

## Santa Claus is Hacking to Town

Happy holidays, challenge fans! In the spirit of the season, I've written a Santa Claus challenge for you, titled "Santa Claus is Hacking to Town." This one is adapted from the classic 1970 Rankin & Bass television production, which used stop-motion animation and nifty puppets to tell the story of Kris Kringle. As a child, this was one of my favorite Christmas TV specials, and I'm thrilled to recast it as an ethical hacking challenge. You don't need to be familiar with the original TV show to participate in the challenge, of course. Analyze the clues, devise your strategy, and carefully answer the questions to win a prize. Answers are due by December 31, 2008. We'll choose three winners (best technical answer, most creative answer that is technically correct, and a random draw winner) to get a copy of my book, Counter Hack Reloaded, the ultimate stocking stuffer. Even if you can't answer all the questions, send in your best guess to qualify for that random draw slot.

Even though you don't have to be familiar with the original TV show to answer the challenge questions, for those of you who haven't seen the original Santa Claus is Coming to Town TV show or want to relive that childhood wonder of watching Kris Kringle grow up into Santa, you can watch its five parts on YouTube here:

"Santa Claus is Coming to Town" Part 1 - Part 2 - Part 3 - Part 4 - Part 5

And now... on with the challenge!

--Ed Skoudis

Co-Founder, InGuardians, SANS Fellow, EthicalHacker.net Challenge Master, Author of Counter Hack Reloaded, Santa Elf Trainee

del.icio.us

Discuss in Forums {mos\_smf\_discuss:Dec 08 - Santa Claus Is Hacking to Town}

Santa Claus is Hacking to Town

By Ed Skoudis

## WORLD NEWS

Today, children everywhere are making preparations for an event of world-shaking significance: the annual visit of Santa Claus. Informed sources report legions of junior citizens are making monumental efforts not to cry and not to pout. Meanwhile, e-mail messages by the thousands have been flooding postal facilities at the North Pole.

Enter the postman, who runs the North Pole SMTP server. He begins to speak, spinning the following tale:

Well, hello there! My name is Sk0D0 Kluger, or Sk0d0 for short. Ohhhh&hellip;. I&rsquo;ve got lots of e-mail messages for Santa today. And every year, they&rsquo;re the same. Some ask for toys. But a lot ask questions. Like, take this one. I&rsquo;ll bet one of you wrote it.

&ldquo;Dear Santa, when did you first get interested in penetration testing?&rdquo;

Uh-huh. I thought so. And this one:

&ldquo;My turn&hellip; Dear Santa, what was your first really elegant hack?&rdquo;

How about these?

&ldquo;Dear Santa, how did you develop your love of computer hacking tools?&rdquo;

&ldquo;What is your favorite exploit?&rdquo;

&ldquo;Which tools in your pen testing arsenal do you find most useful?&rdquo;

Ok&hellip; hold on a minute. So, you want to know all about Santa and his hacks? The best place to start is at the beginning. Now this was years and years ago, way back. In one of the Northern Countries, there was a small city named Sombertown near the North Pole. There, the Kringles, a family of red-suit-wearing elves, were world renowned as the First Tool Makers to the King. These jolly, diminutive coders wrote the foremost vulnerability assessment and penetration testing tools ever, providing them to the King of Sombertown. He loved their finely crafted handiwork and saw that their tools were distributed to all of the citizens in his dominion. Indeed, it was a golden age of tool development and security research.

Unfortunately for the Kringles (and the King), a totalitarian group known as the Burgermeisters staged a coup, deposing

the King and initiating their rule. They installed a new Mayor over Sombertown, a mean old grouch of a fellow known as Burgermeister Meisterburger.

“Herr Burgermeister, Herr Burgermeister!” said Grimsby, the evil Mayor’s henchman. “An evil hacker has exploited a server in our fair town, all because hacking tools are freely distributed throughout the land.”

The Burgermeister responded, “As I suspected… I hate hacker tools! And hacker tools hate me. Either they are going, or I am going. And I am certainly not going.” Rather than focus on improving computer security within Sombertown, the Burgermeister and Grimsby dealt with the problem by passing a new law, which they called 202c, the Sombertown Anti-Hacking Tool Edict. This brief law simply stated that, “Hacker tools are hereby declared illegal, immoral, unlawful. And, anyone found with a hacker tool in his possession will be placed under arrest and thrown in the dungeon.”

