高技术通讯 2024 年 第 34 卷 第 11 期:1153-1163

doi:10.3772/j.issn.1002-0470.2024.11.003

一种基于行为特征的网络靶场大规模攻击流量生成方法①

王梦雨②*** 朱树永* 张玉军③***

(*中国科学院计算技术研究所 北京 100190)

(**中国科学院大学 北京 100049)

摘 要 网络靶场是进行网络安全研究和攻防对抗演练的重要基础设施,生成攻击流量是网络靶场复杂行为模拟的主要组成内容。现有的攻击流量生成方法存在攻击类型有限、生成速率低下、流量内容单一等问题,难以满足网络靶场的应用需求。针对上述问题,本文提出了一种基于行为特征的网络靶场大规模攻击流量生成方法,根据攻击的动作序列和关键载荷等行为特征构建攻击模型,通过动态填充数据包模板的方式高速生成内容可变的大规模攻击流量。在此基础上,本文实现了攻击流量生成系统 FATG。实验结果表明,与现有工具相比,FATG 在攻击类型、可扩展性、流量内容灵活性以及生成速率等方面均存在优势,能够有效地模拟漏洞利用、拒绝服务等攻击行为支撑对网络靶场各类靶标设备的安全测试。

关键词 网络靶场;攻击模拟;行为特征;流量生成

近年来,网络攻击事件频发,网络安全形势愈发严峻。为了应对层出不穷的网络威胁,网络靶场的概念被提出并引起了广泛的重视。作为一种进行网络空间安全研究和攻防对抗演练的重要基础设施[1],网络靶场可以通过生成流量的方式模拟各类复杂的用户行为和攻击行为,在安全可控的环境下对靶标设备进行评估分析,从而支撑网络安全防御体系的优化加固与网络新技术的实验验证。

在网络靶场中,生成攻击流量是测试靶标设备的重要手段,能够有效地评估靶标设备对各类网络攻击的防御能力。相较于其他测试流量,网络靶场对攻击流量提出了更高的要求,具体表现在以下 3 个方面。

(1)攻击类型的扩展能力。物联网和网络虚拟化技术的不断进步促使网络靶场进入支撑大规模虚实结合泛在网的发展阶段[2],涉及到的攻击场景更加广泛,面临的网络攻击也更加多样。因此,在网络靶场中生成攻击流量需要具备良好的可扩展性,支持各类攻击手段的扩充升级和针对不同的业务场景进行定制化设计。

(2)攻击流量的生成速率。网络攻击朝着高速化的方向不断发展,以分布式拒绝服务攻击为例,其峰值速率已达到每秒百万兆比特级别[3]。网络靶场的部分测试场景要求对大规模的网络攻击行为进行模拟,需要在有限的软硬件资源下实现攻击流量的高速构造与发送。

(3)流量内容的灵活性。由于单一的攻击载荷很容易被防火墙或入侵检测系统等网络安防设备设置的规则识别过滤,现实世界发生的网络攻击中攻击流量的内容通常是变化的。为模拟真实的攻击效果,网络靶场下生成的攻击流量在内容上需要具备足够的灵活性,支持关键载荷的动态变化,实现对复杂网络攻击行为的模拟。

满足上述要求的关键在于攻击的建模方法和攻

① 国家自然科学基金(62372429,U2333201)和国家重点研发计划(2018YFB1800403)资助项目。

② 男,1995 年生,博士生;研究方向:互联网安全评估,未来网络;E-mail:wangmengyu@ict.ac.cn。

③ 通信作者,E-mail:zhmj@ict.ac.cn。

(收稿日期:2023-12-15)

击数据包的构造方式。现有的攻击模型主要基于检测的目的设计,不适用于攻击行为模拟,并且可扩展性有待提升;而在数据包构造方面,传统内核协议栈的组包过程效率低下,难以匹配网络靶场高速灵活生成攻击流量的应用需求。

针对上述问题,本文提出了一种基于行为特征的网络靶场大规模攻击流量生成方法,并在该方法的基础上实现了攻击流量生成系统 FATG (fast and flexible attack traffic generator),可高速生成动态变化的大规模攻击流量,模拟漏洞利用、拒绝服务等多种攻击行为,有效支撑对网络靶场各类靶标设备的安全测试。该方法首先根据攻击的动作序列和关键载荷等行为特征构建攻击模型,自动获取开源漏洞库攻击信息形成攻击知识库;其次,对数据包的生成流程进行改进,通过动态填充模板的方式高效地构造内容不同的攻击数据包,并基于数据平面开发套件 DPDK 实现其快速发送。

本文的整体结构如下:第 1 节列举了相关的研究工作,第 2 节对所提出的攻击流量生成方法进行阐述,第 3 节介绍了攻击流量生成系统 FATG 的具体实现,第 4 节通过实验验证了 FATG 的攻击流量生成能力以及攻击行为模拟的有效性,第 5 节总结全文并对未来的工作进行展望。

1 相关工作

网络攻击的本质是攻击者和目标主机之间的数据包交互,因此在网络靶场中模拟攻击行为主要通过生成攻击流量的方式实现。现有的攻击流量生成方法主要有以下几种[4]。

基于建模的方法。该类方法应用最为普遍,包括建立攻击模型和解析模型生成攻击流量 2 个部分,代表性的工作有:Sun 等人[5]提出了一种基于攻击图和马尔可夫链对攻击进行建模的方法,可生成用于风险评估的攻击流量。Wang 等人[6]使用可扩展标记语言(extensible markup language,XML)描述攻击模型,通过 Socket 和 Jpcap 编程模拟有状态和无状态的网络攻击流量。朱亚锋和程光[7]设计了一种通过时空特性构建攻击模型的方法,攻击的空间特征来自反向解析入侵检测系统的规则库,时间特征使用泊松模型描述,基于 Libnet 函数库生成攻击流量。Bradatsch 等人[8]在开源安全测试工具 Metasploit[9]的基础上设计实现了高速通用网络测试框架(general purpose network testing framework,GPNTF),通过解析执行 Metasploit 中集成的攻击模块生成攻击流量。Wang 等人[10]以攻防树模型为基础,设计了一种针对工控系统的网络安全风险评估方法。基于建模的方法生成攻击流量不依赖于网络环境条件和原始流量数据,根据攻击的具体原理即可构造相应的攻击数据包,具有较强的适用性。

