

DDoS攻击的防御方法研究

文 / 邓家宏

摘要: 分布式拒绝服务攻击(DDoS)是近年来网络上流行的、能导致巨大经济损失的攻击方式之一,为其建立有效的防御机制是当前维护网络安全的重要目标。本文对DDoS攻击原理与特点进行了分析,并对预防DDoS攻击的措施、受到DDoS攻击时的应对方法进行了探讨。

关键词: 网络安全; DDoS攻击; 预防措施; 应对方法

近年来,随着网络的普及,各种网络攻击事件在互联网上不断出现,其中分布式拒绝服务攻击不断升级,对社会经济造成了巨大的损失。分布式拒绝服务攻击是从最初的、简单的DoS发展起来的。DoS(Denial of Service,拒绝服务)攻击,是一种利用单台计算机对另一台计算机进行攻击,在网络中是一种很简单但又很有效的攻击方式,它的攻击原理是非法利用TCP/IP协议漏洞中合理的服务请求来占用大量的网络服务资源,从而使合法的用户无法得到正常的网络服务。DDoS(Distributed Denial of Service,分布式拒绝服务)攻击,是一种特殊的DoS攻击方式。DDoS的攻击原理与DoS的攻击原理有所不同,DDoS是DoS的升级,它采取的攻击方法是:通过一大批受控制的机器(计算机)向一台机器(计算机)发起攻击,即通过仿真多个客户端来向服务器发起连接,利用了TCP/IP的协议中不可避免的漏洞,造成服务器无法处理如此多的客户端连接请求,从而达到使受攻击的机器(计算机)无法提供正常的网络服务的目的。

由于DDoS攻击是利用TCP/IP协议漏洞来进行攻击的,并且TCP/IP协议会话机制的漏洞是无法修改的,故DDoS的攻击具有来势迅猛、受攻击机器难以防备、对受攻击的机器具有较大破坏性的特点。很多网络用户对这种攻击缺少直接有效的防御手段。DDoS的攻击对象主要是比较大的站点服务器,比如一些商业公司数据中心、各知名WEB服务器、游戏服务器、电子商务服务器、政府部门网站,往往会造成较大的经济损失,危害性较大。

DDoS攻击虽然来势迅猛,破坏性又大,不等于我们就没有办法阻挡DDoS的攻击。根据本人在实际工作中的体会,如果我们在平时能够做好预防DDoS攻击的措施、在受到DDoS攻击时能正确地应对,我们就能有效的减少DDoS的攻击。

一、做好预防DDoS攻击的措施

为了防止DDoS的攻击,在平时我们应做好如下几个方面的预防措施。

1. 定期查看并保留各种日志,以助分析各种情况。日志看起来很枯燥,而且绝大多数时候没什么作用,可一旦意外发生,它就能为你提供很重要的信息参考,所以要提前做好计划,每天定时查看日志并及时对可疑的信息做好应对措施。

2. 定期扫描,及早发现系统漏洞,及时安装系统补丁程序。要定期扫描网络骨干节点,检测可能存在的安全漏洞,及时对新发现的漏洞进行修补。骨干节点的网络具有较大的带宽,是黑客最想利用的位置,因此对这些网络设备加强安全防范是非常有必要的。而且与网络主节点连接的计算机都基本是服务器级别的计算机,所以对它们定期扫描漏洞并及时修补就显得更加重要了。对系统配置的一些重要信息,要建立完善的备份机制,对一

些特权账号(例如管理员账号)的密码设置要谨慎。

3. 提防错误配置造成的隐患。错误配置通常发生在硬件搭配、服务器系统或者应用程序中,有时候问题还很隐蔽。通过反复检查来确保路由器、交换机等网络连接设备和服务器系统都进行了正确的配置,这样才会减小各种错误和减少入侵、攻击发生的可能性。

4. 关闭不必要的服务和端口。要经常检查系统的物理环境,禁止那些不必要的网络服务。建立边界安全界限,确保输出的数据包受到正确限制,经常检测系统配置信息,并注意查看每天的安全日志,只让必须要用的端口打开,其余的都关掉。

5. 利用网络设备保护网络资源。网络设备是指交换机、路由器、防火墙等负载均衡设备,它们可以有效地对网络进行保护。当网络被攻击时最先崩溃的是路由器,但其他设备并没有崩溃。我们可以及时将崩溃掉的路由器重启,网络会恢复正常,而且路由器重启的速度很快,不会造成太大的损失。如果是服务器崩溃,服务器中的数据有可能会丢失,而且重启服务器后对其进行配置达到正常使用是一个漫长的过程。所以,每个公司都很有必要配置负载均衡设备,当其中一台机器被攻击死机时,另一台将马上工作,从而在最大程度上削减DDoS攻击的危害。

