
AKM

Кто мы?


phd
Positive Hack Days
DELL
git
JET BRAINS

Зачем мы этим занимаемся?

Связь CTF с учебой

CTF = Хакеры ???

Не хакер

Хакеры

Ожидание

Реальность

Популярность CTF

Name	Date
Syskron Security CTF 2020	21 Окт., 00:00 UTC — 26 Окт. 2020, 00:00 UTC
Hack.lu CTF 2020	23 Окт., 13:37 UTC — 25 Окт. 2020, 13:37 UTC
RaziCTF 2020	23 Окт., 20:30 UTC — 25 Окт. 2020, 20:30 UTC
Hack The Vote 2020	23 Окт., 23:00 UTC — 25 Окт. 2020, 23:00 UTC
peaCTF Round 1	24 Окт., 04:00 UTC — 31 Окт. 2020, 03:59 UTC
MetaCTF CyberGames 2020	24 Окт., 12:00 UTC — 25 Окт. 2020, 12:00 UTC
AppSec-IL 2020 CTF	24 Окт., 17:00 UTC — 26 Окт. 2020, 17:00 UTC
Cyber Cyber Security Rumble	30 Окт., 19:00 UTC — 01 Ноя. 2020, 19:00 UTC
CyberYoddha CTF 2020	30 Окт., 19:00 UTC — 01 Ноя. 2020, 19:00 UTC
Newark Academy CTF 2020	30 Окт., 22:00 UTC — 04 Ноя. 2020, 21:59 UTC

Place	Team	Country	Rating
1	More Smoked Leet Chicken		1037,886
2	perfect blue		961,332
3	Plaid Parliament of Pwning		764,157
4	TokyoWesterns		725,119
5	Balsn		647,054
6	A*0*E		602,889
7	p4		595,126
8	0ops		537,458
9	hxp		527,819
10	ALLES!		512,009

А зачем?

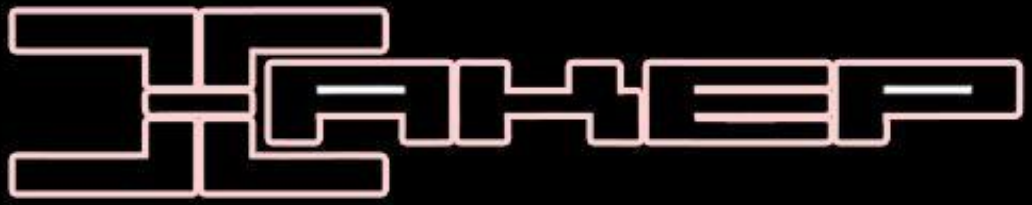
Востребованность в специалистах

Яндекс

Спонсорство компаниями

Как стать хакером?

Познавательные ресурсы



А что надо делать?

AKM{Eazy_f1Ag_3x4Mp1e}

```
[→ ~ ssh bandit6@bandit.labs.overthewire.org -p 2220
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.

bandit6@bandit.labs.overthewire.org's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 4.4.0-92-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

bandit6@bandit:~$
```

AKM{username_hostname}

AKM{bandit6_bandit}

Виды тасков

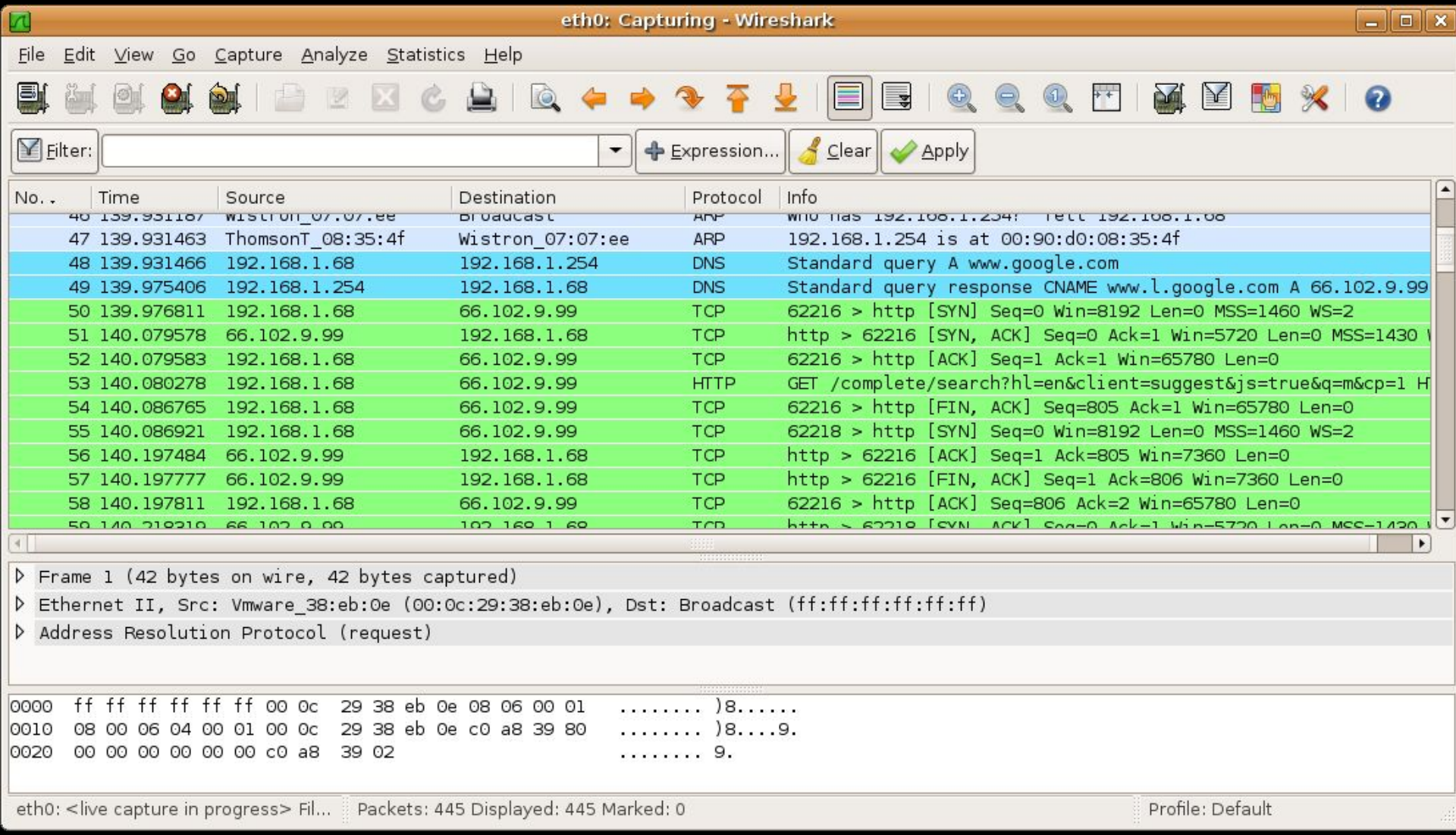
- Forensic
- Web
- Reverse
- Crypto
- Stegano
- Pwn
- Osint
- Misc

