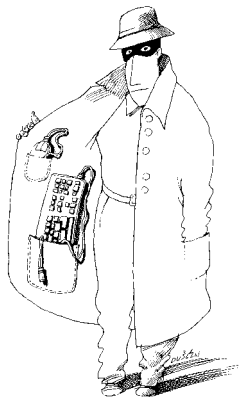
How Hackers Break In...



Port scanners, core dumps and buffer overflows are but a few of the many weapons in every sophisticated hacker's arsenal. Still, no hacker is invincible

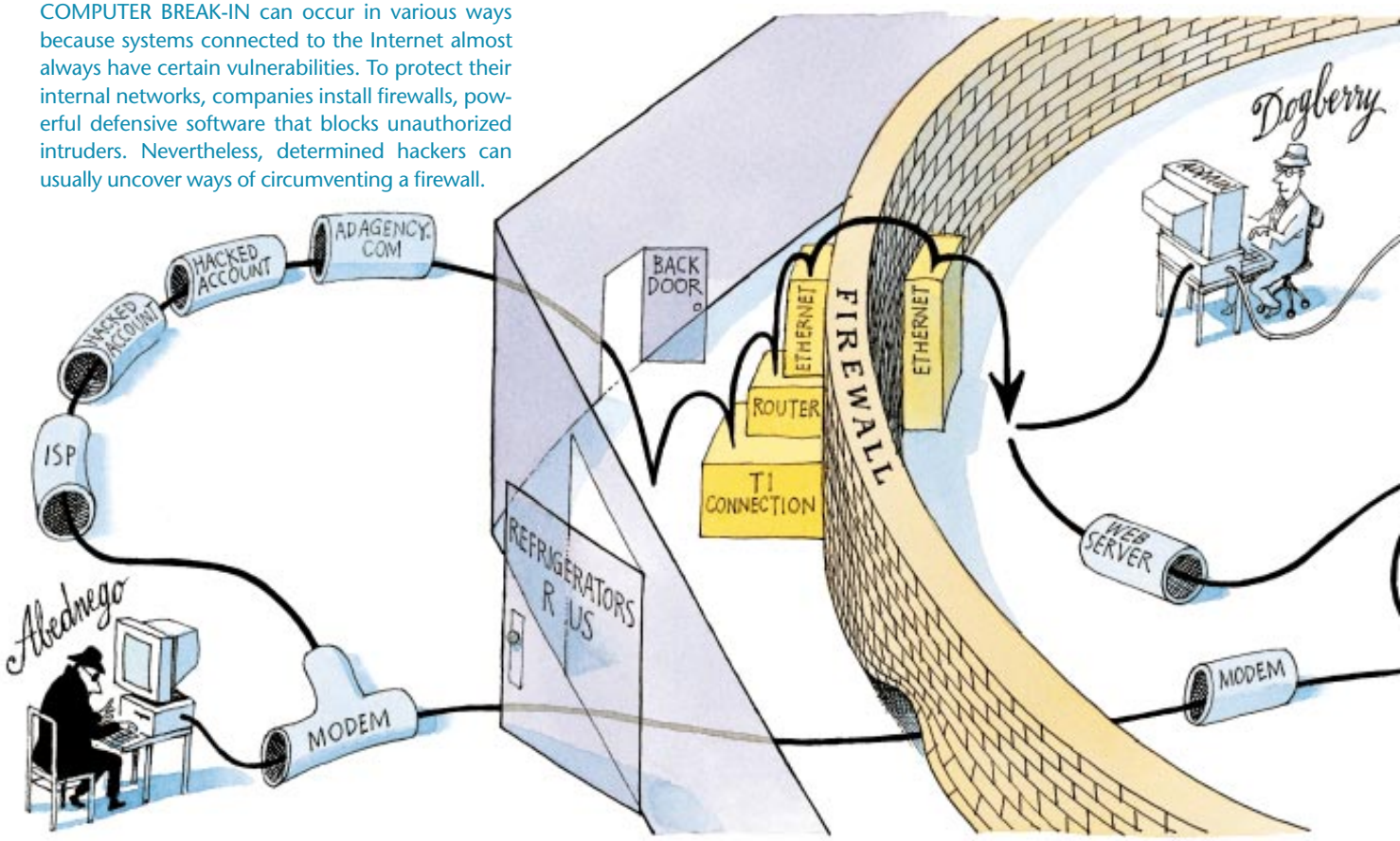
by Carolyn P. Meinel

Editors' note: *This fictionalized account is a composite of many incidents that have occurred, at one time or another, somewhere in cyberspace. The names of people and other details have been changed, but the technologies and software do exist. Some of the events reported here are drawn from the firsthand experiences of the author, who is known both in the computer underground and among security experts for her hacking skills and for her countless battles against hackers.* SCIENTIFIC AMERICAN *thanks Rt66 Internet, an Internet service provider in Albuquerque, N.M., which tested much of the software and hardware described in this article to verify the technologies involved.*

Sitting at his home computer one night, Abednego logs on to the Internet Relay Chat, the cyberspace equivalent of CB radio. After connecting to a channel devoted to the powerful Unix operating system, he watches as the on-line habitués meet to make contacts, build alliances and exchange knowledge. The scene is reminiscent of the cantina in *Star Wars*.

Eager to interject himself into the conversation—and to impress others—Abednego waits for someone to ask a simple-minded question so that he can incite a "flame war," in which the participants begin hurling venomous insults at

COMPUTER BREAK-IN can occur in various ways because systems connected to the Internet almost always have certain vulnerabilities. To protect their internal networks, companies install firewalls, powerful defensive software that blocks unauthorized intruders. Nevertheless, determined hackers can usually uncover ways of circumventing a firewall.



