SECCON for Beginners2018
Misc

[Warmup]plain mail

Write up

問題

- Pcapファイルが渡されるだけ
- タイトル的にメール関係だろうと思いながら進める

解法

- とりあえず、wiresharkでパケットを見てみる。
- するとTCP/SMTP/SMTP | IMFプロトコルのやりとりが確認できる。問題から察するにTCPは関係ないと思われるので、「smtp」でパケットをフィルターする。SMTP | IMFがメールの実態らしいのでIMFをエクスポートする。

解法

- 得られたIMFファイルを除いてみる。
  1.eml:
  I will send secret information. First, I will send encrypted file.
  Second, I wll send you the password.
  「まず、実態あげるね。次にパスワードをあげるよ」的なこと書いてあるので、2.emlがメール本体で3.emlがflagを得るために必要なパスワードなんだろうなとわかる。

解法

- 2.eml:

```
Content-Type: multipart/mixed; boundary="================0309142026791669022=="
MIME-Version: 1.0
Content-Disposition: attachment; filename="encrypted.zip"

--================0309142026791669022==
Content-Type: application/octet-stream; Name="encrypted.zip"
MIME-Version: 1.0
Content-Transfer-Encoding: base64

UEsDBAoACQAAAOJVmOzEdBgeLQAAACEAAAAIABwAZmxhZy5OeHRVVAkAA6f/4Iqn/+JadXgLAAEE
AAAAAAQAAAAASsSDOp8jUFIaCtIYOyp4JcP9Nha32VYd2BSwNTG83tIdZyU4x2VJTGyLcFquUEsH
CMROGB4tAAAAIQAAAFBLAQIeAwoACQAAAOJVmOzEdBgeLQAAACEAAAAIABgAAAAAAAAEAAACkgQAA
AABmbGFnLnR4dFVUBQADp//iWnV4CwABBAAAAAAEAAAAAFBLBQYAAAAAAQABAE4AAAB/AAAAAAA=
--================0309142026791669022==--
```

- これを眺めてると、zipが添付されたメールだろうとわかる。これ、そのままメールソフトで開けばいいんじゃねと思って開いてみたが、何も表示されなかった。

解法

- Content-Type: application/octet-stream;というのが何か調べてみるとファイルの形式を表しているらしく、octet-streamはexeファイルを表すらしい。とりあえずここをzipに直してみる。
- しかし、結果は変わらず。宛先や件名などの情報も必要なのかなと思った。
  ので、gmailで適当なzipファイルを添付したメールを自分に送り、ソースコードをコピペする。そして、zipファイルの本体、base64でエンコードされてる部分をこの問題で得られたものに書き換える。
- すると無事にzipが添付されたメールとして開くことができた。

解法(flag)

- あとは、得られたzipファイルに鍵がかかっているので3.emlの中身に書いてある鍵を入力してzipを開く。flag.txtがあるのでそれを開いて終わり。

  3.eml: _you_are_pro_

  ctf4b{email_with_encrypted_file}