Почти как своя игра

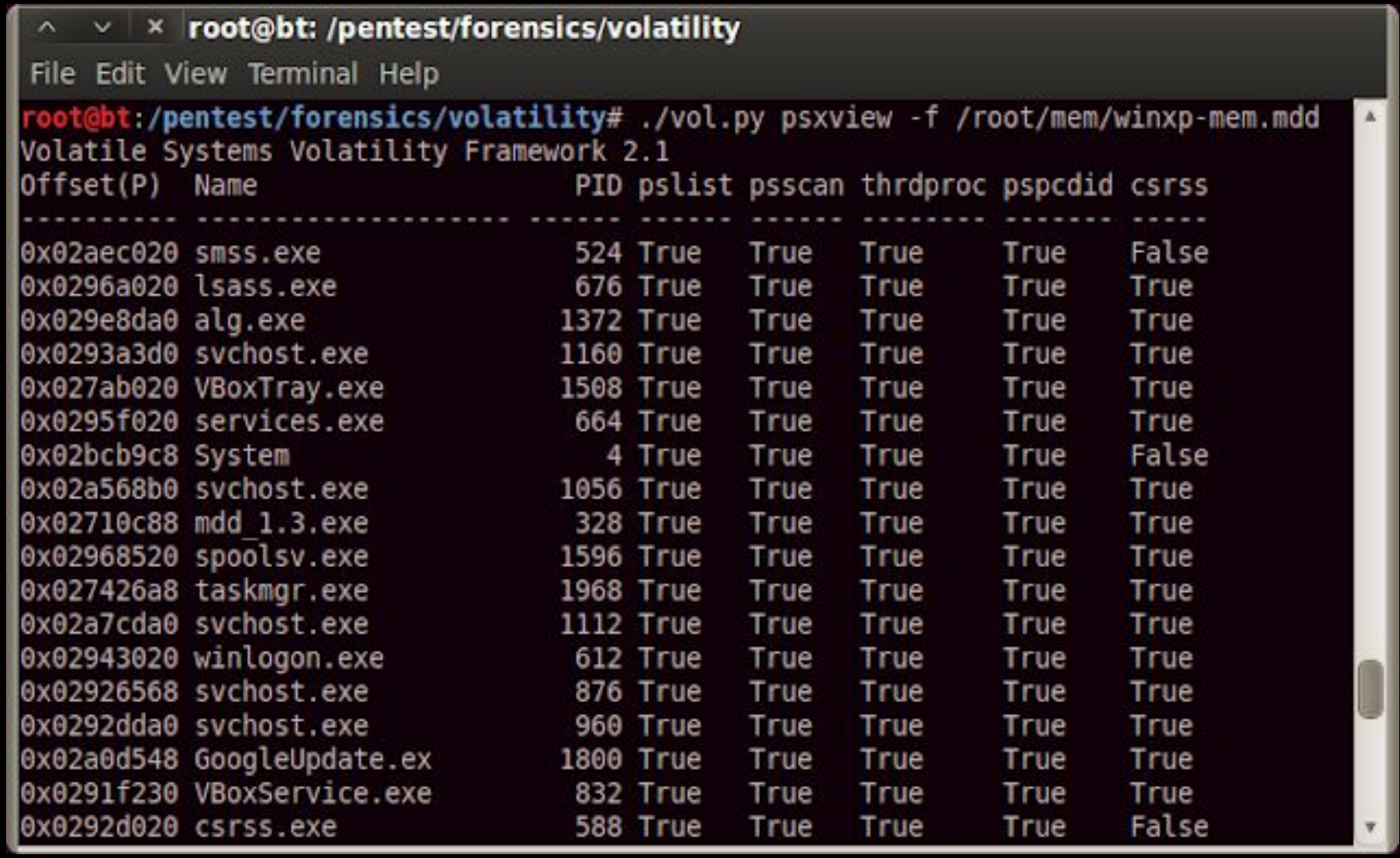
Web	Crypto	Forensics	Reverse	Misc	Pwn
1	165	100	50	50	50
150	150	150	100	100	150
204	150	150	150	165	200
203	200	200	200	150	250
206	257	200	300	200	323
318	334	250	300	300	440
325	400	347	400		
	430	350			

