

## The Nightmare Before Charlie Brown's Christmas

Happy Holidays, challenge fans! Ed Skoudis here, with this year's holiday hacking challenge. Have you ever seen the classic video A Charlie Brown Christmas, and pondered why Charlie Brown is so upset at the start of the video? Also, have you ever wondered why the rest of the Peanuts gang is so focused on the materialism of the Christmas season? Well, this year's hacking challenge answers these questions. In our tale, you'll discover that something happened before the start of the Charlie Brown Christmas video that put these characters into such a state. That something is what we like to call...

### The Nightmare Before Charlie Brown's Christmas

These challenges, which are an annual tradition here at EthicalHacker.net, are designed to help people develop their skills, show off their abilities, and have some fun. During past holiday seasons, you got to tangle with the Grinch, Rudolph, that Messy Marvin kid, Frosty, and even Santa himself. And who can forget last year's Miracle on Thirty-Hack Street. Read this challenge, answer the questions, and send your responses in by January 3, 2011 to skillz1210 (at) ethicalhacker.net. We'll choose three winners, each of whom will get an autographed copy of my Counter Hack Reloaded book. One prize will go to the best technical answer, another to the most creative answer that is technically correct, and the final prize is based on a random draw from every person who submits an answer. Even if you have no idea whatsoever for how to answer the questions, send in your best shot to be entered in the random draw. And now, without further adieu, the curtain rises on our story...

--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 2010 - The Nightmare Before Charlie Browns Christmas}

By Ed Skoudis & Yori Kvitchko

December 2010

It was two weeks before Christmas. Jack Skellington, the gaunt skeleton-headed Pumpkin King of Halloween Town, was on his way back to the portals that interconnected the holiday Worlds of Old. He had visited Christmas Town once before, a few weeks earlier, when he wandered far away from home after phoning in his performance for yet another booooring Halloween. Jack was exhausted with the tediousness of his hometown holiday, and longed for the excitement and newness of Christmas.

Jack fondly recalled his first visit to Christmas Town weeks ago, "Color everywhere! Little creatures laughing! Electric lights on strings!" But what impressed him most about Christmas was his understanding of its true meaning. "Presents! Commercialism! Gimme, Gimme, Gimme... Get, Get, Get! What a wonderful orgy of greed!" He smiled as he prepared to jump back into Christmas Town to share in this exciting holiday spirit.

Gazing at the doors, each a portal into another holiday world, Jack noticed a new door -- one that wasn't there before. The heart, shamrock, and turkey doors were joined by not just one Christmas tree door, but two. The first, with its traditional full Christmas tree, was the door he had used before to enter Christmas Town. But the newer Christmas tree door was even more appealing to Jack. "It's sickly, even spidery... a ghoulish Christmas tree! This is the one for me!" As he opened the door to peer inside, he slipped and fell into an alternate Christmas world.

As before, Jack awoke in a snow bank and gazed upon a Christmas scene. But, instead of the spooky Danny Elfman music infused in the other Christmas Town, this world was permeated with the jazzy stylings of Vince Guaraldi. Jack approached some children skating on a nearby pond. All of them ran away as the ghastly stranger approached, except for two little boys. One boy carried a blue blanket, while the other was hideously messy, covered with grime and soot.

"Wh-wh-who are you?" the boy with the blanket stuttered nervously.

"Me? Why, I am the Pumpkin KING!" Jack shouted with pride.

"Eeeeeek! The Great Pumpkin is finally here!" shrieked the blanket boy, who quickly ran away.

Jack addressed the messy child who still remained, "Little boy, you look like my kind of kid. What is your name, and who is the Ruler of this Christmas Land?"

The boy responded, "I'm Pig Pen. I'm not sure about a ruler, but Lucy did mention that she was

going to invite Charlie Brown to be the director of our Christmas play.”

“Ah-ha! Director Charlie Brown is the Sandy Claws of this Christmas world,” said Jack. To reward the boy for this useful information, Jack plucked off his own skeletal head and shouted “Boo!” causing Pig Pen to run away in horror.

Jack wanted to share the wonderful Christmas spirit with all of the other children in this place… but how? He looked around. Near the skating pond, he saw a small booth advertising psychiatric help for 5 cents.

As he walked near the booth, Jack saw a telephone and a piece of paper on the desk behind the booth. The phone was plugged into an RJ45 jack. “A VoIP phone,” Jack smiled as he sat down and opened his laptop, a Linux machine full of tools used for Halloween trickery. “I bet some of these tools will be useful in this Charlie Brown Christmas world!”

