

破解 email 账号的方法

September 13, 2001

Sinbad Technical Publications
Website: <http://sinbad.zhoubin.com>
© Copyright 2001, All Rights Reserved

电子邮件并不是安全的，在邮件的发送、传送和接收整个过程中的每个环节都可能存在薄弱环节，恶意用户如果利用其漏洞，就能够轻易的破解出账号，获得邮件内容。

一. 利用邮件服务器操作系统的漏洞

邮件服务器软件是运行在特定的操作系统上的，如 Linux、Windows NT/2000 等。这些操作系统的默认安装和配置都是不安全的，黑客可以轻易入侵系统，获得所有用户名和密码。

1、Windows 服务器

如果是基于 Windows2000 的 Exchange Mail Server，系统本身未做任何安全配置，开放了若干服务。入侵者可以利用终端服务器结合中文输入法漏洞或者 IIS 的 Buffer Overflow 程序获得 Administrator 权限，用 pwdump3 导出 Hash 过的密码，再用 L0pht 挂接字典或者 Brute Force 就能破解出用户密码。根据经验，如果密码简单，几分钟之内就能破解出，长度在 8 位及以下的用 Brute Force 方式在一天内就能解出。

2、Linux/UNIX 服务器

UNIX 类系统一般采用 Sendmail 作为邮件系统，在获得了系统的控制权之后，用 John 等软件就能从/etc/passwd 或者/etc/shadow 中破解出密码。如果采用了数据库方式来保存用户信息和密码，也是很容易被导出。

二. 利用邮件服务器软件本身的漏洞

最常见的邮件服务器程序有 Sendmail, Qmail 等，在不同程度在都存在安全缺陷。以 Sendmail 为例，再以前的老版本中，telnet 到 25 端口，输入 wiz，然后接着输入 shell，就能获得一个 rootshell，还有 debug 命令，也能获得 root 权限。Qmail 相对 Sendmail 安全，但是 Qpopper 存在 Buffer Overflow 缺陷，能够远程得到 rootshell，进而控制系统。

即使邮件服务器是安全的，但是入侵者还能获得更多的信息，比如用户名。telnet 到 25 端口，输入 expn tom 或者 vrfy tom 就能查询系统是否有 tom 用户。最新版本的 Sendmail 虽然禁用了这两个命令，但是可以通过伪造发信人然后用 rcpt

to 来判断该用户是否存在。

得到了用户名，可以 telnet 到 110 端口，尝试简单密码的连接，或者套用字典破解。

所以，必须禁止非本域的中继利用（relay），或者采用现在很多 ISP 都采用的给 SMTP 加上发信认证的模块，这样能够增强邮件服务器的安全。

除了 POP3 方式收信之外，比较流行的是在 WEB 界面上处理邮件。这种方式也不无弱点，一般是通过 CGI 来接受用户传递的表单 FORM 参数，包括 username 和 password，如果正确，就可以进入处理邮件的页面。破解已知用户的密码，有很多套用字典或者暴力组合的软件可用，比较著名的是小榕的溯雪，在密码简单的情况下，很快就有结果。

WEB 邮件系统都有“忘记密码”的选项，如果能破解寄回密码的另外一个邮箱或者猜出提示问题的答案，也能成功。

三. 在邮件的传输过程中窃听

在网络中安装 Sniffer，指定监听往外部服务器 110 端口发送的数据包，从收集下来的信息中查看 user 和 pass 后的字符串就能看到用户名和相应的密码。