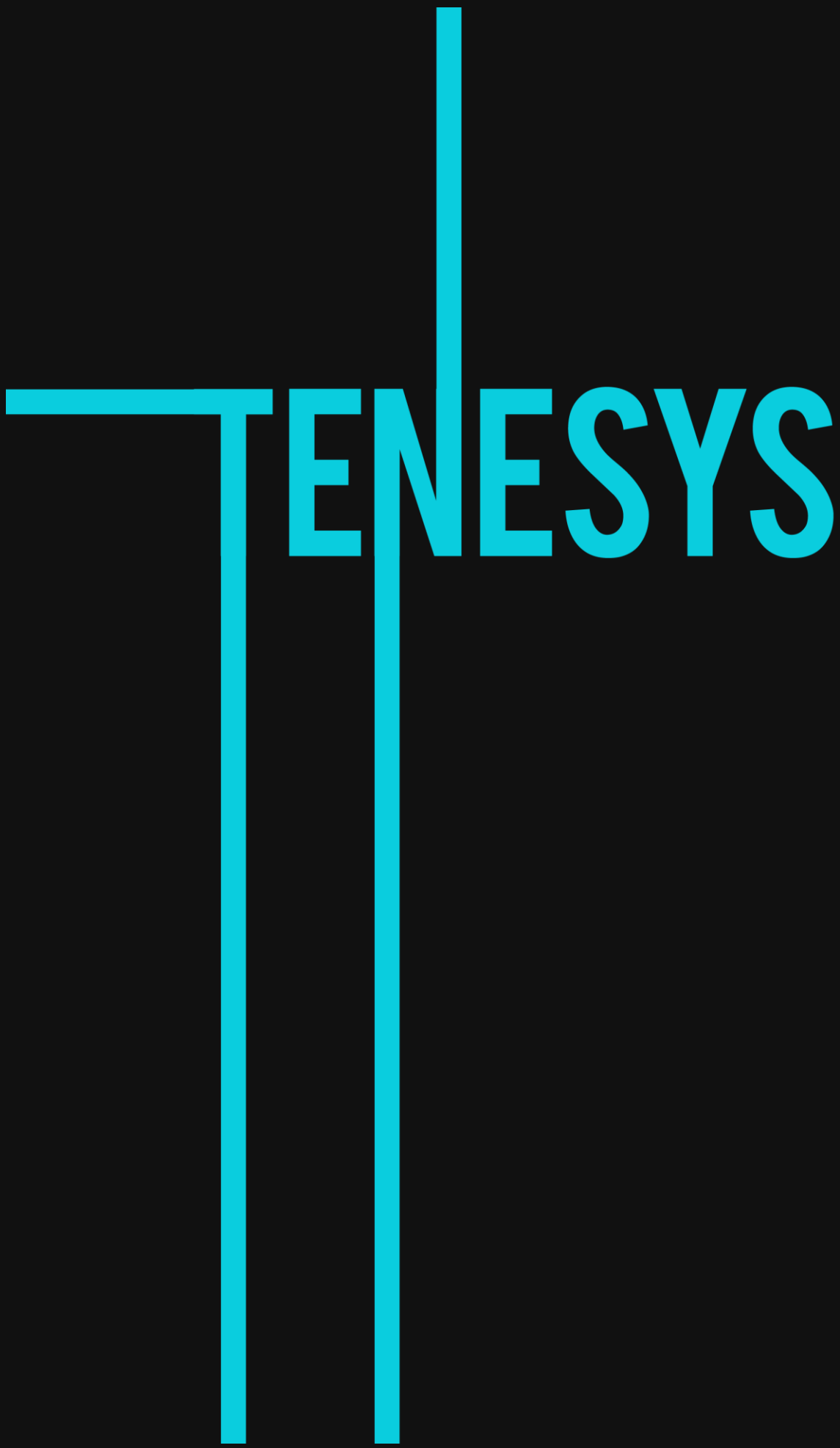
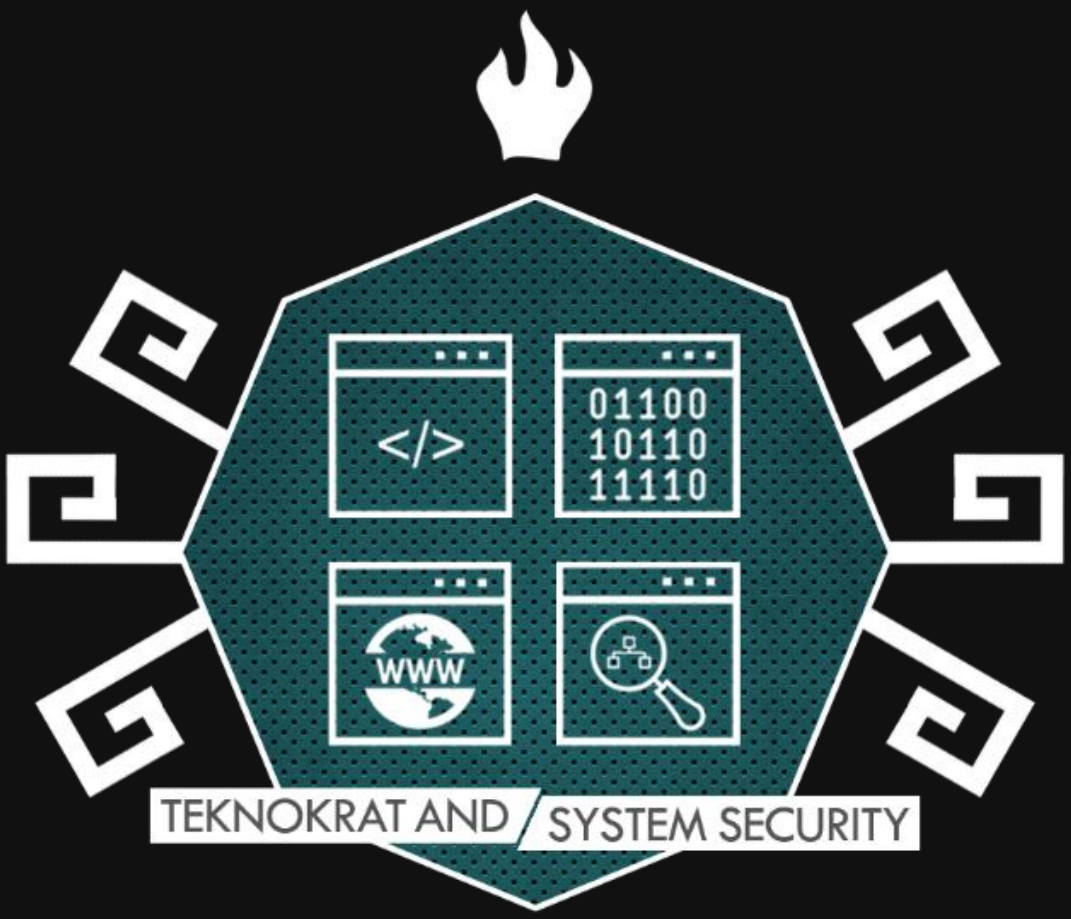

