黑客防线

2002（上册）

精华本

双光盘

http://www.hacker.com.cn

超值：60例《黑客防线》原创全程攻防录像演示

赠送：2001年《黑客防线》精华本的电子版

超值大奉送

- 名家专访
- 专题综述
- 系统安全
- 服务器安全
- 数据库安全
- 网站安全
- 网管之家
- 编程解析
- 安全方案

- 经验交流
- 病毒前线
- 拒绝服务
- QQ专栏
- 恶意攻击防范
- 案例分析
- 攻防工具
- 网吧攻略
- 密界寻踪

人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

黑客防线精华本

2002（上册）

《黑客防线》编辑部　编

人民邮电出版社

图书在版编目（CIP）数据

《黑客防线》精华本.2002/《黑客防线》编辑部编.
北京：人民邮电出版社，2003.2
ISBN 7-115-10806-4

Ⅰ.黑… Ⅱ.黑… Ⅲ.计算机网络—安全技术
Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2003）第 000465 号

内容提要

《黑客防线》是一本网络及计算机安全普及性电子媒体，致力于中国网络安全和计算机安全事业，从创刊至今，深受读者喜爱，发行量直线上升，呈良性发展趋势，在业界和网络安全界影响较大，深受读者关注。

《黑客防线》精华本由《黑客防线》2002年全年内容浓缩而成，经过编辑重新加工，按照文章内容和梯度进行了详细分类；全书内容通俗易懂，涵盖面广，突出实用，更加便于读者阅读、学习和研究。书中重点涉及了人物、专题、系统安全、服务器安全、数据库安全、网站安全、网管心得、案例、编程、工具、破解、病毒分析、网友交流等20个方面。

本书附赠2张配套光盘。光盘中包括书中涉及到的不便于书面印刷的所有代码和大量流行的经典工具、技术文档、系统最新补丁；更有价值的是收录了《黑客防线》原创全程攻防录像演示和2001年《黑客防线》精华本的电子版。

黑客防线精华本2002（上册）

编　　：《黑客防线》编辑部
责任编辑：魏雪萍

出版发行：人民邮电出版社发行　北京市崇文区夕照寺待14号A座（100061）
读者热线：（010）62141445-8013
印　　刷：中煤涿州制图印刷厂
经　　销：全国各地新华书店

开　　本：787×1092　1/16
印　　张：36
字　　数：2800千字
2003年2月第1版　　2003年2月北京第1次印刷

ISBN 7-115-10806-4/TP·3185

定价：35.00元（上下册2CD）

目 录

走近袁哥

访中联绿盟信息技术公司袁仁广

本刊记者 / 秦丁可

一个在中国网络安全界内无人不知的名字，一个在谈到与中国黑客相关话题时“点击率”极高的“关键词”，公认的中国网络安全及黑客界最高层次技术精英的代表之一，为国内网络安全技术发展做出重要贡献的关键人物，微软 Windows 系统底层分析发现 Windows 9x 共享密码、IIS 等系统漏洞第一人，所有这些冗长的“定语”都为修饰同一个“主语”：袁哥！

袁哥真的很出名，知道其本名“袁仁广”的人不很多，但一提“袁哥”在圈内快应了那句广告词儿：“地球人都知道！”，在网上任何一个中文搜索引擎敲入“袁哥”二字，就会有上千个相关链接。在网络安全与黑客的社会知名度越来越高的今天，这种出名还表现在圈外人对他的认知，很多人对网络安全很外行，但知道有“袁哥”这么一个“牛人”，正如从未上过网的人对互联网的认知，人们通过一些传统媒体的相关报道知道了 2000 年夏天那次中国黑客首度大聚首，也或多或少记住了袁哥的名字。或许社会上太多构建在炒作、包装之上的“成名”令人们开始习惯对一切名誉光环中极易蒸发的水分产生“盛名之下难符其实”的本能怀疑，但袁哥的“成名”却是一个无心插柳柳成荫的自然过程，很大程度上缘于伴随互联网而兴起的网络安全技术的发展，所谓“时事造英雄”，在袁哥与网络安全技术的关系上是又一个集中体现。这种“成名”也是因人们对科学攻关与技术钻研者的敬佩心理而自发树立与传播的结果，而不是“成名”者的本意，诚如袁哥在接受我们采访时所说，我过去、现在和将来都只为个人兴趣而从事这份工作，对成名我从不看重，更不是我努力的初衷。这也是为何“成名”数年来他绝少与各类媒体接触的重要原因之一。难得的是我们终于通过努力得到了采访他的机会，希望在此为读者展示袁哥的一个真实侧面。

初见其人

四月底一个春风和煦下午，我按约来到位于京西北洼路比邻香格里拉饭店的益泰大厦，在这个较众多京城高档写字楼很不起眼儿的建筑物的五层，却进驻了一家全国网络安全最起眼的企业，那就是中联绿盟。说到袁哥就不能不提一句中联绿盟，可以说，2000 年袁哥的加盟，令绿盟如虎添翼，实力大增，而绿盟亦给予袁哥在网络安全技术领域一展才华的宽阔舞台。

步入绿盟的办公区，所看到的室内装修、陈设与办公设备如普通公司一样并无特别，惟有满目的绿色提示着企业文化的主题。

负责此次采访联络工作的市场部盛男小姐见到笔者后一边热情寒暄让座一边拿起电话通知袁哥出来接受采访，在盛小姐去为笔者倒水的片刻，一位身材不高且较胖的男士由一间办公室走出，从笔者所在办公隔板傍的走廊经过，我们双方的目光随意瞬间交错后都自然地移开，我完全没有意识到此人与我今天来这的目的有任何关系，直到片刻后盛小姐对着折返回来再次路过这里的他叫道“袁哥！”，我楞了一下后才反应过来，他就是今天的主角，握手的时候我不再怀疑：我真的见到了袁哥！袁哥个头不高、较胖，发型随意，浓眉大眼，肤色微重，一件天蓝色衬衫，一条深蓝色西裤，质地都极普通，我特别注意到他腰间那条有点“爆皮”的皮带，很陈旧的样子，让人感到他对穿着的极端随意，沉稳凝重的神态与思辨机敏的目光，使他整体上看去要比实际年龄成熟许多。短短几句寒暄，他带有浓重川味的普通话平易中透着朴实。盛小姐将我们让到一个小会议室，蓝色的四壁与办公家具凭添了一种静谧安详的交流氛围。落座后，我按下数字采访机的录音按键，开

始了与这位网络安全奇才的对话。

用“反汇编”解读事业成功的“代码”

话题很自然地从袁哥网络安全技术的最初入门开始，袁哥至今认为，中学时代自己对数学的着迷与投入炼就了自己严谨缜密的逻辑推理和分析能力，进入大学后，在以汇编语言为主的计算机系统底层学习钻研的经历又为他今后在包括网络安全在内的众多计算机技术研究打下了坚实的知识基础 。

