

## A Christmas (Hacking) Story

del.icio.us

Discuss in Forums {mos\_smf\_discuss:Dec 06 - A Christmas (Hacking) Story}

To help you get into the holiday spirit, this month's challenge is based on one of my all-time favorite Christmas movies, A Christmas Story. If you haven't seen the movie, or have forgotten it, you can get a brief overview of the movie in 30 seconds and reenacted by bunnies. I hope you enjoy the challenge! And, have a very Merry Christmas!

--Ed Skoudis

Intelguardians

Author, Counter Hack Reloaded

Please read Ed's challenge, compose your answers, and e-mail them to [skillz1206@ethicalhacker.net](mailto:skillz1206@ethicalhacker.net) with the Subject: 'Skillz Submission' by December 22, 2006. Ed will choose three winners in early January who will receive an autographed copy of his book, Counter Hack Reloaded. We'll award the best technical answer, the most creative technically correct answer, and a third will be drawn from all answers submitted, correct or not. So, even if you can't answer all of the questions, send in what you have. You just might win the prize in the random draw category.

Skillz Sponsored by Core Security Technologies

Ralphie's Mother: Is this another one of your silly puzzles?

Ralphie's Father: Yeah, another one of my silly puzzles. But, this one could be worth AN AUTOGRAPHED COPY OF COUNTER HACK RELOADED!

Mother: What kind is it this time?

Father: Solve a hacking challenge... why, I could win a MAJOR AWARD!

Written in the voice of Mr. Ralph Parker, a 40-year old man writing in the year 2037.

Ahhh... I remember way back when... I lived on Cleveland Street. I was nine years old and Christmas was on its way! Lovely... glorious... beautiful... Christmas, around which the entire kid year revolved. For Christmas, I wanted an official Red Rider, carbine action, two-hundred Gig model laptop, and I wanted it with every fiber of my nine-year-old being. It was sheer computerized, electronic joy -- the Holy Grail of Christmas gifts. For weeks, I had been scheming to get my mitts on one of these fearsome silicon beauties, which I could use to defend motherhood and apple pie against all sorts of evil.

My fevered brain seethed with the effort of trying to come up with the infinitely subtle devices necessary to implant the laptop indelibly into my parents' subconscious. I struggled for exactly the right laptop hint. It had to be firm, but subtle, so my parents would know what I wanted without me being too overt. At the breakfast table, I blurted out, "Skodo says he saw some bot-net traffic near Pulaski's candy store!" They looked at me as if I had lobsters crawling out of my ears. I could tell I was in imminent danger of overplaying my hand. They were oblivious to how much I needed that laptop to defend us all against evil bot-nets.

Mom then asked the inevitable question, "Ralphie, what would you like for Christmas?" Horrified, I heard myself blurt out, "I want an official Red Rider carbine-action, two hundred Gig model laptop!" My heart sank as my Mom responded, "No, you'll hack your eye out!" It was the classic Mother response to a kid who engages in marathon hacking sessions bathed in the feeble light of a laptop display uninterrupted for 72 hours. And she wasn't the only one. "You'll hack your eye out!" was a common refrain from my Old Man and schoolteachers whenever I brought up that trusty laptop, protector of freedom and goodwill. I tried to recover with my Mom using a subtle change in tactics, "But, Skodo is getting one this year!"

Dreary, worried days passed slowly. But had my hint worked its magic on my unwitting parents? I desperately needed to know... But how? Just then, fate intervened, giving me a magnificent chance to peek at my parent's Christmas gift list. While doing my chores emptying the trashcan from my Old Man's den, I found a crumpled up network diagram my Dad had created and discarded carelessly. As I looked at this treasure, I instantly recognized that it included the computer equipment my father used to manage several items around our house.

[Click Diagram for Larger Picture](#)

My Old Man worked in obtuse network architectures the way other artists might work in oils or clay. It was his true medium. Looking through the diagram, I immediately noticed the reference to my ultimate goal, the Christmas gift list that Dad stored on the Windows 2003 server used to manage our furnace. My Old Man was one of the most feared furnace fighters in north New Jersey, and he rigged up quite a system to manage the beast. He had a port listener on TCP 2222, awaiting with a cmd.exe shell that ran with the privileges necessary to access the coveted Christmas gift list. Next, I noted Dad's glorious lamp, a major award he had one in a contest that year, which could be turned on or off by sending e-

mail with a command to a Linux box that controlled the lamp. I also realized that my Old Man had firewalled off the more sensitive elements of our home with a firewall that allowed only inbound e-mail to the lamp, but transmitted any traffic outbound from any system on the protected network to TCP port 80 and 443. I guess the Old Man wanted to be able to surf the Internet from the lamp and furnace systems.

