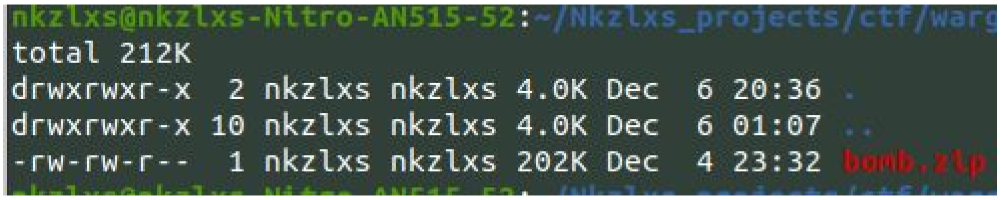
Wargames MY 2020 write-up

Category: Miscellaneous (a.k.a. Misc)

Challenge Name: Defuse The Bomb!

Introduction

In this challenge we're presented with a zip bomb, which we think by unzipping it, will cause an explosion bigger than the one that happened in russia roughly 59 years ago.



```
nkzlxs@nkzlxs-Nitro-AN515-52:~/Nkzlxs_projects/ctf/warg
total 212K
drwxrwxr-x  2 nkzlxs nkzlxs 4.0K Dec  6 20:36 .
drwxrwxr-x 10 nkzlxs nkzlxs 4.0K Dec  6 01:07 ..
-rw-rw-r--  1 nkzlxs nkzlxs 202K Dec  4 23:32 bomb.zip
```

Tools used

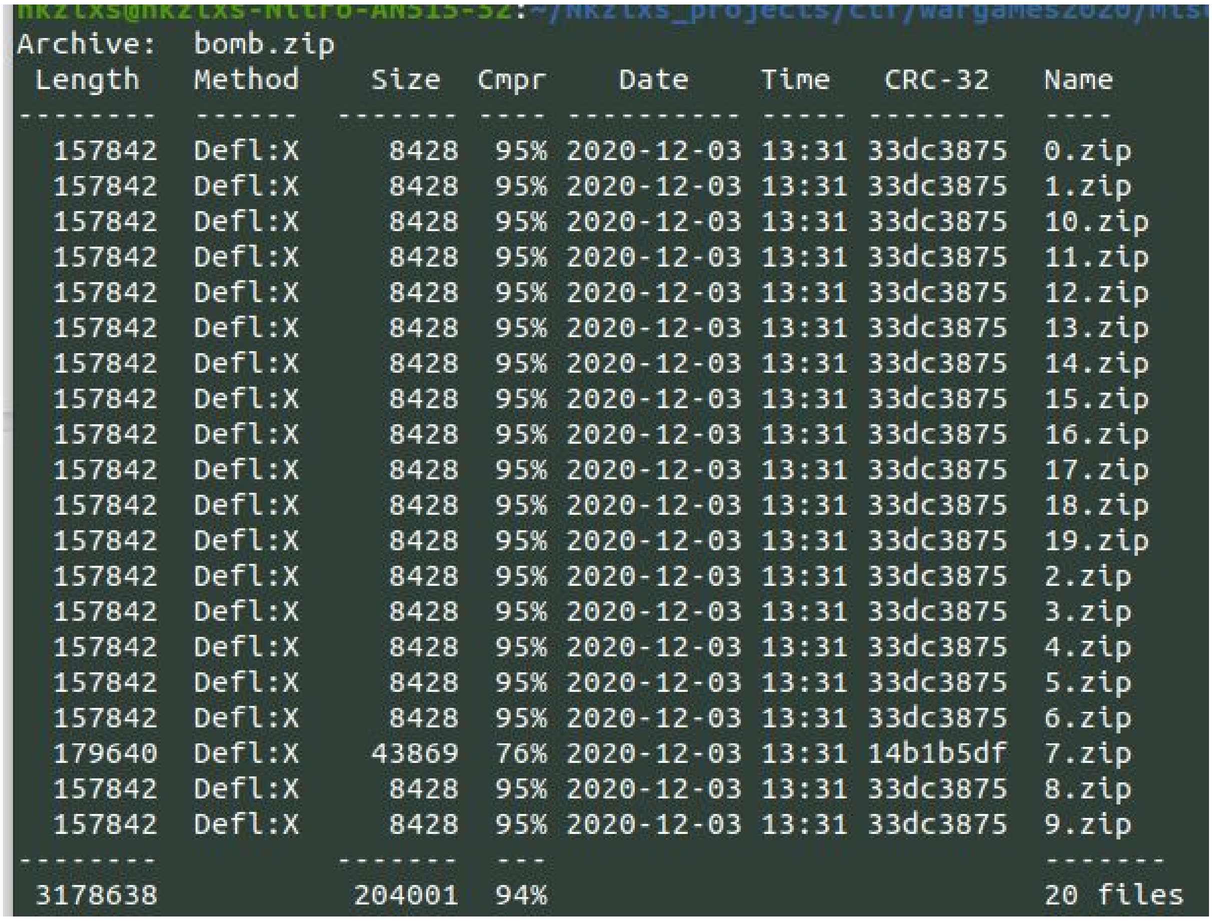
1. Unzip - from ubuntu 20.04
2. Grep - from ubuntu 20.04

