Frontier Scientific Publishing
Modern Education Forum 现代教育论坛
第 2 卷◆第 1 期◆版本 1.0◆2019 年 1 月
文章类型：论文|刊号（ISSN）：2630-5178

网络信息安全技术浅析

林日升
瑞安中学
DOI:10.32629/mef.v2i1.46

[摘　要] 本文就计算机网络信息安全的安全隐患,黑客的攻击强度,针对黑客攻击强度的分析,对网络安全端口的监控,保证网络工作顺利进行的方法以及 HTML5 技术的分析进行阐述,以提高网民的安全意识和增强其防范手段。
[关键词] 网络安全；黑客；端口；HTML5

1 网络信息存在的安全隐患

虽然计算机专家和360安全卫士等公司开发了许多安全保护工具,执法机关也建立了打击网络犯罪的机制和执法队伍,但网络安全安全问题却越来越严重,本文认为安全隐患主要由以下几点造成。

(1)安全机制的局限

确定的应用程序和应用程序环境的范围存在于每个安全机制当中。计算机中所有网络通信都要途径防火墙,这就使防火墙对于计算机具有一定的保护性,但是防火墙对于网络内部的信息流通还是没有办法阻止的。因此,防火墙找到并阻止内部网络之间入侵和勾结入侵也是很困难的。

(2)安全工具的影响

由于我国人口众多,国民的受教育水平程度普遍不是太高,计算机操作能力有限。许多网民都是跟风上网,对计算机的安全工具知识了解的很少,都是安装程序是自带的,所以使用时不当的操作在很大程度上会影响到安全工具的实际效率。设置不合理将会造成一个不安全的因素并且他们的安全工具也存在漏洞。没有及时升级很容易被别人作为一个攻击工具所利用。

(3)bug 可能存在于任何程序当中

没有任何程序不存在 bug,bug 是无穷无尽的,甚至无处不在的,我们可以这样认为,安全工具本身就存在 bug。差不多每天都会发现并公布一个新的 bug,程序设计师在修改一个知名的 bug 的同时他们可能会产生一个新的错误。由于利用程序本身存在的错误进行攻击的手段一般都不会产生日志并且查询不到任何数据,这种方法得到黑客的青睐并产生了出乎意料的结果。举个例子,许多项目现在有一个内存溢出的 bug,使用现有的安全工具几乎不能避免 bug 的攻击。

(4)线上黑客任意畅行

根据 Ernst 和 Young 报告,曾经几乎 80%的大型企业遭到黑客攻击的情况的原因是信息安全被窃或盗用。在黑客大规模攻击下,许多跨国大公司都无法制止,顷刻间网络瘫痪,信息泄露,造成巨大的损失。据统计,在全世界每年因为黑客攻击造成的经济损失高达几百亿美金。由于该行业人心惶惶,亚马逊(Amazon.com)、美国在线、雅虎(Yahoo)、易趣网的股价均告下跌。这些个事件使人们心惊胆战,人们自心里觉得“网络并不安全”。黑客们每天都在不断攻击不一样的系统安全问题。黑客本身就是技术超强的计算机专家,他们对计算机知识了解的很透彻,很清楚当前计算机的发展程度,安全工具还达不到绝对的安全,也很清楚计算机系统存在漏洞的地方。

2 黑客攻击强度的分析

近年来,黑客的攻击日渐频繁,对黑客的要求有从技术领域逐渐降到操作领域的趋势。较为出名的 ddos 攻击以及 ping 攻击,是比较早期的攻击方式,攻击者并不依赖个人主机强大的性能,甚至攻击方也不提供服务器,这对于攻击方来说成本是巨大的,黑客以团队的方式进行瘫痪式攻击,比如 ping 命令攻击,利用成百上千的网络用户共同向同一个服务器进行报文请求,从而使得目标网络在一时间之内由于无法处理正常用户的合法请求而导致瘫痪,这也是就是人们所说的洪泛式攻击,这种方法往往很粗暴。

随着时代的进步,洪泛式攻击从主流的攻击方式逐渐淘汰,黑客的攻击以独特的个体攻击逐渐代替以前的群体式攻击,如一个黑客现在想要窃取目的主机的数据信息,首先通过端口扫描的手段对目的地址进行漏洞扫描,根据端口开放信息确认攻击方式。接下来,利用网段劫持的方式对已劫持的主机进行大规模的命令指示,也就是黑客们常说的“肉鸡”,利用一人的命令使得被劫持主机共同进行服务器攻击,利用服务器短时间的瘫痪,利用已经进行 ip 地址欺诈的主机进行监听处理,在利用监听信息对主机进行看似合法的请求攻击,进入目标服务器。

黑客的攻击强度从之前的群体暴力攻击逐渐走向单体的多组合式攻击,一个黑客可以通过不同手段的组合攻击从而达到之前需要一个群体的攻击目的。当我们假设一个黑客群体的基数不变的情况下,当黑客的攻击数量从群体到单体时,攻击强度不变的情况下,实际上网络安全问题就尤为突出,这使得网络安全的方法如果处理不得当会使得防御会显得十分无力。黑客们对目的主机的信息把和攻击方式较之前更为准确快捷。如 zmap 仅仅只需几个小时即可对世界的全网络主机进行一次扫描,这也证明了网络安全的攻击是逐渐在提高的,而对网络安全的方法则显得有心无力。

