网络入侵防护系统研究与应用

林光琪
广西壮族自治区烟草公司北海市公司

[摘　要]网络入侵防护系统是指主动智能的侵入监测与预警系统，旨在通过预先对侵入活动和攻击性的网络流量实施拦截，以防止网络环境和网络系统运行状态遭受破坏，从而完成由被动防范向主动防御的过渡，还可以整合侵入活动监测、病毒检测、防火墙等功能，以完成对网络安全的深度保护，并保证互联网的安全与正常运营。近年来，网络安全已成为信息安全领域和通讯科技领域的热点话题，网络安全环境越来越复杂，网络安全威胁数量也持续上升，现有数据传输保护工具由于线性反应逻辑问题，难以满足放下网络安全服务需求，防护系统亟须改革研究。基于此，本文针对网络入侵防护系统发展现状与未来发展趋势进行分析，并提出此系统的实际应用领域，旨在为其优化提供思路。

[关键词]网络入侵防护系统；网络安全；防御
【DOI】10.12252/j.issn.2096-627X.2021.10.1559

引言

由于互联网技术的蓬勃发展，网络安全日益引起我们的关注，我们不断开发各种网络安全防护系统以对抗网络攻击。防火墙技术是互联网的第一道防线，由于互联网环境的日趋复杂化，它已无法适应当下人类对网络服务的要求。入侵侦测技术是挡风墙的有效补充，它在预防非法侵入方面具备一定效果，但它通常只是被动的侦测，没有主动将网络危险阻隔在互联网之上的技术。在此背景下，人们亟须能够主动防护入侵的系统，在人们受到网络攻击时能够及时给予相应保护，以确保网络环境的正常使用，这便是入侵防护系统。基于此，本文针对入侵防护系统进行研究与分析。

一、网络入侵防护系统概念

入侵防护系统简称IPS系统，是主动智能的入侵检测与防范的系统，其能够预先对入侵活动或攻击性网络流量进行拦截，防止在正常使用时出现损失问题。此防御过程并非简单进行警报，在出现恶意流量传输时或之后才发出警报，而是通过特定的网络端口接收来自外部系统的流量，对全部输入流量进行检测，确认其存在不可疑内容后，再通过另外特定端口将其传送到内部系统中。这样针对疑问数据包或来自同一数据流的后续数据包，都可以在IPS设备中被清除掉，进而实现对网络环境的安全实时保护。在实际应用中，其主要分为三类部署：一是基于主机的入侵保护，通过对主机资源、网络服务和客户端程序的检测来阻断违反安全策略的行为，其可以在主机或服务器上安全相关代理程序，避免了网络攻击侵入操作系统和应用程序。通过针对不同的主机服务器操作系统，设置了不同的代理软件程序。二是基于对网络的攻击防护，通过监测流经操作系统的网络流量进行对网络的防护，其主要采用网络连接方法，而针对侵入行为则通过消除整个系统相关的网络会话方法加以消除。在实际使用中，其往往需要通过专门的网关或硬件平台，来完成对高流量的深度数据包检测的拦截功能。三是应用攻击防护系统。此系统是基于互联网攻击防护的特例系统，它主要设置在应用数据的网关链路上，对具体应用服务进行防护。