Разбор примеров

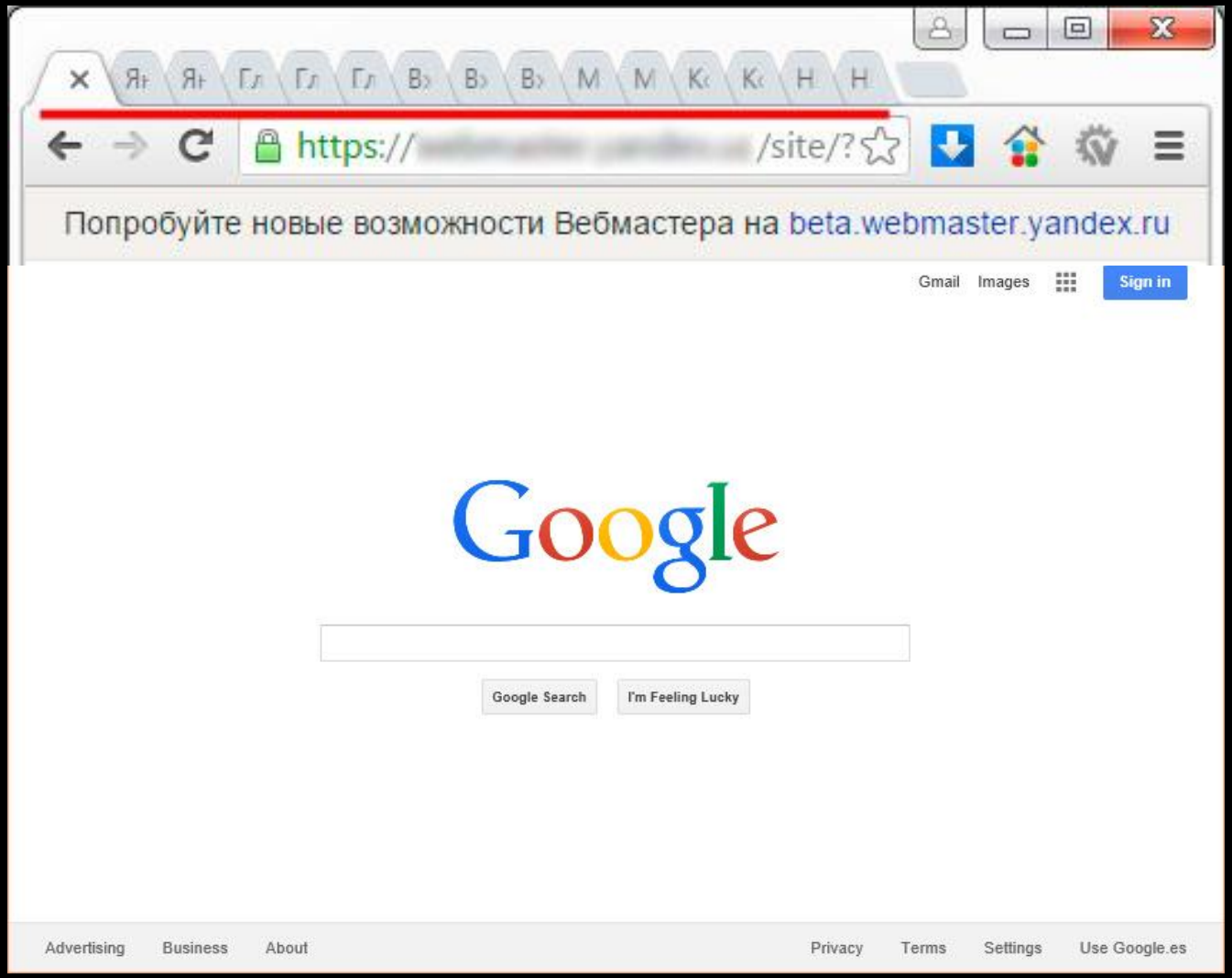
Forensic (Network)



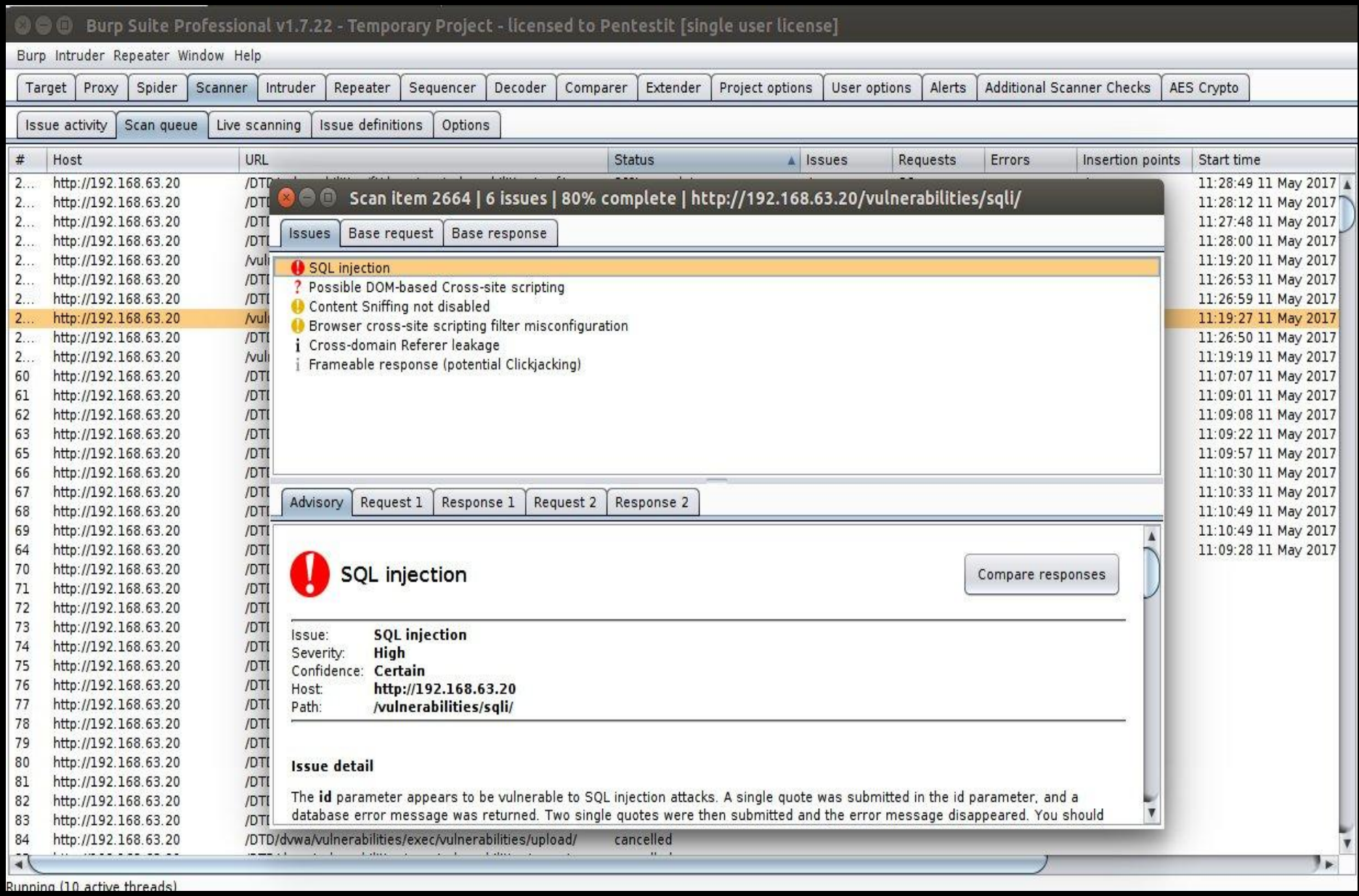
Forensic (Memory)