Getting more information and get the flag

Let’s get more information about the zip file with the command:

```
unzip -v ./bomb.zip
```

Here are the outputs:



```
nkzlxs@nkzlxs-Nitro-AN515-52:~/nkzlxs_projects/ctf/wargames2020/mis
Archive:  bomb.zip
 Length   Method    Size  Cmpr    Date    Time   CRC-32   Name
--------  ------  ------- ---- ---------- ----- --------  ----
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  0.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  1.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  10.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  11.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  12.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  13.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  14.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  15.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  16.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  17.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  18.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  19.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  2.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  3.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  4.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  5.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  6.zip
  179640  Defl:X    43869  76% 2020-12-03 13:31 14b1b5df  7.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  8.zip
  157842  Defl:X     8428  95% 2020-12-03 13:31 33dc3875  9.zip
--------          -------  ---                            -------
 3178638           204001  94%                            20 files
```

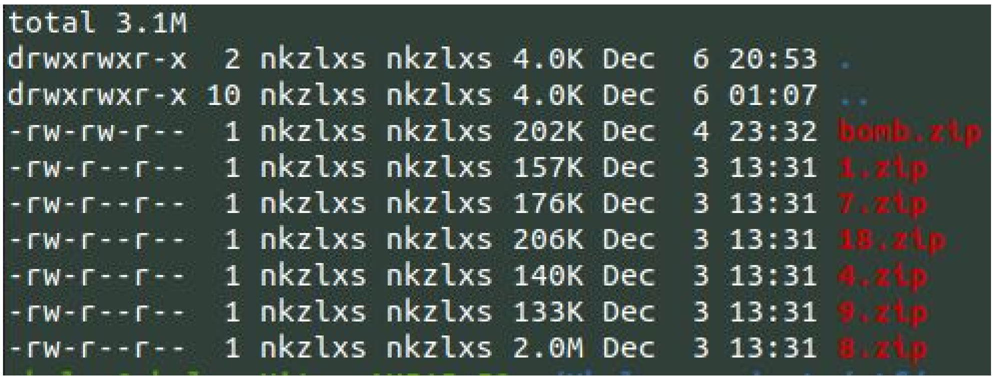
As we can see, 7.zip’s file size is particularly larger than others. And its CRC-32 value is not the same too.

It turns out that for every zip file in the zip there is one zip file that is significantly larger and its CRC-32 value is not the same.

So let’s unzip only the file which appears different.

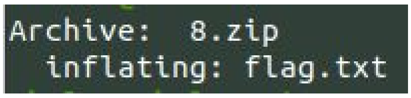
```
unzip bomb.zip 7.zip
```

In the end, we will get 6 extra files by doing so. The last one will be 8.zip in this case.



```
total 3.1M
drwxrwxr-x  2 nkzlxs nkzlxs 4.0K Dec  6 20:53 .
drwxrwxr-x 10 nkzlxs nkzlxs 4.0K Dec  6 01:07 ..
-rw-rw-r--  1 nkzlxs nkzlxs 202K Dec  4 23:32 bomb.zip
-rw-r--r--  1 nkzlxs nkzlxs 157K Dec  3 13:31 1.zip
-rw-r--r--  1 nkzlxs nkzlxs 176K Dec  3 13:31 7.zip
-rw-r--r--  1 nkzlxs nkzlxs 206K Dec  3 13:31 18.zip
-rw-r--r--  1 nkzlxs nkzlxs 140K Dec  3 13:31 4.zip
-rw-r--r--  1 nkzlxs nkzlxs 133K Dec  3 13:31 9.zip
-rw-r--r--  1 nkzlxs nkzlxs 2.0M Dec  3 13:31 8.zip
```

Unzip the last zip, we get flag.txt.

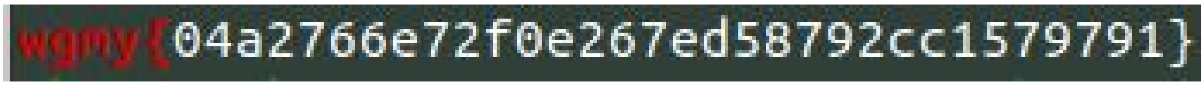


```
Archive:  8.zip
  inflating: flag.txt
```

Last, grep the “wgmy{“ pattern in the flag.txt file to get the flag.

```
grep --binary "wgmy{" ./flag.txt
```

Result:



```
wgmy{04a2766e72f0e267ed58792cc1579791}
```

References:

1. https://github.com/ctfs/write-ups-2015/tree/master/asis-quals-ctf-2015/forensic/keka-bomb