基于原始流量回放的方法。在该类方法的相关研究中,美国加州大学 Cheng 等人[11]和 Google 共同设计了流量回放系统 Monkey,支持记录客户端和服务器的交互流量并进行回放,可模拟二者之间的攻击行为。Hussain 等人[12]使用流量分析工具 LANDER 对真实的网络流量进行捕获,并在 DeterLab 的实验床中通过开发代理实现了攻击流量的回放。黄宁等人[13]设计了一种基于分布式云平台的交互式流量回放方法,支持模拟复杂虚拟网络中的用户行为进行安全测试。通过回放的方式生成攻击流量能够真实地模拟现实世界已发生的网络攻击,但生成流量的规模和内容都会受到原始流量数据的限制,无法满足网络靶场对海量攻击行为的模拟需求。

基于机器学习的方法。该类方法通过在正常流量中添加扰动生成对抗性的攻击流量[14],根据流量的生成原理分为基于梯度的方法[15]、基于优化的方法[16]、基于生成对抗网络的方法[17-18]、基于决策的方法[19]和基于迁移的方法[20]。该类方法生成的攻击流量主要用于训练机器学习的检测模型,通过对抗性的流量样本提升模型检测效果,适用场景有限且包含的攻击载荷一般无法生效,不适用于网络靶场攻击行为模拟。

组织人员进行渗透测试。近年来,渗透测试被广泛应用于网络安全测试领域[21-22],能够以真实的攻击行为快速发现设备存在的漏洞,是验证其网络攻击防御能力最直接有效的方式。但实施渗透测试的技术门槛较高,目前尚无成熟的自动化操作平台,实践中需要专业技术人员手动进行,应用于网络靶

场存在效率、成本等方面的问题。

综上所述,在网络靶场中基于建模的方法生成攻击流量模拟各类攻击行为具有较强的可行性。但该类方法受到具体建模方式和数据包生成流程的限制,在支持的攻击类型、攻击流量的生成速率和流量内容的灵活性等方面存在不足,无法高效地生成内容动态变化的大规模攻击流量。因此,本文考虑在其基础上设计新的攻击建模方法,并通过改进数据包的生成流程提高流量的生成速率和内容灵活性,从而满足网络靶场攻击行为模拟的应用需求。

2 方法设计

根据网络靶场生成攻击流量的具体要求和对相关工作优缺点的分析,本文设计了一种基于行为特征的网络靶场大规模攻击流量生成方法,包括攻击建模与知识库构建、基于动态填充模板的快速组包流程 2 个部分,可高效地生成内容动态变化的大规模攻击流量。下面分别对这 2 个部分展开介绍。

2.1 攻击建模与知识库构建

建立攻击模型、使用统一的框架描述攻击行为可以提升流量生成方法的泛化性,在相同的执行流程下构造不同类型的攻击流量;同时还有助于攻击的扩充升级和维护管理。现有的攻击树[23]、攻击图[24]、Petri 网[25]、攻击链 IKC(intrusion kill chain)[26]等攻击模型侧重于在攻击路径、漏洞利用关系等宏观角度描述攻击,缺乏生成攻击流量所必需的数据包交互信息,无法直接用于网络靶场攻击行为的模拟。

为重现网络攻击过程中详细的数据包交互,本文基于行为特征对攻击进行建模,记录每一种攻击在实施过程中的动作序列和关键载荷。其中动作序列为按照真实攻击过程发生顺序排列的一系列攻击数据包,关键载荷指数据包中产生攻击效果的关键字段。考虑到网络攻击存在于海量不同类型的应用服务,本文在传输层对攻击的动作序列和关键载荷进行描述,使用二进制或字符串的形式将不同的上层应用数据统一封装在传输控制协议(transmission control protocol,TCP)或用户数据报协议(user datagram protocol,UDP)的数据段以提高可扩展性。除动作序列和关键载荷外,模型中还可以添加攻击类型、攻击原理等基本信息,方便靶场用户更加直观地了解攻击行为、构造攻击测试例。

在具体实现上,使用数据库和 XML 文件 2 种形式的载体存储攻击模型:攻击的基本信息存储于数据库,用于快速检索和更新;攻击的行为特征存储于 XML 文件,借助 XML 语言灵活的数据结构在 CDATA 段详细地描述攻击的动作序列和关键载荷。每一种攻击的模型都对应数据库中的一条记录和一个 XML 文件,通过构建不同的攻击模型形成攻击知识库为攻击流量的生成提供数据支持。在执行攻击流量生成任务时,根据攻击知识库中对应模型存储的攻击行为特征确定需要生成的数据包数量、顺序、流向及内容,然后通过底层的数据包处理框架和发送引擎构造数据包并发送。

攻击知识库的完备性与时效性是影响攻击行为模拟效果的关键因素。为实现网络靶场下对各类业务场景海量攻击行为的模拟,知识库需要支持攻击模型的扩充更新。针对这一需求,本文提出了一种攻击知识库的自动更新方法,通过爬虫自动获取 Exploits-DB[27]等开源漏洞库的攻击信息,转换格式后形成知识库中的攻击模型。其主要流程如算法 1 所示:首先根据子域名的变化规律基于索引批量生成攻击页面网址列表 L(第 2 行);对 L 中的任一网页 l_m,使用 Python 的 BeautifulSoup 库获取页面上所有攻击的原始信息集合 A_m(第 3 ~4 行);对 A_m 中任一攻击原始信息 a_j,根据 HTML 标签和关键字提取攻击的基本属性 i_j 和动作序列 c_j,通过正则表达式匹配数据包中的关键载荷 P_j,然后使用 XML 生成器创建包含动作序列和关键载荷的攻击模型文件 d_j,并将攻击的其他基本信息写入数据库(第 5 ~9 行)。该方法可以快速提取攻击的动作序列和关键载荷,高效地将开源漏洞库中的攻击信息转化为基于行为特征的攻击模型,实现攻击知识库的自动更新。通过该方法本文构建了包含 33 000 余个模型的攻击知识库,能够有效地支撑网络靶场对不同类型攻击行为的模拟。