“刚上大学时，还没有机会接触网络，但那时就对单机上的电脑病毒和加解密技术产生了强烈的学习研究兴趣，掌握了相当的汇编语言能力后，我就常找来一些当时流行的病毒，把它们的源代码反汇编出来逐行研究，甚至还包括一些防毒卡的加解密原理，我都想搞个清楚，事实上直到我现在做的这些分析 Windows 下系统漏洞的工作，用的还是这套基本功，就是要阅读和分析源代码！说起来好像挺简单，但实际上这对分析者阅读及分析代码的能力要求非常非常高！为什么有些技术人员虽然也具备一定的汇编语言能力，但分析起来仍感吃力，说明这种阅读分析能力还是不够熟！因为代码量非常之大，有时表面看去很小的程序反汇编出来的代码量仍很可观，如果阅读代码能力强，便可在短时间看一遍后迅速搞清程序结构与编程设计思路，预感到有可能出现问题的地方，从而重点地去分析这些地方的代码。数学对锻炼我全面严谨的思维方式帮助很大，因为分析漏洞是个要求很细致和全面的工作，考虑问题一定要细，要全面，别人没想到的，你要想到，别人容易忽略的你不能忽略掉，这样漏洞才会被你而不是别人发现，或根本谁都没发现。现在回想起在学校那段经历也觉得挺不容易，那时因条件限制上机机会少的可怜，上机时反汇编出来的代码不可能当场分析出来，也没有打印条件，只好一行行抄在本子上拿回宿舍细读，这一抄就是成百上千行，老实讲大学四年我的大部分时间都用在学计算机上了，大学课程没太认真投入地学，这也是没办法，这并不是说我认为大学课程全不重要，我觉得一些重要的基础理论知识还是应该认真掌握的。但说起这个话题有一点让我对大学教育感到很失望，这个阶段本应该是鼓励和培养学生从兴趣出发的主动自学能力，这样对开发学生的创新能力很有好处，也为以后工作打下好的思维方式的基础，而事实上中国的高校教育还停留在学生被迫去上课学很多自己不感兴趣的东西的状态，这种照本宣科的教学方式真的效果有限，可以讲我对大学上课四年最深的印象就是老师上面讲，学生下面睡觉。”

图为袁哥在接受采访中

我可以想见大学时代袁哥的样子，一个表面上再普通不过的理工科学生，在学习条件远不及计算机专业学生的情况下顷注了全部精力醉心于计算机知识研读，可能在本专业课老师的眼中这是一个“不务正业”的学生，但是现在看来，如果他是个很“本分”的好学生，那也许在母校不计其数的优等生中又多了无足轻重的一员，但今天的中国网络安全界却少了一个叱诧风云的专业奇才！

微软 Windows 共享及 IIS 系统漏洞是袁哥的“成名作”，谈及发现过程，他的语气依旧平静，毫无一点兴奋，更不要说得意了，像是在谈论别人的事情，

“刚到公司（绿盟）时因为我们的定位就是要做服务，所以就意识到必须要对系统安全配置以及漏洞十分地熟悉和掌握，大家就根据自己的特长选题入手分析研究，我个人觉得自己对看代码和反跟踪比较熟，逆向分析有一定能力，就先选了 IIS，看它的安全性，如果发现问题就可有针对性地补漏，当时是 2000 年，分析了几个月后就发现了这些结构和配置上的问题，那时是在 Windows NT4.0 下的 IIS4.0，还没有现在 Windows 2000 及 IIS5.0 应用这么广泛。”我没想到他在说这件事时话这么简短且没有任何评论，说得就像普通网友在网上论坛发个贴子那么简单和随意，这个令世界软件巨人微软吃惊与汗颜继而帮助无数企业和个人用户避免重大网络安全隐患的技术发现就这样被发现者自己轻描淡写地一笔带过了。袁哥就是这样一个不太

喜欢评价他人与讲述自己的人。作为访谈对象，他令采访者感到有些“难度”，但有“难度”话题也得继续，因为对他的了解才刚刚开始。

从痴迷数学到与网络安全结缘

上面说过，袁哥求知道路上的“初恋”是数学，如果不是因计算机而“移情别恋”，他的数学家之梦也许会有朝实现，至少可能会一直做下去。但计算机彻底改变了他的人生轨迹。对于由痴迷数学到醉心于计算机学习的“情变”过程，袁哥言语中多少留露些许留恋与无奈。

“虽然一直喜爱数学，但渐渐地感到如果选择数学研究作为自己未来的发展方向，那将意味着终身从事一种基础理论的研究，也难免枯燥，如果不能有重大的研究成果和理论发现，那从某种角度上讲也意味终生一事无成，还不如做些很具实用价值的工作，而恰在上高中时接触了苹果电脑，马上产生了浓厚的兴趣，并且计算机学习又最得益于数学的思辨方式，更重要的是我也感到了计算机科学未来广阔的发展前景，再加上感觉很有趣味性，于是转了过来。初次接触病毒感觉很神秘，就有强烈的想搞懂的愿望，这就要过第一道难关，那就是汇编语言，当时我读的计算数学系是不开这门课的，就只能自学，而自学对我来说已经习惯了，就像当年自学数学一样，而且两者也有很多相通的地方，一直以来，我对自己的自学能力还是挺有信心的，其实对于从事网络安全技术研究的人来说自学能力与上面提到的代码阅读能力、推理分析能力一样重要，特别是在没有先例与他人经验借鉴的时候，就尤为重要。”

本来我准备了一个这样的提问：“要在网络安全技术领域做出成绩，最应具备哪些素质与能力？”袁哥上述的话已清楚的做出了回答，简言之就是浓厚的兴趣加很强的自学能力以及不懈的努力，这对现在那些有着与当年的袁哥同样兴趣和志向的少年们是很好的启示与经验之谈。紧接上一个问题在谈到自己“成名”前后有无变化时袁哥提出了更为深刻的忠告：“我从未觉得自己成了什么名！也就更谈不上有何影响，我的心态也没有发生任何变化，我觉得从事这项技术工作必须得能静下心来，老老实实专心看代码才可能有所收获，要耐得住寂寞，以我个人的体会觉得，一个人只要认准自己感兴趣的事然后尽自己最大的努力专心去做，就一定会有比较好的结果，而在选择和决定自己发展方向的时候最不好的就是盲目追赶潮流，现在时兴什么，大家都在做什么我也就跟着去做，或是出于一种很虚荣的目的去做，而不认真思考自己真正的兴趣与特长是什么，再缺乏必要的充分准备与知识积累，这样很难成功。比如我当初一点没有想到自己会在今天很热的网络安全领域从事研究，我只是从自己的兴趣出发去学习这些东西，而且，如果不是在校时对病毒、加解密感兴趣进而在汇编语言等系统底层知识上下大功夫，打下好的基础，就是赶上现在的机遇也没有能力胜任。所以，首先是自己喜欢的事情，也有一点能力，再努力去做了，就会有一个瓜熟蒂落的自然结果。”