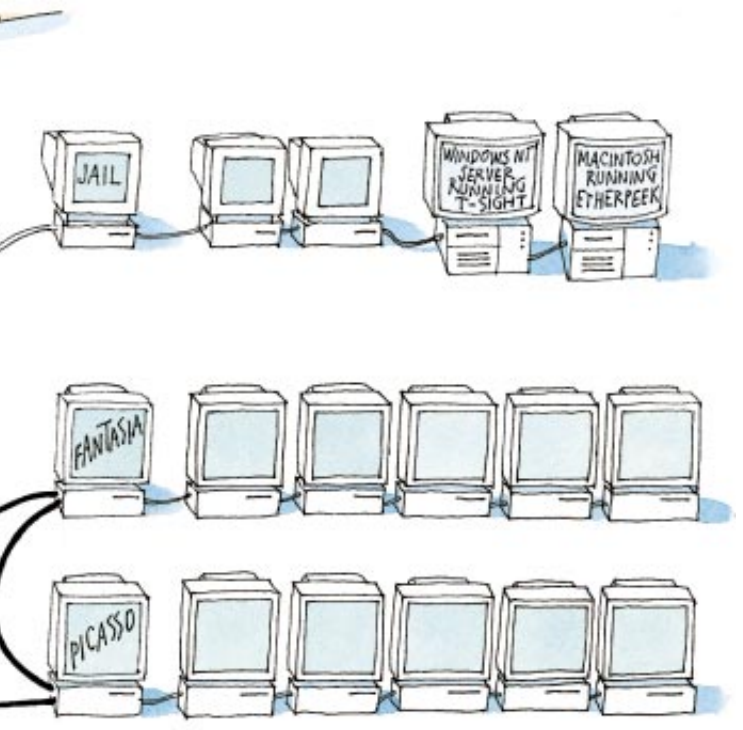
and How They Are Caught

one another. Just then, someone with the handle "Dogberry" asks about writing a device driver for a home weather station. Abednego seizes his chance. "RTFM" is his response. It stands for "read the f——g manual."

Others begin launching nasty insults, but not at Dogberry. Apparently, the question was far more complex than Abednego had realized. Dogberry's terse put-down—"Newbie!"—fans the flames. Humiliated, Abednego vows revenge.

Using the "finger" command on Internet Relay Chat, Abednego obtains the e-mail address "Dogberry@refrigerus.com." Abednego figures that if Dogberry is such a Unix whiz, he might be manager of the computers at refrigerus.com. To confirm his hunch, Abednego uses "telnet" to connect to the mail server of that computer. He then issues the command "expn root@refrigerus.com" and learns that Dogberry is indeed the head system administrator there.

His interest sufficiently piqued, Abednego runs Strobe, a program that attempts to connect with each of the thousands of virtual ports on refrigerus.com. The scanner will meticulously record responses from any daemons, which are automatic utility programs, such as those that handle e-mail. Abednego knows that each port might be an open door—or a door that he might be able to break down—if he can take advantage of some flaw in its daemon.



ALL ILLUSTRATIONS BY DUSAN PETRICIC

But Strobe hits a wall—Dogberry's firewall, to be exact. That powerful defensive software intercepts each incoming packet of data, reads its TCP/IP (transmission control protocol/Internet Protocol) header and determines with which port it seeks to connect. The firewall compares this request with its own strict rules of access. In this case, refrigerus.com has decreed that there should be only one response to Abednego's scanner.

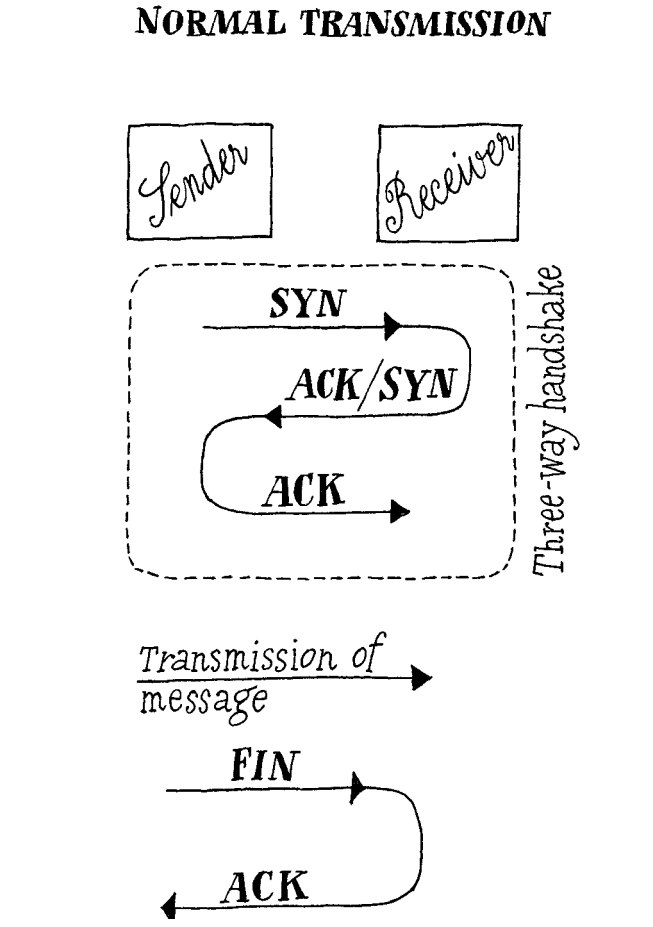
From that instant on, a program on refrigerus.com sends a blitzkrieg of meaningless data, including random alphanumeric characters, back to Abednego, overwhelming his home PC. Meanwhile another daemon sends e-mail to Abednego's Internet service provider (ISP), complaining that someone is attempting to break into refrigerus.com. Within minutes, the ISP closes Abednego's account for suspicion of computer crime.