算法 1 攻击知识库自动更新算法

输入：漏洞库主页网址 H

输出：攻击模型集合 $D = \{d_1, d_2, \cdots, d_n\}$

```
function AttackTransfer(H)
    L = {l_1, l_2, ..., l_m} = Modify_Index(H)
    for each l_m ∈ L
        A_m = {a_1, a_2, ..., a_j} = Get_Attack(l_m)
        for each a_j ∈ A_m
            i_j, c_j = Extract(a_j)
            P_j = {p_1, p_2, ..., p_k} = Analyze(c_j)
            d_j = CreateMod(i_j, c_j, P_j)
            D.append(d_j)
        end for
    end for
    return D
end function
```

2.2 基于动态填充模板的快速组包流程

在基于建模的方法生成攻击流量的相关工作中，通常使用 Libnet、Socket 等函数库构造数据包，由内核协议栈自上而下地进行各层报文首部及数据部分的封装，并借助相关系统调用完成数据包的发送。上述过程中复杂的执行逻辑时间成本较高，而且用户态和内核态的频繁切换引入了额外的处理开销，极大地限制了流量的生成速率；另一方面，数据包的构造主要基于特定规则或脚本，各字段内容预先设定，导致生成的攻击流量缺乏变化，影响了模拟攻击行为的测试效果。

为解决现有方法在流量生成速率和内容灵活性方面存在的问题，本文提出了一种基于动态填充模板的快速组包流程，改进数据包的生成机制和使用高性能的发送引擎提升攻击流量的生成效率，通过动态填充载荷数据实现流量内容的灵活变化，最终达到快速生成动态变化的大规模攻击流量的目的。

2.2.1 数据包快速构造与发送流程

针对攻击流量生成速率的问题，考虑传统内核协议栈组包机制的复杂性，本文对攻击数据包的生成流程进行了改进，不再进行自上而下逐层的报文封装，而是通过创建数据包模板填充关键载荷实现攻击流量的快速生成。改进后的数据包生成流程如图 1 所示，在收到生成攻击流量的指令后，根据攻击知识库中模型包含的动作序列信息确定需要生成的攻击数据包的序列；对序列中的每一个数据包，在开始流量生成任务之前为该数据包创建模板，根据攻击模型中储存的基本信息和关键载荷以及具体的任务配置参数设置数据包相应字段的内容——对协议类型、标志位等内容相对固定的字段直接填入预设值，对关键载荷、源目的 IP、端口号、标识等内容动态变化的字段进行显式标注并分别计算其相对数据包起始位置的偏移量；开始流量生成任务后，创建多个用于组包的工作线程，分别设置亲和性将线程与内核绑定（可减少 CPU 上下文切换的开销），然后将数据包模板分发至各线程，每个线程每次构造一个数据包，根据提前计算的字段偏移量将变化的载荷等数据填入相应字段，形成完整的数据包后调用底层数据包发送引擎的相关接口完成发送。

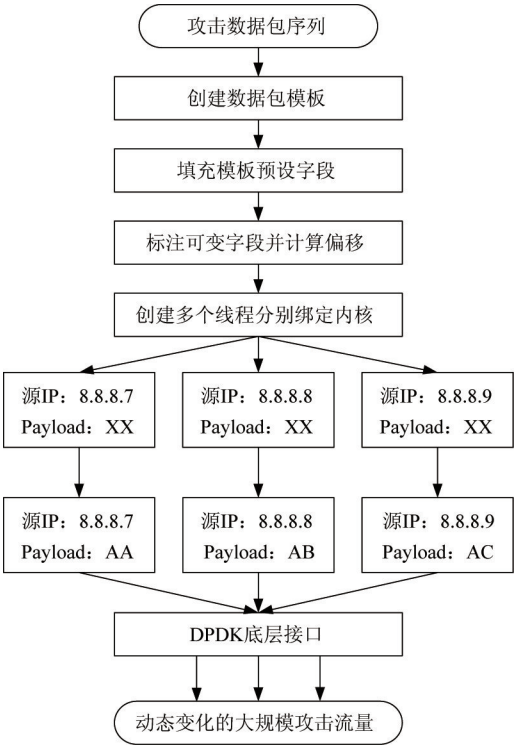


图 1 基于动态填充模板的快速组包流程

上述流程的设计主要考虑了网络靶场攻击行为模拟的流量特性——通常情况下数据包中大部分字段的内容是固定的[28]，少部分字段的内容由于攻击目标的不同和对攻击隐蔽性的考虑而存在差异，应避免对相似的数据包重复调用协议栈进行处理。在

协议格式确定的情况下,待填入不同内容的字段在数据包中的偏移量可以提前计算,工作线程在构造数据包时仅需要将变化的载荷等数据填入相应位置即可,对模板进行局部修改的时间代价远小于协议栈逐层组包的时间代价,因此该流程可大幅提高攻击数据包的构造效率。

