入侵检测安全解决方案

摘要:

随着互联网技术的飞速发展，网络安全逐渐成为一个潜在的巨大问题。但是长久以来，人们普遍关注的只是网络中信息传递的正确与否、速度怎样，而忽视了信息的安全问题，结果导致大量连接到Internet上的计算机暴露在愈来愈频繁的攻击中。因此，保证计算机系统、网络系统以及整个信息基础设施的安全已经成为刻不容缓的重要课题。本文先介绍入侵检测的概念和基本模型，然后按不同的类别分别介绍其技术特点。

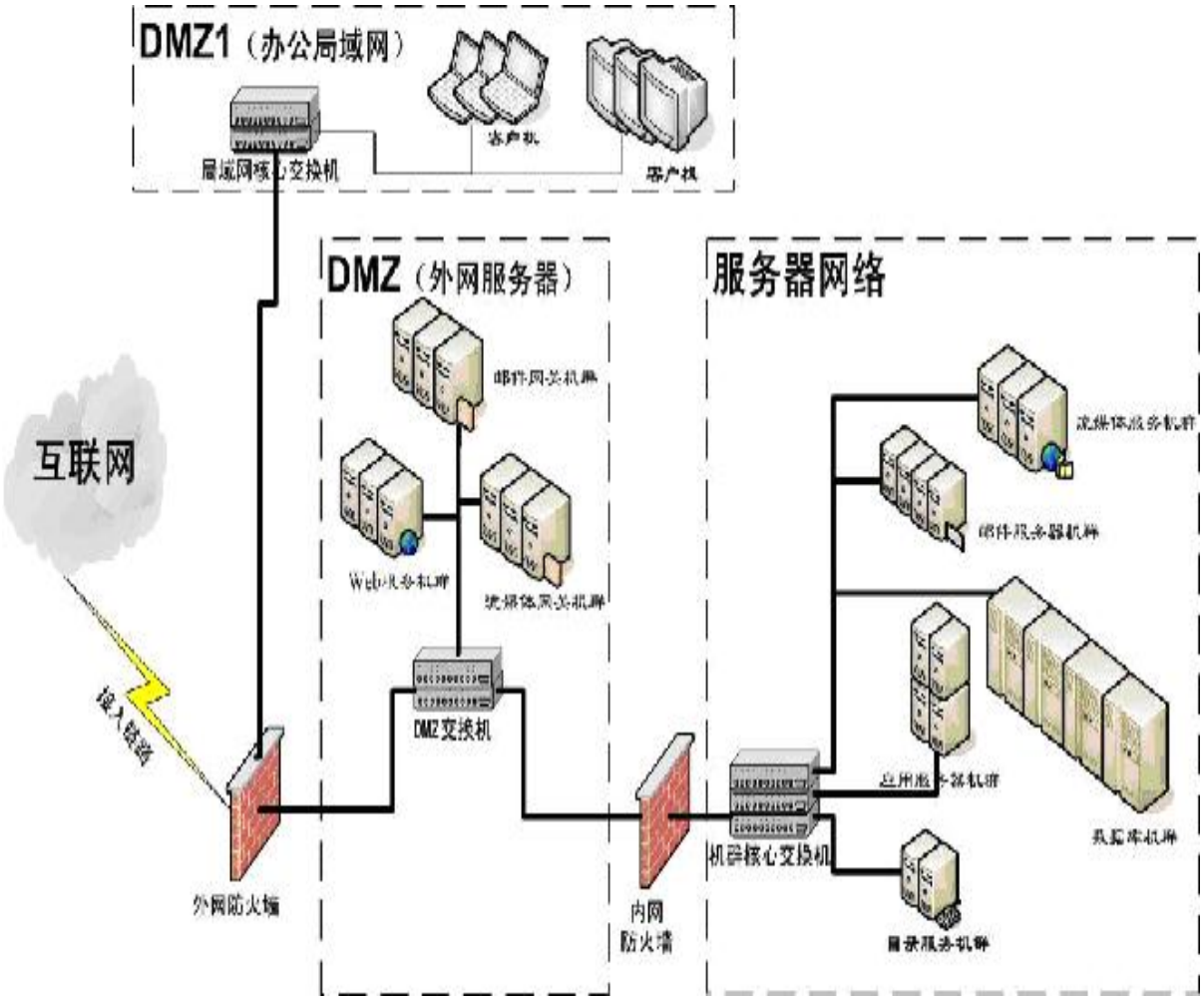
关键词:

