Rich Cassara
@rjcassara

It was the biggest job I'd ever been offered. I thought it was impossible to pull off…that kind of hack, against that level of security? You'd have to be crazy to accept.

Call me crazy.

I don't know if was for the challenge of it, the potential windfall, or the target's comeuppance; but I had to try.

Thankfully, it was an inside job. Without the knowledge coming from inside the organization, I wouldn't have gotten past square one.

So how would we get Scrooge, one of the most notorious blackh(ear|a)t hackers around, to succumb our social engineering experiment and renounce his malicious tendencies?

There was only one thing that could work…we had to scare the Dickens out of him.

STAVE 001 - THE SETUP:

Though he was a rational man, Scrooge harbored quite a few superstitions. We settled on using the ghost angle, so our first investment was in top-of-the-line holographic projection equipment. With that in hand, we decided to start him off with a visit from his beloved old server. Mrs. Lynn Crachit, Scrooge's clerk, had kept EXCELLENT inventory records of the technology Scrooge employed, so it wasn't too difficult to set up a machine that looked just like his old one. We spoofed the MAC and IP addresses, and used the keypair she had archived. Then we just had to create an account for Scrooge with his public key, and fake it's last login date. We prepared the server room with the holographic projections and

brought the box online.

After Scrooge got the MOTD we killed the box so he couldn't dig too deeply into it and discover the ruse. He went to the server room as expected, and when the door was opened it triggered our holographic display to begin. I even threw in a phantasm of my Lumia 928 that I just traded in for an iPhone 6. Now that the stage was set, the real show could begin.

STAVE 010 - THE FIRST "GHOST":

For the apparitions and visions we had planned out to finish out our hack on Scrooge's brain, the holographic projectors weren't going to be enough. So we created some custom software and acquired the latest iteration of the Occulus Rift from a good friend who happened to have access. It's gotten very lightweight, and we thought Scrooge wouldn't notice the VR helmet when aroused from deep sleep. To be safe, we had his maid slip some extra-strength Nyquil into his evening tea, then she strapped on the helmet while he was asleep.

The first "ghost" arrived, and scrooge found himself in a vision we had programmed just for him. When the animated image of Turing handed him a slip of paper, we had to have precise timing to have his maid give him a piece of paper with the IP address of the server written on it, then swiftly remove the VR headset and disappear (we used some old magician's tricks: smokebombs and a hollowed out space under his floorboards we created when he was on a business trip a month back). We set up a simple ELIZA chatbot at the IP address for him to find on port 31124 (we assume he did a full port scan with nmap). Once connected we knew he would have to solve the puzzle…the curiosity of a hacker is insatiable. He quickly found the keywords to trigger non-stock answers from her. He'd have to enter "secret", "puzzle", "game", or "enigma" three times before she would request a website to "surf" to. But, he'd also have to unlock her ability to visit links by referencing Dr. Turing twice. (Entering "Turing test", however only resulted in an easter egg we found amusing). The second time, the bot would pull Turing's Wikipedia entry, and only

then could Scrooge send her to arbitrary locations. After he figured out to use her own words, "surf to http://****", he poked around a bit - figured out he could crash the session by sending her to her own address and port - then finally sent her to his own webserver where he had access to the logs. Then he read our first message in her browser identification:
Eliza Secret: "Machines take me by surprise with great frequency. - Alan Turing"

STAVE 011 - THE SECOND "GHOST":
After passing out into a deep slumber again, we prepared for the second ghost. This time, we skipped the VR setup. Johnny Long was flown in from Africa to appear before Scrooge in person. He shared our vision of a world where Scrooge used his computer skills to make lives better. We had made a video recording of Mrs. Crachit and Tiny Tom, and used a scrim and the latest smell-o-vision technology to project the deli scene into Scrooge's room. As for the website, it was trivial to "hack" when Scrooge's own staff was in on it. They simply didn't patch against some of last year's biggest exploits: Heartbleed and Shellshock. However to do nothing at all about those exploits would be very dangerous, so we worked together to carefully limit what information could be accessed…only the secrets for Scrooge to find. For the Heartbleed vulnerability we made sure to always have the secret inserted into the viewable memory space of the server, so when Scrooge launched an attack on the site he would see:
Website Secret #1=Hacking can be noble.