各线程完成数据包构造后,需要调用底层数据包发送引擎的相关接口将数据包传输至网卡并发送。为提升攻击流量的发送速率,本文基于数据平面开发套件 DPDK(Data Plane Development Kit)[29]实现高效的数据包发送引擎。DPDK 是一个开源的数据包处理程序开发平台,提供重载的网卡驱动和工作在用户态的数据包处理函数库,具备内核协议栈旁路、零拷贝和直接内存访问等优势,能够实现高性能的报文发送与接收。在基于动态填充模板的快速组包流程中,线程完成数据包构造后将数据包暂存入软件队列,根据预先设定的突发量,采用批处理的方式逐次调用 DPDK 的 rte _ eth _ rx _ burst( )接口将各数据包在软件队列中的地址写入描述符,然后由直接内存访问(direct memory access,DMA)控制器根据地址读取数据包完成其在网卡的发送过程。

2.2.2 基于共享内存动态填充载荷数据

针对攻击流量内容灵活性的问题,本文采用图 2所示的基于共享内存的载荷数据动态填充方法将同一数据包模板扩展为多个包含不同载荷数据的攻击数据包,生成内容动态变化的攻击流量。在开始流量生成任务之前,首先将知识库中储存的关键载荷和其他动态数据读取至一块预先分配的内存区域,该区域由后续创建的工作线程组共享;开始攻击流量生成任务后,各组包线程通过共享指针访问该内存区域,读取数据填入模板中的相应字段。为避免访问冲突,使用互斥锁对共享指针进行管理,同一时刻仅有单个线程可以访问并占有共享指针。线程在每次访存完成后都会向后移动共享指针,使其不断指向新的数据,不同线程先后访存获取到的数据将会存在差异,因此可以构造内容动态变化的攻击流量。

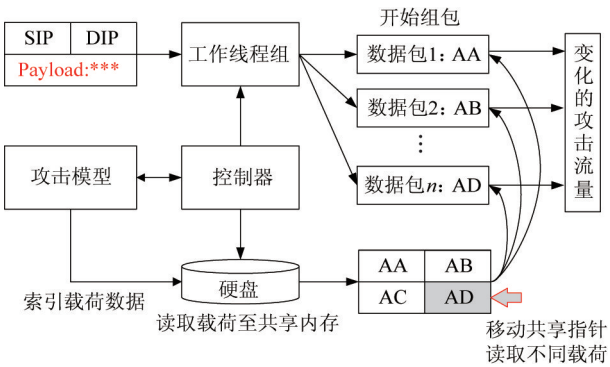


图 2 基于共享内存的载荷数据动态填充方法

考虑网络靶场部分测试场景下要求持续生成攻击流量,测试过程中攻击数据包的总数可能超过知识库模型中载荷数据的总量,本文将存储载荷数据的共享内存区域设计为环形结构,当指针指向该区域的末尾时继续后移将重新指向区域的起始位置,在载荷数据的数量少于待生成攻击数据包的数量时线程依然可以循环地进行数据包的构造。使用共享内存动态填充数据包模板的优势在于可以实现数据索引的快速变化,能够在不产生大量硬盘 I/O 开销的前提下构造内容不同的攻击数据包,在保证攻击流量内容灵活性的同时进一步提高了流量的生成效率。

3 系统设计与实现

在上述方法的基础上,本文设计实现了攻击流量生成系统 FATG,其整体架构包括用户交互层、业务处理层和流量生成层,如图 3 所示。

用户交互层基于 Extjs 框架设计开发,通过 Restful 接口与系统后端的业务处理层进行交互,为靶场用户提供可视化的操作界面,开放编辑测试用例和配置参数以及添加网络攻击的接口。用户可根据网络靶场具体的测试需求在界面上对攻击类型、生成速率以及流量内容进行配置,FATG 将按照用户的配置信息生成相应的攻击流量。用户交互层还支持实时地监控、展示攻击流量生成过程中的各项统计数据,方便靶场用户及时对攻击行为的模拟过程进行干预。

