✨4. Exploit Development Section

05 January 2022 09:48 PM

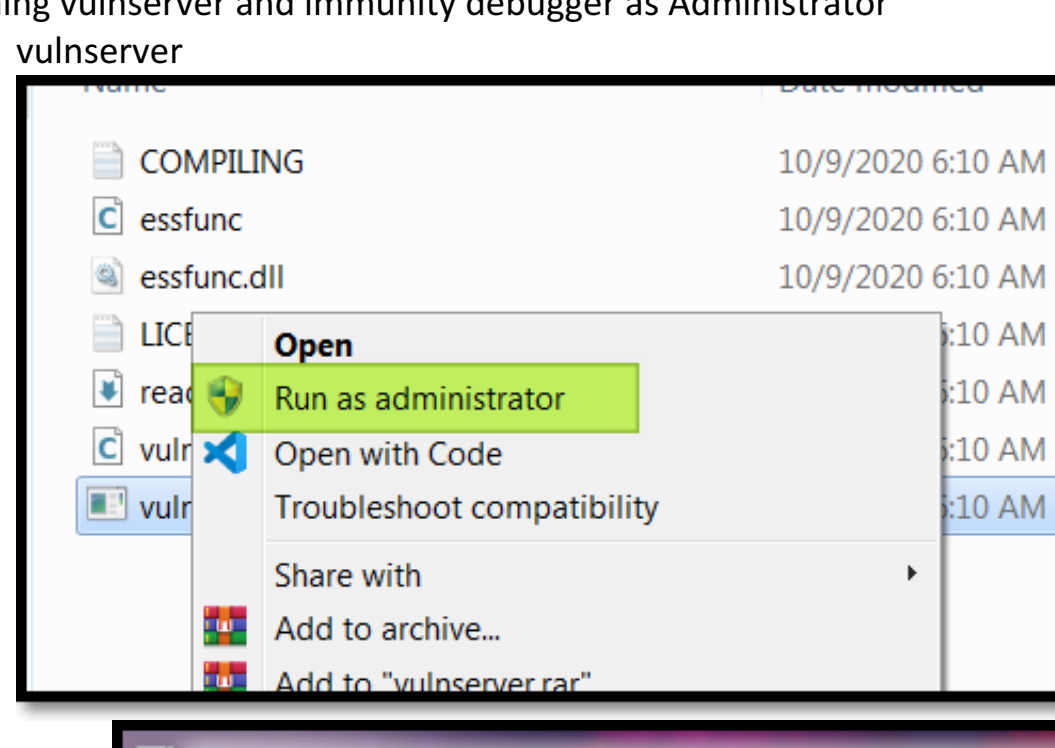
1. Required Files :-

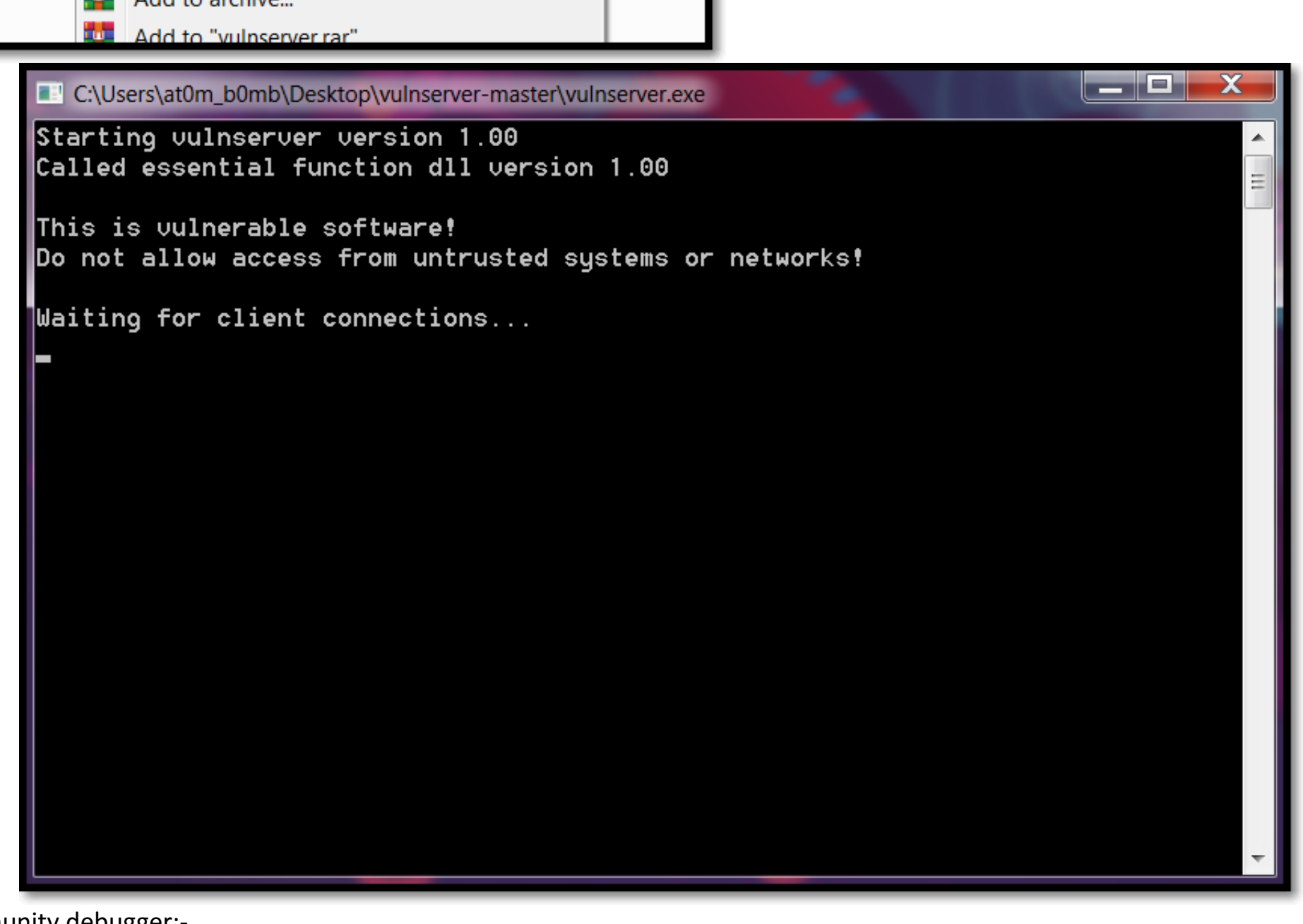
a. Vulnserver: git clone https://github.com/stephenbradshaw/vulnserver.git
b. Window 7 or Up (VM or Bare Metal)
c. Immunity Debugger: https://www.immunityinc.com/products/debugger/

