

# Scooby Doo and the Crypto Caper

Ruh-Roh, challenge fans...

Ed Skoudis here to introduce a new infosec- themed challenge for you to solve. In this one, challenge writer-extraordinaire Kevin Bong has brewed up a real doozy for you all based on a Scooby Doo theme. Grab a Scooby-Snack, hop in the Mystery Machine, and help the gang solve one of their toughest capers yet. Along the way, you'll contend with some fascinating forensics puzzles and develop your skills. Answers are due back by November 15, 2008. As always, we'll award the fine prize of a book to the best technical answer, the most creative technical answer that is also technically correct, and to a random-draw winner.

Please note that I'll be announcing the winner of our previous challenge, It Happened One Friday, in the next few days, so please stay tuned!

If you can't answer this challenge 100%, still send something in to qualify as a random winner. This month's prize is my book, Counter Hack Reloaded, which I authored with Tom Liston. Each winner gets a signed copy.

Thank you,

--Ed Skoudis, InGuardians

The Ethicalhacker.net Challenge Guy

```
digg_url = 'http://digg.com/security/Scooby_Doo_and_the_Crypto_Caper';  
digg_bgcolor = '#ffffff';  
digg_skin = 'compact';  
digg_window = 'new';
```

del.icio.us

Discuss in Forums {mos\_smf\_discuss:Oct 2008 - Scooby Doo and the Crypto Caper}

ChicagoCon 2008f  
Scooby Doo and the Crypto Caper  
By Kevin Bong

STI University Lot 16 - Ullrich Hall, Department of Cryptography.

"It sure was nice of Professor Taylor to invite us out to visit her at the University for the weekend," said Freddie, as he parked the van in an open spot. "Yeah," replied Velma, "but she also said she needed help figuring out some problems with their final exams."

As the group walked through the building past the classrooms and lecture halls, they were greeted by Dr. Taylor. "Hi guys, I'm so glad you could make it. Let me show you to the cryptography lab."

Dr. Taylor pointed out the faculty offices as they headed down the hallway. "That's my office," she said, indicating a bright, well organized office filled with plants. "This office is Dr. Johnson's." The group looked in and saw tall stacks of books and papers on every surface. "That's Dr. Miller's office," she said, pointing to a cluttered office decorated with anime figurines. "And this one is Dr. Wilson's office. He's the head of the cryptography department." The office was large, spotlessly clean, and empty except for a bookshelf, the desk, chairs, a computer, and a telephone. Finally she stopped at the door at the end of the hall, scanned her keycard, and with the click of the magnetic lock opening they entered the lab.

The lab was actually a very nice data center with raised floor, eight racks filled with computing equipment, and what appeared to be relatively new of power, cooling, and fire suppression systems. Dr. Taylor lead them over to a computer set up next to a high-capacity printer.

"Thanks again for coming guys. We're continuously having problems with students somehow getting copies of our exams before the exam dates. I'm hoping you can help solve this mystery."

"Exams are printed from this computer. We each store our exams on the local drive of the computer, PGP encrypted in our own folders. I'm pretty sure that my last exam was stolen off this computer, because on my last test I made some changes to the copy stored on this computer the day before I printed and handed out the exam, and some students' answers indicate they knew those questions before the exam began. I've logged in and scanned the computer, and I'm confident there aren't any viruses, keystroke loggers or other backdoors or rootkits installed. Exams are printed immediately before the test, so I don't think the weakness is in the print process. The computer is not on any network, and the only people who have access to this room are the four of us faculty in the STI Cryptography Department - Dr. Taylor, Dr. Johnson, Dr. Miller, and Dr. Wilson. Someone would have to be getting our PGP passwords to be able to open the exams before we print them."

At this point, three men in lab coats and a young woman who appeared to be a student entered the room. Dr. Taylor introduced them as Dr. Johnson, Dr. Miller, Dr. Wilson, and Dr. Wilson's research assistant, Kim.

Shaggy and Scooby were getting bored with the conversation. They had wandered away from the group and were both scrutinizing a big red button on the wall.

"Hey Scoob, what do you think this does?"

Scooby shrugged his shoulders.

"You should, like, push it Scoob."

"Ruhn Ruh," replied Scooby, shaking his head no.

"Come-on Scoob, you know if we do something reckless and ill-advised we always find a clue."

While this banter continued, Dr Taylor shared with her colleagues, "I've asked them to come to help us figure out how the exams are getting stolen." Dr Wilson groaned and replied, "You really don't need to do that. I -"

At that instant what had been a room bright with fluorescent light and loud with computer fans suddenly became silent and pitch black. There was a rustle, and a loud scream. Dr. Taylor flipped open her cell phone and used the light to find the power supply emergency cutoff and flipped a few switches. The lights and computers slowly started coming back to life. Scooby and Shaggy were standing by the red emergency power cutoff button, looking guiltily at the group and pointing at each other. Dr. Wilson lay face-down on the floor, a knife sticking out of his back and blood seeping into his lab coat.

When Shaggy saw the body on the floor, he grew very pale and slowly stuttered, "Like, I - I told you we'd find a clue, Scoob."

Freddie knelt down by the body and checked its pulse. "Yup, he's dead alright." Daphne reached down and swiped some blood on her hand and said, "No he's not. That's a fake body and this is fake blood. Its never a real body." To which Freddie replied, "No, I'm quite sure its really him, and he's really dead."

On hearing the truth, Daphne also became very pale. She looked at the blood on her hand and fainted onto the floor. Looking over at her limp, prostrate body Freddie commented, "I've heard if someone faints you are supposed to loosen their clothing." Velma quickly retorted, "Cool it Freddie, this isn't that kind of fan fiction." She pushed Freddie out of the way and knelt down by the body of Dr. Wilson. Studying the knife, Velma said, "Jinkees, this isn't just any knife, this is one of those USB Swiss Army knives." Velma yanked the knife out of the corpse, pulled her laptop out of her bag, flipped open the USB memory stick on the knife, and plugged it into her USB port.

Dr. Taylor cautiously said, "Uh, Velma, shouldn't you wait for the police before you start to touch all that stuff?" "Nah, we do this all the time," Velma replied.

After staring for a minute at the scene, Kim blurted out, "Oh no. Dr. Wilson's final exam is this afternoon, and he never gave me the exam to print out or the answer key." The others looked over Velma's shoulder and saw her feverishly typing commands like "strings" and "foremost" and saw data streaming past on her screen.

After working on her laptop for a few minutes, Velma said, "Well, I was only able to get a portion of a disk image, and it looks like there's some corruption in it. I think some blood has shorted out the circuitry. But it looks like there's enough information on it to figure out how the exams were being stolen, who killed Dr Wilson, and to continue with this afternoon's cryptography final exam."

Questions:

Here is a copy of the partial disk image that Velma obtained.

1. Can you figure out who killed Dr. Wilson, and why?
2. How were the passwords stolen to steal the exams?
3. Can you provide a copy of the cryptography final exam? Can you create an answer key?
4. Also, provide some analysis of Velma's incident handling process. What did she do right? What should she have done differently?

Submit your answers to [skillz1008@ethicalhacker.net](mailto:skillz1008@ethicalhacker.net) with the subject line "Skillz Submission" by November 15, 2008 for a chance to win an autographed copy of my book, 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)

Thanks again,

--Ed Skoudis, InGuardians

The Ethicalhacker.net Challenge Guy

Scooby Doo trademarks and copyright belong to Hanna-Barbera. The laptop image is from 2003's "What's New, Scooby-Doo?"