



**ESCUELA COLOMBIANA DE INGENIERIA
JULIO GARAVITO**

**IT SECURITY AND PRIVACY
GRUPO 1L**

**OSINT PRACTICE
LABORATORY 4**

**SUBMITTED BY:
JUAN PABLO FERNANDEZ GONZALES
MARIA VALENTINA TORRES MONSALVE**

**SUBMITTED TO:
Ing. DANIEL ESTEBAN VELA LOPEZ**

BOGOTÁ D.C.

**DATE:
03/03/2025**

Tabla de contenido

| | |
|---|---|
| Twitter post Exercise | 2 |
| Objetivo | 3 |
| Metodology | 3 |
| 1. Simple query using Google. | 3 |
| 2. Identification of the festival name using Google Lens..... | 4 |

Reverse Exercise

Objective

The objective of this exercise is to identify la contraseña almacenada

1. Descargamos el archivo y lo almacenamos en una carpeta específica para no confundirlo con otro ejecutable.

```
reverse -- -zsh -- 119x33
WhatsApp Image 2025-02-28 at 23.09.28.jpeg
anydesk.dmg
ar-2.png
ar.png
arXiv-2106.07542v1.tar
babys-first
binaryninja_free_macosx.dmg
componentes.png
contrato.png
debate-2.png
debate.png
derechos-civiles.png
ida-free-pc_90_x64mac.app
illustration-digital-devices-collection
mejoramiento.png
p1245-ma.jpg
p1245-ma.mp4
preload
preparcial
propuesta-comercial.png
prueba
ret
timer.apk
unpackme-upx
www2007-cantina-final-2.pdf
www2007-cantina-final.pdf
~$ia de trabajo 3-8.docx
~$oceso_11001310303120180062400_20241126_20125.docx
~$rmato_informe-laboratorio.docx
maritzamonsalvebautista@MacBook-Pro-de-Maritza Downloads % cd reverse
maritzamonsalvebautista@MacBook-Pro-de-Maritza reverse % ls
ret
maritzamonsalvebautista@MacBook-Pro-de-Maritza reverse %
```

2. Identificamos que el archivo es de tipo: archivo ELF (Ejecutable y Vinculable) de 64 bits.

```
reverse -- -zsh -- 119x33
ar.png
arXiv-2106.07542v1.tar
babys-first
binaryninja_free_macosx.dmg
componentes.png
contrato.png
debate-2.png
debate.png
derechos-civiles.png
ida-free-pc_90_x64mac.app
illustration-digital-devices-collection
mejoramiento.png
p1245-ma.jpg
p1245-ma.mp4
preload
preparcial
propuesta-comercial.png
prueba
ret
timer.apk
unpackme-upx
www2007-cantina-final-2.pdf
www2007-cantina-final.pdf
~$ia de trabajo 3-8.docx
~$oceso_11001310303120180062400_20241126_20125.docx
~$rmato_informe-laboratorio.docx
maritzamonsalvebautista@MacBook-Pro-de-Maritza Downloads % cd reverse
maritzamonsalvebautista@MacBook-Pro-de-Maritza reverse % ls
ret
maritzamonsalvebautista@MacBook-Pro-de-Maritza reverse % file ret
ret: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=888d1ba834fd1239330e280dc72d4af290aca14d, for GNU/Linux 3.2.0, not stripped
maritzamonsalvebautista@MacBook-Pro-de-Maritza reverse %
```

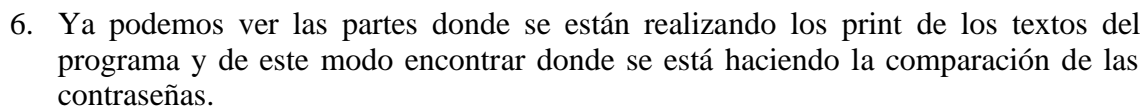
3. Asignamos permisos de ejecución al usuario actual.

```
reverse --zsh -- 119x33
arXiv-2106.07542v1.tar
babys-first
binaryninja_free_macosx.dmg
componentes.png
contrato.png
debate-2.png
debate.png
derechos-civiles.png
ida-free-pc_90_x64mac.app
illustration-digital-devices-collection
mejoramiento.png
p1245-ma.jpg
p1245-ma.mp4
preload
preparcial
propuesta-comercial.png
prueba
ret
timer.apk
unpackme-upx
www2007-cantina-final-2.pdf
www2007-cantina-final.pdf
~$ia de trabajo 3-8.docx
~$oceso_11001310303120180062400_20241126_20125.docx
~$rmato_informe-laboratorio.docx
maritzamonsalvebautista@MacBook-Pro-de-Maritza Downloads % cd reverse
maritzamonsalvebautista@MacBook-Pro-de-Maritza reverse % ls
ret
maritzamonsalvebautista@MacBook-Pro-de-Maritza reverse % file ret
ret: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so
.2, BuildID[sha1]=888d1ba834fd1239330e280dc72d4af290aca14d, for GNU/Linux 3.2.0, not stripped
maritzamonsalvebautista@MacBook-Pro-de-Maritza reverse % chmod u+x ret
maritzamonsalvebautista@MacBook-Pro-de-Maritza reverse %
```