网络安全、入侵检测、入侵检测系统、蠕虫、入侵检测系统的发展

引言:

随着Internet的迅速扩张和电子商务的兴起，越来越多的企业以及政府部门依靠网络传递信息。然而网络的开放性与共享性使它很容易受到外界的攻击与破坏,信息的安全保密性受到了严重影响。与此同时，网上黑客的攻击活动也逐渐猖狂。人们发现保护资源和数据的安全，让其免受来自恶意入侵者的威胁是件非常重要的事。因此，保证计算机系统、网络系统以及整个信息基础设施的安全已经成为刻不容缓的重要课题，入侵检测技术随即产生。

正文:



1□ 该网络的拓扑结构分析

从网络拓扑图可以看出，该网络分为办公局域网、服务器网络和外网服务器，通过防火墙与互联网连接。在办公局域网中有一个交换机和一些客户机。对于办公局域网络，每台计算机处于平等的位置，两者之间的通信不用经过别的节点，它们处于竞争和共享的总线结构中。这种网络适用于规模不大的小型网络当中，管理简单方便，安全控制要求不高的场合。在服务器网络中，有目录服务器、邮件服务器等通过核心交换机，在经过防火墙与外网服务器相连，在通过外网防火墙与互联网相连。

网络拓扑结构安全性考虑

网络拓扑结构与网络的安全性关系很大，如果设备再好，结构设计有问题，比如

拓扑结构不合理，使防火墙旋转放置在网络内部，而不是网络与外部的出口处，这样整个网络就不能抵挡外部的入侵了。设计好网络的拓扑结构，也就是使其进出口减少了收缩，把防御设备放置到网络的出入口，特别是防火墙和路由器，一定要放置在网络的边缘上，且是每个出入口均要有。

内网防火墙是一类防范措施的总称，它使得内部网络与Internet之间或者与其他外部网络互相隔离、限制网络互访用来保护内部网络。防火墙简单的可以只用路由器实现，复杂的可以用主机甚至一个子网来实现。设置防火墙目的都是为了在内部网与外部网之间设立唯一的通道，简化网络的安全管理。

防火墙的功能有：

1、过滤掉不安全服务和非法用户

2、控制对特殊站点的访问

3、提供监视Internet安全和预警的方便端点

由于互连网的开放性，有许多防范功能的防火墙也有一些防范不到的地方：

1、防火墙不能防范不经由防火墙的攻击。例如，如果允许从受保护网内部不受限制的向外拨号，一些用户可以形成与Internet的直接的连接，从而绕过防火墙，造成一个潜在的后门攻击渠道。

2、防火墙不能防止感染了病毒的软件或文件的传输。这只能在每台主机上装反病毒软件。

3、防火墙不能防止数据驱动式攻击。当有些表面看来无害的数据被邮寄或复制到Internet主机上并被执行而发起攻击时，就会发生数据驱动攻击。

因此，防火墙只是一种整体安全防范政策的一部分。这种安全政策必须包括公开的、以便用户知道自身责任的安全准则、职员培训计划以及与网络访问、当地和远程用户认证、拨出拨入呼叫、磁盘和数据加密以及病毒防护的有关政策。

2. 网络的安全威胁

该网络网的特点是有一个办公局域网和服务器网络。这种情况下，网络面临着许多安全方面的威胁：

1)黑客攻击，特别是假冒源地址的拒绝服务攻击屡有发生。攻击者通过一些简单的攻击工具，就可以制造危害严重的网络洪流，耗尽网络资源或被攻击主机系统资源。但是同时，攻击者常常可以借助伪造源地址的方法逍遥法外，使网络管理员对这种攻击无可奈何；

2)病毒和蠕虫，在高速大容量的局域网络中，各种病毒和蠕虫，不论新旧都很容易通过不小心的用户或有漏洞的系统迅速传播扩散。其中特别是新发的网络蠕虫，常常可以在爆发初期的几个小时内就闪电般席卷全校甚至全球，造成网络阻塞甚至瘫痪；

3)
滥用网络资源，在校园网中总会出现滥用带宽等资源以致影响其它用户甚至整个网络正常使用的行为。如各种扫描、广播、访问量过大的视频下载服务等等。

3 系统功能需求

在以上安全威胁面前侵检测系统(Intrusion Detection System, IDS)必须满足以下需求：

(1)确定攻击是否成功。由于基于主机的IDS使用含有已发生事件信息，它们可以比基于网络的IDS更加准确地判断攻击是否成功。在这方面，基于主机的IDS是基于网络的IDS完美补充，网络部分可以尽早提供警告，主机部分可以确定攻击成功与否。