About twenty years earlier… the Kringles had adopted a foundling baby, whom they named Kris. They decided to raise Kris themselves as a genuine Kringle, red suit and all. After the Burgermeister coup, the Kringles fell out of contact with Sombertown as Kris grew up. They knew nothing about 202c or the Burgermeister, and continued writing new tools and exploits, which began to pile up in their lab. When Kris reached adulthood, the Kringles decided that he was the obvious choice to deliver the latest batch of hacker tools to the residents of Sombertown.

As Kris traveled to Sombertown with a sack full of tools and exploits for the kiddies, he met the Winter Warlock, an evil old wizard who controlled the mountain between the North Pole and Sombertown using magic. The Warlock was evil through and through. That is, he was until Kris gave him a copy of the latest version of Metasploit, which melted his cold, malevolent heart, and turned him into a friendly chap. With his newfound warmth, however, the old Warlock’s magic powers began to dissipate quickly.

Upon arriving in town, Kris set about distributing some of the Kringles’ latest tools to children he saw in the main town square. Almost instantly, their teacher, a beautiful woman named Jessica, intervened. “How dare you! Distributing hacker tools? Don’t you know about 202c? If the Burgermeister saw you, we’d all be in great danger. Hacker tools are frivolous, impractical, unproductive, and…” As she explained the law to Kris, he pulled a DVD with the latest version of Nmap from his sack and handed it to her, showing her the man page on a terminal of the MacBook Pro he carried with him. She exclaimed, “I remember running the Strobe port scanner when I was a little girl. But, Nmap is so much more powerful and useful. Well, maybe 202c is a silly law, after all.” Jessica broke into song, singing of the joys of hacker tools while tacky 1970’s tie-dyed graphics swirled about her. From that point forward, Jessica committed to helping Kris and the Kringles distribute their tools.

Suddenly and unexpectedly, the Burgermeister, Grimsby, and several soldiers ambushed and arrested Kris, Jessica, and the Winter Warlock in a raid that later became known as “Operation Christmas Crackdown.” As 202c specified, the new inmates were placed in the Sombertown dungeon.

From inside their cell, the group peered through the prison bars. Twenty feet from their locked cell door, they could see a Windows computer with a sign next to it, saying “Door1: Fully Patched Windows Server Controlling Prison Door.” In slightly smaller print, there was another sign with a reminder for the Jail Master: “Run dooropen.exe to open prison door using jailmaster account.” Hanging next to it was a tattered copy of a network diagram, showing the network architecture of the prison itself.

Kris, Jessica, and the Warlock watched as the Jail Master logged into that system, but weren't able to shoulder surf his password, which seemed excessively long and cumbersome to type. However, listening carefully, they could hear the Jail Master utter, "I'll just log in with my account name of jailmaster, and the same password I use to manage every Windows system in this dungeon." The Burgermeisters didn't worry about keeping this stuff secret, because they figured they were secure given that 202c outlawed hacking tools. The Jail Master ran a few commands and then logged out of the system, walking away from the cells to eat some Sombertown gruel for lunch.

Using a technique borrowed from the Brady Bunch TV show, Kris, Jessica, and the Warlock tried using their boots to hit the keyboard of the door1 machine. Their plan for typing by throwing their footwear failed because the keyboard was just too far away. Physical access to any boxes outside of their cell was simply impossible. Furthermore, they didn't know the password for the jailmaster account.

As he studied the network diagram, Kris thought out loud, "Perhaps we can hack our way out of here!" He fired up the wireless client on his trusty Mac, and discovered the prison access point. He associated with it, and smiled as it gave him an IP address. Kris tried to surf to the Internet, but quickly realized that he was on an isolated network. Using the copy of Nmap he had given Jessica, he ran a ping sweep, identifying only two systems on the network he could reach: a Windows client called jailmasterlaptop and a Linux web server named web1. He then ran a port scan, discovering that he could access the NetBIOS and SMB ports of jailmasterlaptop and TCP port 80 on the web1 server.

