

Miracle on Thirty-Hack Street

Merry Christmas, challenge fans! As you know, my friends and I write several challenges per year for EthicalHacker.net. But, we've made it a bit of a tradition around here of reserving the December challenge slot for me, an honor which I sincerely appreciate. During past holiday seasons, you got to tangle with the Grinch, Rudolph, that Messy Marvin kid, Frosty, and even Santa himself.

This year, Kevin Johnson and I worked together on a challenge in which you'll get to save Santa Claus from the insane asylum! We call it "Miracle on Thirty-Hack Street", after the classic 1947 movie. In this tale, you'll get to analyze some Facebook accounts to see if you can draw out the secrets needed to decrypt a file. Remember, we'll award an autographed copy of my Counter Hack Reloaded book to three winners: the best technical answer, the best creative answer that is technically correct, and a random draw winner from anyone who happens to send in, well, pretty much anything in association with the challenge. Even if you can't answer all of the questions, send us what you've got to try for that random draw slot. Thank you again for reading and participating in these challenges. I hope you enjoy this one! All entries are due by January 11, 2010.

--Ed Skoudis

EthicalHacker.net Challenge Master

Author of Counter Hack Reloaded, Co-Founder, InGuardians, SANS Instructor

del.icio.us

Discuss in Forums {mos_smf_discuss:December 2009 - Miracle on Thirty-Hack Street}

SANS vLive SEC 560 Network Pen Testing w/ Ed Skoudis Starts Feb 16

Miracle on Thirty-Hack Street

By Ed & SantaMan & Skoudis and Kevin & Jingle Bell & Johnson

The e-mail was courteous but forceful:

From: Santa@TheRealSantals.Me

Subject: Error in Reindeer Positioning

Date: November 25, 2009 8:37:17 AM EST

To: [Manager at Big-Name E-Commerce Retailer]

I've always enjoyed your website, especially during the holidays. You can imagine my surprise when I looked at the picture of me and my reindeer on your main page. I regret to inform you that you're making a serious mistake. Consider this image from your site:

As you can see from my annotations above, you've got Cupid where Blitzen should be, and Dasher should be on my right-hand side. Please do re-arrange them. Also, we still haven't fully resolved last year's unpleasantness between Rudolph and the elderly lady who claims he ran over her (referred to as the "ReindeerGate" incident in the press). Rudolph has been on the lam since then so please remove him from the picture until we resolve this unfortunate misunderstanding amicably.

Sincerely,

Kris Cringle

a.k.a., The Real Santa Claus

After clicking "Send", Kris started walking toward the Thanksgiving Day parade in Manhattan. As he approached 34th Street, the organizer of the parade, Mrs. Walker, abruptly stopped him. "You! You'll do. Our parade Santa had to drop out at the last minute, the victim of a hit-and-run accident by a renegade reindeer. Put on this costume and sit on that sleigh parade float!" Kris, although not in the habit of substituting for spurious Santas, decided to fill in so that the children wouldn't be disappointed.

Kris did such a marvelous job that the large retail sponsor of the parade, a company very jealous of its important trademark brand name, insisted on hiring this kindly old gentlemen to be their in-store Santa for the Christmas shopping season. Kris was a huge success among the children and their parents, with an almost magical way of bonding with people.

While working at the large, not-to-be-infringed-upon Manhattan-based retailer on 34th Street, Kris befriended a little girl named Suzie, age 8. Suzie was becoming quite a computer geek, spending a lot of time on her laptop building her infosec abilities. Although she didn't yet have mad skillz, she was well on her way. Kris also met a friendly and honest lawyer (yes, the only one) named Fred Gailey.

While working at the large trademark-sensitive New York City department store, Kris ruffled some feathers with the store psychiatrist. In a routine mental examination, it became clear that Kris believed he was the real Santa Claus, a preposterous thought as far as the psychiatrist was concerned. To protect society from Kris, the psychiatrist filed paperwork with a court to have Kris Cringle committed to Bellevue mental institution. The State of New York scheduled a courtroom hearing for the following Monday. For the hearing, Kris asked Fred to be his lawyer and Suzie to provide technical support. Both offered to help their friend.

"All rise!" declared the bailiff as Judge Harper walked solemnly into the courtroom.

After Kris was sworn in, the attorney from the State of New York began his questioning. "Do you, sir, believe that you're Santa Claus?"

Kris's eyes twinkled as he responded matter of factly, "Of course."

"The state rests, Your Honor."

It was now Fred's turn. He put on his most authoritative voice and said, "It all comes down to this: You believe that Mr. Cringle is not sane because he believes himself to be Santa Claus. But, he would be perfectly sane if he is indeed Santa Claus."

Judge Harper asked, "So, can you prove that your client is Santa?"

Fred responded hesitantly, "Ummm... not at this time, Your Honor." Things were looking pretty grim for Kris.

Because of a hard-fought election campaign for his judgeship, Judge Harper wasn't keen on how this case was proceeding. He feared a voter backlash if he had Kris institutionalized, yet he had to follow the law. The judge's consigliere, who bore more than a passing resemblance to Fred Mertz from the I Love Lucy television show, had told him that he'd lose the next election if he decided against Kris.

But Judge Harper hit upon on a novel idea, a way out of this mess. He explained it to Fred, "Using my computer browser, I've found that the real Santa Claus has a website at <http://www.therealsantais.me/>. And, because we can trust everything we see on the InterTubes, this must be the Real Santa's site. Even more, Santa has placed his GPG public key there. I downloaded his key just this morning. I simply encrypt a message for Mr. Cringle using the Real Santa's public key. If your client can decrypt the message, that'll prove that he has the private key, and therefore must be the Real Santa Claus."