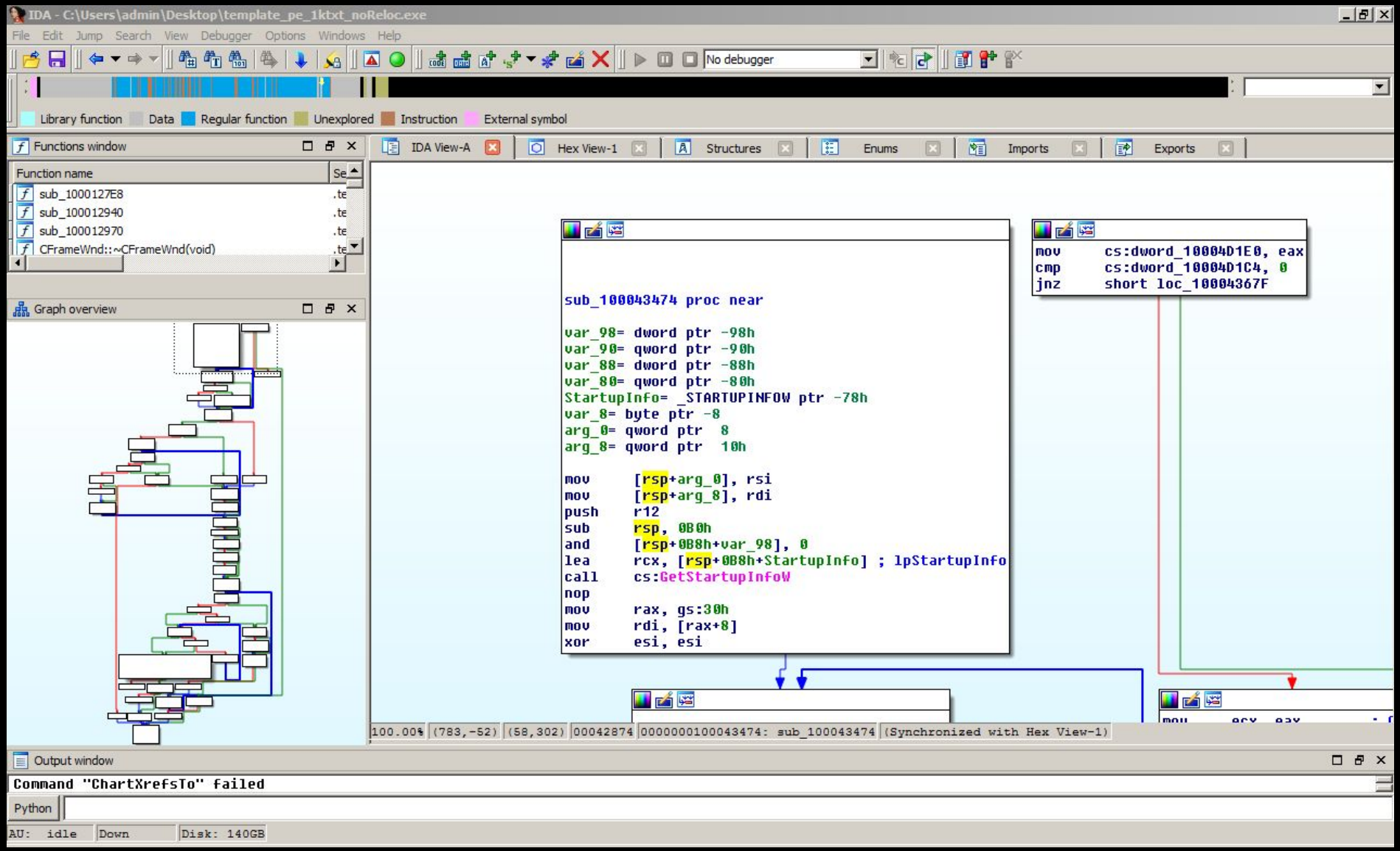
Osint


https://
/site/?
Попробуйте новые возможности Вебмастера на beta.webmaster.yandex.ru
Gmail
Images
Sign in
Google
Google Search
I'm Feeling Lucky
Advertising
Business
About
Privacy
Terms
Settings
Use Google.es