As for me, I was stuck on the kid's network, without the ability to access anything directly on the protected network. I could only e-mail commands to the lamp and receive the responses. To get a better feel for what I was up against, I e-mailed the lamp a simple command: id. The e-mail I got back contained the following:

```
$ id
```

```
uid=502(lamp) gid=502(lamp) groups=502(lamp)
```

Then, I sent it e-mail with the "ls -la" command, which responded with:

```
$ ls -la
```

```
total 448
```

```
dr-x----- 2 lamp lamp 4096 Sep 24 02:08 .
```

```
drwxr-xr-x 6 root root 4096 Sep 24 01:55 ..
```

```
prw-rw-rw- 1 root root 0 Sep 24 02:02 chimney
```

```
-rwxr-xr-x 1 root root 444228 Sep 24 01:59 nc
```

With further commands sent to the lamp, I realized that the command shell the mail server was using to run my commands was severely limited, because I couldn't navigate to or even see any other directories in the file system. What's more, I couldn't write new files anywhere at all in the file system, not even to the directory my commands were running in. Heck, I couldn't even run a shell such as sh, bash, or anything else. All I could do was run that nc file and interact with the chimney file. My first thought was to hack the lamp, trying to get more powerful access on it. But, on second thought, that was a very bad idea. My Dad took the security of his precious lamp seriously, so I wasn't going to be able to get any more powerful privileges on it. Also, if I reconfigured the lamp, my Old Man would certainly notice any changes, upsetting him to the point of destroying my chances at getting the Christmas gift I wanted.

As I pondered these severe limitations and shook my head at the contrivances my Old Man put on the network, I noticed that iTunes on my old beat-up laptop had begun downloading my favorite podcast! Little OphCrack Annie was on, and she had a secret message that likely involved the fate of the free world. As I listened to the show, the announcer read these characters, one at a time:

```
62B7CD49704064BDAAD3B435B51404EE
```

```
97E61E27B7599ADFAAD3B435B51404EE
```

04BAF1615A04764EAAD3B435B51404EE

C90B9E4F1B743404AAD3B435B51404EE

4EAF812DAFA29CF7AAD3B435B51404EE

AAB65B7207A5FAF9AAD3B435B51404EE

9D82CDFF56B35758AAD3B435B51404EE

E414A2208C930D79AAD3B435B51404EE

ECED132790CB280BAAD3B435B51404EE

F6F2790B99137838AAD3B435B51404EE

BBC70D3C8F0049A5AAD3B435B51404EE

A5CD742A1FF7DD5AAD3B435B51404EE

Whew! That was an avalanche of gobbledygook. I carefully wrote down each character, planning on using my special decoder ring to see what mysterious messages Annie was trying to send. I simply had to know.

And, here's your chance to help Ralphie get a copy of the Christmas gift list by answering the following questions:

1) What is interesting about the files that Ralphie could see on the lamp server?

2) What is the significance of the Annie cyphertext?

3) What command could Ralphie e-mail to the lamp to get access to the command shell on the furnace server from the kid's network to read the Christmas list? What should Ralphie do on his own laptop for this to work? Assume that you cannot alter the configuration of the lamp or get any higher privileges on that machine, nor can you reconfigure the firewall.

4) How can Ralphie make the activities you describe above less likely to be detected by his Old Man?

Remember: Use Subject: 'Skillz Submission' or get your tongue on a pole!

Please submit your answers to [skillz1206@ethicalhacker.net](mailto:skillz1206@ethicalhacker.net) with the Subject: 'Skillz Submission' by December 22, 2006. In early January, we'll announce three winners, one from each of these categories:

- Best technical answer
- Most creative and technically correct answer
- Random draw from all answers submitted, correct, incorrect, complete, partially complete, etc.

Each winner gets a copy of Counter Hack Reloaded, autographed by author Ed Skoudis, congratulating you on your victory and amazing abilities!

For more fun, try this Christmas Story Mac Theme.

For you Windows users out there, it's just too scary to recommend anything that you can download for free online.

The Red Rider Laptop picture, although actually green in more ways than one, is one of the prototypes for the One Laptop per Child Project. Help support this worthy cause, because every child in the world deserves to dream like Ralphie.