二、传统网络安全技术存在的不足

目前在网络环境中存在一些安全保护技术，但其在应用中存在一些不足，具体如下：首先是防火墙系统。此系统是将内部网络与外部网络从直接连接转化为间接连接的格力技术。在实际应用中主要借助网络安全规则设置允许经过授权的应用数据进出内部网络，同时可以阻断不许可的通信。此技术可以阻断来自外部网络的黑客更改、摧毁内部网络重要信息等行为，不仅能检测来自外部的入侵行为，同时也监督内部用户的未授权活动，有效保护身后网络不受外界干扰与损坏。但随着网络技术的不断发展，网络环境日益复杂，传统防火墙系统的问题逐渐凸显，具体包括：一是入侵流量可通过伪造数据绕过防火墙，或找到防火墙中可能敞开的后门。二是不能防止来自网络内部的袭击，目前大多数网络攻击来自网络内部，使得其功效无法发挥。三是无法实时监控，受到防火墙性能特点影响，其不能进行实时监控入侵行为。四是无法处理病毒侵袭。其次是入侵检测系统（IDS）。此系统能够弥补防火墙的不足，为内部网络环境提供实时监控，能够在发现入侵行为初期采取相应的保护措施，是安全防护有效的附加手段。随着网络技术的不断发展，入侵检测系统产品进入快速成长期，系统逐渐功能趋于完善，网络用户逐渐提升了对此系统的认同，越来越多的用户认可了其在网络安全防火工作中的重要作用。但随着网络环境的不断复杂，其存在的问题逐渐凸显，具体包括：一是错误问题较多，此系统在实际应用存在较高的漏报率和误报率。二是后续维护与管理工作难度较大。此系统在实际管理与维护过程中，需要安全管理员耗费大量的时间与精力。此系统的复杂程度较高，对安全管理人员的知识储备要求较高，以确保传感器更新工作与网络安全维护工作的顺利进行。三是实效开放机制为黑客攻击提供条件。当此系统受到拒绝服务攻击时，其实效开放机制会为黑客攻击行为提供条件，使其实施攻击而不被发现。实效开放机制是指系统停止作用时，整个网络或主机会转为开放状态。四是工作方式为被动形式。此系统以被动方式进行工作，只能被动检测攻击，不能有效组织攻击。在目前网络安全事件中，病毒攻击发生率较高，依次是系统渗透、拒绝服务、内部误用等，其中大多数用户应用了防火墙系统，部分用户还使用了入侵监测系统。这也意味着，以上二种体系都无法有效抑制新发生的网络安全事故。最后是入侵防护体系（IPS）。是指监测侵入行为，并采取适当方法实时停止侵入活动产生影响和进展的高自动化产品，它能够保障整个网络系统不遭受实质性的入侵影响。此系统也可以融合了网络安全防火墙和入侵侦测系统的优势，不但可以有效履行主动防御任务，同时还能够保障企业安全。而目前的如上监测管理系统已可成为中国企业安防的技术前沿，它能够在系统遭遇入侵时及时发布提示和警告信息，但具体操作访问的各种监控列表等仍需要由网络管理人员完成，以防止入侵行为的逐步蔓延，并尽可能减少入侵影响范围。而相比于IDS管理系统，IPS系统不仅能够及时检测到入侵行为的出现，同时还可以在攻击入侵初期进行处理，将其抵挡于网络环境外部。除此之外，此系统可以不断更新病毒库与模式库，以及时发现各种新的入侵方式，进而作出更加智能的保护操作，避免出现攻击漏报或误报情况。不同

的应用系统其实现方式不同，但大多具有防火墙防御功能和入侵检测系统网络数据包检测功能，以实现对受保护网络更加全面的防护。

三、网络入侵行为的分类与特点

（一）拒绝服务攻击行为

拒绝服务攻击是较为常见的网络攻击行为，其可以通过多种途径促使目标机器停止服务，是黑客经常应用的攻击方法。此攻击方法能够对网络安全产生较为严重的影响，在实际场景中，网络攻击者借助各种攻击方法，对网络与服务器自身的弱点进行攻击，同时制造出海量的毫无意义的数据流量，将数据流量通过接口进行传输，正常系统对此数据进行大量检测与处理，以不断占用正常使用者所提供的请求服务，使得正常系统无法及时处理正常使用者的请求。经过上述处理后，攻击者不断采取不同的攻击手段，不间断向目标即系发送大量非法IP报文、ICMP数据报文等，促使主机对大量报文进行传输与处理，进而实现对主机处理能力的消耗与占用。

（二）扫描探测攻击行为

扫描探测攻击行为是较为普遍的攻击手段，属于主要面向目标主机发出的攻击手段。在实际场景中，攻击者可借助此手段获取主机的相关信息，对主机信息进行扫描并根据扫描结果进行进一步攻击。在预防工作中，为避免攻击者获取主机信息并进行一系列监控扫描行为的发展，入侵检测系统可对主机系统与此类行为进行实时监控。比如当出现网络主机蠕虫病毒时，考虑到此病毒攻击行为的特点是自动攻击与快速发展，相关工作人员需要对网络端口与主机进行不断扫描，对此病毒攻击方式与攻击特点进行不断检测与分析，以确保主机SYNACK位与同步序列编号位进行详细的查看。当发现网络主机所含有的报文数量具有极其明显的差异，则可以将其看成爆发蠕虫病毒的一个源头。

