第28章　使用r系列实用工具

作者：Neal S. Jamison

本章内容包括：

- 理解r系列命令
- 使用r系列命令的替代方法
- r系列命令详解
- 在非UNIX环境实现r系列命令的功能

我们已经知道，通过 TCP/IP协议包可以使计算机间相互通信。但建立互联网络仅依靠协议是不够的，还需要使用 TCP/IP协议和服务的应用层程序。这些程序主要实现高层通信。本章讨论一组特殊的程序，它们使远程计算机以不同的方式通信。

28.1　理解r系列命令

r系列命令由伯克利大学 BSD UNIX组织开发，使计算机编程人员和用户可在远程主机上运行会话和命令。这些命令至今仍流行于 UNIX系统和TCP/IP应用中，且功能仍与当时一样。r系列命令可使用户在主机间拷贝文件，执行远程主机上的命令，甚至创建远程主机的登录会话。与Telnet和FTP不同，运行这些命令时不需要用户认证 (即敲入用户名和口令)。

表28-1列出了常见的r系列命令。

表28-1　UNIX r系列命令

命　令	描　述
rsh	远程Shell：在远程计算机上执行程序。在一些非 BSD UNIX发布中称为rshell、rmsh或rcmd，而其中的rsh为受限的Shell
rcp	远程拷贝：将文件从一台主机拷贝到另一台主机，其功能与FTP类似
rlogin	远程登录：登录到远程主机。Hogin的功能与 Telnet类似
rup	远程更新：显示远程主机的状态
ruptime	远程更新：显示远程主机的状态(与rup类似)
rwho	远程who：显示远程主机上当前用户
rexec	远程执行：与rsh类似，但需要口令

28.1.1　安全问题

r系列命令的理论支持是“ 主机等价 ”。计算机可通过配置指定可信主机和用户以透明地登录到主机并运行命令。这种方法存在许多问题：首先用户的系统安全性与安全性最弱的主机一致，一旦配置不正确，用户系统将需要在所有用户面前敞开。其次，用户口令在网络上是明文传输。非法用户可以很轻易地监听到用户口令获取非法访问权限。

由于r系列命令的安全问题，许多专家建议不使用，但是，它仍被广泛接受，因此，三章

主要讨论它的正确配置和使用。同时，讲述了如何禁止 1R系列命令的使用(见本章28.2节)。

关于正确配置的信息将在28.3节中详细讨论。

注意 因为操作系统的多样化，且每个操作系统特性不同，本章主要讨论Linux环境下的r系列命令。不同的操作系统关于命令的用法及作用基本相同。某些特性请查阅特定命令的OS文档。

28.1.2 禁止使用r系列命令

如果用户需要禁止R系列命令，则需要在文件/etc/inetd.conf文件中注解相应的行。即在相应行的开始添加字符“ # ”。以下是注解相应行后的 /etc/inetd.conf文件(注意：为了节省空间，已作了必要缩略)：

```
#
# inetd.conf   This file describes the services that will be available
#    through the INETD TCP/IP super server.  To re-configure
#    the running INETD process, edit this file, then send the
#    INETD process a SIGHUP signal.
# Version:   @(#)/etc/inetd.conf   3.10   05/27/93
# Authors:   Original taken from BSD UNIX 4.3/TAHOE.
#   Fred N. van Kempen, <waltje@uwalt.nl.mugnet.org>
# Modified for Debian Linux by Ian A. Murdock <imurdock@shell.portal.com>
# Modified for RHS Linux by Marc Ewing <marc@redhat.com>
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
# Echo, discard, daytime, and chargen are used primarily for testing.
#
# These are standard services.
#
ftp     stream  tcp   nowait  root   /usr/sbin/tcpd   in.ftpd -l -a
telnet  stream  tcp   nowait  root   /usr/sbin/tcpd   in.telnetd
#
# Shell, login, exec, comsat and talk are BSD protocols.
#
#shell  stream tcp    nowait  root   /usr/sbin/tcpd  in.rshd
#login  stream tcp    nowait  root   /usr/sbin/tcpd  in.rlogind
#exec   stream tcp    nowait  root   /usr/sbin/tcpd  in.rexecd
#
...
```

如上所示，字符“ # ”被分别置于in.rshd, in.rlogind和in.rexecd所在的行的开头。

注意 修改本章提到的文件或运行本章讨论的命令均需要管理员权限。

在注解了r系列命令的守护进程后，用户需要重新启动 inetd守护进程。可通过下述命令完成：

```
killall -HUP inetd
```

UNIX系统守护进程的作用

在UNIX系统中，守护进程是在后台运行的一组程序，它等待某些事件的发生。守护

进程(demon)又称为精灵进程，精灵介于人与神之间，相应的，守护进程介于两个事件或进程之间。例如， in.rlogind守护进程，它等待rlogin请求。当rlogin请求到达时，in.rlogind对用户进行认证。若用户可信，则允许进入；否则， in.rlogind拒绝请求。

