Homework 2

50.520: Systems Security

Requirements:

- A Linux (x86) 32-bit Operating System. Install Guest Additions if using VirtualBox. http://sg.releases.ubuntu.com/12.04/ubuntu-12.04.5-desktop-i386.iso.torrent

1. Report on memory protection mechanisms that your platform (OS and compiler) provide.
2. Buffer Overflow

   There are two types of buffer overflow:

   a) Stack Based Buffer Overflow – Destination buffer resides in stack
   b) Heap Based Buffer Overflow – Destination buffer resides in heap

   Buffer overflow bugs lead to arbitrary code execution. Arbitrary code execution allows attacker to execute his/her own code in order to gain control of the victim machine (e.g. root shell, add a new user, open a network port etc…)

   Compile `vuln1_hw2.c` with the code below. Then find and exploit errors (crashing the application).

```
1 #sudo echo 0 > /proc/sys/kernel/randomize_va_space
2 $gcc -g -fno-stack-protector -z execstack -o vuln1_hw1 vuln1_hw2.c
3 $sudo chown root vuln1_hw2
4 $sudo chgrp root vuln1_hw2
5 $sudo chmod +s vuln1_hw2
7 $gdb vuln1_hw2
```

   Line 1: Disables Address Space Layout Randomization (ASLR)
   Line 2: `-fno-stack-protector` → Disables Stack Canary
   `-z execstack` → Disables NX bit

   Use gdb vuln1_hw2 to debug the program. See gdb commands below.

   Modify the code below to overwrite EIP with ‘FFFF’. Use info registers to see value of EIP

```
r `python -c 'print "F"*4'`
```

   What is the offset from Destination Buffer?
   (Hint: Offset = buffer size + alignment space + caller’s EBP)

   Modify the code to override EBP with ‘FFFF’ and EIP with ‘PPPP’.

   Resources:
   a) https://en.wikipedia.org/wiki/Stack_buffer_overflow
   b) http://searchsecurity.techtarget.com/definition/address-space-layout-randomization-ASLR

c) https://www.cs.cmu.edu/~gilpin/tutorial/
d) http://www.asciitable.com/

3. Integer Overflow

Storing a value greater than maximum supported value is called integer overflow. Integer overflow on its own doesn't lead to arbitrary code execution, but an integer overflow might lead to stack overflow or heap overflow which could result in arbitrary code execution.

Data types size and its range:

Data Type	Size	Unsigned Range	Signed Range
char	1	0 to 255	-128 to 127
short	2	0 to 65535	-32768 to 32767
int	4	0 to 4294967296	-2147483648 to 2147483647

When we try to store a value greater than maximum supported value, our value gets wrapped around. For example, when we try to store 2147483648 to signed int data type, its gets wrapped around and stored as -21471483648. This is called integer overflow and this overflow could lead to arbitrary code execution.

Compile vuln2_hw2.c with the code below. Then find and exploit errors (crashing the application).

```
1 #sudo echo 0 > /proc/sys/kernel/randomize_va_space
2 $gcc -g -fno-stack-protector -z execstack -o vuln2_hw1 vuln2_hw2.c
3 $sudo chown root vuln2_hw2
4 $sudo chgrp root vuln2_hw2
5 $sudo chmod +s vuln2_hw2
7 $gdb vuln2_hw2
```

Use `gdb vuln2_hw2` to debug the program. See `gdb` commands below.

Modify the code below to overwrite EIP with 'FFFF'. Use info registers to see value of EIP

```
r `python -c 'print "F"*4'`
```

What is the offset from Destination Buffer?
(Hint: Offset = buffer size + alignment space + EDI + caller's EBP)

Modify the code to overwrite EBP with 'FFFF' and EIP with 'PPPP' and remaining space with W's. Use `x/80x ($esp-28)` view remaining space.

4. Hand in. If submitting an image, image of desktop must be shown. Do not crop.
   a. Buffer Overflow.
      i. code which crashed `vuln1_hw2`.
      ii. EIP overwritten with 'FFFF'

iii. What is the offset from Destination Buffer?
iv. EBP overwritten with ‘FFFF’ and EIP are overwritten with ‘PPPP’

b. Integer Overflow
   i. code which crashed `vuln2_hw2`.
   ii. EIP overwritten with ‘FFFF’
   iii. What is the offset from Destination Buffer?
   iv. EBP overwritten with ‘FFFF’ and EIP are overwritten with ‘PPPP’ and remaining space with W’s.

GDB commands

```
# show debugging symbols
list main

# show the assembly code
disas main

# run the program, with input
r Hello
r `python -c 'print "A"*3'`

# confirm overwrite of ebp register
info registers

# examine memory address
x/200x ($esp - 550)

# show value of Instruction Pointer Register (EIP)
p/x $eip
```

For technical help/question please consult with Francisco.