3 网络安全体系的探讨

(1)网络环境下的网络病毒防范

当今的网络环境很复杂,网民很多,各类网站如雨后春

笋般的发展,各网络公司为了推销自己产品,设置添加各种链接,给病毒提供了可乘之机,导致病毒的快速传播,大面积扩散,造成严重损害。要想彻底防止病毒感染,就要切断和外部网络联系,这样又不能共享信息资源。如果你想要链接到互联网上那么我们需要一个网关杀毒软件,这个软件加强了计算机网络的安全性。我们现在需要一款既能防备病毒攻击又能很好地运用互联网资源的杀软件。这样才能保护我们正常的生活,如发电子邮件,传递各类知识信息等。基于现实的需要,我们要针对网络中病毒善于发现漏洞,攻击弱点的特点,开发一套能自动识别病毒,修复漏洞,不断自动升级系统,发送修复补丁通过全方位、多层次,保护好我们正常使用网络,免受病毒入侵。

(2)防火墙的配置

3.1 防火墙就是组织外面的人对你的网络进行访问的设备,可以将web服务器置于防火墙内部,将web服务器放在防火墙内部的优势就是能够使它得到很好的保护,黑客很难入侵到它。但是它也有一个很明显的缺点,那就是不容易被外界所应用。

3.2 将 web 置于防火墙的外面,虽然这样就可以解决我们上面所说的问题,并且能切实的保护好我们的内部网,就算真有黑客入侵 web 服务器,我们的内部网络还是很安全的。但是这种配置的缺点是无法对 web 服务器起到很好的保护作用。

3.3 另外一些管理者为了提高 web 服务器的安全性能,将防火墙加在 web 服务器上,这样虽然起到增强 web 服务器安全性能的作用,但这样也有很大的隐患：如果 web 服务器出现问题,互联网就会暴露在黑客和病毒入侵的危险之中了。

防火墙作为目前能够限制黑客入侵的有效手段,本身也有许多不尽人意的地方：没有办法防范其他途径的攻击入侵,所有的防火墙配置都需要根据实际情况来操作,不能一概而论。

(3)使用入侵检测系统

互联网入侵检测系统,是指按照一定的安全策略,通过互联网软件、硬件,加强对网络系统的运行状况进行监视,尽可能地发现各种攻击企图、攻击行为或者攻击结果,从而保证网络资源安全。打个比方：防火墙好比是一幢大楼的门锁,那么入侵检测系统就是这幢大楼的监视系统。如果发现小偷企图爬窗进入大楼,或者内部人员有越界行为,实时监视系统就会发现情况并发出警告。入侵检测系统分为基于主机的模型和基于网络的模型,两种模型具有互补性,入侵检测系统好比是防火墙之后的第二道安全门,两者互相配合,优势互补,才能正在提高网络安全。

(4)Web、Email、BBS 的安全监控系统

通过对网络的 www 服务器、邮件服务器等网络系统的安全监控,采用实时跟踪、监听控制等方法,截获通过互联网传输的各种信息内容,并且将其还原成完整的 www、电子邮件、FTP、Telnet 应用程序的内容,建立相应的日志记录来维护数据库。及时通过安全监控系统检测在网络中传输的各种非法内容,并及时向上级网络安全管理中心报告,采取必要措施,制止非法传播,保护网络干净。

(5)漏洞扫描系统

通过扫描掌握网络存在哪些安全隐患和漏洞是我们处理保护网络安全问题的目的。网络是复杂的、更新变化很快,如果仅局限于依靠网络管理员的技术和经验寻找安全漏洞、做出风险评估,很明显是不够的,也不能正在保护网络安全。要解决这些问题只有一种方案。那就是找到一种能查找出网络安全漏洞、通过系统评估分析,给出修改建议的网络安全扫描工具,并且使用优化的系统配置和修改补丁等方式,以便最大可能地弥补发现新的安全漏洞和消除安全隐患。在可控的范围内,我们自己可以利用各种黑客工具和病毒,对网络进行模拟攻击从而使网络安全的漏洞暴露出来,以便发现问题,解决问题。

(6)建立网络监控保护子网系统安全

我们通过安装防火墙来加强网络外部黑客和病毒的入侵,但是对于网络内部攻击则显得很无能为力。在这种情况下,我们通常采取的措施就是对每个子网做一个具有一定防护功能的审计文件的方法,为网站管理人员分析自己的网络运作状况提供依据。并且设计一个子网专们用于的监听内部信息软件,这款软件的主要功能是为长期监控子网络内计算机之间相互联系的情况,并为内部网站的系统中各个服务器的审计文件提供备份,以便全面掌握内部信息,做到安全保护计算机的目的。

4 结束语

总的来说,对网络安全的分析是复杂的,是需要不断的更新的,对攻击方来说一个漏洞就可以进行的攻击,对防御方来说就相当于是百密一疏的不可估量的损失。我们要积极投身到网络安全建设当中去,为我们的祖国发光发热,将我们的祖国建设成为网络安全大国。

[参考文献]

[1]张卫航.计算机网络信息安全中数据加密技术应用[J/OL].电子技术与软件工程, 2019(02):184[2019-02-20].http://kns.cnki.net/kcms/detail/10.1108.TP.20190201.1451.582.html.

[2]孙素萍.基于网络信息安全技术管理的计算机应用[J/OL].电子技术与软件工程, 2019(03):165-166[2019-02-20].http://kns.cnki.net/kcms/detail/10.1108.TP.20190201.1451.568.html.

[3]刘洋.网络通信中的数据信息安全保障技术[J/OL].电子技术与软件工程,2019(03):188[2019-02-20].http://kns.cnki.net/kcms/detail/10.1108.TP.20190201.1452.652.html.

[4]樊小龙.计算机网络信息安全中数据加密技术的研究[J].科技风,2019(03):93.

作者简介：

林日升(2001--),男,汉族,浙江瑞安人。