



Attackers Using Non-Network Methods to Gain Access

IT security professionals spend a lot of time hardening servers, configuring router and firewall rules, running vulnerability scanning tools, and even performing some penetration tests. Consequently, it is very easy to overlook the two simplest ways of gaining access to information assets—asking for it and taking it. To this point, this book has covered penetration testing through the use of computers. Now you'll take a look at penetration testing that uses two methods that do not employ computers—physical access and social engineering—and you'll see how threats can be mitigated.

Gaining Physical Access to Information Resources

As information security has evolved into the high-tech maze of computer and network security, many IT professionals have lost sight of physical security. Providing physical security for paper records is not necessarily the same as providing physical security of electronic data. For example, 100,000 paper files might take up a room full of file cabinets; however, these same files as electronic media might fit on a single CD. Obviously, it would be much more difficult to sneak a room full of file cabinets out the door than it would a CD in a portable CD player. Once an attacker has physical access to a resource, there is little if nothing that you can do as a security administrator to prevent the

attacker from gaining access to information on it. Your best approach is to prevent the attacker from gaining access to more computers and devices on your organization's network. You can do things in advance to prevent attackers from gaining physical access to these information assets, and you can conduct penetration tests to ensure your methods are effective.

The skills of a physical penetration tester are very different from those of their electronic brethren, but the thought processes of each tester are very similar. To be an effective physical penetration tester, you need to have a lot of composure, think quickly on your feet, and easily blend into your surroundings. And, much like an electronic penetration tester, you need to be patient, methodical, creative, and—in the end—think of the things that the people securing the information will not.

If you have been assigned or contracted to perform a penetration test and physical penetration testing is specifically included in the project, here are some types of tests to run:

- Physical intrusion
- Remote surveillance
- Targeted equipment theft
- Dumpsters and recycling bins
- Lease returns, auctions, and equipment resales

Physical Intrusion

How easy would it be for someone to walk right in the front door to your organization? Not so easy, you say, but what about going through the side door or the loading dock? The best way to gain entry into a facility is to identify and exploit poor security dependencies. A more trusted component should never trust a less trusted component. For example, the main entrance of a building might be protected by badge scanners, security guards, receptionists, cameras, and other security measures (the more trusted component), but at almost any time of day a group of people stand at a side door smoking (the less trusted component). After you stand with the group gossiping, odds are that you can walk right in behind them, a situation commonly called *tailgating*. The flaw in this security design is that building security is dependent on the side door, which compared with the front door has little security.

People who already have physical access represent another possible physical entry point for attackers. A great example of this was shown in the 1987

film *Wall Street*. An eager stock trader, Bud Fox, played by Charlie Sheen, wants to get information about the merger plans of a company. After his initial attempts to get information from friends associated with the company, he simply buys half of the company that does the janitorial work for the company that he wants to get information about, and then himself dons a janitor's uniform and rifles through the company's files at night. In this case, the company possessed information that had very high security requirements, requiring 24/7 mobile security guards, but the security of its offices were dependent on the janitorial service. Certainly, this example should not cause suspicion of contract workers; an attacker can just as easily gain this type of access by purchasing a delivery uniform and walking right into a building by way of the loading dock where packages are normally dropped off. Once inside the facility, the attacker could gain access to:

- Computers
- Wiring closets
- Mailrooms, file cabinets, labs, and equipment rooms

Computers

An attacker can find an empty office or cubical and, by using a bootable CD-ROM, load an operating system shell and replace the administrator credentials on the host. As the local administrator, the attacker can install whatever type of software she wants, including keyboard logging software or rootkits. The attacker can also extract other information from the computer, such as password hashes, stored credentials from Microsoft Internet Explorer, or service account credentials. The attacker can install hardware-based keystroke monitoring. Of course, the attacker could just steal the computer, but this would likely be noticed fairly quickly. If the attacker is able to get access to servers, where highly valued assets are more commonly stored, the potential impact on information security is much greater.

One of the most obvious methods of gathering information from an organization's network is simply to search for it. If an attacker can gain access to a computer, she will likely be able to find the organization's intranet portal and search it for key terms. An attacker might do this to get information about marketing plans, product release plans, legal documents, and company strategy. You might be surprised at what you can find just by searching for it. Kiosk computers and computers left unattended and unlocked are particularly good targets.