TENESYS



Reversing	Easy	10 Points

Soal

This one is easy.

Soal berupa file:
easy-64: ELF 64-bit LSB executable, x86-64

Solusi

- Cari string flag pada file soal

  strings easy-64 | grep FLAG

Flagnya adalah **FLAG:db2f62a36a018bce28e46d976e3f9864**

Reversing	Skipper	75 Points

Soal

The given binary will give you the password... if you meet its criteria!

Soal berupa file:
skipper-32: ELF 32-bit LSB executable

Solusi

- Saat file soal di jalankan, muncul output seperti berikut:

Output:

```
Computer name: fredrica
Sorry, your computer's name - fredrica - is not correct!
Killed
```

- Analisa file soal dengan IDA Pro 32bit
- Berikut isi fungsi sub_804A060

Source Code:

```
int __cdecl sub_804A060(int a1)
{
  int v1; // eax@7
  int result; // eax@8
  int v3; // ebx@8
  char s1; // [sp+10h] [bp-40Ch]@1
  char v5; // [sp+11h] [bp-40Bh]@4
  int v6; // [sp+410h] [bp-Ch]@1
  int *v7; // [sp+418h] [bp-4h]@1

  v7 = &a1;
  v6 = *MK_FP(__GS__, 20);
  sub_8048871(&s1);
  printf("Computer name: %s\n", &s1);
  if ( strcmp(&s1, "hax0rz!~") )
  {
    printf("Sorry, your computer's name - %s - is not
correct!\n", &s1);
```

```
    raise(9);
  }
  sub_8048975(&s1);
  printf("OS version: %s\n", &s1);
  if ( strcmp(&s1, "2.4.31") )
  {
    printf("Sorry, your OS version - %s - is not supported!\n",
&s1);
    s1 /= v5 / v5 - 1;
  }
  sub_804880B(&s1);
  puts(&s1);
  if ( strcmp(&s1, "AMDisbetter!") )
  {
    printf("Sorry, your CPU - %s - is not supported!\n", &s1);
    v1 = sys_exit(0);
  }
  sub_8048A63();
  result = 0;
  v3 = *MK_FP(__GS__, 20) ^ v6;
  return result;
}
```