28.1.3 增强r系列命令的安全性

如果用户需要r系列命令提供的功能，就可以采取一些额外的步骤使它们尽可能安全。以下是一些用户可用的认证：

- TCP Wrapper
- Kerberos认证
- 数据加密标准(DES)

1. TCP Wrapper

TCP Wrapper(又称tcpd)是一种主机访问控制机制，它位于 TCP守护进程的外围，为 TCP程序提供监听和过滤功能。使用 TCP Wrapper，用户可以通过配置使系统仅响应来自特定网络计算机或特定域的r系列请求。

大多数Linux版本都预装了Wrapper功能(详细信息参见http://www.linux-howto.com /LDP/HOWTO/NET-3-HOWTO-5.html#ss5.10或关于host_access (5)的帮助文档)。根据用户系统不同，某些用户可能需要下载并安装 TCP Wrapper。

配置/etc/hosts.allow和/etc/hosts.deny文件

主机访问或TCP Wrapper程序使用这两个文件决定哪些用户可以或不能运行系统中的某些命令。文件中每一项的基本语法格式为：

daemon: client

例如：系统中hosts.deny文件可能包含：

All: WAll

hosts.allow文件可能包含：

```
in.telnetd:   All
in.ftpd:   All
in.rshd:   *.mydomain.com
in.rlogind   *.mydomain.com
in.rexecd   *.mydomain.com
```

在上例中， hosts.deny文件中的All:All表示拒绝任何人对主机的访问。在 hosts.allow文件中列出了不受hosts.deny限制的项。其中，所有用户均可使用 FTP和telnet程序访问主机，但仅有在可信域mydomain.com中的主机才可使用r系列命令访问主机。

本节仅简单讨论了主机访问和 TCP Wrapper支持的功能和属性，详细信息请参见用户的操作系统文档。

使用IP欺骗入侵系统

IP欺骗是使用假冒的方法使计算机误以为请求来自可信主机的一种技术。它通常用于侵入可信任系统如使用 r系列命令和TCP Wrapper的系统。

IP欺骗的方法超出了本章讨论的范围，但其基本方法是入侵者修改网络报文头使报文像是来自于可信任网络。

2. Kerberos认证

为了加强r系列命令的安全，rsh.rcp和rlogin的许多版本都使用了Kerberos认证。

Kerberos是一种认证系统，它允许两台主机在不安全的网络上交换安全信息。每个通信主机有一个分配的信元，其中包含消息和发送方的认证口令。

关于Kerberos的详细信息参见：http://web.mit.edu/kerberos/www/。

3. 数据加密标准(DES)

某些rsh的版本使用功能强大的加密标准 DES来加强其安全性。在1970年中期，DES提供了一种较强的加密方法。

关于DES的详细信息，参见站点http://www.itl.nist.gov/fipspubs/fip46-2.htm。

28.2 使用r系列命令的替代方法

由于r系列命令存在许多安全隐患，因此可以考虑采用其他方法替换 r系列命令。那么最佳选择是安全Shell(SSH)。

安全Shell

安全Shell是登录远程主机、执行远程命令及拷贝文件的安全方式。用户可以使用 SSH获得与使用安全性差的rlogin.rsh和rcp相同的功能。

SSH的安全性得益于使用了加密机制认证主机，它使用的加密机制有数据加密标准 (DES)和RSA。这些机制可使SSH保护用户系统免受以下攻击：

- IP欺骗
- 明文口令监听

RSA公用密钥/私有密钥认证

Rivest、Shamir和Adelman(三人的缩写名字)发明了RSA算法，该算法提供了公用密钥/ 私有密钥加密。基本的思想是：经过公有密钥加密的数据只能通过私有密钥解密。在主机认证的环境中，发送主机使用接收方 (远程)主机的公用密钥加密一个随机字符串。如果远程主机能够通过私有密钥成功解密，则两台主机之间就是信任的。

有关RSA的更多信息，请参考http:/www.rsa.com/.有关公用密钥/私有密钥加密的介绍，请参考http:/www.rsa.com/rsalabs.pubs.pkcs/。

