Slashdot News for nerds, stuff that matters

News: DefCon Contest Rattles FBI's Nerves **Comments: 136**

Posted by Soulskill on Friday July 30, @07:34PM
from the par-for-the-course dept.
snydeq writes

> *"A DefCon contest that invites contestants to trick employees at 30 US corporations into revealing not-so-sensitive data has rattled nerves at the FBI. Chris Hadnagy, who is organizing the contest, also noted concerns from the financial industry, which fears hackers will target personal information. The contest will run for three days, with participants attempting to unearth data from an undisclosed list of about 30 US companies. The contest will take place in a room in the Riviera hotel in Las Vegas furnished with a soundproof booth and a speaker, so an audience can hear the contestants call companies and try to weasel out what data they can get from unwitting employees."*

The group organizing the contest has established a strict set of rules to ensure participants don't violate any laws. **Update: 07/31 04:45 GMT** by S : PCWorld has coverage of one of the day's more successful attacks.

Submission: Defcon Contest Rattles FBI's Nerves by snydeq (1272828)
DefCon Contest Rattles FBI's Nerves

Dumbasses @ FBI (Score:4, Interesting)

by blackraven14250 (902843) on Friday July 30, @07:37PM (#33091232)

What dumbasses at the FBI and in the financial industry:

"The list of target organizations will not include any financial, government, educational, or health care organizations;"

Re:Dumbasses @ FBI (Score:5, Funny)

by msauve (701917) on Friday July 30, @07:42PM (#33091278)
Well, that leaves retail.

"Do you have Prince Albert in a can?"

Re: (Score:2)

by HungryHobo (1314109)

If you make any false claims at all then it would probably come under wire fraud.

A straightforward "Please tell me your password" probably isn't illegal (IANAL though)

Keep in mind though that false claims would probably include *implied* things as well so even if you speak no word which is not the truth you may still be trying to mislead someone and there's probably laws covering that.

Re: (Score:2)

by digitalunity (19107)

The definitions of unauthorized access to a computer system vary quite a lot by state, but rest assured, all 50 states have their own laws against accessing a computer system against the owners wishes.

Even if you finagled router logins from a company(*), the courts could find such information does not constitute authorization to use the login to access private data on the network.

*This of course being wildly unlikely, since even if they're open to clients outside the LAN, the only people who would have the

Now - I'm in the IS department, so it may be that those in lending ops, etc have a different story. For us the "measures" in place rely solely on the common sense of each employee.

Scary, isn't it?

Re: (Score:2)

by clarkkent09 (1104833)
The publicity hardly helps. I wonder if any of the organizations called will know what's going on and use the opportunity to mess with the contestants.

Re: (Score:3, Insightful)

by tuomoks (246421)

Unfortunately - yes! Hide the head in the sand, that seems to be the answer nowadays for any- and everything? For a long time, excuse me - started in 60's, I was either responsible of or designing systems and infrastructures for safe and secure, often global environments - can't say that they were perfect, nothing ever is. Time to time (often) the hired security testing groups / companies were able to find some problems, even if documents in wastebaskets - in IT(?) which should have known better, but the ma

This is refreshing (Score:5, Insightful)

by Majik Sheff (930627) on Friday July 30, @07:44PM (#33091300) Journal

It's nice to see the hacker community making a move to acknowledge its roots. Social engineering is the oldest and easily the most challenging/rewarding form of real hacking.

What's more gratifying, beating the password out of a hash after weeks of brute force or having the mark just tell you in a five-minute phone call?

Re: (Score:3, Funny)

by al0ha (1262684)
Yeah - social engineering used to be called grifting. But I guess grifting is not as cool a buzzword as anything associated with engineering. Social engineering, puhleez; like it takes a lot of brains to grift a rube.

Re: (Score:2)

by Majik Sheff (930627)

You forgot to tell me to get off your lawn, old timer. :P

Re:This is refreshing (Score:5, Funny)

by Hatta (162192) on Friday July 30, @08:10PM (#33091540) Journal

I prefer to beat the password out of the mark after 5 minutes of brute force.

Re: (Score:3, Informative)

by KlaymenDK (713149)

http://xkcd.com/538/ [xkcd.com]

That is all.

