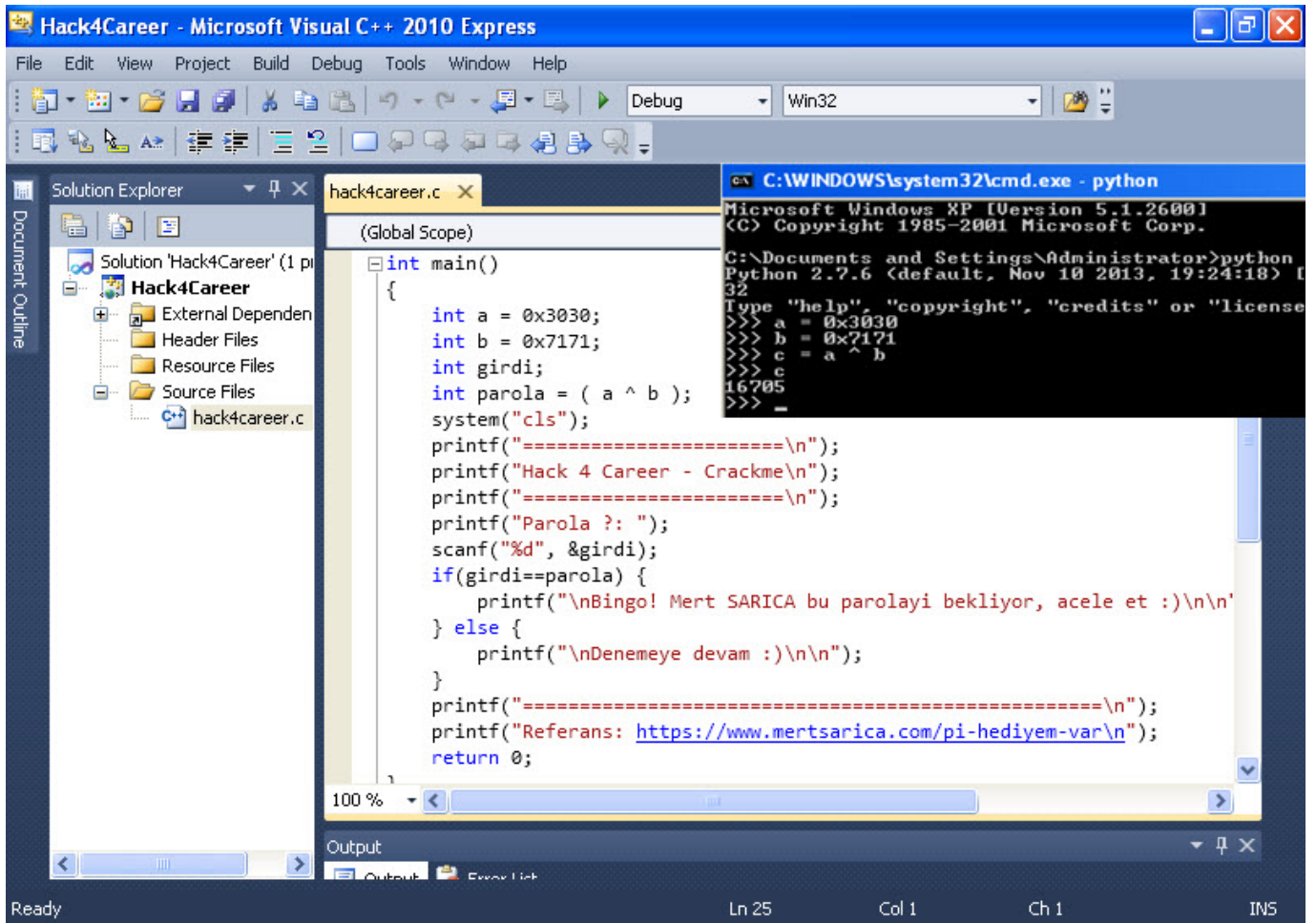


# Pi Hediye Vardı, Verdim, Gitti :)

written by Mert SARICA | 3 March 2015

Takip edenleriniz, 13 Şubat 2015 tarihinde parola bulma oyunu ile üniversite öğrencisi olan iki takipçime, Raspberry Pi (B Model) hediye etme kararı aldığımı hatırlayacaklardır. Bu yazıda hem talihli iki takipçimi hem de oyunun çözümünü açıklayacağım.