Although Abednego is caught off guard—many ISPs would not have taken such a strong measure so quickly—the setback is minor. The closed account was only one of several he had created after breaking into that ISP. But the termination of the account at that particular moment causes him to be dumped from Internet Relay Chat in the midst of the flames against him. To the others on-line, it looks as if Abednego has been unceremoniously booted or, worse, that he has fled for cover.

Abednego burns for retaliation. His next step is to try a stealth port scanner. Such programs exploit the way in which IP transmissions work. When one computer wishes to talk to another, it must first transmit a short message packet containing a SYN (synchronize) flag. The header of the packet also contains other important information, such as the IP address of both the source and destination. In response, the recipient daemon sends back a packet that contains an ACK (to acknowledge the received packet), a SYN and a sequence number that is used to coordinate the upcoming transmission. When the first computer gets the return ACK/SYN, it issues an ACK of its own to confirm that all is ready, thus completing a three-way handshake. Then, and only then, can the sender computer begin transmitting its message using the sequence number provided. At the end of the communication, the sender transmits a packet with a FIN (finish) flag, and the receiver returns an ACK to signal that it is aware the transmission has ended.

Abednego knows that a stealth port scanner can take advantage of this process by sending just premature FIN packets to each port on a computer. Typically if a port is open, the recipient daemon will not send any response. If a port is closed, however, the computer will return an RST (reset) packet. But because this computer does not truly recognize a connection until it has completed the opening three-way handshake, it does not record the transmission in its logs. Thus, a FIN scanner can probe a computer in relative secrecy, without ever having opened any official connections. (Yet, as Abednego will soon learn, there is enough information in even one FIN packet to establish a sender's identity.)

Abednego surfs the Internet to search for an advanced



INTERNET TRANSMISSIONS follow certain rigid protocols. Normally, the sender first transmits an introductory message packet containing a SYN flag to synchronize the upcoming communication (*top*). The receiver then returns an ACK, which acknowledges the request, and a SYN. After obtaining this information, the sender transmits an ACK, which completes the necessary three-way handshake. Only then can the sender dispatch the message itself. When finished, he issues a FIN flag, and the receiver returns an ACK, which officially closes the correspondence. A hacker can circumvent the process by sending just a premature FIN, from which the hapless receiver might return an RST, or reset, packet (*bottom*). The response—or lack of one—reveals certain information about the receiver, but because no three-way handshake was ever completed, the transmission is not recorded in the receiver's logs. The hacker can thus probe an unwitting computer in relative secrecy.

stealth port scanner and finds one at an underground Web site. The program, like most other hacker tools, is written in the C computer language. Abednego struggles to compile, or convert, the scanner from C into a form that can be executed on his home PC, which runs on Linux, one of the many variants of Unix.

Abednego's difficulty in converting the software is not unusual because of the many peculiarities of the different flavors of Unix. And Abednego, like many hackers, did not formally study computer science. In fact, also like most hackers, Abednego never learned to program because he never had to: almost any software a computer criminal might ever want is available on the Internet, already written and free for the taking—as long as the hacker knows how to compile it (or has cohorts who do).

The young Dogberry had taken a different path. After befriending a technician at a local ISP, he learned how to administer a network. Before long, Dogberry and the technician were playing computer break-in and defense games. The payoff came when they used the results to help the ISP improve its security. With that success, Dogberry was hired by the ISP to work part-time while he pursued his computer science degrees.

Thus, when Abednego decided to take on Dogberry, he had already made his first mistake. Dogberry is a white-hat (or nonmalicious) hacker and a veteran of many cyberbattles.

Casing the Joint

As dawn breaks, Abednego has finally finished compiling the code and is ready to deploy it. Within minutes, the FIN scanner has given him a snapshot of the services that refrigerus.com offers to those coming only from an approved IP address. Two that draw his attention are a secure-shell daemon, which is a way to make encrypted Internet connections, and a Web server.

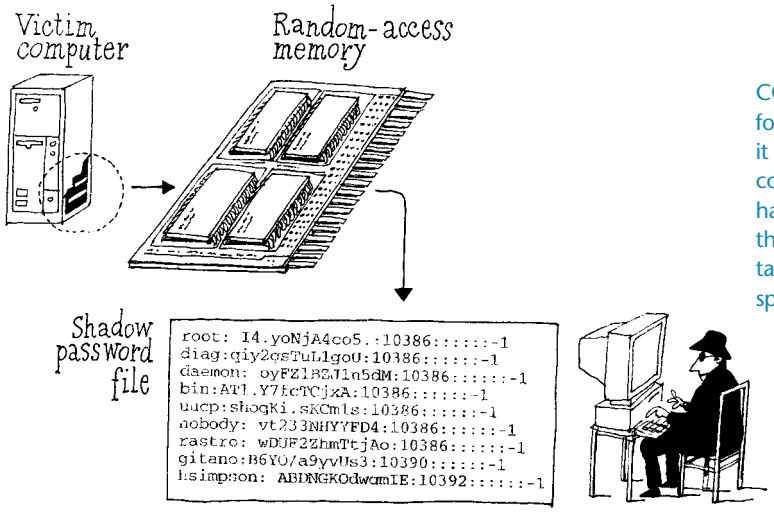
Then Abednego's heart skips a beat. An unusual port number, 31,659, has also turned up on his FIN scan. Could another intruder have preceded him and left a back door, a secret passage to enter the system undetected?