(2)监视特定的系统活动。基于主机的IDS监视用户和访问文件的活动，包括文件访问、改变文件权限，试图建立新的可执行文件并且／或者试图访问特殊的设备。例如，基于主机的IDS可以监督所有用户的登录及下网情况，以及每位用户在联结到网络以后的行为。对于基于网络的系统经要做到这个程度是非常困难的。基于主机技术还可监视只有管理员才能实施的非正常行为。操作系统记录了任何有关用户帐号的增加，删除、更改的情况，只要改动一旦发生，基于主机的IDS就能检察测到这种不适当的改动。基于主机的IDS还可审计能影响系统记录的校验措施的改变。基于主机的系统可以监视主要系统文件和可执行文件的改变。系统能够查出那些欲改写重要系统文件或者安装特洛伊木马或后门的尝试并将它们中断。而基于网络的系统有时会查不到这些行为。

(3)能够检查到基于网络的系统检查不出的攻击。基于主机的系统可以检测到那些基于网络的系统察觉不到的攻击。例如，来自主要服务器键盘的攻击不经过网络，所以可以躲开基于网络的入侵检测系统。

(4)适用被加密的和交换的环境。交换设备可将大型网络分成许多的小型网络部件加以管理，所以从覆盖足够大的网络范围的角度出发，很难确定配置基于网络的IDS的最佳位置。业务映射和交换机上的管理端口有助于此，但这些技术有时并不适用。基于主机的入侵检测系统可安装在所需的重要主机上，在交换的环境中具有更高的能见度。某些加密方式也向基于网络的入侵检测发出了挑战。由于加密方式位于协议堆栈内，所以基于网络的系统可能对某些攻击没有反应，基于主机的IDS没有这方面的限制，当操作系统及基于主机的系统看到即将到来的业务时，数据流已经被解密了。

(5)近于实时的检测和响应。尽管基于主机的入侵检测系统不能提供真正实时的反应，但如果应用正确，反应速度可以非常接近实时。老式系统利用一个进程在预先定义的间隔内检查登记文件的状态和内容，与老式系统不同，当前基于主机的系统的中断指令，这种新的记录可被立即处理，显著减少了从攻击验证到作出响应的时间，在从操作系统作出记录到基于主机的系统得到辨识结果之间的这段时间是一段延迟，但大多数情况下，在破坏发生之前，系统就能发现入侵者，并中止他的攻击。

(6)不要求额外的硬件设备。基于主机的入侵检测系统存在于现行网络结构之中，包括文件服务器，Web服务器及其它共享资源。这些使得基于主机的系统效率很高。因为它们不需要在网络上另外安装登记，维护及管理的硬件设备。

(7)记录花费更加低廉。基于网络的入侵检测系统比基于主机的入侵检测系统要昂贵的多。

4.入侵检测安全解决方案

单一的安全保护往往效果不理想，而最佳途径就是采用多层安全防护措施对信息系统进行全方位的保护结合不同的安全保护因素，例如防病毒软件、防火墙和安全漏洞检测工具，来创建一个比单一防护有效得的多的综合的保护屏障。分层的安全防护成倍地增加了黑客攻击的成本和难度，从而大大减少了他们对该网络的攻击。在内网防火墙后增加一个IDS入

侵检测系统，在外网防火墙和互联网之间增加一个IDS入侵检测系统，入侵检测系统的漏洞的存在，通过对防火墙的配置提供稳定可靠的安全性。风险管理系统是一个漏洞和风险评估工具，用于发现、发掘和报告网络安全漏洞。防病毒软件的应用也是多层安全防护的一种必要措施。防病毒软件是专门为防止已知和未知的病毒感染企业的信息系统而设计的。它的针对性很强，但是需要不断更新。

入侵检测系统

入侵检测系统是指监视入侵或者试图控制你的系统或者网络资源的那种努力的系统。作为分层安全中日益被越普遍采用的成分，入侵检测系统将有效地提升黑客进入网络系统的门槛。入侵监测系统能够通过向管理员发出入侵或者入侵企图来加强当前的存取控制系统，例如防火墙;识别防火墙通常不能识别的攻击，如来自企业内部的攻击;在发现入侵企图之后提供必要的信息，帮助系统的移植。

