毕业论文(基于对抗的网络攻防实践)

三亚学院

本科生毕业论文（设计）

论文（设计）题目：基于对抗的网络攻防实践

分　　院：理工学院

专　业（方　向）：软件工程

年　级、班　级：0801

学　生　学　号：

学　生　姓　名：

指　导　老　师：杨婷婷

2012 年 5 月 17 日

论文独创性声明

本人所呈交的毕业论文（设计）是我个人在指导教师指导下进行的研究工作及取得的成果。除特别加以标注的地方外，论文中不包含其他人的研究成果。本论文如有剽窃他人研究成果及相关资料若有不实之处，由本人承担一切相关责任。

本人的毕业论文（设计）中所有研究成果的知识产权属海南大学三亚学院所有。本人保证：发表或使用与本论文相关的成果时署名单位仍然为海南大学三亚学院，无论何时何地，未经学院许可，决不转移或扩散与之相关的任何技术或成果。学院有权保留本人所提交论文的原件或复印件，允许论文被查阅或借阅；学院可以公布本论文的全部或部分内容，可以采用影印、缩印或其他手段复制保存本论文。

加密学位论文解密之前后，以上申明同样适用

论文作者签名：　　日期：　　年　　月　　日

摘　　要

当今世界,信息是无形的重要资源，信息网络化促进现代社会的快速发展，正在影响到商业、工业、教育、政府、国防等各个领域的变革，电子商务、电子政务、远程教育、电子军务、数字地球等相关新概念不断出现。

目前，信息网络的日益发展已让“地球”降格变成了“村”，天涯近在咫尺，一切近可企及，沟通肆意畅快.正是因为网络的飞速发展，在给人们带来巨大的利益和便捷生活的同时，也伴随着许许多多安全问题，这些问题有的可以顷刻间造成数十亿乃至数百亿的经济损失，有的甚至可以危害到某个国家的国防机构，对地球生命造成致命的危险，以致于酿成一场灾难。所以网络安全的研究，在当代社会，是一个不容忽视的课题，网络安全的更好的发展，可以为以后地球科技进化的方向和发展提供更加完善的环境。

网络攻防作为网络安全领域中的一个子集，对于它的研究是非常有价值的。网络攻防技术在对抗中的螺旋式发展，很大程度决定了网络安全领域的前进方向及各种安全标准的制定。由于网络攻防技术是目前唯一不能从实践中反馈信息的工程技术，所以为了减少学习攻防技术的成本，攻防技术的仿真模拟就显得更加重要和迫切。

【关键词】网络 信息 对抗 攻防 安全

Abstract

Nowadays,informations is the important and invisible resource,the modem society have been rapidly progress and fast development by the information networking, and the information networking is effecting revolution of many area of modem society,such as education,commerce,industry,government,national defense,as result of the new concept was born one after another,such as e-business,EG ,e-military affair,remote eduction,digital earth.

At present,the rapid development of information network have made the rapid development of the network ,network become a double edge.it can bring huge profit and convenient life,but it have many security issues,some of the issues can lose billions and even ten billions property in a moment,some even can threat institution of national defense,it's a disaster for life of earth.Therefore,the research of network security is a task which can't be ignored in modem society,the better it is developed,the more perfect milieu for the technical progress and development.

It is a much valuable research for network attack&defense(A&D) which is a subclass of network security.The network A&D technique has a spiral development by counterwork,then,it is so important for the network security to where it will go,and draft a variety of security standards.Because network A&D technique is a unique project technique which can not get feedback from practice,we should use the simulation condition to learn the network A&D technique ,then,we also cut down much cost for leaning technique.

【Key Words】 network information security counterwork attack defence

目录

1 绪论

1.1 选题背景

以 Internet 为代表的信息化浪潮席卷全球，信息网络技术的应用日益普及和深入。伴随着网络技术的高速发展，各种各样的安全问题也相继出现，网络信息资源的安全备受关注。保证网络系统的保密性、完整性、可用性、可控性、可审查性方面就显得非常重要。

目前，因为网络的开放性、黑客的攻击和系统本身的缺陷导致网络内的计算机并不安全，网络入侵也经常发生，往往造成严重的后果，为了尽早恢复网络或系统的正常运转，降低入侵的风险成为了急待解决的问题。由于攻防实验技术以入侵技术为前提，因此防御实验存在着时间滞后性。使得攻防成为一堆对立且统一的矛盾体，攻防实验也成螺旋状态不断地发展变化。

正是因为网络的迅速发展及网络安全问题的日趋严重，使得网络变成了一把“双刃剑”:用得好(安全可靠)就获益良多，用得不好(漏洞百出)就会贻害无穷。在全球化竞争的大环境之下，作为最为重要的信息、载体的支撑平台一一计算机网络，其自身安全已日益成为备受关汪的核心和焦点。网络安全作为国家安全战略的重要组成部分，其重要性毋庸置疑也自不必说。

