



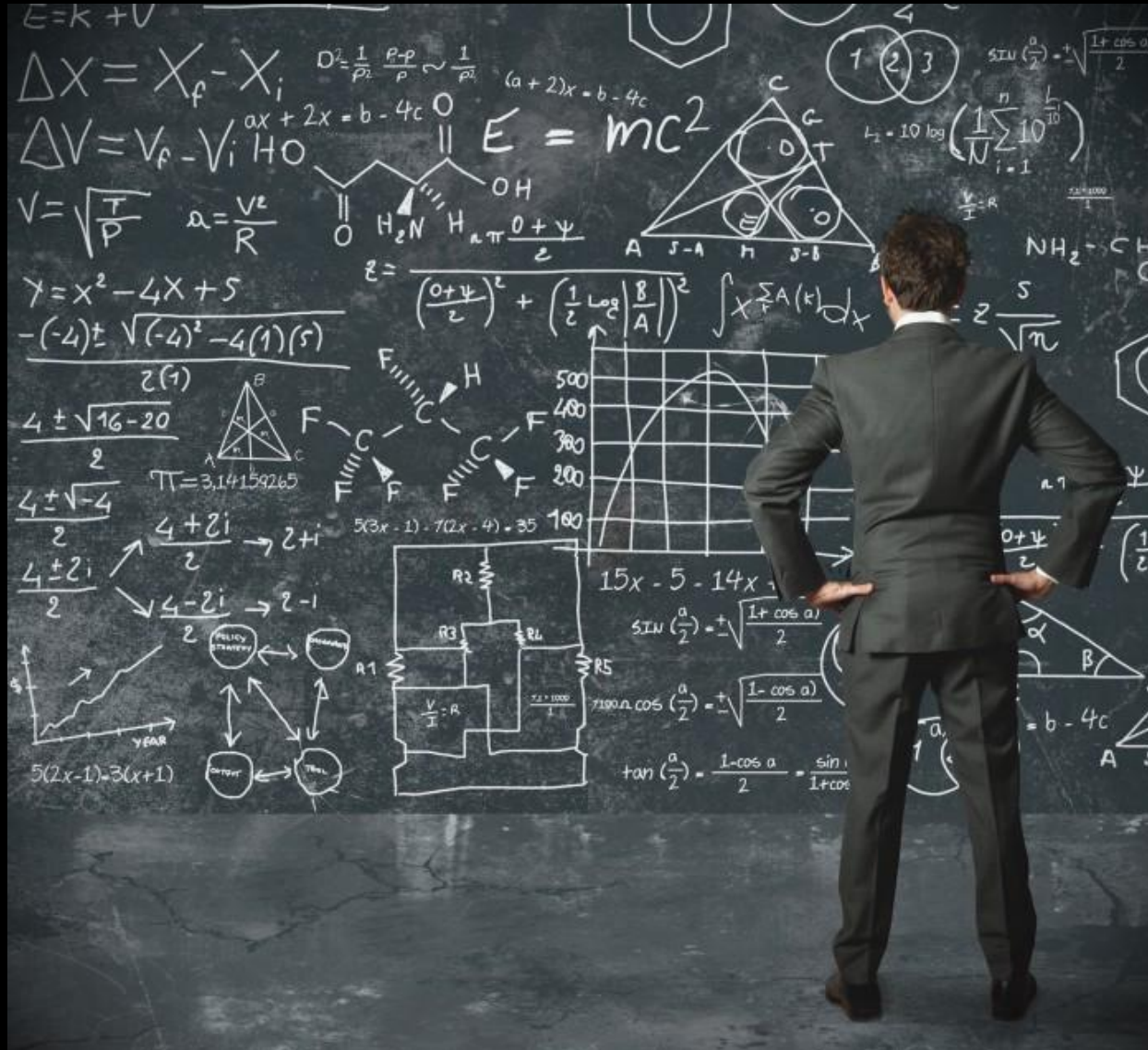


КТО МЫ?



Зачем мы этим
занимаемся?

Связь STF с учеббой



CTF = Хакеры ???

Не хакер



Хакеры



Ожидание












Реальность



Популярность СТФ



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

КОМПАНИИ



+1000
more companies

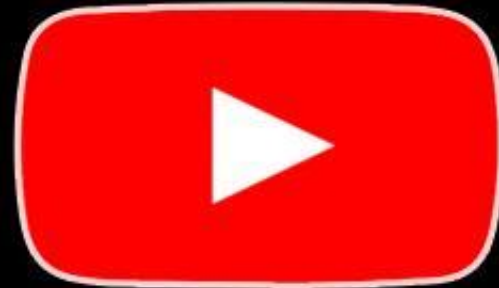
Как стать хакером?



