linux认证:linux中让NMAP命令跟防火墙躲猫猫Linux认证考试
PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/581/2021_2022_linux_E8_AE_A4_E8_AF_c103_581824.htm 在Linux操作系统中部署有防火墙，通过这个防火墙可以实现不让其他主机扫描本机。如果企业网络中有独立防火墙的话，再也可以实现类似的限制。如有些企业部署了入侵检测系统可以主动的阻止可疑的恶意行为，如NMAP扫描等等。但是NMAP命令结合一些选项使用，却可以跟防火墙或者入侵检测系统躲猫猫。 虽然有的管理员质疑NMAP开发者提供这些选项的意图，这些选项容易被攻击者利用。但是工具没有好坏，就看人怎么利用了。一些系统管理员往往利用NMAP命令的这些选项来提高网络部署的安全性。如我就喜欢利用这个命令来跟防火墙等安全软件玩躲猫猫的游戏。也就是说笔者伪装成一个攻击者，来测试这些安全系统能否阻挡我的攻击或者能否在安全系统日志内留下我的踪迹。换个角度思考，或许就能够发现企业的安全漏洞。 类似的选项有很多。出于篇幅的限制，不能够过多的阐述。我就只拿一些常用的选项来进行说明。 一、把报文进行分段。 像防火墙等类似的安全设备，都可以用来过滤扫描报文。但是这个过滤的策略并不是很安全。如现在利用NMAP命令的-f选项，可以将Tcp头分段在好几个包中。如此的话，防火墙或者入侵检测系统中的包过滤器就很难过滤这个TCP包。从而可以让SNMP扫描命令跟这些安全措施玩躲猫猫的游戏。 当使用-f选项时，一个20字节的TCP头会被分割成三个包，其中两个包分别有TCP头的八个字节.另外一个包具有TCP头剩下的四个字节。通常情况下安全措施所采用的

包过滤器会对所有的IP分段进行排队，而不会直接使用这些分段包。由于对报文进行了分段，那么这些过滤器就很难识别这些包的类型。然后这些包会在主机处重新进行整合，变成一个合法的TCP包。在大多数情况下这些安全措施应该禁止这些包。因为这些包会给企业的网络带来很大的性能冲击，无论是防火墙或者终端设备都会受到影响。如Linux系统的防火墙中有一个配置项，就可以通过禁止对IP分段进行排队而限制对TCP包进行分段。 可见nmap f命令对防火墙等安全措施具有一定的欺骗性。我们刚好可以利用这个命令来测试我们所采用的安全软件是否真的安全。据我了解，虽然这个安全隐患已经出现许多年了，但是现在不是所有的安全产品都能够对此进行有效的预防。所以采用这个-f选项可以帮助系统管理员一针见血的判断所采用的安全产品能否应对这个可能的攻击。如在防火墙上设置禁止扫描，然后系统管理员再利用nmap f命令无法得到应有的结果时，则表明防火墙策略有效。但是相反其仍然可以正常的返回结果(可能时间会长一点)，则表明nmap f命令可以成功的跟防火墙玩猫猫。系统管理员需要注意一下Linux防火墙的安全性了。 二、利用假的IP地址进行扫描。 通常情况下像防火墙或者客户端电脑都可以记录下访问者的相关信息，如IP地址等等。为此如果采用nmap命令来进行扫描的话，那就会在防火墙或者客户端主机上留下扫描着的IP地址。留下这个“ 罪证 ”对于扫描着可就非常不利了。另外在防火墙的配置上，系统管理员可能允许某个特定的IP地址可以进行扫描作业。而其他IP地址发出的扫描数据包都会被过滤掉。在这种情况下，无论是为了隐藏自己的真实身份，又或者是冒用合法地址进行NMAP扫描

