Lab 4 Fuzzing with Spike  
CIS 450  
Krutarth Panchal  
  
Section 1: Starting up VulnServer

1. Installation Path and Directory  
   A screenshot of a computer

   Description automatically generated
2. Running vulnserver.exe  
   A screenshot of a computer

   Description automatically generated
3. Listening on Ghost VM (port 9999)  
   command: *nc 192.168.1.124 9999*  
   A screenshot of a computer

   Description automatically generated
4. Command on cmd to see what port applications are listening on  
   command: *netstat -an*  
   A screenshot of a computer

   Description automatically generated
5. Successful connection to Vulnserver  
   A computer screen with white text

   Description automatically generated
6. HELP command from Ghost VM  
   A screenshot of a computer

   Description automatically generated

Section 2: Working with Spike to Fuzz VulnServer.exe

1. Opening Vulnserver.exe from Immunity Debugger  
   A screenshot of a computer

   Description automatically generated
2. Command to create .spk file and the three commands placed in the .spk file to fuzz VulnServer?  
   - command to create:  
   *vim /usr/share/spike/audit/*  
   - three lines to add to .spk file  
   *s\_readline();  
   s\_string(“TRUN”);  
   s\_string\_variable(“COMMAND”);*A screenshot of a computer

   Description automatically generated
3. Fuzzing / Sending .spk file from Ghost VM to Win10 machine.  
   Command: generic\_send\_tcp\_192.168.1.124 9999 vulnserver.spk 0 0  
   A screenshot of a computer

   Description automatically generated
4. Vulnserver on Win10 machines stops working.

A screenshot of a computer

Description automatically generated  
  
Error message in the console indicate our fuzzing was successful.  
--------------------------------------------- End of Lab ----------------------------------------------------