有关网络安全的个人看法

作为网络安全技术开发与服务企业的从业者，袁哥在绿盟这几年对国内企业的网络安全状况应是很有发言权的：

“前两年企业用户可能从网络安全意识到技术上都比较薄弱吧，我们去给他们做项目的时侯看到的情况基本都是系统设备刚买回来时的初始设置，几乎没做一点安全方面的配置修改，有的甚至连操作系统的补丁都不知道打，现在大家的网络安全意识普遍增强了，也知道关闭一些隐患明显的端口和服务，但是技术环节上还有很大的欠缺，相比较而言，国内较大的骨干网络或企业网络系统因有较一定的安全意识与技术能力，做得还是不错，配备有相当技术能力的专职网络管理员，也能经常关注类似绿盟这种专业公司网站上的“系统漏洞公告”和安全配置方面的技术文章，再针对自身网络情况进行安全维护。现在看来意识是普遍有了，但企业网管的技术能力还急需大大地提高，目前高水平的人才比较缺乏，在这方面我们绿盟也尽企业所能做了很多客户培训与技术支持工作。大批的中小企业网络系统的安全状况更急需有大量的工作要做，可能企业出于成本考虑，不太舍得在网络安全方面增加投入，想在这方面省下点钱，但实际上到头来反而有点得不偿失，现在越来越多的企业决策者意识到网络安全方面的投入是非常必要的，说来这还是个观念问题。”

谈到企业网络安全问题的长久解决方案，袁哥又继续说道：“开始阶段如果单靠企业自身的能力

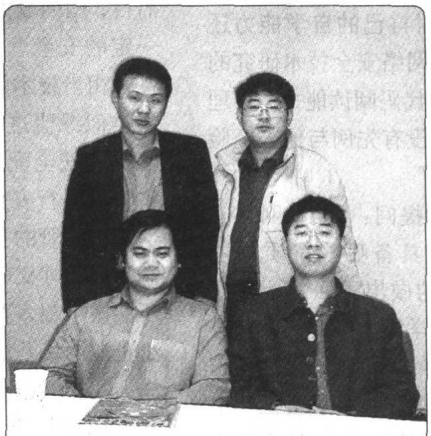
构建较专业完善的安全体系不太现实，构建速度也会很慢，这时需要象绿盟这样专业的网络安全公司为其设计搭建一个基础解决方案平台，并负责一段时间的后续技术支持服务，但长远的网络安全工作还是必须依靠企业培养出自己的高水平技术人员。企业对于自身的网络安全建设千万不能有一次投入笔钱全交由网络安全厂商包办的依赖感和一劳永逸的想法，网络安全不是买几套防火墙再做些系统安全配置就万事大吉的事情，网络安全是一个庞杂和永远动态变化着的系统工程，刚配置好的系统暂时可能是相对安全的，但随着软件升级、系统更新以及网络攻击手段的变化，新的安全隐患和系统漏洞还会显现，你又必须重新评估其安全可靠度，继而有针对性地重作安全配置，这也是计算机网络科学本身的规律决定的，完全依赖厂商和产品的结果就是忽视了人的关键作用，从而放弃了对人才的培养，这是要不得的，是完全错误的。企业一定要寻求一种整体的解决方案。”

对于中国网络安全与西方发达国家的差距袁哥个人认为总体上的差距还是有的，但也分具体领域，有些要求有基础积累与经验积累的领域，比如管理理念和法律法规建设，差距会大点，也是需要时间的，而对于一些具体安全技术本身差距虽有，但不大，赶上也快些、容易些。中国在人才资源上和个体能力水平上是从来不差的，就是一个如何充分开发和利用的问题，这牵扯到一些非技术性因素，包括管理体制问题。

袁哥与绿盟

袁哥与绿盟可谓分别是中国网络安全领域中优秀个体与强势集体的代表，两者的结合更让人有强强联手的夺人气势。那么袁哥加盟绿盟的前前后后自然也是令人关注的话题，回忆旧事，袁哥记忆犹新，尾尾道来：

“1997 年我大学毕业后分配到海信集团，具体工作是电视机单片编程，工作不是很忙，所以我业余时间就看一些自己感兴趣的操作系统的书籍，主要是微软的 Windows 系统。那时互联网也刚刚兴起，我不仅多了一个获取技术参考资料的手段，对互联网技术本身也产生了浓厚的兴趣，于是就开始学习分析 TCP/IP 这类的网络协议，看它的实现，再反汇编一些 Windows 下的程序来看来分析它，在分析代码的过程中就现发了一些漏洞，比如 98 年发现的 Windows 9x 共享密码漏洞，由此让我发现原本只为搞清代码内容的动机却无意中得到如此有趣的意外收获，感觉挺神奇，继而就想到自己是不是就试着向这方面发展，以后就特别关注互联网上这方面的东西，而在认识到这是一个很好的发展方向后就开始考虑专门从事这方面的工作了，但那时国内专业的网络安全公司还不多，所以经历了一段等待的过程，到 2000 年时，我这种转行的愿望已非常的强烈和急切，于是 2000 年春节我在绿盟的网页上贴了一个自己想‘跳槽’贴子，刚好被绿盟的沈总看到，他很快就给我打了一个长途，约我面谈一下，正好春节放假，我就来了北京，一来和他谈，二来也想实地看看公司环境，结果一谈感觉氛围很好，当时绿盟正是初创起步阶段，而发展定位正好与我的想法吻合，我就决定留下来了。在此前也曾与一位作杀病毒软件的企业老总有过类似接触，但最终选择去了绿盟主要是看好公司的环境和发展前景，且更适合自己的兴趣和能力，现在看来当初的选择是明智正确的，绿盟今天的成绩说明这确是一个有技术实力和发展前途、经营管理与运作机制都很健康的公司。来绿盟后我一直负责 Windows 下的案件研究，最初是 IIS 漏洞分析，然后就是别的一些系统服务和常用软件的漏洞研究，现在还准备就多年来分析查找漏洞的规律和经验进行一些归纳总结，并为实现一种利用计算机程序自动化查找分析系流漏洞的方法进行研发，比如用软件代替人眼和大脑进行一些代码的分析，这样就不会象自己当初看代码那样辛苦了。应该说绿盟在网络安全产品开发上与服务是并重的，二者也是相附相承的，开发出了过硬的产品，才可以围绕产品更好地为客户服务，绿盟的网络入侵侦测系统(NIDS)、主机入侵侦测系统（HIDS）、远程安全评估系统(RSAS)、高性能防火



图为袁哥（前排左一）与本刊编辑部人员合影：前排左二：执行主编郭聪辉，后排左二：编辑部主任肖亦然，后排左一：本文作者。

墙(SFW)、抗拒绝服务产品(COLLAPSAR)、个人防火墙(GREENGUARD)都是比较优秀网络安全产品。绿盟在技术研发队伍的能力上也是有一定优势的，这也是得到圈内认可的，但我要强调的是这绝不是我个人或其他少数几个人的能力所能达到的，这需要公司所有人的智慧，我们是一个团队！现在计算机软件开发与技术研究早已告别个人英雄主义的时代，个人能力只有与团队其他成员的智慧很好的融合才能充分体现其价值，提升团队的整体竞争力，我总是爱说这句话：'个人价值汇聚成团队价值后再平分下来要大于个人原有的价值，这里有一个无形的增值！'绿盟最吸引我的地方就是这里的工作氛围，很年轻很有朝气，没什么职务等级观念，大家工作中都很自然地保持着朋友般的融洽关系，现在人才流动很大，如果有公司找我去，薪金条件不会是我惟一或说最主要的考虑因素，我会很看重企业发展前景与自己发展空间，还有就是工作环境，现在绿盟工作心情很舒畅，公司为了我能专心从事系统分析工作，很多甚至与技术相关的杂事儿都不让我来做，同事之间的工作配合也很默契，感觉自己在这里的事业发展还有很大空间。"就在这次采访后的第三天，笔者在与一位网络安全界朋友聊天时还得知这样一件事：绿盟曾因一度资金问题；连续三个月没发员工工资，但从袁哥这些技术骨干到其他普通员工竟无一人离开公司，绿盟的企业凝聚力可见一斑。