2. Spiking :-

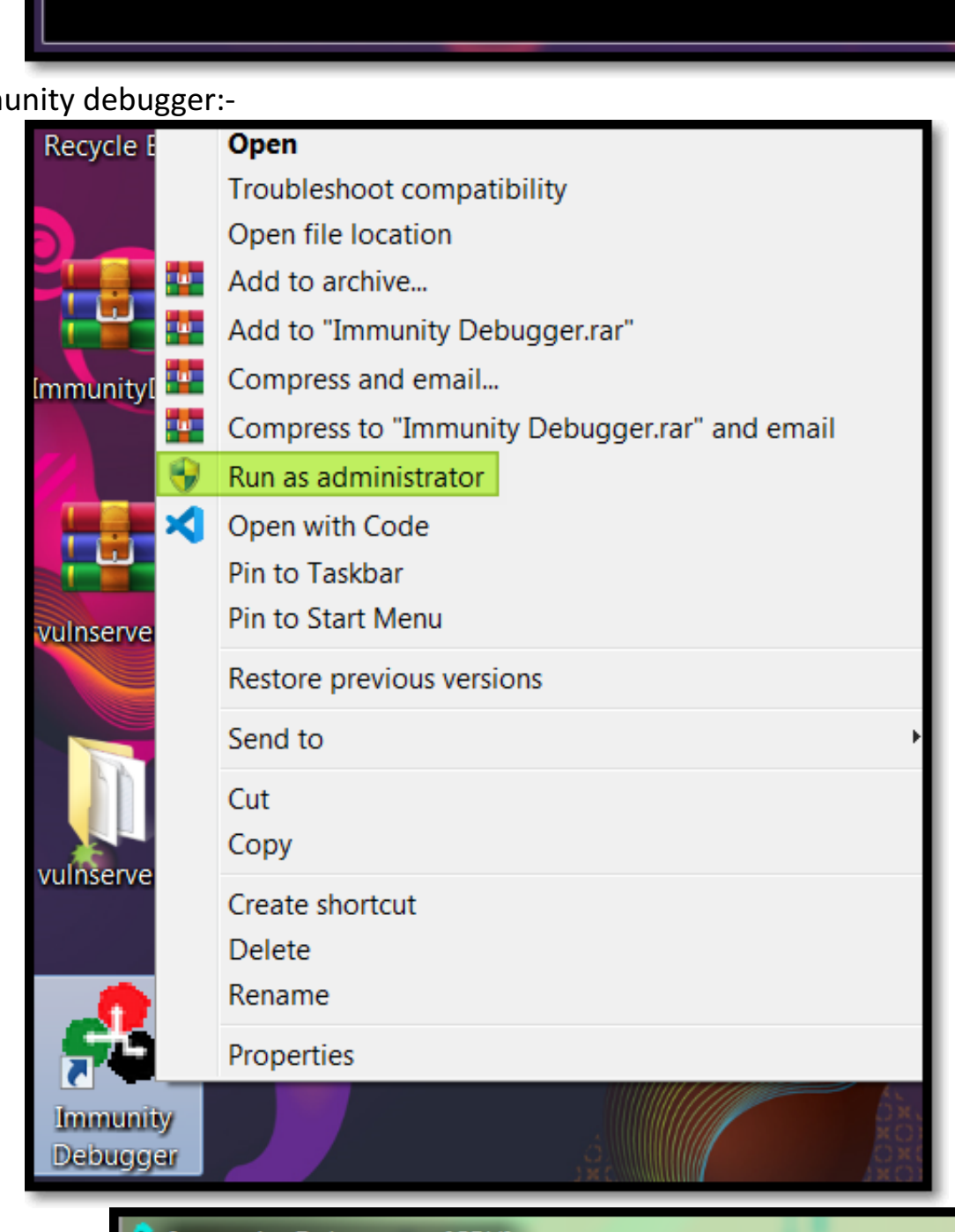
a. Running vulnserver and immunity debugger as Administrator