KAYNAK KODU:



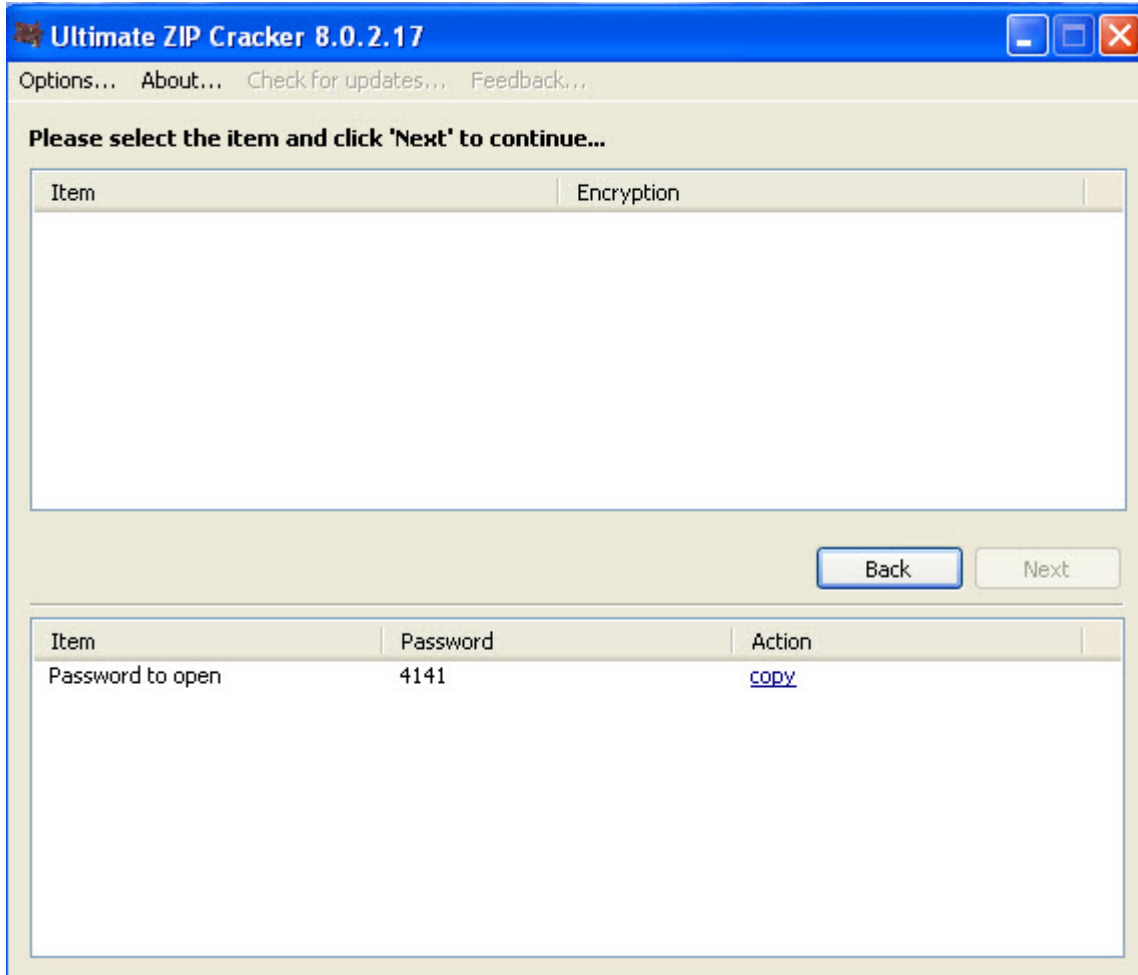
```
hack4career.c
(Global Scope)
int main()
{
    int a = 0x3030;
    int b = 0x7171;
    int girdi;
    int parola = ( a ^ b );
    system("cls");
    printf("=====\n");
    printf("Hack 4 Career - Crackme\n");
    printf("=====\n");
    printf("Parola ?: ");
    scanf("%d", &girdi);
    if(girdi==parola) {
        printf("\nBingo! Mert SARICA bu parolayı bekliyor, acele et :)\n\n");
    } else {
        printf("\nDenemeye devam :)\n\n");
    }
    printf("=====\n");
    printf("Referans: https://www.mertsarica.com/pi-hediye-var\n");
    return 0;
}
```

```
C:\WINDOWS\system32\cmd.exe - python
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

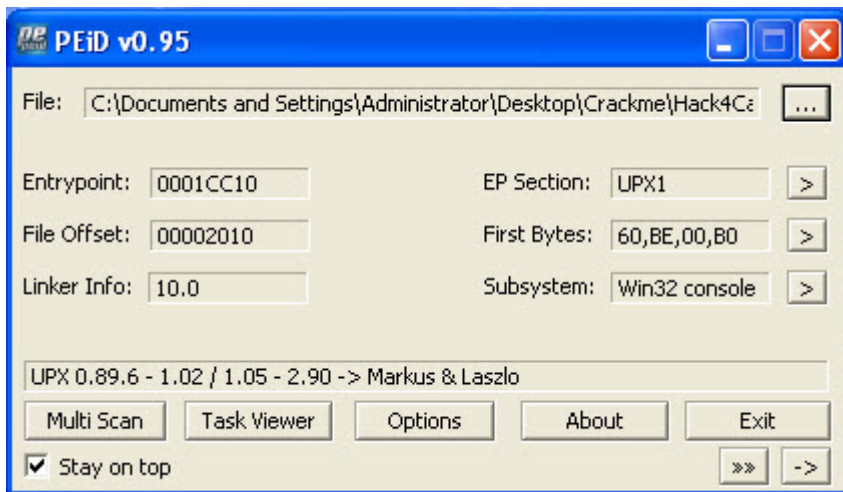
C:\Documents and Settings\Administrator>python
Python 2.7.6 (default, Nov 10 2013, 19:24:18) [
32
Type "help", "copyright", "credits" or "license
>>> a = 0x3030
>>> b = 0x7171
>>> c = a ^ b
>>> c
16705
>>> _
```