业务处理层包括基于正则表达式的用户指令解析器、基于MySQL数据库和XML文件的配置信息

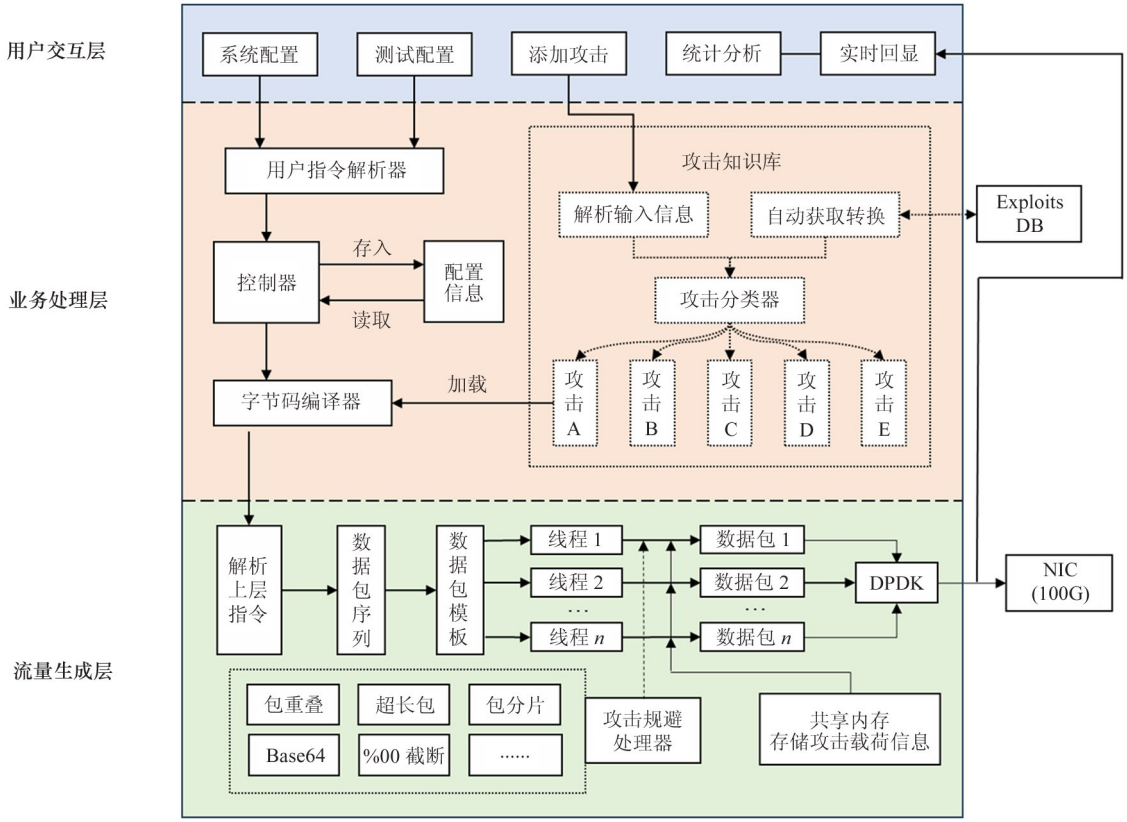


图 3　攻击流量生成系统 FATG 整体架构

及攻击模型存储、基于自定义指令集的控制器和编译器等功能实体，主要作用为接收用户交互层传递至后端的用户请求并解析请求中包含的指令或配置信息，根据指令内容进行配置信息或攻击模型数据的读写、控制流量生成任务的执行与终止以及根据指令执行结果和状态监控数据对用户请求进行反馈。在执行流量生成任务时，业务处理层使用自定义指令集生成包含攻击数据包序列和用户配置的其他流量生成参数的字节码文件，该文件能够被流量生成层高效地解析执行。

流量生成层以 DPDK 动态链接库的形式设计开发，根据第 2 节中提出的基于动态填充模板的快速组包流程，实现基于虚拟机的字节码文件解析及执行、基于多线程并发的快速组包、基于共享内存的载荷数据动态填充等功能。流量生成层与底层网卡驱动使用 DPDK 提供的专用接口进行通信，执行初始化网卡和将数据包从软件队列传输至网卡发送队列等操作。另外，在流量生成层中还实现了攻击规避处理功能，可以根据靶场的测试需求使用数据包级别或字符串级别的规避手段（超长包、包重叠、错误包头、载荷加密、修改扩展名等）处理攻击流量，提高攻击流量的隐蔽性，使攻击行为的模拟效果更加真实。

4　实验评估

4.1　攻击流量生成能力对比

本节将攻击流量生成系统 FATG 与目前网络靶场中常用的攻击流量生成工具进行了对比，参考相关的测量分析研究工作[28,30-32]并结合靶场攻击行为模拟的实际应用需求对评估指标进行设计。表 1 展示了不同工具攻击流量生成功能的对比。在支持的攻击类型方面，FATG 通过自动获取开源漏洞库的攻击信息形成了包含海量模型的攻击知识库，可模拟的攻击类型最多；Metasploit 也在内部集成了大量的攻击模块，支持的攻击类型位居其次。在攻击流量的可扩展性方面，靶场在测试时需要根据实际网络环境对数据包的部分字段进行配置，多数工具能够支持用户自定义各层协议首部部分区域的内容

(如 IP 地址、端口号等),Hping3、Raven-Storm、Trafgen 和 FATG 则具备更好的可扩展性,能够支持用户根据需求灵活调整数据部分的内容。在流量内容的灵活性方面,现有的攻击流量生成工具主要通过随机的方式构造标识、端口号等首部字段动态变化的攻击数据包,FATG 在此基础上还支持通过载荷数据集在给定变化范围内以更加灵活的方式生成多变的攻击流量。

表 1　攻击流量生成工具功能对比

工具名称	支持的攻击类型	可自定义的区域	可变区域	变化方式
LOIC[33]	TCP/UDP/HTTP 泛洪	不支持自定义数据包内容	IP 协议的标识,TCP、UDP 协议的端口号等	随机生成
Hping3[34]	无内置攻击,但可以根据攻击原理构造流量	各层协议首部的部分字段及数据部分	IP 协议的源地址、标识,TCP、UDP 协议的端口号、校验和等	随机生成区间遍历
MHDDoS[35]	内置 56 种攻击流量	不支持自定义数据包内容	IP 协议的标识,TCP、UDP 协议的源端口号、数据部分等	随机生成
Raven-Storm[36]	无内置攻击,但可以根据攻击原理构造流量	各层协议首部的部分字段及数据部分	IP 协议的标识,TCP、UDP 协议的源端口号、数据部分等	随机生成
Metasploit[9]	内置 5 478 个攻击模块,包括漏洞利用、拒绝服务等多种攻击类型	各层协议首部的部分字段及数据部分,不同模块可自定义的区域不同	各层首部的部分字段及数据部分,不同模块的可变区域不同	随机生成
Trafgen[37]	无内置攻击,但可以根据攻击原理构造流量	各层协议首部的部分字段及数据部分	各层协议首部的部分字段及数据部分	随机生成
FATG	内置 33 000 余种攻击流量	各层协议首部的部分字段及数据部分	各层协议首部的部分字段及数据部分	随机生成指定范围

为对比不同工具生成攻击流量的性能表现,本文在表 2 所述的硬件条件下安装部署了上述工具,通过模拟泛洪攻击行为测试各工具攻击流量的生成速率。由于不同工具支持的攻击类型存在差异,以同步序列编号(synchronize sequence numbers,SYN)泛洪攻击模拟和 UDP 泛洪攻击模拟 2 个场景进行实验,另外设置一台服务器作为被测设备接收攻击流量并使用抓包软件 tcpdump 统计流量的生成速率。表 3 列举了各工具攻击流量生成速率的统计结果,可以看到 FATG 在 2 个场景下均表现最优,速率最高可以达到每秒钟生成超过 1 800 万个攻击数据包,验证了其高速构造大规模攻击流量的能力。上述对同类型工具功能及性能的对比说明,FATG 在支持的攻击类型、攻击流量的可扩展性、流量内容的灵活性以及流量的生成速率方面均表现出色,综合各项指标优于现有的其他工具。

