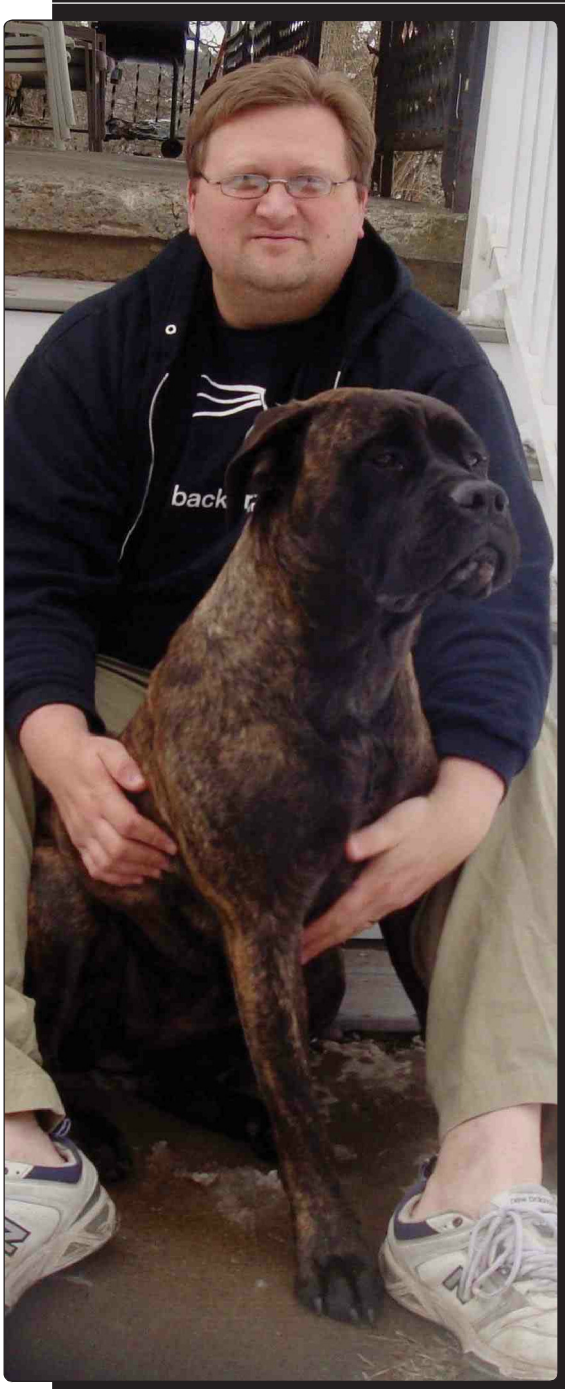


Asked whether his book might serve as a primer for people looking to learn how to break into networks, Hadnagy says, "I don't think the bad guys are shopping Amazon looking for a 'How to be a criminal' section. What this book does do is alert people to the way that criminals work, so that they can be aware and protected."

Is This The Most Dangerous Man In America?

Security Specialist Breaches Networks For Fun & Profit

Chris Hadnagy doesn't look like a criminal mastermind. More like a big, friendly teddy bear, actually. Maybe a bit like a slightly rumpled Chris Farley. Hardly intimidating. He certainly doesn't seem like the type who could take down just about any network he encounters, thereby bringing a company to its knees. But he can. And he does. Hadnagy, a security specialist and author of "Social Engineering: The Art of Human Hacking," has probably broken into more networks than you've ever logged on to, and he gets paid for it.

Hadnagy is a pentester, or penetration tester: a white-hat social engineer who breaks into corporate networks just to see if it can be done. (The answer, by the way, is yes, it almost always can.) He's very good at it, possibly among the best. We all know that social engineering is the art of getting people to part with seemingly innocuous information that can then be used against them, but few of us have had a chance to talk to a bona fide practitioner of this dark art about exactly how an SE exploit goes down. We did, and it was an eye-opening experience.

Information Gathering

Napoleon once said that war is 90% information, and a successful SE breach begins with gathering information. Lots of it. Much of it is useless, of course, but buried in all the garbage will be the one shining nugget that gives the social engineer the leverage needed to crack open your network.

If someone wishes to harm or take advantage of you, the more he knows about you the better. Do you collect stamps? A social engineer wants to know that. Do you read e-books? What kind of car do you drive? Where do you get your hair cut? Your clothes cleaned? When's the last time you went to an ice cream parlor? What

flavor did you get when you were there? A skilled SE can use these seemingly innocuous details against you.

"Your SE exploit is only as good as your info," says Hadnagy. "There is no such thing as irrelevant information, and the better your info, the more likely your success."