ÇÖZÜM:

Crackme.zip ZIP dosyasının şifresi, herhangi basit bir şifre çözme programı ile kolaylıkla bulunabilirdi. (ZIP şifresi: 4141)



ZIP dosyası içinden çıkan Hack4Career.exe programını PEiD aracı ile incelediğinizde bunun UPX aracı ile sıkıştırıldığını görebilir ve yine UPX aracı ile açabilirdiniz.



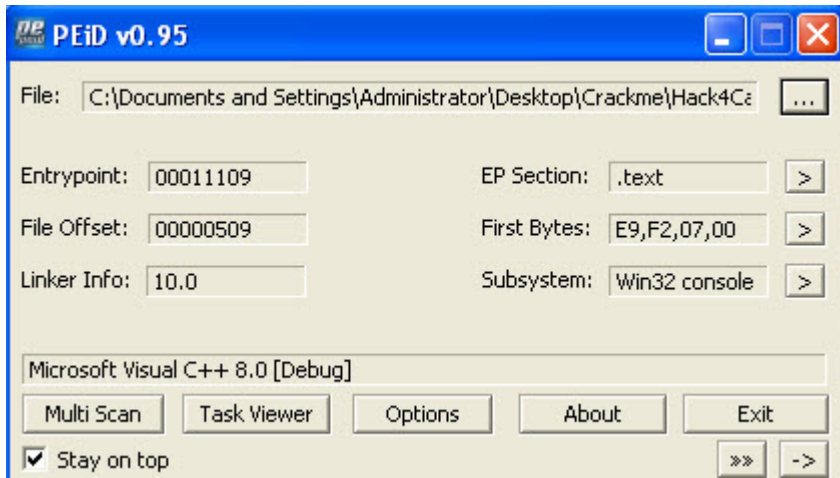
```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd Desktop
C:\Documents and Settings\Administrator\Desktop>cd Crackme
C:\Documents and Settings\Administrator\Desktop\Crackme>upx -d Hack4Career.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2013
UPX 3.09w Markus Oberhumer, Laszlo Molnar & John Reiser Feb 18th 2013

-----
File size      Ratio      Format      Name
-----
29184 <-      9728      33.33%     win32/pe     Hack4Career.exe

Unpacked 1 file.
C:\Documents and Settings\Administrator\Desktop\Crackme>
```

Yine PEiD ile bu programını incelediğinizde programın Visual C++ ile derlendiğini görebilirdiniz.



