IDS 防逃避攻击测试方法①

李 旋, 李 毅, 陈 妍

(公安部第三研究所 检测中心, 上海 200031)

摘 要: 在对 IDS(Intrusion Detection Systems)产品进行防逃避攻击测试时, 对传统的测试方法进行了改进, 设计了一种简单有效的软件测试方法, 该方法使用 VMware 虚拟机, 将测试软件分别运行于物理机和虚拟机上, 通过设置虚拟机网卡的工作模式搭建测试环境, 简化了测试方法, 节约了测试所需要的物理设备, 且测试结果正确有效. 同时, 与测试仪表 BPS(Breakpointing Systems)对逃避攻击的测试方法相比, 改进的软件测试方法无需昂贵的仪表作为测试基础.

关键词: IDS; 逃避攻击; 测试; BPS

Testing Methods for IDS Anti-Evasion Attack

LI Xuan, LI Yi, CHEN Yan

(Testing Center, the 3rd Research Institute of Ministry of Public Security, Shanghai 200031, China)

Abstract: Based on the test for anti-evade attack of IDS(Intrution Detection Systems), traditional software testing method was improved, and a simple and effective software method was designed. This improved method use VMware virtual maching, test software were running on physical and virtual machine, the network cards of the virtual maching were set in different operation mode to build the test environment, simplifying the testing method, saving the testing equipment and the test result is correct and effective. Meanwhile, compared with the instrumentation BPS(Breakingpoint Systems) expensive instrumentation isn't required.

Key words: IDS; evasion attack; testing; BPS

随着 Internet 的迅猛发展, 针对计算机网络的攻击和破坏事件越来越多, 归纳起来, 主要可以分为两种, 一种是入侵获取, 另一种是入侵破坏. 入侵获取是指通过违反安全策略的非法访问或登录目标(主机或网络)等, 从而获取信息. 入侵获取的方法不胜枚举, 主要包括利用目标漏洞、木马以及病毒等对目标进行入侵渗透. 入侵破坏是指通过某种非授权的方法使目标不再提供服务或使目标设备(软件或硬件)损坏等, 入侵破坏主要包括拒绝服务攻击、蠕虫等方法. 针对愈演愈烈的计算机网络安全问题, 众多信息安全产品应运而生, 如防火墙、IDS、IPS、网闸等等.

基于网络的入侵检测系统(NIDS Network Intrusion Detection Systems)可提供对来自网络内部、外部的攻击和误操作行为等进行实时保护的功能, 能在网络系统受到攻击之前以及攻击正在发生的同时进行检测、报警甚至拦截攻击, 可对入侵进行实时检测, 应用领域广泛. IDS 常用的检测方法分为特征检测和异常检测, 特征检测是对已知的攻击或入侵的方式作出确定性的描述, 形成相应的事件模板, 当检测到的事件与已知的入侵事件模式相匹配时, 即发出报警信息. 异常检测包括事件的统计、初始化的规则库等, 形成统计模型, 以发现入侵行为, 常用的测量参数包括事件的数量、间隔时间、资源消耗情况等[1-5].

针对 IDS 的检测原理, 一些逃避攻击方法被设计和使用, 以期逃避 IDS 的检测, 本文基于传统的 IDS 防逃避测试方法设计了一种改进的防逃避攻击软件测

① 基金项目: "新一代宽带无线移动通信网"科技重大专项(2012ZX03002011)
收稿时间:2014-02-16;收到修改稿时间:2014-03-31

试方法, 用以测试 IDS 防逃避检测功能, 文章还介绍了通过使用仪表(BPS Breakpoint Systems)对入侵攻击进行模拟, 测试 IDS 的防逃避攻击功能.

1 测试工具

逃避攻击是使用新的技术手段及方法躲避或者旁路 IDS 产品检测的网络入侵行为, 逃避攻击方法包括代码变形、数据分片等[6,7].因此要求 IDS 产品具有逃避攻击的检测功能, 本文对该功能进行测试.