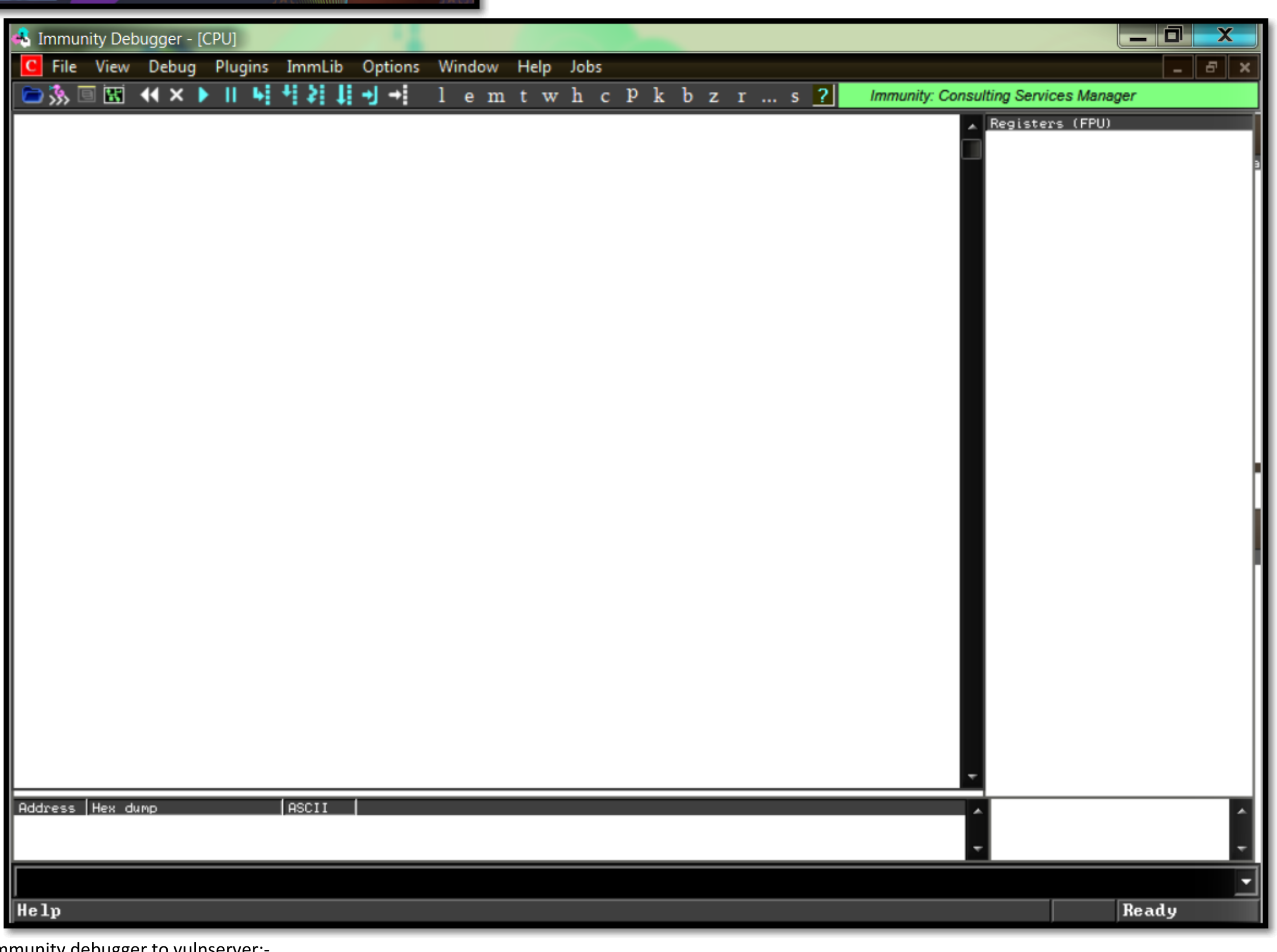
i. vulnserver

ii. 

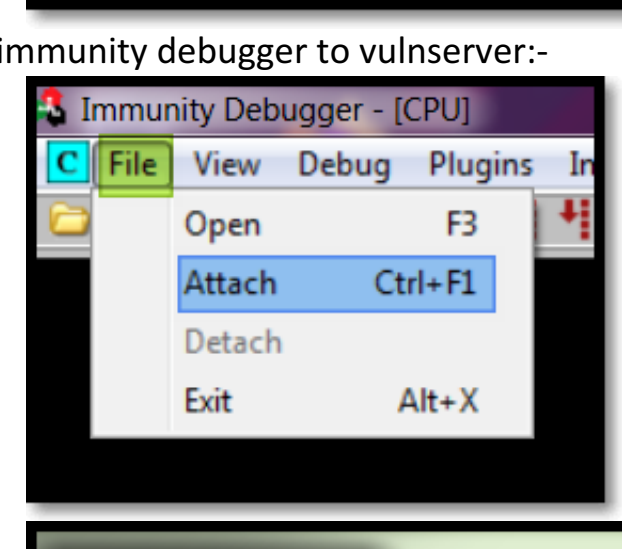
1) 

