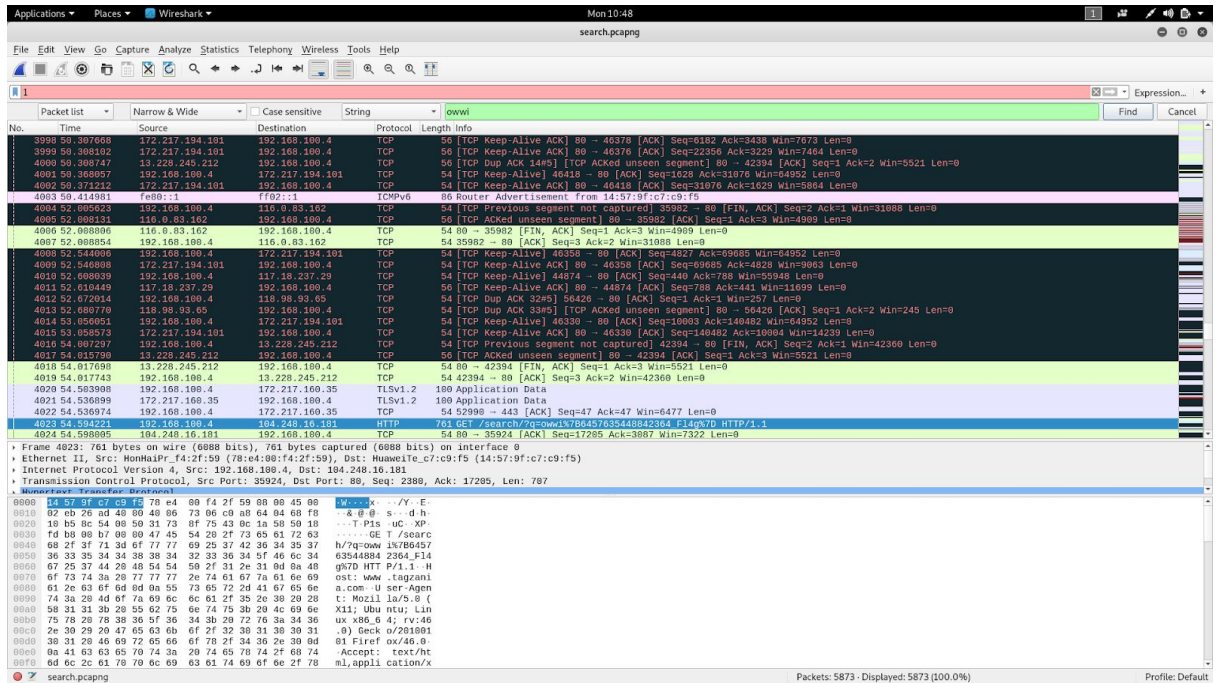


OWWI CTF 2019 Writeup

By : We Have Hazboy

1. Network Analysis

Paket yang telah diunduh dari website dibuka menggunakan aplikasi wireshark lalu memanfaatkan fitur pencarian dengan CTRL+F untuk mencari kosa kata “owwi” sebagai format flag.



Didapatkan string data berikut **?q=owwi%7B6457635448842364_FI4g%7D** yang merupakan hasil encoding dari format flag asli.

String data tersebut di decode menggunakan url entities decoder online dan menghasilkan format data flag.