Hadnagy recounted for us a story he tells in his book: A friend of his was tasked with breaking into a corporate network. Searching the Internet, the SE stumbled across an executive who'd used his corporate email on a stamp-collecting forum. He registered a likely-sounding URL, found a photo of a bunch of old stamps, and created a dummy Web site to show off the stamps. Then he emailed the exec, offering to send him a link to a collection that his "grandfather had left him" that he was interested in selling. The executive accepted and, when the email arrived, clicked the link, which took him to a page with an embedded malicious frame that exploited a vulnerability in Internet Explorer. Once there, the target's computer was compromised. The SE now owned this man, his machine, and—through the machine—the company's network. All because he discovered that the man collected stamps.

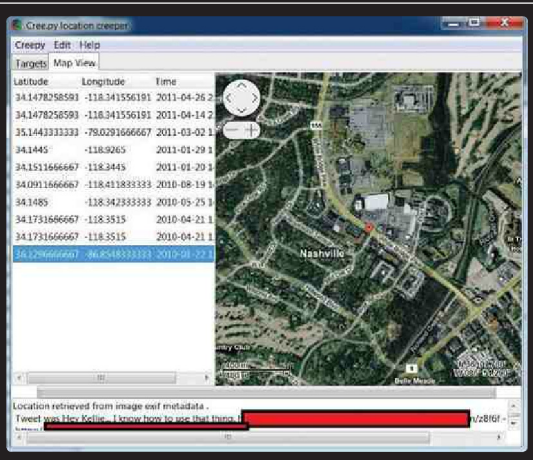
It used to be difficult to collect or elicit information about someone you intended to scam. Not anymore. These days, our information is plastered all over the Internet, and to a social engineer all of that information is valuable.

In fact, there's now so much information available that an SE's biggest task is not finding data, but organizing and sifting through the information he's acquired. For that reason, there are tools aimed solely at helping a social engineer make sense of the data he's collected during this phase.

"Social media is a social engineer's best friend," says Hadnagy. "People put their lives on the Web for anyone to browse. In one pen-test, we were tasked with obtaining information from a business professional by any means, even if that meant involving family members or friends. We quickly created a Facebook profile that matched the daughter of the target; within a day or two we were friended and chatting. Those chats revealed a lot of information that could have been used in a malicious attack to compromise the company." That's pretty creepy.

And speaking of creepy, consider Cree.py. Written by Yiannis Kakavas as an educational tool, Cree.py (the "py" is a Python suffix, of course) scours Twitter accounts, looking for photos that include geo-location data. From that data, Cree.py maps the poster's location. Over time, Cree.py knows where you are (and where you are not), where you've been, and where you spend your time. ("Oh, look. She runs a specific route in this particular park three days a week, always beginning at 6:40 a.m.")

Creepy indeed.



According to Cree.py, a certain female television talk show host spends much of her time at the network studios in Burbank, Calif., but also often visits a private home in that area. She divides much of her time between Southern California and North Carolina, with occasional visits to Nashville.

The Pretext

A good social engineer is a good actor, and that skill stands him in good stead during the pretext, the portion of the exploit during which he pretends to be something or someone he is not, in order to gain access to a building or to information so that he can play out the scam he has in mind.

"Good acting," says Hadnagy, "is a skill that can really help a social engineer. Being able to elicit emotion is easier if your acting skills are strong. And taking an acting class or watching a good DVD can help you to practice some skills that will make you better at it."

The SE's pretext can involve pretending to be almost anything: an office equipment salesperson, a tech support rep, or a building maintenance person, for example. In any of those cases, the person would have a legitimate reason to be in the building, and perhaps even a good reason to be wandering around the building unaccompanied. All he has to do is convince whoever's at the front desk that he's there to, oh, "reset the calibration on the copier/printer." Whatever that means. Let's face it: If a likely-looking man or woman walked in with a toolbox and a well-made ID badge claiming to have been asked by your currently vacationing CEO (whose name and travel plans he seems to know fairly well) to come by and service a piece of equipment, how many people would see through that ruse? Not many.

The Breach

And the reason they would not see through such a ruse is that people are . . . well, nice. They like to be helpful, to do the right thing. To aid someone who needs their help. And they're trusting, to boot.

"People have an inherent desire to help others," says Hadnagy, "and they trust what people say without asking. Because most people do not have a healthy level of paranoia or distrust, it makes it very easy to manipulate most people into taking actions not in their best interests."

In a sense, then, it's people's very best qualities that work against them. That's a little disheartening, says Hadnagy, but he hates to think that people would become unhelpful or completely distrusting as a result.

