CSE 484 In-Class Worksheet #6 – 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: What might an attacker be able to accomplish even if they cannot execute code on the stack?

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

Q3: The goal of this code is to allow a program to open regular files, but not symlinks.

```
int openfile(char *path) {
        struct stat s;
        if (stat(path, &s) < 0)
                return -1;
        if (!S_ISRREG(s.st_mode)) {
                error("only allowed to regular files!");
                return -1;
        }
        return open(path, O_RDONLY);
}
```

Can you spot any potential problems? What problems do you spot, if any?

Q4: Consider this code:

```
char buf[80];
void vulnerable() {
    int len = read_int_from_network();
    char *p = read_string_from_network();
    if (len > sizeof buf) {
        error("length too large, nice try!");
        return;
    }
    memcpy(buf, p, len);
}
```

And note the following definitions:

```
void *memcpy(void *dst, const void * src, size_t n);
typedef unsigned int size_t;
```

Can you spot any potential problems? What problems do you spot, if any?

Q5: Consider this code:

```
size_t len = read_int_from_network();
char *buf;
buf = malloc(len+5);
read(fd, buf, len);
```

Can you spot any potential problems? What problems do you spot, if any?

Q6: What issues, if any, do you see with the following code for password comparisons?

```
// The following is the functional description of the code -- what it should do
PwdCheck(RealPwd, CandidatePwd) should:
    Return TRUE if RealPwd matches CandidatePwd
    Return FALSE otherwise
RealPwd and CandidatePwd are both 8 characters long

// The following is the implementation, like on the TENEX system
PwdCheck(RealPwd, CandidatePwd)  // both 8 chars
    for i = 1 to 8 do
        if (RealPwd[i] != CandidatePwd[i]) then
            return FALSE
    return TRUE
```