- Program akan membandingkan nama komputer dengan string "hax0rz!~", OS versi dengan string "2.4.31", dan nama CPU dengan string "AMDisbetter!". Apabila semua kondisi terpenuhi makan program akan menampilkan flag.
- Karena itu, kita akan coba untuk melewati semua proses komparasi tersebut.

```
gdb skipper-32

(gdb) b *0x0804A095
(gdb) r
(gdb) jump *0x0804A1DE
```

Flagnya adalah **FLAG:f51579e9ca38ba87d71539a9992887ff**

Web	the-year-2000	100 Points

Soal

Wait, what year is it?

http://theyear2000.ctf.bsidessf.net/

Soal berupa web dengan alamat:
http://theyear2000.ctf.bsidessf.net

Solusi

- Lakukan dumper git
  ./gitdumper.sh http://theyear2000.ctf.bsidessf.net/.git/ /home/fredrica/CTF/git

- Lakukan ekstraksi dari file dumper tadi
  ./extractor.sh /home/fredrica/CTF/git /home/fredrica/CTF/git2

- Lakukan pencarian string FLAG pada folder hasil ekstraksi
  grep -r FLAG

  0-9e9ce4da43d0d2dc10ece64f75ec9cab1f4e5de0/index.html:Your flag is... FLAG:what_is_HEAD_may_never_die

---

Flagnya adalah **FLAG:what_is_HEAD_may_never_die**

Web	easyauth	30 Points

Soal

Can you gain admin access to this site?

http://easyauth-afee0e67.ctf.bsidessf.net

Soal berupa web dengan alamat:
http://easyauth-afee0e67.ctf.bsidessf.net

Solusi

- Login menggunakan akun guest:guest
- Aktifkan add-on tamper data
- Klik link yang diberikan, kemudian lakukan tamper pada request tersebut
- Ubah value dari param username pada header cookie menjadi administrator, lalu submit.

Flagnya adalah **FLAG:0076ecde2daae415d7e5ccc7db909e7e**

Crypto	vhash	450 Points

Soal

---- Due to a bug, the challenge might be easier than intended. Enjoy the free points! ----

Can you gain admin access to this site?

(The vhash binary is what's used for signing the cookie)

http://vhash-c6bb0e85.ctf.bsidessf.net:9292

Soal berupa web dengan alamat:
http://vhash-c6bb0e85.ctf.bsidessf.net:9292

Solusi

- Login menggunakan akun guest:guest

Output:

Login successful!

Setting cookie:
auth=ddd52d5a1d743847697929334ff2afc4a9cfbb21ebe5e6cd42b43f3e4cc9c625febc38a0dcc537740bf026a50fe16dc2e27a783fce6f3fbaf191df3080d5ab69457aaa31a331d5e0bfdc61d001597e473636c5077dacd8ee5563c93d46ccc00855c55461228376c8496f9013e316c80626e2499c7911d9a941dc0aa08ae63284|username=guest&date=2017-02-14T22:57:42+0000&secret_length=8&

Click here to continue!

- Aktifkan add-on tamper data
- Klik link yang diberikan, kemudian lakukan tamper pada request tersebut
- Ubah value dari param username pada header cookie menjadi administrator, lalu submit.

Flagnya adalah **FLAG:180e2300112ef5a4f23c93cfdec8d780**

Forensics	easycap	40 Points

Soal

Can you get the flag from the packet capture?

Solusi

- Analisa file soal pcap dengan Wireshark
- Semua traffic melalui protocol TCP
- IP 172.31.98.199 mengirimkan data sebesar satu byte ke 192.155.81.86 yaitu huruf 'F', yang kemungkinan adalah awal dari flag yang kita cari
- Kumpulkan semua data yang dikirimkan.

Flagnya adalah **FLAG:385b87afc8671dee07550290d16a8071**