The Forensic Adventures of Scapy the Elf.

By Brian Finn

December 29, 2011

It was a particularly snowy day at the North Pole, even by North Pole standards. Scapy the elf was chatting with his friend Skippy over mugs of hot chocolate. Skippy was taking a break from the frenetic toy-making that went on just before Christmas. Scapy, while a competent toy maker, was fascinated with computers and security. Santa put in a good word with the North Pole CISO, and got Scapy an apprenticeship there. He was doing well in his training in the forensics division. Suddenly the VOIP phone rang:

"Scapy the Elf", answered Scapy.

"Uh huh. Yes. Oh goodness! Yes, sir! Send that packet capture right over and I'll get to work on it!" said Scapy into the phone.

"What's going on?" asked Skippy.

"Christmas Crackers!" exclaimed Scapy. "Rudolph has been implicated in a murder! He's accused of killing somebody's Grandmother!"

Skippy dropped his hot chocolate in surprise, unable to process this information.

"Santa is sending over a packet capture from the lady's computer. He thinks Rudolph is innocent. After all, the lady is on the Naughty list." said Scapy.

"Great Gumdrops!" exclaimed Skippy. "Do you mind if I watch after I clean up this mess? I've always wanted to see what you were up to over here."

"Sure, if you like." said Scapy.

Skippy cleaned up the hot chocolate in a hurry and rushed back to sit next to Scapy at his ElfBook laptop. They were waiting for an email from Santa. Finally, it arrived:

TO: Scapy scapy@northpole.org
FROM: Santa thebigredone@northpole.org
SUBJECT: Grandma's packet capture
ATTACHMENT: Evidence.pcap

Scapy saved the packet capture to his hard drive and opened up Wireshark, his favorite protocol analyzer.

He began to skim through the information, watching the packets go back and forth from the computers in his mind. “Ooh, there’s an SMTP transmission” said Scapy. Seeing the confusion on Skippy’s face, he clarified “Somebody sent an email”.

“Oh!” replied Skippy, “Can we see it?”

“Yes”, said Scapy as he right-clicked on a packet and selected “Follow the TCP stream”.

220 mail.gma ESMTP Postfix

EHLO [192.168.1.10]

250-mail.gma250-PIPELINING250-SIZE 10240000250-VRFY250-ETRN250-ENHANCEDSTATUSCODES250-8BITMIME250 DSN
RSET
250 2.0.0 Ok
MAIL FROM:<root@grandma.gma> BODY=8BITMIME
250 2.1.0 Ok
RCPT TO:<cousinmel@mail.gma>
250 2.1.5 Ok
DATA

354 End data with <CR><LF>.<CR><LF>

Date: Sun, 25 Dec 2011 07:42:26 -0500 (EST)From: Grandma <root@grandma.gma>X-X-Sender: root@btTo: cousinmel@mail.gmaSubject: ChristmasMessage-ID: <alpine.DEB.2.02.1112250741440.7396@bt>User-Agent: Alpine 2.02 (DEB 1266 2009-07-14)MIME-Version: 1.0Content-Type: MULTIPART/MIXED; BOUNDARY="0-471592043-1324816946=:7396"
This message is in MIME format. The first part should be readable text, while the remaining parts are likely unreadable without MIME-aware tools.
--0-471592043-1324816946=:7396Content-Type: TEXT/PLAIN; format=flowed; charset=ISO-8859-7Content-Transfer-Encoding: 8BIT
Dear Mel,
Our plans are almost complete, and I am very excited. Soon, you and I shall be spending the rest of our days relaxing in the surf and sun!
The plan is highly sensitive, a deep secret that only the two of us share. Never tell another soul about our clever scheme as long as you live.
As we discussed, I recently made you the sole beneficiary of my life insurance policy. On Christmas Eve, I plan on faking my own death, whi
ch I will frame as murder on Rudolph, Santa.s obnoxious reindeer.
The details of my plan are included in the attached document below. Read it carefully.
Merry Christmas!Grandma
--0-471592043-1324816946=:7396Content-Type: APPLICATION/msword; name=LetterToMel.docContent-Transfer-Encoding: BASE64Content-ID: <alpine.DEB.2.02.1112250742260.7396@bt>Content-Description: Content-Disposition: attachment; filename=LetterToMel.doc

“Santa’s Sleigh!” exclaimed Skippy. “Grandma faked her death to cash in on her life insurance policy!”

“It looks that way.” said Scapy. “No wonder she’s on the Naughty list. It looks like she attached some directions in a Microsoft Word file.”

“That’s a file? It looks like Mrs. Claus’ cat typed it.” said Skippy.

“No, it’s base-64 encoded.” said Scapy. “So it can be transferred across the Internet using the mail protocol. I can extract it though and turn it back into a regular file.”

Scapy fired up Network Miner and extracted the file. It was still base-64 encoded, so he used the base64 tool to decode it and transform it back into binary file. Finally, he opened it in Word:

Dear Mel,

Here are the details of my secret plan.

After the investigation turns up the evidence I plant, you provide eyewitness testimony in court, and Rudolph is convicted, you will receive the insurance payout. We can then use that money to fund our Caribbean retirement.