。

1.2 研究现状

世界各国(机构、组织等)当前对网络安全的研究仍然侧重于技术和管理方面的传统层面探讨，但是传统的研究思路几乎雷同、鲜有新意，无非是技术或管理方面的宣讲。总体上给人以“不识庐山真面目，只缘身在此山中”的感觉，不能从宏观上全局把握网络安全的现实尺度。

国内对网络攻防的研究表现为信息战、网络战等，其注意力是军事战场上的信息和网络系统的较量，代表性的成果是我国著名学者沈伟光的信息战思想。大多研究侧重在管理层面上讨论，涉及的技术层面相对较少。国外对网络攻防的研究明显倾向于理工科式的逻辑思维，不少专家、学者从各自学科领域的角度阐述网络对抗的思想，出现了许多对抗模式、模型来解析对抗这一博弈过程;将攻防看成是跨领域的课题予以探讨，重点仍是孤立地研究单独的攻击或防御的数学模型、体系结构等，对攻防的整体性把握仍有欠缺。对于网络安全，比较而言，国内研究的是重点领域(军事)，国外探索的整个人类社会的全过程、多领域，前者比较细致但不精确，后者比较全面但不专一。很少有人专门把攻击和防御作为一个整体、一对矛盾单独考察，也鲜有文献或著作把攻防当作一门独立的学问或艺术予以研究。以前的研究总是将这本是一体的事物割裂开来加以讨论，得出的结果往往就是“矛与盾”的评价。网络安全本身就没有固定的尺度和科学的标准来衡量，迫切需要新的可视化的标准对其规范(或参照)。

1.3 论文的主要工作

计算机网络入侵会给系统带来灾难性的后果,为了降低网络入侵带来的风险，可以运用网络攻防实验来模拟网络入侵。本文阐述了攻防实验是对系统风险评估的有效手段，是信息安全技术的重要组成部分。攻防实验在刚起步的时候仅仅是对信息安全技术的有效提升，而之后它的重要性会逐渐增加并开始成为信息系统

风险评估的重要技术补充。重点从技术的角度叙述了攻防实验的主要方法，从而使攻防实验井然有序地进行。

2 网络攻防与安全

在网络领域里，安全和攻防有着天然的联系。在网络对抗上，攻防最终的效果直接决定了网络的安全结果和性能。

2.1 网络攻防

攻防本是一体:攻击即是防御，防御也可以是攻击;二者你中有我、我中有你。在网络安全领域，攻防(攻击+防御)具有天然的、身份突出的“非对称性”。攻击者总可以“攻其一点，不及其余”，为达攻击目的甚至可能“无所不用其极”;而防御方却不得不面面俱到，时刻担心哪怕有极小的疏忽大意便会导致满盘皆输。

1、攻防技术非对称

操作系统、应用软件、网络协议等不可避免地存在和隐藏了大量漏洞和脆弱性，而这些漏洞信息和脆弱性资料在 Internet 上几乎完全公开。针对这些漏洞和脆弱性，攻击者不但自行开发了有力、针对性强的攻击工具、入侵软件，还完善了详尽的教程，使得计算机应用初级水平的人都可以掌握这些看起来很复杂的攻击行动。攻防技术之间的知识不对称，即攻击者所获得的攻防对抗知识总是大于防御者。这个不对称包含两个方面的原因：①每个防御措施必定针对一个漏洞或者攻击技术，但并非每漏洞或者攻击形式都存在相应的有效防御，同一漏洞可能存在很多种攻击方式，增加了对攻击行为的预测难度，相对于攻击知识，防御措施总是有一定滞后。②虽然是从攻防对抗中获取知识，但由于攻守地位的不同，防御者需要掌握所有的攻击技术和漏洞信息才能达到与攻击者相平衡。

2、攻防成本非对称

一台再普通不过的计算机、一条极不起眼的网线就可以组成有效的攻击工具，一个普通的攻击者可能顷刻间就能使许多人花费大量人力、物力、财力建设起来的网络失效或瘫痪，入侵成本极低。如在一个销售攻击工具的网站价目表中，一个分布式拒绝服务(DDoS)攻击软件为1500元，除去计算机等一次性购置成本和微不足道的网络资费外，这几乎是一个攻击者所需要花费的全部成本，但DDoS造成的破坏则可以使一个电子商务网站在数天内损失几百乃至上千万元的营业额。