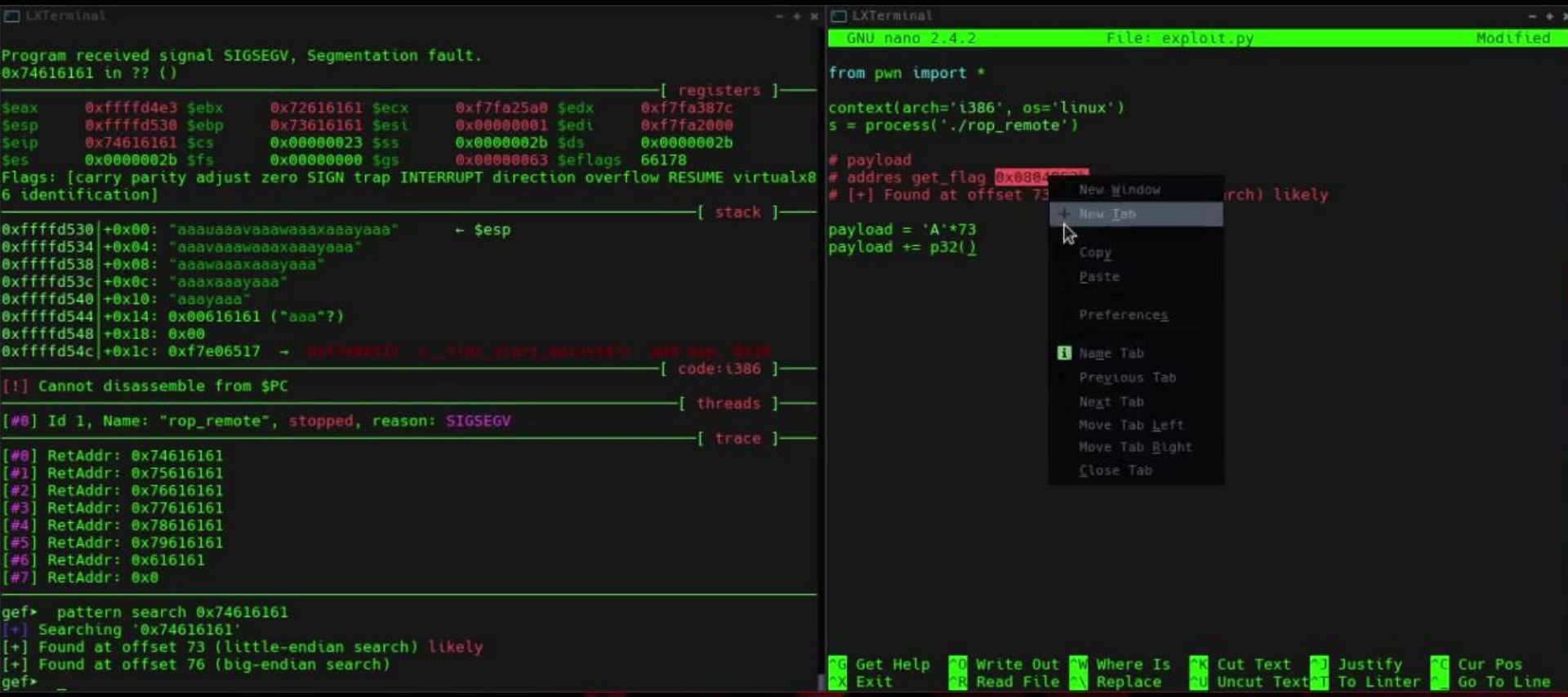
Web


Burp Suite Professional v1.7.22 - Temporary Project - licensed to Pentestit [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Additional Scanner Checks AES Crypto
Issue activity Scan queue Live scanning Issue definitions Options
Host URL Status Issues Requests Errors Insertion points Start time
Scan item 2664 | 6 issues | 80% complete | http://192.168.63.20/vulnerabilities/sqli/
Issues Base request Base response
SQL injection
Possible DOM-based Cross-site scripting
Content Sniffing not disabled
Browser cross-site scripting filter misconfiguration
Cross-domain Referer leakage
Frameable response (potential Clickjacking)
Advisory Request 1 Response 1 Request 2 Response 2
SQL injection
Compare responses
Issue: SQL injection
Severity: High
Confidence: Certain
Host: http://192.168.63.20
Path: /vulnerabilities/sqli/
Issue detail
The id parameter appears to be vulnerable to SQL injection attacks. A single quote was submitted in the id parameter, and a database error message was returned. Two single quotes were then submitted and the error message disappeared. You should
84 http://192.168.63.20 /DTD/dvwa/vulnerabilities/exec/vulnerabilities/upload/ cancelled
Running (10 active threads)