6. 正确设置防火墙。禁止对主机的非开放服务的访问,限制同时打开的SYN最大的连接数,缩短Syn半连接的time out时间。限制特定IP地址的访问,启用防火墙的防DDoS的属性,为了防止自己的服务器被控制当成工具去攻击别人,应严格限制对外开放的服务器的向外访问。

7. 正确设置路由器。以Cisco路由器为例,使用Unicast Reverse Path Forwarding等通过反向路由器查询,检查访问者的IP地址是否真实,对假的IP予以屏蔽。许多黑客在攻击时常使用假的IP地址迷惑用户,很难查出它来的出处。因此,利用Unicast Reverse Path Forwarding的方法可减少假IP地址的出现,有助于减轻服务器的负担,提高网络安全性。

在路由器上设置SYN/ICMP的最大流量值来限制SYN/ICMP数据包所能占用的带宽。这样,路由器当出现大量的超过所限定的SYN/ICMP最大流量时,说明存在不正常的网络访问,有可能是黑客入侵我们的网络。通过限制SYN/ICMP流量是最好、最有效的防范DOS攻击的方法,虽然目前该方法对于DDoS攻击效果已经不太明显了,但还是能够起到一定的作用。另外,还要对访问控制列表(ACL)进行过滤,并为路由器建立log server。

二、受到DDoS攻击时的应对方法

当主机受到DDoS攻击时,我们可以抓住机会,及时采取应对措施,减少不必要的损失,应对方法主要有如下几个方面。

1. 首先要检查攻击来源地址。通常黑客先控制了一些傀儡机,由这些傀儡机和一些假的IP地址进行攻击,这时,网络管理员如果能够分辨出IP地址的真伪和IP来自于哪些网段,如果含有公司内部IP地址,应及时将这些计算机关闭,从而可以做到在第一时间消除攻击。如果发现这些IP地址是来自于公司外部,可以采取临时过滤的方法,将可疑的IP地址从服务器或路由器上过滤掉。

(下转第85页)

《电子商务技术》及《网上开店实务》。《电子商务技术》主要在二年级使用,而《网上开店实务》则是为三年级学生开设的电子商务实践教材,为学生的就业增加专业的电子商务技能。针对各个年级学生的实际情况,我们对这两门教材进行了整合,剔除过时的技术操作,增加实操课程以及实用的互联网操作等,特别是网上开店方面设计了相关的专题和内容,如网上开店二三事、支付宝的充值及付款以及物流选择等,根据时代的发展,大力培养学生的电子商务应用能力。

二、课堂模式

课堂模式方面,根据我校2012-2013学年的教改要求,我选择了技能新授课这个模式作为研讨课,教学流程较为顺畅,第一步是揭示上机目标,第二步是进行课程技能示范,第三步是学生进行模仿练习,第四步是我对学生的模仿操作进行纠错点评及总结,第五步是学生进行提高练习,最后是教师进行点评及布置作业。《支付宝的充值与支付》,揭示的两个上机目标分别是“使用支付宝,充值其实很简单”、“在淘宝购物,付款其实很容易”,当学生大声朗读这两句话的时候,心情已经变得轻松愉悦了,感受到这节课的目标很简单。有了愉快的开头,课程的开展更加顺畅了,后面的几个步骤都是有条不紊的进行,唯独受限于技术条件,学生练习环节出现了延误,让学生的实操不够充分和彻底。

三、教法的使用

《网上开店实务》从专业卖家的角度,以网上开店的经营流程为主线,通过体验申请、经营一家店铺的过程,熟悉网上交易的基本流程以及网上销售的一系列环节。而对于学生来说,以买家的身份使用支付宝的机会更多,因此在课程内容整合的基础上,为了让学生系统的学习和掌握支付宝的注册、充值和付款,培养团队意识和自主学习能力,我主要采用以下几种教学方法:

1、任务驱动法的灵活运用

任务驱动的显著特点是“以任务为主线、教师为主导、学生为主体”,创造以学定教、学生主动参与、自主协作、探索创新的新型学习模式。

在本课例中,每课时均创设一个真实的支付宝情境,如注册、充值及付款等,使学生能够带着真实的学习任务进入真实的学习环境,这样能够显著唤起学生原有认知结构中有关支付宝的知识、经验及表象,通过对新知识的同化吸收,形成支付宝独立运用的能力。