Notes from the Field

Years ago I was leading PC support at a financial company. One afternoon I looked out my window and saw a person I had never seen before walking across the parking lot with one of the company's computers in a shopping cart. I recorded the license plate number as I watched him load the computer into the trunk of his car. After the person left, I went to the reception area and asked the two security guards whether they saw the person taking the computer. One admitted that he held the door for him. Neither knew who the man was or when he had entered the building. Reviewing the sign-in log proved that the man had not signed in. Much to my surprise, minutes later, the man returned—apparently he had forgotten the power cord to the monitor. As it turned out, the man was a contract programmer who had been hired earlier in the day. The manager who had hired him reported that the programmer did not have permission to remove the company's computer from the premises. The programmer was fired, the security guards reprimanded, and I wound up leading a complete review of the physical security of the facility. This was my entry into physical penetration testing. It turned out that the building where my office was located was the only facility that had serious physical security issues. This was in part because it housed the IT staff, and the security guards and other employees were accustomed to seeing PCs being carried around (although not in shopping carts). The point of this example is that you might never know how effective your company's physical security is until you test it.

Wiring Closets

An attacker can also carry out a more passive attack, such as monitoring network traffic for authentication packets and other types of information on the wire by locating a network wiring closet. More interesting and certainly much more threatening is an attacker's ability to attach a network access point to the local area network and carry out surveillance from afar. A good component of your penetration test would be to determine whether your network would be vulnerable to this: place a wireless access point on your network in an area that is generally public, such as a mailroom or reception area, and see how long it takes before it is detected.

To prevent network disruption, you probably will want to disable Service Set ID (SSID) broadcasting on the access point and configure it to require MAC

authentication. This will also help prevent an attacker from using the planted wireless access point as an entry to attack the network while the penetration test is ongoing. Many software packages not only enumerate wireless access points, but also plot them geographically relative to other access points.

In addition to network wiring closets, telephone closets are targets of attackers. If your organization has an office in a large office building, you might be sharing network and telephone closets. If this is the case, analyze whether this sharing constitutes acceptable risk. For example, for a small family real estate business, the risk of someone tapping into your network or telephone system through the wiring closet is probably low; however, this risk might be a very real concern for a defense contractor or pharmaceutical company.

More Info For detailed information about network sniffing and detection, see Chapter 19, “Network Sniffing.” For additional information, see Robert Graham’s website at <http://www.robertgraham.com/pubs/sniffing-faq.html>.

Mailrooms, File Cabinets, Labs, and Equipment Rooms

Attackers might also target mailrooms, file cabinets, and equipment rooms, especially in the facility in which the IT services are located. These places often hold confidential information that the attacker might be searching for. If your organization has labs or equipment rooms, attackers could steal equipment or look for documents left lying around. If your organization does any type of research and development, in addition to analyzing the physical security of the facility that houses these operations, carefully analyze what type of materials are left in plain view.

Remote Surveillance

Physical intrusion is very risky, and many attackers would find doing it very difficult in many organizations. Furthermore, many would-be attackers do not have the constitution and confidence to walk right into the enemy’s stronghold. So another way of getting access to resources inside the facility is remote surveillance. This gives the attacker a relatively safe buffer while still allowing him to gain a level of physical access to a facility.

Remote surveillance takes on many forms, from burying audio bugs into the concrete foundation of a building and reading electromagnetic impulses from typewriters, to less high-tech methods such as peeking into windows and

shoulder surfing. One famous example of remote surveillance that was originally thought to be impossible was a technique first theorized and then built by a Dutch researcher named Wim van Eck. van Eck was able to reproduce the image on a cathode-ray tube (CRT) monitor on his own monitor by intercepting the ambient radiation of the raster drawing of the display and reconstructing the image on his own screen. The lesson to be learned here is that although a type of remote surveillance might at first appear impossible, cost prohibitive, or improbable at best, it might actually be in use by governments and private individuals. Most organizations do not need to lose sleep over van Eck's methods, but remember that today's well-known remote surveillance technique was yesterday's underground tool. As a penetration tester, you should examine several types of remote surveillance techniques to determine your organization's susceptibility to them, including these:

- Looking in windows
- High-tech shoulder surfing
- Electronic eavesdropping

Looking in Windows

Yes, I am sure that visions of Peeping Toms are rushing through your head, but in reality, looking in windows, either from immediately outside the window or from a long distance, is a real threat. Common targets include conference room whiteboards, computer monitors, and keystrokes. For example, a video game design firm is pitching its idea to a rival company or testing its game. A rival competitor could gain an edge on negotiation by using binoculars from across the street to see game demos and financial projects from meetings in the game platform maker's offices. Turning monitors away from windows, isolating computers with secret information in rooms without windows, and erasing conference whiteboards after use are all good methods of preventing this type of remote surveillance. You might also consider moving certain business groups to higher floors to increase the difficulty of looking in windows.

High-Tech Shoulder Surfing

Although shoulder surfing—which is looking over someone's shoulder to read a screen or some papers, or to watch keystrokes—is a time-tested way of getting information, it is at best risky, difficult, and inefficient. Unfortunately, technology has come to the rescue and made shoulder surfing a real threat.

The best examples of high-tech shoulder surfing technologies are camera-equipped cell phones. These devices remove the pressure of having to remember what was seen. In the spring of 2003, a group of attackers used video recording cell phones to empty bank accounts around Modesto, California.

Police estimated that hundreds of people had been victims of the group. The attack was quite simple and highly effective. The attackers found a national bank whose customers were assigned the same PIN for ATMs and for their online banking accounts. The attackers stood behind their victim at the ATM, fiddling with a cell phone as the unsuspecting victim completed her transaction. If the victim threw the receipt away, the attacker waited until the victim left and then retrieved the receipt from the garbage. The attacker was then able to obtain the victim's PIN from the video recorded at the ATM, and along with the account number on the ATM receipt, empty the victim's bank account over the Internet. At the time of this book's printing, no one had been apprehended for these thefts. This same technique would be very effective in capturing password keystrokes or information on a screen. Also, if your organization restricts access to certain types of information to being viewed in person only, this type of technique might be a threat.

Electronic Eavesdropping

Another type of remote surveillance is electronic eavesdropping. By intercepting information in transit, an attacker can gain information leaving few to no footprints. In addition to remote audio and video surveillance devices, more commonly known as bugs, common types of electronic eavesdropping include:

- Sniffing wireless networks
- Capturing traffic downstream
- Retrieving voice mail

Note In movies and in television, bugging devices are small and difficult to find, but many common devices can be used for this purpose. For example, a laptop with a wireless network card with the microphone turned on makes an excellent bugging device that no one would think twice about.

Sniffing Wireless Networks Wireless networks are interesting because they exist as part of the local area network just as wired networks do, but the same physical security techniques do not apply at all. Although you can secure the cables used to transmit signals on wired networks, you cannot secure the physical medium of wireless networks; consequently, wireless networks are inherently vulnerable to sniffing.

More Info See Chapter 13, “War Dialing, War Driving, and Bluetooth Attacks,” for detailed information about penetration testing wireless networks.

Capturing Traffic Downstream One type of electronic eavesdropping that is often overlooked but could provide a wealth of knowledge is capturing traffic downstream from your target. For example, by analyzing e-mail headers, you might see a sudden increase in e-mail between two companies not known to do business together and an investment bank. By connecting the dots, so to speak, an attacker could discover a merger long before the public does. Because this threat is rarely assessed during a penetration test, it will not be covered in depth here, but you should at least be aware of it.

Retrieving Voice Mail Because of the increase in unified messaging and the overall decrease in the popularity of hacking telephone systems, attacks on voice mail systems or mailboxes are not nearly as prevalent as they once were. Just the same, voice mail stores information as much as e-mail does, so you should consider it in your penetration testing and threat models. More importantly, as security systems that rely on multiple methods of distribution become more common, voice mail systems might be interesting to an attacker. Several enterprise password-management systems offer self-service password reset through automated computer or phone systems and use voice mail as the means to inform the user of the new password. The single biggest reason voice mail systems and mailboxes are compromised is the default password, such as 12345.