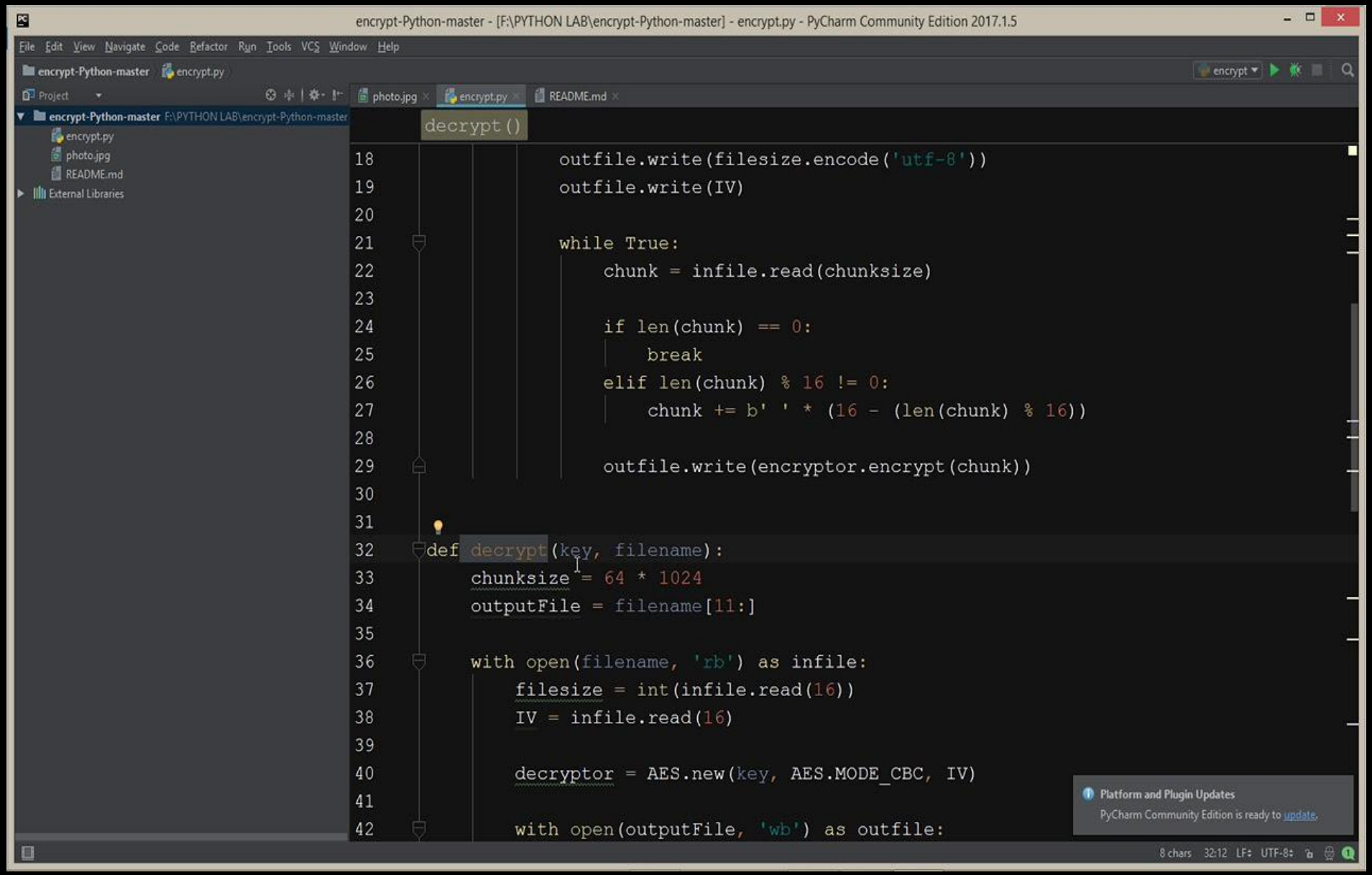
Reverse


IDA - C:\Users\admin\Desktop\template_pe_1ktxt_noReloc.exe
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name
sub_1000127E8
sub_100012940
sub_100012970
CFrameWnd::~CFrameWnd(void)
Graph overview
IDA View-A
Hex View-1
Structures
Enums
Imports
Exports
sub_100043474 proc near
var_98= dword ptr -98h
var_90= qword ptr -90h
var_88= dword ptr -88h
var_80= qword ptr -80h
StartupInfo= _STARTUPINFOW ptr -78h
var_8= byte ptr -8
arg_0= qword ptr 8
arg_8= qword ptr 10h
mov [rsp+arg_0], rsi
mov [rsp+arg_8], rdi
push r12
sub rsp, 0B0h
and [rsp+0B8h+var_98], 0
lea rcx, [rsp+0B8h+StartupInfo] ; lpStartupInfo
call cs:GetStartupInfoW
nop
mov rax, gs:30h
mov rdi, [rax+8]
xor esi, esi
mov cs:dword_10004D1E0, eax
cmp cs:dword_10004D1C4, 0
jnz short loc_10004367F
100.00% (783,-52) (58,302) 00042874 0000000100043474: sub_100043474 (Synchronized with Hex View-1)
Output window
Command "ChartXrefsTo" failed
Python
AU: idle Down Disk: 140GB

