一种新的端口扫描检测方法*

An New Portscan Detection Method

葛志辉，李陶深

Ge Zhihui，Li Taoshen

（广西大学计算机与电子信息学院，广西南宁 530004）

(School of Comp.，Elec. and Info.，Guangxi Univ.，Nanning，Guangxi，530004，China)

摘要：针对现有端口扫描方法存在的缺陷，提出一种端口扫描检测的新方法。该方法充分利用受保护网段内各主机的特征，对可疑事件进行关联分析，不但可以检测现有工具都可以检测的扫描，而且对慢速扫描的检测也非常有效。

关键词：端口扫描 检测 慢速 异常值 分析器

中图法分类号：TP393.08 **文献标识码**：A **文章编号**：1002-7378(2005)04-0247-02

Abstract：A new portscan detection method is presented to overcome the existing defects of current portscan metrods. In this method, the hosts' features in the protected network are fully used to conduct the associate analysis to all the suspicious events. This method can detect all the scans that are detected by current techniques，and is quite efficient in slow scan detect.

Key words：portscan，detection，slow speed，abnormity value，analyzer

端口扫描是网络入侵中一种相当重要的手段，入侵者在实施入侵活动前几乎都会对攻击目标进行扫描，以便获得目标的操作系统信息，从而进一步发现系统的安全漏洞[1]。端口扫描通常分为水平扫描和垂直扫描两种，其中以水平扫描较为常见，常用的端口扫描技术有[1,2]：TCP connect（）扫描、TCP SYN 扫描、TCP FIN 扫描、IP 分段扫描、ICMP 端口不能到达扫描等。以上只是目前发现的常用技术，随着互联网应用的日益广泛，入侵者的扫描技术越来越隐蔽，而且还在不停地变换扫描方式，比如改变扫描顺序、随机化扫描包的一些区域、慢速扫描等，不但扫描到信息，而且又躲避了检测。

1 传统的端口扫描方法分析

入侵者对端口扫描采用的方法有 Snort 方法、Watcher 方法和 PortSentry 方法等三种。它们采用的算法大致可以概括如下：在 M 秒内，监测从同一源端发出的数据包，如果其目的 IP 与目的端口的组合数目超出 N 的话，则认为是一次扫描。

Snort 是一个轻量级的网络入侵检测系统[3]。它的探测引擎采用模块化的插件结构，允许开发者扩展 Snort 的功能，也可以使得用户可以按自己的需要定制功能。Snort 检测端口扫描的方法是：在 Y 秒内，如果检测到从同一个源发出，目的为不同的主机和端口的组合的 TCP 或 UDP 包的数目超出阈值 X，则认为是扫描。其中 X 和 Y 的值可以由用户自己设定。另外，Snort 也同样可以检测有奇异标志的 TCP 包。

Watcher 是一个比较完整的基于网络的入侵检测系统的设计代码[4]。它检测所有通过的信息包，并且将它认为是恶意的攻击行为记录在 syslog 中。它的检测原理是：如果在短时间内有超过 7 个以上的端口收到信息包（不管类型如何），那么这一事件就被当成端口扫描记录下来。

PortSentry[5]是基于主机的网络入侵检测系统的一个组成部分，主要用来检测外部对主机的端口扫描，它能够对多种扫描方法进行检测。它的检测原理是：对没有开放服务的端口的访问有可能是一次扫描。通过监测没有开放服务的端口，在最近 n 次连接里由同一个源发起的连接超过 X 次则判断为一次扫描。

以上几种扫描方法对端口扫描所采用的检测技术都比较简单，且存在以下缺点：一是无法检测慢速

收稿日期：2005-06-09

作者简介：葛志辉（1980-），男，河北唐山人，博士研究生，主要从事计算机网络与信息安全领域的研究工作。

* 广西留学回国人员科学基金（桂科回 0342001）和广西科技攻关项目（桂科攻 033008-9）联合资助。

扫描，因为在检测中时间窗是个固定值，只要扫描速度低于这个阈值，攻击者就可以成功地逃避检测；二是未考虑到受保护网段的特点，对网段内所有主机都采用相同的检测策略，效率不高而且容易导致误报。针对目前扫描方法存在的缺陷，本文提出了一种检测慢速扫描的新方法。该方法充分利用受保护网段内各主机的特点，来检测扫描。

