CSE 484 In-Class Worksheet #5 – Autumn 2018

Name: ______________________________ UWNetID: ______________ Date: _____________

Email address: ____

Partner names for this activity: ____

Will you want to pick up your worksheet later? Circle one: Yes / No

Q1: Consider the following function:

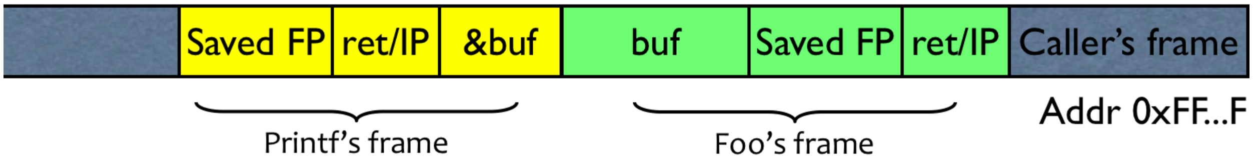
```
foo() {
      char buf[…];
      strncpy(buf, readUntrustedInput(), sizeof(buf));
      printf(buf); //vulnerable
}
```

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

```
 … attackString%n … <shellcode> …
```

How might we be able to use one or more “%n”s 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.)

Here’s what the stack looks like for this program:


Saved FP
ret/IP
&buf
buf
Saved FP
ret/IP
Caller’s frame
Printf’s frame
Foo’s frame
Addr 0xFF…F