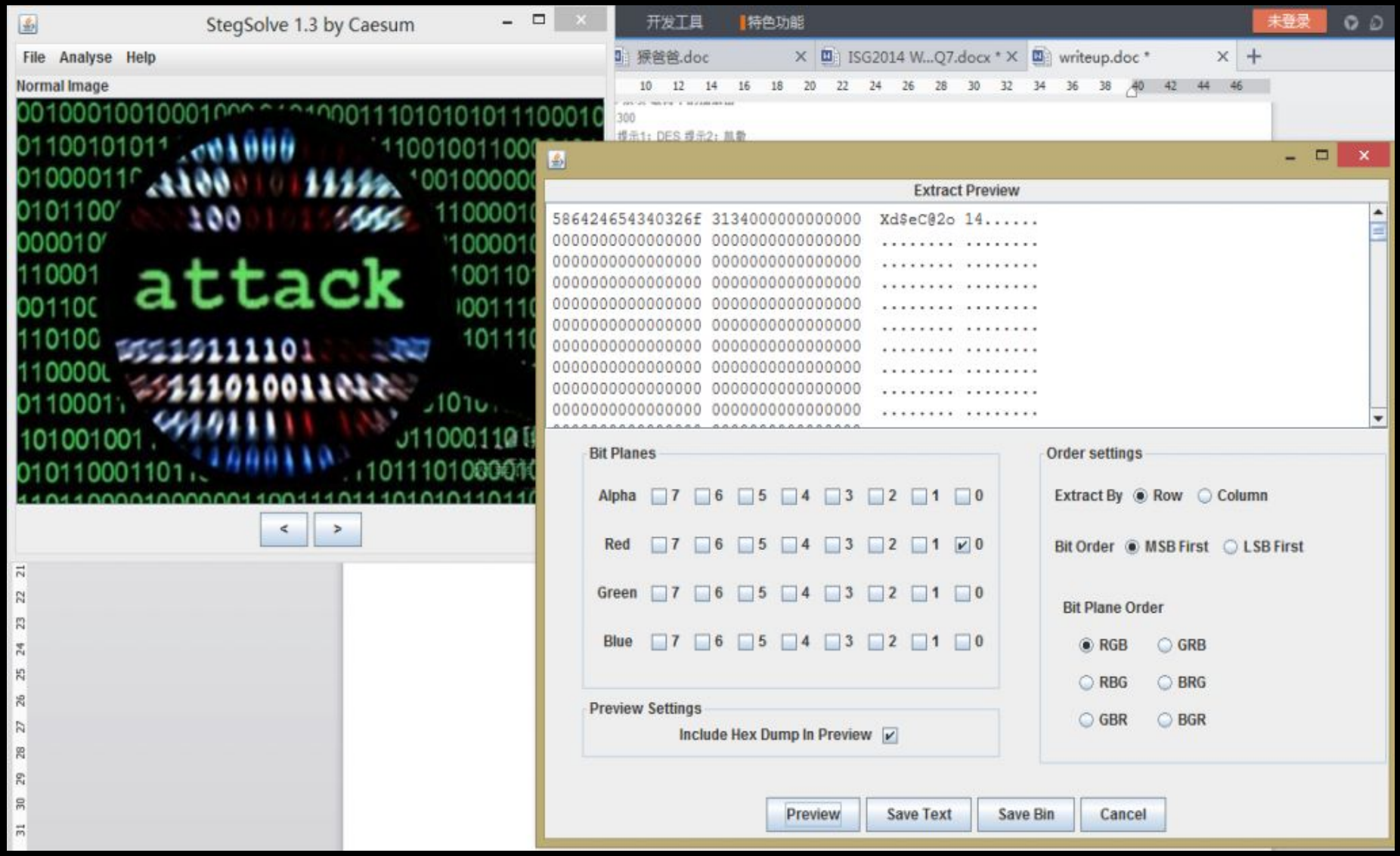
Pwn


LXTerminal
Program received signal SIGSEGV, Segmentation fault.
0x74616161 in ?? ()
[registers]
$eax 0xffffd4e3 $ebx 0x72616161 $ecx 0xf7fa25a0 $edx 0xf7fa387c
$esp 0xffffd530 $ebp 0x73616161 $esi 0x00000001 $edi 0xf7fa2000
$eip 0x74616161 $cs 0x00000023 $ss 0x0000002b $ds 0x0000002b
$es 0x0000002b $fs 0x00000000 $gs 0x00000063 $eflags 66178
Flags: [carry parity adjust zero SIGN trap INTERRUPT direction overflow RESUME virtualx86 identification]
[stack]
0xffffd530|+0x00: "aaauaaavaaawaaaxaaayaaa" ← $esp
0xffffd534|+0x04: "aaavaaawaaaxaaayaaa"
0xffffd538|+0x08: "aaawaaaxaaayaaa"
0xffffd53c|+0x0c: "aaaxaaayaaa"
0xffffd540|+0x10: "aaayaaa"
0xffffd544|+0x14: 0x00616161 ("aaa"?)
0xffffd548|+0x18: 0x00
0xffffd54c|+0x1c: 0xf7e06517 →
[code:i386]
[!] Cannot disassemble from $PC
[threads]
[#0] Id 1, Name: "rop_remote", stopped, reason: SIGSEGV
[trace]
[#0] RetAddr: 0x74616161
[#1] RetAddr: 0x75616161
[#2] RetAddr: 0x76616161
[#3] RetAddr: 0x77616161
[#4] RetAddr: 0x78616161
[#5] RetAddr: 0x79616161
[#6] RetAddr: 0x616161
[#7] RetAddr: 0x0
gef➤ pattern search 0x74616161
[+] Searching '0x74616161'
[+] Found at offset 73 (little-endian search) likely
[+] Found at offset 76 (big-endian search)
gef➤
LXTerminal
GNU nano 2.4.2 File: exploit.py Modified
from pwn import *
context(arch='i386', os='linux')
s = process('./rop_remote')
# payload
# addres get_flag 0x0804
# [+] Found at offset 73
payload = 'A'*73
payload += p32()
New Window
New Tab
Copy
Paste
Preferences
Name Tab
Previous Tab
Next Tab
Move Tab Left
Move Tab Right
Close Tab
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Linter ^_ Go To Line

