



互联安全周刊

2008 年 1 月 第 1 期 刊号 YC2008F01

目录

主管: 广州市计算机信息
网络安全协会
主办: 中国互联安全网
地址: 广州科学城掬泉路 3
号国际企业孵化器 A 区
电话:
400 -6037 -120
网址: www.sec120.com
名誉总编:
黄丽玲 陈三堰
总 编:
陈 彬
责任编辑:
徐 聪 陈康太 涂师芳
夏 旭 张 飞
专家团成员:
吕 琳 沈 林 徐春雷
李成峰 闵家法 何伊圣

信息安全关乎企业存亡，人
人有责！
网站专家专注网站安全，为
您服务！

刊首语

2 2008 年-----信息安全年

专家专栏

3 网站被黑前你还能做什么？

病毒防范

5 五步剿灭“机器狗”病毒

7 07 反病毒市场，毒客投入更具“钱途”产业

安全新动态

8 2007 年发生的安全事件大回顾

安全新生活

9 上网安全防护指南

新好软件

10 个人用户经典国外反病毒反黑客软件组合

办公新天地

11 易记忆而又安全的密码

局域网安全

12 10 大方法减少内部人员安全风险

网管经验谈

14 来者是客—微软内部增强系统安全的秘技

安全特训班

16 熟记安全顺口溜，不懂安全也风流

安全大调查

16 你不能不考虑的安全因素

技术哈哈镜

17 安全管理领域，最神秘的事情

职场美文

18 技术人员必须知道的十条良言

网络笑话坛

19 一个网管的自白

网站风采

20 500WAN----彩民的真诚朋友

服务专家

21 您身边的网站安全服务专家

读编信箱

22 您喜欢本周刊吗？

刊首语

我们送走了硕果累累的 2007 年,迎来了充满希望的 2008 年。

2008 年是奥运年, 2008 年更是信息安全年, 公司的信息越来越决定公司的前途命运。

公司的信息安全包含方方面面, 涉及到很多技术、硬件、软件、程序、人、制度等等, 这是一个庞大的非常专业的工程, 和我们通常在报刊电视上看到的安全生产、安全运输都有类似之处。安全既然不是一劳就永逸的, 那么我们就需要一个完善的团队和机制来确保安全事故减少到最少。而很显然, 绝大部分公司不具备这样的一个技术团队, 几乎是很难完成这项工作。

所以, 许多公司要请第三方评估机构或专家来完成对网络安全的评估。这样做的好处是: 能对自己所处的环境有个更加清醒的认识, 把未来可能的风险降到最小。目前网络安全评估的中介机构, 在国外已经开始将网络的安全评估作为一个新的服务项目向社会推出, 我本人也看过国外很多这方面的书籍。作为一种新兴的业务, 其影响是否能象会计师事务所、审计师事务所之类的中介机构那样重要, 尚需拭目以待。但有一点可以肯定, 那就是网络上的商机同样也与风险同存。要想通过公司的网站渠道服务客户、获得利润、维护公司形象, 就必须将安全问题解决。

“互联安全网”——Sec120.Com 将和大家一起直面黑客安全事件, 共筑网络安全防范体系。我们将在新的一年以更专业的精神, 更良好的态度, 真诚的为大家服务!



专家专栏

网站被黑前你还能做什么？

互联网快速发展，计算机广泛运用，给人类带来高速便捷的服务，与此同时，由互联网安全漏洞引发的黑客事件频频见诸报端，其种类之多，破坏力度之强，令人瞠目结舌。实际上这些得以报道的互联网安全事件不过是冰山一角，世界著名安全软件公司赛门铁克此前发布的报告显示，2006 年下半年全球共有超过 450 万台电脑在用户无意识的情况下被黑客远程控制，超过 10 万家大型企业网站被挂上网页木马或者被入侵篡改。由此可见，检测网站漏洞、关注网络安全已经成为每个企业甚至每个计算机用户不可忽视的日常工作。

网络安全形势日趋严峻，但也不必谈“黑”色变。现在“互联安全网”——Sec120.Com 将和大家一起直面黑客事件，共筑网络安全防范体系。

为什么会有如此频繁的黑客事件出现呢？

Sec120 互联安全网反黑学院负责人陈彬先生指出：“这主要是因为信息时代里，犯罪行为已逐步向高科技蔓延并迅速扩散，利用计算机进行高科技犯罪的案例越来越多，因此，计算机安全问题已成为举世瞩目的焦点。随着计算机在人类生活各领域中的广泛应用，计算机病毒也在不断产生和传播，计算机网络不断被非法入侵，重要情报资料被窃，甚至由此造成网络系统的瘫痪等，给各地众多企业公司造成巨大的经济损失，甚至危害到国家和地区的安全，计算机安全保密问题是现代信息社会一个十分重要并具有普遍意义的问题，必须认真学习、掌握和发展有关的技术和方法。”

为什么会被黑，什么样的网站会被黑？

Sec120 互联安全网首席安全专家李成峰先生介绍说：“目前大多数公司并没有配置专门的网络安全管理人员，通过我们实施过的客户来看，担任此类工作的基本都是对网络安全不是很专业的程序人员和网页设计人员。即使有些公司配置有专业的网络安全技术人员，但毕竟个人力量有限，网络安全是一个整体规划的过程。因此必须重视网络，做全面的安全评估及跟进，这样做的好处是：排除已知网络隐患，预防潜在安全危机，把可能带来的风险降到最小。特别对于一些靠网站运营生存的企业，稳定的服务及网站将会直接影响经济效益。”

目前被黑的大部网站主要有以下几类：

1. 使用网上公开的源代码程序做为网站支撑平台的网站；

这类网站问题最多，因为源代码公开，黑客们可以直接对程序进行分析，找出漏洞。同时基于此类程序先天性的设计缺陷，也给黑客的攻击留下便利之门。目前网上黑客工具泛滥，稍懂黑客技术者就可攻击此类网站。不要以为你的网站黑客找不着，通过这些程序的某一个关键字即可通过某搜索引擎直达你的网站，例如使用动网系统的人，一个漏洞出现后将使数百

甚至数千人被攻击。

2. 一些比较著名的电子商务类网站;

这类网站一般比较大的流量,属于行业中的佼佼者,攻击这类网站可以直接给黑客带来可观的经济收益,亦有可能是竞争对手雇佣黑客所为,还有一个原因就是这类网站一般服务器配置较高,黑客喜欢攻下此类服务器做为“肉鸡”。曾有某公司服务器攻击别人被公安部门检查后发现被人植入木马后远程操作所为。

3. 政府及电子政务类网站

近两年来政府及电子政务类网站逐渐成为黑客的新目标,更是国外黑客攻击的直接目标,据我们调查,某国黑客网站联盟针对全球政府网站进行黑客比赛,将所黑政府网站及上传至该网站的文件罗列出来,据观察仅国内每日就有数十家被黑。至于国内黑客近年也愈来愈胆大,前几日某地方公安厅网站被黑,黑客书:“别以为是公安部门我就不敢黑你,有漏洞照黑!”