Hack4Career.exe programını Immunity Debugger aracı (debugger) ile incelediğinizde 004113A0 fonksiyonunda iki değerin (0x3030 ve 0x7171) XOR işleminden geçirildiğini (XOR işleminin sonucu 0x4141), kullanıcıdan alınan girdi (input) ile ondalık değere çevrilerek (0x4141 değerinin ondalık karşılığı 16705'dir.) karşılaştırıldığını görebilir ve 16705 değerini bana ileterek oyunu başarıyla tamamlayabilirdiniz :)

Immunity Debugger - Hack4Career.exe - [CPU - main thread, module Hack4Car]

File View Debug Plugins Immlib Options Window Help Jobs

Immunity: Consulting Services Ma

```

00411109 E9 F2070000 JMP Hack4Car.00411900
0041110E E9 9D150000 JMP Hack4Car.004126B0
00411113 E9 18160000 JMP Hack4Car.00412730
00411118 E9 8F240000 JMP <JMP.&KERNEL32.QueryPerformanceCount
0041111D E9 42040000 JMP <JMP.&MSUCR100D.scanF>
00411122 E9 BD220000 JMP <JMP.&MSUCR100D._unlock>
00411127 E9 92240000 JMP <JMP.&KERNEL32.GetCurrentProcessId>
0041112C E9 3F050000 JMP Hack4Car.00411670
00411131 E9 7E180000 JMP <JMP.&MSUCR100D._set_app_type>
00411136
0041113E
00411146
00411145
00411140
0041114F
00411154
00411153
0041115E
00411163
00411168
0041116D
00411172
00411177
0041117C
00411181
00411186
0041118E
00411196
00411195
0041119F
0041119F
004111A4
004111A5
004111A5
004111B3
004111B3
004111B8
004111D0
004111C2
004111C2
004111C0
004111C0
004111CE
004111CF
004111D0
004111D1
00411900

```

C:\Documents and Settings\Administrator\Desktop\Crackme\Hack4Career.exe

```

=====
Hack 4 Career - Crackme
=====
Parola ? : _

```

Modules C:\WINDOWS\system32\RPCRT4.dll Running

Immunity Debugger - Hack4Career.exe - [CPU - main thread, module Hack4Car]

File View Debug Plugins Immlib Options Window Help Jobs

Code auditor and software assess

```

004119A0 55 PUSH EBP
004119A1 8BEC MOV EBP,ESP
004119A3 81EC F0000000 SUB ESP,0F0
004119A9 53 PUSH EBX
004119AA 56 PUSH ESI
004119AB 57 PUSH EDI
004119AC 80BD 10FFFFFF LEA EDI,DWORD PTR SS:[EBP-F0]
004119B2 B9 3C000000 MOV ECX,3C
004119B7 B8 CCCCCCCC MOV EAX,CCCCCCCC
004119BC F3AB REP STOS DWORD PTR ES:[EDI]
004119BE C745 F8 30300000 MOV DWORD PTR SS:[EBP-8],3030
004119C5 C745 EC 71710000 MOV DWORD PTR SS:[EBP-14],7171
004119C8 3346 E8 MOV EAX,DWORD PTR SS:[EBP-8]
004119CF 3346 E8 XOR EAX,DWORD PTR SS:[EBP-14]
004119D2 8945 D4 MOV DWORD PTR SS:[EBP-2C],EAX
004119D5 8BF4 MOV ESI,ESP
004119D7 68 70584100 PUSH Hack4Car.00415870 ASCII "cls"
004119DC FF15 B4824100 CALL DWORD PTR DS:[&MSUCR100D.system] MSUCR100.system
004119E2 83C4 04 ADD ESP,4
004119E5 3BF4 CMP ESI,ESP
004119E7 E8 4AFDFFFF CALL Hack4Car.00411136
004119EC 8BF4 MOV ESI,ESP
004119EE 68 50584100 PUSH Hack4Car.00415850 ASCII "=====
004119F3 FF15 B8824100 CALL DWORD PTR DS:[&MSUCR100D.printf] MSUCR100.printf
004119F9 83C4 04 ADD ESP,4
004119FC 3BF4 CMP ESI,ESP
004119FE E8 33FDFFFF CALL Hack4Car.00411136
00411A03 8BF4 MOV ESI,ESP
00411A05 68 30584100 PUSH Hack4Car.00415830 ASCII "Hack 4 Career - Crackme
00411A0A FF15 B8824100 CALL DWORD PTR DS:[&MSUCR100D.printf] MSUCR100.printf
00411A10 83C4 04 ADD ESP,4
00411A13 3BF4 CMP ESI,ESP
00411A15 E8 1CEDEEEE CALL Hack4Car.00411136