On a whim, Kris ran the copy of Metasploit he had given to the Winter Warlock, using the MS08-067 exploit against the Jailmaster's laptop. He was delighted to see that he got shell access on the machine! However, when he tried to connect from the jailmaster laptop to the door1 machine they could see in the network diagram, he was blocked. From his shell on jailmasterlaptop, he ran the command: net accounts. Kris noted that the minimum password length for accounts was set at 50 characters! Apparently, the Jail Master liked to type very long passwords.

Kris then turned his attention to the web1 server. Going through its various user input fields, he found one with a command injection flaw. He could type any command into a form field of a web page, and the target server would run the command and display its output in Kris's browser. He could even ping the door1 machine! Initially overjoyed, he quickly realized this server wouldn't give him the keys to the castle either. He could only run commands as the user "apache," a non-UID 0 account. Furthermore, iptables blocked all inbound connections to the machine, except inbound port 80 for the web server itself and ICMP Echo Request messages. All outbound connections were allowed, though. Kris soon realized that he could not reconfigure iptables from the limited privileges of the apache account. Furthermore, the box was fully patched, without any chance of local privilege escalation. Things got even worse, as Kris explored the machine's file system only to find that Netcat was not included in this distribution, which appeared to be a stripped down Fedora Linux machine.

With this understanding of their target network, the team took an inventory of the resources they had, which included:

\* Kris Kringle's laptop, a MacBook Pro running VMware Fusion with a Windows XP image and a Linux image.

\* The latest version of Metasploit, which includes the MS08-067 exploit to compromise the jailmasterlaptop machine with

local SYSTEM privileges.

\* The latest version of Nmap.

\* A copy of Netcat compiled for Linux.

While this was certainly a useful small arsenal, the team fiddled around with it for several hours, unable to figure out a hack to make it all work.

In desperation, Kris asked, "Mr. Warlock, what magic skills do you have left?"

The Warlock responded, "Please, call me Winter. Alas, since I turned good, my magical powers are rapidly waning. I have nothing but a few meager magical leftovers here in my pockets... A short-circuited wand. Useless. A dried-up magic potion... Powerless. A copy of psexec from Microsoft Sysinternals. Hardly useful here. Oh, and a magic netbook laptop that will let me download any one reasonably sized hacker tool from the Internet. Just junk. It can't dissolve prison walls."

Jessica entered the conversation, and excitedly instructed, "Use that magic laptop to get us a zero-day exploit to hack door1, the machine that controls this prison door, Mr. Warlock."

The old weakened magician responded, "Just refer to me as Winter, please. Sorry, Jessica, but my laptop can magically grab only one tool from the Internet, and it must exist on a publicly accessible website right now and be available for free. It can't grab some hypothetical program from a made-up URL to run some unknown zero-day attack."

Kris thought hard and then asked the wizard, "Mr. Warlock, why don't you conjure up an NT Rainbow table with passwords up to 50 characters!"

Although still kindly, the old wizard was growing annoyed. "Darnit, please stop calling me 'Mr. Warlock.' 'Winter' will suffice! My magic netbook can only grab one file from a public URL with a maximum size of 1 Megabyte. I can't possibly download huge Rainbow tables."

The team was stumped. If they couldn't hack out of the dungeon, Sombertown would suffer forever under the hands of the Burgermeisters. What's more, Kris would never become Santa Claus delivering Christmas cheer far and wide.

You have to act! Help save Kris and the gang by answering the following questions:

- 1) What tool would you have the Winter Warlock download? Why?
- 2) Devise a step-by-step approach for gaining control of the door1 server so that Kris can execute the dooropen.exe command with the privileges of the jailmaster account. Describe each tool you would use and how you would use it at each step of your hack.
- 3) Briefly finish this tale by describing how the Burgermeisters could detect the tactics you described in your answer to item 2, as well as how they could have defended against each step you described.

Oh, and one last thing. If you need more Christmas-themed hacker challenges to get you in the mood, feel free to check out my previous challenges in this genre. I've written five of them so far, over the past six years:

- How the Grinch Hacked Christmas, 2002
- Rudolph's XSS Christmas, 2003
- A Christmas (Hacking) Story, 2006
- Frosty the Snow Crash, 2007
- Santa Claus is Hacking to Town, 2008

Thanks for participating, dear readers. I hope you have a joyous and blessed holiday season!

--Ed.

Submit your answers to [skillz1208@ethicalhacker.net](mailto:skillz1208@ethicalhacker.net) with the subject line "Skillz Submission" by December 31, 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)