Liunx架站之限制联机端口2:如何观察端口 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/144/2021_2022_Liunx_E6_9E_B6_E7_AB_c103_144115.htm 如何观察端口： netstat, 删除已建立的联机, nmap 好了，我们现在知道这个 port 是什么鬼东西了，再来就是要去『看他到底在干啥？』对吧！没错！再来就是要来了解一下，我们的主机到底是开了多少的 port 呢？如同我们前面说的，你得要先了解一下，我们的『服务』跟『 port 』对应的档案是哪一个？再提醒一次呦！是『 /etc/services 』 啦！好了，那么常见的 port 对应的服务有哪些呢？大概有这些啦！ 当然还不只这些哩，更详细的信息你应该到你的 Linux 主机之下的 /etc/services 这个档案去看仔细！好了，那么接下来就是要来察看我们主机的 port ！如何察看呢？底下我们介绍两个最常使用的观测指令： netstst ： 在本机上面以自己的程序监测自己的 port ，无危险； nmap ： 在本机上面，以特殊的侦测程序侦测自己，可能会有违法之虞。 见他的大头王！怎么使用 nmap 会违法？呵呵！别担心，由于 nmap 的功能太强大了，所以很多 cracker (怪客，网络上面的闲人) 会直接以他来侦测别人的主机，这个时候就可能造成违法啦！只要你使用 nmap 的时候不要去侦测别人的计算机主机，那么就不会有问题啦！ ^_^"" 底下我们分别来说一说这两个宝贝吧！ 使用 netstat 指令 如前所述，在做为主机的 Linux 系统中，服务项目是越少越好！这样可以避免不必要的入侵管道喔！因此，这个时候请了解一下您的系统当中，有没有哪些服务被开启了呢？要了解自己的系统当中的服务项目，最简便的方法就是使用 netstat 了！这个东西不但简

单（每一部 Linux 机器当中预设都会安装的套件喔！），而且功能也是很不错的，例如我们在侦测线上 WWW 使用者的人数时，就很需要这个咚咚！这个指令的使用方法在 Linux 常用网络功能指令介绍当中提过了，底下我们仅提供如何使用这个工具的方法！ 如上所示，单纯使用 netstat 的时候，仅『列出目前已经接通的服务项目与服务名称』所以你可以看到，由于目前仅有一个 ssh 的联机建立成功，所以就只有显示出一个 ESTABLISHED （联机中的意思）的项目。上面浅黄色的那一行，表示『有一个 ssh 的服务开启信道联机中，是由远程 client 的 192.168.1.11 这个 IP 连接到 192.168.1.2 的主机上面的这个 IP ，而 Client 端联机的信道是以 1391 这个信道连接进入 ssh 的服务中的！』。这里这个 ssh 所显示的服务名称就是在 /etc/services 里面记载的！那如果我需要将所有的项目都列出来呢？例如说：有哪些 port 目前正在监听呢？！ 如上所示，加入 -a (all)就是说将所有在机器上所有的 port 的状态列出的意思，不过，服务的名称已经使用 /etc/services 里面的名称了，而不是使用 port 的数字！如上所示，目前我主机上面的服务共开启了：『 pop3、imap、ftp、ssh、smtp 』等服务（就是在 tcp 封包里头的具有 LISTEN 的那几个咚咚！）至于已经建立的服务就只有 ssh 这一个！那如果我想要知道 port 的号码呢？呵呵，就使用底下的指令吧！ 如上所示，我接通的服务信道只有 22 这一个，而其它的你可以参照上面的指令输出结果来对照，所以你就可以知道：pop3 为 110 而 imap 为 143 呵呵！就是这样！因此，透过此一指令，就可以轻易的了解目前主机的运作状况与服务状态！当然， netstat 的用途不止于此，您可以使用 man netstat 来查阅一番喔！相信对你的

主机会有更大的了解呦！ 使用 netstat 配合 kill 删除已建立的联机： 相信有不少的朋友都会有这个困扰，就是要怎样删除已经建立的联机呢？因为总有些不速之客会连到你的主机来进行一些破坏的工作！或者是你根本不想让对方联机过来！呵呵！还记得 资源管理 里面提到的几个常用的指令吧！？那就是找出那个联机程序的 PID，然后给他 kill 掉就是了！简单呀！不过，大问题是『我要怎样找出联机的 PID 呀！？』呵呵！由于 PID 的管理与整体的系统资源有关，这个时候，虽然可以使用 netstat 来观察 PID，不过只有 root 可以观察到联机状态的 PID 号码呦！(注：还记得资源管理提及的 PID 概念吗？就是说，在 Linux 系统之内，每个『程序』系统都会给予一个号码来管理！这个就是 PID ！) 看到上面那个淡黄色的联机建立的网络状态了吗？嘿嘿！最后面一栏就是显示那个 PID/Program name，那个 PID (上面是 24751)也就是我们要来砍掉的啦！这个时候，如果要将该联机砍掉时，就直接以 kill 来做吧！ 这样就能将该联机给他『踢出去』你的主机啦！！ 使用 nmap 套件：注意安全！ 在本机上面观察 port 最好是使用 netstat 啦！因为他安全又可靠！但是，由于可能有某些 port 会寻找不到，或者不晓得那些 port 是干嘛用的，尤其是 /etc/services 里头没有提到的几个 port 对应的服务！这个时候怎么办？！没关系，不要紧，我们这个时候可以使用那个很流行的『黑客指令』，就是 nmap 这个东西啦！nmap 的套件说明之名称为：『Network exploration tool and security scanner 』，顾名思义，这个东西是被系统管理员用来管理系统安全性查核的工具！他的具体描述当中也提到了， nmap 可以经由内部自行定义的几个 port 对应的指纹资料，来查出该 port

的服务为何，所以我们也可以藉此了解我们主机的 port 到底是干嘛用的！如果你是安装 Red Hat 7.x 版本的话，那么这个 nmap 套件应该已经安装妥当了，万一没有这个套件的话，也可以来 这里 下载去安装呦！什么？不知道如何安装！？该死，看一下 RPM 的指令吧！好了，我们谈一谈 nmap 的使用吧！