短短的一个多小时很快过去，我很清楚，繁重的研发任务不可能允许袁哥有太多的时间花的接受采访上，所以也尽量缩短谈话时间，令我有点感动的是袁哥没有表现出丝毫倦怠敷衍，更没有抬腕看表这样的结束暗示，但我不得不在意犹未尽的不舍中终止了采访，与袁哥话别后步出会议室，扑面而来的又是办公区的满眼绿色，诗人说绿色象征着生命和希望，绿色也是春天主色调，那么绿色的绿盟无疑是承载着民族信息安全事业的希望在迎接IT业的春天吧。

袁哥印象

采访札记

一个不懂网络安全技术的人与袁哥对话会很快感到无聊和尴尬，因为没有共同语言；一个很爱说话的人也会令袁哥很到不自在，因为古人云：君子敏于事，而呐于言。但袁哥说起话来语言思路如严谨的程序语句行般条理清晰，丝丝入扣。

重庆人爱"摆龙门阵"，爱吃"火锅"可谓全国闻名，但凡事都有例外，袁哥就是重庆人中的"另类"，不善辞令，性情内敛温和，浑身难觅重庆人的健谈与"麻、辣、烫"般的火爆，但他内在的坚毅执着与聪慧仍与巴蜀才俊的优秀基因一脉相承。

采访袁哥不是件很容易的事，这难度来自他内敛的个性，来自他的不示张扬的做人原则，在网络安全技术的数字王国他才华横溢，晦涩古奥的程序代码在他智慧之光的"逐行扫描"中神秘全无，袁哥在所有知道他并敬佩他的人中很有传奇色彩，人们的无限想象力可以让这种传奇也无限，但当袁哥真的站在你面前，你会发现，原来这传奇只存在于袁哥那别人无法真正走进的思维空间与精神世界，其貌不扬、衣着随意、平易朴实才是一种看得见摸得着的真实。

袁哥平时的生活圈子很窄，盛誉之下始终保特低调，生活状态有点象一个"封闭式开发"任务中的程序员，除了袁哥的公司同事及技术圈里的好友，鲜有"外人"走近袁哥，通常只会在高水平网上技术论坛看到他的一些最新技术文章，袁哥的文章总是令人关注的，但这与名气无关，要知道，在高手云集、藏龙卧虎的网络安全界，绝少存在所谓"权威迷信"，相反，挑战权威却是圈内的普遍个性体现，袁哥文章永远是在"以理服人"。对很多普通的慕名者，袁哥更像是个"传说中的人物"，与偶象的距离使"传奇"越"传"越"奇"，其实走近袁哥你会发现原来丰富内涵与平庸外表的反差会愈发彰显人的内在魅力 。

从袁哥的平淡自述中，我可以想见他在计算机领域求知道路上的艰辛，在他人看来可能还充满了孤独寂寞，但我想袁哥自己一定不会觉得孤寂，因为这有属于他的智力游戏，也有他释放才情的"系统平台"。

从上大学后首次离开山城，袁哥就如侯鸟般开始了长距离迁徙，从重庆到济南"山大"上大学，毕业分配工作到青岛"海信"，直至跳槽到中联绿盟，交谈中，袁哥对自己这段不断北迁的飘泊经历颇有些慨叹与无奈，他坦言自己身为南方人至今仍不太适应北方的干燥多风的气侯与生活环境，很想回到南方，并声明北京肯定是他北方工作城市的最后一站，但他承认，这里有他所钟爱

的网络安全事业最好的发展环境，相比较起来，气侯及生活环境真算不了什么，因为他生来就是对生活本身要求不高的人。投入地工作，简单地生活，这可能就是他基本的生存状态。

原本设计采访方案时不想涉及太多的技术内容，为的是希望使读者了解更多技术以外的袁哥，然而采访开始后就发现，要想和袁哥多聊一会儿，就得谈技术，于是就硬着头皮谈，谈论了很久技术后，我试着往一些轻松话题上转，问他的兴趣爱好，但一聊又发现，原来这个话题也轻松不了太久的时间，因为除了一种比较少见的名叫“够级”的扑克牌玩法，以及偶尔去一个山清水秀的地方休息休息，再没有吸引袁哥的所谓兴趣爱好了，常人眼里丰富多彩、目不暇接的娱乐活动，在袁哥看来无大兴趣，可能在袁哥的世界里，没有比计算机代码更能让他感到兴奋的东西了，好像他这类人的大脑生来就是为思考和运算而准备的，就连“够级”扑克牌这种非常讲究团队合作精神的休闲方式也与思考和运算相关，如果有一天这种思考和运算嘎然停止，可能也就意味着智慧源泉的枯竭吧。

真会有这一天吗？不敢想象，如果真有这一天，他会如何重新安排自己的生活？回到生于斯长于斯的南国故乡？觅一处山青水秀、碧草如茵的所在遍历美景？这答案或者只存在于袁哥大脑的“底层代码”中，除了他自己，谁会有兴趣“反编译”一下呢？

哲人说：“我思故我在”，年轻的袁仁广就是这样一个闪耀着思辨之光的生命存在。

袁哥小传

网名：袁哥(yuange)

姓名：袁仁广

别名：大兔子(datuzi)

年龄：27岁

性别：男

籍贯：重庆市

1997年7月毕业于山东大学数学院计算数学及应用软件系。

工作经历：

1997年7月—2000年2月　青岛海信集团技术中心网络所任工程师。负责电视单片软件开发和内部网络管理。开发的1238系列彩电已经成为公司主力产品，实现了公司产品的全面更新换代。公司站点：http://www.hisense.com.cn 。

2000年2月—至今　中联绿盟信息技术（北京）有限公司。负责Windows等操作系统的安全研究。公司站点：http://www.nsfocus.com。

技术专长简述：

袁哥有熟练的单片开发经验且具相关硬件知识水平；精通汇编、c等各种编程语言，熟悉TCP/IP等各种协议，对Windows等操作系统及INTEL的CPU指令结构的研究也颇具功力；其理解力、洞察能力、软件跟踪调试能力与代码阅读分析能力极其出众，再兼具很强的自学能力，使其能很熟练的进行源代码、二进制代码的安全审核与分析；发现微软操作系统、Web服务器软件的许多严重漏洞，早期最著名的当属Windows 9x共享密码及IIS系统漏洞。亦使微软出台了相应的漏洞补丁；除此之外，病毒编写，防、杀等技术也是袁哥的强项。

