就可以查到该大学的一长串IP地址，也可以使用nslookup或者dig程序（还可以通过向机器中键入“DNS query”来从网络中查找可以进行免费DNS查询的网站，例如www.dnsstuff.com）。因为许多机构都拥有65 536个连续的IP地址（过去常用的一整个分配单元），所以骇客一旦得到IP地址的前2个字节（dnsquery命令的结果），就可以连续地使用ping命令来看一看哪些地址有回应，并且可以接受telnet连接。完成这一步后，骇客就可以通过我们前面所介绍的猜用户名和口令的方法闯入系统。

毫无疑问，从解析主机名称找到IP地址的前2个字节，到ping所有的地址看哪些有反应，再看这些地址是否支持telnet连接，到最后大量地进行诸如（登录名和口令）对一类的猜测，这些过程都可以很好地自动完成。这一过程会进行大量的尝试，以便闯入，而且如果骇客的计算机性能稳定的话，可以不断地重复运行某些命令直到进入系统。一个拥有高速电缆或DSL连接的骇客可以一整天让计算机自动尝试进入某个系统，而他所做的只是偶尔看一下是否有反馈信息。

除了远程登录服务（telnet service）以外，很多计算机还提供了很多其他可以应用于互联网的服务。每个服务都与65 536个端口（port）中的一个相关联（attach），当骇客找到了一个活动的IP地址，通常情况下他会执行端口扫描（port scan）来确定每个端口允许哪些服务。某些端口可能会提供额外的服务，而骇客则可能利用这些服务侵入系统。

使用telnet攻击或端口扫描很明显比军用拨号器要快（无须拨号时间），而且成本低（无须长途电话费）。但它仅适用于攻击Internet上的计算机和telnet连接。而的确有许多公司（包括几乎所有的大学）都接受telnet连接，以保证雇员在出差时或在不同的办公室（或在家里的学生）进行远程登录。

不仅用户口令如此脆弱，而且超级用户口令有时也十分脆弱。特别是有些刚刚安装好的服务器从不更改出厂时的默认口令。一位Berkeley大学的天文学家Cliff Stoll曾经观测到自己计算机系统的不正常，于是他放置了一个陷阱程序来捕捉入侵者（Stoll，1989）。他观察到了一个如图9-18的入侵过程——某个骇客闯入了Lawrence Berkeley 实验室（LBL）并想进入下一个目标。用于网上交换的uucp（UNIX到UNIX的COPY程序）账号拥有超级用户的权力，这样骇客可以闯入系统成为美国能源部计算机的超级用户。幸运的是，LBL并不是设计核武器的实验室，而它在Livermore的姐妹实验室却的确是设计核武器的。人们希望自己的计算机系统更加安全，但当另一家设计核武器的实验室Los Alamos丢失了一个装有2000年机密信息的硬盘以后，大家就没有理由相信系统是安全的了。

```
LBL> telnet elxsi
ELXSI AT LBL
LOGIN: root
PASSWORD: root
INCORRECT PASSWORD, TRY AGAIN
LOGIN: guest
PASSWORD: guest
INCORRECT PASSWORD, TRY AGAIN
LOGIN: uucp
PASSWORD: uucp
WELCOME TO THE ELXSI COMPUTER AT LBL
```

图9-18　骇客是如何进入美国能源部位于LBL实验室的计算机的

一旦骇客闯入了系统并成为超级用户，他就可能安装一个叫做*包探测器*（packet sniffer）的软件，该软件可以检查所有在网上进出的特定信息包。其中之一是查看哪些人从该系统上远程登录到别的计算机上，特别是作为超级用户登录。这些信息可以被骇客隐藏在某一文件下以便闲暇之余来取。通过这个办法，骇客可以从进入一个安全级别较低的计算机入手，不断地闯入更强安全性能的系统里。

目前越来越多的非法入侵都是一些技术上的生手造成的，他们不过是运行了一些在Internet上找到的脚本程序。这些脚本要么使用我们上面介绍的极端攻击，要么试图找到特定程序的bug。真正的骇客认为他们只是些*脚本爱好者*（script kiddy）。

通常脚本爱好者没有特定的攻击目标也没有特别想偷窃的信息。他们不过是想看看哪些系统较容易闯入罢了。有些脚本爱好者随便找一个网络攻击，有些干脆随机选取网络地址（IP地址的高位）看看哪些有反应。一旦获得了一个有效IP地址的数据库，就可以依次对计算机进行攻击了。结果是，一台全新的、有安全保卫的军方计算机，刚联网数小时后就受到了来自Internet的攻击，甚至除了系统管理员外还没有多少人知晓这台机器。

2. UNIX口令安全性

有些（老式的）操作系统将口令文件以未加密的形式存放在磁盘里，由一般的系统保护机制进行保护。这样做等于是自找麻烦，因为许多人都可以访问该文件。系统管理员、操作员、维护人员、程序员、