4. 各大商业银行网站

银行网站一直是被众多不法分子偷窥的重点对象,同时也不缺乏恶作剧者,前几天工商银行网站被黑,网站上被黑客写下:“工商银行倒闭,所有存款没收!”的字样,引起一片轰动。同时也是钓鱼者模仿攻击最多的网站,使用网上银行者需要小心提防。

5. 流量较大的行业门户网站

黑客攻击此类网站的直接目的是为了给其它网站带来流量或者是通过此类网站往用户电脑中植入木马或者流氓软件。通过调查发现不少被黑的行业门户网站上均有黑客所留下的某个网址或者是某个网页木马,或许很多朋友浏览网站后自己中了木马仍不知晓。

在你的网站被黑之前,你可以做些什么?

“只有绝对的不安全,没有绝对的安全”,所有互联网相关企业都会面临网站被攻击的危险。目前中国互联网领先的大网站,无不遭受过被黑、被攻击的命运,那么你的网站迟早都会被攻击。那么在此之前,你可以为自己的网站安全作些什么呢?

1、做好数据备份

对于任何网站,都必须做好数据备份,你可以采取的备份措施有多种多样,但是无论备份如何,都只是做到了最坏的打算,大不了我恢复数据。但是备份是一种必须要做的措施,但无法主动应对安全问题。而且,在被黑之后,恢复备份之前,你的网站处于不可服务状态,你的直接损失无法金钱衡量。

2、购买更好的硬件

购买硬件是可以提高服务质量,但很遗憾,根本无法抵挡黑客攻击,而且,更快的硬件、更

高的带宽只会带来更大的攻击后危险。什么？你说防火墙！？相信不少被黑的大型网站肯定会有数百万元购置的防火墙，但仍然无法抵挡黑客的入侵。因为你只要开放一个“80”服务端口，都将有被黑的可能性，因为网站程序的缺陷硬件设备是无法帮助你解决的。

3、让程序开发部门做安全检查

不错，这是个积极的做法。但问题是：

你相信那些成天被网站老板催促的程序员真的有时间来仔细检查代码？即使检查了，你认为任何人能够轻松找出自己的代码安全隐患？另外，当产品开发追在屁股后，你真能够下决心让自己的开发停顿下来？算算程序员的开支和可能提升的安全质量吧，会有多少？

4、完善公司的内部安全机制

嗯，不错，是搞管理的，但问题是，你能够弄清楚防火墙、路由器的区别已经是花费了半天时间了，你可以将安全制度做得更好吗？或者说，即使出来了一个规范，你认为它适合你的公司现状吗？安全等级管理是一个很专业的问题。

5、聘请资深的安全管理员

嗯，是，这样加强安全措施思路没错！但接下来的问题是：

我在哪里找有实践经验的安全专家？你每年的预算是多少？你能够请多少安全专家来为你的网站规划安全计划？一个完善的解决方案应该来自于一个有丰富经验的技术团队！

6、等着被黑

不要不承认，你大部分时间是出于这种状态。当网站访问量越来越高，当用户越来越多，你的担心就越来越大，服务器可承受的压力，程序的安全性及处理数据的能力，网站被黑客骚扰的烦恼事儿会让你夜不能寐……



病毒防范

五步剿灭“机器狗”病毒

近日，江民反病毒中心率先截获的“机器狗”病毒在互联网加速传播，很多网吧用户通过邮件、论坛、电话等多种方式向江民反病毒中心求助。由于“机器狗”病毒是一种可以穿透冰点、还原卡等电脑保护系统的木马病毒，并可以借助 ARP 病毒在局域网中传播，还会下载 20 多款恶性网游木马，盗取游戏玩家的帐号和密码，危害十分巨大。同时，该病毒还可以

借助 U 盘进行传播,这样就大大增加了病毒传播的范围,即使连个人电脑用户也很有可能被感染。

江民反病毒专家介绍道,“机器狗”病毒由于采用了更为先进的传播方式,其威胁甚至超越了去年的“熊猫烧香”。该病毒会首先通过网页木马或 U 盘传播方式入侵到电脑中,然后在局域网中通过 ARP 欺骗等方式进一步的传播。江民反病毒专家预计,该病毒将会持续出现变种,威胁不可小视,因此不论是网吧用户或是个人用户,都需要及时采用防范措施,防止病毒的进一步入侵。

由于该病毒多发生于网吧和企业,因此江民科技反病毒专家建议采取以下安全策略来加固自己的网络:

1、由于机器狗病毒是借助于 ARP 欺骗的方式在局域网中传播,因此做好 ARP 欺骗的防范工作十分必要。建议有条件的网吧和企业,采用双向绑定策略,在交换机或路由器上绑定好全网的 IP-MAC 地址,在客户端绑定好网关的 IP-MAC。这样即便是局域网中某台电脑感染了 ARP 病毒,该电脑也不会干扰全网的运行。双向绑定策略是抵御 ARP 病毒的好办法。

如果不具备双向绑定的条件,可以采用划分 VLAN 的方法,来隔离网络的不同区域,这样可以把 ARP 病毒的危害降低到最小。

2、更新好系统漏洞补丁,尤其是网页木马常用漏洞:MS06-014 和 MS07-017。目前根据江民科技反病毒中心恶意网址跟踪结果来看,发现绝大部分的网页木马都是利用以上两个系统漏洞入侵到计算机中的,因此打好补丁十分关键。

MS06-014 中文版系统补丁下载地址:

<http://www.microsoft.com/china/technet/security/bulletin/MS06-014.msp>

MS06-014 英文版系统补丁下载地址:

<http://www.microsoft.com/technet/security/Bulletin/MS06-014.msp>

MS07-017 中文版系统补丁下载地址:

<http://www.microsoft.com/china/technet/security/bulletin/MS07-017.msp>

MS07-017 英文版系统补丁下载地址:

<http://www.microsoft.com/technet/security/bulletin/MS07-017.msp>

3、注意应用软件版本的及时更新。“机器狗”病毒除了利用以上两个系统漏洞通过网页木马的方式入侵到电脑中,还利用时下最为流行的应用软件漏洞进行挂马传播,例如一些聊天工具漏洞、播放器软件漏洞、网络电视软件漏洞、游戏软件漏洞、甚至是一些常用的下载工具的漏洞都会成为病毒的传播途径。由于应用软件的用户群体更为广泛,这也就成了病毒作者传播病毒的又一“利器”。因此要注意软件的版本,一定要使用从官方网站下载的最新版本的软件,这点十分重要,不要使用老版本,因为老版本还有很多漏洞。

4、禁用 Windows 系统的自动播放功能。这一点对个人用户来说同样重要,由于“机器狗”病毒还会利用 U 盘传播,因此如果 U 盘中含有此病毒时,如果直接双击打开 U 盘,就会激活病毒,从而感染进电脑中。建议用户通过组策略的方式禁用 U 盘的自动播放功能。