SSH版本1和2对非商业用途是免费的。更多有关 SSH的信息，请参考http:// www.ssh.fi/sshprotocols2/。

28.3 r系列命令详解

本节讲述r系列命令的格式及用法。正如前面提到过的，这些命令的信息来自 Linux操作系统。用户系统的r系列命令的用法及格式可参阅操作系统的相关文档。

r系列命令守护进程

表28-2列出了服务器上运行的守护进程，它们用以保证 r系列命令的正确执行，这些守护进程也可以由inetd启动。详细信息参见服务器文档及用户手册。

表28-2 r系列命令守护进程

守护进程	描述
rshd	远程shell服务器。不需认证提供远程执行功能
rlogind	远程登录服务器。不需认证提供远程登录
rwhod	系统状态服务器
rstatd(或rcp, rstatd)	远程状态服务

1. rsh

远程shell命令(rsh)允许用户在远程系统中执行命令。

注意 rsh与某些UNIX版本的rshell、remsh或rcmd类似，在这些UNIX版本中，rsh表示严格认证的shell。

用法：rsh [.kdnx] [-k realm] [-l username] host [command]

属性：

-k —— 不启用kerberos认证。

-d —— 启用socket调试。

-n —— 从/dev/null中重定向输入。

-k —— 远程kerberos认证密钥可在指定域中获取，而不需在远程主机中获取。

-l —— 指定远程用户名以取代当前用户名。

-x —— 启用DES加密机制。

如果未指明属性，用户将激活rlogin会话。

示例：

```
%rsh hostname1 who
jamisonn    pts/1    Jul 26 09:13    (hostname2)
evanm       pts/13   Jul 25 12:30    (hostname3)
```

本例在远程主机hostname1上执行who命令。输出显示两个用户正在使用系统。

2. rcp

远程拷贝(rcp)可将文件从一台主机拷贝到另一台主机。它可看作非交互的 ftp。

用法：

```
rcp [-px] [-k realm] file1 file2
rcp[-px] [-r] [-k realm] file… directory
```

文件或目录的格式为*username @ hostname: filepath*。

属性：

-r —— 执行递归拷贝(目的地为目录)。

-p —— 保存源文件的修改时间及方式。

-k —— 使远程kerberos认证密钥可从指定域获取而不需从远程主机获取。

-x —— 在允许的情况下使用DES加密。

示例：

```
%rcp /home/jamisonn/report jamison @ hostname2:report
```

本例将report文件从本地主机的home目录拷贝到远程主机hostname2的home目录下。

3. rlogin

rlogin命令在远程主机上启动一个终端会话。

用法：rlogin [-8EKLdx] [-e char] [-k realm] [-l username] host

属性：

-8 —— 允许8位输入数据。

-E —— 禁止使用ESC键。

-K —— 不能使用kerberos认证机制。

-d —— 使用socket调试。

-e —— 允许用户指定退出字符，缺省字符为“ ~ ”。

-k —— 使远程kerberos认证密钥可在指定域获取，而不需从远程主机获取。

-x —— 在允许的情况下使能DES加密机制。

示例：%rlogin -l jamisonn hostname1

本例为用户jamisonn在远程主机hostname1上创建登录会话。

Rlogind守护进程必须在远程主机上运行。

4. rup

rup命令用以显示指定远程系统的状态。如果指定主机， rup返回网络中所有主机的状态。

用法：rup [-dhlt] [host…]

属性：

-d —— 显示主机的本地时间。

-h —— 按主机名的字母顺序排列输出。

-l —— 根据平均负载排列输出。

-t —— 根据启动时间排列输出。

示例：

```
% rup hostname1
hostname1    up 15 days, 11:13,  load average: 0.21, 0.26, 0.19

%rup -d hostname1
hostname1    4.08pm  up 15 days, 11:13,  load average: 0.21, 0.26, 0.19
```

远程主机必须运行rstatd(或rpc.rstatd)守护进程，以保证rup正常工作。

5. ruptime

ruptime的功能与rup类似。

用法：ruptime [-alrtu]

属性：

-a —— 显示已空闲数小时的主机。

-p —— 按负载排列输出。

-r —— 返转输出顺序。

-t —— 按启动时间排列输出。

-u —— 按用户数量排列输出。

远程主机必须运行rwhod守护进程以保证ruptime正常运行。

6. rwho

rwho命令显示登录到远程系统的用户。它的输出与 UNIX系统中的who命令类似。缺省情况下，rwho命令仅显示正在使用远程系统的用户。

用法：rwho [-a]