```

Registers (FPU)

```

EAX 003A30A0
ECX 003A2B40
EDX 00000001
EBX 7FFDB000
ESP 0012FF6C
EBP 0012FFB8
ESI 00790074
EDI 0069006E
EIP 004113A0 Hack4Car.004113A0
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_PROC_NOT_FOUND
EFL 00000202 (NO,NB,NE,A,NS,PO,GE)
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
FST 0000 Cond 0 0 0 0 Err 0 0 0
FCW 027F Prec NEAR,53 Mask

```

Address	Hex dump	ASCII
00417000	01 00 00 00 01 00 00 00	0...0...
00417008	01 00 00 00 01 00 00 00	0...0...
00417010	01 00 00 00 00 00 00 00	0.....0
00417018	FE FF FF FF 01 00 00 00	# 0...
00417020	FF FF FF FF FF FF FF	.....+
00417028	00 00 00 00 C1 63 78 3A	...+c#:
00417030	3E 3C 87 C5 00 00 00 00	>#?....
00417038	00 00 00 00 00 00 00 00	.....
00417040	00 00 00 00 00 00 00 00	.....
00417048	00 00 00 00 00 00 00 00	.....
00417050	00 00 00 00 00 00 00 00	.....

0012FE6C 00411A0F →A. RETURN

Show references Paused



Immunity Debugger - Hack4Career.exe - [CPU - main thread, module Hack4Car]

File View Debug Plugins Immlib Options Window Help Jobs

Immunity: Consulting Services Ma

```

0041144A 8D45 E0      LEA EAX, DWORD PTR SS:[EBP-20]
0041144D 50          PUSH EAX
0041144E 68 1C584100 PUSH Hack4Car.0041581C      ASCII "%d"
00411453 FF15 C0824100 CALL DWORD PTR DS:[&MSUCR100.scanf] MSUCR100.scanf
00411459 83C4 08      ADD ESP, 8
0041145C 3BF4        CMP ESI, ESP
0041145E E8 D3FCFFFF CALL Hack4Car.00411136
00411463 8B45 E0      MOV EAX, DWORD PTR SS:[EBP-20]
00411466 3B45 D4      CMP EAX, DWORD PTR SS:[EBP-2C]
00411469 75 19        JNZ SHORT Hack4Car.00411484
0041146B 8BF4        MOV ESI, ESP
0041146D 68 D8574100 PUSH Hack4Car.004157D8      ASCII 0A,"Bingo! Mer"
00411472 FF15 B8824100 CALL DWORD PTR DS:[&MSUCR100.printf] MSUCR100.printf
00411478 83C4 04      ADD ESP, 4
0041147B 3BF4        CMP ESI, ESP
0041147D E8 B4FCFFFF CALL Hack4Car.00411136
00411482 EB 17        JMP SHORT Hack4Car.0041149B
00411484 8BF4        MOV ESI, ESP
00411486 68 BC574100 PUSH Hack4Car.004157BC      ASCII 0A,"Denemeye d"
0041148B FF15 B8824100 CALL DWORD PTR DS:[&MSUCR100.printf] MSUCR100.printf
00411491 83C4 04      ADD ESP, 4
00411494 3BF4        CMP ESI, ESP
00411496 E8 9BFCFFFF CALL Hack4Car.00411136
0041149B 8BF4        MOV ESI, ESP
0041149D 68 7C574100 PUSH Hack4Car.0041577C      ASCII "=====
004114A2 FF15 B8824100 CALL DWORD PTR DS:[&MSUCR100.printf] MSUCR100.printf
004114A8 83C4 04      ADD ESP, 4
004114AB 3BF4        CMP ESI, ESP
004114AD E8 84FCFFFF CALL Hack4Car.00411136
004114B2 8BF4        MOV ESI, ESP
004114B4 68 3C574100 PUSH Hack4Car.0041573C      ASCII "Referans: https://www.m
004114B9 FF15 B8824100 CALL DWORD PTR DS:[&MSUCR100.printf] MSUCR100.printf
004114BE 83C4 04      ADD ESP, 4
  