Targeted Equipment Theft

At nearly any grocery store during the evening rush in any city, a walk through the parking lot reveals computer bags and briefcases on the front seats of cars. Many organizations, especially larger ones, are synonymous with the cities where they are based—Redmond, WA and Microsoft, for example. One way a motivated attacker might begin her attack on a network is by stealing a computer from an employee at the organization she is targeting. If an attacker wanted to target Microsoft, staking out a grocery store near the company headquarters might be a viable avenue of targeted equipment theft.

Easier than you might think

This might sound paranoid, but targeted equipment theft is not unprecedented. Two good examples of this were widely reported by the mainstream media in 2000. In July 2000, a commander in the British Royal Navy had his laptop stolen from his car, which was parked outside his house. His laptop was reported to hold top-secret information. The corporate world has not been immune to such incidents of laptop theft either. In 2000, the laptop belonging to the CEO of Qualcomm was stolen after he delivered a presentation at an industry conference. According to the media, the CEO was less than 30 feet away when his laptop was stolen from the podium from which he had been speaking. Because the CEO had been using his laptop to give the presentation, he probably left it unlocked when he walked off the podium, making many types of data protection, such as encrypting file system (EFS), useless.

Mobile telephone devices also have a high incidence of theft and loss. At the very least, a thief can use a stolen phone to make long-distance and international phone calls, creating very expensive phone bills for the owner. A thief can also retrieve contact information from a phone's address book, potentially subjecting the phone owner's friends and family to identity theft. A more serious vulnerability, however, is the Internet access or even full computing power that many mobile phones have, for example, the Smartphone and Pocket PC Phone Edition devices. Such devices can have confidential information stored on them, such as passwords and private e-mail messages. Other types of devices in this category include handheld e-mail devices such as the BlackBerry, PDA devices such as the Palm Pilot, and handheld PCs such as the Compaq iPAQ. Because users of these devices often find entering data difficult, perhaps because they must use an onscreen keyboard or handwriting recognition software, they frequently store network credentials such as passwords persistently. An attacker could retrieve these credentials to later attack the network of the device user's organization. These mobile devices also have the capability to store files, which an attacker could retrieve from the device, if stolen.

Note To be certain, targeted equipment theft is not a very probable threat for most small to mid-sized companies; however, for companies that have high-value intellectual property information assets and for government agencies, this threat should not be dismissed.

Dumpsters and Recycling Bins

Every day, employees discard paperwork, manuals, electronic media, and notes; although these items are no longer useful to the employee, they could contain valuable and useful information for the attacker. At the end of the day, the janitorial staff takes these items out with the garbage. They have to go somewhere.

Microsoft itself has been the victim of “dumpster diving.” In June 2000, the Oracle Corporation admitted to hiring Investigative Group International (IGI), a private detective firm, to gather information from Microsoft that could be used by anti-Microsoft lobbying groups. Though Oracle maintained that they did not suggest or direct any methods for obtaining this information, IGI’s methods included targeting garbage. In a related incident, a known investigator for IGI offered night janitors for an industry trade group cash for two bags of garbage. If you walk around the Microsoft campus in Redmond, you will notice that there are no dumpsters in the open, and those that are around are used only for food waste and non-paper recycling—a consequence of the IGI incident. Instead, waste and recycling from offices is gathered and disposed of through a more secure process.

The bottom line is that attackers, in this case a private detective firm, will go to nearly any length if the motivation is ample. As a penetration tester, you should consider determining whether an attacker could get access to dumpsters and recycling bins, and if so, what information an attacker could obtain from these sources.

