 二、利用“ 肉鸡 ”进行攻击 前面说的都是黑客如何利用“ 肉鸡 ”做一些其他的事情，在第二大部分里就要谈一下黑客是如何利用“ 肉鸡 ”进行攻击其他计算机和网络行为的。黑客利用“ 肉鸡 ”攻击的原因主要有两个：首先是万一攻击行为被下一个目标发现了，对方管理员在追查的时候只能找到这台“ 肉鸡 ”，而不能直接抓出黑客自己，这为对方管理员追究责任造成了更大的困难；其次，对于某些类型的攻击手段，“ 肉鸡 ”所在的位置也许比黑客计算机所在的位置更有利。 下面介绍一下黑客利用“ 肉鸡 ”来攻击时的几种方式。 2.1非法扫描/监听平台原理介绍 扫描和监听是黑客对“ 肉鸡 ”最常使用的借用手段，目标是本网络和其他网络中的计算机。被攻击网络中总有一台计算机会被首先攻破，一旦打开了这个缺口，整个网络就都危险了。这是由于在大多数的网络进行安全设置时，主要的防卫方向是向外的，也就是说他们主要是防备外来的攻击。黑客可以利用其对内部计算机防备较少的弱点，在控制一台计算机后，从这里直接扫描。 请看一下前后两种情况的对比。防火墙是很常见的网络安全设备，在网络入口处起到了一个安全屏障的作用，尤其在黑客进行扫描的时候防火墙将堵住对绝大多数端口的探测。这时“ 肉鸡 ”就有了用武之地，从这里扫描本地网络中的其他计算机是不需要经过防火墙的，可以随便地查看它们的漏洞。而且这时候防火墙上也不会留下相应的日志，不易被发觉。黑客可以在扫描结束时

返回“ 肉鸡 ”取一下结果，或者命令“ 肉鸡 ”把扫描结果直接用电子邮件发送到指定信箱。 对于在某个网络中进行非法监听来说，本地有一台“ 肉鸡 ”是必须的条件。由于以太网的设计特点，监听只能在本地进行。虽然随着交换式以太网的普及，网络非法监听能收集到的信息大大减少，但对于那些与非法监听软件所在的“ 肉鸡 ”通讯的计算机来说，威胁还是很大的。如果这个“ 肉鸡 ”本身还是一台重要的服务器，那么危害就更大了，黑客在这上面会得到很多诸如用户帐号、密码、服务器之间不合理的信任关系的信息等，对下一步攻击起到很大的辅助作用。 防御方法 防止扫描一般主要设置在防火墙上，除了内部那些开放了的服务以外，不允许其他的访问进入，可以最大限度地防止信息泄露。至于同一网段上某个服务器成了“ 肉鸡 ”，一般情况下是没法防止它扫描其他服务器了，这就需要我们的防御方向不但要向外，也要向内。关闭每一台计算机上不需要的服务，进行安全加强，让内部的非法扫描器找不到可以利用的漏洞。 防御监听一般使用网络传输加密和交换式网络设备。管理员远程登录系统时候，还是有很多人喜欢使用默认的telnet，这种明文传输的协议是黑客的最爱。使用SSH代替telnet和那些r命令，可以使网络上传输的数据成为不可读的密文，保护你的帐号、口令和其他重要的信息。交换式网络设备可以使单个计算机接收到的无用信息大大减少，从而降低非法监听器的危害性。不过相对来说，它的成本还是比较高的。 2.2 攻击的实际出发点 原理介绍 这里所说的攻击是指那些取得其他计算机控制权的动作，如溢出和漏洞攻击等。与扫描监听相同，从内部的“ 肉鸡 ”发起的攻击同样不必经过防火墙，被阻挡和发现的

可能减少了。从这里攻击时被发现了之后，追查时会找到黑客吗？同样也不行，只能先找到“ 肉鸡 ”，再从这里找黑客就困难了。 如果说“ 肉鸡 ”做为扫描工具的时候象黑客的一只眼睛，做监听工具的时候象黑客的一只耳朵，那么“ 肉鸡 ”实际进攻时就是黑客的一只手。黑客借助“ 肉鸡 ”这个内应来听来看，来攻击，而“ 肉鸡 ”成为了提线木偶，举手投足都被人从选程看不到的地方控制着。 防御方法 也是需要对计算机进行严密的监视。请参考前面的内容。 2.3 DDoS攻击傀儡 关于黑客利用“ 肉鸡 ”进行DDoS攻击的手段就不再赘述了，详见IBM DeveloperWorks曾经刊登的文章《分布式拒绝服务攻击(DDoS)原理及防范》 2.4端口跳转攻击平台 原理介绍 这种攻击方式一般是用来对付防火墙的访问限制的。在很多网络中都使用了防火墙对外封闭一些危险的端口（这种防御又是向外的），这里黑客就可以在内部已经有“ 肉鸡 ”的提前下，让“ 肉鸡 ”去访问这些端口，注意这时不经过防火墙是不会被阻挡的，而黑客从一个不被防火墙限制的端口去访问“ 肉鸡 ”。在进行这种攻击之前，黑客会在“ 肉鸡 ”上进行设置，利用特殊的软件把黑客对“ 肉鸡 ”的访问发送到目标计算机上，端口也会变成那个危险端口，这样黑客就绕过防火墙直接对目标计算机的危险端口进行攻击了。 只用文字描述比较抽象，我们来看一个例子。 这是一个我们在实际的安全响应中的处理过程，这里黑客使用了组合式的攻击手段，其中包括对Windows服务器常见的139端口攻击，对Solaris系统的溢出攻击，攻击前的信息收集，还有2.4要里着重介绍的端口跳转攻击的方式。 