

CSE 484 In-Class Worksheet #4 – Fall 2017

Name: _____ UW Student #: _____ Date: _____

Email address: _____

Partner names for this activity: _____

Q1: Consider the following function:

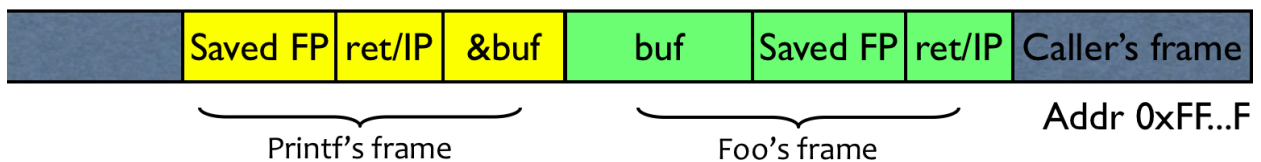
```
foo() {
    char buf[...];
    strncpy(buf, readUntrustedInput(), sizeof(buf));
    printf(buf); //vulnerable
}
```

Suppose `readUntrustedInput()` provides an attack string of the form:

```
... attackString%n ... <shellcode> ...
```

How might we be able to use `%n` to overwrite the saved EIP (aka RET) on the stack? (You don't need to give the exact attack; just brainstorm about the general approach you might try.)

As a reminder, here's what the stack looks like for this program:



Q2: What might be a good value for a stack canary?