1.1 软件工具

逃避攻击的测试工具包括 Blade, Nikto 以及 Fragrouter 等软件, 使用上述三种软件可以较全面的检测 IDS 的防逃避攻击能力, 对此三种软件做简要介绍.

1.1.1 Blade

Blade 软件是一个包重发工具, 允许用户在两块网卡之间或者在单块网卡上产生(广播)预先定义的攻击数据, 在硬件级别模拟电脑系统的操作, 模拟任何一个源 IP 地址和目的 IP 地址, 无需担心随之而来的额外的风险. 攻击操作可以随时重复, 或者根据预先定义操作发生.

Blade 软件包括 4 个主要模块 Blade 控制台、IDS Informer、攻击库和报告浏览. Blade 控制台允许在一个应用中调用多个模块或者程序, 是运行和控制 Blade 软件的载体. IDS Informer 模块实现攻击模拟和相关的参数选择, 该模块可以在两块网卡之间发送单独的、复合的或者多组的工具包, 支持修改协议特征等功能. 攻击库中包含超过 600 种的预先记录的攻击模拟数据, 用以检测各种攻击情况下 IDS 的反应情况. 报告浏览允许用户在报告生成之前控制报告的内容和格式.

1.1.2 Nikto

Nikto 是一款开源的(GPL)网页服务器扫描器, 它可以对网页服务器进行多种扫描, 可以检查 HTTP 和 HTTPS 服务, 同时支持基本的端口扫描以判定网页服务器是否运行在其他开放端口. Nikto 可对远程主机发送大量请求, 可能会损害宿主机、远程主机和网络.

Nikto 具有逃避入侵探测功能, 可使用诸如随机 URL 编码(非 UTF-8 方式)、自选路径(/./)、虚假的请求结束等技术逃避 IDS 的检测.

1.1.3 Fragrouter

Fragrouter 是一个具有路由功能的应用程序, 它能够对攻击者发送的攻击流量进行分片处理之后, 向攻击目标转发, 还可以截取、修改和重写向外发送的报文, 实现多种 IDS 欺骗技术, 包括 IP、TCP 层的数据包碎片以及数据包数据重叠等.

1.2 仪表

Breakingpoint Systems 是一款具有包检测、模拟百万级用户行为等诸多功能的网络安全设备. 该设备可模拟网络层、传输层以及应用层等数据流量, 并可以模拟 TCP、IP 碎片等攻击, 能够支持测试 IDS 的防逃避攻击功能.

2 测试环境及方法设计

2.1 传统测试方法

传统测试方法的网络拓扑图如图 2 所示, 使用 Fragrouter 工具软件测试碎片逃避攻击时, 在 PC1 上使用 Blade 软件模拟子网 1 通过网关(PC2)向子网 2 发送攻击包, 在 PC2 上启用 Fragrouter, 将攻击包分片, 则在子网 2 中的集线器上可广播分片后的攻击包, 若 IDS 能够发现网络攻击且还原的攻击类型与 Blade 所发送的攻击类型一致, 则说明 IDS 具有针对发现分片攻击的功能, 否则无法发现该种攻击类型下的分片攻击手段. 由于 Blade 攻击类型丰富, Fragrouter 具有多种逃避手段, 此处可使用正交试验的方法测试其他逃避攻击[8-12].

使用 Nikto 工具软件针对 Web 网站进行逃避攻击测试时, 在子网 2 中的服务器上搭建 Web 网站(包含动、静态网页和数据库等), 在 PC2 上开启 Nikto, 使用处于子网 2 中的网卡向 Web 网站发送随机 URL 编码逃避攻击, 在子网 2 中的集线器上可广播该攻击包, 若 IDS 能够发现网络攻击且还原的攻击类型与 Nikto 所发送的攻击类型一致, 则说明 IDS 具有检测随机 URL 编码的逃避攻击功能, 否则不具有该功能, 遍历其他 Nikto 具有的逃避攻击.