关闭自动播放功能方法如下:在“开始”菜单的“运行”框中运行“gpedit.msc”命令,在“组策略”找到“计算机配置”和“用户配置”下的“管理模板”功能,打开其中的“系统”菜单中的“关闭自动播放”的设置,在其属性里面选择“已启用”,接着选择“所有驱动器”,最后确定保存即可。江民杀毒软件“移动存储接入杀毒”能杜绝病毒利用移动设备(如:U 盘、移动硬盘等)入侵用户计算机,保护计算机系统安全。

5、及时升级 KV 杀毒软件病毒库,上网时确保打开“网页监控”、“邮件监控”功能。

建议企业级用户和网吧部署 KV 网络版杀毒软件,KV 网络版具有全网统一升级,统一杀毒功能,可以快速彻底清除网络中的 ARP 病毒和“机器狗”病毒及其变种。

07 反病毒市场杂谈 毒客投入更具“钱途”产业

2007 年是互联网蓬勃发展的一年，电子商务、搜索引擎、视频网站、社交网络都触手可及。2007 年是网络安全问题大爆发的一年，从 06 年隐藏在木马背后的灰色产业链走到台前，有越来越多的毒客、准毒客转身投入这一更有“钱途”的产业，网页挂马、ARP 欺骗、0Day 漏洞、U 盘病毒、Rootkit 钩子令大家耳熟能详。

从年内几家杀毒软件厂商不约而同推出的互联网安全报告中我们可以看到，虽然统计数字略有差异，但都显示了一个事实，即：变化多端、针对性强的木马程序成为了安全威胁的主流，而其他蠕虫、漏洞病毒也几乎都是为木马来服务的，其目的就是通过自身传播能力、攻击能力，以自身为载体将木马安装到用户系统中。

病毒分布

在 2007 年上半年，仅金山毒霸就截获新增病毒样本十多万种，这还不包括那些小范围传播的木马、病毒，或者病毒作者为特定目标制作的定向感染病毒。也就是说，每天安全厂商发现和未发现的病毒数量已经数以千计，病毒数量的激增导致传统病毒特征库越来越大，而杀毒引擎要在庞大的病毒库中准确的发现并查杀病毒，必然会消耗大量的系统资源。国外某老牌杀毒厂商的一款网络杀毒产品就因为消耗系统资源巨大而一直饱受诟病。

而且随着软件漏洞的频频出现，尤其是 0day 漏洞的广为传播，再加上用户安全意识匮乏，常常出现反病毒软件查不到、杀不掉的病毒，用户怨声载道。为了查杀一个病毒，必需“耐心”等待反病毒厂商将相应病毒特征码加入病毒库中，升级了又发现无法彻底清除，只能返回到连盖茨都不知道是否该放弃的 DOS 系统中解决病毒。

显然传统杀毒引擎的低效率和高能耗已经跟不上安全发展的步伐，于是在下半年推出的几款杀毒软件新品中，我们都看到了主动防御的功能。这种技术比较好的弥补了传统杀毒软件采用“特征码查杀”和“监控”相对滞后的技术弱点，可以在病毒发作时进行主动而有效的全面防范，从技术层面上有效应对未知病毒的肆虐。

主动防御结构图

然而，经过几个月的使用，很多杀毒软件用户都在反映一个问题：主动防御太过敏感，稍有动静就要用户判断是否把联网的程序、进程列入黑名单。可是起码有 99% 的杀毒软件用户是对电脑一知半解的初级用户，对网络的认识更只是停留于上网聊天、看新闻、玩游戏的阶段，要我们拥有孙悟空的火眼金睛显然是强人所难。但如果不加辨别把所有可疑程序、进程统统杀掉，大概也会让电脑里的大多数程序陷入瘫痪。

三层互联网防御

据金山毒霸技术总监陈睿介绍，“互联网可信认证”通过“网络蜘蛛”技术，能够将互联网上每秒钟内生成的可执行文件进行收集，并经过自动以及人工的分析，以秒为单位对服务器端的“互联网可信认证中心”进行刷新。一旦在客户端遇到可疑行为，依据特征码不能够判定的，立即链接至服务端进行判定。这样就可以实现从新病毒出现到被识别出来，再到被查杀的周期以秒来进行计算，从而让金山毒霸 2008 对新病毒的响应速度提升了 60 倍。

此外，“互联网可信认证”可以利用服务器海量的数据库对可疑文件自行做出判断，极大的减少用户对杀毒的干预，同时也大大提高了判断的准确率，而网民不论是上网聊天、玩游戏还是日常工作中，都不会轻易被打断了。

虽然“互联网可信认证”作为新兴的互联网防木马、反病毒技术，其成功与否在没有经历时间和大量网络攻击的考验之前尚言之过早，但至少有了来自互联网的安全防卫，我们不再必提心吊胆的上网了。

2007 年已经过去，我们期待着 2008 年电脑病毒能够有所收敛，然而这一想法似乎有些不切实际；所以我们只能期盼着我们的杀毒软件能够更加强悍一些，魔高一尺，道高一丈，希望杀毒软件能够真正担负起保护用户电脑的重任！



安全新动态

2007 年发生的安全事件大回顾

病毒越来越多，ARP 猖獗，一个烧香的熊猫带来了很大的危害，黑客攻击越来越多，2007 年已经在一系列的安全事件中结束了。在迎接 2008 的同时我们也对 2007 年发生的安全事件做一个全面的总结。

2007 年安全日历：

MSN 蠕虫病毒借助“圣诞照片传播”-12 月
Google 大清洗 4 万恶意网站被删除-11 月
Leopard 遭破解 苹果干不过“黑客”帝国-11 月
国庆期间近百万台电脑感染两万余种病毒-10 月
中国女解码高手十年破译五部顶级密码-09 月
黑客入侵中国游戏中心系统 盗 22 亿游戏币-08 月
北京警方破获首例 DDoS 黑客攻击案-07 月
少年黑客狂攫千万之谜-06 月
半年 22 次重大误杀 瑞星称卡巴斯基蔑视中国用户-05 月
温柔地“杀”死你 诺顿误杀事件专题报道-05 月
取代美国 中国成“恶意软件”头号基地-04 月
灰鸽子病毒 新一轮“熊猫烧香”来袭？-03 月
互联网遭受五年以来最大规模黑客袭击-02 月
“熊猫烧香”病毒作者已被逮捕！-01 月

2007 年需关注的其它安全事件：

灰鸽子，你大规模爆发了吗？(3 月)
金山官方网站遭恶性木马团伙攻击(3 月)
特洛伊手机病毒已开始“招摇撞骗”(4 月)
全国首例 Q 币盗窃案：两 Q 币大盗获刑 13 年(4 月)
我国测试首个量子系统 密码将不可破译(4 月)
加大打击力度“反恶意软件法”明年出台(7 月)
深度揭秘：黑客如何通过虚拟世界生财？(8 月)
黑客公布 iPhone 破解软件 2 分钟摆脱限制(9 月)
外交部：我军黑客攻击美国防部毫无根据(9 月)
“熊猫烧香”案已宣判 主犯李俊获刑四年(9 月)

