思科认证辅导:让黑客远离DNS和SMTP服务器攻击思科认证
 众所周知，服务器是计算机网络中最重要的资源，对其安全要求很高。如果我们正在运行的服务器没有进行正确的谨慎配置，就可能将大量的有用信息泄漏出去，从而使得黑客可以借此破坏你的网络。因此我们应该检查服务器以确保黑客不能得到其需要的关键信息。 如今，几乎每一个组织都运行着DNS服务器及SMTP服务器。任何精明的黑客几乎都会毫无疑问地试图对其进行渗透。如果成功，黑客就可以查看从中收集的任何信息。 DNS服务器安全 黑客可做的一件事情就是从首选DNS服务器执行区域传递。一个区域的备用DNS服务器意味着能够执行区域传递来获得并从首选DNS服务器复制源记录的完整副本。这样做有几种原因：一是由首选服务器通知区域已经发生改变，二是第一次启动，三是到了预定的更新时间不得不刷新。另一方面，黑客并不打算执行一次区域传递。 黑客不如此做有很好的理由。因为一次区域传递包含着特定区域中计算机的大量关键信息，包括IP地址、服务器名称及其暗示的服务器的功能等等。毫无疑问，如果黑客对这些东西感兴趣的话，这应该是极有价值的信息。 如果你的DNS服务器进行了正确设置，就不应该有问题。备用DNS服务器能够执行区域传递，但黑客不能。另一方面，如果你设置DNS服务器时不够重视，任何人都能执行区域传递并获得重要信息。要发现你的DNS服务器是否正在泄漏信息，在Linux中可使用这个命令： # host -t ns yourcompanydomainname.com (这

里yourcompanydomainname用你的公司域名代替) 要获得你公司DNS服务器的列表： yourcorporatedomainname.com name server ns1.yourcorporatedomainname.com yourcorporatedomainname.com name server ns2.yourcorporatedomainname.com 要执行一次区域传递，键入如入的命令： # host -l yourcompanydomainname.com ns1.yourcorporatedomainname.com Host yourcorporatedomainname.com not found: 5(REFUSED) . Transfer failed(传递失败) 如果你收到这个信息，那祝贺你。你的DNS服务器已经正确设置，或者至少在这方面正确配置。如果你没有这么幸运，看到了域中所有机器的名称和IP地址的完整列表。那么任何获得这些信息的黑客会收到公司网络布局的概况，毫无疑问这是极有价值的。 offensive-security.com 的网络安全专家和培训师Mati Aharoni 说，“ 我已经看到了企业错误配置它们的DNS服务器的几种情况，企业并没有将其内部DNS名字空间与外部DNS名字空间划分到不同的、不相关的区域中 ”“ 这导致了对外部网络结构和内部网络结构的完整视图。 ”因此，如果你的DNS服务器允许任何人执行区域传递，就应该立即进行修复。 SMTP服务器安全 虽然SMTP服务器不一定将你的网络地图拱手交给黑客，却可以透露合法的邮件用户名。邮件用户名是极有价值的信息，因为有些用户名可以被重新利用作为其它系统的登录证据。如果通过使用在线的口令工具(如Hydra)，使得这些用户名与合法的口令相匹配，黑客就可以使用更有威胁力的工具来破坏你的系统。 有两个SMTP命令：VRFY 和EXPN值得注意。这两个命令可以用于确认(VRFY)某个特

定的用户名正在服务器上使用，并扩展(EXPN)邮件列表名称来展示列表中的用户名称。 当我们从内部诊断电子邮件的故障或问题，去检查特定的用户名是否正确并被服务器重新验证的时候，VRFY命令是很有用的。如果你有一个合法的用户在使用电子邮件时出现了问题，可以使用Netcat这种工具连接到SMTP服务器的IP地址和端口： # nc -v xxx.xxx.xxx.xxx 25 (xxx.xxx.xxx.xxx代表IP地址) 一旦你收到SMTP服务器确认你与服务器连接的标志后，发出如下的命令： VRFY validuser (合法的用户名) 如果这个用户名实际上合法的，就会收到如下的反馈信息： 250 2.1.5 validuser validuser@yourcorporatedomainname.com 否则，你会看到： 550 5.1.1 validuser … User unknown 这种信息对故障诊断有用，不过对黑客可能会更加有用。这是因为有了简单的Python脚本和包含某些可能的用户名的列表的一个文本文件的协助，黑客可以快速地浏览用户名列表，确认哪些是SMTP服务器上合法的用户名，哪些是非法的。同样地，黑客可以使用EXPN命令来检查可能的用户名列表，找出潜在的用户是谁。例如，EXPNing “ postmaster ”会显示postmaster邮件到底是发给谁的。一旦有了合法的用户名列表，就可以试图将其与很容易就得到的常用口令列表进行匹配。 禁用VRFY和EXPN通常是一个相当简单的配置问题，而且对日常的管理工作不太可能有什么大的影响。 实际上并没有什么绝对的方法能够阻止黑客“ 接近 ”你的服务器，不过采取这些措施阻止服务器泄漏可能对你不利的信息的确是方向正确而且十分值得。毕竟，为什么要让黑客们那么容易就得手呢? 更多优质资料尽在百考试题论坛 百考试题在线题库 思科认证更多详细资料 100Test