表 2　服务器配置

CPU	Intel(R) Core(TM) i7-6700 CPU@3.40 GHz
内存	16 GB
网卡	Mellanox MT27800[ConnectX-5]
操作系统	Ubuntu 16.04

表 3　各工具攻击流量生成速率/千数据包每秒

工具名称	SYN 泛洪攻击流量生成速率	UDP 泛洪攻击流量生成速率
LOIC	/	436.8
Hping3	352.3	380.8
MHDDoS	/	38.0
Raven-Storm	/	133.9
Metasploit	2.9	/
Trafgen	5 280.9	5 956.6
FATG	18 115.6	18 249.4

4.2　攻击行为模拟效果验证

为验证 FATG 能够模拟不同的网络攻击行为,本文搭建了图 4 所示的由 FATG、交换机、域名系统(domain name system,DNS)服务器、模拟用户服务

器组成的局域网实验拓扑,通过两类最具代表性的攻击行为——漏洞利用攻击和拒绝服务攻击测试 FATG 的攻击模拟效果。FATG 向 DNS 服务器发送攻击流量模拟网络攻击,DNS 服务器作为被测设备接收并捕获攻击流量用于后续的统计分析,模拟用户服务器通过与 DNS 服务器正常的请求应答交互监测其域名解析服务的运行情况。

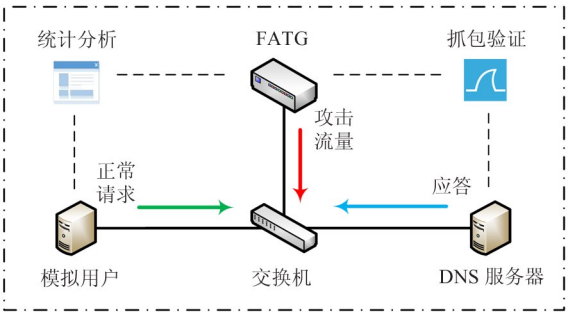


图 4　攻击行为模拟效果验证实验拓扑

4.2.1　漏洞利用攻击模拟

为挖掘网络靶场中靶标设备可能存在的安全漏洞,需要模拟漏洞利用攻击对靶标设备进行测试。本节以 DNS 域传送漏洞为例验证 FATG 对漏洞利用攻击的模拟效果,该漏洞的原理为:当 DNS 服务器配置不当时任意用户均可通过域传送方式获取全部域名记录,导致网络拓扑结构外泄。FATG 能够生成包含不同查询域名的 DNS axfr 请求,探测 DNS 服务器上各个域的全部解析数据,验证其是否存在域传送漏洞。使用 FATG 生成域传送漏洞利用攻击流量发送至 DNS 服务器,在服务器上抓包记录交互过程中的流量数据。对捕获流量的分析结果如图 5 所示,上方线框标识区域为FATG生成的攻击数据包和 DNS 服务器的应答数据包,下方线框标识区域为应答数据包“Answers”部分的具体内容,可以看到在未认证 FATG 身份的情况下 DNS 服务器应答了全部的解析数据,说明其存在域传送漏洞,同时也验证了 FATG 模拟漏洞利用攻击行为的有效性。

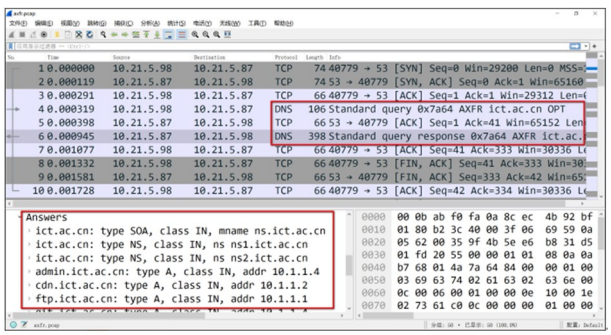


图 5　域传送漏洞利用攻击流量分析结果

4.2.2　拒绝服务攻击模拟

借助僵尸网络控制主机向目标发起拒绝服务攻击是最常见的网络攻击手段之一[38],也是网络靶场中的重要测试内容。为验证 FATG 对拒绝服务攻击行为的模拟效果,本文控制 FATG 生成大规模的 DNS 查询流量,通过耗尽 DNS 服务器的计算及网络资源攻击其域名解析服务。攻击流量在内容上设置为源 IP 地址、DNS 查询标识和 DNS 查询域名 3 个字段动态变化,模拟分布式多源的攻击效果;攻击速率以 100 万数据包每秒为步长从 0 开始不断增长。模拟用户服务器负责监测不同攻击速率下域名解析服务的可用性,每次向 DNS 服务器查询 100 条域名对应的 IP 地址,根据返回结果计算平均解析时延、总超时次数和整体解析成功率。

拒绝服务攻击行为模拟开始后,在 DNS 服务器上捕获攻击流量并分析流量内容。从图 6 中可以看到服务器收到了具有不同源 IP 地址、DNS 查询标识和查询域名(线框标识区域)的攻击数据包,说明 FATG 支持生成内容动态变化的攻击流量,能够真实地模拟拒绝服务攻击行为。

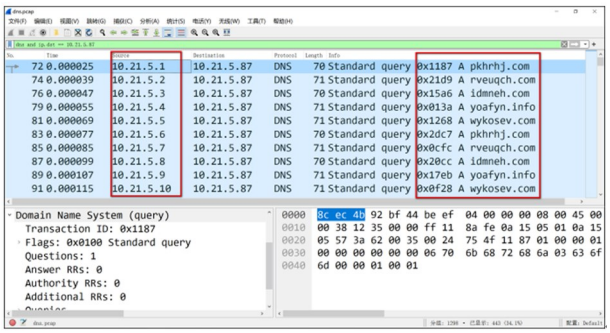
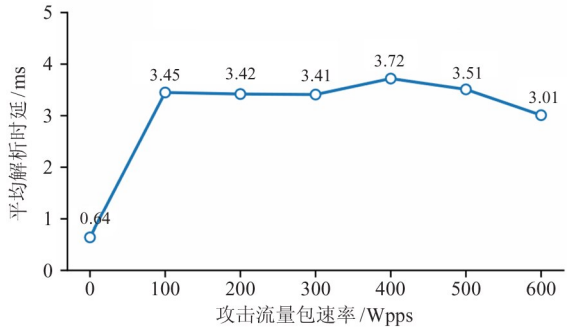