The beeping of a pager jolts Dogberry out of a deep sleep. EtherPeek, a sniffer program installed on the refrigerus.com network, has detected the port scan. Dogberry rushes into the office to watch for more attacks from the console of his administrative computer. His best defensive programs run only from that machine and only for someone who is physically there, so that they cannot be tampered with remotely by an attacker.

Meanwhile, despite the powerful temptation of that 31,659 daemon, Abednego leaves the chase for now. Something—his hacker intuition—tells him that he should return on another night. So by the time Dogberry arrives at work, he sees no more activity.

Curious about the unusual attack, though, Dogberry begins analyzing his computer logs and is able to retrieve the source address from the hacker's FIN packets. With this information, he sends an e-mail to Abednego's ISP, advising the firm of the break-in attempt and asking for details about Abednego's account. But the system administrator at the ISP rejects Dogberry's request, citing a confidentiality policy, because merely running a scanner breaks no law.

Three evenings later Abednego resumes the hunt. But when his computer dials into his account, he finds out his



CORE DUMP can be used by hackers to obtain secret information. When a program running on a computer fails, it sometimes causes the machine to dump, or flush, the contents of a part of its random-access memory (RAM). A hacker can force such an incident to occur so that he can then sift through the discarded data, which might contain important information, such as the passwords for specific accounts on the network system.

password is no longer good. Upset, he phones the ISP and learns that his account has been shut down because of the FIN scan. Yet this turn of events does little to discourage him. In fact, he is now even more determined.

With his credit-card number and a telephone call to a different ISP, he is back on-line within minutes. This time, though, Abednego is more cautious. Through this new account, he logs on to one of his hacked accounts at yet another ISP. Once there, he gives the simple command "whois refrigerus.com." The response tells him the domain name belongs to Refrigerators R Us, a national retail chain.

Next, Abednego tries to log on to refrigerus.com through the 31,659 port by issuing the command "telnet refrigerus.com 31,659." The response is, "You lamer! Did you really think this was a back door?!" Then the 31,659 daemon attempts to crash his PC by sending corrupt packets, while e-mailing the system administrator at Abednego's hacked ISP that someone has attempted to commit a computer crime. Within minutes, Abednego's connection dies.

More determined, Abednego now tries to tiptoe around the firewall instead of forcing his way through it. Using yet another of his many hacked accounts, he begins by attempting to catalogue the computers that belong to refrigerus.com. To obtain this information, he tries "nslookup," which initiates a search throughout the Internet for master databases containing directories of IP addresses.

But "nslookup" is unable to retrieve anything useful. Dogberry must have set up the refrigerus.com network so that all packets destined for any of its internal addresses are sent first to a name-server program, which then directs them to the appropriate computers within the network. This process hinders anyone on the outside from learning details about the computers inside the firewall.

Abednego's next attempt is through an IP address scanner. First, he converts refrigerus.com to a numerical address, using "nslookup." With that number as a starting place, he scans the IP addresses above and below it. He discovers some 50 Internet host computers. Although there is no guarantee that these belong to refrigerus.com, Abednego knows it is a good bet they do.

Next, he uses "whois" to ask whether any other domain names are registered to Refrigerators R Us. The response reveals another: refrigeratorz.com, with an address that is numerically distant from that of refrigerus.com. The IP address scanner soon reveals five additional Internet hosts on numbers nearby refrigeratorz.com.

HACKER LEXICON

Abednego—A biblical Israelite held in Babylonian captivity who walked through a wall of fire and survived.

ACK—See illustration on page 100.

Back door—A secret way to enter a computer that bypasses normal security procedures.

Buffer overflow—See illustration on page 102.

Core dump—See illustration on this page.

Daemon—An automatic utility program that runs in the background of a computer.

Dogberry—The constable in William Shakespeare's *Much Ado about Nothing.*

FIN—See illustration on page 100.

Firewall—Defensive software that protects a computer system from unauthorized intruders.

FTP—File transfer protocol, a common protocol and program used to transfer files over the Internet.

IP—Internet Protocol, a low-level convention that allows computers to move packets of data across the Internet.

Internet Relay Chat—An on-line chat service.

ISP—Internet service provider.

Keystroke logger—A program that records everything a user types at a keyboard.

Port—A connection, or channel, into a computer.

RAM—Random-access memory.

Root—The highest level of access to a Unix computer.

Root kit—A program that hackers implant in a victim computer to hide their nefarious activities.

RST—See illustration on page 100.

Scanner—A program that attempts to learn about the weaknesses of a victim computer by repeatedly probing it with requests for information.

Sequence number—A number used to coordinate an upcoming IP transmission.

Shell—A software layer that provides the interface between a user and the operating system of a computer.

Sniffer—A program that records computer and network activity.

Spoof—See illustration on page 104.