- Para poder ejecutar este programa debemos estar desde una terminal de Linux, en nuestro caso tendremos que instalar un emulador para seguir realizando el ejercicio., luego de esto ejecutaremos el programa con el comando `./ret` y nos pedirá ingresar una contraseña, a lo que ingresamos cualquier cosa y nos sale el mensaje de ***Access denied***

```
jstm_@SEBASTIANTORRES: ~
/home/jstm/.hushlogin file.
jstm_@SEBASTIANTORRES:~$ cp /mnt/c/Users/TU_USUARIO/Downloads/reverse/ret .
cp: cannot stat '/mnt/c/Users/TU_USUARIO/Downloads/reverse/ret': No such file or directory
jstm_@SEBASTIANTORRES:~$ cp /mnt/c/Users/jstm_/Downloads/reverse/ret.unknown
cp: missing destination file operand after '/mnt/c/Users/jstm_/Downloads/reverse/ret.unknown'
Try 'cp --help' for more information.
jstm_@SEBASTIANTORRES:~$ cp /mnt/c/Users/jstm_/Downloads/reverse/ret.unknown .
jstm_@SEBASTIANTORRES:~$ ls
ret.unknown
jstm_@SEBASTIANTORRES:~$ ./ret
-bash: ./ret: No such file or directory
jstm_@SEBASTIANTORRES:~$ chmod u+x ret
chmod: cannot access 'ret': No such file or directory
jstm_@SEBASTIANTORRES:~$ chmod u+x ret.unknown
jstm_@SEBASTIANTORRES:~$ ls -la
total 48
drwxr-xr-x 4 jstm_ jstm_ 4096 Mar 3 23:37 .
drwxr-xr-x 3 root  root  4096 Mar 3 23:35 ..
-rw-r--r-- 1 jstm_ jstm_ 220 Mar 3 23:35 .bash_logout
-rw-r--r-- 1 jstm_ jstm_ 3771 Mar 3 23:35 .bashrc
drwx----- 2 jstm_ jstm_ 4096 Mar 3 23:35 .cache
drwxr-xr-x 2 jstm_ jstm_ 4096 Mar 3 23:35 .landscape
-rw-r--r-- 1 jstm_ jstm_ 0 Mar 3 23:35 .motd_shown
-rw-r--r-- 1 jstm_ jstm_ 807 Mar 3 23:35 .profile
-rwxr-xr-x 1 jstm_ jstm_ 16080 Mar 3 23:37 ret.unknown
jstm_@SEBASTIANTORRES:~$ ./ret.unknown
Enter the password to unlock this file: hdhfgdhfg
You entered: hdhfgdhfg
Access denied
jstm_@SEBASTIANTORRES:~$
```

- Usando Binary Ninja, realizaremos ingeniería inversa



```

000011f8 489545d8 mov     qword [rbp-8x38 (str)], rax (0x7b4654436f636970)
000011fc 489555d8 mov     qword [rbp-8x28 (var_30)], rdx (0x337633725f666c33)
00001200 48b723596e75f mov     rax, 0x75735f676e693572
00001204 48b43535353566 mov     rdx, 0x6c75663353563633
00001214 489545d8 mov     qword [rbp-8x20 (var_20)], rax (0x75735f676e693572)
00001218 489555d8 mov     qword [rbp-8x18 (var_18)], rdx (0x6c75663353563633)
0000121c 48b5f266383133 mov     rax, 0x613133313866325f
00001220 48945f9b mov     qword [rbp-8x10 (var_10)], rax (0x613133313866325f)
00001224 48b3d670d0000 lea     rdi, [rel_data.2080] ("Enter the password to unlock thi...")
00001228 b800000000 mov     eax, 0x0
0000122c e775feffff call    printf
00001230 48b455d8 lea     rax, [rbp-8x60 (var_68)]
00001234 4895c6 mov     rsi, rax (var_68)
00001238 48b3de8d0000 lea     rdi, [rel_data.2031]
0000123c b800000000 mov     eax, 0x0
00001240 e77dfeffff call    __isoc99_scanf
00001244 48b455d8 lea     rax, [rbp-8x60 (var_68)]
00001248 4895c6 mov     rsi, rax (var_68)
0000124c 48b3d670d0000 lea     rdi, [rel_data.2034] ("You entered: %s\n")
00001250 b800000000 mov     eax, 0x0
00001254 e77dfeffff call    printf
00001258 48b455d8 lea     rdx, [rbp-8x80 (str)]
0000125c 48b455d8 lea     rax, [rbp-8x60 (var_68)]
00001260 4895c6 mov     rsi, rdx (str)
00001264 4895c7 mov     rdi, rax (var_68)
00001268 e77dfeffff call    strcmp
0000126c 4895c6 mov     rsi, rax (var_68)
00001270 4895c7 test    eax, eax
00001274 jne     0x129c
00001278 48b3d670d0000 lea     rdi, [rel_data.2048] ("Password correct, please see fla...")
0000127c b800000000 mov     eax, 0x0
00001280 e77dfeffff call    puts
00001284 48b455d8 lea     rax, [rbp-8x38 (str)]
00001288 4895c7 mov     rdi, rax (str)