网吧频遇离奇病毒 病毒“机器狗”被截获(11 月)
首例自动升级的“U 盘寄生虫”病毒被截获(11 月)
英媒编造解放军指使黑客攻击英企业(12 月)
惠普 82 款笔记本存在严重网络安全漏洞(12 月)



安全新生活

上网安全防护指南

1.如果不是必须，不必填写你的个人资料

在允许留空的地方留空就行了。

2.如果不是必须，不必填写你的真实资料

如果可以，不妨填写一个虚拟的资料。如果你怕以后忘了，可以填写一个固定的虚拟的资料，把它保存在一个地方，如你的邮箱里。

3.E-mail、手机号码不要直接发布在公开显示的地方

E-mail 只要公开了，处于可被搜索引擎抓取的地方，100%会成为一个垃圾场。

4.避免你的昵称和真实身份联系在一起

如果你不想让身边的人知道你网上的身份，或者不想让网上的人知道你现实的身份。

5.谨慎使用“记住密码”的功能

随时清除 Cookies，这一点对多人共用计算机适用。

6.不要一个邮箱通天下

用于和机器打交道的 E-mail 应该和用于和人打交道的 E-mail 分开。你可以用某个信箱专门用来注册，这样可以保证最大的安全。

7.不要一个昵称通天下

想想 Mop 的人肉搜索吧，你应该知道，如果在多个网站、论坛使用同一个昵称，如果别人需要，很容易可以追踪到。

8.不要一个密码通天下

至少，你使用某一个服务时，你的服务密码和在这个服务里所留的 E-mail 密码不要一样。如果你的某帐号被盗，你取回密码到邮箱，发现邮箱已经顺带被搞定了。

9.如果短时间内有大量 QQ 添加你为好友，拒绝

QQ 号码申诉的条件之一就是知道你好友里的五个号码。

10.不要点击任何 E-mail 里和 IM 里传送过来的网址



新好软件

个人用户经典国外反病毒反黑客软件组合

经典个人用户国外反病毒防火墙组合主要有以下几款：

1. 卡巴+OP 防火墙（兼容好防范强，占用资源相对较大）推荐高配置：CPU2.0 以上 512 内存
2. Mcafee +LNS 或(OP)（很经典的杀防组合，不过设置较复杂）中配置以上的都能用
3. NOD32+LNS 或(OP)（NOD32+LNS 组合占用资源最小，官方推荐的 OP 占用大些但很稳定）低配置用户可参考使用
4. AVK+jetico 或(OP)（AVK 双引擎杀毒，非常酷的组合，可惜 AVK key 太难找...）占用资源相对较大，推荐有能力找到 key 的高配置电脑使用。
5. Avast+ZA（比较讲究实用性的组合）占用资源相对不大。
6. 目前人气非常好的反病毒软件：

AntiVir 小红伞免费版：杀毒好兼容强，除了没有没有中文版的遗憾外，其他表现都不错。
dr.web 绿蜘蛛：杀毒强悍，资源占用小，缺点 key 比较难找，不过有升级器可以方便升级。
与之相配的防火墙在(LNS, OP, jetico, Tiny, ZA)任选一款都可以。

辅助杀毒可装费尔（国产软件兼容好占用非常小，对国产病毒木马反映敏感），监控可考虑 GSS，还可加装 AVK2006 精简免安装版不占用系统资源按时扫描杀毒效果与安装版一样的好。另 ZA 防火墙易用省心不过占用资源相对较大，与某些软件有冲突。jetico 防火墙占用很小效果很棒，但设置过于复杂，还有很好的墙 Tiny 推荐有一定基础的网友使用。呵呵，总之看自己喜好决定吧。~

个人认为：选用 Mcafee 8.0i+LNS 或(OP)组合再加装 AVK2006 精简免安装版是最强悍全面的杀防组合。。偶的配置不高选用了 NOD32+费尔+LNS 外加 AVK2006 精简免安装版+ewido 绿色版扫描，另有一些防杀间谍木马广告的，个人感觉已经够用的了。

选用软件的基本原则应该是：不讲最新，而求最稳定最适合自己配置和使用习惯的才是正确的。另外需说明一下的除非你对杀软有兴趣要研究杀软或有别的用处，一般用户不要安装两个以上的正式反病毒软件，设置使用不当容易造成严重的软件冲突而崩溃系统。



办公新天地

易记忆而又安全的密码

用户们经常会忘记自己的密码。为了不忘记密码，他们就是用些简单的信息来创建密码，比如用养的狗的名字，儿子的名字和生日，目前月份的名称——或者任何可以帮助他们记住密码的东西。

对于那些侵入你的计算机系统的黑客来说，你创建的这些密码毫无作用，就好比把门锁上了却把钥匙扔在门外的擦鞋垫上一样。黑客不需要使用特殊工具就能发现你个人的基本信息——名字，孩子的名字，生日，宠物名字，等等。他可以把这些作为破解你密码的线索——尝试。

想要创建安全又好记的密码，请遵循如下几个简单的要求：

1) 别用个人信息

永远不要用个人信息来创建密码。别人很容易猜到你可能用姓，宠物名字，孩子的出生日期或者其他类似的细节。

2) 别用真实的单词

黑客们能用某些工具猜出你的密码。现今的计算机不需要花很久的时间就可以把字典中的所有单词都试一遍，然后找出你的密码。所以你最好别用真实的单词做密码。

3) 混用不同体的字符

混用不同的字体的字符可以使你的密码更安全。既用大写字母也用小写字母，以及数字，甚至诸如‘&’和‘%’等。

4) 使用惯用语

除了记住那些用各种字符组成的密码，你还可以使用惯用语，它同样可以组成不是字典中的单词的密码。你可以想出一句话或者一行你喜欢的歌曲或诗歌，用它每个单词的首字母创建一个密码。

例如，与其创建一个‘yr\$1hes’这样的密码，你不如用“i like to read the about.com internet / network security web site”这句话，把它转成如“il2rta!nsws”这样的密码。这个密码中，我们用‘2’取代‘to’，并且用惊叹号代替‘internet’的首字母‘i’。你也可以用各种各样的字符来创建难以被破解的密码，并且便于自己记忆。

5) 使用密码管理工具

安全地储存和记忆密码的另一个办法就是使用密码管理工具。这类工具把用户名密码加密后保存。有些甚至可以在你访问网站时自动向站点或者应用程序填写用户名和密码信息。

6) 使用不同的密码

如果想要保护你的账户和程序，你应该为每个应用使用不同的用户名和密码。即使其中的某一个密码被破解了，你其他的密码还是安全的。另一个方法比这种方法的安全性略低，但是它可以使你在安全与方便之间取个折衷。这种方法就是对那些不需要额外保障其安全性的应用都是用一套用户名和密码，而在你的银行或者信用卡的网站则用单独的用户名和更安全的密码。

