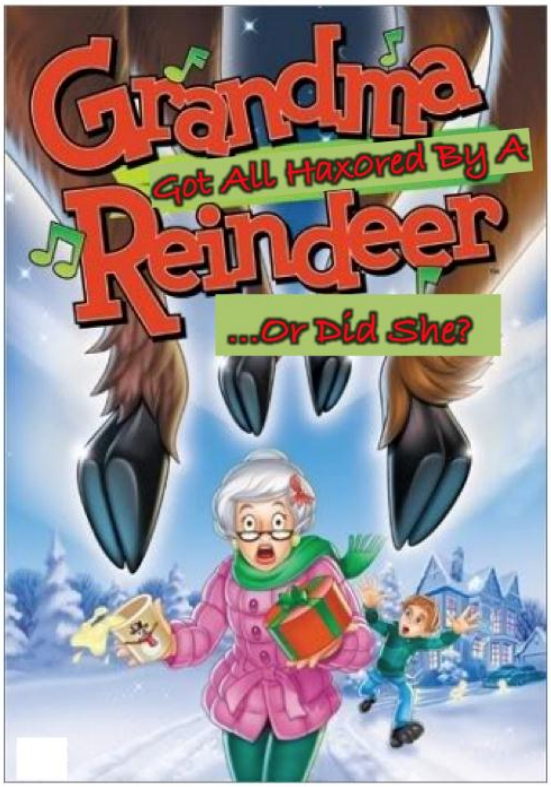


"…But you're… ah…"

**"…Seasonal employee?"**

"…ah…"

"**...migrant worker?**"

"…ah…"

**"… SANS Certified Information Security Professional?"**

"…ah….a talking reindeer…"

**"Yes…. I am also one of those. Though to be honest, after mastering flying, most of us don't find learning to talk that big of an accomplishment. I understand even some humans can manage it fairly well."**

"…Ah….Yes…ah…Well Mr. Donner…"

**"Call me Donny."**

"…You are here as an expert witness for the defense…?"

**"Yes"**

"…As an information security professional…"

**"A SANS Certified information security professional. I have GCFA, GCIH as well as GCIA to name a few."**

"…a few of what???"

**"Certifications, of course. I have completed a number of certifications, however I believe the most relevant here would be my work in the areas of Certified Forensic Analyst, Certified Intrusion Analyst and as a Certified Incident Handler"**

"…SANS certifies *REINDEER*???"

**"They certify… *PROFESSIONALS*… and only after a course of study and rigorous testing. Fortunately, since my formal work schedule is 24 hours on and 8736 off I have had time train and assist our operations team in others areas. It not just 'reindeer games' in the off season you know."**

"…So you studied information security???"

**"Yes. Most reindeer tend to study either particle or theoretical physics, but I preferred a challenge."**

"…Particle or theoretical…physics???"

**"Yes. Someone had to figure out how we could fly and deliver presents to the entire 'nice' world in a single night and… well… *your* physicists have not made much progress in that regard to date…"**

"…Ah….Yes….Well to the matter at hand then… The defense attorney believes that you have uncovered evidence regarding this case that supports the innocence of Mr. Rudolph."

**"Not supports…Proves. Rudy may be a gullible kid, but he's no killer. It was all part of the old lady's plan."**

"Well then I am afraid that there are four key questions that would have to be answered in order to clear him."

**"And they are?"**

"First, just what was Grandma's grand plan for Christmas day?"

**"A forensic analysis of Grandma's USB token showed it all. (More people get into trouble leaving those things laying around….) Well, anyway, it proves that between at 7:51 and 7:59 AM on the morning of December 25th Grandma put into motion a carefully prepared scheme to frame Rudy and then went into hiding."**

"You claim a grandmother did all this?"

**"Yes, there is no age limit on skill any more than there is a 'species' requirement."**

“You claim a 73 year old grandmother did all this in under ten minutes?”

**“Yes… I believe we may finally know the fate of the missing RTD.”**

“RTD?”

**“Ah….yes… RTD… Reindeer Time Dilator… It allows an individual, and whatever they are connected to, to escape certain ‘constraints’ of physics. Properly used an RTD allows us to pull a sleigh through the air around the entire world in a single night. But in this case it allowed Grandma to communicate her entire plan to her partner, infiltrate the North Pole information infrastructure, craft and plant a reasonably sophisticated piece of malware and exploit the security vulnerability it provided, all in about nine minutes of real-time.”**

“And where would she have gotten this… RDT?”

**“About sixty years ago the boss had to let a couple of my coworkers go. Fellows by the names of “Rocky” and “Rekko”. They claim it was because their names did not rhyme… (They were replaced by “Dancer” and “Prancer”.) Officially our RR department says they were released because of equipment loss. Apparently an RDT went missing around the time of their last *outing*“**

“…RR department…”

**“Yeah, “Reindeer Resources” , sort of like your HR department, only more humane. Anyway, most of us kind of think it was a combination of poor hygiene and a generally bad attitude that finally pushed the boss to take action. Basically they were kind of flea-bitten and given to post-christmas rampages through some random village during the ‘naughy nice gap’.”**

“Naughy… nice… gap?”