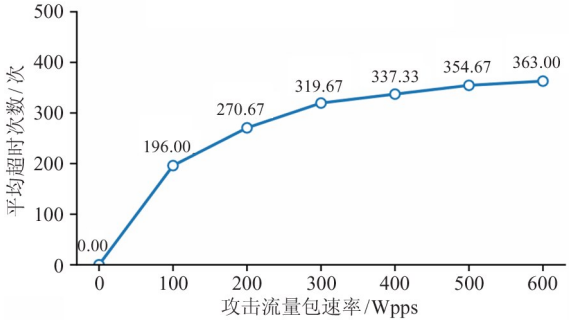
图 6　DNS 查询拒绝服务攻击流量分析结果

模拟用户服务器对域名解析服务的监测结果如图 7 所示,在无攻击流量的状态下(攻击速率为 0),DNS 服务器域名解析服务平均解析时延为 0.64 ms,平均超时次数为 0,平均解析成功率为 100%,说明

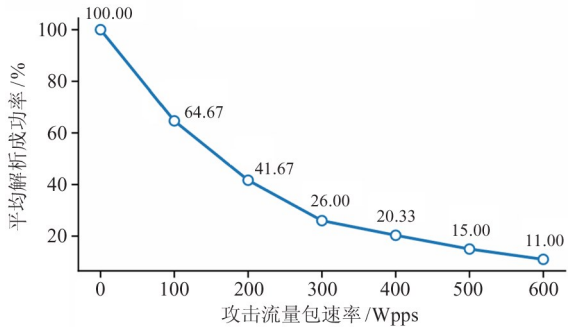
服务正常运行。随着攻击速率不断增大,平均解析时延出现明显增长;平均超时次数也在不断增加并最终接近 400 次(每条查询请求默认允许的超时次数为 3 次,理论上最多出现 400 次超时);平均解析成功率则不断下降,当攻击速率为 600 万数据包每秒时平均解析成功率仅为 11%。以上实验结果证明 FATG 生成的攻击流量对 DNS 服务器的域名解析服务有效地造成了拒绝服务攻击的效果,当攻击速率不断增大时,服务器出现丢包现象并且服务崩溃。



(a) 平均解析时延



(b) 平均超时次数



(c) 平均解析成功率

图 7　不同攻击速率下 DNS 服务器域名解析服务指标变化情况

5　结　论

针对网络靶场攻击行为模拟的具体要求和现有研究工作存在的各项问题,本文提出了一种基于行为特征的网络靶场大规模攻击流量生成方法,通过构建以动作序列和关键载荷等行为特征为主体的攻击模型和动态填充模板的快速组包流程实现了大规模动态变化攻击流量的高效构造与发送。在该方法的基础上,设计实现了攻击流量生成系统 FATG,对比分析了其相对于同类型工具在支持的攻击类型、攻击流量的可扩展性、流量内容的灵活性以及流量生成速率上的优势,并通过实验验证了其对不同类型攻击行为的模拟效果。未来将围绕提高攻击流量的生成速率、自动化部署测试等问题进一步开展研究工作,促进其在网络靶场中的广泛应用。

参考文献

[1] YAMIN M M, KATT B. Use of cyber attack and defense agents in cyber ranges: a case study[J]. Computers and Security, 2022,12:1-20.

[2] 方滨兴, 贾焰, 李爱平,等. 网络空间靶场技术研究[J]. 信息安全学报, 2016(3):1-9.

[3] 腾讯安全, 电信安全, 绿盟安全. 2022 年 DDoS 攻击威胁报告[EB/OL]. [2023-12-15]. https://share.weiyun.com/nmfYRths.

[4] 符永铨, 赵辉, 王晓锋, 等. 网络行为仿真综述[J]. 软件学报, 2021,33(1):274-296.

[5] SUN F, PI J, LV J, et al. Network security risk assessment system based on attack graph and Markov chain [J]. Journal of Physics: Conference Series, 2017,910(1): 012005.

[6] WANG J, DOU W, KAI S. A scalable simulation method for network attack[J]. International Journal of Wireless and Microwave Technologies, 2011,1(3):21-28.

[7] 朱亚锋, 程光. 基于时空特性的恶意流量生成方法的研究与实现[J]. 网络空间安全, 2018(1):7.

[8] BRADATSCH L, LUKASEDER T, KARGL F. A testing framework for high-speed network and security devices [C]//2017 IEEE 42nd Conference on Local Computer Networks (LCN). Singapore: IEEE, 2017:506-509.

[9] Metasploit. The world's most used penetration testing framework [EB/OL]. [2023-12-15]. https://www.metasploit.com/.

[10] WANG S, DING L, SUI H, et al. Cybersecurity risk assessment method of ICS based on attack-defense tree model[J]. Journal of Intelligent and Fuzzy Systems: Applications in Engineering and Technology, 2021(6):40.

[11] CHENG Y C, HÖLZLE U, CARDWELL N, et al. Monkey see, monkey do: a tool for TCP tracing and replaying [C]// Proceedings of the Annual Conference on USENIX Annual Technical Conference. Berkeley, USA: ACM, 2004: 1-7.

[12] HUSSAIN A, PRADKIN Y, HEIDEMANN J. Replay of malicious traffic in network testbeds[C]//2013 IEEE International Conference on Technologies for Homeland Security (HST). Waltham, USA: IEEE, 2013:322-327.

