pugpug's 2020 Holiday Hack writeups

Intro

One bright spot in 2020 was the annual Holiday Hack Challenge put on by SANS. This year Santa opened his newly renovated castle to the world. However, all was not merry and bright at the North Pole, as nefarious powers are working against Santa and his elves. Our job in the challenge is to solve the mystery of who is behind the problems the elves are experiencing and bring them to justice. As we progress through the castle we'll investigate such topics as why public S3 Amazon buckets aren't a good idea, dig into CAN-BUS traffic, discover why "pseudo-random number generators" aren't truly random, and why one shouldn't use MD5 as a hash algorithm.

Organization

This writeup covers all of the objectives (yes, even 11b!), but not necessarily all of the elf terminals or other non-objective challenges. I'll include any sample code I used to complete the objectives in a separate section.

Objectives & Answers

1. Uncover Santa's Gift List: `Proxmark`
2. Investigate S3 Bucket: `North Pole: The Frostiest Place On Earth`
3. Point-of-Sale Password Recovery: `santapass`
4. Operate the Santavator
5. Open HID Lock
6. Splunk Challenge: `The Lollipop Guild`
7. Solve the Sleigh's CAN-D-BUS Problem:
8. Broken Tag Generator: `JackFrostWasHere`
9. ARP Shenanigans: `Tanta Kringle`
10. Defeat Fingerprint Sensor
11. Naughty/Nice List with Blockchain Investigation Part 1: `57066318f32f729d`
12. Naughty/Nice List with Blockchain Investigation Part 2: `fff054f33c2134e0230efb29dad515064ac97aa8c68d33c58c01213a0d408afb`

> **Note**
>
> Four of the objetives don't require answers to be submitted. Instead, the objectives are completed by operating the elevator, opening a locked door, fixing Santa's sleigh, and bypassing a fingerprint sensor