```

- Identificamos que str es la contraseña almacenada y correcta, mientras que var_68 es la que ingresan los usuarios, llegamos a esta conclusión ya que más arriba se están realizando los procesos de cargar valores en registros (rax y rdx) que luego se almacenan en la pila en la variable str.

```

000011c8 void frame_dummy()
000011cc endbr64
000011d0 jmp     register_tm_clones
000011d4
000011d8
000011dc
000011e0
000011e4
000011e8
000011ec
000011f0
000011f4
000011f8
000011fc
00001200
00001204
00001208
0000120c
00001210
00001214
00001218
0000121c
00001220
00001224
00001228
0000122c
00001230
00001234
00001238
0000123c
00001240
00001244
00001248
0000124c
00001250
00001254
00001258
0000125c
00001260
00001264
00001268
0000126c
00001270
00001274
00001278
0000127c
00001280
00001284
00001288
0000128c
00001290
00001294
00001298
0000129c
000012a0
000012a4
000012a8
000012ac
000012b0
000012b4
000012b8
000012bc
000012c0
000012c4
000012c8
000012cc
000012d0
000012d4
000012d8
000012dc
000012e0
000012e4
000012e8
000012ec
000012f0
000012f4
000012f8
000012fc
00001300
00001304
00001308
0000130c
00001310
00001314
00001318
0000131c
00001320
00001324
00001328
0000132c
00001330
00001334
00001338
0000133c
00001340
00001344
00001348
0000134c
00001350
00001354
00001358
0000135c
00001360
00001364
00001368
0000136c
00001370
00001374
00001378
0000137c
00001380
00001384
00001388
0000138c
00001390
00001394
00001398
0000139c
000013a0
000013a4
000013a8
000013ac
000013b0
000013b4
000013b8
000013bc
000013c0
000013c4
000013c8
000013cc
000013d0
000013d4
000013d8
000013dc
000013e0
000013e4
000013e8
000013ec
000013f0
000013f4
000013f8
000013fc
00001400
00001404
00001408
0000140c
00001410
00001414
00001418
0000141c
00001420
00001424
00001428
0000142c
00001430
00001434
00001438
0000143c
00001440
00001444
00001448
0000144c
00001450
00001454
00001458
0000145c
00001460
00001464
00001468
0000146c
00001470
00001474
00001478
0000147c
00001480
00001484
00001488
0000148c
00001490
00001494
00001498
0000149c
000014a0
000014a4
000014a8
000014ac
000014b0
000014b4
000014b8
000014bc
000014c0
000014c4
000014c8
000014cc
000014d0
000014d4
000014d8
000014dc
000014e0
000014e4
000014e8
000014ec
000014f0
000014f4
000014f8
000014fc
00001500
00001504
00001508
0000150c
00001510
00001514
00001518
0000151c
00001520
00001524
00001528
0000152c
00001530
00001534
00001538
0000153c
00001540
00001544
00001548
0000154c
00001550
00001554
00001558
0000155c
00001560
00001564
00001568
0000156c
00001570
00001574
00001578
0000157c
00001580
00001584
00001588
0000158c
00001590
00001594
00001598
0000159c
000015a0
000015a4
000015a8
000015ac
000015b0
000015b4
000015b8
000015bc
000015c0
000015c4
000015c8
000015cc
000015d0
000015d4
000015d8
000015dc
000015e0
000015e4
000015e8
000015ec
000015f0
000015f4
000015f8
000015fc
00001600
00001604
00001608
0000160c
00001610
00001614
00001618
0000161c
00001620
00001624
00001628
0000162c
00001630
00001634
00001638
0000163c
00001640
00001644
00001648
0000164c
00001650
00001654
00001658
0000165c
00001660
00001664
00001668
0000166c
00001670
00001674
00001678
0000167c
00001680
00001684
00001688
0000168c
00001690
00001694
00001698
0000169c
000016a0
000016a4
000016a8
000016ac
000016b0
000016b4
000016b8
000016bc
000016c0
000016c4
000016c8
000016cc
000016d0
000016d4
000016d8
000016dc
000016e0
000016e4
000016e8
000016ec
000016f0
000016f4
000016f8
000016fc
00001700
00001704
00001708
0000170c
00001710
00001714
00001718
0000171c
00001720
00001724
00001728
0000172c
00001730
00001734
00001738
0000173c
00001740
00001744
00001748
0000174c
00001750
00001754
00001758
0000175c
00001760
00001764
00001768
0000176c
00001770
00001774
00001778
0000177c
00001780
00001784
00001788
0000178c
00001790
00001794
00001798
0000179c
000017a0
000017a4
000017a8
000017ac
000017b0
000017b4
000017b8
000017bc
000017c0
000017c4
000017c8
000017cc
000017d0
000017d4
000017d8
000017dc
000017e0
000017e4
000017e8
000017ec
000017f0
000017f4
000017f8
000017fc
00001800
00001804
00001808
0000180c
00001810
00001814
00001818
0000181c
00001820
00001824
00001828
0000182c
00001830
00001834
00001838
0000183c
00001840
00001844
00001848
0000184c
00001850
00001854
00001858
0000185c
00001860
00001864
00001868
0000186c
00001870
00001874
00001878
0000187c
00001880
00001884
00001888
0000188c
00001890
00001894
00001898
0000189c
000018a0
000018a4
000018a8
000018ac
000018b0
000018b4
000018b8
000018bc
000018c0
000018c4
000018c8
000018cc
000018d0
000018d4
000018d8
000018dc
000018e0
000018e4
000018e8
000018ec
000018f0
000018f4
000018f8
000018fc
00001900
00001904
00001908
0000190c
00001910
00001914
00001918
0000191c
00001920
00001924
00001928
0000192c
00001930
00001934
00001938
0000193c
00001940
00001944
00001948
0000194c
00001950
00001954
00001958
0000195c
00001960
00001964
00001968
0000196c
00001970
00001974
00001978
0000197c
00001980
00001984
00001988
0000198c
00001990
00001994
00001998
0000199c
000019a0
000019a4
000019a8
000019ac
000019b0
000019b4
000019b8
000019bc
000019c0
000019c4
000019c8
000019cc
000019d0
000019d4
000019d8
000019dc
000019e0
000019e4
000019e8
000019ec
000019f0
000019f4
000019f8
000019fc
00001a00
00001a04
00001a08
00001a0c
00001a10
00001a14
00001a18
00001a1c
00001a20
00001a24
00001a28
00001a2c
00001a30
00001a34
00001a38
00001a3c
00001a40
00001a44
00001a48
00001a4c
00001a50
00001a54
00001a58
00001a5c
00001a60
00001a64
00001a68
00001a6c
00001a70
00001a74
00001a78
00001a7c
00001a80
00001a84
00001a88
00001a8c
00001a90
00001a94
00001a98
00001a9c
00001aa0
00001aa4
00001aa8
00001aac
00001ab0
00001ab4
00001ab8
00001abc
00001ac0
00001ac4
00001ac8
00001acc
00001ad0
00001ad4
00001ad8
00001adc
00001ae0
00001ae4
00001ae8
00001aec
00001af0
00001af4
00001af8
00001afc
00001b00
00001b04