**“Ah… I probably shouldn’t have said that... It’s kind of a sore point with management. Our behavior tracking software had a glitch that dated back to when it was first installed that caused it reset at midnight on New Years’ day… So basically you could get away with being pretty Naughty between Christmas and New Years and not have it count against you. It *finally* got fixed back during the Y2K upgrades… but between you and me I think the boss still cuts us all a little slack during the holidays…”**

“So you have no actual evidence that she has this… device….”

**“Well I certainly don’t see how she could have accomplished what she did in such a short time without it. Or how a 73 year old lady would have kept a 23 year old Cousin Mel *entertained* without a little something extra going for her…”**

“Well then why did the geo-location data on Rudolph’s computer downloaded from his cell phone, place him in Central Park at the time of the attack. Please explain each step that lead up to that.”

**“Well first off, there is no way Rudy should have been walking around with an iPhone. Santa banned us from carrying those the year they came out after he got a $1,234,523 bill for international data**

**roaming charges after D-Day…(That's Delivery Day… or night as the case may be…) Anyway after that Santa said "it's prepaid cell phones or nothing…." (and he ordered an extra load of coal as stocking stuffers for some telco executives…) Anyway I think the old lady must have gotten the phone to Rudy in the last couple of weeks and somehow conned him into carrying it. She needed it to frame him."**

"A frame that you have yet to provide any details of…"

**"You wants details…**

**At 7:51 the packet trace shows she shared her plans with this Mel by email, both for the frame-up and their later rendezvous.**

**By 7:52 She confirmed that the Naughty/Nice web site was still in place and that her and Mel's status were…well… unfavorable. So she began her attack. The fact that the site was vulnerable to SQL injection is not really surprising. Even at the North Pole the InfoSec guys are there 'to explain' and 'to blame' when things go wrong, not to set and enforce policy. Since the database had been in use for years as an in house app it was considered secure even though no one had ever tested it… Not to mention the new customer facing web interface someone tacked on to it… but when the Big Man gets an idea and deadlines are close, everybody just kind of falls into line. Someday they will start taking InfoSec seriously…and someday pigs will fly….. (Flying pigs, what a silly idea…)**

**Anyway by 7:52 mal formed URL requests and SQL injection attempts were coming fast and furious and by 7:53:42 she had inserted a bogus DNS entry for apple.com.**

"And it was this… RTD… that made all this possible so quickly?"

**"Sadly no. While it's not quite as easy as it looks in the movies, a skilled hacker who has taken time to plan can accomplish a lot in an amazingly short period of time.**

**By 7:54 the old lady had tweaked an iTunes "update" executable to deliver a little extra 'holiday magic' in form of "Backdoor.Bifrose". After that she just had to wait for Rudy to walk into her trap. That's where the RTD really came into play. You remember I said it can effect time for the person using it and whatever they are connected to? Grandma was connected to the North Pole IT infrastructure, so she had all the time in the world to wait for Rudy to fire up iTunes.**

**Because of the bogus DNS entry, at 7:57:54 Rudy's PC *attached to her machine* to download and install the doctored iTunesSetup.exe. It seems that *someone* had left Rudy a couple of the $50 special edition Beetles iTune gift cards under the tree. Since we had started blocking torrents and Usenet at the proxy server a while back, the kid was kind of a sitting duck."**

How is it that Grandma seemed to have such ready physical access to pass along these gifts?

**"I don't think a reindeer would look very good in a blue blazer. That's why I went into INFORMATION security instead of PHYSICAL security. If you want an answer to that question, you will need to ask someone who carries a flashlight.**

**Anyway, by 7:58 Rudy's malware infested machine was calling hers and she was off and running. In less than a minute she was able to remotely login back into her own ftp server and pull a copy of sqlite3.exe down to Rudy's machine. She quickly preformed a silent install and by 7:59 was already using that application to insert false geo-location information into the backup copy of the data from his phone stored on Rudy's PC. And she probably was not really using the RTD much by then, although it can really improve download speeds and install times on Windows XP…**

**From there, for Grandma, it was just a walk in the park, so to speak…. Not that she actually went to Central Park… that just was just part of the frame-up."**

**"**So where do you think we should look for Grandma?**"**

"**Well her email referred Mel to a document attachment. And while the *text* of the document of the document did not really give any clues, if you check the comments you would find that she expected Mel to meet her in the lobby of the Plaza Hotel at noon one week after Rudolph is found guilty… Which I don't think is to likely now…. But it sounds like she was set to hold up there for several weeks till that happened…**"

"So who do you believe is guilty?"

"**Well it certainly looks like the old lady pulled off the hack. And Mel contributed his acting skills to sell the frame. Those are certainly the criminal elements. But the IT department up North should have done a better job protecting critical infrastructure. Maybe even Santa shares some of the blame for pressuring them to push a new service into production without proper testing. Even Rudy could have foiled the plot if he had kept the anti-virus software up to date on his computer.**

**And anyone getting electronics from unknown sources should show a little caution before hooking them up to their computer and installing lots of updates. Sometimes it really is a good idea to look a gift horse in the mouth… (Although why anyone would even accept one of those mangy beasts as a gift…)**

**Maybe now management will finally back a proper IT Security audit…. That really would be a Christmas Miracle…**"