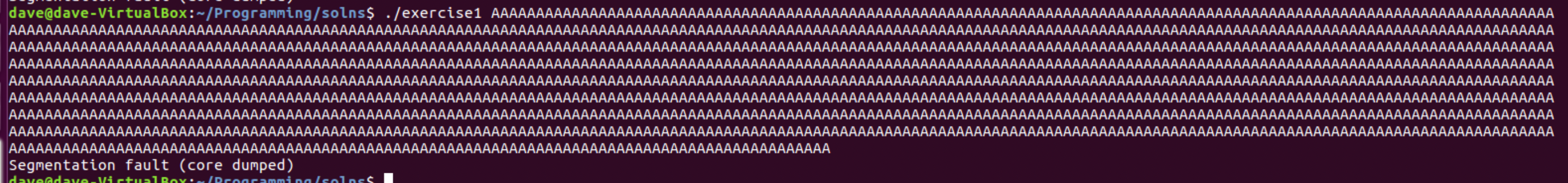
Nem Negash

CMSC 426

11/07/2021

**Buffer Overflow Lab**



Graphical user interface, text

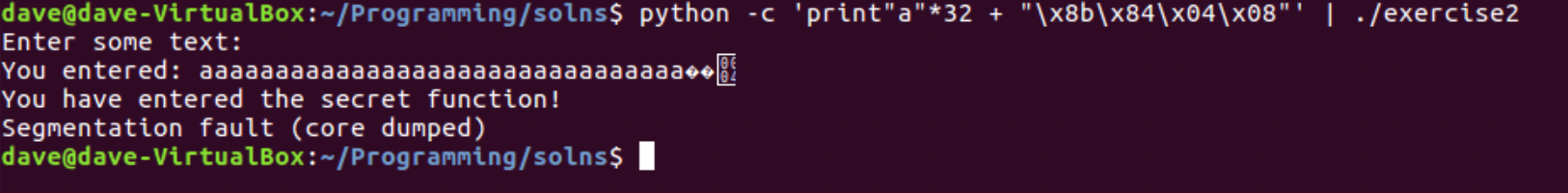
Description automatically generated

Graphical user interface

Description automatically generated

A picture containing graphical user interface

Description automatically generated



Text

Description automatically generated

Text

Description automatically generated

**Conclusion and Lab Report:**

Now that you have completed the lab exercises it is a good idea to take a snapshot so you can save your work and return to it later. Once that’s done you can either exit the virtual machine and select “*Save the machine state*” or power off completely.

1. Describe what you have learned about buffer/stack overflows in this lab?

This lab gives a great understanding of how buffer/stack overflows occur in programs. I was able to learn that, Buffer overflow is one of the best known forms of software security vulnerabilities. In a classic buffer overflow exploit, the attacker sends data to a program which stores it in an undersized stack buffer. The result is that information on the call stack is overwritten, including the function’s return pointer. At the code level, buffer overflow vulnerabilities usually involve the violation of a programmer’s assumptions. This usually happens when a value is given to a variable that goes over the size set for that variable.

1. Did these exercises make you think of other capabilities that you would find helpful for gaining user credentials on targeted systems?

Application crashes: The seg fault can cause the application to crash which can lead to giving access to the application’s data such as user credentials.

1. What are some well-known exploits that have utilized buffer overflow to gain access?
   1. SQL Slammer: a 2003 computer worm that caused a denial of service on some Internet hosts and dramatically slowed general Internet traffic. It spread rapidly, infecting most of its 75,000 victims within ten minutes. The program exploited a buffer overflow bug in Microsoft's SQL Server and Desktop Engine database products. Although the MS02-039 patch had been released six months earlier, many organizations had not yet applied it.