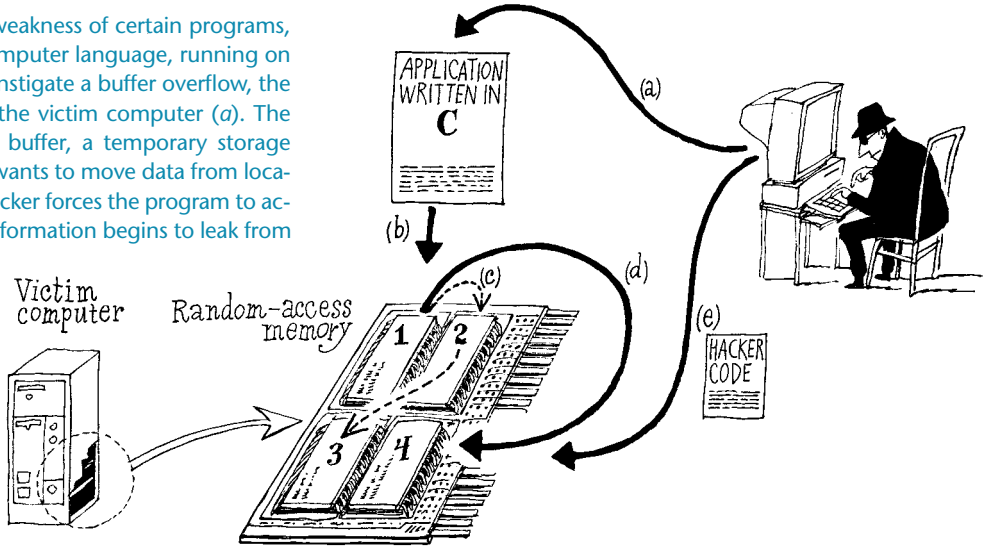
SYN—See illustration on page 100.

TCP—Transmission control protocol, the set of communications conventions that enable the sending and receiving of data over the Internet.

Telnet—A Unix command that enables a user to log on to a computer from a remote location.

Unix—A powerful operating system.

War dialer—A program that will automatically dial a range of telephone numbers.



BUFFER OVERFLOW is an exploitable weakness of certain programs, for example, those written in the C computer language, running on an operating system such as Unix. To instigate a buffer overflow, the hacker might run a C application on the victim computer (*a*). The program begins to write data into a buffer, a temporary storage space in memory (*b*). The application wants to move data from location 1 into 2, then into 3 (*c*). But the hacker forces the program to accept excess data so that some of the information begins to leak from location 1 into 4 (*d*). The hacker can take advantage of the overflow to insert his own code (*e*), which has been written to help him gain high-level privileges to the victim computer.

As a safety precaution, Abednego telnets from his current hacked account into another of his pirated accounts. He then telnets from that location to yet another account that he has hacked, remotely logging on to it in preparation to run more FIN port scans. The extra steps will force anyone in law enforcement to obtain search warrants for three companies, encumbering the process.

He also decides to hide on the third hacked computer under the protection of a root kit, a Trojan horse program that, despite its harmless appearance, will automatically delete any evidence of his actions from the logs used to detect abnormal activities. The software also defeats other programs that seek to detect alterations to system files on that computer. A root kit will even prevent people from determining that he is logged on and running programs.

From this safe perch, Abednego scans one after another of the Internet host computers at refrigerus.com and refrigeratorz.com. The FIN scanner slips straight through the firewall to every one of them. The activity, though, is detected by the EtherPeek sniffer, which again sets off Dogberry's beeper.

A haggard Dogberry, after rushing to work, soon identifies the origin of the FIN scans and alerts the system administrator at Abednego's third hacked account. But the root kit has done its job, hiding Abednego from mystified computer operators there. Abednego boldly continues, switching from the stealth scanner to Strobe in hopes of finding an IP address that the firewall does not protect.

He succeeds only in having the refrigerus.com firewall unleash a flood of meaningless data. The sudden load finally convinces the system administrator at Abednego's hacked account that there really must be an attacker at work. She takes the drastic step of cutting the entire system off from the Internet. As his connection fizzles, Abednego realizes there is no elegant way around the firewall.

Finding a Workaholic

For each of the several dozen Internet hosts at Refrigerators R Us, Abednego guesses that there are probably many other desktop computers sitting quietly in employees' cubicles and offices. What are the chances, he muses a few nights later, that somewhere among those hundreds of users are workaholics who circumvent the company firewall by phoning into their computers from their homes to perform late-night tasks? It's simple, really, for someone to buy a modem, connect it to a computer at work and plug a phone line into it before leaving for the day.

Knowing that almost every large corporation has at least one unauthorized modem on its network, Abednego sets up ShokDial, a war-dialer program that will call each of the extensions to the phone system at Refrigerators R Us as well as other numbers within that exchange. At the headquarters building of the company, the night watchman hears the ringing of one office phone after another but thinks nothing of it.

Then, at 2:57 A.M., the war dialer pulls up a modem, and Abednego is greeted with the log-on screen of a Silicon Graphics computer: "Refrigerators R Us Marketing Department. Irix 6.3." Great, Abednego thinks, because Irix is a type of Unix, which means he has found a potent portal into Dogberry's world.

Abednego's next strategy is to try brute force, using a program that will repeatedly dial the Irix box and guess passwords for root, a top-level account (usually reserved for system administrators) from which he can run any command and access all information on that particular computer. He is hoping that the owner of the Irix machine, like many harried workaholics, has negligently allowed remote access to a root account.

The password guesser starts with common words and names and from there tries less obvious choices. The slow, painstaking process can take months, even years, as the program exhausts every word in an unabridged dictionary, all names in an encyclopedia and each entry from a local phone book. But Abednego gets lucky. Around 5 A.M. he learns that the password is simply "nancy."

"Yes!" Abednego shouts as he logs on to a root shell, from which he can then issue other commands to run on that machine. Next, he secures his beachhead, using FTP (file transfer protocol) to plant a root kit and sniffer onto his latest victim. He sets the program to capture and record everything typed in at the console (a process known as keystroke logging), as well as any log-on sessions from the network. The sniffer will hide this information in an innocuously named file right there on the unwitting host. Within min-

utes, Abednego's root kit has even set up an additional way to log on: user name "revenge," password "DiEd0gB."