除技术成本低廉外，攻击具有很好的隐蔽性，攻击者的风险成本也极低。不同于攻击物理设施，对网络系统的攻击不需要物理、位置上的接近。攻击者可以来自世界上的任何地方，跨越多个通信网络，可以有效掩盖其身份和位置，而追踪这些攻击却非常困难且耗时极多。就当前的技术水平而言，针对网络攻击还缺乏卓有成效的反击和跟踪手段。一些经验丰富的攻击者往往通过控制“宿主”机实行远程跳跃式跨国、跨洲入侵，防范难度大为增加。对国家安全来说，攻防成本的非对称性还有着特殊的意义。一些实力弱小、尚不发达的国家(或地区)很难承受军事进攻的巨额成本，但借助网络攻击，他们获得了极大的攻击机会和空间。他们不用劳师动众、兴师远征，也不费一枪一弹，就可以轻易撕破对手依靠传统国防力量构筑的国家安全屏障。

3、攻防主体非对称

网络攻击者掌握主动权，而防御者被动应付，攻击者与防御者处于非对称状态，前者占据有利位置。另外，依靠网络的级连和放大作用，单独的个体就可以向信息对抗中强大的另一方发起攻击。

4、攻防信息不对称

攻击者在攻防对抗知识上有自身的优势，但在目标系统信息获取上往往还只是一个盲目搜索和攻击试探的过程；而防御者虽然熟悉自己的安防系统，但却无法预测攻击在何时、何地以何种

方式进行，只能全面考虑所有可能的攻击，针对存在的弱点处处设防、时时警惕。

正是由于攻防中这些“非对称性”的存在，致使网络安全的衡量需要一个“有效”的标准，所谓“有效”保证网络的安全，是指为了有效保护网络的资源(有形或无形资产)，应尽可能地降低资产受危害的潜在代价;与此同时，由于采取了安全措施，也要付出相应的安全的操作代价(安全成本)。过高的安全强度带来过高的安全代价，有时甚至得不偿失，而过低的安全强度又不能对攻击(入侵)产生足够的压制和打击，危险并不能抵御和消除，二者皆不可取。因此，必须综合权衡管理的复杂性、对系统的整体影响性、对不同平台的支持性、技术的可实施性用户的方便程度等诸多因素，在安全强度和安全代价之间找到合理的平衡点，达到最高的“安全性价比”。

2.2 网络安全

网络安全是安全在网络中的反映，直接反映网络的可靠性、可信度。绝对的网络安全是永远都不存在的，能有效抵御外部入侵和攻击的网络系统是可接受的“安全”。总之，网络系统是否安全，最终都必须接受网络攻击的检验。网络自上世纪 90 年代后期迅猛崛起和高速发展以来，对于世人还是个新鲜事物，有许多未知和混沌的领域等待人们去发现和研究。网络本身不断变化、延伸、发展，和诸多学科交叉、融合，衍生出众多新概念、新体系、新技术。对网络的攻击总是层出不穷、花样繁多，网络的防御同样也是应运而生，网络安全就在这样的交替中动态地演变、发展。网络安全问题的产生很有戏剧性:多协议、多应用、多用户、多系统组成的网络环境，复杂性高(越复杂，安全性就越低)，开放性强(越开放，入侵就越容易，保密就越困难)，分布性好(越分散，越难发现攻击者)，可用性高(应用越多，潜在漏洞就越多)，

互联互通性良(联通越容易，攻击也就越容易)，跨平台强(操作系统越多，自身安全脆弱点就越多，防不胜防)……可是，假如去掉了网络的这些优越性，网络马土失去了最核心的价值，其强大的生命力立即丧失!网络安全网络是不断发展、永远变化的事物，而安全系统必须跟上这一变化并随着同步发展，这就要求安全对抗、攻防技术也不断进化、发展，自身必须象人一样不断地学习、“充电”，否则就会过时、落后而遭到无情淘汰。网络安全象人一样拥有记忆性、智能性、是安全系统必然的选择:不断学习新的对抗机理、新的安全技术、新的攻防手段，能自动识别安全漏洞、潜在威胁等，网络系统才有可能保持生命力。

2.3 攻防与安全的关系

大量研究发现:网络安全的最终结果必然会归结到攻击和防御这对最为实际的行为上来，不论研发者如何研发“攻击”或“防御”的新技术、新手段，网络安全的质量和效(Quality&Benefit ，记为 QB)就是攻击(Attack ，记为 A)和防御(Defense ，记为 D)相互作用、彼此抵消的最后结果。用公式表达为:

QB=D— A(即“安全质量效益一内部防御力量一外界攻击实力”)

当 D>A时，QB处于正值，网络是安全、可信赖的;

当 D<A时，QB降为负值，网络是危险、不安全的;

当 D=A时，QB为 0，网络安全处于临界状态。

实际上，安全是非常复杂、多领域、多学科的网络问题，牵涉面非常广泛，绝不是这么简单的线性关系式所能准确表达的，但该公式在理论上仍具有一定的参考、概括价值。