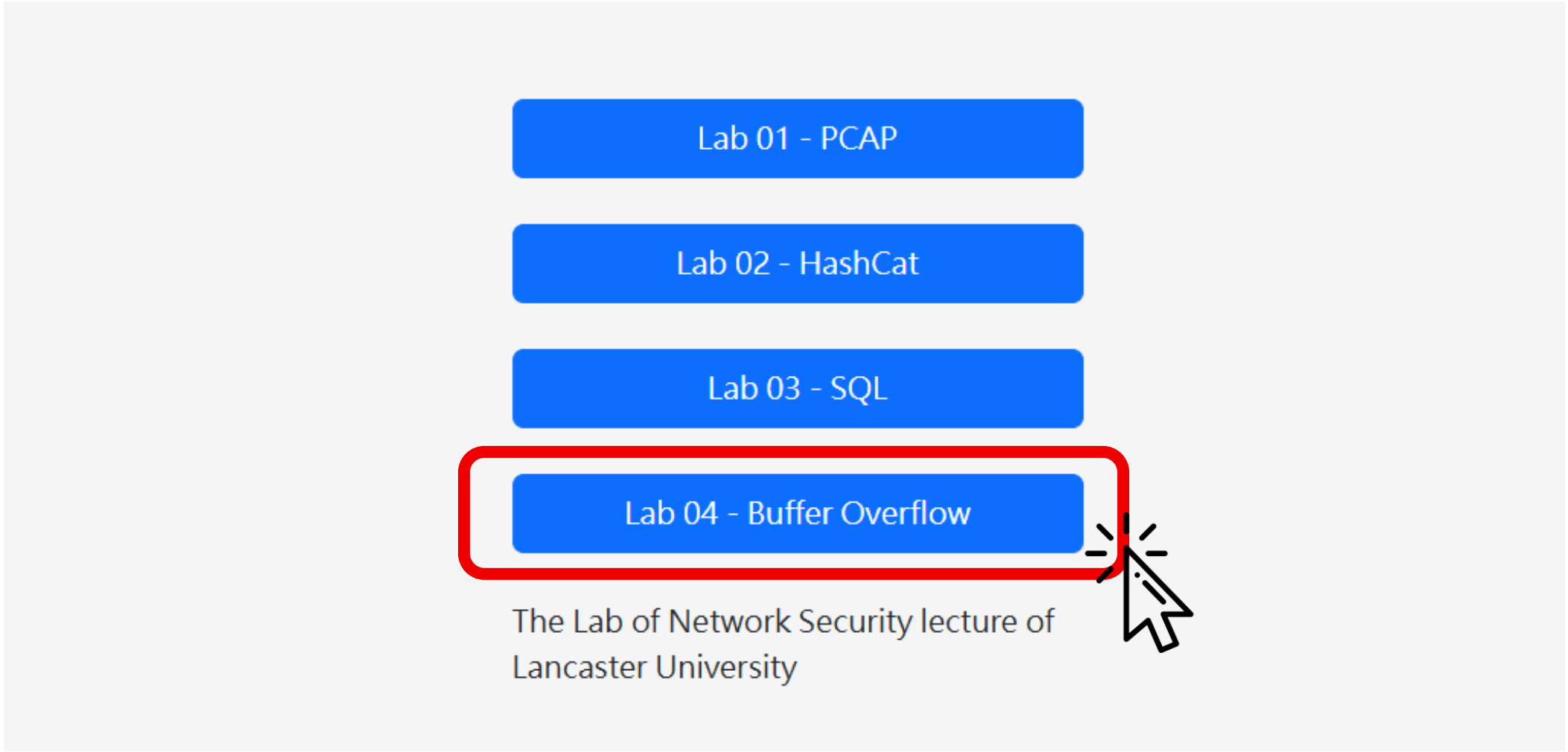
Lancaster University

Network Security Lab 04 Instruction

0. Open Lancaster.waynechiu.cc



1. Observe the backend code of PING tester

This Lab04 Overflow of Network Security lecture of Lancaster University

The backend code of this ping tester is here.

There are some known programs located at the same directory of ping. They are passwd, whoami, and ls

Try to trigger those programs.

I need instructions.

```
#include <iostream>
#include <cstring>
using namespace std;

char ip_addr[15];
char *program_to_run = "ping.exe";

void exec(char* program, char* args)
{
    char* sysCmd = new char[255];
    strcpy(sysCmd, program);
    for (int i = 0; i < 255; i++)
    {
        if (sysCmd[i] == '\0')
        {
            sysCmd[i] = ' ';
            strcpy(sysCmd + i + 1, args);
            break;
        }
    }
    system(sysCmd);
}

int main()
{
    printf("Please enter the IP you would like to PING\n");
    gets(ip_addr);
    exec(program_to_run, ip_addr);
}
```

Notice some important hints within

2. Enter any IP address and observe

```
You executed ping 192.168.200.111
The result is:
IP 192.168.200.111 is reachable from 203.0.113.10
```

Tips: Trying to enter more than 15 characters. Observe the differences.

3. Hint : 192.168.254.254whoami

Please be advised.

This program is compiled in special manner

Some effects made by the code may not be reproduce with usual compiler.