00001b08
00001b0c
00001b10
00001b14
00001b18
00001b1c
00001b20
00001b24
00001b28
00001b2c
00001b30
00001b34
00001b38
00001b3c
00001b40
00001b44
00001b48
00001b4c
00001b50
00001b54
00001b58
00001b5c
00001b60
00001b64
00001b68
00001b6c
00001b70
00001b74
00001b78
00001b7c
00001b80
00001b84
00001b88
00001b8c
00001b90
00001b94
00001b98
00001b9c
00001ba0
00001ba4
00001ba8
00001bac
00001bb0
00001bb4
00001bb8
00001bbc
00001bc0
00001bc4
00001bc8
00001bcc
00001bd0
00001bd4
00001bd8
00001bdc
00001be0
00001be4
00001be8
00001bec
00001bf0
00001bf4
00001bf8
00001bfc
00001c00
00001c04
00001c08
00001c0c
00001c10
00001c14
00001c18
00001c1c
00001c20
00001c24
00001c28
00001c2c
00001c30
00001c34
00001c38
00001c3c
00001c40
00001c44
00001c48
00001c4c
00001c50
00001c54
00001c58
00001c5c
00001c60
00001c64
00001c68
00001c6c
00001c70
00001c74
00001c78
00001c7c
00001c80
00001c84
00001c88
00001c8c
00001c90
00001c94
00001c98
00001c9c
00001ca0
00001ca4
00001ca8
00001cac
00001cb0
00001cb4
00001cb8
00001cbc
00001cc0
00001cc4
00001cc8
00001ccc
00001cd0
00001cd4
00001cd8
00001cdc
00001ce0
00001ce4
00001ce8
00001cec
00001cf0
00001cf4
00001cf8
00001cfc
00001d00
00001d04
00001d08
00001d0c
00001d10
00001d14
00001d18
00001d1c
00001d20
00001d24
00001d28
00001d2c
00001d30
00001d34
00001d38
00001d3c
00001d40
00001d44
00001d48
00001d4c
00001d50
00001d54
00001d58
00001d5c
00001d60
00001d64
00001d68
00001d6c
00001d70
00001d74
00001d78
00001d7c
00001d80
00001d84
00001d88
00001d8c
00001d90
00001d94
00001d98
00001d9c
00001da0
00001da4
00001da8
00001dac
00001db0
00001db4
00001db8
00001dbc
00001dc0
00001dc4
00001dc8
00001dcc
00001dd0
00001dd4
00001dd8
00001ddc
00001de0
00001de4
00001de8
00001dec
00001df0
00001df4
00001df8
00001dfc
00001e00
00001e04
00001e08
00001e0c
00001e10
00001e14
00001e18
00001e1c
00001e20
00001e24
00001e28
00001e2c
00001e30
00001e34
00001e38
00001e3c
00001e40
00001e44
00001e48
00001e4c
00001e50
00001e54
00001e58
00001e5c
00001e60
00001e64
00001e68
00001e6c
00001e70
00001e74
00001e78
00001e7c
00001e80
00001e84
00001e88
00001e8c
00001e90
00001e94
00001e98
00001e9c
00001ea0
00001ea4
00001ea8
00001eac
00001eb0
00001eb4
00001eb8
00001ebc
00001ec0
00001ec4
00001ec8
00001ecc
00001ed0
00001ed4
00001ed8
00001edc
00001ee0
00001ee4
00001ee8
00001eec
00001ef0
00001ef4
00001ef8
00001efc
00001f00
00001f04
00001f08
00001f0c
00001f10
00001f14
00001f18
00001f1c
00001f20
00001f24
00001f28
00001f2c
00001f30
00001f34
00001f38
00001f3c
00001f40
00001f44
00001f48
00001f4c
00001f50
00001f54
00001f58
00001f5c
00001f60
00001f64
00001f68
00001f6c
00001f70
00001f74
00001f78
00001f7c
00001f80
00001f84
00001f88
00001f8c
00001f90
00001f94
00001f98
00001f9c
00001fa0
00001fa4
00001fa8
00001fac
00001fb0
00001fb4
00001fb8
00001fbc
00001fc0
00001fc4
00001fc8
00001fcc
00001fd0
00001fd4
00001fd8
00001fdc
00001fe0
00001fe4
00001fe8
00001fec
00001ff0
00001ff4
00001ff8
00001ffc
00002000
00002004
00002008
0000200c
00002010
00002014
00002018
0000201c
00002020
00002024
00002028
0000202c
00002030
00002034
00002038
0000203c
00002040
00002044
00002048
0000204c
00002050
00002054
00002058
0000205c
00002060
00002064
00002068
0000206c
00002070
00002074
00002078
0000207c
00002080
00002084
00002088
0000208c
00002090
00002094
00002098
0000209c
000020a0
000020a4
000020a8
000020ac
000020b0
000020b4
000020b8
000020bc
000020c0
000020c4
000020c8
000020cc
000020d0
000020d4
000020d8
000020dc
000020e0
000020e4
000020e8
000020ec
000020f0
000020f4
000020f8
000020fc
00002100
00002104
00002108
0000210c
00002110
00002114
00002118
0000211c
00002120
00002124
00002128
0000212c
00002130
00002134
00002138
0000213c
00002140
00002144
00002148
0000214c
00002150
00002154
00002158
0000215c
00002160
00002164
00002168
0000216c
00002170
00002174
00002178
0000217c
00002180
00002184
00002188
0000218c
00002190
00002194
00002198
0000219c
000021a0
000021a4
000021a8
000021ac
000021b0
000021b4
000021b8
000021bc
000021c0
000021c4
000021c8
000021cc
000021d0
000021d4
000021d8
000021dc
000021e0
000021e4
000021e8
000021ec
000021f0
000021f4
000021f8
000021fc
00002200
00002204
00002208
0000220c
00002210
00002214
00002218
0000221c
00002220
00002224
00002228
0000222c
00002230
00002234
00002238
0000223c
00002240
00002244
00002248
0000224c
00002250
00002254
00002258
0000225c
00002260
00002264
00002268
0000226c
00002270
00002274
00002278
0000227c
00002280
00002284
00002288
0000228c
00002290
00002294
00002298
0000229c
000022a0
000022a4
000022a8
000022ac
000022b0
000022b4
000022b8
000022bc
000022c0
000022c4
000022c8
000022cc
000022d0
000022d4
000022d8
000022dc
000022e0
000022e4
000022e8
000022ec
000022f0
000022f4
000022f8
000022fc
00002300
00002304
00002308
0000230c
00002310
00002314
00002318
0000231c
00002320
00002324
00002328
0000232c
00002330
00002334
00002338
0000233c
00002340
00002344
00002348
0000234c
00002350
00002354
00002358
0000235c
00002360
00002364
00002368
0000236c
00002370
00002374
00002378
0000237c
00002380
00002384
00002388
0000238c
00002390
00002394
00002398
0000239c
000023a0
000023a4
000023a8
000023ac
000023b0
000023b4
000023b8
000023bc
000023c0
000023c4
000023c8
000023cc
000023d0
000023d4
000023d8
000023dc
000023e0
000023e4
000023e8
000023ec
000023f0
000023f4
000023f8
000023fc
00002400
00002404
00002408
0000240c
00002410
00002414
00002418
0000241c
00002420
00002424
00002428
0000242c
00002430
00002434
00002438
0000243c
00002440
00002444
00002448
0000244c
00002450
00002454
00002458
0000245c
00002460
00002464
00002468
0000246c
00002470
00002474
00002478
0000247c
00002480
00002484
00002488
0000248c
00002490
00002494
00002498
0000249c
000024a0
000024a4
000024a8
000024ac
000024b0
000024b4
000024b8
000024bc
000024c0
000024c4
000024c8
000024cc
000024d0
000024d4
000024d8
000024dc
000024e0
00
```

