

# Frosty the Snow Crash

The Clock Has Struck 12

Like it or not, it's that time of year again. At least we have the continuing EH-Net tradition of an Ed Skoudis Holiday Challenge to get you through those days of brain freeze... and maybe even system freezes. Dive into the head of Ed Skoudis as he takes you into the cyberpunk world of Neal Stephenson with a little twist as only Ed can deliver.

Remember Challenge Fans, as always, we'll award three prizes: One for the best technical answer, one for the most creative answer that is technically correct, and one awarded to a winner chosen randomly. Thus, if you can't answer all of the questions, still send something in to qualify for the random winner. This month's prize is my book, *Malware: Fighting Malicious Code*, which I authored with Lenny Zeltser.

--Ed Skoudis, Intelguardians

Author, *Counter Hack Reloaded*

[del.icio.us](http://del.icio.us) Slashdot It!

Discuss in Forums {mos\_smf\_discuss:Dec 07 - Frosty the Snow Crash }

Sponsored by Core Security  
Frosty the Snow Crash

By Ed Skoudis

snow n.... 2.a. Anything resembling snow. b. The white specks on a television screen resulting from weak reception.

crash v.... -intr.... 5. To fail suddenly, as a business or an economy.

--The American Heritage Dictionary

frosty adj.... 1. (of the weather) very cold with frost forming on surfaces.

--The Oxford English Dictionary

The Frostinator belonged to an elite order, a hallowed subcategory. Yes, the snowman the children built had indeed come to life one day, waking up and shouting "Happy Birthday!" There must have been some magic in that old silk hat they found, for when they placed it on his head, he began to dance around. Actually, saying that the children "found" the hat is a bit controversial. An evil magician had carelessly thrown it away, not realizing the hat's enormous enchanting potential. But, when the magician witnessed the Frostinator come to life, he claimed that the children had stolen his hat, and vowed to get it back.

Meanwhile, the Frostinator established himself as the best belly-whopper in the Metaverse, an online virtual world with its own Winter-themed town where the most popular sport was sliding down virtual hills on one's belly. No one could out-belly-whop Frosty, as the kids came to know the Frostinator. Children from around the world looked up to Frosty, a role model firmly ensconced in the celebrity-industrial complex of the Metaverse.

While powerful, Frosty did have an Achilles heal, a nemesis, his own personal kryptonite, if you will. Quite simply, heat was a big problem for the Frost-man. If it got too hot, Frosty would melt, first turning into that gray sloppy slush that annoys pizza delivery drivers on deadline and then... well, the grim picture of a melting quickened snowman is too

gruesome to cite here. As Frosty melted, you could tell that he was reaching the point of no return when he would begin to see visions of "snow," the erratic static from old TV sets with bad reception. Rather like a man dying of thirst in the desert seeing visions of a non-existent lush watery oasis, when Frosty started hallucinating an oasis of snow, he was well on his way to puddle-dom. The condition was called a "Snow Crash".

Frosty accessed the Metaverse for his belly whopping escapades using a laptop he had named "icebox". To keep the temperature of the machine down so that his own computer wouldn't melt him, he was careful not to overexert the CPU. Did he run Vista? Are you crazy? The intense CPU chomping needed to display the Aero GUI would, by itself, heat up the box and spell certain doom for Frosty. Instead, he relied on a pre-Lenovo-brand-change IBM ThinkPad T43, with Windows XP Pro SP2 installed, keeping everything as cool as a polar bear eating an icicle in a snowstorm, more or less.

Because of his major concern about his system getting too hot, Frosty whipped up a command to display the internal temperature of the icebox every 15 seconds in tenths of degree Kelvin:

As he belly-whopped his way through the Metaverse, Frosty periodically glanced at the script's output on his screen to make sure he was keeping his cool. If the icebox ever hit 3333, he was toast. But, for now, Frosty was chilling quite nicely.

But then, the evil magician unleashed his plan to cook Frosty, using the much-vaunted icebox itself to turn up the heat on the unsuspecting snowman. He began his attack by running an automated password-guessing tool across the network, directed against the icebox via Windows file and print sharing protocols. He was trying to access the administrator account using a dictionary of words the magician composed himself from the screenplay of the Frosty the Snowman Christmas TV Special. Within minutes, he had determined the administrator password for the icebox: happybirthday. "Figures," the evil magician muttered to himself, "Frosty's security is pretty lame, with an admin password set to the phrase he utters every time someone puts my hat on his head. With such security, I'll bet he's not even running a personal firewall." The icebox admin password was practically taunting the magician, so he unfurled the next element of his plan.

The magician typed the following into a command prompt on his own Windows machine, to keep track of the status of his diabolical scheme:

As that command ran in one window, the evil magician moved to another cmd.exe window on his own box to get some further work done. He typed:

Then, back in a separate cmd.exe window on his own machine, the evil magician typed the following long, maniacal screed:

Within thirty seconds, Frosty started to feel a bit flush. He glanced at his temperature-checking script, however, and everything looked totally fine. He continued belly-whopping for a little while, when then, it started to happen. He began to see static everywhere he looked... the first stages of Frosty's Snow Crash had begun.

And, that's where you come in. Answer the following questions to save our hero from that evil magician, ensuring happy holidays for everyone in the Metaverse.

Questions:

- 1) Why didn't Frosty's temperature-checking script work properly?
  
- 2) What did each of the evil magician's commands do? Why did he use these commands in this way?
  
- 3) What should Frosty do next to stop the heat and expel the magician from his machine? Remember, he's got to work fast or else he'll end in a horrible Snow Crash!

Submit your answers to [skillz1207@ethicalhacker.net](mailto:skillz1207@ethicalhacker.net) with the subject line "Skillz Submission" by Friday, December 21, 2007 Monday January 7, 2008 for a chance to win an autographed copy of my book, Malware: Fighting Malicious Code, a great stocking stuffer for everyone on your holiday list. The autograph will congratulate you on your prowess in mastering this Frosty 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 (so send in a response for a chance to win even if you can't answer all of the questions)

Oh, and as a special holiday bonus, I've been able to get ahold of Mike Poor's super-secret recipe for cooking a holiday turkey using your MacBook Pro. I managed to swipe it from him in an elite hack called... umm... well... "cut-n-paste" from an e-mail he sent me. Anyway, I'd like to unveil this culinary delight to the world now:

Just set a turkey (up to 20 lbs) on your lap. Then, place your MacBook Pro atop the turkey. In under the time it takes to charge your battery, you will have a fully cooked (or at least warm) turkey.\*

Finally, above all, I hope you have a most blessed Holiday season, enjoying time with family and friends.

Ed Skoudis

Author, Counter Hack Reloaded

SANS Institute Fellow

Co-founder, Intelguardians

\*The government of the Metaverse warns that consuming undercooked or raw foods can adversely affect your health.