(Scrooge had built his own POC for Heartbleed months ago, but he could have easily found one on github had he wanted to)

The Shellshock vulnerability was trickier to set up, but we settled on a highly restricted shell, with no escape possible (to the best of our knowledge). The secret was set in the root directory, but without any file reading capabilities, how would Scrooge see what we wanted him

to see? After recognizing the vulnerability, Scrooge simply made requests using curl and altered his User-Agent string to "(){ foo;};echo;<commands>", where <commands> were the shell commands he tried to execute. Sending the "help" command to the shell was his biggest asset, since it showed which limited set of commands were allowed. Without "ls", he resorted to using "echo *", a neat trick that he had read about on the SANS Penetration Testing site (http://pen-testing.sans.org/blog/2012/06/06/escaping-restricted-linux-shells). On top of that, he found he could set shell options, so by executing "shopt -s globstar" he could then run "echo **" from the root directory and see everything available on the system. Ultimately, he needed to get that secret, and figured the best way was to set a variable equal to the file contents and then print out the variables. He appended this to the initial Shellshock string of his User-Agent:

```
cd /; declare input=$(<secret);declare;
```

Then he saw our second website secret:
Website Secret #2: Use your skills for good.

STAVE 100 - THE THIRD "GHOST":
To prepare for the final vision, we really had to pull out all the stops. If we didn't succeed, all of our efforts would have been for naught. I took point and dressed in a long black cloak. I'd written to the USB drive from a machine with the clock set 20 years into the future to set the illusion. The biggest challenge was the transition. We carefully carried the passed-out Scrooge into a nearby graveyard, but how would we "magically" whisk him back to his bedroom?

In a feat of engineering and a dash of good luck, we successfully did it with a trebuchet.

As for the USB drive, the first secret I left out for him pretty

trivially. Looking at the raw data of the document that celebrated his death with a hex editor, he could easily find:

USB Secret #1: Your demise is a source of mirth

The second file he could immediately see was a network capture (again, spoofed to take place 20 years in the future). Scrooge could read a husband and wife discuss their massive debt to him and how it would all be better now that Scrooge was dead. With his ever careful eye, Scrooge noticed some packet comments when he viewed expert info in Wireshark, one of which contained a base64 encoded string (VVNCIFNlY3JldCAjMjogWW91ciBkZW1pc2UgaXMgYSBzb3VyY2Ugb2YgcmVsaWVmLg==). When decoded he saw:

USB Secret #2: Your demise is a source of relief.

The other packet comment was a link to the f5 steganography algorithm (https://code.google.com/p/f5-steganography/), which he would have to use for the fourth secret. But first, while examining the raw data of the USB drive with his hex editor, Scrooge discovered two more files not immediately available. The first was a compressed file locked with a password. Scrooge had a number of cracking dictionaries available and easily decompressed bed_curtains.png using the zip2john extension of John the Ripper. (We had Johnny try to lead him to this answer as well, since if CeWL were used on Scrooge's website one would easily find the password - shambolic. However, it's hard to differentiate CeWL from cool when spoken.) Once decompressed, Scrooge found the third secret in the raw data of the file:

USB Secret #3: Your demise is a source of gain for others.

Finally, Scrooge found the jpg file of Tiny Tom's crutches. He rightfully assumed it had a secret hidden via steganography, and having seen the packet comments, he downloaded the f5.jar and

easily extracted our final secret:

USB Secret #4: You can prevent much grief and cause much joy. Hack for good, not evil or greed.

(In testing phases to make sure Scrooge could successfully retrieve the secrets with the proper amount of effort, one of our testers got stuck working on the jpg before seeing the packet comments. This lead to some custom scripting to use a dictionary file with Steghide to try and brute force their way in.)

STAVE 101 - CONCLUSION:

In the end it went off almost exactly as planned. The experiences we crafted for Scrooge changed his outlook on hacking and life. His employees were happier and more productive, his family welcomed and enjoyed his company, Scrooge himself was happier and took more pride in his own work, and the world was better off. I had never cared much for working with wetware, but hacking Scrooge's brain was one of the most fulfilling jobs I'd ever done.
In fact, I don't think we had actually hacked him, but instead removed some particularly nasty malware that was corrupting his true self.

It was truly a Christmas miracle.