7) 经常更换密码

你应该至少每 30 到 60 天就应该更换密码。并且至少一年之内不应当重复使用同一个密码。

8)加强密码的安全性

与其依靠计算机的每一位使用者去理解并遵循以上的建议,你还不如给操作系统配置密码策略,这样系统将不接受那些不符合最低安全要求的密码。



局域网安全

10 大方法减少内部人员安全风险

如今内部人员给公司的安全造成的威胁非同小可。近来的一些报告指出,内部人员对公司的损害在所有的危害事件中已从 80%上升为 86%,而且超过半数发生在雇员的终端。无疑,拥有访问公司系统权限的内部雇员极有可能被误导到那些欺诈性的或危险的链接上。而在所有的雇员中,IT 工作人员拥有的这种访问权限最多。因此,IT 审核应关注从多个方面确认风险。下面我们给出实施有关控制和减少工作人员对管理员欺诈的方法。

1.IT 安全策略

管理人员应该审视那些能够管理特权账户(如域管理员账户、应用程序管理员账户、数据库管理员)的 IT 安全策略,要保障安全策略的存在,还要清楚存取访问是如何被处理、验证、证明的,要确保对这些策略定期进行审查。否则,基本上就不存在管理特权访问的基础了。在没有相关报告的情况下,管理特权账户的策略是不完整的。特权账户的口令审核报告经常要涉及到如下的问题:口令何时更新、更新失败有哪些,以及在一个共享账户下,个别用户如何执行任务等等。

制定的策略应具有这样的目标:能够终止明显的不可防御的用户活动。要确保所有的雇员、订约人和其它用户清楚其责任,从而与 IT 的安全策略、方法以及与其角色相适应的相关指导等。

2.“超级用户”账户和访问

了解公司与用户访问有关的暴露程度是很重要的。应该决定拥有访问特权的账户和用户的人员,并获得对网络、应用程序、数据和管理功能的访问有较高权力的所有账户列表。包括通常被忽视的所有计算机账户。由此,要确保用户访问能够被检查,并确保其拥有恰当的许可。一个好方法是定期地审查用户访问,并决定数据和系统的“所有者”已经得到明确授权。

3.账户和口令配置标准

要保证所有的管理员账户能够根据策略更新。在特定设备上,不应存在默认的口令设置。对那些拥有足够的默认账户和口令资源的用户来说,其信息是很丰富的。有一些安全账户,其

账户名就是口令，这简直是自寻烦恼。设置口令的期限也是很重要的，禁用某些明显的临时账户也是很聪明的作法。

4. 对口令的受控访问

对权力有所提升的账户和管理员的口令存取要加以管理。其道理可能很明显，不过对口令的共享访问并非总能得到控制。离线的记录或开放性的访问，如包含口令的电子邮件，就不应当存在。即使一个加密的口令文件也是不足取的。在最糟的情形中，口令文件的口令并没有得到控制。

5. 服务账户(“机器”账户)

服务器也可以被提升权限，并用于各种罪恶的目的。这些账户典型情况下并不分配给人类用户，并且也不包括在传统的认证或口令管理过程中。这些账户可被轻易地隐藏。管理员应该保障服务账户只拥有必要的访问权。这些账户应该定期检查，因为它们经常拥有超级用户的能力。这种用户的数量是很多的，而且还有许多不用的账户也需要注意。

6. 高风险用户和角色

有一些公司积极地监视某些角色，这些角色对企业会造成极高的风险，企业的监视会发现其潜在的“不可接受”的行为。许多企业拥有一些风险极高的关键角色。例如，一位采购经理为谋求一个职位可能会将自己能够访问的敏感数据带到另外一家竞争公司那里去。这种情况下，其访问是被授权的，不过却存在着滥用的情况。岗位、职责的轮换以及设定任命时间是对付高风险的一个重要方案。注意：IT 安全专家通常都属于高风险角色的范围。

7. 安全知晓项目

任何雇员或用户都可能造成一种威胁。贯彻执行一个可以处理上述所有要点的安全知晓项目，并能保证其强制实施势在必行。现在有许多方案能够确保所有的用户已经阅读并同意有关规则和政策。其中一种工具是在用户登录时要求其在警告消息上签名，要求用户确认其同意并选择窗口中的“接收”或“同意”复选框。

8. 背景筛选

背景筛选就是要认真地问雇员一些措词严格的问题，以揭示其特定行为和态度的危险信号，例如：

- 违规的或异常的工作经历：离开工作的可疑理由、长期未被雇用的原因
- 欺诈：在某些事实上（例如教育、以前的雇佣关系）的虚伪陈述
- 人格/态度问题：与同事或管理人员的糟糕关系
- 挫败、威信问题、猜疑、无力接受改变等

9.事件记录

安全事件记录提供了实时使用和活动的透明度。精确而完整的用户及其活动的记录对于事件分析和制定额外的安全措施是至关重要的。获取访问的方法、访问范围和过去的活动是很重要的。为保证有充足的记录，应考虑改善对较高风险领域和服务的记录利用。

10.证据

管理人员应熟悉所使用的不同存储设备，如果有任何可疑迹象，还应具备“指纹”知识的足够知识水平。这可以是 cookie 数据、隐藏的操作系统数据等。从公司系统中获取关键文件并将其放置到闪速存储器上是很简单的事情，这些闪速设备可被伪装为数码相机、个人数字助理（PDA）或移动电话等。还有一些调查人员从移动电话中收集和分析信息，因为这种设备可包含语音邮件、正文消息、地址文件、电话号码和许多遗漏电话、已接电话等。如果有任何可疑的非法活动，就应保留相关证据，直至最终决定其结果。



网管经验谈

来者是客-—微软内部增强系统安全的秘技

本实战内容将需要管理员权限。所谓入侵，无非就是利用某种方法获取到管理员级别的权限或系统级的权限，以便进行下一步操作，如添加自己的用户。如果想要使入侵者“进来”之后不能进行任何操作呢？永远只能是客人权限或比这个权限更低，就算本地登录，连关机都不可以。那么，他将不能实施任何破坏活动。

注意：此法有较高的危险性。建议完全不知道以下程序用途的读者不要尝试，以免误操作引起系统不能进入或出现很多错误。

第一步：确定要设置的程序

搜索系统目录下的危险程序，它们可以用来创建用户夺取及提升低权限用户的权限，格式化硬盘，引起电脑崩溃等恶意操作：`cmd.exe`、`regedit.exe`、`regsvr32.exe`、`regedt32.exe`、`gpedit.msc`、`format.com`、`compmgmt.msc`、`mmc.exe`、`telnet.exe`、`tftp.exe`、`ftp.exe`、`XCOPY.EXE`、`at.exe`、`cacls.exe`、`edlin.exe`、`rsh.exe`、`finger.exe`、`runas.exe`、`net.exe`、`tracert.exe`、`netsh.exe`、`tskill.exe`、`poledit.exe`、`regini.exe`、`cscript.exe`、`netstat.exe`、`issync.exe`、`runonce.exe`、`debug.exe`、`rexec.exe`、`wscript.exe`、`command.com`、`comsdupd.exe`

第二步：按系统调用的可能性分组设置

按照下面分组，设置这些程序权限。完成一组后，建议重启电脑确认系统运行是否一切正常，查看“事件查看器”，是否有错误信息（“控制面板→管理工具→事件查看器”）。

(1)`cmd.exe`、`net.exe` `gpedit.msc` `telnet.exe` `command.com`

（仅保留你自己的用户，SYSTEM 也删除）

(2)mmc.exe、tftp.exe、ftp.exe、XCOPY.EXE、comsdupd.exe

(仅保留你自己的用户，SYSTEM 也删除)