Lease Returns, Auctions, and Equipment Resales

When administrators think about the life cycle of computers and security, one stage they often overlook is the final stage: retirement. At the end of a computer’s lifetime, it gets redeployed elsewhere in the company, returned to the leasing company, given to charity for resale, or just disposed of in the dumpster. The same is true of electronic storage media, such as floppy disks, disk-on-devices, and backup tapes. What happens to the information that was once stored on these devices? Even you if format the disk drive of the computer or

most other types of rewritable media, the information is likely still stored on the disk. For example, the format command in Windows systems only marks the portions of the hard drive where the data is stored as writable; the file system does not track the information, but the actual data bits are still there and can be retrieved by directly reading the disk. If fact, there are several companies that perform physical data reconstruction in which they can recover data from even badly damaged removable media. As part of a targeted attack, an attacker could gain access to disposed media devices through dumpster diving or auctions, or he could obtain the sources to information haphazardly through purchasing used computers from leasing companies or charities. As a penetration tester, you might want to analyze the manner in which the following items are decommissioned:

- Computers
- Removable storage devices and specialized hardware
- Media
- Documentation

Computers

Many components of a computer, including Flash RAM, proprietary ROM modules, and hard disks, contain information that is stored persistently. These devices should be erased (and perhaps even destroyed) through a secure process. For example, the U.S. Department of Defense recommends a three-phase process for secure data cleansing from magnetic material not marked as top secret. First, zeros are written to each addressable area on the media serially, then ones are written serially, then random blocks of ones and zeros are written serially. Additionally, magnetic material that contains or once contained top-secret information must be physically destroyed after this process to ensure that attackers cannot retrieve confidential information.

Removable Storage Devices and Specialized Hardware

Careless employees might leave compact discs, floppy disks, tape backup devices, or other removable media in a drive when they dispose of a computer. Additionally, some organizations, such as military and defense contractors, might use specialized hardware that could be disposed of with computers, such as encryption modules. These items should be removed before disposal.

Media

All data and data artifacts on storage media should be removed before you dispose of the storage media, or the media should be physically destroyed beyond the point that data could be retrieved through physical examination. For example, if your organization disposes of large amounts of magnetic media, you

might want to consider investigating the requisition of a degaussing device and/or an industrial shredder.

Documentation

Printer ribbons can reveal what was printed on them. If your printers print confidential information, consider destroying these items before you dispose of the hardware. Granted these types of printers are no longer commonly used for most printing tasks, but they are still frequently used to write checks. Also ensure that you dispose of printed confidential information, such as manuals, memos, and copies of e-mail in a secure manner, for example, by crosscut shredding and incineration.

More Info For official United States government standards on the display of data sources, see “Section 8-306: Maintenance” in the United States Department of Defense’s National Industrial Security Program Operating Manual (NISPOM) at <http://www.dss.mil/isec/nispom.htm>.

Using Social Engineering

“You never know unless you ask.” How many times have you heard that expression? For penetration testing, social engineering is a highly effective way of getting access to information, and when executed with skill, it is very *very* difficult to prevent. Attackers use social engineering to exploit human behavior, particularly around trust. There is good news and bad news here. The good news is that if your organization’s employees are properly trained and stick with the established process, they will become the backbone of your organization’s security. The bad news is that people are not nearly as easy to configure as software. At its heart, social engineering depends on the attacker’s ability to convince someone to do something they ordinarily would not do, to somehow bend the rules for this one time. Four common techniques that attackers use to socially engineer people are:

- Bribery
- Assuming a position of authority
- Forgery
- Flattery

Frequently, attackers combine one or more of these techniques to achieve their desired results.

Bribery

Bribery is simple, painless, and efficient. In an organization, the individuals most susceptible to bribery have some degree of control over information assets and the least to lose, such as those working the help desk. The help desk employees can reset passwords on user accounts, which for all intents and purposes means that they could become any user on the network temporarily, probably without being caught. Help desk analysts are also frequently the lowest paid employees in the IT department. Additionally, because help desk services are often contracted out to third-party companies, the workers' loyalty to your organization is likely to be less than it would be if they were employees.

What if someone offered a help desk analyst \$4,000 for access to the network for 12 hours? What if they offered \$10,000? Quickly, this discussion can become very non-academic. After all, it is a victimless crime, right? No one is going to be physically hurt—somebody just wants to have a peek. This is how the attacker will make the sell. Furthermore, if the attacker is an employee or is close to the employees in your company, it might not be difficult for him to find someone in the company who is in need of money quickly or has scorn for the organization. Blackmail might also fit into the equation here. Both of these further reduce ethical barriers. The effective social engineer pushes all these buttons. Many of you reading this book would like to believe that you are immune to bribery, but just as many of you are either on the fence or wishing that you would be offered a bribe soon.