From: Hexadecimal To: Text

Open File Sample

Paste hex code numbers or drop file

70 69 63 6f 43 54 46 7b

Character encoding: ASCII

Convert Reset Swap

picoCTF{

9. La siguiente instrucción será 000011ee con el valor 0x337633725f666c33

From: Hexadecimal To: Text

Open File Sample

Paste hex code numbers or drop file

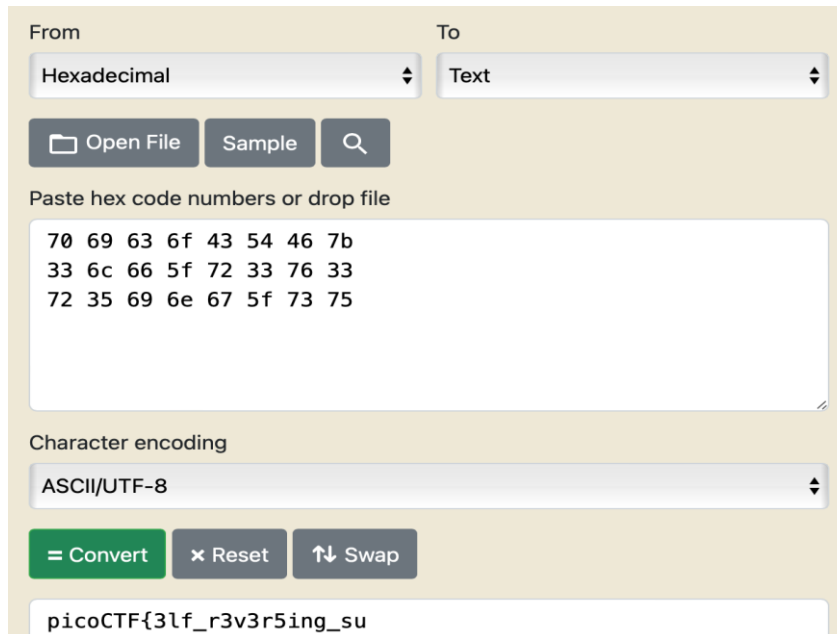
70 69 63 6f 43 54 46 7b
33 6c 66 5f 72 33 76 33