(3)regedit.exe、regedt32.exe、format.com、compmgmt.msc、at.exe、cacls.exe、edlin.exe、rsh.exe、finger.exe、runas.exe、debug.exe、wscript.exe、cscript.exe、rexc.exe

(保留你自己的用户和 SYSTEM)

(4)tracert.exe、netsh.exe、tskill.exe、poledit.exe、regini.exe、netstat.exe、issync.exe、runonce.exe、regsvr32.exe

(保留你自己的用户和 SYSTEM)

第三步：用户名欺骗

这个方法骗不了经验丰富的入侵者，但却可以让不够高明的伪黑客们弄个一头雾水。

打开“控制面板—管理工具—计算机管理”，找到“用户”，将默认的 Administrator 和 Guest 的名称互换，包括描述信息也换掉。完成后，双击假的“Administrator”用户，也就是以前的 Guest 用户。在其“属性”窗口中把隶属于列表里的 Guests 组删除。这样，这个假的“管理员”账号就成了“无党派人士”，不属于任何组，也就不会继承其权限。此用户的权限几乎等于 0，连关机都不可以，对电脑的操作几乎都会被拒绝。如果有谁处心积虑地获取了这个用户的权限，那么他肯定吐血。

第四步：集权控制，提高安全性

打开了组策略编辑器，找到“计算机设置→windows 设置→安全设置→本地策略→用户权利指派”(见图 4)，接着根据下面的提示进行设置。

(1)减少可访问此计算机的用户数，减少被攻击机会

找到并双击“从网络访问此计算机”，删除账户列表中用户组，只剩下“Administrators”；找到并双击“拒绝本地登录”，删除列表中的“Guest”用户，添加用户组“Guests”。

(2)确定不想要从网络访问的用户，加入到此“黑名单”内

找到并双击“拒绝从网络访问这台计算机”，删除账户列表中的“Guest”用户，添加用户组“Guests”；

找到并双击“取得文件或其他对象的所有权”，添加你常用的账户和以上修改过名称为“Guest”的管理员账户，再删除列表中“Administrators”。

(3)防止跨文件夹操作

找到并双击“跳过遍历检查”，添加你所使用的账户和以上修改过名称为“Guest”的管理员账户，再删除账户列表中的“Administrators”、“Everyone”和“Users”用户组。

(4)防止通过终端服务进行的密码猜解尝试

找到并双击“通过终端服务拒绝登录”，添加假的管理员账户“Administrator”；找到“通过终端服务允许登录”，双击，添加你常用的账户和以上修改过名称为“Guest”的管理员账户，再删除账户列表中的“Administrators”，“Remote Desktop User”和“HelpAssistant”(如果你不用远程协助功能的话才可删除此用户)。

(5)避免拒绝服务攻击

找到并双击“调整进程的内存配额”，添加你常用的账户，再删除账户列表中的“Administrators”

安全特训班

熟记安全顺口溜，不懂安全也风流

密码设全，文件收好；
外出锁屏，下班关机；
常打补丁，定期杀毒；
版权保护，法不容情；
便携设备，注意监护；
网络内外，品行一致；
复印传真，严格程序；
邮件论坛，言必由“忠”；
执行制度，贵在坚持；
信息安全，人人有责；

安全大调查

你不能不考虑的安全因素

信息安全工作是复杂的，正是由于它是受多方面因素影响的。作为网络技术主管人员，以下安全因素中你会考虑哪些？

- 1、安全管理
- 2、安全意识
- 3、应用安全
- 4、数据安全
- 5、操作系统安全
- 6、容灾、备份、恢复
- 7、其他

欢迎登陆 <http://bbs.sec120.com> 参与调查。



技术哈哈镜

安全管理领域，最神秘的事情

在安全管理领域，最神秘的事情之一就是入侵者的行为方式。入侵者会做什么事情？以及他们是如何来做的？同所有重大的秘密一样，它也让许多人产生了浓厚的兴趣，同时也解释了关于实际网络攻击的书籍和教程大受欢迎的原因。如果你不具备所有正当访问权限的话，抛开违反法律不谈，对网络进行攻击可能令人乐趣无穷并且增长见识，然而事实却是，我们当中的绝大多数人并不需要知道如何去进行攻击。坦率地说，成为一名优秀的渗透测试人员仅仅需要参加一个多星期的课堂教育。而此外还需要信守承诺、奉献精神、直觉及对技术的良好悟性，不用说，还有对做事情的规则及正当方法的公然漠视。在许多情况下，这些技术并非绝大多数安全管理员能够具备，或者说必需的。

在绝大多数时候，雇佣一些这样的人来实施网络渗透测试，这样做成本低廉并且能够达到更好的效果。职业渗透测试人员发现问题的能力将会高人一筹，同样还能清晰地找出导致这些问题的根源。那么，为什么那些讲述网络攻击的书籍或课程如此受到欢迎呢？嗯，坦率地说，这主要归咎于网络攻击的神秘性和其认知难度。同样地，如果一名系统管理员有能力实施基本渗透测试的话，那么他的价值将会得到提升。

然而，本刊物的侧重点稍有不同。对于具体网络攻击如何发生的细节，本刊物主要目的是为了帮助大家对于导致问题的那些操作实践有相当清醒的认识。这样你可以通过避免犯这些可能被入侵者所利用的错误，来保护你的网络。



职场美文

技术人员必须知道的十条良言

1、好好规划自己的路，不要跟着感觉走！根据个人的理想决策安排，绝大部分人并不指望成为什么院士或教授，而是希望活得滋润一些，爽一些。那么，就需要慎重安排自己的轨迹。从哪个行业入手，逐渐对该行业深入了解，不要频繁跳槽，特别是不要为了一点工资而转移阵地，从长远看，这点钱根本不算什么，当你对一个行业有那么几年的体会，以后钱根本不是问题。频繁地动荡不是上策，最后你对哪个行业都没有摸透，永远是新手！

2、可以做技术，切不可沉湎于技术。千万不可一门心思钻研技术！给自己很大压力，如果你的心思全部放在这上面，那么注定你将成为孔乙己一类的人物！适可而止为之，因为技术只不过是你今后前途的支柱之一，而且还不是最大的支柱，除非你只愿意到老还是个工程师！

3、不要去做技术高手，只去做综合素质高手！在企业里混，我们时常瞧不起某人，说他“什么都不懂，凭啥拿那么多钱，凭啥升官！”这是普遍的典型的工程师的迂腐之言。8051 很牛吗？人家能上去必然有他的本事，而且是你没有的本事。你想想，老板搞经营那么多年，难道见识不如你这个新兵？人家或许善于管理，善于领会老板意图，善于部门协调等等。因此务必培养自己多方面的能力，包括管理，亲和力，察言观色能力，攻关能力等，要成为综合素质的高手，则前途无量，否则只能躲在角落看示波器！技术以外的技能才是更重要的本事！！从古到今，美国日本，一律如此！