袁哥的主要研究成果：

1. Absent Directory Browser Argument Vulnerability;
2. Share Level Password Vulnerability;
3. Web Server Folder Traversal Vulnerability;
4. Web Server File Request Parsing Vulnerability;
5. Microsoft IIS for Far East Editions File Disclosure Vulnerability;
6. Microsoft IIS CGI Filename Decode Error Vulnerability;
7. fp30reg.dll Buffer Overrun Vulnerability;
8. ssinc.dll Buffer Overrun Vulnerability;
9. WebDav Denial of service Vulnerability;
10. WebDav view the source code Vulnerability ;
11. WebDav Buffer Overrun Vulnerability ;
12. asp.dll Buffer Overrun Vulnerability;
13. shtml.dll view the source code Vulnerability ;
14. the other Denial of service Vulnerability ;
15. the other view the source code Vulnerability ;
16. winlogon.exe Buffer Overrun Vulnerability ;
17. the system api Buffer Overrun Vulnerability ;
18. Windows kernel Buffer Overrun Vulnerability ;
19. apache for win32 Search File Vulnerability ;
20. apache for win32 Run Discretional Command Vulnerability ;
21. php4.0 Buffer Overrun Vulnerability;

……

“Warning3”——网络安全的警示者

访中联绿盟信息技术公司左磊

本刊记者／秦丁可

左磊小传

左磊，男，27岁。中联绿盟信息（北京）技术有限公司任研发部总监，CIW Security Professional，具备深厚网络安全研发功底，负责对多种国内外著名的安全产品的测试项目，主持负责绿盟“冰之眼入侵检测系统”的开发工作，长期从事网络安全的深层研究。并著有大量网络安全专著。特别对基于UNIX操作系统的安全问题研究有着极深的造诣与丰富实践，“Solaris 2.6 IN.FTPD CWD用户名猜测漏洞”、“UNIX系统locale格式字符串漏洞”、“inews 缓冲区溢出漏洞”、“Cxterm的漏洞”、“FreeBSD内核溢出攻击”等大量UNIX/Linux系统安全问题的发现者，深谙各种黑客攻击手法以及防御手段，在对各种防火墙、入侵检测系统等安全产品的测试方面有丰富经验。

有点英文基础的人都知道“Warning”是“警告”的意思，而有点计算机网络安全基础的人也多数会知道“Warning3”是国内网络安全技术界顶尖级人物左磊的网名！

说起“Warning3”网名的来历，想必有一种凭借字面意思的揣度。“Warning”是“警告”，那加上3就该是“警告3次”了，所谓事不过三嘛，而这看似合理的分析经求证名字主人后才知完全是种不明就里的想当然，其实此名的妙处不在“Warning”而在其后那个不起眼的“3”。当年左磊发现一个网站存在被攻击安全隐患后，准备就此给该站网管发一封善意的警告信，提醒其及时修补防范。由于他还没有合适的网名与电邮账号，就先到HOTMAIL上去注册。第一次他以“Warning”注册个人账号，但邮件服务器系统马上告之此名已存在，请改名；于是按多数网友的习惯，第二次他以“Warning1”注册，孰料又被告之重名；于是第三次以“Warning2”再试，没想到依然遭到执着的拒绝。这一来，令左磊笑哭不得的同时也激起了他的“拧劲儿”，又以“Warning3”为名发起第四次“冲击”，结果这次真应了那句“事不过三”：注册成功！于是“Warning3”从此就成为左磊一直沿用不变的网名，因日后他在网络安全界的成名，这个名字也随之变得比其真名更为人熟知。

与UNIX的不解之缘

要讲“Warning3”其人其事，还必须先说说UNIX，因为“Warning3”这个名字与UNIX是密不可分的，可以说“Warning3”在中国网络安全界的至尊声望与UNIX在计算机科学技术领域的不朽地位是相配的，他为完善这一古老经典的计算机操作系统的网络安全性能所作的贡献也有目共睹。

众所周知，微软Windows系列产品的商业运作比其本身的技术创新还要成功，比尔·盖茨这位颇有争议的“上帝宠儿”确实创造了一个商业神化，他让全世界很多不用电脑的人都知道了有一个“Windows”的东西，虽然这个“窗口”在电脑业界刚打开不过短短数年，相反，UNIX这个“古董”却曲高和寡，因为在以“鼠标”指点“图形界面”IT江山的今天，众多天天泡网的新新人类对“UNIX”一词闻所未闻，更不知道那是一个操作系统。经典与流行是两个不同的概念，在多元化与市场化的时代，优胜劣汰，完全取决于人们需求的自由选择，无论你是否喜欢微软，如果你已习惯了图形界面的操作环境，那Windows当然是首选；而如果你是个技术的狂热追求者与传统的“卫道士”，那么在UNIX的

SHELL命令行中的每一次键盘输入也会带给你无尽的快感，当然现在还有了Linux这一集传统与现代优点之大成的另类选择。但经典就是经典，经典是由时间来定义和证明的，UNIX卓越非凡的稳定表现与网络性能，决定了其在互联网服务器及企业级网络应用中不可撼动的地位。但选择并研究经典则需要一定的修养与驾御能力，一种平和稳健、甘于寂寞的学术心态，卓而不群成绩的背后是对心智和毅力的艰苦磨砺与考验，“Warning3”选择了UNIX，也就选择了一条艰辛孤独的研究之路。

在中联绿盟公司一间静谧的会议室里，Warning3语气舒缓地开启被岁月尘封的旧事：

1997年国际互联网在国内刚刚兴起，那时的Warning3还在合肥中国科技大学就读，学的也是非计算机专业——机电一体化。对正钻研UNIX操作系统的他来说，互联网无疑是一个取之不尽的学习资源，同时也令他开始了对网络安全的特别关注 。

最初他在科大自学UNIX操作系统的日子是艰苦的。开始阶段是自己到书店买一些关于UNIX的书看，但由于UNIX没有Windows系统这么普及，相对来说UNIX的书也很少，所以可供选择的学习资料、特别是那种很符合自己学习方向的参考教程很难找，后来有了互联网，就开始在网上特别是国外UNIX技术网站查找学习资料。那时，国内上网的人还远没有现在这么多，Warning3最初接触了一些国外安全网站的邮件列表，了解到网络安全相关的技术内容，继而又看了不少国外的黑客网站，进一步激发起对网络安全的浓厚兴趣。但上网对Warning3来说也不是件容易事儿，首先当时在学校以及后来工作的东方电子没有提供上网条件，又没有一个UNIX操作系统环境可供学习研究，怎么办呢？只好跑到外面找。他工作所在地烟台的网吧也不普及，再加之花销也很大，不可能长时间地上。好在那时常有国家电信部门为推广客户上网而开办一些免费试用的上网场所，但“免费的午餐”是不可能让你舒舒服服地尽情吃个饱的，每次排很长时间的队，每人也只能上网半个小时。没办法，为了有足够时间尽可能多地搜集UNIX的学习资料， 半个小时一到只好出来再次加入到排队等候“试用”的长龙之中。很多节假日，他一整天的时间就用在了这种排队上网的过程中。