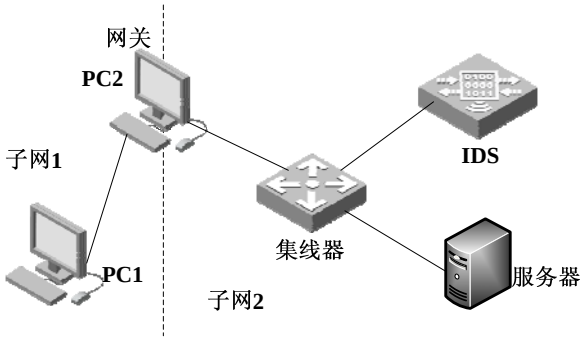

图 1 防逃避攻击传统测试拓扑图

2.2 改进的测试方法

2.1 节中的测试方法中涉及两个子网以及网关的配置, 测试环境搭建复杂, 且不容易维护和重复使用, 使用 VMware 虚拟机可替代图 2 中 PC2 的功能, 并在物理机上搭建 Web 网站, 从而减少了两台物理设备, 同时虚拟机方便管理, 易于重复使用.

2.2.1 环境搭建

改进后的测试环境如图 2 所示, 使用 PC 机及虚拟机模拟各种逃避攻击.

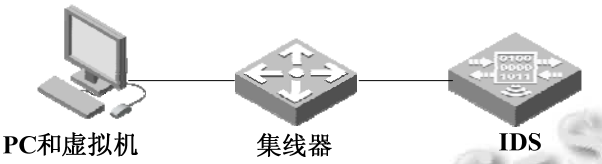

图 2　改进的防逃避攻击测试拓扑图

PC 机的设置如图 3 所示, 在 PC 机上安装 Blade 和 VMware 软件. 使用 VMware 搭建 Linux 虚拟机, 为虚拟机添加两块网卡, 在虚拟机上安装 Fragrouter 和 Nikto 软件, 测试环境搭建完成.

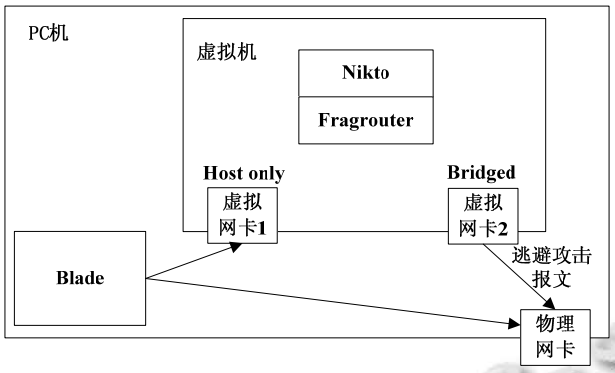

图 3　测试 PC 设置

2.2.2 测试步骤

测试过程与传统测试类似, 此处由于使用了虚拟机替代了双网卡的 PC, 以下对测试步骤进行简要说明.

步骤 1: 配置虚拟机两块网卡的 IP 地址和掩码, 使其处于两个子网, 如: 网卡 1: 192.168.217.145/24, 网卡 2:　192.168.187.145/24;

步骤 2: 将网卡 1 设置为 Host only 模式, 使经过该网卡的数据不被映射至真实网卡, 网卡 2 设置为 Bridged 模式, 与物理机共享网卡;

步骤 3: 在 Blade 的 IDS Informer 模块中, 配置 Source machine 为网卡 1, IP 地址与网卡 1 处于相同子网, GATEWAY 设为网卡 1 的 MAC 地址. 配置 Destination machine 为 PC 的物理网卡, IP 地址与网卡 2(或 PC 网卡)处于相同子网, GATEWAY 设为网卡 2 的 MAC 地址, 如图 4 所示;

步骤 4: 虚拟机打开 Fragrouter 软件, 使用命令 fragrouter –i eth1 –F1, 将到达网卡 1 的数据包进行 8 字节 IP 分片;

步骤 5: PC 机上开启 Wireshake 网络协议分析工具, 查看网卡 1 和网卡 2 之间的网络通信报文;

