

CTF

Siber güvenlik bilmeceleri

07.03.2015

Halit Alptekin

BILMOK

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

PLAN

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

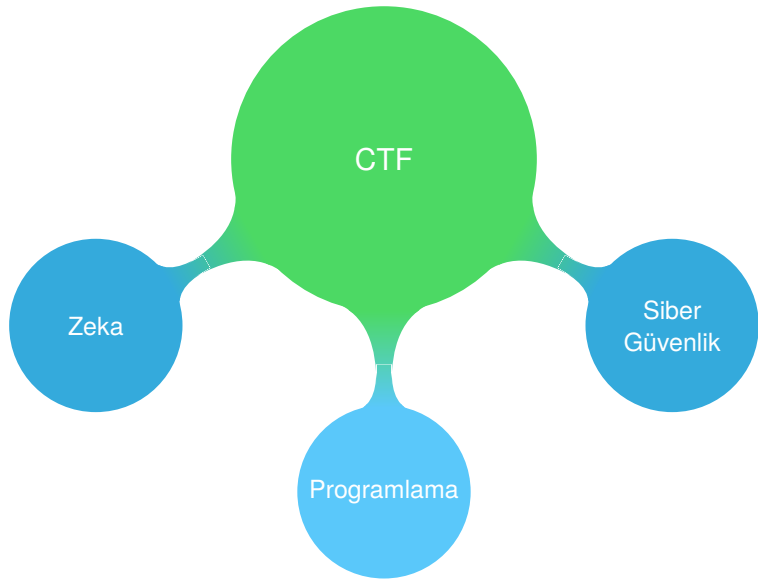
CTF

NEDİR?

- 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

- 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?



TÜRLERİ?

- 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, UUID=bc6c2b24-106a-4570-bc4f-ae09abbd7a88
65536	0x10000	Linux EXT filesystem, rev 1.0 ext3 filesystem data, UUID=bc6c2b24-106a-4570-bc4f-ae09abbd7a88
72704	0x11C00	Linux EXT filesystem, rev 1.0 ext3 filesystem data, UUID=bc6c2b24-106a-4570-bc4f-ae09abbd7a88
1113088	0x10FC00	ELF 64-bit LSB executable, AMD x86-64, version 1 (SYSV)
1116896	0x110AE0	LZMA compressed data, properties: 0x89, dictionary size: 1 MB
1117024	0x110B60	LZMA compressed data, properties: 0x9A, dictionary size: 1 MB
1117216	0x110C20	LZMA compressed data, properties: 0xB6, dictionary size: 1 MB
1117408	0x110CE0	LZMA compressed data, properties: 0xD8, dictionary size: 1 MB

```
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 linked, interpreter /lib64/ld-linux-x86-64.so.2
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 c2VjY29uMjAxNDpZb3VyQmF0dGxIRmllbGQ=
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..0.[wZ..i..$......b...6....f...0.Q.h...0....o...>K.
```

FORENSIC 2

```
black@blackarch ~ % echo -n "c2VjY29uMjAxNDpZb3VyQmF0dGxIRmllbGQ=" | base64 -d
secon2014:YourBattleField
black@blackarch ~ % curl --user 'secon2014:YourBattleField' 'http://133.242.224.21:6809/nw100/key.html'
<HTML>
SECON{Basic_NW_Challenge_Done!}
</HTML>
black@blackarch ~ %
```

```
[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
```

```
#!/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[90..=`..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..!...:0...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^iH.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 Schnei',  
'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\nMDS flag']  
  
In [11]:
```

```
In [12]: b[-1]  
Out[12]: 'ION HEX\nMDS flag'  
  
In [13]: b[5]  
Out[13]: 'edisStore...\nGET'
```


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 = "%AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA%34719c%36$hn%32836c%37$n"

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

EXPLOIT 2

[illegible]

PROGRAMMING 1

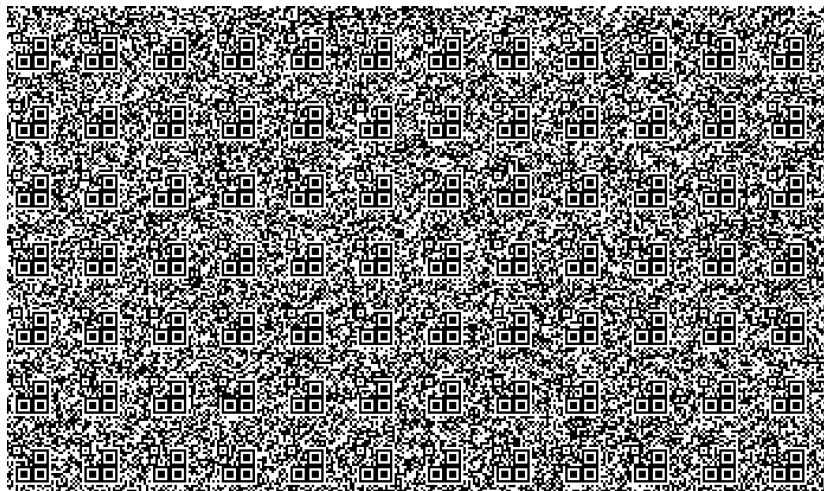


PROGRAMMING 1



PROGRAMMING 2

```
black@blackarch /mnt/backup/s3curity
% nc adctf2014.katsudon.org 43010
^C
black@blackarch /mnt/backup/s3curity
% python s.py
101011110110010110101000110110010010110100010101011000110010010110100010110100
*UNECLECTIC1+*
10101111011010110101100100110010010110110010101001100100101100101011000100100
*THERMOLOGY$W*
101011110110101000101000110110010010100010110101100010100010110101011000100100
*ANEPIPIOIC$*
101011110110101000101011000110100110110101000110110010100010110101100010110010
*ALTARPIECE$V*
101011110110100110110101000110110010101100010110001010110001010101011000110010
*TARIFFLESSG2*
101011110110010100110010010101100100101100010110101100110100010110010010101000
*DEHISCENCEG9*
101011110110100010101100100101011000100101100110110010110101000101011000101100
*CHLORALIDECD*
101011110100010110110110010110010010110101100101100100100101100110110010110100
*PRESHORTEN0/*
101011110110100110110101000110010010101000110101100010110101000110001010110010
*TAENIAFUGEKV*
101011110101000110110010110110100010101100010110001010110010010110110010100100
*NUCIFEROUSMU*
the flag is: ADCTF_4R3_y0U_B4rC0d3_R34D3r
```



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_wlth_r3v3R$iNg}
-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
[*] Current password: -----_mUcH_FuN_wlth_r3v3R$iNg}
-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
[*] Current password: -----0_mUcH_FuN_wlth_r3v3R$iNg}
-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
[*] Current password: -----$0_mUcH_FuN_wlth_r3v3R$iNg}
-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
[*] Current password: -----${0_mUcH_FuN_wlth_r3v3R$iNg}
-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
[*] Current password: ---g{$0_mUcH_FuN_wlth_r3v3R$iNg}
-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
[*] Current password: --ag{$0_mUcH_FuN_wlth_r3v3R$iNg}
-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
[*] Current password: -lag{$0_mUcH_FuN_wlth_r3v3R$iNg}
-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
[*] Current password: flag{$0_mUcH_FuN_wlth_r3v3R$iNg}
[*] Password founded: flag{$0_mUcH_FuN_wlth_r3v3R$iNg}
```



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

- APK decompile
- IOS forensic
- Android kernel exploitation

ETKİNLİKLER

TÜRKİYE?

- 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

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

Sunumu kaynak kodları ile beraber Github adresimde bulabilirsiniz.

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