Character encoding: ASCII

Convert Reset Swap

picoCTF{3lf_r3v3

10. 00001200 con valor , 0x75735f676e693572



From: Hexadecimal To: Text

Open File Sample

Paste hex code numbers or drop file

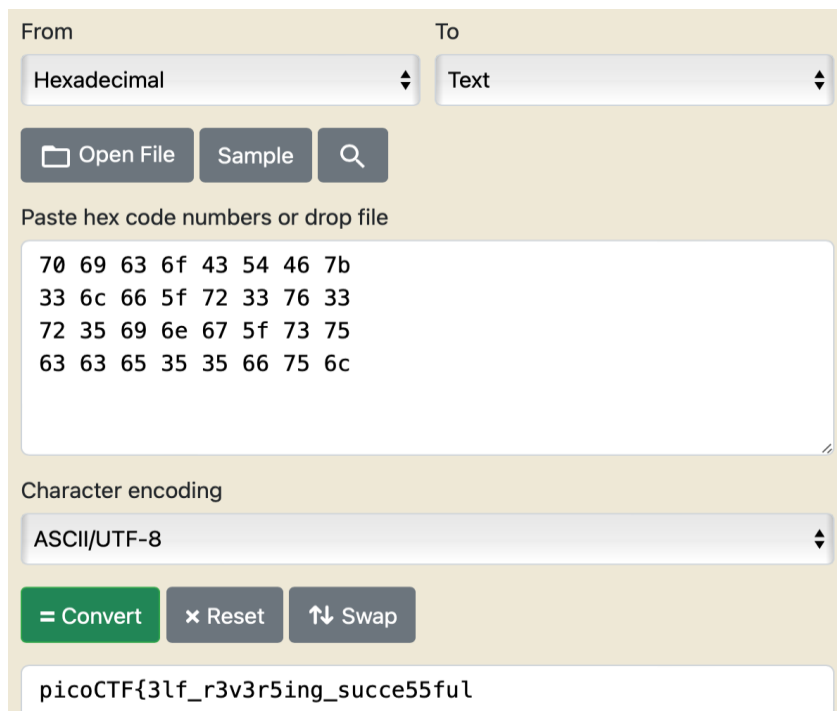
```
70 69 63 6f 43 54 46 7b
33 6c 66 5f 72 33 76 33
72 35 69 6e 67 5f 73 75
```

Character encoding: ASCII/UTF-8

= Convert x Reset ↑↓ Swap

picoCTF{3lf_r3v3r5ing_su

11. 0000120 con valor, 0x6c75663535656363



From: Hexadecimal To: Text

Open File Sample

Paste hex code numbers or drop file

```
70 69 63 6f 43 54 46 7b
33 6c 66 5f 72 33 76 33
72 35 69 6e 67 5f 73 75
63 63 65 35 35 66 75 6c
```

Character encoding: ASCII/UTF-8

= Convert x Reset ↑↓ Swap

picoCTF{3lf_r3v3r5ing_succe55ful

Ejecutaremos el programa. Nos pedirá una contraseña.


```
jstm_@SEBASTIANTORRES: ~
/home/jstm_/.hushlogin file.
jstm_@SEBASTIANTORRES:~$ cp /mnt/c/Users/TU_USUARIO/Downloads/reverse/ret .
cp: cannot stat '/mnt/c/Users/TU_USUARIO/Downloads/reverse/ret': No such file or directory
jstm_@SEBASTIANTORRES:~$ cp /mnt/c/Users/jstm_/Downloads/reverse/ret.unknown
cp: missing destination file operand after '/mnt/c/Users/jstm_/Downloads/reverse/ret.unknown'
Try 'cp --help' for more information.
jstm_@SEBASTIANTORRES:~$ cp /mnt/c/Users/jstm_/Downloads/reverse/ret.unknown .
jstm_@SEBASTIANTORRES:~$ ls
ret.unknown
jstm_@SEBASTIANTORRES:~$ ./ret
-bash: ./ret: No such file or directory
jstm_@SEBASTIANTORRES:~$ chmod u+x ret
chmod: cannot access 'ret': No such file or directory
jstm_@SEBASTIANTORRES:~$ chmod u+x ret.unknown
jstm_@SEBASTIANTORRES:~$ ls -la
total 48
drwxr-xr-x 4 jstm_ jstm_ 4096 Mar 3 23:37 .
drwxr-xr-x 3 root  root  4096 Mar 3 23:35 ..
-rw-r--r-- 1 jstm_ jstm_ 220 Mar 3 23:35 .bash_logout
-rw-r--r-- 1 jstm_ jstm_ 3771 Mar 3 23:35 .bashrc
drwx----- 2 jstm_ jstm_ 4096 Mar 3 23:35 .cache
drwxr-xr-x 2 jstm_ jstm_ 4096 Mar 3 23:35 .landscape
-rw-r--r-- 1 jstm_ jstm_ 0 Mar 3 23:35 .motd_shown
-rw-r--r-- 1 jstm_ jstm_ 807 Mar 3 23:35 .profile
-rwxr-xr-x 1 jstm_ jstm_ 16888 Mar 3 23:37 ret.unknown
jstm_@SEBASTIANTORRES:~$ ./ret.unknown
Enter the password to unlock this file: hdhfgdhfg
You entered: hdhfgdhfg
Access denied
jstm_@SEBASTIANTORRES:~$
```