[13] 黄宁, 刘渊, 王晓锋. 基于交互式流量回放的用户行为仿真技术[J]. 计算机工程, 2021,47(10):103-110.

[14] 王珏, 芦斌, 祝跃飞. 对抗性网络流量的生成与应用综述[J]. 计算机科学, 2022,49(S02):11.

[15] RIGAKI M. Adversarial deep learning against intrusion detection classifiers[J]. Intelligent Autonomous Agents for Cyber Defence and Resilience, 2017:1-14.

[16] WANG Z. Deep learning-based intrusion detection with adversaries[J]. IEEE Access, 2018,6:38367-38384.

[17] YAN Q, WANG M, HUANG W, et al. Automatically synthesizing DoS attack traces using generative adversarial networks[J]. International Journal of Machine Learning and Cybernetics, 2019,10(12):3387-3396.

[18] 胡永进,郭渊博,马骏, 等. 基于对抗样本的网络欺骗流量生成方法[J]. 通信学报, 2020, 41(9):59-70.

[19] HASHEMI M J, CUSACK G, KELLER E. Towards evaluation of NIDSS in adversarial setting[C]// Proceedings of the 3rd ACM CoNEXT Workshop on Big Data, Machine Learning and Artificial Intelligence for Data Communication Networks. Orlando, USA: ACM, 2019:14-21.

[20] USAMA M, QAYYUM A, QADIR J, et al. Black-box adversarial machine learning attack on network traffic classification [C] // 2019 15th International Wireless Communications and Mobile Computing Conference (IWCMC). Tangier, Morocco: IEEE, 2019:84-89.

[21] CARTHERN C, WILSON W, RIVERA N. Introduction to network penetration testing[C]// Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA. Berkeley, USA: Apress, 2021:933-950.

[22] BHATIA G, BHATIA O, BHANDARE A, et al. Vulnerability assessment and penetration testing[J]. International Journal of Engineering Research and Technology, 2021(5):395-403.

[23] VIGO R, NIELSON F, NIELSON H R. Automated generation of attack trees[C]//2014 IEEE 27th Computer Security Foundations Symposium (CSF). Vienna, Austria: IEEE, 2014:337-350.

[24] WANG Y J, XIAN M, LIU J, et al. Study of network security evaluation based on attack graph model[J]. Journal on Communications, 2007(756-759):2374-2378.

[25] CHEN T M, SANCHEZ-AARNOUTSE J C, BUFORD J. Petri net modeling of cyber-physical attacks on smart grid [J]. IEEE Transactions on Smart Grid, 2011,2(4): 741-749.

[26] HUTCHINS E M, CLOPPERT M J, AMIN R M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains [M]. Montgomery: Lockheed Martin, 2011.

[27] Exploit Database. [EB/OL]. [2023-12-15]. https://www.exploit-db.com/.

[28] ADELEKE O A, BASTIN N, GURKAN D. Network traffic generation: a survey and methodology[J]. ACM Computing Surveys (CSUR), 2022,55(2):1-23.

[29] Intel DPDK. Data plane development kit project page [EB/OL]. (2016-09-12)[2023-12-15]. http://www.dpdk.org.

[30] MOLNÁR S, MEGYESI P, SZABÓ G. How to validate traffic generators? [C]//2013 IEEE International Conference on Communications Workshops (ICC). Budapest, Hungary: IEEE, 2013:1340-1344.

[31] BEHAL S, KUMAR K. Characterization and comparison of DDoS attack tools and traffic generators: a review[J]. International Journal of Network Security, 2017,19(3): 383-393.

[32] EMMERICH P, GALLENMÜLLER S, ANTICHI G, et al. Mind the gap—a comparison of software packet generators [C]//2017 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS). Bei-

jing, China: IEEE, 2017:191-203.

[33] LOIC. [EB/OL]. [2023-12-15]. https://sourceforge.net/projects/loic/.

[34] Linux. hping3(8)-Linux man page[EB/OL]. [2023-12-15]. https://linux.die.net/man/8/hping3.

[35] Github. MHDDoS: DDoS attack script with 56 methods [EB/OL]. [2023-12-15]. https://github.com/MatrixTM/MHDDoS.

[36] Github. Raven-Storm Toolkit[EB/OL]. [2023-12-15]. https://github.com/Tmpertor/Raven-Storm.

[37] Linux. trafgen(8)-Linux manual page[EB/OL]. [2023-12-15]. https://www.man7.org/linux/man-pages/man8/trafgen.8.html.

[38] BOCK K, ALARAJ A, FAX Y, et al. Weaponizing middleboxes for TCP reflected amplification[C]// USENIX Security Symposium. Vancouver, Canada: USENIX, 2021: 1-17.

A method of generating large-scale attack traffic in Cyber ranges based on behavioral features

WANG Mengyu[*,**], ZHU Shuyong[*], ZHANG Yujun[*,**]

([*]Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190)

([**]University of Chinese Academy of Sciences, Beijing 100049)

Abstract

Cyber range serves as an important infrastructure for conducting network security research as well as offensive and defensive adversarial exercises. Generating attack traffic is the main component of simulating complex behaviors in Cyber ranges. Existing attack traffic generation methods suffer from limitations in terms of attack types, generation rates, and traffic content, making it challenging to meet the requirements of Cyber ranges. To address these problems, this article proposes a method of generating large-scale attack traffic in Cyber ranges based on behavioral features. It constructs attack models with action sequences and key payloads, and efficiently generates large-scale traffic with variable content through the process of dynamically filling packets' templates. On this basis, a fast and flexible attack traffic generator (FATG) is implemented. The experimental results show that FATG has advantages in attack types, scalability, flexibility of traffic content and generation rate compared to existing other attack tools. It can effectively simulate various types of attacks, such as vulnerability exploitation and denial of service, to support security testing of diverse target devices in Cyber ranges.

Key words: Cyber range, attack simulation, behavioral feature, traffic generation