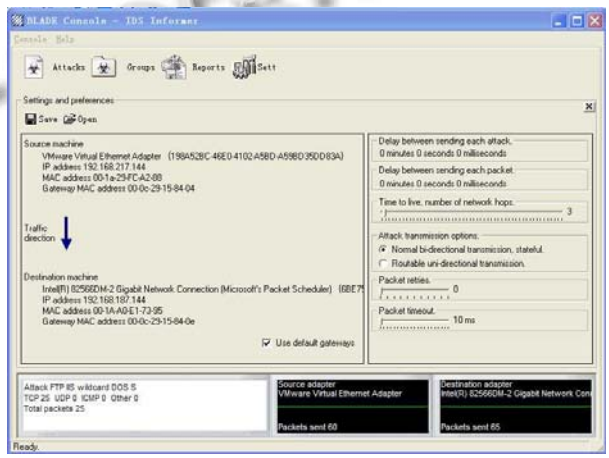

图 4　IDS Informer 配置

步骤 6: 使用 Blade 发送攻击报文(此处选择了 Attack FTP IIS wildcard DOS S), 在 Wireshake 网络协议分析工具界面上查看网络中的攻击报文, 如图 5 所示, 同时查看 IDS 产品能否正确发现攻击.

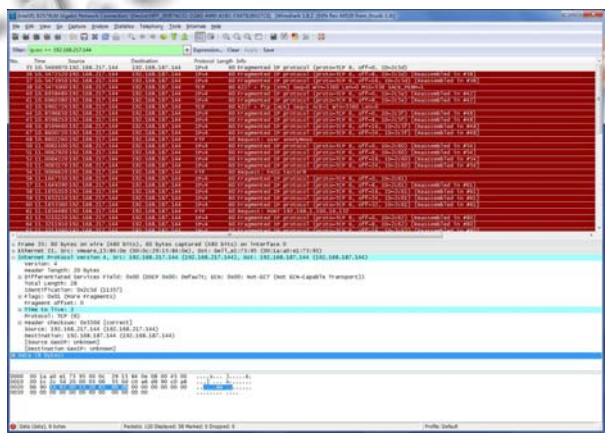

图 5　Wireshake 抓取的网络中的攻击报文

由 Wireshake 分析的数据报显示, Blade 发出的攻击报文能够被 Fragrouter 正常打碎, 形成欲逃避 IDS

检测的分片报文, 并能够在试验环境中(集线器)进行广播, 说明该试验方法有效, 可以用以 IDS 防逃避攻击功能的测试, 在测试其他攻击报文及逃避方式时可使用正交试验的方法对其他逃避攻击进行测试.

使用 Nikto 软件的测试步骤与上述类似, 测试时使用虚拟机的网卡 2 作为攻击源, 向物理机发送攻击报文, 只需要开启在物理机上搭建的 Web 服务器即可, 攻击发生时, 检查 IDS 产品能否正确发现逃避攻击.

2.2.3 注意事项

使用本文设计的软件测试方法对逃避攻击进行测试时, 需要注意以下 3 点:

1. IDS Informer 模块中设置目标设备(网卡 2)的 MAC 地址时不可以设为与物理机的真实网卡一致, 否则报文不出网卡, 无法被广播;

2. Wireshake 网络协议分析工具可能会显示未被打碎的攻击报文, 这与 Wireshake 的配置有关, 它可以识别并重组碎片包展示给使用者, 实际网络中并不存在该报文;

3. 应保证虚拟机中网卡的工作模式正确, 避免碎片包(逃避攻击)中出现未被虚拟机处理的源攻击包, 否则会影响 IDS 的检测效果.

2.3 仪表测试

2.3.1 仪表测试方法

Breakingpoint Systems 仪表具有强大的测试功能, 可以模拟各种攻击, 包括代码变形、报文分片等, 测试时将 IDS 旁路部署于测试环境中, 如图 6 所示.