Познавательные

ресурсы

ЭФНЕР



А что надо делать?

AKM{Eazy_f1Ag_3x4Mp1e}

```
ssh bandit6@bandit.labs.overthewire.org -p 2220
```

20/35

```
WARGAME
```

```
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)

eth0: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: + Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
46	139.931187	wistron_07:07:ee	Broadcast	ARP	who has 192.168.1.254? Tell 192.168.1.68
47	139.931463	ThomsonT_08:35:4f	Wistron_07:07:ee	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
48	139.931466	192.168.1.68	192.168.1.254	DNS	Standard query A www.google.com
49	139.975406	192.168.1.254	192.168.1.68	DNS	Standard query response CNAME www.l.google.com A 66.102.9.99
50	139.976811	192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51	140.079578	66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52	140.079583	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53	140.080278	192.168.1.68	66.102.9.99	HTTP	GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
54	140.086765	192.168.1.68	66.102.9.99	TCP	62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55	140.086921	192.168.1.68	66.102.9.99	TCP	62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56	140.197484	66.102.9.99	192.168.1.68	TCP	http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57	140.197777	66.102.9.99	192.168.1.68	TCP	http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58	140.197811	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
59	140.219219	66.102.9.99	192.168.1.68	TCP	http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430

Frame 1 (42 bytes on wire, 42 bytes captured)

Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

```

0000  ff ff ff ff ff ff 00 0c 29 38 eb 0e 08 06 00 01  ..... )8.....
0010  08 00 06 04 00 01 00 0c 29 38 eb 0e c0 a8 39 80  ..... )8....9.
0020  00 00 00 00 00 00 c0 a8 39 02  ..... 9.

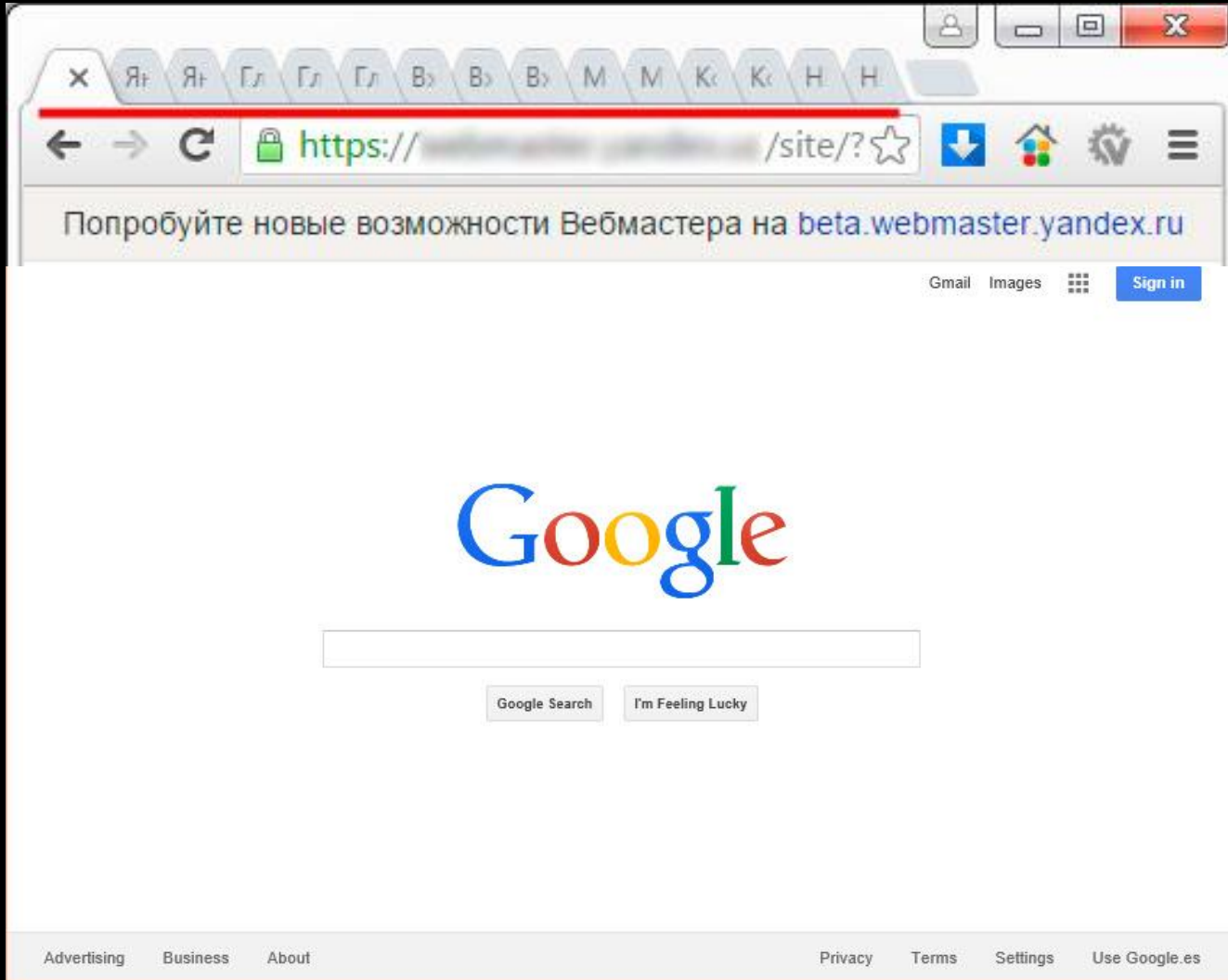
```

eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default

Forensic (Memory)