4、多交社会三教九流的朋友！不要只和工程师交往，认为有共同语言，其实更重要的是和其他类人物交往，如果你希望有朝一日当老板或高层管理，那么你整日面对的就是这些人。了解他们的经历，思维习惯，爱好，学习他们处理问题的模式，了解社会各个角落的现象和问题，这是以后发展的巨大的本钱，没有这些以后就会笨手笨脚，跌跌撞撞，遇到重重困难，交不少学费，成功的概率大大降低！

5、知识涉猎不一定专，但一定要广！多看看其他方面的书，金融，财会，进出口，税务，法律等等，为以后做一些积累，以后的用处会更大！会少交许多学费！！

6、抓住时机向技术管理或市场销售方面的转变！要想有前途就不能一直搞开发，适当时候要转变为管理或销售，前途会更大，以前搞技术也没有白搞，以后还用得着。搞管理可以培养自己的领导能力，搞销售可以培养自己的市场概念和思维，同时为自己以后发展积累庞大的人脉！应该说这才是前途的真正支柱!!!

7、逐渐克服自己的心里弱点和性格缺陷！多疑，敏感，天真（贬义，并不可爱），犹豫不决，

胆怯，多虑，脸皮太薄，心不够黑，教条式思维。。这些工程师普遍存在的性格弱点必须改变！很难吗？只在床上想一想当然不可能，去帮朋友守一个月地摊，包准有效果，去实践，而不要只想！不克服这些缺点，一切不可能，甚至连项目经理都当不好--尽管你可能技术不错！

8、工作的同时要为以后做准备！建立自己的工作环境！及早为自己配置一个工作环境，装备电脑，示波器（可以买个二手的），仿真器，编程器等，业余可以接点活，一方面接触市场，培养市场感觉，同时也积累资金，更重要的是准备自己的产品，咱搞技术的没有钱，只有技术，技术的代表不是学历和证书，而是产品，拿出象样的产品，就可技术转让或与人合作搞企业！先把东西准备好，等待机会，否则，有了机会也抓不住！

9、要学会善于推销自己！不仅要能干，还要能说，能写，善于利用一切机会推销自己，树立自己的品牌形象，很必要！要创造条件让别人了解自己，不然老板怎么知道你能干？外面的投资人怎么相信你？提早把自己推销出去，机会自然会来找你！搞个个人主页是个好注意！！特别是培养自己在行业的名气，有了名气，高薪机会自不在话下，更重要的是有合作的机会...

10、该出手时便出手！永远不可能有 100%把握!!! 条件差不多就要大胆去干，去闯出自己的事业，不要犹豫，不要彷徨，干了不一定成功，但至少为下一次冲击积累了经验，不干永远没出息，而且要干成必然要经历失败。不经历风雨，怎么见彩虹，没有人能随随便便成功！



网络笑话

一个网管的自白

现在的网吧客人 98%都他妈的 SB，开机不会，输入法切换不会，字母大小写转换不会，玩私服登陆器怎么用不会，QQ 开语音不会，进了游戏不会退出，私服服务器关了说我机子问题，**，老子真想一把捏死他，捏死再揉成一团，再搓成麻花，放油锅里炸，再拿出来一脚踩的粉碎

语音聊天不会开 MIC,说网吧耳机是坏的.

看电影嫌不是普通话的!

问我:"网管,有没有毛片看?"我说没,他怪电影不全!

QQ 登陆不上说机器不好!老子跑过去一看,密码不对,那丫的还问我密码多少!!!!

还有一个更厉害的 sb 小姐,.接了一个不认识的网友的视频,喊我过去,问我视频里的人是谁!!!

MD,老子还有这本事????!!!!!!

打个 CS 别人放颗烟雾弹，他遭闪了，狂喊：网管死机了……

操 TM 的，前天一个 SB MM 聊 QQ 问我怎么打字的。我问她，你不会打字吗。她说会。我说，哪你打字就行了(同时帮她调好输入法)，一会又叫我。说：网管，我怎么打不出来字啊。我说你要打什么字打不出来，她告诉我说：你先打个"你好吧"，我帮她打了。然后你们

知道她怎么说的吗。你别走了。就坐在我边上帮我打字吧。操 TM 的，长的全然就是一个恐龙。今天有 SB 问我，网管我这里怎么没有 QQ 币呢，你帮我下载点 QQ 币……我靠 TM 的那玩意要是能下载～！我他妈地就不用上班了～



网站风采

500WAN-----彩民的真诚朋友

500WAN 彩票网 (www.500wan.com) 是一家服务于中国彩民的互联网彩票合买代购交易平台,是当前中国彩票互联网交易行业的领导者。500WAN 彩票网以服务中国彩民为己任,为彩民提供全国各大联销型彩票的在线合买、代购和彩票软件开发、增值短信业务、WAP 移动业务等服务。

500WAN 彩票网注册用户超过八十万,日交易笔数近 70 万,是网络彩民最受推崇的互联网彩票合买交易平台。500WAN 彩票网自成立以来,已经诞生了 7 个 500 万大奖,64 个百万大奖,中奖金额近 7 个亿。

经过近 6 年的发展,500WAN 彩票网已经成为中国最受推崇的网络购彩品牌,还获得了政府主管部门的认可与扶持。湖南省体育彩票管理中心、湖南省福利彩票管理中心及江西省体育彩票管理中心已与 500WAN 彩票网达成紧密的合作关系。

凭借领先的技术和优质的服务,500WAN 彩票网深受广大彩民的欢迎并享有极高的声誉。在 500WAN 彩票网上进行彩票合买代购服务,不仅中奖简单,且操作起来十分简单。“500WAN,就这么简单!”也深刻的表达了彩民的购彩体验。

目前,500WAN 彩票网拥有了一批高素质的计算机专业人才及彩票分析专家,500WAN 彩票网良好的购买环境也吸引了大批合买高手的入住,网站平均每期中奖率达到全国 10% 的范围。

作为新型的互联彩票代购合买交易平台,500WAN 彩票网非常重视用户的个性化要求,人性化的购彩界面,没有技术门槛,使用简单,且网站 365×24 小时为彩民服务。

500WAN,就这么简单!