```

Registers (FPU)

```

EAX 003A30A0
ECX 003A2B40
EDX 00000001
EBX 7FFDB000
ESP 0012FF6C
EBP 0012FFB8
ESI 00790074
EDI 0069006E
EIP 004113A0 Hack4Car.004113A0
  
```

Address Hex dump ASCII

```

00417000 01 00 00 00 01 00 00 00 0...0...
00417008 01 00 00 00 01 00 00 00 0...0...
00417010 01 00 00 00 00 00 00 00 0...0...
00417018 FE FF FF FF 01 00 00 00 0...0...
00417020 FF FF FF FF FF FF FF FF
00417028 00 00 00 00 C1 63 78 3A ...+cw:
00417030 3F 3C 87 C5 00 00 00 00 >8pt+...
00417040 00 00 00 00 00 00 00 00
00417048 00 00 00 00 00 00 00 00
00417050 00 00 00 00 00 00 00 00
  
```

0012FF6C 00411AD5 +A. RETURN

```

0012FF70 00000001 0...
0012FF74 003A2B40 0+...
0012FF78 003A30A0 30:...
0012FF7C 3A6A9C79 u8j:
0012FF80 0069006E n.i:
0012FF84 00790074 t.y:
0012FF88 7FFDB000 7FFDB000
0012FF8C 00369E99 036:
0012FF90 00000000 ...
0012FF94 00000000 ...
0012FF98 00130000 ...! ASCII
0012FF9C 00000000
  
```

Immunity Debugger - Hack4Career.exe - [CPU - main thread, module Hack4Car]

File View Debug Plugins Immlib Options Window Help Jobs

Code auditor and software assess

```

0041144A 8D45 E0      LEA EAX, DWORD PTR SS:[EBP-20]
0041144D 50          PUSH EAX
0041144E 68 1C584100 PUSH Hack4Car.0041581C      ASCII "%d"
00411453 FF15 C0824100 CALL DWORD PTR DS:[&MSUCR100.scanf] MSUCR100.scanf
00411459 83C4 08      ADD ESP, 8
0041145C 3BF4        CMP ESI, ESP
0041145E E8 D3FCFFFF CALL Hack4Car.00411136
00411463 8B45 E0      MOV EAX, DWORD PTR SS:[EBP-20]
00411466 3B45 D4      CMP EAX, DWORD PTR SS:[EBP-2C]
00411469 75 19        JNZ SHORT Hack4Car.00411484
0041146B 8BF4        MOV ESI, ESP
0041146D 68 D8574100 PUSH Hack4Car.004157D8      ASCII 0A,"Bingo! Mer"
00411472 FF15 B8824100 CALL DWORD PTR DS:[&MSUCR100.printf] MSUCR100.printf
00411478 83C4 04      ADD ESP, 4
0041147B 3BF4        CMP ESI, ESP
0041147D E8 B4FCFFFF CALL Hack4Car.00411136
00411482 EB 17        JMP SHORT Hack4Car.0041149B
00411484 8BF4        MOV ESI, ESP
00411486 68 BC574100 PUSH Hack4Car.004157BC      ASCII 0A,"Denemeye d"
0041148B FF15 B8824100 CALL DWORD PTR DS:[&MSUCR100.printf] MSUCR100.printf
00411491 83C4 04      ADD ESP, 4
00411494 3BF4        CMP ESI, ESP
00411496 E8 9BFCFFFF CALL Hack4Car.00411136
0041149B 8BF4        MOV ESI, ESP
0041149D 68 7C574100 PUSH Hack4Car.0041577C      ASCII "=====
004114A2 FF15 B8824100 CALL DWORD PTR DS:[&MSUCR100.printf] MSUCR100.printf
004114A8 83C4 04      ADD ESP, 4
004114AB 3BF4        CMP ESI, ESP
004114AD E8 84FCFFFF CALL Hack4Car.00411136
004114B2 8BF4        MOV ESI, ESP
004114B4 68 3C574100 PUSH Hack4Car.0041573C      ASCII "Referans: https://www.m
004114B9 FF15 B8824100 CALL DWORD PTR DS:[&MSUCR100.printf] MSUCR100.printf
004114BE 83C4 04      ADD ESP, 4
  