Abednego's last deed that morning is simple. To find the Internet address of the hijacked box, he types the "who" command, and his computer shows user "revenge" logged on to picasso.refrigeratorz.com. Later that morning the rightful owner of picasso logs on and sees no indication that someone has usurped control of her computer. Abednego's root kit is doing its job.

For Dogberry's part, all that his log reveals is an early-morning attempt to enter refrigeratorz.com from the Internet. Remembering the recent FIN scans, Dogberry is troubled by this latest incident, but he has too little information to take action.

Two nights later Abednego dials in and connects with picasso to view his logs. To his dismay, he sees that information on the internal network traffic has been encrypted. But the keystroke logger of his sniffer has recorded that someone on picasso had logged on to another computer named fantasia. Abednego now owns a user name and password for fantasia. Open sesame!

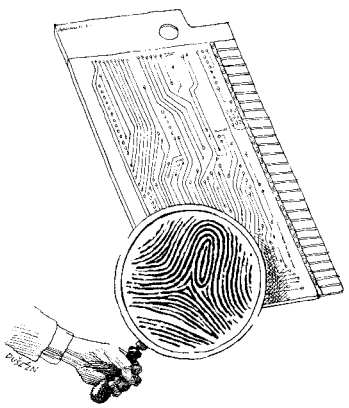
Abednego discovers that the computer is a SPARC workstation used for rendering animated sequences, perhaps for television ads. Because the box is probably a server used by many other computers, Abednego begins hunting for a password file, hoping that some of the passwords he finds will also work on other machines inside the company network.

He locates the file but discovers only "x" characters where the encrypted passwords should have been. Apparently, the information he seeks is hidden elsewhere in a shadowed file. Smiling to himself, Abednego runs the FTP program and tricks it into crashing. Bingo, core dump!

Fantasia is forced to flush a part of its random-access memory (RAM). Fortunately for Abednego, the discarded information—a record of what was being held in that RAM sector at that moment—ends up in the user directory.

The legitimate purpose of a core dump is to enable programmers to perform an autopsy on the digital remains in search of clues to a program's failure. But, as Abednego well knows, a core dump has other uses. A shadowed password system sometimes places encrypted passwords in RAM. When a person logs on, the computer does a one-way encryption of the password the user attempts and compares that with the encrypted password from the shadowed file. If the two match, the person gets in.

The shadowed password file that Abednego is able to retrieve from the core dump on fantasia is encrypted, so he starts running his password cracker. The program could be busy for the next few days, maybe even weeks.



Too impatient to wait, Abednego is already working on his next maneuver—exploiting a common vulnerability of Unix. When a program running on that operating system pours excessive data into a buffer (a temporary storage space in memory), the information will leak, infiltrating other areas of the computer's memory.

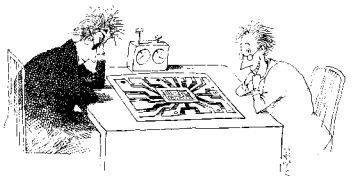
Abednego takes advantage of the buffer overflow by using it to insinuate his own code into the SPARC. The added software helps him create a root shell, from which he can then run other commands and programs. Pleased with his latest effort, Abednego next installs a root kit and sniffer. Because the kit will hide evidence of his activities only from the time when the program was activated, Abednego must mop up by deleting previous actions of his busy night.

One task remains. Is there anyone who is allowed to log on to fantasia from the Internet? Abednego types the "last" command to display records of connections people may have made to fantasia. He perks up as he sees that user names vangogh and nancy have recently entered fantasia from the Internet through the domain "adagency.com," which lies outside the Refrigerators R Us firewall.

Abednego can hardly fall asleep that morning. His adrenaline flowing, he buzzes with the knowledge that he will soon "own" Refrigerators R Us.

Closing in for the Kill

The next evening Abednego makes short work of breaking into adagency.com. At first he uses IP spoofing to trick that computer into recording a false IP address for his location. By probing adagency.com with SYN packets to elicit ACK/SYN responses with an assortment of sequence numbers, Abednego's program is able to tease out a pattern from which he can then guess the next sequence numbers and use that knowledge to fake his origin. Abednego quickly installs a sniffer on adagency.com and uses a secure-shell program to create an encrypted connection for logging on to fantasia.



From that computer, he types the "netstat" command to view tables of active connections within the network. He discovers a computer that he had missed in his earlier search. Its name, "admin.refrigerus.com," is promising. Could that be from where Dogberry oversees the system?

Meanwhile every time Abednego's PC cracks yet another combination of user name and password, he tries it on various refrigerus.com computers. But none of them works anywhere except on fantasia, which he already "owns."

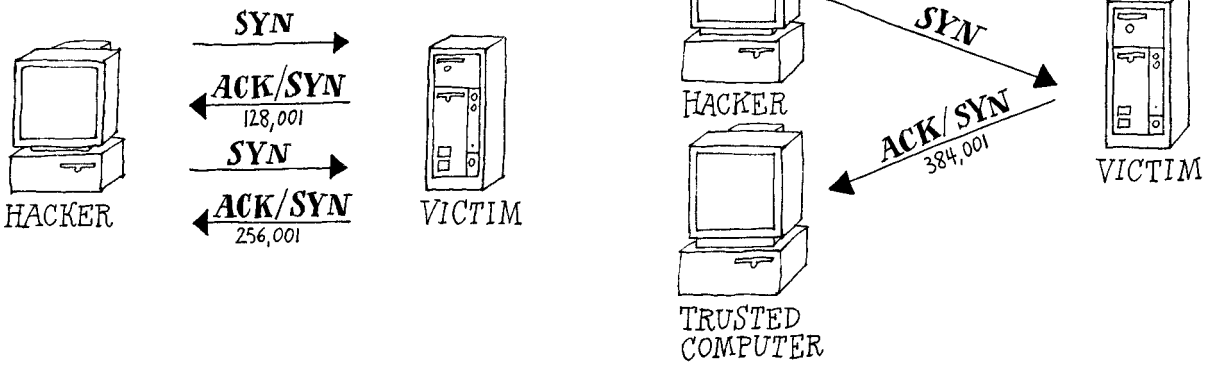
Then Abednego hits the jackpot. Twice.