网站介绍

网站简介:

中国互联安全网是一家从事网络安全咨询、技术研究及提供相关服务的专业机构，拥有一流的专家团队、领先的技术优势、丰富的实践经验及完善的信息化整体解决方案。

中国互联安全网的客户遍涉军队、政府、金融、大型企业和其他行业，目前，中国互联安全网已成功为近 2000 家客户提供安全服务，同时成为多家银行、电信、政府机构及数十家全球 500 强企业最值得信赖的重要安全顾问。

我们坚持“以人为本、科技领先”的经营理念，本着团结、创新和主人翁的企业精神，努力将每个产品，每个服务做到最好“。

网站业务:

本机构致力于网络安全研究多年，以自身技术和服务为广大站长的网站保驾护航，机构主要为广大用户提供以下网站安全相关服务。

(一) 网站安全服务产品类别

产品类别名称	内容概述	适用客户对象
免费测试 (一星级服务)	为客户进行安全检测及风险评估，提供检测报告及安全系数等级（高危、高、普通、良好）。	有意向类的客户，意向协议书
YCSEC-01-1 (二星级服务)	网站安全风险评估、网站安全加固、远程安全培训、安全虚拟主机（100M 共享）	适用于虚拟主机的企业及个人用户
YCSEC-01-2 (三星级服务)	网站安全风险评估、网站安全加固、远程安全培训、主机压力测试、应用渗透测试、数据库渗透测试、网站应急响应、24 小时应急服务	适用对象：适合拥有独立的服务器，要保持网站运营稳定、数据安全的客户
YCSEC-01-3 (四星级服务)	专业防黑方案、主机防火墙方案、网站安全风险评估、网站安全加固、远程安全培训、主机压力测试、应用渗透测试、数据库渗透测试、网站应急响应、24 小时应急服务、实地安全培训、安全咨询服务	适合部分对网站安全要求相对较高的客户，例如地方门户、大型电子商务交易网站
YCSEC-01-4 (五星级服务)	网络调查取证、网络设备渗透测试、等级保证设计、网站防盗链系统、专业防黑方案、主机防火墙方案、网站安全风险评估、网站安全加固、远程安全培训、主机压力测试、应用渗透测试、数据库渗透测试、24 小时网站应急响应、实地安全培训、安全咨询服务	适合政府、金融系统等针对信息化安全管理要求较高的客户
备注说明	1、 上述服务均指单一域名，单一服务器； 2、 上述星级服务均不包含源代码审计；若有需要源代码审计费用另计； 3、 以三个月为工作周期；时间周期可协商进行；	

YCSEC-07-1 (内网安全)	计算机软硬件服务有硬件故障检查, 操作系统维护, 电脑安全等维护. 服务器有安全维护, 备份数据, 服务器的配置等维护. 打印机有故障检查与维修等服务. 网络有线路检查, 设备检查等服务.	适合于各企事业单位
----------------------	--	-----------

(二)、单项产品服务类别

YCSEC-02-1 网站风险评估	对客户给定网站进行应用渗透测试、系统渗透测试, 提供检测报告、指出具体网站安全隐患、安全漏洞等;	
YCSEC-03-1 网站安全加固	对客户操作系统、WEB 系统, 数据库, 应用程序进入安全加固. 修补安全漏洞	
YCSEC-04-1 网站应急响应	对受攻击的主机进行快速安全处理	
YCSEC-05-1 防 DDOS 攻击方案	抵御 SYN Flood 洪水攻击; 检测并阻止针对 Web 的攻击; 抵御 XDOS、HGOD、SYNKILLER、CC、GZDOS、PKDOS、JDOS、KKDOS、SUPERDDOS、FATBOY、SYNKFW 等数十种攻击; 封闭未用的服务端口	
YCSEC-06-1 APR 解决方案	抓包分析锁定攻击者+ARP 防火墙软件+网关硬件规则配置	

机构实力:

本机构实力雄厚, 拥有众多专家组成的技术团队、拥有国家颁发的资质证明。



读编信箱

您喜欢本周刊吗?

问卷调查表

随着《互联安全周刊》邮寄量的迅猛增长, 为了让更多有需要的人士收到我们的刊物, 我们将在公司网站内增加《互联安全周刊》的链接的同时, 拟发行电子版, 将月刊用 E-MAIL 的形式, 发给业内同仁。

若您觉得《互联安全周刊》确实能带给您资讯及潜在商机, 希望长期拥有, 敬请下载表格或将下述表格打印填写后, 传真或 E-MAIL 给我们。未填写问卷调查表的读者, 我们将保留不再邮寄《互联安全周刊》的权力。

通过填写此问卷, 您可以: 获得我司 08-09 年全年《互联安全周刊》及电子期刊

一、您本人是

互联安全周刊 2008 年第 1 期

产品商 采购商 企业网站负责人 技术主管 技术爱好者 其它_____

二、您了解信息安全服务的途径是（可多选）

不了解 专业杂志 《互联安全周刊》
 销售人员推荐 电视/报纸广告
 其它：_____

三、您对信息安全服务的理解是（可多选）：

防病毒防木马 365 天永远不被黑客骚扰
 网站的安全保镖 必要的投资
 其它：_____

四、您认为什么样的信息安全服务是最愿意接受的，应成为（可多选）：

网站建设、网站托管、网站安全等最齐全的服务
 有关安全人才、安全产品买家、卖家需求最集中的平台，成为安全服务中心
 国内安全产品集中展示平台，让各企事业单位买家对安全产品有最全面的了解
 成为业内最新资讯、产品最新潮流、创新研发最新成果的发布渠道
 其它：_____

五、您对《互联安全周刊》的建议和意见：

六、我希望能收到整年免费的《互联安全周刊》：

姓名：_____ 部门：_____ 职位：_____
公司名：_____
地址：_____ 邮编：_____
E-MAIL：_____ 电话：_____

七、我想把整年的《互联安全周刊》寄给我的朋友/生意伙伴：

姓名：_____ 部门：_____ 职位：_____
公司名：_____
地址：_____ 邮编：_____
E-MAIL：_____ 电话：_____

请填写此表后，传真或 E-MAIL 给： 020-020-32068532 32068416 32068703 32051815
32051816 / kf@sec120.cn 唐湘香 小姐。



支持单位：

鸣谢以下单位的支持：

广东省科学技术厅
广东省劳动和社会保障厅
广东省公安厅
广东省对外经济贸易厅
广东省总工会技协办

广州市计算机信息网络安全协会
广西壮族自治区计算机信息网络安全协会
云南省计算机信息网络安全协会
网易科技
四川君和会计师事务所
广东金桥百信律师事务所
广东源通律师事务所
广东太格有限责任公司
天融信科技公司广州分公司
启明科技公司广州分公司

本刊声明：

为适应网络安全事业发展的需要，配合广东乃至全国网络安全工作的开展，中国互联安全网经过慎重决定，经报请主管机构广州市计算机信息网络安全协会审核；特组织专家技术团队撰稿编辑《互联安全周刊》，以实际行动为全国信息安全工作做出应有的贡献。

《互联安全周刊》以网络安全技术为主导内容，让读者更好地了解安全知识，做好各种安全防范工作；提高读者安全意识及安全技能。周刊为公益性质免费周刊，本刊不承担任何版权及连带法律责任，版权归各作者所有。本刊创办的目的是为更好地推进中国网络安全信息化工作的发展贡献一份力量，任何人不得利用本刊从事任何违法活动，否则后果自负！

《互联安全周刊》特邀请广州市计算机信息网络安全协会黄丽玲女士担任周刊名誉主编，中国互联安全网信息安全专家担任周刊的技术顾问。

广大读者，如有需要订阅，均免费提供，请发送申请至 KF@sec120.cn，真诚的感谢您的支持，并欢迎您的参与，帮助本刊纠正错误，共同为网络安全事业发展做贡献。