Re: (Score:2)

by Majik Sheff (930627)

Ah yes, rubber hose decryption. Effective but not for the faint of heart.

Re: (Score:2)

Very close, actually.

Rules and Do-Not-Do list (Score:5, Informative)

by Zerth (26112) on Friday July 30, @07:52PM (#33091374) Homepage

The CTF Rules

Each Social Engineer is sent via email a dossier with the name and URL of their target company chosen from the pool of submitted names.

Pre-Defcon you are allowed to gather any type of information you can glean from the WWW, their websites, Google searches and by using other passive information gathering techniques. You are prohibited from calling, emailing or contacting the company in any way before the Defcon event. We will be monitoring this and points will be deducted for "cheating".

The goal is to gather points for the information obtained and plan a realistic and appropriate attack vector. The point system will be revealed during the Defcon event. All information should be stored in a professional looking report. 1 week prior to Defcon you will submit your dossiers for review to the judging panel.

They will be sent their time slot (day/time) to perform their attack vector at Defcon. At Defcon each social engineer will be given 5 minutes to explain to the crowd what they did and what their attack vector is.

They are then given 20 minutes to perform their attack vector and points are awarded for information gathered as well as goals successfully accomplished during the process.
A scoreboard will be kept and at the end some excellent prizes will be awarded.

The Flag

The "flag" is custom list of specific bits of information, which you will have to discover during your 20-minute phone call.The judging panel created the list, and points will be awarded for each item present on the list. This list will be presented to you on the day of the event

THE DO NOT LIST:

Underlying idea of this contest is: No one gets victimized in the duration of this contest. Social Engineering skills can be demonstrated without engaging in unethical activities. The contest focuses on the skills of the contestant, not who does the most damage.

Items that are not allowed to be targeted at any point of the contest:

1) No going after very confidential data. (i.e. SS#, Credit Card Numbers, etc). No Illegal Data
2) Nothing that can get Social-Engineer.org, Defcon, or the participants in the contest sued
3) No porn
4) At no point are any techniques allowed to be used that would make a target feel as if they are "at risk" in any manner. (ie. "We have reason to believe that your account has been compromised.")
5) No targeting information such as passwords.
6) No pretexts that would appear to be any manner of government agency, law enforcement, or legally liable entity.
7) The social engineer must only call the target company, not relatives or family of any employee
8) Use common sense, if something seems unethical - don't do it. If you have questions, ask a judge
If at any point in the contest it appears that contestants are targeting anything on the "No" list, they will receive one warning. After the one warning they are disqualified from the contest.

Re: (Score:3, Insightful)

by Score Whore (32328)

If they aren't going after confidential data, then what exactly is the point here? What I mean is, why would a company care about non-sensitive data, so what protections/security/whatever are they supposedly penetrating here?

Re:Rules and Do-Not-Do list (Score:5, Insightful)

by rotide (1015173) on Friday July 30, @08:14PM (#33091572)

Not everything needs to be about obtaining damaging information. Imagine talking to a random stranger and trying to solicit information from them. It's not as easy as it sounds.

Seriously, try this some time, just go up to a stranger and get their middle name. It will be harder than you think in most cases, if not impossible.

There are very cool pranks done at HOPE, which was enlightening. Emmanuel Goldstein called to BP and ended up convincing an employee to leave open the office door, and telling him that because it was too late he wouldn't be appearing with the company van. He didn't get any confidential information regarding to the store (surprisingly, some of the employees seemed to be trained and others seemed to be very stupid to understand the questions) but if wanted he could have gone to the gas station with a free pass to the office, from an unmarked unbranded van. That is social engineering.

what if that info just comes out? like the other s (Score:2)

by Joe The Dragon (967727)

what if that info just comes out? like the other side just start saying it all or some act's like a VP that need help and some one just gives them way to much info?

Re: (Score:2)

by Snowmit (704081)

Wait back up to the part where the organisers can detect wrongdoing before the contest starts because "we will be monitoring this." How?

Re: (Score:2)

by HungryHobo (1314109)

Doesn't this cover everything?
I've heard it said many times that you can be sued for anything.