Warning3的这段经历不禁让我联想起袁哥当年在校期间因条件艰苦而“手刃”千行汇编代码的壮举，我相信在网络安全的求知道路上，Warning3所付出的努力和劳动也必然是艰苦卓绝的，如果说网络安全技术水平达到一个极高层次要得益于勤奋加天赋的话，我宁愿相信前者所占的成分更多一些。而在亲自采访Warning3以及袁哥之前，我还一直以为主要是天赋造就了他们令人称奇的超人技艺，与他们接触之后，我的这个观点发生了很大的改变：原来再聪慧的大脑也必须经历反复的甚至是痛苦的思考磨炼才可能与世间奥秘碰撞出耀目的神奇火花。我再次感受到什么是成功背后的艰辛与寂寞。思考的过程是痛苦的、也是永恒的，与之相比，每一次成功与失败的结果都是另一个思考过程的开始。在与Warning3谈及系统漏洞分析研究的过程时，他几次用了“痛苦”这个字眼，也谈到了做这项工作要能“吃苦”，虽然他是用一种无可奈何的谈笑语气在讲这两个词，但我对此却印象格外深刻，因为我知道，不管他如何轻描淡写地对此事一带而过，但“痛苦”一定是个真实的过程与心理感受。

“你要问我如何才能在网络安全技术方面取得一定的成绩，我的回答很简单，除去每个人的一些不同条件与环境机遇等客观因素外，能吃苦肯钻研一定是个最共同最基本的条件与素质，因为这是一项很枯燥的研究工作，需要很长的时间、极大的精力去阅读分析大量源代码，常有百思不得其解乃至不得其门而入的苦闷，有时你会感到很无助，因为没有人能帮你，甚至任何可借鉴的先例与他人经验也没有，只能靠自己思考，那真可以用‘痛苦’两字来形容。当然，一旦经过努力有所发现或最终找到解决答案，那种兴奋与成就感也是常人体会不到的，你会觉得一切辛苦付出都是值得和有意义的。只要有恒心和毅力长期坚持下去，不断地摸索与总结积累经验，就一定会取得成绩。其实做别的工作与学术研究也是一样的道理。”Warning 3如是说。

要论在UNIX/Linux系统特别是SUN公司solaris系统漏洞分析与发现方面的能力与成绩，Warning3理应占有当仁不让的至尊地位，在网上搜索引擎键入“Warning3”后全都是UNIX/Linux相关系统漏洞的分析论述文章：《Solaris 2.6 IN.FTPD CWD 用户名猜测漏洞》、《UNIX系统locale格式字符串漏洞浅析》、《inews 缓冲区溢出漏洞》、《C x t e r m 的漏洞分析》、

《FreeBSD内核溢出攻击》、《RedHat man缓冲区溢出漏洞》、《Qualcomm qpopper远程溢出漏洞》、《Bind 8.2.x堆栈信息泄漏以及TSIG单字节溢出》等等数不胜数。“Warning3”的首次牛刀小试还是在他从科大毕业前后，当时热衷上BBS的他偶然间在一个名为火鸟的BBS站点上发现了其POP3远程溢出问题，从此一发而不可收拾。在UNIX/Linux系统下的各种漏洞中，对“溢出”的分析是Warning3的拿手好戏，普通“堆栈溢出”之类对他来说已是一种入门级必备的基础东西，现在已转向兴趣很浓的“堆溢出”、“格式串溢出”等方面的研究及经验总结。经过对“solaris”系统的长时间研究，Warning3现在对该系统最易出隐患的地方已很熟悉，凡有诸如环境变量或参数过长以及该做的限制没有做的地方都是Warning3查找漏洞的重点突破口，可以说对这些系统规律的了如指掌、丰富的经验再加之敏感的洞察分析能力，使现在Warning3的分析研究更有针对性及效率。当然，由于SUN公司并没有全部公布其系统源代码，也就决定了他的分析更多情况下只能采取半靠经验半靠灵感的“黑箱测试”，沿着大方向“摸着石头过河”。说到这个艰难过程，Warning3再次用到了“痛苦”一词，看着他微笑无奈地说这两个字儿时，我相信，真正的痛苦可不是说说而矣。

图为warning3(右)在接受采访中

令“Warning3”更为“痛苦”的是那段没有系统环境可用甚至上网都很困难的日子。在东方电子上班的时侯，所用的电脑一不能上网，二没有UNIX和Linux环境，而计算机技术学习最讲究实践出真知，总凭看书，理论知识再多不上机实践也不能真正掌握，更何况是网络安全技术，没有实验环境，无异于纸上谈兵。过了一段“无机可用”的日子，“Warning3”再也无法忍受，于是用大量3.5寸软盘考贝了一套Linux装在了公司电脑上。那时刻录机与CDR盘对他来说还是一种奢侈品，可令他无法忍受的事情还在继续发生，经常在系统已安装至一半要求插入第N张盘时，这张盘发生读写错误！“别提多郁闷了，软盘真是不可靠，总爱坏，用了不知有多少张，但是当时又没有别的办法拷系统，也只能用它。” 抚今追昔，Warning3对那段“艰苦岁月”没齿难忘，感慨良多，“回想起当时条件虽然不好，但很珍惜，现在公司的研发条件差不多可谓应有尽有了，可以24小时专线上网，各种系统测试环境与工具也一应俱全，真有天壤之别。”

UNIX与Windows“比较测评之Warning3版”

作为国内UNIX系统安全的专家，Warning3对UNIX操作系统的研究与熟知程度已达到相当高的层次，所以他对UNIX系统优缺点的了解以及UNIX与Windows的比较评价应是很有发言权的。

“首先就系统稳定性而言，UNIX的表现无疑是极其优秀的，几乎不存在死机现象，有也是机率极低，仅此一点就极胜任企业服务器的角色。而且除了对UNIX系统内核进行重新编译，其他情况下，无论对系统进行什么添加、删改或配置都不需要重启系统。当然了，在这一点上Windows系统现在也已做了很大的改进，重启系统情况越来越少，但似乎还未完全做到与UNIX相同的水平。

关于系统安全漏洞问题，客观公正地讲，微软Windows系统在设计上也是相当出色的，但之所以出现漏洞问题，原因是比较多的，比如其所运行的硬件环境相对于UNIX系统要杂一点，也要求低一点，而作为商业操作系统，其源代码的不公开性反而更激发了“黑客”的好奇心与挑战欲望，加之企业应用也比较广泛，在其上开发的各类商业实际应用程序也多，比如IE若存在问题就会直接威胁到Windows系统的安全。基于这些原因，Windows受攻击的机率也就更大一些。更糟糕的是，一旦其系统漏洞被攻击者发现与控制掌握，攻击者往往并不通知微软，使其身处危情仍浑然不知，以至不能及时对外发布系统漏洞公告及补丁程序，并采取升级等补救防范措施。相对而言，UNIX也有漏洞，但由于其内核代码（部分商业版UNIX除外）是开放的，漏洞被发现后，全球具有开发能力的UNIX专业人士及爱好者都可以加入到编译修补改进的行列中来，大家都可以自