Crypto

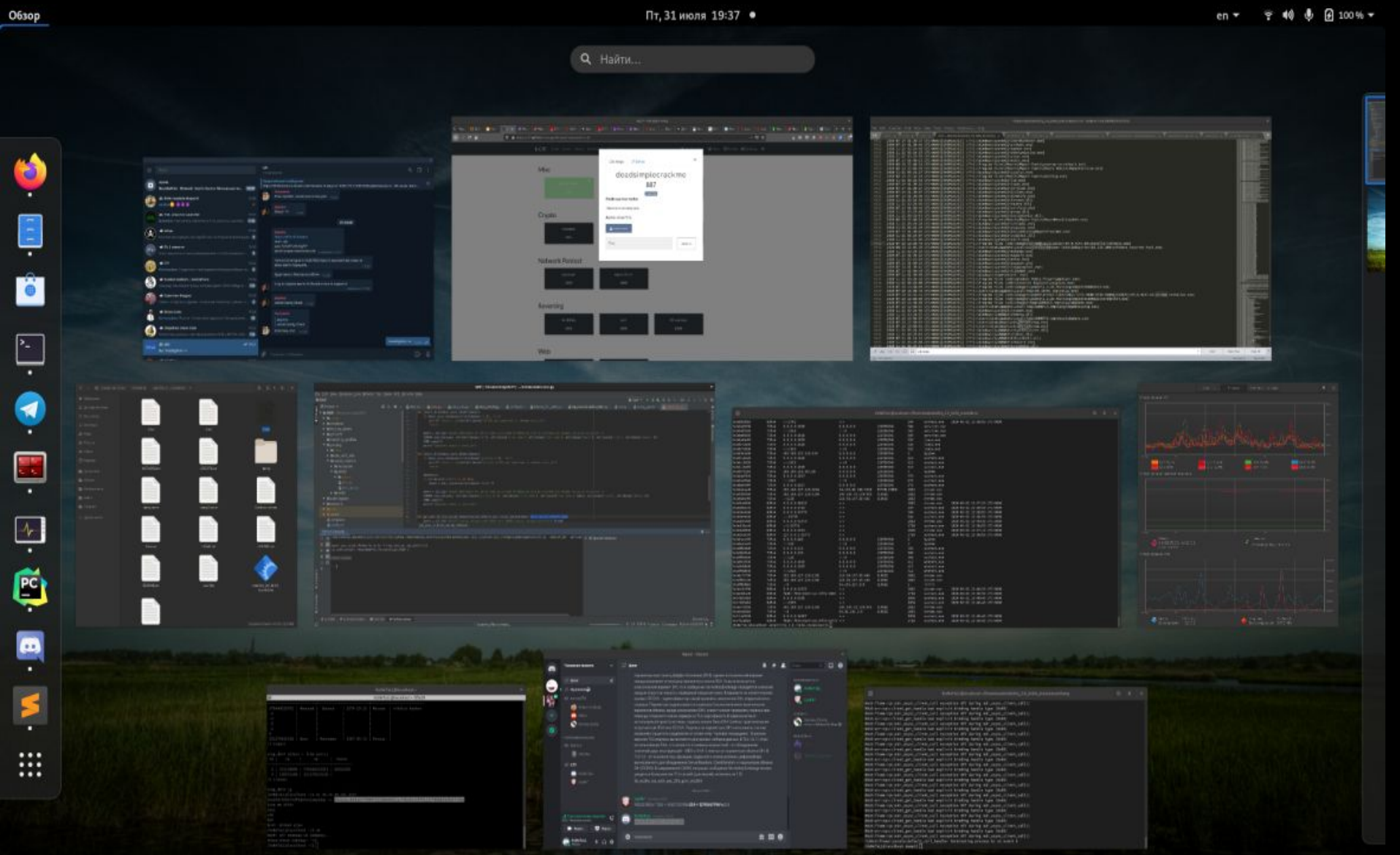

encrypt-Python-master - [F:\PYTHON LAB\encrypt-Python-master] - encrypt.py - PyCharm Community Edition 2017.1.5
File Edit View Navigate Code Refactor Run Tools VCS Window Help
encrypt-Python-master
encrypt.py
Project
encrypt-Python-master F:\PYTHON LAB\encrypt-Python-master
encrypt.py
photo.jpg
README.md
External Libraries
photo.jpg
encrypt.py
README.md
decrypt()
outfile.write(filesize.encode('utf-8'))
outfile.write(IV)
while True:
chunk = infile.read(chunksize)
if len(chunk) == 0:
break
elif len(chunk) % 16 != 0:
chunk += b' ' * (16 - (len(chunk) % 16))
outfile.write(encryptor.encrypt(chunk))
def decrypt(key, filename):
chunksize = 64 * 1024
outputFile = filename[11:]
with open(filename, 'rb') as infile:
filesize = int(infile.read(16))
IV = infile.read(16)
decryptor = AES.new(key, AES.MODE_CBC, IV)
with open(outputFile, 'wb') as outfile:
Platform and Plugin Updates
PyCharm Community Edition is ready to update.
8 chars 32:12 LF: UTF-8:

Stegano


StegSolve 1.3 by Caesum
File Analyse Help
Normal Image
attack
<
>
开发工具
特色功能
未登录
猴爸爸.doc
ISG2014 W...Q7.docx *
writeup.doc *
Extract Preview
586424654340326f 3134000000000000 Xd$eC@2o 14.....
Bit Planes
Alpha 7 6 5 4 3 2 1 0
Red 7 6 5 4 3 2 1 0
Green 7 6 5 4 3 2 1 0
Blue 7 6 5 4 3 2 1 0
Order settings
Extract By Row Column
Bit Order MSB First LSB First
Bit Plane Order
RGB GRB
RBG BRG
GBR BGR
Preview Settings
Include Hex Dump In Preview
Preview
Save Text
Save Bin
Cancel

Misc

Общее для всех тасков




Reverse
Crypto
WEB
PWN
Forensic
Osint
Пойду лучше в
компуктер поиграю

А что ботать-то?

- Linux

Ну и поиграть в бандита
overthewire.org/wargames/bandit/

Уже можете в Linux?

- Просто залетайте на любую CTF
- Такайте и гуглите задания которые вам интересны
- Читайте врайтапы прошлых CTF
- Смотрите курсы от spbCTF


AKM