On fantasia he captures keystrokes made by vangogh as that user updated the company's Web server. Now Abednego has the password he needs to hack the Refrigerators R Us Web site. In addition, his sniffer on picasso reveals that someone, Nancy, has dialed into that computer and from there used a back door to log on to a root account, hidden by her root kit, at admin.refrigerus.com.

He slips right behind Nancy into admin.refrigerus.com. Using the root account there, he tries logging on to one Refrigerators R Us computer after another. Dogberry, however, has been exceedingly careful. On the Refrigerators R Us network, even root privileges do not allow someone to enter other computers without providing new passwords.

Only briefly distracted, he turns his attention back to the Web server and logs on to it using his recently acquired password. From his home PC, he then uploads a new version of the Refrigerators R Us home page that he had put together in anticipation of this day.

Back at Refrigerators R Us, Dogberry is working late, poring over his logs. It seems the marketing people have been



IP SPOOFING enables a hacker to fake his identity. The hacker first probes his victim by sending multiple SYN packets [*see illustration on page 100*] to obtain ACK/SYN messages with sequence numbers (*left*). From these responses, the hacker is able to uncover a pattern. In this example, he notices that the numbers increase by an increment of 128,000. Next, the hacker sends a SYN that impersonates another computer that the victim trusts. The victim then transmits an ACK/SYN to this authorized host (*center*). Although the hacker does not receive this particular response, he can nonetheless continue the correspondence as if he had: he is-

getting an unusual number of connections from adagency.com. Tomorrow he will ask those folks exactly what is going on. He will also call the system administrator at adagency.com, a colleague whom he once helped to install some new system software.

Just as Dogberry is about to head home for the night, the phone in his office rings. An angry customer complains that Refrigerators R Us's Web site features a pornographic movie with a refrigerator as a prop. After bringing up and viewing the defaced Web page, Dogberry moves quickly to sever the umbilical Ethernet cable that connects the company network to the Internet.

Abednego is enraged when his obscene masterpiece is taken down so quickly. But he is also worried that he has left too much evidence behind, so he returns using the dial-up line to picasso—an entryway that is still unknown to Dogberry. He buys time by reformatting completely the administrative computer's hard disk, which shuts down the company network, temporarily thwarting Dogberry's efforts to gather details of the attack.

Dogberry rushes to the administrative computer with hopes to reboot it from the console, but he is too late. Dogberry must now rebuild the software on that computer from scratch. (Unbeknownst to Abednego, though, the EtherPeek sniffer running on a nearby Macintosh has also been making logs.)

Abednego, still peeved about the Web site, has one final act that night: he unleashes a flood of data packets against refrigerus.com. Soon Dogberry gets a frantic call from a company salesperson who, using her laptop PC and a phone line in her hotel room, wants to retrieve her important e-mail but has been unable to connect to the mail server at Refrigerators R Us.

The next morning an exhausted Dogberry begs the vice president of technology at Refrigerators R Us for an okay to wipe clean every computer in the network, reinstall every program and change all passwords. But the extensive—though prudent—measure would require shutting the system down for days, and the vice president denies the request.

At this point, Abednego's malicious and destructive exploits have gone well past the legal bounds for hacking. But the FBI, which is severely understaffed, has been busy investigating some recent break-ins at several army and navy computer systems around the U.S. Dogberry will have to gather more evidence himself.

Because the attacker remained on the system even after it had been physically disconnected from the Internet, Dogberry suspects there must be a contraband modem somewhere in the building. He runs his own war dialer and discovers the culprit. He will soon have words with the marketing department!

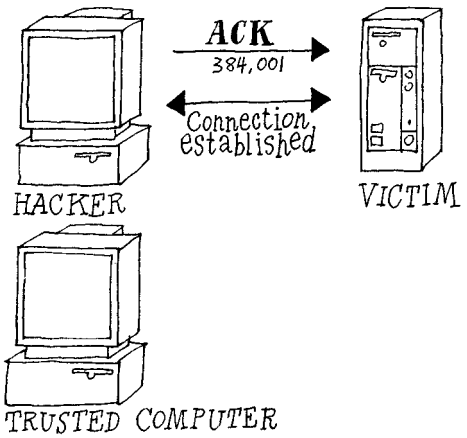
Dogberry then reloads a clean version of his main administrative computer. Next, on a Windows NT server that Dogberry knows has not been tampered with, he deploys T-sight, an advanced antihacker program that can monitor every machine on the company network.

Last, Dogberry sets his trap. T-sight will watch for the attacker's next connection to admin.refrigerus.com and will redirect the intruder into a "jail" computer. Once there, the culprit can be monitored and traced. To keep the unsuspecting person distracted, Dogberry enlists a team of programmers to make the jail look like an accounting system, complete with the tempting bait of fake financial data.

Pride Goeth Before…

Just two nights later Dogberry is standing watch at 8:17 P.M. when he discovers someone once again entering admin.refrigerus.com. It is Abednego. Why has he returned so soon? Abednego was exhilarated when he learned that his pornographic Web site had become the talk of the hacker underground. He had even rated a brief mention on CNN. The publicity and his hubris were a potent combination, making Abednego feel invincible.