Con gdb haremos un pequeño debugg y analizaremos la comparación de contraseñas.

```
jstm_@SEBASTIANTORRES: ~
Setting up libsource-highlight4t64:amd64 (3.1.9-4.3build1) ...
Setting up gdb (15.0.50.20240403-0ubuntu1) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
jstm_@SEBASTIANTORRES:~$ gdb ./ret.unknown
GNU gdb (Ubuntu 15.0.50.20240403-0ubuntu1) 15.0.50.20240403-git
Copyright (C) 2024 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./ret.unknown...
(No debugging symbols found in ./ret.unknown)
(gdb) start
Temporary breakpoint 1 at 0x11d1
Starting program: /home/jstm_/ret.unknown
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Temporary breakpoint 1, 0x0000555555551d1 in main ()
(gdb)
```

```

jstm_@SEBASTIANTORRES: ~
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./ret.unknown...
(No debugging symbols found in ./ret.unknown)
(gdb) start
Temporary breakpoint 1 at 0x11d1
Starting program: /home/jstm_/ret.unknown
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Temporary breakpoint 1, 0x00005555555511d1 in main ()
(gdb) break strcmp
Breakpoint 2 at 0x7ffff7f30f90: strcmp. (2 locations)
(gdb) c
Continuing.
Enter the password to unlock this file: ghfghdgd
You entered: ghfghdgd

Breakpoint 2.1, __strcmp_avx2 () at ../sysdeps/x86_64/multiarch/strcmp-avx2.S:206
warning: 206 ../sysdeps/x86_64/multiarch/strcmp-avx2.S: No such file or directory
(gdb)
  
```

```

jstm_@SEBASTIANTORRES: ~
Breakpoint 2.1, __strcmp_avx2 () at ../sysdeps/x86_64/multiarch/strcmp-avx2.S:206
warning: 206 ../sysdeps/x86_64/multiarch/strcmp-avx2.S: No such file or directory
(gdb) info reg
rax      0x7fffffffdf70      140737488346992
rbx      0x7fffffffef08      140737488347384
rcx      0x0
rdx      0x7fffffffdfa0      140737488347040
rsi      0x7fffffffdfa0      140737488347040
rdi      0x7fffffffdf70      140737488346992
rbp      0x7fffffffdfd0      0x7fffffffdfd0
rsp      0x7fffffffdf68      0x7fffffffdf68
r8       0x73                115
r9       0x0
r10      0xffffffff          4294967295
r11      0x202                514
r12      0x1
r13      0x0
r14      0x0
r15      0x7ffff7ffdf000      140737354125312
rip      0x7ffff7f30f90      0x7ffff7f30f90 <__strcmp_avx2>
eflags   0x246                [ PF ZF IF ]
cs       0x33                51
ss       0x2b                43
ds       0x0
es       0x0
fs       0x0
gs       0x0
fs_base  0x7ffff7da3740      140737351661376
gs_base  0x0
(gdb) x/
  
```

```
jstm_@SEBASTIANTORRES: ~ + - v
rbp      0x7fffffffdfdf0  0x7fffffffdfdf0
rsp      0x7fffffffdf68  0x7fffffffdf68
r8        0x73          115
r9        0x0           0
r10       0xffffffff    4294967295
r11       0x202        514
r12       0x1          1
r13       0x0           0
r14       0x0           0
r15       0x7ffff7ffd000 140737354125312
rip      0x7ffff7f30f90  0x7ffff7f30f90 <__strcmp_avx2>
eflags    0x246          [ PF ZF IF ]
cs        0x33          51
ss        0x2b          43
ds        0x0           0
es        0x0           0
fs        0x0           0
gs        0x0           0
fs_base   0x7ffff7da3740 140737351661376
gs_base   0x0           0
(gdb) x/s $rsi
0x7fffffffdfa0: "picoCTF{3lf_r3v3r5ing_succe55ful_2f0131a"
(gdb) x/s $rdi
0x7fffffffdf70: "ghfghdgd"
(gdb) quit
A debugging session is active.

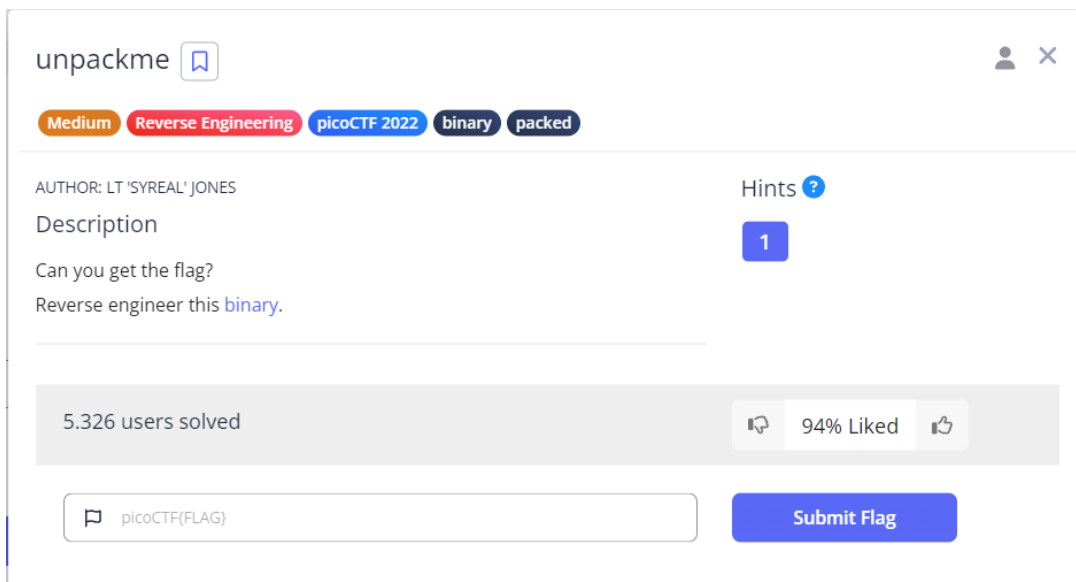
Inferior 1 [process 1166] will be killed.

Quit anyway? (y or n) E
```

Al final con la contraseña obtenida habremos encontrado la bandera.