As a penetration tester, you are not likely to ever feel empowered to bribe people as part of a penetration test, because doing so would push ethical boundaries and certainly cause ill will between the organization and its employees if entrapment through bribery was revealed. You should carefully analyze situations in which employees have more responsibility and control over information assets than they are compensated for, especially when there are no effective means to audit their activities. The simplest solution to this problem, though not an inexpensive one, is to assign more than one person to carry out these activities, thus requiring all the individuals to collude to subvert the system. Rotating people through positions also makes it easier to detect and prevent situations in which a single person is solely responsible for carrying out activities with high-value assets and has no one overseeing his work.

Assuming a Position of Authority

Sometimes the easiest way to get information about a network or to break into a network is to ask. As strange as it sounds, employees have been known to reveal important information about their company—wittingly or unwittingly—to attackers who assume the position of authority. For the attacker, it is about asking the right

questions of the right person using the right tone. This exploitation of trust is what most people think of when they talk about social engineering. As with physical intrusion, the key to conducting this type of social engineering penetration testing is to know when to blend in and when to assume authority. When you are attempting to get someone to do something she ordinarily would not do, having the appearance of knowing more about the situation than your target is a powerful tool. People naturally defer to others who assert power, whether that power is suggested through information or commands.

The assumption of authority is all in the presentation. For example, a clever attacker could obtain a business card from a company she is targeting and easily make her own, granting herself the title Director of Security or Senior Attorney. Through remote surveillance of employees, she could gain enough visual detail of the company's ID badge to create a fake badge that looks very real. She could also scour the company website to learn who is in the company and what the important company initiatives are. Armed with this information, the attacker is now ready to walk in the front door and right into the office of an employee she has targeted. By researching posts the employee has made to newsgroups, she could start a conversation confidently: "Brad? Hi, I am Susan. I work for Ben Smith, our Chief Counsel. We were discussing your work on the new product line. He appointed me to take a quick look at the work product to check for any potential intellectual property issues like the ones that hit us last year. We certainly don't want to wind up in court again. Can you have copies of the core plans made for me? I am still waiting for the IT guys to get my account and e-mail straightened out. Can you believe it? They managed to spell my name wrong."

An incident along these lines grabbed headlines in July 2002. A student at the University of Delaware was caught changing her grades in the school's database system by calling the university's human resources department and pretending to be her professors. In two cases, she reportedly stated that she had forgotten her password and asked to have it reset, and in all cases, the HR department obliged even though, according to police records, the HR worker told police the voice on the phone sounded "young, high-pitched, and desperate." In another case, she was able to guess the professor's password. She was then able to log on to the university's network as the professor and alter her grades.

If you've ever seen a good psychic, you can appreciate how easy it is for a skilled imposter to field any questions related to a particular subject, but at the same time stay generic enough to always be correct, or at least have a way out. It is not inconceivable that the attacker in our scenario could walk right out the door with the company's top-secret plans for the next product line in a matter of minutes.

Forgery

Another for avenue for social engineering that does not take on such an interpersonal dimension is forgery. The form factor for the forgery could be anything from a well-placed letter to an elaborately spoofed e-mail and website. For forgeries to be effective, they need to look real and present some compelling reason for the target to act, while at the same time not arouse too much suspicion.

Sean Michael Breen provides very good example of a temporarily effective forgery campaign. In February 2004, Breen (aka “Razor 1911”) was sentenced to 50 months in prison and fined nearly \$700,000 for his role masterminding an Internet-based piracy ring that sold cracked video games before the authentic versions hit store shelves. To obtain advance copies of the games, Breen and his associates sent letters to video game design studios claiming to be reviewers for a video game magazine that in actuality did not exist. Nevertheless, these game studios sent Breen some of the most popular PC games, such as Warcraft III, Quake, and Terminal Velocity, well before they were released. To run the infrastructure for his Internet website in which the illegal games could be purchased and finance his operation, Breen acquired several hundred thousands of dollars in equipment from Cisco Systems by posing as an existing customer and having the equipment sent to a rented storefront on the other side of the country. In this example, any number of simple checks from the game studios or Cisco could have prevented Breen from carrying out his attacks, but because he blended in so well with normal business, his scam went unnoticed.