入侵检测系统工具方面，基于主机与基于网络两条腿并行。在基于主机方面，ITA入侵检测系统中唯一基于规则的、实时的、集中管理的主机监测系统，它可以在网络边界和网络内部检查和响应来自外界的攻击和可疑行为。从功能上看，它可以探测出潜在的危险--

包括审计日志外不正常的"印迹"，并且根据安全管理员设定的规则，还可以对这些"印迹"进行分类并作出相应的反击响应。由于ITA即代表了网络IDS技术的发展趋势，所以在主动安全防护方面，富有创见性。NetProwler是一个基于网络的动态入侵检测系统，它提供了动态、实时、透明的网络IDS，能记录日志，同时可中断内部不满者和外部黑客的非授权使用、误用和滥用。尤其在动态扩展攻击特征库方面，NetProwler可使用SDSI虚拟处理器能够立即展开自定义攻击信号，中断严重的恶意攻击。总体上讲，可以帮助企业避免内部、远程、乃至授权用户所进行的网络探测、系统误用及其它恶意行为。作为一套战略工具，它还可帮助安全管理员制定杜绝未来攻击的可靠应对措施。在实施基于网络的IDS系统同时仍

然在特定的敏感主机上增加代理是一个比较完善的策略。因为，基于主机的IDS与基于网络的IDS并行可以做到优势互补:网络部分提供早期警告，而基于主机的部分可提供攻击成功与否的情况分析与确认。所以如果企业将赛门铁克的Net Prowler与Intruder Alert配合使用，能够达到更佳效果。

防火墙

由于，防火墙的就成为多层安全防护中必要的一层。一个防火墙为了提供稳定可靠的安全性，必须跟踪流经它的所有通信信息。为了达到控制目的，防火墙首先必须获得所有通信层和其它应用的信息，然后存储这些信息，还要能够重新获得以及控制这些信息。防火墙仅检查独立的信息包是不够的，因为状态信息--
以前的通信和其它应用信息--
是控制新的通信连接的最基本的因素。对于某一通信连接，通信状态(以前的通信信息)和应用状态是对该连接做控制决定的关键因素。因此为了保证高层的安全，防火墙必须能够访问、分析和利用通信信息、通信状态、应用状态，并做信息处理

而在防火墙方面，底层建立的应用程序代理防火墙产品更安全、更快速，并且更便于管理与公司的网络集成，以其独特的混合体系结构将多种功能基于一身，易于集中管理，可对企业提供全面的安全性防护。

风险管理系统

风险管理系统是一个漏洞和风险评估工具，用于发现、发掘和报告网络安全漏洞。的风险管理系统不仅能够检测和报告漏洞，而且还可以证明漏洞发生在什么地方以及发生的原因。在系统间分享信息并继续探测各种漏洞直到发现所有的安

全漏洞;还可以通过发掘漏洞以提供更高的可信度以确保被检测出的漏洞是真正的漏洞。这就使得风险分析更加精确并确保管理员可以把风险程度最高的漏洞放在优先考虑的位置。

在风险管理解决方案方面,ESM是一种基于主机的安全漏洞扫描和风险评估工具,它通过简化整个安全策略的设置和安全过程,可最大可能的检测出系统内部的安全漏洞障碍,并且使管理人员能够迅速对其网络安全基础架构中存在的潜在漏洞进行评估并采取措施。NetRecon可根据整体网络视图进行风险评估,同时可在那些常见安全漏洞被入侵者利用且实施攻击之前进行漏洞识别,从而保护网络和系统。由于NetRecon具备了网络漏洞的自动发现和评估功能,它能够安全地模拟常见的入侵和攻击情况,在系统间分享信息并继续探测各种漏洞直到发现所有的安全漏洞,从而识别并准确报告网络漏洞,并推荐修正措施。

在整个企业网络系统风险评估过程中,基于主机的ESM在内的安全漏洞扫描工具只限于在单一位置自动进行并整合安全策略的规划、管理及控制工作,其对于整个网络系统内的风险评估,尤其对于基于不同网络协议的网络风险评估不能面面俱到。

蜜罐(Honeypot)

蜜罐(Honeypot)是一种在互联网上运行的计算机系统。它是专门为吸引并诱骗那些试图非法闯入他人计算机系统的人(如电脑黑客)而设计的,蜜罐系统是一个包含漏洞的诱骗系统,它通过模拟