[illegible]

SEGUNDO EJERCICIO



Primero tendremos que descargar el archivo. En este caso como el archivo es un archivo binario tendremos que modificarlo de tal manera que podamos ejecutarlo. Para esto haremos lo siguiente (en mi caso no tengo una maquina con sistema operativo linux) usaremos primero un comando para descargar un entorno de linux en windows y facilitar asi la manipulacion de los archivos y ejecutables.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\WINDOWS\system32> wsl --install
Ubuntu ya está instalado.
Iniciando Ubuntu...
Installing, this may take a few minutes...
Please create a default UNIX user account. The username does not need to match your Windows username.
For more information visit: https://aka.ms/wslusers
Enter new UNIX username: juanito
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
New password:
Retype new password:
passwd: password updated successfully
Installation successful!
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

Ahora después de haber ejecutado ese comando visto en la imagen, y después de haber terminado toda la instalación. Procederemos a obtener el archivo del reto.

```
home/juanito/.hushlogin file.
juanito@DESKTOP-J5LE1JC:~$ ls
juanito@DESKTOP-J5LE1JC:~$ cp /mnt/c/Users/juanp/Downloads/spti/unpackme-upx ~/
juanito@DESKTOP-J5LE1JC:~$ ls
unpackme-upx
```

Ahora si podremos ejecutarlo

```
juanito@DESKTOP-J5LE1JC:~$ chmod +x ~/unpackme-upx
juanito@DESKTOP-J5LE1JC:~$ ./unpackme-upx
What's my favorite number?
```

```
strings unpackme-upx | grep "UPX"
```

```

juanito@PCjuanpis:~$ strings unpackme-upx | grep "UPX"
UPX!<
$Info: This file is packed with the UPX executable packer http://upx.sf.net $
$Id: UPX 3.95 Copyright (C) 1996-2018 the UPX Team. All Rights Reserved. $
UPX!u
UPX!
UPX!
juanito@PCjuanpis:~$

```

```

juanito@PCjuanpis:~/upx-4.2.2-amd64_linux$ cd ..
juanito@PCjuanpis:~$ /snap/bin/upx -d unpackme-upx
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2024
UPX 4.2.2      Markus Oberhumer, Laszlo Molnar & John Reiser      Jan 3rd 2024

      File size      Ratio      Format      Name
-----
1006445 <-  379188  37.68%  linux/amd64  unpackme-upx

Unpacked 1 file.
juanito@PCjuanpis:~$

```

The screenshot displays the Unpackme-uxp application interface. The top menu bar includes File, Edit, View, Analysis, Window, and Help. The main window is divided into three panes:

- Symbols:** Lists various symbols and their addresses, such as `_Unwind_Resume` at `0x00401792`, `base_of_encoded` at `0x0040179c`, and `read_encoded_va` at `0x004017a1`. The symbol `rotated_encrypt` at `0x00401835` is highlighted.
- Cross References:** Shows references to the selected symbol, including `_libc_start_main` at `0x00401c81` and `_libc_start_main` at `0x00401c88`.
- Disassembly:** Shows the assembly code for the `main` function. The code includes instructions for setting up the stack, calling `rotated_encrypt`, and printing the result. The function `main` is defined as follows:


```

00401e02      if (rax_13 <= 0x7e)
00401e29      {
00401e29          *i1 = result = 0x13.b
00401e02      }
00401e17      else
00401e17          *i1 = result = rax_13.b - 0x5e
00401e17
00401e42      return result
      
```

The bottom status bar indicates the analysis phase is `Analysis Phase 1: Analysis (MSA/9278)` and the memory address is `0x00401835`.

13

```

if (var_44 != 0xb83cb)
    _IO_puts("Sorry, that's not it!")
else
    void* rax_2 = rotate_encrypt(0, &var_38)
    _IO_fputs(rax_2, stdout)
    putchar(0xa)
    __free(rax_2)

if (rax == *(fsbase + 0x28))
    return 0

__stack_chk_fail()
noreturn
  
```

Como podemos ver la clave es 0xb83cb. Sin embargo, si intentamos colocar eso como clave nos diría que no es correcto ya que debemos darle un valor en base 10. Por lo tanto, buscaremos algo que transforme eso en la base que necesitamos.

Hexadecimal

Decimal

Ingrese el número hexadecimal:

= Convertir

✕ Reset

↕ Cambiar

Valor Decimal:

Valor Binario:

Pasos de Cálculo:

Paso 1: Multiplicar cada dígito de 0xb83cb hexadecimal

$$(0xb83cb)_{16} = (0 \times 16^6) + (NaN \times 16^5) + (11 \times 16^4) + (8 \times 16^3) + (3 \times 16^2) + (12 \times 16^1) + (11 \times 16^0)$$

Como podemos ver aquí la clave sería 754635. Ahora la intentaremos para verificar si es correcto o no.

```

juanito@DESKTOP-J5LE1JC:~$ ./unpackme-upx
What's my favorite number? 754635
picoCTF{up><_m3_f7w_e510a27f}
  
```

Lo que nos dice que el ejercicio fue resultado con éxito.