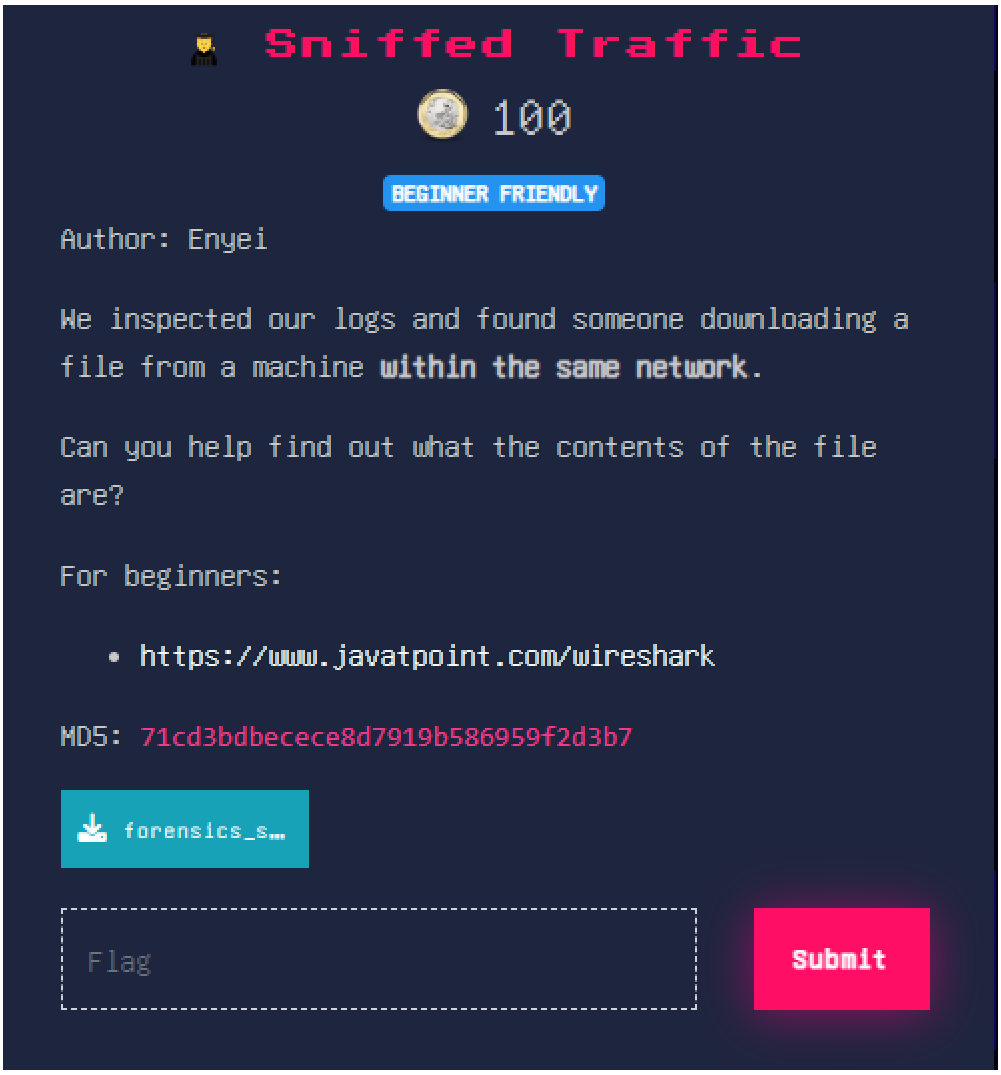
Sniffed Traffic

Event	SEETF 2022
Tags	Forensics
Author	KH Lai

Challenge Description



Sniffed Traffic

100

Author: Enyei

We inspected our logs and found someone downloading a file from a machine **within the same network**.

Can you help find out what the contents of the file are?

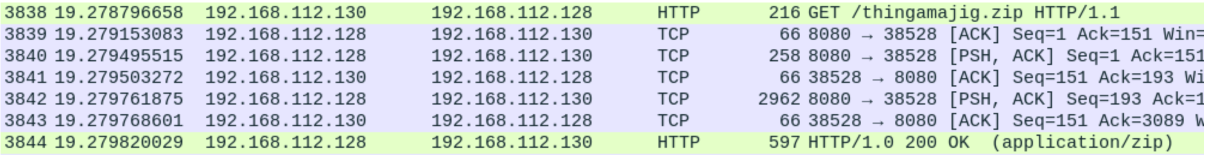
For beginners:

- https://www.javatpoint.com/wireshark

MD5: 71cd3bdbecece8d7919b586959f2d3b7

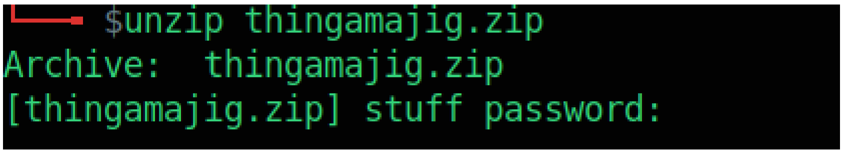
Challenge Walkthrough

We are given a `.pcapng` file and we are supposed to find a particular file that is being downloaded. After going through the packets, we found a HTTP GET request of a `.zip` file thingamajig.zip.