In fact, tonight he has brazenly reentered Refrigerators R Us without his customary caution. After dialing into a guest account on an ISP, he telnetted directly to adagency.com to gain faster access to fantasia's back door.



sues an ACK message with the correct predicted sequence number, thus establishing a connection between his computer and the victim (*right*). The hacker can then transmit information that the victim will assume is benign because of the mistaken belief that it is coming from the trusted host computer.

From admin.refrigerus.com, Abednego is lured to the jail by T-sight. He can hardly control his excitement as he begins sifting through what he believes are sensitive financial records.

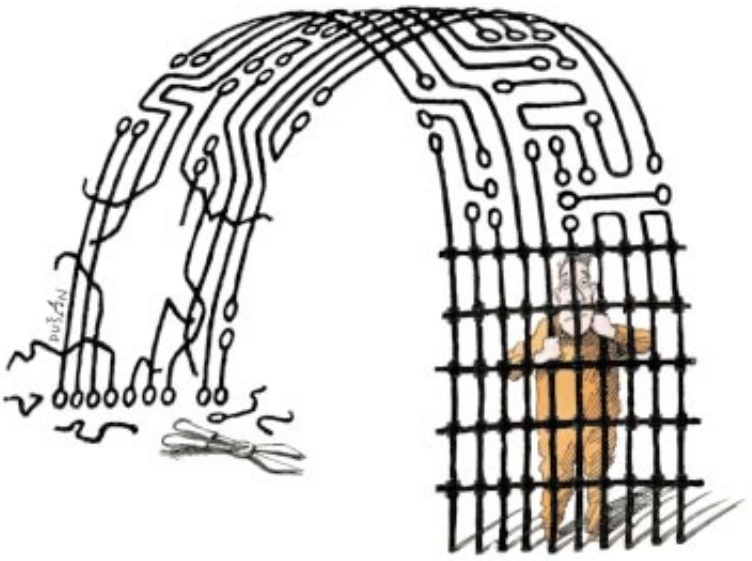
Dogberry, too, is busy. Quickly analyzing data from T-sight, he obtains Abednego's root password on fantasia—DiEd0gB—and is able to trace the intruder back to adagency.com. Dogberry calls the pager of the system administrator there. She has already left work, but she phones Dogberry from a restaurant to help him continue tracking Abednego.

So while Abednego is retrieving a huge file containing bogus credit-card numbers, Dogberry installs a sniffer on adagency.com. He is even able to sneak unnoticed into Abednego's account on that computer by typing DiEd0gB, because Abednego has lazily used the same password for all his root kits. Then, just minutes before Abednego finishes his download and logs off, Dogberry succeeds in tracking the trail of the plundered credit-card file back to Abednego's dial-up account at the ISP.

The information Dogberry has obtained is enough to bring in the FBI, which contacts the ISP the next day to obtain Abednego's identity from the company's phone logs. With enough evidence in hand, including the Macintosh's high-quality EtherPeek logs, the U.S. Attorney's office approves a search warrant.

Soon after, FBI agents raid Abednego's apartment and confiscate his PC. The hard disk of the computer will reveal all. Abednego had taken the precaution of erasing incriminating files from his PC after each night's escapade. He is chagrined to learn that the FBI can extract that information from his hard drive even after it had been erased and overwritten several times. Soon a laboratory has recovered details of his past trespasses, including the time he romped through the computer system at a major banking institution in the Northeast.

The megabytes of incriminating data provide the smoking gun necessary to indict Abednego on multiple counts of computer fraud. Unfortunately for him, the trial judge assigned to his case is known for her tough stance on cybercrime. Taking his attorney's advice, Abednego wisely accepts a plea bargain even though, like many hackers who have crossed the line, he insists that his activities—which, for Refrigerators R Us alone, resulted in thousands of dollars in damages—were just playful pranks. Abednego is currently serving a two-year sentence in a federal prison. SA



The Author

CAROLYN P. MEINEL is addicted to the frontiers of technology. She is the author of *The Happy Hacker: A Guide to (Mostly) Harmless Computer Hacking* (American Eagle Publications, 1998) and the president of Happy Hacker, Inc., a nonprofit organization devoted to teaching people how to hack responsibly and legally. The group runs a hacker wargame on its World Wide Web site (http://www.happyhacker.org). Meinel holds an M.S. in industrial engineering from the University of Arizona. She is currently working on a book with Jason Chapman, recounting her many adventures battling hackers. Meinel wishes to acknowledge the help of Michael and Diana Neuman, Damian Bates, Emilio Gomez, Mahboud Zabetian and Mark Schmitz in researching this manuscript.

Further Reading

ESSENTIAL SYSTEM ADMINISTRATION. Second edition. Æleen Frisch. O'Reilly & Associates, Sebastopol, Calif., 1995.

INTERNET FIREWALLS AND NETWORK SECURITY. Second edition. Chris Hare and Karanjit Siyan. New Riders Publishing, Indianapolis, 1996.

MAXIMUM SECURITY: A HACKER'S GUIDE TO PROTECTING YOUR INTERNET SITE AND NETWORK. Anonymous. Sams Publishing, Indianapolis, 1997.

THE GIANT BLACK BOOK OF COMPUTER VIRUSES. Second edition. Mark Ludwig. American Eagle Publications, Show Low, Ariz., 1998.

Additional information can be obtained at http://www.geek-girl.com/bugtraq, http://ntbugtraq.ntadvice.com, http://rootshell.com, http://www.infowar.com, http://www.antionline.com and http://www.happyhacker.org on the World Wide Web.

Details of EtherPeek and T-sight can be obtained at http://www.aggroup.com and http://www.engarde.com, respectively.