"Nothing that can get Social-Engineer.org, Defcon, or the participants in the contest sued"

The companies could sue for their feelings being hurt, they could sue for damage to their reputation, they could sue for the wasted time of their employee, they could sue the organizer for being ugly, they could sue for the sky being blue.

Now weather they'd win for some of those things is a different matter.

Not-so-sensitive?! (Score:4, Funny)

by zyxwvutsr (542520) on Friday July 30, @08:03PM (#33091468) Homepage

> What participants can do is collect data on less sensitive subjects such as, "who does your dumpster removal; who takes care of your paper shredding," Hadnagy said.

"If you don't tell me, I'll look at the dumpster behind your building and read the name on it!"

I feel sorry (Score:5, Insightful)

by blantonl (784786) on Friday July 30, @08:04PM (#33091484) Homepage

I feel sorry for the poor fish in the barrel that gets shot on this one.

Unwittingly, right now, some guy/gal is sitting in their cubical and is on the cusp of getting the phone call that thrusts them into the international spotlight when the tape of the winning team's efforts is played. They might even lose their job for doing nothing more than, well, doing their job, or answering a harmless set of questions.

Re: (Score:3, Interesting)

by T Murphy (1054674)
If their boss actually follows what happens at DefCon, that boss might be smart enough to know how to handle the situation without firing anybody.

No, this is good (Score:4, Insightful)

by i_want_you_to_throw_ (559379) on Friday July 30, @08:26PM (#33091672) Homepage Journal
If anything social engineering is THE weakest link in the security chain. Let the geeks handle the hardware

ahem... (Score:3, Insightful)

by Anachragnome (1008495) on Friday July 30, @09:15PM (#33091982)

"The group organizing the contest has established a strict set of rules to ensure participants don't violate any laws. "

I think what REALLY scares these guys (the Feds and the Banks) is that they know damn well that MOST hackers out there do not limit themselves with any silly, self-imposed rules.

Just imagine what the contestants could do without legality/illegality issues hindering them. Anything learned here will simply be repeated, by someone, with no such hindrances in place.

Can they spoof CallerID? (Score:4, Interesting)

by HockeyPuck (141947) on Friday July 30, @09:16PM (#33091992)

On my desk phone at work, if someone calls from their desk or a number that is currently listed in the directory, their name and number shows up on the display. It's pretty obvious if someone calls up from an outside line. Now if the contestant is allowed to try to spoof my company's phone system into thinking they are from say, HR, more power to them..

Re: (Score:3, Informative)

by radish (98371)

The usual approach is to call someone pretty much at random, and ask to be transferred to the real target. That person then sees an internal number (typically of someone they don't know) calling them and to some degree lets their guard down.

Re: (Score:3, Informative)

by JWSmythe (446288)

Usually it's not that tough to get info. I always maintained an East coast US phone number, regardless of where I was working. I was always doing work things from my cell phone, like dealing with datacenter folks.

Sometimes in the course of normal work, I'd need to acquire access for a coworker to a site. My name was usually listed as a person authorized to make account changes. If it wasn't, I knew the people who would be. A few times, I called as the owner of the company,

Is this what the cyberczar wants? (Score:3, Insightful)

by Nyder (754090) on Friday July 30, @09:43PM (#33092142) Homepage Journal

Just the other day we had a submission about how we aren't prepared for the "cyberwarz" because we can't get people who knows this sort of stuff, or thinks along these lines.

Well, damn, seems to me this would be a great excerise for the fbi/ hls, and whoever else to see about hiring/training peeps for those sort of jobs.

Of course, that makes sense and wouldn't be used.

Re: (Score:2)

by rotide (1015173)

Careful, that creaking sound that comes from your chair isn't actually a creak.. The gubment put a listening device in it and sometimes you hear feedback from their end. In fact, that's how you can tell it's a new version of the bug. They can whisper suggestive things to you as a form of mild brainwashing. I mean, really, your libido isn't that great, they're just failing to get you to go to the kiddie porn sites. Sadly they only keep catching you viewing the granny porn.

Shhhh!

Re:If they go to my bank... (Score:4, Insightful)

by John Hasler (414242) on Friday July 30, @08:25PM (#33091668)

> They probably won't have to do much. They've sent a letter stating that my personal