I am not sure I ever told you this, Mel, but as a child, my village was attacked by a ravenous band of rampaging reindeer, instilling a life-long hatred in me for the flea-bitten beasts. I’ll never forget their horrible ***comment***s as they galloped through our village. Because of that chilling childhood experience, I’m going to fake my death and blame it all on Rudolph, the most well-known reindeer of all. He’ll rot away in jail forever.

Merry Christmas,

Grandma

“Peppermint Patties!” exclaimed Skippy. “She got this Mel guy to plant evidence and receive the life insurance money!”

“He’s on the Naughty list too.” said Scapy.

“Why is the ‘comment’ part of ‘comments’ written in bold?” wondered Skippy aloud.

“Hmm…” thought Scapy. “I wonder if Grandma is trying to direct Mel’s attention to something else. Let’s look at the comment properties of this document.”

Scapy brought up the document meta-data and discovered:

Author: Grandma

Title: Dear Mel,

Comments:

I will hide out at the Plaza Hotel near Central Park for several weeks, and meet you there in the lobby exactly one week after the trial concludes with a guilty verdict for Rudolph, precisely at noon local time. Make sure you bring the money in a suitcase full of cash. I'll be wearing one red shoe.

"Crackling Candy Canes!" yelled Skippy. "She's hiding out in the Plaza Hotel. She's probably there right now!"

Scapy picked up his Elfatel 530 VOIP phone and let Santa know the important information they just discovered.

"Santa is calling his contacts at the NYPD right now." said Scapy. "All right, let's figure out what else is here."

Scapy started scanning the packets in the packet capture. He looked at some of the HTTP packets.

"It looks like Grandma found the Naughty and Nice web form." said Scapy. A look of concern then crossed his face. "Oh no, that form is vulnerable to a SQL injection attack."

"Is that like injection molding?" asked Skippy.

"No, it's completely different. Grandma is being tricky and adding database commands to the names to search for in the Naughty or Nice list. The database thinks that she is the database administrator, and is giving her information she isn't supposed to have access to." explained Scapy.

"Like what?" asked Skippy.

"Well, see here." Skippy pointed to a packet on his eLfCD screen. "There she asked the database server for a list of databases, and the server just handed over the list!"

"information_schema, mydns, mysql, naughtylist" read Skippy from the screen.

"There she is asking for Start Of Authority table information from the mydns database." said Scapy. "That means that our DNS server is the authority for asking about the santaslist.northpole domain."

"She shouldn't be able to see that information, but I don't see the harm in that." said Skippy.

"Well, if she can read information, she can also add or change information too." said Scapy.

"Oh…..OH!" said Skippy.

"I think you've got it now." said Scapy.

"With the SQL injection flaw, Grandma changes our DNS server to be authoritative for 'apple.com'. Then she adds resource records for 'itunes.apple.com', 'ax.init.itunes.apple.com',

‘swcatalog.apple.com’, ‘swcdn.apple.com’, and ‘swscan.apple.com’. They all point to her machine at 192.168.1.10.”

“So our computers will think that her computer is really Apple’s computers.” said Skippy as he followed along.

“Right.” said Scapy. “Look, what happens next.”

“Rudolph is trying to use iTunes!” said Skippy, a little too loudly.

“Right again, my excitable friend. Grandma’s computer is telling Rudolph’s that there is a new version of iTunes that he should download and run. I bet that’s not really iTunes.” said Scapy.

“It’s…..NAUGHTYWARE!” yelled Skippy.

“Yes!” said Scapy seeing the gravity of the situation sink in with his elf buddy.

“What does it really do?” asked Skippy.

“It opens a shell from Rudolph’s computer to Grandma’s computer” said Scapy. Seeing a quizzical look on Skippy’s face, he added “It lets Grandma run commands on Rudolph’s computer.”

As the horror of this sank in with Skippy, Scapy continued “This is the really, really naughty part. Grandma navigates to Rudolph’s Apple iTunes Backup directory. She downloads sqlite3.exe which lets her look at the geo-location data on Rudolph’s phone”.

“That information is just a list of where Rudolph has been, right?” asks Skippy.

“Yes.” replied Scapy. “However Grandma also uses it to add the coordinates of Central Park in New York City.”

“So, the police will think Rudolph was really there! That’s super sneaky!” exclaimed Skippy.

“You bet.” said Scapy. “Then she deletes the sqlite3.exe file and lets everybody think that Rudolph committed a horrible crime.”

“We have to tell Santa!” yelled Skippy.

“Already on it.” Scapy picked up his VOIP phone and made a call to Santa and explained how Grandma framed Rudolph and about her insurance fraud. Scapy then hung up the phone and sent the details of his analysis to Santa and his boss in the forensics division. He also called a developer elf in the web division to them know about the SQL injection flaw.

“Is that it?” asked Skippy.

“I think so. For now anyway.” answered Scapy.

“Gee, it seems exciting here in the forensics division.” said Skippy.

“It’s not always like this.” answered Scapy. “Last week I was in a chain of custody class. Sprinkles the Elf is a good teacher, but he can get sidetracked pretty easily.”

Skippy said “Hey! Do you want to take a break and make some toys with me? We’re working on some exciting things in the toy foods department.”

Scapy smiled and said “Sure, that sounds like fun.”

The two friends grabbed another mug of hot chocolate and sauntered off in search of elves who were making realistic, yet inviting toy rutabagas, secure in the knowledge that Grandma and Mel would soon be headed for Riker’s Island.

The End.

(Oh, and Skippy says “Merry Christmas!”)