

MacroHard WeakEdge

The following is the question:

MacroHard WeakEdge

60 points

Tags: picoCTF 2021 Forensics

AUTHOR: MADSTACKS

Description

I've hidden a flag in this file. Can you find it? [Forensics is fun.pptm](#)

Hints ?

(None)

13,270 solves / 14,087 users attempted (94%)

76% Liked

Submit Flag

It's a pptm file that contains the flag.

pptx	pptm
It does not contain macros, so is less vulnerable to security risks	Contains macros which makes it more vulnerable to security risks

(source: LifeWire)

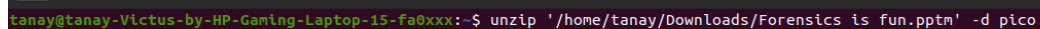
A macro is a small piece of code that automates certain tasks. It is an efficient tool but poses a security risk as they are imported from across the web and may contain malicious code.

I initially opened the pptm file, but it was simply a blank ppt. There was nothing to be found even in the properties of the file.

After some reading about pptx and pptm online, I found that both these files are essentially zipped files.

Since it is a pptm file, not in a bz2 or gz format, none of the tools we learnt about in Bandit will help. Therefore I used the unzip command.

unzip command is a powerful command in linux that can easily unzip and extract zipped files.



```
tanay@tanay-Victus-by-HP-Gaming-Laptop-15-fa0xxx:~$ unzip '/home/tanay/Downloads/Forensics is fun.pptm' -d pico
```

Since we need to store the extracted files somewhere, I created a directory 'pico' for the purpose.

Following is the output:

```

inflating: pico/ppt/slideLayouts/slideLayout11.xml
inflating: pico/ppt/slideMasters/_rels/slideMaster1.xml.rels
inflating: pico/ppt/slideLayouts/_rels/slideLayout1.xml.rels
inflating: pico/ppt/slideLayouts/_rels/slideLayout2.xml.rels
inflating: pico/ppt/slideLayouts/_rels/slideLayout3.xml.rels
inflating: pico/ppt/slideLayouts/_rels/slideLayout4.xml.rels
inflating: pico/ppt/slideLayouts/_rels/slideLayout5.xml.rels
inflating: pico/ppt/slideLayouts/_rels/slideLayout6.xml.rels
inflating: pico/ppt/slideLayouts/_rels/slideLayout7.xml.rels
inflating: pico/ppt/slideLayouts/_rels/slideLayout8.xml.rels
inflating: pico/ppt/slideLayouts/_rels/slideLayout9.xml.rels
inflating: pico/ppt/slideLayouts/_rels/slideLayout10.xml.rels
inflating: pico/ppt/slideLayouts/_rels/slideLayout11.xml.rels
inflating: pico/ppt/theme/theme1.xml
extracting: pico/docProps/thumbnail.jpeg
inflating: pico/ppt/vbaProject.bin
inflating: pico/ppt/presProps.xml
inflating: pico/ppt/viewProps.xml
inflating: pico/ppt/tableStyles.xml
inflating: pico/docProps/core.xml
inflating: pico/docProps/app.xml
inflating: pico/ppt/slideMasters/hidden
tanay@tanay-Victus-by-HP-Gaming-Laptop-15-fa0xxx:~$

```

We see a file 'hidden'. This must contain the flag.
So we change the cwd to that.

```

tanay@tanay-Victus-by-HP-Gaming-Laptop-15-fa0xxx:~$ cd pico
tanay@tanay-Victus-by-HP-Gaming-Laptop-15-fa0xxx:~/pico$ cd ppt
tanay@tanay-Victus-by-HP-Gaming-Laptop-15-fa0xxx:~/pico/ppt$ cd slideMasters
tanay@tanay-Victus-by-HP-Gaming-Laptop-15-fa0xxx:~/pico/ppt/slideMasters$ ls
hidden  _rels  slideMaster1.xml
tanay@tanay-Victus-by-HP-Gaming-Laptop-15-fa0xxx:~/pico/ppt/slideMasters$

```

Now we display the contents of 'hidden'

```

tanay@tanay-Victus-by-HP-Gaming-Laptop-15-fa0xxx:~/pico/ppt/slideMasters$ cat hidden
ZmxhZzZogcGljb0NURntEMWRfdV9rbjB3X3BwdHNfcml96MXA1fQ

```

These characters appear to be encoded in base64.

Decoding them, we get:

flag: picoCTF{D1d__u__know__ppts__r__z1p5}

This is our needed flag.

[Source: RapidTables]