，都需要用到一种叫做源地址哄骗的技术。 说到这种技术，我不得不说说最近出现的一种手机诈骗手段，跟这个源地址哄骗非常类似。有时候我们会接到朋友打过来的电话或者发过来的短消息，要求我们汇钱过去。虽然此时手机上显示的是朋友的手机号码，其实发短信的人不一定是你的朋友。因为现在有一种技术可以把发送者的手机号码进行修改。发送者想显示什么号码就是什么号码。其实这个源地址哄骗跟这个手机号码欺骗是类似的道理。通过“ nmap s 扫描者IP地址 被扫描者IP地址 ”这种方式，攻击者可以把自己的IP地址隐藏掉，而采用一个假冒的IP地址。无论这个IP地址是否在网络中存在，都可以使用。在防火墙或者操作系统的日志上显示的都是伪装过的那个IP地址。 为此在选购防火墙等安全产品的时候，Linux系统管理员可以利用nmap s命令来测试防火墙是否具有应对源地址哄骗攻击的手段。如先在防火墙上启用日志功能，然后利用nmap s命令来扫描防火墙或者其他主机设备。再去查看相关的日志。看看这个日志中纪录的IP地址信息是伪装的IP地址还是扫描者真实的IP地址。通过这种方式就可以简单的判断出防火墙等安全产品能否应对类似的源地址欺骗攻击。虽然日志记录的攻击者真实身份有点像放马后炮，但是对于我们迅速查找攻击者，防止其再次发动攻击具有很大的价值。为此一些安全产品中需要具备一些源地址哄骗的预防功能。 三、利用诱饵实现隐蔽扫描。 通过源地址哄骗可以隐藏扫描者的身份，不过这种技术的话在一次扫描过程中之能够伪装一个IP地址。而目前比较流行的隐藏IP地址的方法是使用诱饵主机。简单的说，非法供给者可以采用网络中正在使用的几个IP地址当作自己的IP地址，对网络

主机进行扫描。而安全设备的话，并不知道哪个IP地址是真实的IP地址。如在防火墙上可能会纪录某个IP地址的5-8个端口扫描。这是一种比较隐蔽的隐藏自身IP地址的有效手段。更有趣的是攻击者还可以把自己的真实IP地址也放入进去，以增加攻击的挑战性，挑战防守者的智慧。如系统管理员可以通过ME选项将自己的IP地址放入到诱饵IP地址当中。通常情况下把自己的IP地址放在靠后的位置，则防火墙就很难检测到这个真实的IP地址。不过这个诱饵的IP地址数量不在于多，而在于精。如把这一些具有比较高的权限的IP地址(如在Linux服务器上根据IP地址来实现一些防火墙策略)加入到诱饵主机列表中，将起到出奇制胜的效果。而过多的诱饵地址反而会使得扫描时间过长或者结果不准确。最要命的是可能会导致被扫描网络性能下降，从而引起对方网络管理员的注意。 其实诱饵技术现在也有了预防的方法。如通过路由追踪、响应丢弃等方法，可以用来防止攻击者使用诱饵隐蔽扫描。有时候这种安全机制对于企业很重要。因为诱饵隐蔽攻击不但可以秘密收集到企业网路主机的重要信息，为其后续攻击做好准备。而且nmap D命令还容易引起SYN洪水攻击。如当非法攻击者所采用的诱饵主机并不在工作状态时，就会对目标主机发起SYN洪水攻击。这是一个比较危险的攻击手段。 既然现在已经有了解决方案来应对诱饵隐蔽扫描，那么Linux系统管理员或者网络工程师所要做的就是来测试防火墙或者其他的安全产品是否提供了类似的解决方案。有时候往往不能够光靠对方业务员的描述，而需要我们来进行测试。那么利用这个nmap 命令显然可以帮助我们来进行这方面的测试。 在nmap命令中，类似的选项还有很多。如可以通

过source-port选项，来实现源端口哄骗.如利用date-length选项，在发送报文时附加有害的数据.通过spoof-mac选项，实现MAC地址哄骗，这个跟源地址欺骗结合可以让MAC地址与IP地址捆绑等安全策略失效.等等。这些选项如果被非法攻击者利用，无疑会威胁到Linux网络的安全。但是，如果我们能够事先采用这些选项来测试自己网络与主机的安全性，并率先把这些漏洞补上了。那么非法攻击者也只好无功而返了。所以我认为工具无所谓好坏，主要就看使用者的心态了。为此我建议各位不妨利用NMAP命令跟自己企业的防火墙等安全产品玩玩躲猫猫的游戏，来判断一下所谓的安全防护体系是否真的安全。 