FEATURE

UNITED STATES

Social Engineering: Anatomy of a Hack

As the founder of Lares, a Colorado-based security consultancy, social-engineering expert Chris Nickerson is often asked by clients to conduct penetration testing of their on-sight security. Nickerson leads a team which conducts security risk assessments in a method he refers to as Red Team Testing. Watch Nickerson and his team pull off a $24,000 heist in this video.

By Joan Goodchild

Content Director, CSO

FEB 4, 2009 7:00 AM PST

As the founder of Lares, a Colorado-based security consultancy, social-engineering expert Chris Nickerson is often asked by clients to conduct penetration testing of their on-sight security. Nickerson leads a team which conducts security risk assessments in a method he refers to as Red Team Testing. Watch Nickerson and his team pull off a $24,000 heist in this video.

Nickerson and crew recently took on such an exercise for a client he describes as "a retail company with a large call center." With some prep work, Nickerson says the team was able gain access to the company's network and database quite easily. Read on to find out how they did it, and what lessons you can take away for shoring up your organization's defenses.

Subscribe

Chris Nickerson: On-site security vulnerability testing requires the most memory and intelligence gathering because you need to start off by gaining information on your target. When I'm doing my information gathering, I like to find holiday or time-relative events. In this particular exercise, there was a large horserace going on in the area. In the town where the company was located, it was the big thing to go to this horse race. Everyone in the city and around it geared up and left the office to go to it. That was a perfect time for me to come in and say I have an appointment.

[Beware the 9 warning signs of bad IT architecture and see why these 10 old-school IT principles still rule. | Sign up for CIO newsletters.]

I said I had to meet with someone we'll call Nancy. I knew Nancy wasn't going to be in the office because on her MySpace profile it said she was getting ready to go to the race. Then her Twitter profile said she was getting dressed to go to the event. So I knew she wasn't in the office.

UNITED STATES

Before I went to the office, I went to a thrift shop and got a Cisco shirt for $4. Then I went in and said "Hi. I'm the new rep from Cisco. I'm here to see Nancy." The front desk attendant in this situation said "She's not at her desk."

I said "Yeah. I know. I've been texting back and forth with her. She told me she is in a meeting and the meeting is going over."

Subscribe

This was right around lunch time and I said "Since I'm waiting, is there anywhere around here where I can go get some food?" I knew full well that after surveying the area the closest thing was about five miles away because they were sort of out in the sticks.

BrandPost Sponsored by HPE

The CIO's Guide to 'IT as a service'

The receptionist said "Four or fives miles down the road there is a McDonalds. But we have a nice cafeteria here. If you want, you can just eat in there."

SponsoredPost Sponsored by Velocity

How To Build A Business Case That Actually Works

Being allowed to go to the cafeteria gave me full access to the facility because the only thing that was guarded was the door. The cafeteria lead right into the rest of the building.

So I went into the cafeteria and ate. While I was there, I did USB key drops. I put files on them with names like 'Payroll' or 'Strategy 2009.' The USBs had rootkits on them. Many contained an autorun rootkit. Others had Hacksaw, which is a little piece of tech that you can use with a U3 drive. You plug it into a machine and, if the machine has auto run on the CD-Rom running it, it will just start dumping all the passwords, usernames, all that. It will also put a hook into the machine to start emailing that information out to an email account that you give it to contact. So, even after I left, I could still be filtering information. It only takes about 30 seconds to enable itself.

Subscribe

When I do this kind of exercise, I put USBs in areas that people are in where they might forget something: The bathroom, for instance, on the sink. Another good area is near the coffee machine. Areas where people naturally put things down where they might not remember to pick it back up. I've never done USB key drops without success.

Meanwhile, I had another one of my guys go in through the smoking door in the back. He hung out, waited, had some cigarettes with people who came out to smoke on break, and when they were done, the door opened and he just cruised in. Yet another exercise to prove it really doesn't take much to get inside.

SponsoredPost Sponsored by Vertex Inc
Critical Tax Technologies For Today

VERTEX®

Eventually, once he was in, I had him come and get me in the cafeteria. That was so it appeared on

UNITED STATES

the security tapes as though someone was coming to get me out of the cafeteria to escort me to whatever meeting I was going to attend. We went through and found inside of this giant 100,000-square-foot cube farm a few seats that were wide open and just sat down.

There was no one around us. So, we started pulling keys. We used things like Ophcrack to start cracking Windows passwords and dump them into Linux. We started putting our machines on the networks so we could start doing pen testing and hacking active servers in the environment. We put up things like WRT 54G routers: the little blue Linksys wireless units. We took those, stuck them under a cube, put Unix on them and opened WRT. That made it so I had a wireless access point I could hit not only from the parking lot, but it also beacons and calls home so I had a Unix box that sits inside their network.