After fiddling with his laptop for about ten minutes, the judge provided this file for Kris to decrypt.

Judge Harper then announced, "We'll reconvene in 48 hours. If you can provide a decrypted copy of this file at that time to this court, you'll have proved that Kris Cringle is the Real Santa Claus, and the case will be dismissed. In the mean time, this court stands adjourned."

Fred was overjoyed given this clear path to legal victory! Within the hour, Fred had a meeting with Kris and Suzie in his office. Fred started the meeting with a big smile, "This should be a cinch. Just decrypt the message, Kris."

Kris was troubled. "Unfortunately, I can't," he lamented.

Suzie piped in, "Did you lose your private key?"

"No, it's right here," Kris answered as held up an adorable little Teddy bear.

Fred shrugged, "Uh, Kris. That's a teddy bear, not a GPG private key. Perhaps you really do belong in Bellevue."

Kris smiled and answered, "No, silly, it's not just a teddy bear. It's a USB key, where I keep some private data." Kris popped the head off of the bear and inserted it into Fred's laptop.

Fred copied off the private keyring file, which is located here.

"So, we've got everything we need!" said Fred. "Let's decrypt the judge's message."

Kris glumly responded, "I'm afraid this isn't going to work. I was trying to tell you that I plum lost the passphrase for my key. I know it has something to do with my past vacation experiences, but I just can't remember which one. When you are as old as I am, you tend to forget things, and I've taken numerous summer vacations in my life."

Suzie's mind was working on overdrive as she said, "Wait... we may be able to work something here. Mr. Cringle, you do have a Facebook account, right?"

Kris answered, "Why, sure I do. Everyone does these days. It is here. I do keep a good amount of information, including my holiday travel plans on my page, but I've marked those items as private to keep them hidden from public view. You can't be too careful these days, you know. However, unfortunately, I've lost my password for my Facebook account too. I did make sure that my GPG passphrase is different from my Facebook password, though. Darn these modern times with their multiplicity of passwords."

Suzie's eyes darted around as she thought about how to jump past this roadblock, "Well, you've friended Fred here, right? As a friend, he could pull the private information from your account."

Fred interrupted, "Yes, Kris friended my account, which is located here. But, now I've got a problem. Someone has compromised my Facebook account and changed my password. It really bugs me, because the hijacker accepts friend requests from anyone who asks within 24 hours. I can't log in to my account, but this promiscuous friender can. Can't we just hack into Kris's account or mine and snag the data?"

Suzie didn't like the way this was going, "No, we shouldn't do that. We certainly don't want to violate any Facebook terms of service and launch an attack to try to take over anyone's account, even your own. We don't even want to engage in password guessing. We just need to get access to the items that Kris marked as private." She paused for a second, and then blurted out, "Wait! I still think there may be a way for us to get this information."

Kris and Fred looked at the genius 8-year old and said simultaneously, "But how?"

Suzie pointed to her laptop screen and said, "The Facebook developer kit may offer us some way to get the private data we need about Kris's vacations. Check out this Facebook app I've been working on..."

For larger image, [click here](#).

Fred and Kris looked at the gibberish on the screen. It was nonsense to them.

Suzie explained that it was the code for a FaceBook application. "It allows us to retrieve information from various accounts." Suzie explained. "But, it doesn't seem to be working for some reason."

Fred, worried about the time available to debug the application, said, "Isn't there a way we can grab this information from Kris's account without writing and debugging an app?"

Suzie then had her eureka moment, "Actually, I think we can do this without creating an app. We might be able to just use the Facebook API test page located at <http://developers.facebook.com/tools.php> to try out code snippets. I just went there and ran an FQL query to look up Kris's name based on his user ID." She pointed at her laptop screen to show the information. "I wonder if we might be able to get more information this way."

For larger image, [click here](#).

And, that, dear reader, is where you get involved. Follow Suzie's advice and figure out a way to decrypt Judge Harper's file. Note that you should not do anything that violates Facebook's terms of service. You should not attempt to take over the Facebook account for Kris, Fred, or Suzie, nor should you perform password guessing against these Facebook accounts. You do not need the Facebook passwords to solve the challenge.

Follow the evidence, solve the challenge, and help save Santa from the asylum by answering the following questions:

- 1) "What is the name of the following mathematical property? If $a=b$ and $b=c$, then $a=c$."
- 2) What FQL query or API call can be used to retrieve information about vacations from Kris Cringle's (uid 100000565751882) Facebook account?
- 3) What Facebook privacy setting allowed this data leakage? What is the default value of this setting?
- 4) What is the text from the decrypted message from the Judge?

Bonus Question: What other information can you pull from the Kris Cringle Facebook account (uid 100000565751882)?

Submit your answers to [skillz1209 \(at \) ethicalhacker.net](mailto:skillz1209@ethicalhacker.net) with the subject line "Skillz Submission" by January 11, 2010 for a chance to win an autographed copy of Counter Hack Reloaded. The autograph will congratulate you on your prowess in mastering this challenge! We'll choose three winners, as usual, one in each of the three following categories:

- Best Technical Answer
- Best Creative Answer (that is also technically correct)
- Random Draw (Anyone can win, so send in a response, any response... it doesn't matter)

Happy Holidays!!