任务驱动法还能够促使学生形成自主学习和协作学习能力,在本课例中,每课时均设置了教学资源包和小组学习任务,倡导学生之间的讨论和交流,通过不同观点的交锋,补充、修正和加深每个学生对支付宝相关问题的解决方案。在效果评价方面,一方面是对学生学习支付宝的意义构建进行评价,这主要是通过学生的课堂作业来体现;另一方面是对学生自主学习及协作学习能力的评价,这要从小组的课堂表现及结果进行评价并给予适当奖励。

2、创新的课堂导入及评价机制

作为技能新授课,本课例是生动有趣的,这首先体现在导入设计上。支付宝的注册、充值及使用等课程,每课时均设置了视频、小品或生活事件讨论,通过这些多媒体手段或生活情境手法的运用,能够快速吸引学生的学习兴趣,调动课堂气氛。


而在学生的学习评价中,因为学生的实际上机操作过程难以用纸质作业记录,本课例创设了截图上交操作界面的方法,这种方法能够快速真实的记录学生的各个操作步骤,为教师提供及时的教学反馈,形成快速准确的评价机制。

3、网络资源、多媒体技术的有效利用

本课程的开展依托于互联网,从支付宝的注册、充值及付款,到学生各项互联网操作技能的运用,如浏览器、电子邮箱等的使用,在一定程度上锻炼了学生的现代信息技术综合运用能力。另外,在课堂任务中本课例设置了相应的教学资源包,使学生在书本之外学习更多的支付宝知识,这一切都得益于现代信息技术的发展。值得一提的是在支付宝的充值课程中,实拍了一段学生到网点进行充值的视频,这在很大程度上推动了学生的学习积极性,多媒体技术为我们的课堂带来了无限的乐趣和魅力。

4、无限延伸的课堂

学习知识和技能,仅靠课堂是远远不够的,作为教育者,我们更多的是希望授之以渔,通过教学资源包的运用,引导学生充分利用互联网资源进行拓展学习,把课堂无限延伸下去,这对于学生特别是课外时间充裕的职中生来讲是一片更大的天地。

总之,电子商务近几年的蓬勃发展,给电子商务专业的建设和发展提供了千载难逢的机遇。做好教学改革工作,建设好电子商务专业,是我辈电子商务从教者的历史使命,任重道远,仍需努力! 

参考文献:


- [1] 余浩,陈年友.《基于教学做合一的方法研究》[N].《黄冈职业技术学院学报》.2012-04-28.
- [2] 孙启新,钱抒.《高职院校室内设计课程教学方法》[J].《教育与职业》,2012年,3月刊:P17
- [3] 赵金龙.《以就业为导向,培养电子专业应用性人才的实践研究》[J].《教育前沿(综合版)》,2008年,9月刊:P25

作者简介:孟飞,东营市技师学院讲师,电子商务专业教研组长、专业负责人。

(上接第32页)

2. 在路由器禁掉ICMP。在路由器禁掉ICMP,虽然无法完全消除DDoS入侵,但是可以有效的防止攻击规模的升级,也可以在一定程度上降低攻击造成的危害。

3. 打开路由器日志,查看哪个路由器收到的攻击数据包最多。根据路由器日志所记录的数据包来源的IP地址,确定哪个网段的资料量最大。在这个路由器上调整路由器针对这个网段为“黑洞”状态,并用修改子网掩码的方法将这个网段隔离开。接下来为了让服务和合法流量通过,你可以将其它一些攻击情况较轻的路由器恢复正常。

对于DDoS的攻击,由于其攻击的突然性和数据流的无限膨胀性,至今在网络安全界还没有找到绝对有效的方式来杜绝。网络管理员平时必须要留意防火墙或其他安全设备的异常情况,及早发现系统存在的攻击漏洞、及时安装系统补丁程序,以及不断提升网络安全策略、经常检查日志情况,做好各个环节的防护措施,争取在攻击泛滥前及时采取有效的应对措施,才能保证网络安全顺畅。 

参考文献:

- [1] (美)麦克克鲁尔,(美)斯坎布雷,(美)克茨.黑客大曝光:网络安全机密与解决方案(第7版)[M].清华大学出版社,2013
- [2] 刘建伟.网络安全实验教程[M].清华大学出版社,2012
- [3] 王煜林,田桂丰,王金恒.网络安全技术与实践[M].清华大学出版社,2013

作者单位:惠州市技师学院