```

Registers (FPU)

```

EAX CCCCCCCC
ECX 3B2033AE
EDX 10361F18 MSUCR100.10361F18
EBX 7FFDB000
ESP 0012FF6C
EBP 0012FFB8
ESI 0012FF6C
EDI 0012FF68
EIP 00411466 Hack4Car.00411466
  
```

Stack SS:[0012FF3C]=0004141  
EAX=CCCCCCCC

Address Hex dump ASCII

```

00417000 01 00 00 00 01 00 00 00 0...0...
00417008 01 00 00 00 01 00 00 00 0...0...
00417010 01 00 00 00 00 00 00 00 0...0...
00417018 FE FF FF FF 01 00 00 00 0...0...
00417020 FF FF FF FF FF FF FF FF
00417028 00 00 00 00 C1 63 78 3A ...+cw:
00417030 3F 3C 87 C5 00 00 00 00 >8pt+...
00417040 00 00 00 00 00 00 00 00
00417048 00 00 00 00 00 00 00 00
00417050 00 00 00 00 00 00 00 00
  
```

C:\Documents and Settings\Administrat

Hack 4 Career - Crackme

Parola ?: Mert

Calculator

16705

Hex Dec Oct Bin Degrees Radians Grads

Inv Hyp Backspace CE C

Sta F-E ( ) MC 7 8 9 / Mod And

Ave dms Exp ln MR 4 5 6 \* Or Xor

Sum sin x^y log MS 1 2 3 - Lsh Not

s cos x^3 nl M+ 0 +/- . + = Int

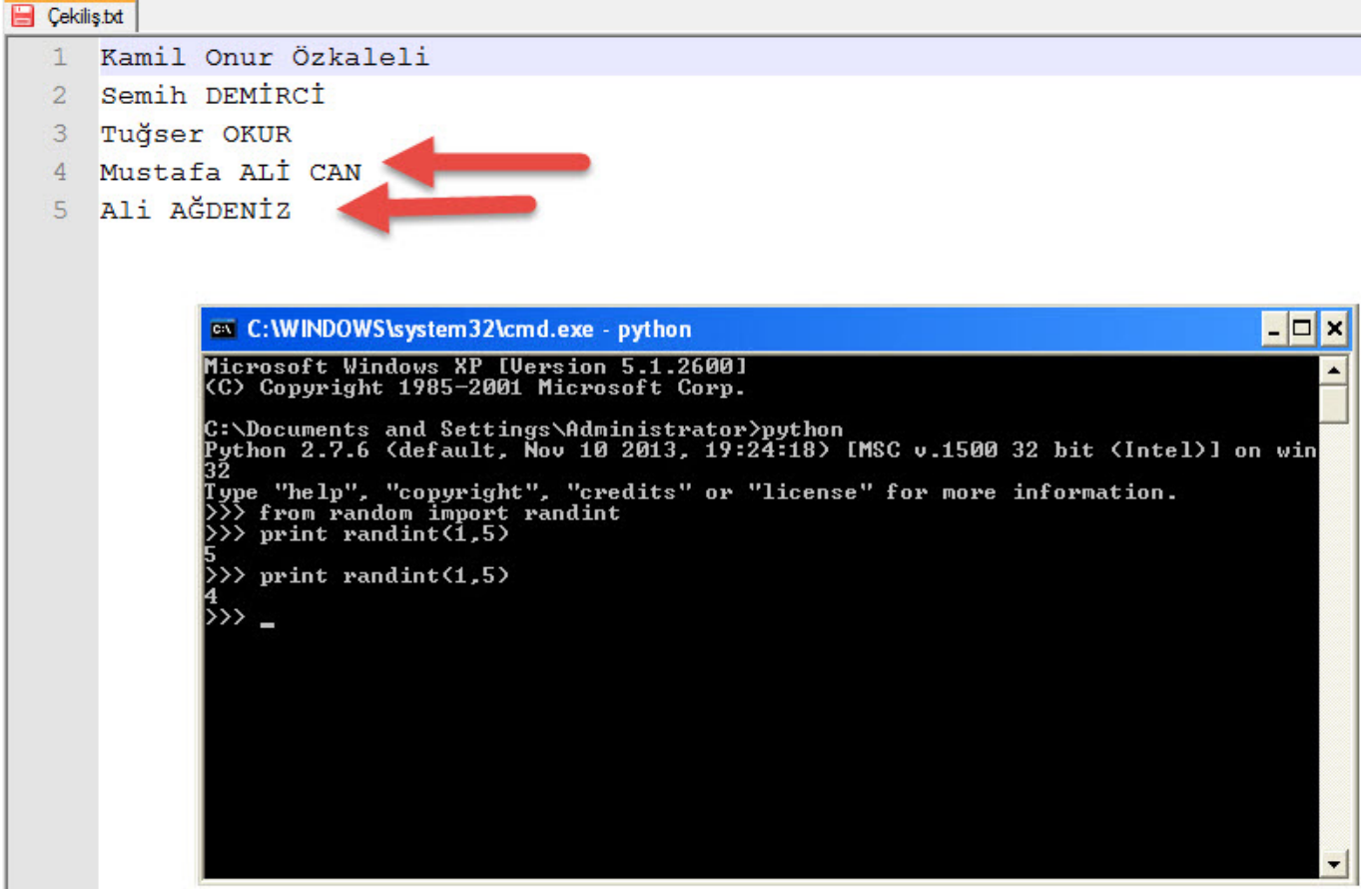
Dat tan x^2 1/x pi A B C D E F

sed

09:21

OYUNU BAŞARIYLA TAMAMLAYANLAR: Kamil Onur Özkaleli, Ali AĞDENİZ, Semih DEMİRCİ, Mustafa ALİ CAN, Musa ANTİKE, Tuğser OKUR, Kenan GÜMÜŞ, Onur ALANBEL, Osman ERÇELİK