属性：-a —— 显示所有用户，包括已空闲数小时的用户。

远程主机必须运行rwhod守护进程以保证rwho正常工作。

7. rexec

rexec命令在功能上与rsh类似，但它需要用户输入口令。

28.3.2 相关文件

正确运行r系列命令还需配置以下文件：

- /etc/hosts
- /etc/hosts.equiv
- .rhosts
- /etc/hosts.allow and /etc/hosts.deny

1. /etc/hosts

通信的计算机相互了解十分重要，这一功能通过 /etc/hosts文件实现。如果主机1想允许主机2运行r系列命令，主机1需在其/etc/hosts文件中为主机2添加一项，反之亦然。

2. /etc/hosts.equiv

hosts.equiv文件指定主机及用户，它们不需认证即可使用 r系列命令。 hosts.equiv命令的不正确使用将给系统安全带来更大危害。

/etc/hosts.equiv文件的基本格式如下：

[+ | -] [hostname] [username]

在主机或用户名前的“ + ”允许主机或用户访问主机，类似的，“ - ”表示拒绝相应的用户或主机访问系统。表28-3列出了主机示例项的简短解释。

表28-3 hosts.equiv项及其含义

项	含 义
hostname1	允许hostname1上的所有用户访问
-hostname1	拒绝hostname1上的所有用户访问
hostname2+-root	拒绝 hostname2上的根用户访问
hostname2+-admin	允许 hostname2上的admin用户访问
-root	拒绝任何系统的根用户访问
+admin	允许任何系统上的admin用户访问
+	允许任何用户访问
-	拒绝任何用户访问

警告 某些UNIX版本中hosts.equiv文件中包含“ + ”。它使系统可被任何系统上的用户访问，其危害十分严重。如果hosts.equiv文件中包含“ + ”，建议删除。

3. .rhosts

.rhosts文件与hosts.equiv文件类似。但是， .rhosts文件还可用于允许拒绝对特定帐号的可

信访问，而hosts.equiv文件应用范围为整个系统。

.rhosts文件的通常用法为允许某用户可信访问多个系统，只要拥有合法帐号。例如，某用户在主机1上有合法帐号，用户名为jamisonn。在其他系统的相应帐号下创建 .rhosts文件，可使用户可信访问其他系统。

主机1上用户jamisonn的主目录下包含文件.rhosts示例如下：

```
hostname2 +jamisonn
```

主机2中相应文件也包含以下项：

```
hostname1 +jamison
```

上述两个文件将使用户jamisonn获得两个系统的可信访问权限。

r系列命令可信任主机或用户最薄弱的地方在于欺骗十分简单。用户可以假冒其他用户进入系统。在前面的示例中，如果某个入侵者获取了第一个系统的访问权限，就可使用jamisonn或超级用户登录主机1，入侵者不需任何认证登录到主机上，这是用户假冒。 IP或主机假冒与此类似。

4. etc/hosts.allow与/etc/hosts.deny

主机访问或TCP Wrapper程序使用这些文件确定谁能或不能在主机上运行特定命令。文件的详细描述及构成参见本章28.1.3节。

/etc/hosts.deny示例如下：

```
ALL:ALL
```

/etc/hosts.allow示例如下：

```
in.telnetd: All
in.ftpd: All
in.rshd: *.mydomain.com
in.rlogind: *.mydomain.com
```

在本例中， hosts.deny文件拒绝任何用户的任何操作。这是一个非常好的安全策略。hosts.allow文件任何用户使用Telnet及ftp命令访问主机，并且允许来自 mydomain.com域中的用户使用r系列命令。

28.4 在非UNIX环境下实现r系列命令的功能

r系列命令通常仅在UNIX环境下实现。但是，目前开始出现实现类似功能的其他 TCP/IP产品，如Windows NT 4.0下的Microsoft TCP/IP组件。也存在少量第三方产品可使其他系统实现r系列命令的功能。

表28-4显示出了少量厂商及其URL，用户可以从中获取更详细的信息。

表28-4 第三方r系列命令产品

Manufacturer	URL
Hummingbird Communications LTD	http://www.hummingbird.com/products/nc/inetd/
Denicomp Systems	http://www.denicomp.com/products.htm
Didier CASSEREAU	http://www.loa.espci.fr/winnt/rshd/rshd.htm
Markus Fischer	http://www.uni-paderborn.de/StaffWeb/getin/getservice.htm

28.5 小结

本章介绍了UNIX环境下的r系列命令，用户可以使用这些命令登录远程主机、拷贝远程文件及执行远程命令，运行这些命令及服务所带来的安全威胁不容忽视。因此，本章提供了一些对策如采用安全Shell(SSH)等。同时，本章还讨论了非UNIX环境下r系列命令的使用。用户可根据本章提供的大量URL获得详细信息。

本章所讲述的命令及用法均来自Linux系统，用户需要查阅自己操作系统的帮助文件获取操作系统命令的用法及属性信息。