Other, more common types of forgery include forged e-mails to individuals asking them to verify their passwords or to download software updates. Microsoft customers are often targeted by spyware vendors and attackers attempting to install rootkits. They send near-perfect forgeries of Microsoft-branded communications to users, telling them to deploy the latest security update by clicking a link in the message or running the executable file attached to the message. In these messages, all the links, except the exploit, which is linked to an IP address, are actual live links to Microsoft’s website. Many of these forgeries are very convincing and compelling. Only careful evaluation of the spoofed SMTP headers and source of the HTML mail, both of which are hidden by default in most e-mail programs, will reveal that the e-mail is an attempt at social engineering. Similar types of attacks often target credit card numbers and website passwords.

Flattery

In any type of relationship building, personal or professional, flattery is a powerful tool. Everybody knows at least one “gusher”—the person who, smiling brightly, lavishly thanks people for even the lamest gifts. To the disinterested

outside observer, this display can be at times nauseating, but to the recipient, nothing could make the day more. After all, the giver spent a lot of time choosing this gift, and now he walks away with a tremendous sense of pride. Flattery is also a very powerful tool to manipulate and distract people. Attackers skilled at social engineering nearly always employ this tactic.

For example, an attacker might find the telephone number for the company switchboard operator and ask to be transferred to the help desk, posing as a newly hired employee. Because the call is transferred rather than directly dialed, the call identification will appear to the help desk as though it originated internally. This simple action immediately enables the attacker to gain a level of trust from the help desk that he would not normally have. The attacker might then explain that he is a new employee and is very afraid of computers. The attacker might continue by saying he is not sure what his account name is and how long his password needs to be and that his manager is out for the day. He goes on to say how stupid he is, because his manager explained how account names were created at the company and how important it was that he stick to company rules regarding passwords, but in all the excitement of the new job and the monotony of paperwork at employee orientation, he forgot. After the help desk administrator patiently explains how account names are generated and the organization's password policy, the attacker might explain—while going out of his way to compliment the help desk administrator on how smart she is and how well she explained the account and password problem—that his boss told him his account was enabled for remote access but that he lost the information about which server to connect to.

By the end of the conversation, the attacker will have a good idea of how hard it might be to break into the network by logging on with a valid user's credentials. The attacker can use the names of employees he has gathered from the website and information learned from the help desk about the password policy to attempt to log on to the remote access server by using passwords that users are likely to pick. Meanwhile, the help desk administrator ends the conversation feeling as though she did a great job in assisting a user who really needed help.

Social engineering is difficult for networks to defend against, especially when network administrators and other employees in key positions (such as administrative assistants) do not know that they might be the targets of such attacks. Consequently, security awareness training is essential for everyone in the company. The single most effective defense is sticking to process when asked to skip steps or do things not normally done, and then reporting these abnormal incidents.

Frequently Asked Questions

- Q.** I am a good penetration tester with computers. Will I be good at physical penetration testing or social engineering?
- A.** Maybe. But just as you have developed skills and learned from your experience to become a better penetration tester on computers and networks, you will need to develop the skills required for physical penetration testing or social engineering. In the end, each type of penetration testing requires certain personality traits and talents that not everyone has.
- Q.** This sounds like spy stuff from a Tom Clancy novel. I don't believe you.
- A.** OK. But there are tons of examples where no believed until it happened to them. (Just think about some of the examples in this chapter.) The bottom line is that like other aspects of security, you must assess the attacks discussed in this chapter in the context of the security threats your organization faces. A small real estate company and a global biotechnology company have completely different threat profiles.
- Q.** Do physical penetration testing and social engineering testing require more care in planning?
- A.** To some degree, yes. Because you are dealing with people, not computer systems, you might need to review federal and state employment laws and employee conduct agreements before engaging in the types of assessments in this chapter.