"I don't think the solution is to become distrusting or less helpful. Instead, I think the solution is to become more self-aware. That lost 75-year-old grandma in the parking

lot may very well not be malicious, but the new charity that popped up to support Japan could be." The only sensible option, says Hadnagy, is to be aware of potential threats and to learn not to automatically believe everything you're told.

In the case of that "copier repair tech," by the time he's gained access to your building, it's too late. There are a dozen ways he could get to your network, partly depending on how much time he has and on how closely he feels he's being observed.

USB

One of the easiest gambits is a USB drop. All the "salesman" has to do is prep a few thumb drives with a poisoned PDF or autorun app, for example, and then leave some drives lying about: one in the restroom, one in the break room, maybe one near the copier. If you have 25 people in your building, odds are that someone will find a thumb drive and insert it into a machine, "just to check it out," perhaps even in a well-intentioned attempt to return it to its rightful owner. The "helpful" staffer just helped the "salesman" breach your network.

Some penetrations require no physical presence at all; SEs like them because they require less work and present less risk than walking into a target building under a pretext. For example, say a malicious social engineer pretends to be a sales rep for an office equipment vendor. In a "sales" call to a target company, he determines that the company uses Adobe Reader 8. Armed with that information (and knowing of a security hole in that version of Adobe Reader), he closes the call by requesting an email address and saying that he'll send a bid in PDF format for their approval. A day later a document called Yourbid.pdf arrives. But it's not a real PDF. Instead, it's a maliciously encoded document that gives the social engineer a reverse shell on the target's computer, thus allowing outside access to the machine. The network is compromised, all because someone told the SE what version of Adobe Reader the company used.

Keep in mind that making (well, stealing) money may not be the purpose of an SE hack, and it may not be some kind of industrial espionage—although both of those motives are fairly common. Sometimes the goal is simple meanness.

"Last year at DEFCON, a hacker group hacked a security person and released all of his personal emails, ones that showed he was cheating on his girlfriend or wife," says Hadnagy. "There's no point in that but to ruin someone."

How Big Of A Problem?

So, perhaps you're thinking, "OK, but surely people are too smart to fall for this sort of thing in large numbers." Think again.

A 2007 government-sponsored study showed that 60% of IRS employees fell for a social engineering hack in which they were called by a "fellow employee" and asked to change their passwords. And this was after similar tests had been run earlier and the employees warned about the ploy. A University of Idaho study found that 40% of the school's employees provided their passwords to someone claiming to be a fellow employee over the telephone, while phishing experiments that sent targeted emails to specific recipients showed success rates between 45% and 80%.

But that's nothing. At a recent DEFCON, teams of SEs using nothing more high-tech than a telephone called companies and got them to give up such "harmless" information as who handles their dumpster removal, delivers their cafeteria food, and shreds their paper waste. Companies told callers what antivirus applications they have installed, what browsers and PDF software they use, and more. That's exactly the sort of information a social engineer can use to penetrate a company's network. The SE teams' success rate was a startling 100%.

Plugging The Leak

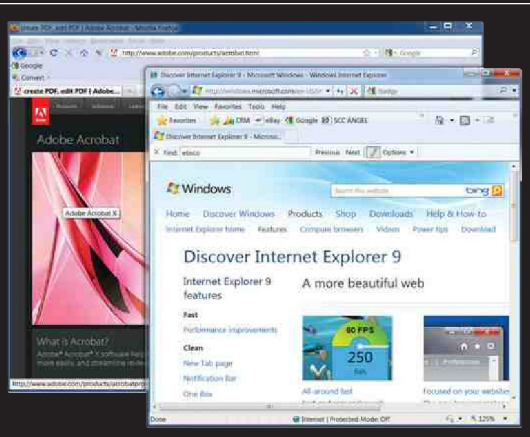
There's no way you can completely protect your (or your company's) network from social engineering hacks, but the first step, says Hadnagy, is limiting the amount of information that's floating around out there.

"Every step can be made harder for the SE by you being smarter," he says. "Information release is inevitable in this day and age, but how much is too much? Do you have to tweet your geo-location every 15 minutes? Do we really need pics of you and your family? Do we need your whole life story on the Web? Making it harder for the SE to gather useful information is the first step."

The second thing to do is to train the people who use the network, making them aware of the threat. When a stranger asks a question of you, says Hadnagy, stop and think: "Does the person asking deserve this information? Why is he asking for it? And what are the possible repercussions of giving it up?"

In reality, you don't need to make your network 100% safe—not that you could do that if you tried. Like putting good locks on the door or owning a dog, your goal is not to crime-proof your home; your goal is to make the bad guy look for an easier mark. ■

BY ROD SCHER



It may seem unimportant, but knowing the Web browser or the version of Acrobat Reader a company uses can provide a social engineer with exactly what he needs to breach the organization's network.