```
root@bt: /pentest/forensics/volatility
File Edit View Terminal Help
root@bt:/pentest/forensics/volatility# ./vol.py psxview -f /root/mem/winxp-mem.mdd
Volatile Systems Volatility Framework 2.1
Offset(P)  Name                PID  pslist  psscan  thrdproc  pspcid  csrss
-----
0x02aec020 smss.exe             524  True   True    True     True    False
0x0296a020 lsass.exe            676  True   True    True     True    True
0x029e8da0 alg.exe              1372 True   True    True     True    True
0x0293a3d0 svchost.exe          1160 True   True    True     True    True
0x027ab020 VBoxTray.exe         1508 True   True    True     True    True
0x0295f020 services.exe         664  True   True    True     True    True
0x02bcb9c8 System                4    True   True    True     True    False
0x02a568b0 svchost.exe          1056 True   True    True     True    True
0x02710c88 mdd_1.3.exe          328  True   True    True     True    True
0x02968520 spoolsv.exe          1596 True   True    True     True    True
0x027426a8 taskmgr.exe           1968 True   True    True     True    True
0x02a7cda0 svchost.exe          1112 True   True    True     True    True
0x02943020 winlogon.exe          612  True   True    True     True    True
0x02926568 svchost.exe           876  True   True    True     True    True
0x0292dda0 svchost.exe           960  True   True    True     True    True
0x02a0d548 GoogleUpdate.ex     1800 True   True    True     True    True
0x0291f230 VBoxService.exe       832  True   True    True     True    True
0x0292d020 csrss.exe             588  True   True    True     True    False
```

Osint



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
2...	http://192.168.63.20	/DTI						11:28:49 11 May 2017
2...	http://192.168.63.20	/DTI						11:28:12 11 May 2017
2...	http://192.168.63.20	/DTI						11:27:48 11 May 2017
2...	http://192.168.63.20	/DTI						11:28:00 11 May 2017
2...	http://192.168.63.20	/vul						11:19:20 11 May 2017
2...	http://192.168.63.20	/DTI						11:26:53 11 May 2017
2...	http://192.168.63.20	/DTI						11:26:59 11 May 2017
2...	http://192.168.63.20	/vul						11:19:27 11 May 2017
2...	http://192.168.63.20	/DTI						11:26:50 11 May 2017
2...	http://192.168.63.20	/vul						11:19:19 11 May 2017
60	http://192.168.63.20	/DTI						11:07:07 11 May 2017
61	http://192.168.63.20	/DTI						11:09:01 11 May 2017
62	http://192.168.63.20	/DTI						11:09:08 11 May 2017
63	http://192.168.63.20	/DTI						11:09:22 11 May 2017
65	http://192.168.63.20	/DTI						11:09:57 11 May 2017
66	http://192.168.63.20	/DTI						11:10:30 11 May 2017
67	http://192.168.63.20	/DTI						11:10:33 11 May 2017
68	http://192.168.63.20	/DTI						11:10:49 11 May 2017
69	http://192.168.63.20	/DTI						11:10:49 11 May 2017
64	http://192.168.63.20	/DTI						11:09:28 11 May 2017
70	http://192.168.63.20	/DTI						
71	http://192.168.63.20	/DTI						
72	http://192.168.63.20	/DTI						
73	http://192.168.63.20	/DTI						
74	http://192.168.63.20	/DTI						
75	http://192.168.63.20	/DTI						
76	http://192.168.63.20	/DTI						
77	http://192.168.63.20	/DTI						
78	http://192.168.63.20	/DTI						
79	http://192.168.63.20	/DTI						
80	http://192.168.63.20	/DTI						
81	http://192.168.63.20	/DTI						
82	http://192.168.63.20	/DTI						
83	http://192.168.63.20	/DTI						
84	http://192.168.63.20	/DTD/dvwa/vulnerabilities/exec/vulnerabilities/upload/	cancelled					

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

Running (10 active threads)

Reverse

IDA - C:\Users\admin\Desktop\template_pe_1kbt_noReloc.exe

File Edit Jump Search View Debugger Options Windows Help

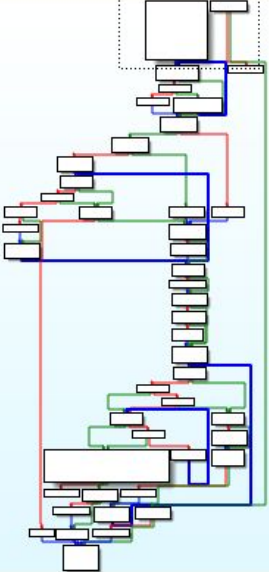
No debugger

Library function Data Regular function Unexplored Instruction External symbol

Functions window

Function name	Se
sub_1000127E8	.te
sub_100012940	.te
sub_100012970	.te
CFrameWnd::~CFrameWnd(void)	.te

Graph overview