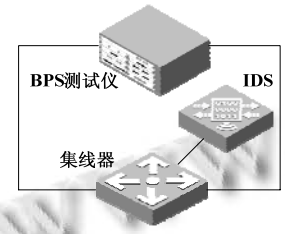

图 6 BPS 测试环境拓扑图

图 7 BPS 攻击测试过程截图

测试时选择使用的检测模块(Security 模块), 调整攻击参数, 并选择攻击包的个数, 进行逃避攻击, 攻击过程如图 7 所示, 攻击发送过程中, 查看 IDS 对攻击的发现能力, 并检验是否正确.

2.3.2 测试结果分析

选取 22 种不同类型的攻击方法, 并对攻击方法进行逃避攻击设计, 使用同一款网络型 IDS 产品分别在传统测试方法、仪表测试方法和本文设计的测试方法下进行防逃避攻击实验, 检验 IDS 对逃避攻击的识别能力, 测试结果如表 1 所示.

表 1 3 种测试方法结果比较 (%)

方法 / 结果	传统测试方法	仪表测试方法	文中测试方法
误报率	4.5	4.5	4.5
漏报率	27.28	27.28	27.28

表中误报率为 IDS 错误识别或还原攻击方法的百分比, 3 种测试方法在对 22 种不同的逃避攻击方法进行测试时, IDS 检测均出现 1 种攻击的检测错误, 且错误的攻击源相同, 漏报率为 IDS 无法检测或正确还原攻击方法的百分比, 3 种测试方法在对 22 种不同的逃避攻击方法进行测试时, IDS 均出现 6 种攻击无法检测或还原, 且无法检测或还原的种类相同. 由测试结果可以看出, 本文设计的测试方法能够正确的对 IDS 产品的防逃避攻击能力进行测试.

3 结语

本文在传统的 IDS 防逃避攻击测试方法的基础上, 对测试方法进行了改进, 在使用少量的(一台 PC)测试设备的情况下, 结合使用虚拟机完成对 IDS 防逃避攻击的测试, 经试验分析, 该测试方法能够有效的对各种逃避攻击进行模拟, 测试 IDS 的识别能力, 克服了传统软件测试方法试验环境复杂, 难以维护等缺点. 同时, 本文简要的介绍了使用仪表的测试方法, 与本文设计的软件测试方法相比, 仪表能够提供大量的攻击方法和攻击手段, 便于修改攻击参数, 但需要硬件工具作为测试依托, 环境难以实现.

参考文献

1 李镇江,戴英侠,陈越.IDS 入侵检测系统研究.计算机工程, 2001,27(4):7–9.

2 蔡旻甫.网络入侵防御系统设计与测试.中国测试, 2013,

39(2),106–109.

3 陈辰,张佐,吴秋峰.入侵检测系统的部署及入侵模式的识别.计算机系统应用,2002,11(11):36–39.

4 叶惠敏,潘正运.IDS 的数据收集机制.计算机系统应用,2002,11(7):37–39.

5 Xiang G, Cao YD. Generating IDS attack pattern automatically based on attack tree. Journal of Beijing Institute of Technology, 2003, 12(2): 138–142.

6 李海龙.入侵检测系统逃避技术和对策的研究.黑龙江科技信息,2007,23:90.

7 周扬.协议分析技术在入侵检测系统中的应用.计算机系统应用,2011,20(6):161–164.

8 陆臻,顾健.正交试验方法在 IDS 测试中的应用.信息网络安全,2010,24.

9 伍银,叶新铭,龚汉明.IDS 主动测试和被动测试相结合测试方法的研究.内蒙古大学学报,2013,44(1):97–103.

10 周明春,杨树堂.针对 IP 分片攻击的 IDS 反欺骗技术研究.计算机应用与软件,2007,24(10):22–25.

11 黄璐,于红.结合 IDS 的网络入侵诱骗模型的研究,大连水产学院学报,2007,22(4):284–288.

12 夏秦,王志文,卢柯.入侵检测系统利用信息熵检测网络攻击的方法.西安交通大学学报,2013,47(2):14–19.