一个或多个易受攻击的主机，给攻击者提供一个容易攻击的目标。由于蜜罐并没有向外界提供真正有价值的服务，因此所有对蜜罐尝试都被视为可疑的。蜜罐的另一个用途是拖延攻击者对真正目标的攻击，让攻击者在蜜罐上浪费时间。简单点一说:蜜罐就是诱捕攻击者的一个陷阱。

防病毒软件

防病毒软件的应用也是多层安全防护的一种必要措施。防病毒软件是专门为防止已知和未知的病毒感染企业的信息系统而设计的。它的针对性很强，但是需要不断更新。最新的诺顿防病毒企业版7.6，提供桌面计算机和文件服务器的全面防毒保护，并可协助企业建立多层次防毒以保护其资产。与此同时，诺顿防病毒企业版7.6特别针对Microsoft Exchange/ Lotus Notes两类邮件服务器设计了自动化电子邮件防毒及内容过滤功能。借助诺顿防病毒企业版7.6对邮件服务器提供的防护功能，即可维持邮件服务器的稳定及正常运作的前提下，只需要一次扫描便能探测出恶意程序及带病毒的进出电子邮件，并可对有毒或可疑的电子邮件实施隔离，从而可以确保企业的邮件系统的高度安全。

多层防护发挥作用

即使网络中的入侵检测系统失效，防火墙、风险评估和防病毒软件蜜罐系统还会起作用。配置合理的防火墙能够在入侵检测系统发现之前阻止最

普通的攻击。安全漏洞评估能够发现漏洞并帮助清除这些漏洞。如果一个系统没有安全漏洞，即使一个攻击没有被发现，那么这样的攻击也不会成功。即使入侵检测系统没有发现已知病毒，防火墙没能够阻止病毒，安全漏洞检测没有清除病毒传播途径，防病毒软件同样能够侦测这些病毒。所以，在使用了多层安全防护措施以后，企图入侵该网络系统的黑客要付出成数倍的代价才有可能达到入侵目的。这时，你的信息系统的安全系数得到了大大的提升。

5 系统特点

(1)误用检测特征库

又称为基于知识的检测。其基本前提是:假定所有可能的入侵行为都能被识别和表示。首先，对已知的攻击方法进行攻击签名表示，然后根据已经定义好的攻击签名，通过判断这些攻击签名是否出现来判断入侵行为的发生与否攻击特征库是所有误用检测系统的核心部件，系统中规则的质量决定了误用检测的准确性和有效性。本系统中的攻击特征库记录有一千多条攻击特征，提供丰富的数据库管理接口，管理员可以很容易的增加或修改规则。同时，系统现有规则描述方法与互联网上常用的 snort
规则兼容，并且支持动态扩展新的描述方法，使管理员可以迅速对新发现的攻击做出相应规则，保障检测系统的有效性。

(2) 异常检测和蠕虫爆发检测

又称为基于行为的检测。其基本前提是:假定所有的入侵行为都是异常的。首先建立系统或用户的“正常”行为特征轮廓，通过比较当前的系统或用户的行为是否偏离正常的行为特征轮廓来判断是否发生了入侵。异常检测子系统可以统计

被检测网络的流量、协议、服务、主机的活动行为，从而发现网络的异常。异常检测可以发现未知攻击，主要针对大规模的攻击行为，与误用检测互为补充。蠕虫是网络攻击的一种，由于具有自主传播的特性，对网络的影响远大于普通的攻击。本系统提出了一种新的蠕虫爆发检测算法，通过分析流量的变化趋势检测蠕虫。它的特点是可以在蠕虫对网络造成阻塞之前发出报警，从而使系统管理员和网络紧急响应组织有更多的时间做出反应。

(3)攻击源追踪

由于路由器在转发IP

包的时候不检查源地址，所以攻击者为了隐藏自己的信息，常常使用伪造源地址的方法，如常见的 DoS

攻击就往往伴随着源地址的伪造。至今，追踪此类攻击的源地址仍是一个尚未圆满解决的问题。

攻击源追踪子系统使用所有监听网络边界路由器的记录目标地址为被攻击主机的流量数目。对于成功的攻击，其目的地址一定是真实的，所以将所有这些 MA 的记录数据通过 SS 汇总，使用 MS

进行分析后，就可以判断是否此攻击由被监测网络发出。如果被检测网络内确实有主机发出 DoS 攻击，则可进一步确定这台主机的位置。