2 新的端口扫描检测原理

检测系统主要由两个部分组成：第一部分为可疑包捕获器，它的功能是从网络上捕获数据包，并判断该包的异常程度，将其赋与一个异常值（范围在0和1之间），然后写入SupIP表中待进一步处理，如果没有异常，则简单的丢弃。第二部分为分析器，通过对可疑包归类、分析以及对异常值的汇总，判断是否有扫描发生。

因为每台机器开放的服务各不相同，为了提高检测的效率，首先根据主机的端口开放情况为网络中的每台主机建立起IP地址与其开放端口的对应链表，如图1所示。

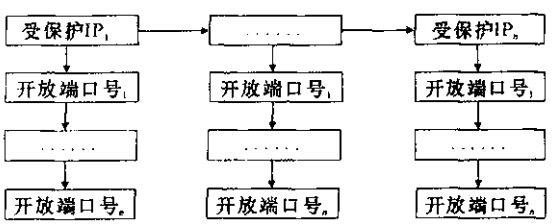

图1 IP-Port对应链表

另外，还需要建立一个可疑IP地址列表（表1）。表1中包括可疑IP地址、其访问的目的地址与目的端口号、可疑IP地址被记录时的时间戳以及被赋予的异常值。

表1 可疑SupIP表

SrcIP	可疑IP地址
DstIP	目的IP地址
DstPort	目的端口
TimeStamp	记录时间更新时间
Value	异常值

3 异常值的确定

在捕获网络数据包后，首先需要一定的准则来确定该数据包的异常程度，并赋给一个异常值。由于我们只检测对受保护网段内未开放端口的访问，所以如果访问次数超出3次，我们就认为是一次扫描。本文采用如下策略：

（1）带有奇异标志的TCP协议肯定是一次扫描，异常值赋值为1；

（2）任何对未开放端口的访问可能是一次扫描，异常值赋值为0.2；

（3）对空IP的访问可能是一次扫描，异常值赋为0.2。

4 分析器的设计

分析器主要的功能是对写入可疑表中的事件进行归类和分析，然后对各事件的异常值进行汇总、更新。分析器的工作步骤如下：

（1）分析器首先按照IP地址进行分析，对来自同一个IP地址的连接进行异常值统计，如果超出设定的阈值，则认为是一次扫描。

（2）对访问同一个目的端口的连接进行异常值统计，如果超出阈值则认为是一次扫描。

（3）对可疑表中的数据进行清除处理，如果受保护网段的网络活动频繁，或者入侵者故意使用伪造的IP地址，都会造成可疑表中数据项过多，从而增加分析器的计算量。这样就需要定期清除那些在一个时间段内并未达到报警阈值的可疑数据。

5 新的端口扫描检测方法特点

本文提出的检测方法具有以下特点：

（1）能检测特征明显的带有奇异标志的扫描，这种扫描可以在第一步中捕获数据包时就被直接检测出来。

（2）可以检测出那些看似为正常数据包的隐蔽扫描。

（3）可以检测慢速扫描。以前的方法都是采用在一个固定的时间窗 T 内查看从同一个源地址发起的连接数 X，如果 X 超出了设定的阀值，则判断为一次扫描。由于网络上的通信量非常大，所以以前的端口扫描方法都会设定一个很小的时间窗 T，防止消耗掉过多的内存和CPU时间。由于本文提出的方法与时间窗无关，所以在不降低系统整体性能的前提下仍能很好的检测慢速扫描。

（4）充分考虑到受保护网段的网络特点，而且在进行分析时对各个可疑事件进行关联分析，使得检测效率更高，检测也更准确。

6 结束语

在分析现有的端口扫描技术和扫描工具存在问

（下转第251页）

等基础学科的理论知识，综合各种学习方法、学习策略而成[5]。在内容筛选过程中，本着博而不杂、专而不单一的原则，充分考虑到使用此专题学习网站的各个阶层。课程内容分散于各个板块中，经过合理的安排，学习者可以根据自己的需要，从课程信息和网络课堂两个板块中自主选择自己感兴趣的内容。