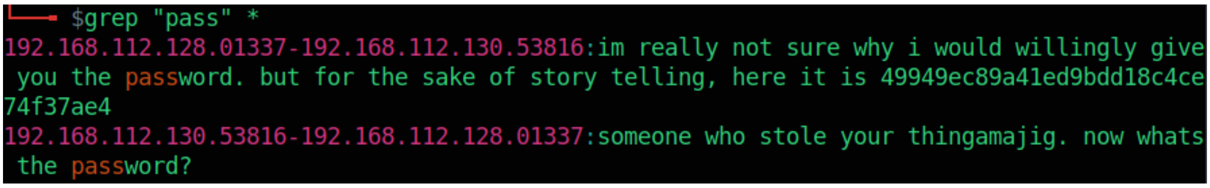
```
3838 19.278796658  192.168.112.130       192.168.112.128       HTTP        216 GET /thingamajig.zip HTTP/1.1
3839 19.279153083  192.168.112.128       192.168.112.130       TCP          66 8080 → 38528 [ACK] Seq=1 Ack=151 Win=
3840 19.279495515  192.168.112.128       192.168.112.130       TCP         258 8080 → 38528 [PSH, ACK] Seq=1 Ack=151
3841 19.279503272  192.168.112.130       192.168.112.128       TCP          66 38528 → 8080 [ACK] Seq=151 Ack=193 Wi
3842 19.279761875  192.168.112.128       192.168.112.130       TCP        2962 8080 → 38528 [PSH, ACK] Seq=193 Ack=1
3843 19.279768601  192.168.112.130       192.168.112.128       TCP          66 38528 → 8080 [ACK] Seq=151 Ack=3089 W
3844 19.279820029  192.168.112.128       192.168.112.130       HTTP        597 HTTP/1.0 200 OK  (application/zip)
```

We can extract the file with wireshark by going to `File > ExportObjects > HTTP`. After obtaining the file, unzipping it tells us that we need a password.



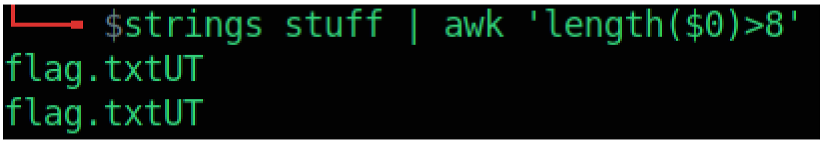
```
└──╼ $unzip thingamajig.zip
Archive:  thingamajig.zip
[thingamajig.zip] stuff password:
```

The password should be either in one of the packets or it will require us to crack it. I first tried cracking the password with JohnTheRipper but unable to get a result. If the password is in one of the packets, we can shorten the search by extracting only the TCP packets with `tcpflow -r [file]`. After getting the TCP packets, we can `grep` the keyword "pass" to see if there is any password hiding in the packets.



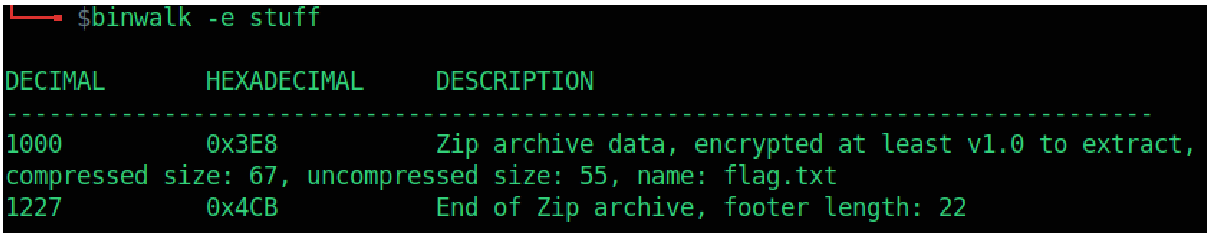
```
└──╼ $grep "pass" *
192.168.112.128.01337-192.168.112.130.53816:im really not sure why i would willingly give
 you the password. but for the sake of story telling, here it is 49949ec89a41ed9bdd18c4ce
74f37ae4
192.168.112.130.53816-192.168.112.128.01337:someone who stole your thingamajig. now whats
 the password?
```

Now we have the password to the file. After unzipping it will give us an unknown file `stuff`. Searching for strings in the file tells us that there is a `flag.txt` embedded within the file.



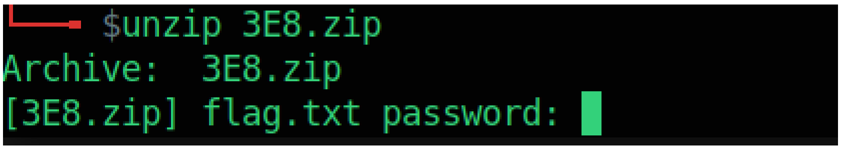
```
└──╼ $strings stuff | awk 'length($0)>8'
flag.txtUT
flag.txtUT
```

We can use Binwalk to extract it.



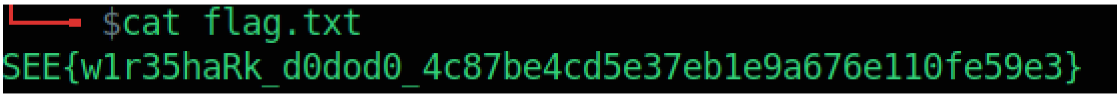
```
└──╼ $binwalk -e stuff

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
1000          0x3E8           Zip archive data, encrypted at least v1.0 to extract,
compressed size: 67, uncompressed size: 55, name: flag.txt
1227          0x4CB           End of Zip archive, footer length: 22
```

Extracting it gives us another zip file which requires another password. This time we can try using JohnTheRipper again. First create the hash for the password with `zip2john [file] > hash.txt`. Then crack the password with `john hash.txt`. The password is john.



```
└──╼ $unzip 3E8.zip
Archive:  3E8.zip
[3E8.zip] flag.txt password: 
```

Flag



```
└──╼ $cat flag.txt
SEE{w1r35haRk_d0dod0_4c87be4cd5e37eb1e9a676e110fe59e3}
```