Jack also looked at the piece of paper on the desk. It was a contract between Lucy van Pelt and Linus van Pelt. It appeared that Lucy, the operator of the psychiatric booth, was a customer of a VoIP service operated by Linus van Pelt. As he skimmed through the contract, one of its provisions caught his attention:

“To ensure the very best service, PRETTY GIRL (Lucy van Pelt) requires a VoIP connection on the same subnet as the VoIP server itself. In exchange for such a prime location, PRETTY GIRL agrees to pay BLANKET BOY (Linus van Pelt) 10 cents per month.”

Jack commented to himself, “It seems our psychiatrist negotiated some prime real estate on the network, with her phone, and more importantly her RJ45 jack, on the same subnet as the VoIP server!” Once he uttered those words with a toothy grin, Jack’s plan for spreading his own special brand of Christmas cheer to children across the land instantly formed in his mind.

Jack started by picking up the phone receiver on the desk. To his chagrin, when he tried to dial a number, the display on the phone indicated that it had a PIN-based local keyboard lock. Unable to get anything more from the phone, he disconnected it from the RJ45 jack and connected his laptop. He then began by running the following commands:

```
# dhclient
```

```
# ifconfig
```

```
eth0  Link encap:Ethernet  HWaddr 00:50:56:10:10:55
      inet addr:10.10.10.55  Bcast:10.10.10.255  Mask:255.255.255.0
      inet6 addr: fe80::250:56ff:fe10:1055/64  Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:31514 errors:0 dropped:0 overruns:0 frame:0
      TX packets:29111 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:21908354 (21.9 MB)  TX bytes:5213298 (5.2 MB)
      Interrupt:19 Base address:0x2024
```

```
lo    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128  Scope:Host
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:252 errors:0 dropped:0 overruns:0 frame:0
      TX packets:252 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:102149 (102.1 KB)  TX bytes:102149 (102.1 KB)
```

```
# msfconsole
```

```
msf > use auxiliary/scanner/sip/options
```

```
msf > set RHOSTS 10.10.10.1-254
```

```
msf > run
```

```
[*] 10.10.10.77 404 server='Asterisk PBX 1.6.2.11' verbs='INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO'
```

```
msf > use auxiliary/scanner/sip/enumerator
```

```
msf > set RHOSTS 10.10.10.77
```

```
msf > set MINEXT 1000
```

```
msf > set MAXEXT 1100
```

```
msf > run
```

```
[*] Found user: 1001 <sip:1001@ 10.10.10.77> [Auth]
```

```
[*] Found user: 1002 <sip:1002@ 10.10.10.77> [Auth]
```

```
[*] Found user: 1003 <sip:1003@ 10.10.10.77> [Auth]
```

```
[*] Found user: 1004 <sip:1004@ 10.10.10.77> [Auth]
```

[\*] Found user: 1005 <sip:1005@ 10.10.10.77> [Auth]

msf > exit

With this initial information, Jack proclaimed, "Now that all the presents are loaded into the coffin, it's time to execute the details of my plan!"

As Jack worked his trickery to convey his Christmas message to all the children, Linus, the VoIP administrator, noticed an alert generated by a Snort sensor he had deployed to monitor attacks against his VoIP server:

[\*\*] [1:5000009:1] Excessive number of SIP 4xx Responses - possible user or password guessing attack [\*\*]

[Priority: 0]

11/29-20:45:10.821941 10.10.10.77:5060 -> 10.10.10.55:5060

UDP TTL:64 TOS:0x0 ID:60495 IpLen:20 DgmLen:456

Len: 428

Upon reviewing this alert, Linus commented to himself, "It's a good thing I'm using those extra Snort rules to detect VoIP attacks! And, because I'm the paranoid type, I'm also capturing all packets going into and out from the subnet of my VoIP server. If I open the packet capture files in Wireshark, I may be able to listen to the audio of those sessions to see what's going on. Between the packet capture and the VoIP server logs, I should be able to piece together what's going on here, but I might need some help."

And, that, Dear Reader, is where you get involved, helping Linus unravel Jack's plot. Please review the story above, the VoIP server log, and the packet capture file to answer the following questions.

Questions:

- 1) What was the purpose of Jack's commands shown above?
- 2) What was Jack's big plan?
- 3) What tools and techniques could Jack have used to implement the whole attack, particularly the ability to listen to conversations in real time, and to inject his message with precision? Please be specific and chronological.
- 4) How could Linus have defended the infrastructure against Jack's tactics?

5) How can Linus set things right?

Remember, read the challenge, answer the questions, and send your response in by January 3, 2011 to skillz1210 (at) ethicalhacker.net. We'll choose three winners, each of whom will get an autographed copy of my Counter Hack Reloaded book. One prize will go to the best technical answer, another to the most creative answer that is technically correct, and the final prize is a random draw from every person who submits an answer.

Happy Holidays!

--Ed Skoudis & Yori Kvitchko

Happy Holidays!!