通过设定Ope H账户登录避免恶意攻击 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/454/2021_2022__E9_80_9A_E8_BF_87_E8_AE_BE_E5_c100_454446.htm 前面我们讨论了如何《保护SSH免受强力口令破解攻击》。今天继续讨论如何限制用户的登录。OpenSSH包括许多用途广泛的并且十分流行的程序。无论是作为客户端或服务器，其广泛性和SSH的实用性，无疑都使SSH成为一些公共的攻击目标。由此导致的结果是，人们开发了许多工具用以对付一些常见的强力攻击企图。 然而，这些攻击不仅仅会转换为一种恼人的东西，更是一种对日志文件空间的浪费。对于刚开始对付这种攻击的人员来说，明确地设置谁能够通过OpenSSH登录到系统中将有助于击溃大约99%的强力攻击，而不管你的系统真实的安全程度如何。 首先，千万不要准许以根用户身份通过SSH登录进入，除非你绝对有必要这样做，而且需要采用SSH密钥。千万不要允许在不需要口令（空口令）的情况下以根据用户登录到系统中。为此，编辑/etc/ssh/sshd_config（在某些系统中即为/etc/sshd_config），并增加： PermitRootLogin without-password 这就会容许根用户身份登录，不过只能采用一个恰当的SSH密钥才可以登录，其对应的公共部分必须在/root/.ssh/authorized_keys中设置。 其次，明确地定义哪些用户能够登录。因此需要再次编辑sshd_config文件，并增加： AllowUsers root AllowUsers freedom 上述的命令仅允许用户root和freedom通过ssh登录。在这里需要注意，一旦你启用了AllowUsers选项，任何没有被列示的用户将不能登录。换句话说，虽然进行了PermitRootLogin设置，如果我们没有设

置PermitRootLogin，并将“ AllowUsers freedom ”放置在配置文件中，即使用了一个正确的口令，根用户也不能登录。因此，随着时间的推移，需要不断地关注这个列表，并确保不再需要访问系统的用户要从列表中清除。 实际上，你不但可以通过指定所允许的用户来强化安全，还可以通过设定一个“ 用户@主机 ”模式指定用户可以从哪台主机登录。 让我们举个例子，如果你设置了freedom@192.168.2.18，那么授与给用户账户“ freedom ”的访问权将只能源自IP地址为192.168.2.18的计算机。在这里我们可以指定多种模式，如freedom@192.168.2.*，就会允许用户freedom可以从网络192.168.2.0的所有主机登录。 OpenBSD的Manual Pages列示了可允许模式的更祥细信息（网址为：http://www.openbsd.org/cgi-bin/man.cgi？query=ssh_config），您不妨一看。 最后一点，如果你不需要基于PAM验证，就要设置： UsePAM no 这本来是默认的选项，如果你需要基于PAM的身份验证（sshd自身不能实现）时，就应当启用之。例如，如果拥有一个通过LDAP验证的用户账户时，就需要启用。如果不启用UsePAM，此用户将永远不能登录。不过，一旦你启用了UsePAM，其它选项并不会象你所期望的那样工作。例如，“ PermitRootLogin without-password ”就不会正常工作，而且如果没有提供一个合法的ssh密钥，就会退回到这样一种情况：对根用户的口令，需要根据身份验证的提示才得以实现。 在这一点上，仅通过采用AllowUsers关键字，就可以减轻多数的强力攻击企图，因为攻击不但需要猜测正确的口令，还需要猜测正确的账户。 任何通过其他用户（即不在被准许用户列表中的用户）的登录企图都会导致失败，即

使提供了正确的口令也是如此。 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