | 检测结果 |
|---|---|---|---|
| SNORT (未配置预处理器) | 分段 | 100 | 0 |
| | UTF-8 编码+分段 | 600 | 0 |
| | %U 编码+分段 | 200 | 0 |
| | 总计 | 900 | 0 |
| SNORT (配置预处理器) | 分段乱序 | 100 | 100 |
| | UTF-8 编码+分段 | 600 | 600 |
| | %U 编码+分段 | 200 | 200 |
| | 总计 | 900 | 900 |

未配置预处理器的 SNORT 对变形攻击无法识别，配有组流和解码功能以后的 SNORT 能够检测到全部变形攻击，证明攻击生成系统有效的生成了变体攻击。

对于播放速率实验，我们生成了 5 组 100Mbyte 的报文序列文件，平均报文长度分别为

500、750、1000、1250、1500 字节，以最大播放速率进行播放，实验结果如下：

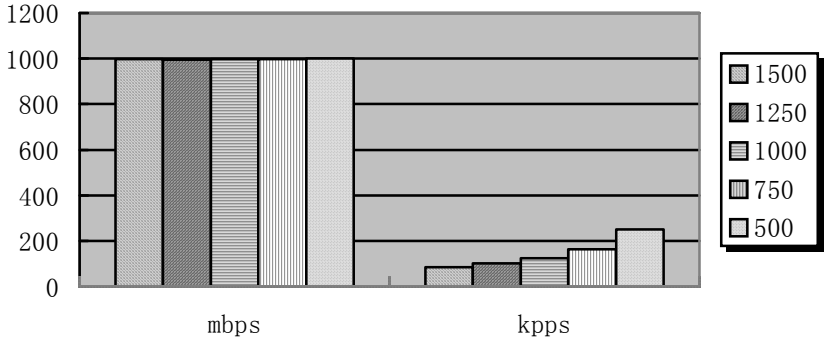


图 3 离线播放性能测试

实验表明，该方法使用本节所定义的商用平台 PC 机就可以满足在千兆网络环境下入侵检测系统测试的需求。

## 5 结论与未来工作

从攻击的检测特征构造攻击报文，采取离线生成播放的方法可以有效的满足测试入侵检测系统的 Web 攻击测试需求。但这种方法受到攻击规则库的限制，目前开源的入侵检测系统大都采用或者翻译 SNORT 的规则，则 SNORT 的规则可以用于测试这些系统，而商用入侵检测系统的规则一般不公开，不了解这些规则，利用 SNORT 规则测试的方法就失去了准确性。下一步的工作我们准备研究如何寻找一个通用的攻击特征的表达方式，作为生成攻击的标准。

## 参考文献

[1] M. Roesch. “Lightweight Intrusion Detection for Networks”, In Proceedings of USENIX LISA’99 Conference, 1999: 229-238

[2] J. Mchugh. “Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory”, ACM Transactions on Information and System Security. 2000, 3(4): 262-294

[3] R. Lippmann, et al. “Analysis and Results of the 1999 DARPA Off-Line Intrusion Detection Evaluation”, In Recent Advance in Intrusion Detection 2000, 2000: 162 - 182

[4] R. Lippmann, et al. “1999 DARPA Off-Line Intrusion Detection Evaluation Design and Procedure”, Technical Report, 2001

[5] NSS Group. “Gigabit Intrusion Detection Systems Group Test (Edition 3)”, http://www.nss.co.uk/gigabitids/edition3/index.htmt, 2005

[6] R. Marty. “THOR A Tool to Test Intrusion Detection Systems by variations of Attacks”, Diploma Thesis, 2002

[7] R. F. Puppy. “A Look At Whisker’s Anti-IDS Tactics”, http://www.hideway.net, 1999

[8] D.Song. “fragroute”, http://www.anzen.com/research/nidsbench, 1999

[9] 汪洋, 龚俭. “入侵检测系统评估方法综述” 计算机工程与应用, 2003, 32:171-173, 2003

[10] P. Mell, et al. “An Overview of Issuses in Testing Intrusion Detection Systems”, NIST Inter Agency Report, 2003

[11] H. Debar, et al. “An Experimentation Workbench for Intrusion Detection Systems”, IBM Zurich GSAL Research Report, 1998

[12] T.H.Ptacek, T.N.Newsham. “Insertion Evasion and Denial of Service: Eluding Network Intrusion Detection”, Secure Networks Technical Report, 1998

<table>
<tr><td>姓名(中文)</td><td>杨　　望</td><td>姓名(英文)</td><td>Yang Wang</td><td>性　别</td><td>男</td><td>出生年月</td><td>1979.3</td></tr>
<tr><td>职称(职务)</td><td>博　士　生</td><td>电　话</td><td>025-83794342-208</td><td>Email</td><td colspan="3">wyang@njnet.edu.cn</td></tr>
<tr><td>手机</td><td>13770636963</td><td>传真</td><td>025-83614842</td><td>通信地址</td><td colspan="3">东南大学计算机系网络中心</td></tr>
<tr><td rowspan="2">研究方向</td><td>中文</td><td colspan="6">入侵检测系统的测试与评估</td></tr>
<tr><td>英文</td><td colspan="6">Test and evaluation of intrusion detection system</td></tr>
<tr><td rowspan="2">基金资助</td><td>中文</td><td colspan="6">国家自然科学基金课题（90104031）、国家973计划课题（2003CB314803）和江苏省网络与信息安全重点实验室（BM2003201）</td></tr>
<tr><td>英文</td><td colspan="6">The China Nature Science Research Program(90104031) The China National Basic Research Program (973 Program) 2003CB314803 and Jiangsu Province Key Laboratory for Information Security (BM2003201)</td></tr>
</table>