```

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= _STARTUPINFOF 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: "aaaaaaaavaaaaaaaayaaa" - $esp
0xffffd534 +0x04: "aaavaaaaavaaaaaayaaa"
0xffffd538 +0x08: "aaawaaaayaaa"
0xffffd53c +0x0c: "aaaxaaaayaaa"
0xffffd540 +0x10: "aaayaaa"
0xffffd544 +0x14: 0x00616161 ("aaa?")
0xffffd548 +0x18: 0x00
0xffffd54c +0x1c: 0xf7e06517 - 0xf7e06517 _start_wchar32b and esp, 0x10

[ 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
# address get_flag 0x08040000
# [+] Found at offset 73 (little-endian search) likely

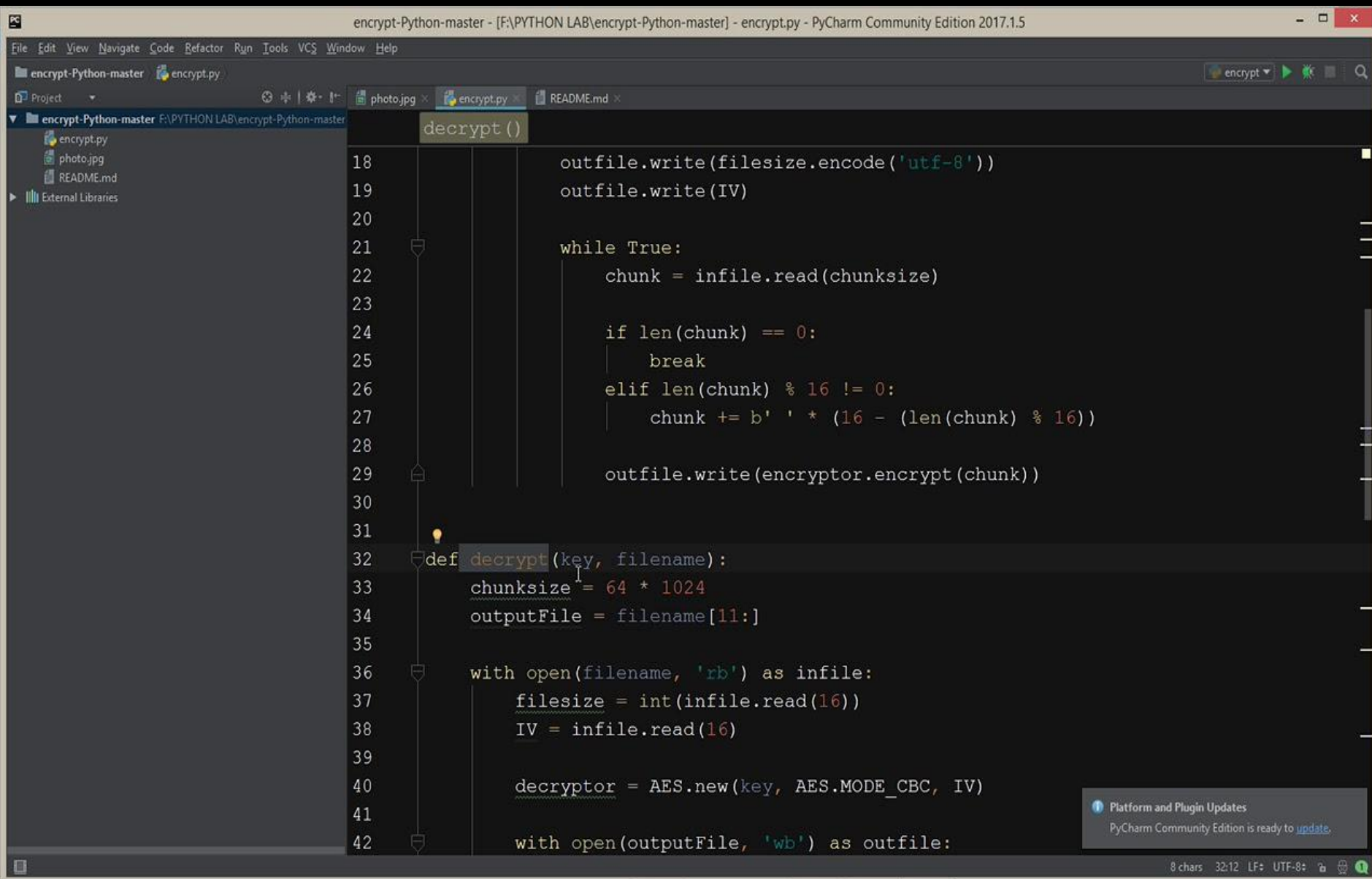
payload = 'A'*73
payload += p32(0)

Get Help  Write Out  Where Is  Cut Text  Justify  Cur Pos
Exit      Read File  Replace  Uncut Text  To Linter  Go To Line

```



Crypto



The screenshot shows the PyCharm IDE interface. The main editor window displays a Python script named `decrypt.py` with the following code:

```
decrypt()
18     outfile.write(filesize.encode('utf-8'))
19     outfile.write(IV)
20
21     while True:
22         chunk = infile.read(chunksize)
23
24         if len(chunk) == 0:
25             break
26         elif len(chunk) % 16 != 0:
27             chunk += b' ' * (16 - (len(chunk) % 16))
28
29         outfile.write(encryptor.encrypt(chunk))
30
31
32 def decrypt(key, filename):
33     chunksize = 64 * 1024
34     outputFile = filename[11:]
35
36     with open(filename, 'rb') as infile:
37         filesize = int(infile.read(16))
38         IV = infile.read(16)
39
40         decryptor = AES.new(key, AES.MODE_CBC, IV)
41
42     with open(outputFile, 'wb') as outfile:
```

The IDE interface includes a menu bar (File, Edit, View, Navigate, Code, Refactor, Run, Tools, VCS, Window, Help), a toolbar, and a project explorer on the left showing the file structure of the `encrypt-Python-master` project. A notification in the bottom right corner indicates that the PyCharm Community Edition is ready to update.

Stegano

The screenshot shows the StegSolve 1.3 by Caesum application window. The main image displays a steganographic pattern with the word "attack" in green. The background is a grid of binary code. A dialog box titled "Extract Preview" is open, showing a hex dump of the extracted data. The hex dump contains the following text:

```
586424654340326F 3134000000000000 Xd$eC@2o 14.....  
0000000000000000 0000000000000000 .....  
0000000000000000 0000000000000000 .....  
0000000000000000 0000000000000000 .....  
0000000000000000 0000000000000000 .....  
0000000000000000 0000000000000000 .....  
0000000000000000 0000000000000000 .....  
0000000000000000 0000000000000000 .....  
0000000000000000 0000000000000000 .....  
0000000000000000 0000000000000000 .....  
0000000000000000 0000000000000000 .....  
0000000000000000 0000000000000000 .....  
0000000000000000 0000000000000000 .....  
0000000000000000 0000000000000000 .....
```

The dialog box also includes settings for bit planes and order settings:

- Bit Planes:** Alpha (7-0), Red (7-0), Green (7-0), Blue (7-0). The Red bit 0 is checked.
- Order settings:** Extract By (Row selected), Bit Order (MSB First selected), Bit Plane Order (RGB selected).
- Preview Settings:** Include Hex Dump in Preview (checked).

Buttons at the bottom of the dialog box are: Preview, Save Text, Save Bin, Cancel.

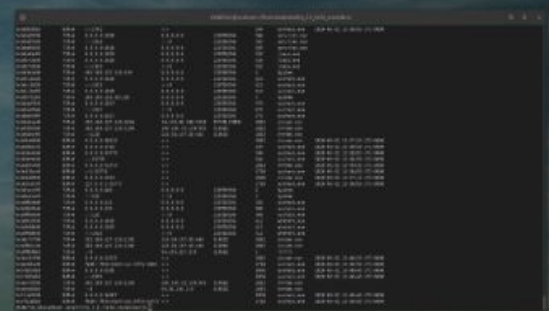
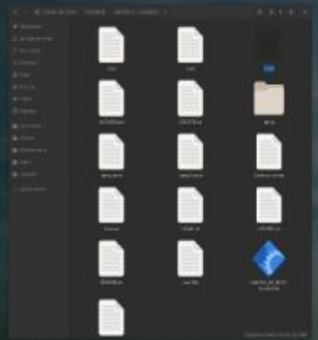
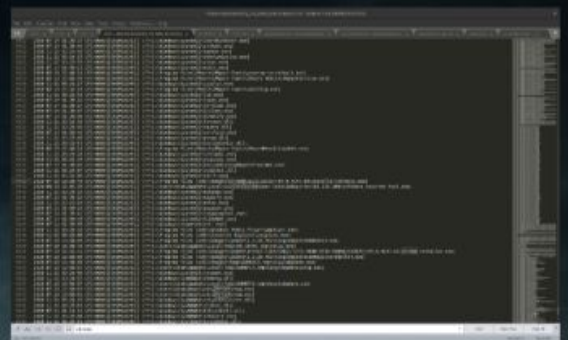
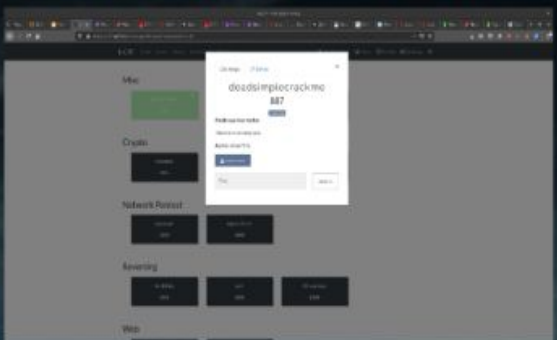
31
30
29
28
27
26
25
24
23
22
21

Misc



Общее для всех задач

Найти...



Reverse
Crypto



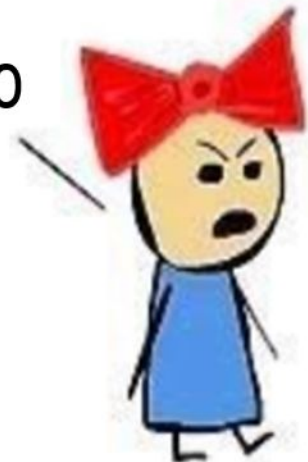
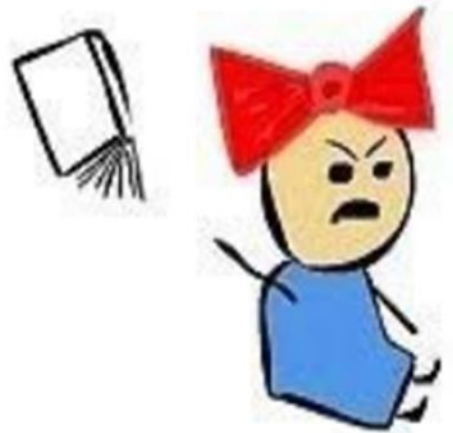
WEB
PWN



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 вайтапы прошлых CTF
- Смотрите курсы от srbCTF