发地贡献自己的力量，从而基本上能做到漏洞随出随补。同时，大家都知道在UNIX系统上开发的商业应用要比Windows少，这也从另一个方面为UNIX减少了漏洞产生的机率。但UNIX肯定也不是铁板一块，仅我个人发现的漏洞已有不少，最近SUN公司solaris方面比较严重的溢出漏洞就又有发现，所以总体来说，以我个人的研究经验感觉UNIX与Windows这两大主流操作系统的漏洞存在机率是大体相同的，差不了太多。

就两大主流操作系统的未来发展走势而言，我认为不会存在谁被谁击败或取代的问题，这也是由两种系统各自不同的特性与优势以及不同用户的需求决定的，且在过去的时间里二者的竞争历史也说明了这一点。不过在UNIX之后出现了现在势头很盛的Linux，作为UNIX的一种演化派生物，Linux的出现在某种意义上讲加大了UNIX这种操作系统体系的应用比率与技术优势，同时也对Windows提出了更有力的挑战。对于国外用户来说，由于信息化历史上的使用习惯以及语言上的因素，接受起UNIX与Linux来很快很方便，而相对国内用户，却存在中文汉化方面的滞后等问题，比如现在市面上可以看到的各类Linux中文版其联机帮助信息却还是英文的，这就给国内用户的使用和学习带来一定的不便。当然，基于UNIX与Linux上的应用开发也是一个问题，可喜的是现在国内外一些知名的软硬件企业厂商已越来越意识到这个问题，也已纷纷推出了自己基于UNIX/Linux的商业应用，相信UNIX/Linux的未来发展前景还是光明的，但这同时也对我们从事这一系统网络安全研究的人提出了更高的要求。”

国内有一个比较知名的UNIX技术专业网站，叫“永远的UNIX”，我很喜欢这个名字，因为它充分表达了一种执着与永恒的信念。在这个站点上有大量Warning3的原创大作，我以为，UNIX这一古老经典的操作系统正需要更多Warning3这样青年才俊的智慧不断“涮新”与“升级”，才能永葆其不朽魅力。

绿盟——有着绿色般希望的同道者联盟

采访中我向Warning3提了这样一个问题：“众所周知，现代企业的竞争说到底还是人才的竞争，绿盟何以能将诸多你与袁哥这样的国内顶尖网络安全人才聚集在旗下呢？”

Warning3：“我觉得首先就是大家都一致看好网络安全这个行业的发展前景，从而也就对公司发展的大方向有信心。再有就是一种非常和谐融洽的工作环境与企业文化氛围，有了这些大前提，再加上有沈总他们这样好的企业领导管理层与科学先进的现代企业管理机制，大家有缘聚在一起成就一番事业也就是一个顺理成章的事情。你可能也听说过绿盟初创阶段在暂时资金周转困难的情况下一度暂停发了员工三个月的工资，但为什么大家都没走，同心同德的一起走到了今天？因为大家都有一个共识，就是对企业发展前景的一致看好，上上下下都有一个长远眼光和信心，资金的暂时紧张是有一定原因的，也是企业发展过程中的正常现象，短期的困难终是能克服的。我还想强调一点的是，大家都非常珍惜这里和谐的人际关系与工作氛围，1999年创业初期我们只有十几个人，原先大家基本都不认识，但相处几天就感觉像老朋友一样亲切自然与和谐，我们这些做技术出身的人彼此之间在技术方面的交流是非常密切的，不搞技术研究的人不会知道，这种交流有多么重要，很多新鲜独特的想法每天都会产生，这对提高自己的技术水平很有帮助，别人的经验和长处也许就是你自己欠缺与急需的。你比如说，我和袁哥研究的技术领域不同，但是他研究Windows时的一些角度与思路或许对我在UNIX分析方面也可能有所启发，反之亦然。我们研究部的人现在或定期在一起开个小型的交流会，或者会随时随地就技术问题聊一聊，可以说在绿盟这个环境中以技术交流促进共同提高也形成一种员工的自发行为，这种情况在别的公司是什么样我不好说，我只是觉得绿盟这方面环境可能是最好的。现在公司人员壮大早已今非昔比，且还在吸引更多的人才加入进来，这样可交流的人又增加了，其实绿盟的人气也就是这么聚集起来的。我觉得良好的技术交流与发展环境，就是最吸引人加入到绿盟的重要原因吧，所以说假使面临跳槽的选择，我一定会非常看重这一点，如果没有比绿盟更好的技术交流与发展环境那又何必呢？”

Warning3的话让我越发感受到了绿盟企业凝聚力的能量，如果说以前与网络安全圈内的朋友聊天对“绿盟人心很齐”之说“耳闻是虚”，那么今天采访Warning3应算是“眼见为实”了吧。联想起“绿盟”这个特点鲜明的企业名称，感觉此名当初的创意是否也有这样一层含意：所谓绿盟，就是“有着绿色生命般希望的志同道合者的联盟”？

一个人的智慧与能力终究是有限的，好比单蕊片机，而团队的力量聚集起来能量则是巨大的，如同多处理器并行服务器！

书生左磊

——采访札记

见左磊的第一面，其外表就给我以过目不忘的深刻印象，这倒不是因为他有很“另类”的身形与五官，相反，倒是他从头至脚一副脸谱化的典型知识分子外型给了我很强的视觉冲击，体形瘦削，皮肤白皙，气质儒雅，镜片后的目光沉静，那种似乎触手可及、扑面而来的书卷气息会让你觉得与此公交流自己务必礼数周全，粗俗造次不得。其实这倒与我心目中网络奇才的外形“模板”之一非常相符。确切地说，他的外形更易让我联想到高等学府的莘莘学子或科研院所里的谦谦学者，与时下网络时代年轻人中较流行的带有极端倾向的另类个性与时尚相比，他的外形与气质都透着正统与保守。

从南下合肥“中科大”求学，到就职于烟台“东方电子”，直至最后加入“绿盟”，他的生活工作轨迹要比他在网络安全领域求知探索的历程简单许多。身为济南人，外表白晰文弱的Warning3完全不似人们传统印象中的山东大汉，但他仍有着山东人典型的健谈与直爽，无论是怎样的话题，在他永远温和沉静的语气里，任何与之交流的人都能感到闲庭信步般的轻松随意，只要你简短地提出问题或开启一个话题，他便可以很准确地围绕主题，条理清楚地娓娓道来，还会适当的引申开来。在这样一位“牛人”身上你找不到一点“牛气”，可能还会让你产生“原来也不过如此”的错觉。当然，这错觉的前提是抛开网络安全技术，一旦涉及技术，你会知道什么是典高和寡与独孤求败。