为了避免网络课堂的单调，特意设计了在线测试模块，登录用户可以进入模块，挑选自己感兴趣的测试题，进行自我的心理测试，以缓解长时间工作和学习的压力。教师心理与良好的教师行为专题学习的主要支持有：

(1)学习素材。在 Web 教学网页中，可以开设课程、讲座及辅导答疑等栏目，其素材作为学习的主体，采用超文本的方法设计。学习素材的内容选择、结构安排、内部链接和界面设计等都很重要，在对知识的认识和关联上，力求方便学习者。

(2)导航支持。在一个多媒体超文本的教学系统中，如果缺少学习导航，容易使学习者迷航。学习者既需要一个学习索引系统，也需要一个学习路径的指导和进程管理系统。

(3)在线测试系统。学习网页中过多陈述性的内容往往会加速学习者的心理疲劳和厌倦。建立一个适宜的在线测试系统是提高学习者的兴趣、加速学习进程的有效方法，学习者可以根据自己的情况，有选择的对自己感兴趣的方面进行测试。

(4)电子邮件与BBS。教学主页上标记的电子邮箱十分重要，学习者可以将学习中遇到的问题写在论坛上与异地的学习者进行讨论。专家可以定期关注学习者的讨论，或提出某些评价意见，或对一些疑问给出参考性答案，或公布一些讨论主题等。学习者通过电子邮件向远程专家以个别方式提出问题。

(5)开放的学习环境。优秀的学习网站不可能包罗全部的学习资源，而应作为学习的一部分向学习者提供尽可能多的、相关的网上其他的学习资源，通过向学习者提供网址与相关链接，鼓励学习者通过访问这些地址，以掌握更多更广的知识。

5 结束语

教师心理与良好的教师行为专题学习网站是在互联网环境下，向学习者提供某一专题进行自主学习、交流和探究等活动的学习系统，学习者可以对本站所提出的观点发表自己的看法和意见，并同过交互模块，如留言板、论坛等方式与其他学习者进行经验和意见的交流，从而达到资源共享以及协同学习的目的。它与一般的网站的区别在于其体现了学习功能。目前国内高等教育的专题学习网站相对稀缺，本文通过“教育心理学”中“教师心理与良好的教师行为”这一较广泛的问题，论述专题学习网站的设计，探讨高等教育专题学习网站设计的新模式。

参考文献：

[1] 路海东. 教育心理学[M]. 长春：东北师范大学出版社，2002.

[2] 彭聃龄. 普通心理学(修订版)[M]. 北京：北京师范大学出版社，2001.

[3] 教育部. 现代远程教育资源建设技术规范(试行)[EB/OL]. http://www.etc.edu.cn，2000-05.

[4] 王志强，蔡 平. 计算机网络与多媒体教学[M]. 北京：电子工业出版社，2002.

[5] 全国高等学校教育技术协作委员会. 计算机教学软件的开发与管理[M]. 北京：高等教育出版社，2003.

(责任编辑：黎贞崇)

(上接第 248 页)

题的基础上，本文给出了一种检测端口扫描的新方法，该方法能充分利用受保护网段内各主机的特征，对可疑事件进行关联分析，从而有效地检测端口扫描。另外，本方法稍加修改也可用于检测DoS(Denial of Service)拒绝服务攻击。

参考文献：

[1] Stuart Staniford，James A Hoagland，Joseph M McAlerney. Practical automated detection of stealthy portscans[J]. Journal of Computer Security，2002，10(1/2)：105-136.

[2] 宋 华，罗 平，戴一奇. 一种新的分布式端口扫描检测方法[J]. 计算机工程与应用，2003，39：163-167.

[3] Caswell B，Beale J，Foster J C，et al. Snort 2.0 Intrusion Detection[M]. Syngress publishing，2003.

[4] Hyperion. Watcher Phrack Magazine. 1998，53(8)：11.

[5] Ido Dubrawsky. PortSentry for Attack Detection[EB/OL]. http://www.securityfocus.com/infocus/1580，2002-05.

(责任编辑：黎贞崇)