


https://docs.google.com/document/d/1xU0tEZOTS_L8u_S5Fbs1Wof7mdpWQrj2NkgWLV9tqns/edit#heading=h.fjh5ay1eg78k

[Task 17] [Day 12] Elfcrption

12/12/2019



Download

You think the Christmas Monster is intercepting and reading your messages! Elf Alice has sent you an encrypted message. Its your job to go and decrypt it!

Read the supporting materials [here](#).

Objectives

1. What is the md5 hashsum of the encrypted note1 file?
2. Where was elf Bob told to meet Alice?
3. Decrypt note2 and obtain the flag!

The contents of tosend.zip {note1.txt.gpg, note2_encrypted.txt, private.key}

```
root@kali:~/Downloads# ls -al
total 44
drwxr-xr-x  2 root root 4096 Mar 25 03:03 .
drwx----- 27 root root 4096 Mar 25 02:59 ..
-rw-r--r--  1 root root 8475 Mar 24 02:34 gunmetalfrogovpn.ovpn
-rw-rw-r--  1 root root  128 Dec 11 17:16 note1.txt.gpg
-rw-rw-r--  1 root root 1114 Dec 11 17:17 note2_encrypted.txt
-rw-rw-r--  1 root root 7011 Dec 11 17:17 private.key
-rw-r--r--  1 root root 7075 Mar 25 03:02 tosend.zip
root@kali:~/Downloads#
```

1. What is the md5 hashsum of the encrypted note1 file?

```
root@kali:~/Downloads# md5sum note1.txt.gpg
24cf615e2a4f42718f2ff36b35614f8f  note1.txt.gpg
root@kali:~/Downloads#
```

- The md5 hash sum is: **24cf615e2a4f42718f2ff36b35614f8f**

2. Where was elf Bob told to meet Alice?

- Looks like note1 is encrypted with gpg, a symmetric key encrypting program.
- The hint says that the gpg key is 25daysofchristmas; I'm not sure if I could have found that some other way with just the tosend.zip file...
- Decrypting with the gpg program:

```
root@kali:~/Downloads# gpg -d note1.txt.gpg
gpg: AES encrypted data
gpg: encrypted with 1 passphrase
I will meet you outside Santa's Grotto at 5pm!

root@kali:~/Downloads#
```

- Alice told Bob to meet outside **Santa's Grotto** at 5pm!

3. Decrypt note2 and obtain the flag!

- We have a private.key file, part of an asymmetric key pair. The hint says the password is 'hello'

```
root@kali:~/Downloads# openssl rsautl -decrypt -inkey private.key -in note2_encrypted.txt -out plaintext_note2.txt
Enter pass phrase for private.key:
root@kali:~/Downloads# cat plaintext_note2.txt
THM{ed9ccb6802c5d0f905ea747a310bba23}
root@kali:~/Downloads#
```

- The flag is **THM{ed9ccb6802c5d0f905ea747a310bba23}**