四、网络入侵防护系统的整体框架

（一）信息采集模块

信息采集模块是对网络信息数据的捕捉，网络是向网络提供数据的主要来源，其主要通过对系统的计算机网卡进行应用。而信息采集模块能够对所捕获信息进行拷贝，将其制作成相应的文件，而后传输至已分配完成的缓冲区，为其他板块工作提供相应准备。此拷贝文件在整个模块运行中占据中要地位，其是采集工作的终点，是后续各项工作的重要支撑，属于特意为系统中其他的模块进行访问时而准备的文件。在网络配置与部署入侵检测系统过程中，为确保数据信息的直接获取，需要在初步测试环节进行应用与分析，准确定位出其应用特点与属性。此系统的全面性较为明显，一旦正式应用于主机系统时，会失去一定的效能。这就表明在充分体现模块主要作用时，需要不断提炼其相关数据信息，以确保后续数据挖掘过程的精准性，为后续模块提供相关数据依据。

（二）信息整理模块与数据挖掘模块

信息整理模块能够处理相关的报文，促使其与相对应的IP汇聚，传递处理后的报文信息。在此过程中，网络相关管理人员需通过连接信息整理板块与数据库之间的关联，建立完善的信息整理周期，促使信息整理工作能够按照一定的周期进行，将经过汇聚的数据信息汇聚于数据库中，为后续检测处理工作提供有效数据支撑，为下一步入侵检测处理过程提供相应的数据源。数据挖掘模块是指对网络系统各项参数的调试与研究，可在离线状态下完成调试工作，以确保系统参数的不断优化与完善。网络安全管理人员可从数据库中定期提取源IP汇聚信息，借助网络技术进行深入分析，判断其是否夹杂攻击行为等，并结合分析结果进行相应处理，最终将攻击信息汇总成报告形式。

（三）报警记录板块

报警记录板块能够在网络受到攻击时，借助对话框功能建立相应的报警信号，及时通知到网络系统管理人员，并将报警信息与攻击情况以最快速度传递给工作人员。在此过程中，管理人员可以通过对系统神经网络参与的应用，结合人工操作方式，对在线分析数据与信息进行不断调整，以确保网络防护系统参数的不断优化与准确。此板块可以提供防护相关功能界面，让安全管理人员能够对整个系统建立直观的掌握，从而对整个检测体系组织进行设置和管理。在实际运用中，此体系大致可以从二部分开展工作，大致分为以下方面：一方面是对输入信号的收集和整理。在对数据库的输入与输出信息之间，此模块一方面对输入输出信息进行收集和汇总，同时对手机和互联网上的信息数据进行汇总，以保证数据传输信息的顺畅，确保可以对数据信息进行深入挖掘。而另一方面是对输入与输出信息的集中管理。由于数据库对信息管理后的输入输出信息部分属于不断分类汇总的信息数据，因此管理人员必须通过网络流量分析功能对这部分数据加以分析和使用，以便于进一步在信息库中获得相关的安全数据。

五、网络入侵防护系统的应用

在实际应用中，此系统主要可从两个方面入手，一是数据挖掘应用。在入侵检测工作中，数据挖掘能够为防护系统提供行为特征确定功能，及时对攻击行为的特征进行定位，并将相关标准视为数据流的具体走向。由于网络攻击行为能够带来大量的毫无意义的信息，为主机处理功能带来挑战，其可以有效降低此类信息的感染，发挥一定的约束与过滤功能。二是数据采集整理应用。对攻击行为相关数据进行整理与分析，并将其属性想数据板块输入，以确保其是否存在具体的攻击行为。在实际工作中相关人员要强化对数据采集整理的应用，以发挥其应有效用。

结束语

综上所述，随着信息技术不断发展，网络环境日益复杂与丰富，网络环境需要处理良好的数据信息，需要以大量应用进行承载，这就带来了大量的数据安全审核工作。如何安全提取与应用数据信息，如何建立对网络入侵行为的特征分析与及时防御，是目前网络安全管理人员需要重点关注的问题。网络入侵防护系统是目前较为前沿的网络安全技术，其可以对安全审计信息进行处理与操作，在海量数据信息中确保对潜在信息进行快速判断与处理，同时也能够对其是否存在或存在的具体网络行为进行判断。对此，相关网络管理人员要强化对网络入侵防护系统的研究，充分挖掘其应用领域，充分发挥其应用效能，为网络环境完善提供有效支撑。

参考文献

[1]张文安，洪榛，朱俊威，陈博.工业控制系统网络入侵检测方法综述[J].控制与决策，2019，34（11）：2277-2288.

[2]朱平哲.网络入侵检测与防护算法系统的实现[J].安徽电子信息职业技术学院学报，2019，18（03）：7-12.

[3]麻时明，陈积常，张扬.基于数据挖掘的网络入侵安全防护系统研究[J].无线互联科技，2018，15（22）：28-29.