ÇEKİLİŞ ve KAZANAN TALİHLİLER:



The image shows two windows. The top window, titled 'Çekiliş.bt', contains a list of names: 1 Kamil Onur Özkaleli, 2 Semih DEMİRCİ, 3 Tuğser OKUR, 4 Mustafa ALİ CAN, and 5 Ali AĞDENİZ. Red arrows point to the names 'Mustafa ALİ CAN' and 'Ali AĞDENİZ'. The bottom window is a command prompt titled 'C:\WINDOWS\system32\cmd.exe - python'. It shows the execution of a Python script that uses the 'randint' function to generate random numbers between 1 and 5. The output shows the number 5, followed by 4, and then a blank line.

```
C:\WINDOWS\system32\cmd.exe - python
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>python
Python 2.7.6 (default, Nov 10 2013, 19:24:18) [MSC v.1500 32 bit (Intel)] on win
32
Type "help", "copyright", "credits" or "license" for more information.
>>> from random import randint
>>> print randint(1,5)
5
>>> print randint(1,5)
4
>>> _
```

Başta kazanan iki talihli (Mustafa ALİ CAN ve Ali AĞDENİZ) olmak üzere parola bulma oyununa katılan ve başarıyla tamamlayan herkesi tebrik eder, yeni oyunlarda görüşmek dileğiyle herkese güvenli günler dilerim :)