 黑客在进行攻击时会借用其他系统来达到自己的目的，如对下一目标的攻击和被侵占计算机本身的利用等等。本文介绍了常见的黑客对被侵占计算机的使用方式和安全管理员相应的应对方法。 黑客进行网络攻击时，除了自己手中直接操作的计算机外，往往在攻击进行时和完成之后利用、控制其他的计算机。他们或者是借此达到攻击的目的，或者是把这些计算机派做其他的用途。本文汇总描述了黑客各种利用其他计算机的手段，希望网络与系统管理员能通过了解这些攻击办法来达到更好地进行安全防范的目的。 一、对“ 肉鸡 ”的利用 “ 肉鸡 ”这个词被黑客专门用来描述Internet上那些防护性差，易于被攻破而且控制的计算机。 1.1、本身数据被获取 原理介绍 这是一台计算机被攻破并完全控制之后，黑客要做的第一件事。很多黑客宣称自己是非恶意的，只是对计算机安全感兴趣，在进入别人的计算机时，不会进行破坏、删除、篡改等操作。甚至还有更"好心"一些的黑客会为这些计算机打补丁，做一些安全加强。 但是他们都回避了一个问题，那就是对这些计算机上本身保存的数据如何处理。确实，对别人的计算机进行破坏这种损人不利已的事情对这大多数黑客来讲没有太大意思，不过他们都不会反对把“ 肉鸡 ”上的数据弄回来保存。这时黑客再说"没有进行破坏"是说不过去的，根据计算机安全的基本原则，当数据的"完整性、可用性和机密性"中任意三者之一在受到破坏的时候，都应视为安全受到了破坏。在

被占领的计算机上可能会保存着用户信息、网络拓扑图、商业秘密、财务报表、军事情报和其他各类需要保密的数据，黑客获得这些数据（即使只是查看数据的内容而不下载）时正是破坏了保密性。在实际情况中，很多商业间谍和政治间谍都是这一类，他们只是默默地拿走你的数据而绝不做任何的破坏，而且尽最大可能地掩盖自己行动的痕迹。这些黑客希望长时间大量地得到珍贵的数据而不被发觉，这其实是最可怕的一种攻击行为。 很多黑客会在“ 肉鸡 ”上安装FTP软件或者开放FTP服务，再下载其数据，但安装软件和开放服务这样的动作很容易在系统中的各类日志留下记录，有可能被发现。而不希望被人发觉的黑客会自己建立一台FTP服务器，让“ 肉鸡 ”做为客户端把自己的数据上传过来。 防御方法 防止本身数据资料不被窃取，当然首先要考虑的是计算机本身不被攻破。如果自己是铁桶一个，水泼不进，黑客无法在你的网络中的计算机取得任何访问的权限，当然就杜绝了绝大多数的泄密可能（请注意，这时候还是有可能会泄密的！比如被黑客欺骗而将数据发送出去）。我们先来看一下如何加强自己的计算机的操作系统，对于所有需要事先控制的攻击方式，这些手段都是有效的，在以后的章节中就不重复说明了。 简单地说，对于操作系统的加强，无论是Windows、Unix或是Linux，都可以从物理安全、文件系统、帐号管理、网络设置和应用服务几个方面来考虑，在这里我们不详细讨论全面的安全防护方案，只是提供一些简单实用的系统安全检查项目。这是安全的必要条件，而不是充分条件。 物理安全 简单地说，物理安全就是你的计算机所在的物理环境是否可靠，会不会受到自然灾害（如火灾、水灾、雷电等）和

人为的破坏（失窃、破坏）等。物理安全并不完全是系统或者网络管理员的责任，还需要公司的其他部门如行政、保安等一起协作，不过因为这是其他安全手段的基础，所以我们网管员还是应该密切注意的。要特别保证所有的重要设备与服务器要集中在机房里，并制订机房相关制度，无关人员不得进入机房等。网管员无特殊情况也不要进入机房，需要可以从外面的指定终端进行管理。 如果重要的服务器暴露在人人都可以接近的外部，那么无论你的口令设得多么强大都没用了，各种操作系统都可以用软盘、光盘启动来破解密码。文件系统安全 文件和目录的权限设置得是否正确，对系统中那些重要的文件，权限要重新设置；在Unix与Linux系统中，还要注意文件的setuid和setgid权限，是否有不适合的文件被赋予了这些权限； 帐号系统安全 帐号信息，用户名和密码是否合乎规则，具有足够的复杂程度。不要把权限给予任何没有必要的人；在Unix/Linux中可以合理地使用su与sudo；关闭无用账号； 网络系统安全 关闭一切不必要的服务。这一点不必多说了吧，每个开放的服务就象一扇开启的门，都有可能会被黑客悄悄地进入；网络接口特性。注意网卡不要处在监听的混杂模式；防止DoS的网络设置。禁止IP转发、不转发定向广播、限定多宿主机、忽略和不发送重定向包、关闭时间戳响应、不响应Echo广播、地址掩码广播、不转发设置了源路由的包、加快ARP表过期时间、提高未连接队列的大小、提高已连接队列的大小；禁用r*命令和telnet命令，用加密的SSH来远程管理；对NIS/NIS 进行安全设置；对NFS进行安全设置； 应用服务安全 应用服务是服务器存在的原因，又是经常会产生问题的地方。因为应用服务的种类太多，这里无法一一

叙述，就请大家注意一下这方面的资料吧。如果有可能，我会在今后继续提供一些相关知识。可以肯定地说，没有一种应用程序是完全安全的，必须依靠我们去重新设置。 对于防止数据被窃取，也有手段可以采用，使黑客侵入计算机之后不能盗窃数据和资料。这就是访问控制和加密。系统访问控制需要软件来实现，可以限制root的权限，把那些重要的数据设置为除了特殊用户外，连root都无法访问，这样即使黑客成为root也没有用。加密的手段有很多，这里也不详细介绍了，文件通过加密会以密文的形式存放在硬盘中，如果不能正确解密，就是一堆没有任何意义的字符，黑客就算拿到了也没有用。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com