A short time later, a full team of people came in. A lot of the work that was done at this facility was shift work, and it was shift change time. Because we did our homework right, we were at the two of three cubes that were vacant so there were no conflicts or questions.

Everyone sat down around us. I announced myself as the Cisco engineer who was working on the phone system. Many of them responded with jokes and said things like "Honey, please don't fix it. I don't want to take any calls today."

Subscribe

One thing I have learned is that cookies are the keys to everyone's heart. When I'm doing the type of exercise where I'm posing as a tech, or a VAR, I like to bring cookies. I did for this exercise and I started passing out cookies to everyone in the area. We were all laughing, having a great time. Meanwhile, we were in the middle of hacking their entire network.

In the end, what we exposed for the client was the vulnerability of their physical access and we showed them some of the blended techniques we used to get in. We were able to demonstrate how, with social engineering, we were able to hack the SQL Server and dump the whole data base of everybody's account information. This kind of breach could have cost them multiple billions of dollars. And we had access to all of it because of these vulnerabilities. We wore button cams and hat cams so they could watch how it was done.

Companies need to run campaign. You need to tell employees what to look for and how to look for it. Companies need to teach employees that it's not that the company doesn't trust the people within the organization, it's that there are people out there trying to do this every day. It is just a good awareness technique to do it.

UNITED STATES

If someone is coming to work on your environment, you should probably know who they are. If you think of your company like your home, you do things differently. You are not going to just let someone walk into your house. That is the kind of philosophy companies need to inject into corporate culture.

This story, "Social Engineering: Anatomy of a Hack" was originally published by CSO.

Next read this:

- *Top 9 challenges IT leaders will face in 2020*
- *Top 5 strategic priorities for CIOs in 2020*
- *7 'crackpot' technologies that might transform IT*
- *8 technologies that will disrupt business in 2020*
- *7 questions CIOs should ask before taking a new job*
- *7 ways to position IT for success in 2020*
- *The 9 new rules of IT leadership*
- *20 ways to kill your IT career (without knowing it)*
- *IT manager's survival guide: 11 ways to thrive in the years ahead*
- *CIO resumes: 6 best practices and 4 strong examples*
- *4 KPIs IT should ditch (and what to measure instead)*

Subscribe

Joan Goodchild is a content director with IDG's marketing services division. She is the former editor in chief of CSO and a veteran editor, writer and content strategist with 20+ years experience. She has a Master's degree from Northwestern University's Medill School of Journalism and received an Edward R. Murrow award for investigative journalism.

Follow

Copyright © 2009 IDG Communications, Inc.

Containers and Kubernetes: 3 transformational success stories

SPONSORED STORIES

UNITED STATES

Plastic Surgeon Tells: “Doing This Every Morning Can Snap Back Sagging
Beverly Hills MD

Why Do People Invest In Gutter Protection? Here is The Truth
leaffilterguards.com

“The #1 Retirement Stock in America”
Empire Financial Research

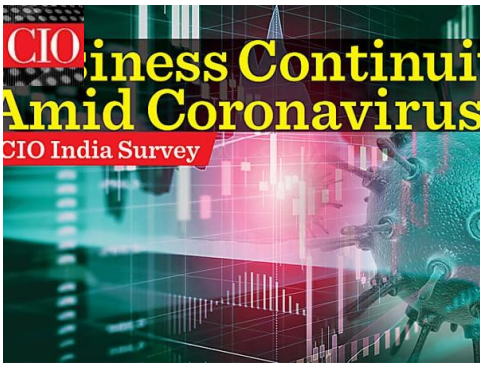
The New 2020 Jeep Wrangler: Take a Sneak Peek
Edmunds

Urologist: Try This If You Have Enlarged Prostate (Watch)
healthbenefits.vip

4 Rules for Defending Your Portfolio Against a Bear Market
Fisher Investments

Subscribe

10 ways you’re getting workplace diversity wrong
CIO



69% of CIOs believe COVID-19 will significantly
CIO

Why Wi-Fi 6 is an essential driver of digital
CIO

UNITED STATES

Photos Of Lucille Ball That Show A Different Side To The Original Queen Of
Collider

1 Clever Trick Every Computer Owner In The U.S Should Do Today
Security Savers Online

SPONSORED LINKS

Transform Your Data Center with Seamless Visibility

Accelerate Digital Transformation With Visibility Without Borders

See What Others Can't. Take control And Solve Problems Faster With NETSCOUT

Your cloud, your way: Why Cloud Verified matters

dtSearch® instantly searches terabytes of files, emails, databases, web data. See site for hundreds of reviews; enterprise & developer evaluations

Subscribe

IDG COMMUNICATIONS Copyright © 2020 IDG Communications, Inc.