对于Warning3这样的“惟技术论者”，我主观地揣测他一定过着漠视世俗娱乐的学究夫子式的生活，而得到的答案并没太出乎意料。刚来北京后，有半年时间Warning3天天在公司里待着，哪儿也没去玩过，后来还是在公司同事的带动下，业余生活稍微丰富了一点，偶尔与同事朋友在茶余饭后唱唱歌或看看电影。令我有点意外的是文质彬彬的Warning3还是个“摇滚”爱好者，当然也不局限于此，好听的音乐他都来者不拒。他还爱看一些球类电视节目，并戏称自己是“伪球迷”，不懂却爱看，看完更不练，偶尔有兴致挥两下乒乓球拍，但履战履败，于是又试着从羽毛球拍中找回信心，孰料两个回合下来便体力不支。从此，在每天下班后公司附近的昆玉河畔，就可见到“绿盟长跑队”里Warning3的纤瘦身影。至于这种训练的效果如何，还有待时间考证。周六周日对Warning3来讲是真正意义上的双休日，更确切的说是睡觉日，一觉醒来必是中午时分，把一周没睡足的觉都补回来了，下午处理一下卫生及私人事务，间或出门转转，一周的生活也可谓有张有弛了。虽不好玩好动，但Warning3还是有一个未了心愿，那就是渴望到中国著名自然风景区“九寨沟”一游，他说是“九寨沟”的风景照片带给他的视觉震撼，使他对这个列入世界自然生态保护计划的“人间仙境”迫切神往。说到这个话题，Warning3显得兴致勃勃，甚至超过了谈UNIX。由此我感到，人的潜在生活情趣其实很丰富，之所以有的人显得兴趣广泛，有的人看起来单调乏味，无外乎是性格、修养、爱好、客观环境及物质条件等因素造成的。以时下爱玩也会玩的时尚一族的标准看，Warning3的生活方式未免单一，但有道是“君子欲有所为必有所不为”，人的时间与精力总是有限的，游山玩水与纵歌豪饮都是费时费力的事情，这些业余“进程”会占用不少的科研“系统内存资源”，权衡一下，以事业为重也是自然的，所以只能说Warning3玩的时间、精力与兴趣少一些，而不能说他不会玩或不懂享受生活。

人如其名，Warning3是网络安全圈内一个富于同情心与责任感的警示者，看他的技术文章，可以从他的智慧与才学中受益，与他进行交流则更能补充一些人格魅力的东西，特别对那些视Warning3为偶像的少年网络安全爱好者们，他可以让他们明白：原来网络安全技术的成功之路由孤独寂寞与痛苦铺就，既想出风头又怕吃苦的人选择这条路是最大的错误；原来用别人开发的黑客工具“黑”几台肉鸡是这么的无聊与幼稚；原来这个领域学无止境又高手云集，穷尽皓首也只修得沧海一粟，原来……一旦懂得了这些“原来”，也就从本质上缩短了与偶像在思想境界上的距离，而赶超偶像的路则只能靠自己一步步脚踏实地地踩出！

这也算是习惯了发“警告”的Warning3发出的一个“敬告”吧：由衷地希望所有有志于网络安全事业的追梦少年们一路走好。

小四的故事

访中联绿盟信息技术公司陈庆

文／本刊记者 秦丁可

“……我一直都希望大家从这里学到的不是技术本身，而是学习方法和一种不再狂热的淡然。很多技术，明天就会过时，如果你掌握的是学习方法，那你还有下一个机会，如果你掌握的仅仅是这个技术本身，你就没有机会了……”

这是网上广为流传的“小四哥”那篇经典之帖——《你尽力了吗》中的精华之语，我用它作为讲述“小四”平淡中见传奇的故事的开始，因为我认为这篇帖子和这句话可以高度概括“小四”其人，包括他的学术态度和处世哲学。

“小四”本名陈庆，是时下国内网络安全界的热门精英人物之一，继袁哥、Warning 3等人后“绿盟科技”又一技术骨干，UNIX/Linux系统底层分析高手。在这众多赞誉与头衔的背后，生活中的陈庆非常低调，盛名之下，他只认可一个自我评价：“我只是一个普通的UNIX程序员。”

流火七月一个酷暑难耐的午后，我在“中联绿盟”的办公楼按约采访小四。面前的小四再次令我感到现实与想像的差距。中等瘦削的身材，白皙骨感的脸庞，树脂镜片后谦逊坦诚的目光。一件印有“绿盟”公司徽记的黑色工作T恤，一条“看似廉价”的米色西裤，一双“绝对廉价”的“千层底”布鞋。于高档Office里满目的名牌西装革履中突显一种洒脱与闲适。在握住他主动伸出的手彼此寒暄时，我感到一种自然随和的热情，一下子淡化了初次见面的陌生感。

随后，我们坐在静静的会客室里面，听小四讲那过去的事情……

“象牙塔”里的故事

故事从“小四”这个名字说起，没人想到“小四”与“MUD”有何相关。1997年在长沙铁道学院电子工程系计算机软件专业上“大四”的陈庆，通过中国教育科研网接触互联网，“MUD”也就是“泥巴”在网上是尽人皆知的经典游戏，陈庆也一度沉迷其中。联网玩“泥巴”的时候，他起了“小四”这么一个用他自己的话说“江湖味道比较浓且具东方色彩”的化名。网名常随着人的使用习惯沿袭下来，所以“小四”叫到今天从未更改。

“小四”高考填报的所有志愿都是与计算机相关专业，且注明不服从分配录取到其他专业。对计算机如此情有独钟，源于高中时接触BASIC语言课程后激发的浓厚兴趣。这兴趣使一度热衷参加各类数学竞赛的陈庆改变了高考报数学系的初衷。很巧合，从袁哥到小四，他们原本都在数学上有很强的天赋与浓厚的兴趣，看来有数学天赋的人更易在计算机技术领域取得突出成绩。

计算机专业的学生少不了天天与电脑为伍。那还是DOS3.1盛行的年代，小四与同学开始研究病毒。这似乎也是当时计算机技术里最能激发人兴趣的东西，成为现在很多高手最初入门的切入口，比如袁哥与黄鑫。研究病毒自然离不开汇编，学校在大二时才开设汇编课程，可小四和很多同学大一就已自学成了汇编的高手，搞汇编“成风”，同学间笑谈：“以后你编病毒，我编杀毒软件，大家各赚各的钱。”大伙写起汇编来，动辄就是成千上万行代码。小四自己则练习着用汇编写一些检查病毒的程序，针对当时病毒喜欢更改系统中断向量的特点，通过硬件编程绕过操作系统对其进行监视。他用这个土方法偶然间还发现了当时已风靡全国的江民KV100杀毒软件存在的一个小问题，那就是KV100每次杀毒，总在电脑内存地址中修改一些内容，但退出后不恢复。后来小四与3个同学又用汇编实现了一个比较“大胆”的设想——更换MSDOS操作系统中的COMMAND.COM执行文件，用自编的文件取而代之，而且做得很成功，加载Windows 3.1一点问题也没有，这让他们小有成就感。正由于汇编和DOS掌握得太熟练了，以至于他们很难接受DOS向Windows3.1的过渡，使他在Windows编程方面出现了一个小小的断档，小四就是跳过Windows 3.1/3.2而直接