Flag : owwi{6457635448842364_FI4g}

2. Reverse

Pada soal kali ini diberikan program class dari bahasa Java. Tanpa basa-basi kami langsung membuka menggunakan **radare2** dan mendapatkan informasi berikut.

```
4e      astore 3
1207     ldc "Masukan Password"
b80006     invokestatic javax/swing/JOptionPane/showInputDialog(Ljava/lang/Object;)Ljava/lang/String;
3a05     astore 5
1905     aload 5
bb0008     new java/lang/StringBuilder
59      dup
b70009     invokespecial java/lang/StringBuilder/<init>()V
120a     ldc "ctf2019"
b6000b     invokevirtual java/lang/StringBuilder/append(Ljava/lang/String;)Ljava/lang/StringBuilder;
1904     aload 4
b6000b     invokevirtual java/lang/StringBuilder/append(Ljava/lang/String;)Ljava/lang/StringBuilder;
b6000c     invokevirtual java/lang/StringBuilder/toString()Ljava/lang/String;
b6000d     invokevirtual java/lang/String/equals(Ljava/lang/Object;)Z
99001a     ifeq 0x03bb
120e     ldc "owwi{/////null6f7777697b373636333532375f6f7777695f666c61677d} "
3a06     astore 6
120f     ldc "Selamat"
3a07     astore 7
01      aconst_null
1906     aload 6
b80010     invokestatic javax/swing/JOptionPane/showMessageDialog(Ljava/awt/Component;Ljava/lang/Object;)V
01      aconst_null
1907     aload 7
b80010     invokestatic javax/swing/JOptionPane/showMessageDialog(Ljava/awt/Component;Ljava/lang/Object;)V
a7000d     goto 0x03c5
from 0x000003a1 (sym.SoiCtf4.main)
1211     ldc "Masih Salah Ya guys dicoba lagi "
3a06     astore 6
01      aconst_null
1906     aload 6
b80010     invokestatic javax/swing/JOptionPane/showMessageDialog(Ljava/awt/Component;Ljava/lang/Object;)V
from 0x000003b8 (sym.SoiCtf4.main)
b1      return
```

Ada informasi yang menurut kami sangat mencurigakan, yaitu **owwi{/////null6f7777697b373636333532375f6f7777695f666c61677d}**. Setelah kami berpusing-pusing ria men-decrypt akhirnya kami mengetahui bahwa ini adalah format heksadesimal.

Setelah di-convert HEX to ASCII kemudian didapatkan flag-nya.

Flag : **owwi{7663527_owwi_flag}**

3. Steganography

Langkah penyelesaian :

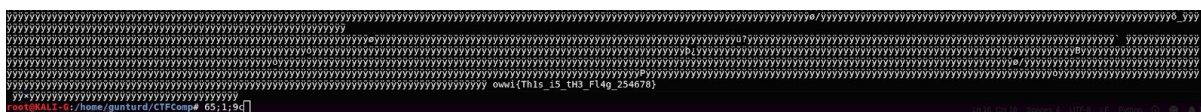
- Lihat LSB pada gambar dengan beberapa tools, terdapat beberapa perbedaan
- Jika kita menginterpretasikan urutan biner (seq) sebagai ascii dan kemudian mencoba menafsirkan urutan biner yang sama dari offset 1 (seq [1:]) sebagai ascii, kita akan menemukan sesuatu yang sangat berbeda
- Untuk memperoleh perbedaan tersebut, beberapa tools (zsteg, pip stegano, pip stegoveritas) tidak dapat langsung membaca pencarian format flag yang diawali dengan owwi. Maka digunakan script code python berikut yang akan langsung memetakan seluruh lsb ke dalam ascii dan akan berhenti ketika menemukan kata owwi

```
bits = ""
for seq in range(16):
    with open("stta_owwi.bmp", "rb") as f:
        data = f.read()
        data = data[seq:]

        for c in data:
            lsb = str(c & 0x1)
            bits += lsb

        bytess = [chr(int(bits[i:i+8], 2)) for i in
range(0, len(bits), 8)]
        lsbstr = "".join(bytess)

        if "owwi" in lsbstr:
            print(lsbstr)
            break
```



```
owwi{Th1s_i5_th3_Fl4g_254678}
```

Flag : owwi{Th1s_i5_th3_Fl4g_254678}

Kritik: Pada saat permulaan lomba, Website untuk platform CTF-nya kurang responsif. Scoreboard tidak ditampilkan. Soal harusnya sudah ter-*publish* semua, tidak satu per-satu yang mengakibatkan setiap anggota tim tidak efisien dalam mengerjakan soalnya.

Saran: Adakan Warming Up sebelum perlombaan dimulai supaya peserta lebih siap menghadapi perlombaan. Penyebaran informasi berupa sosialisasi terutama lewat media sosial ditingkatkan.