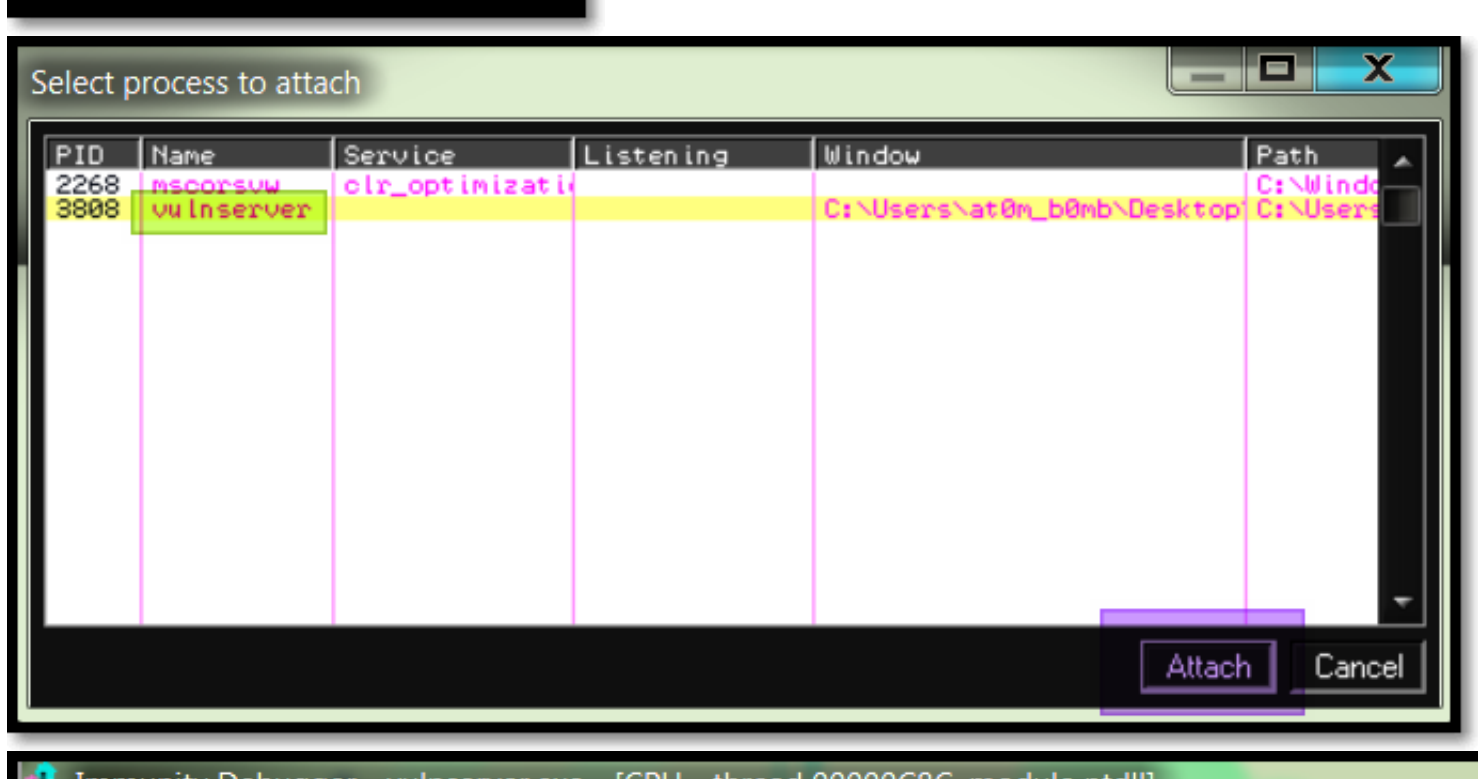
iii. Immunity debugger:-

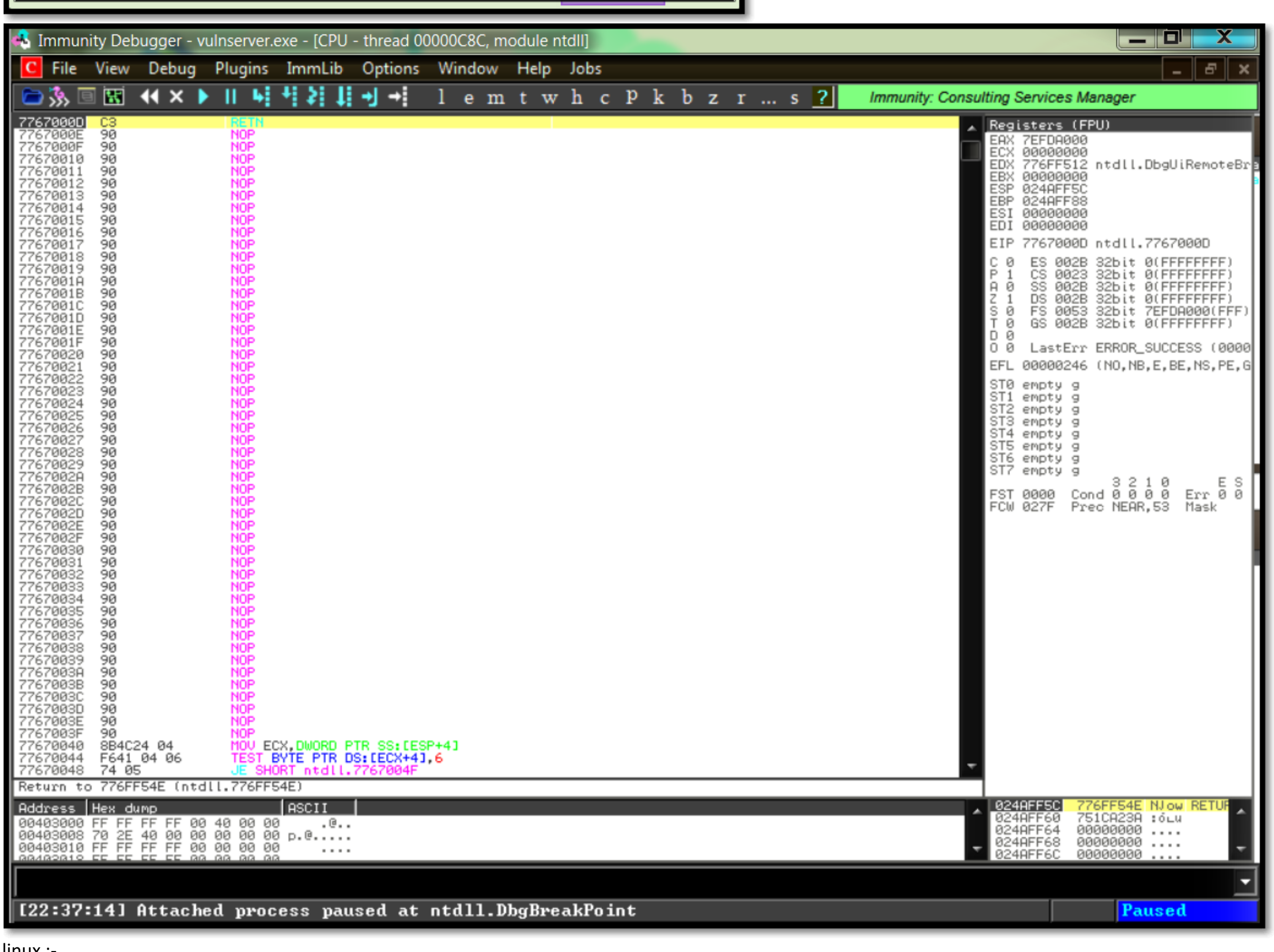




iv. Attaching immunity debugger to vulnserver:-







v. Back to kali linux :-

1) Created a subfolder and started a nmap scan on the target running vulnserver :-

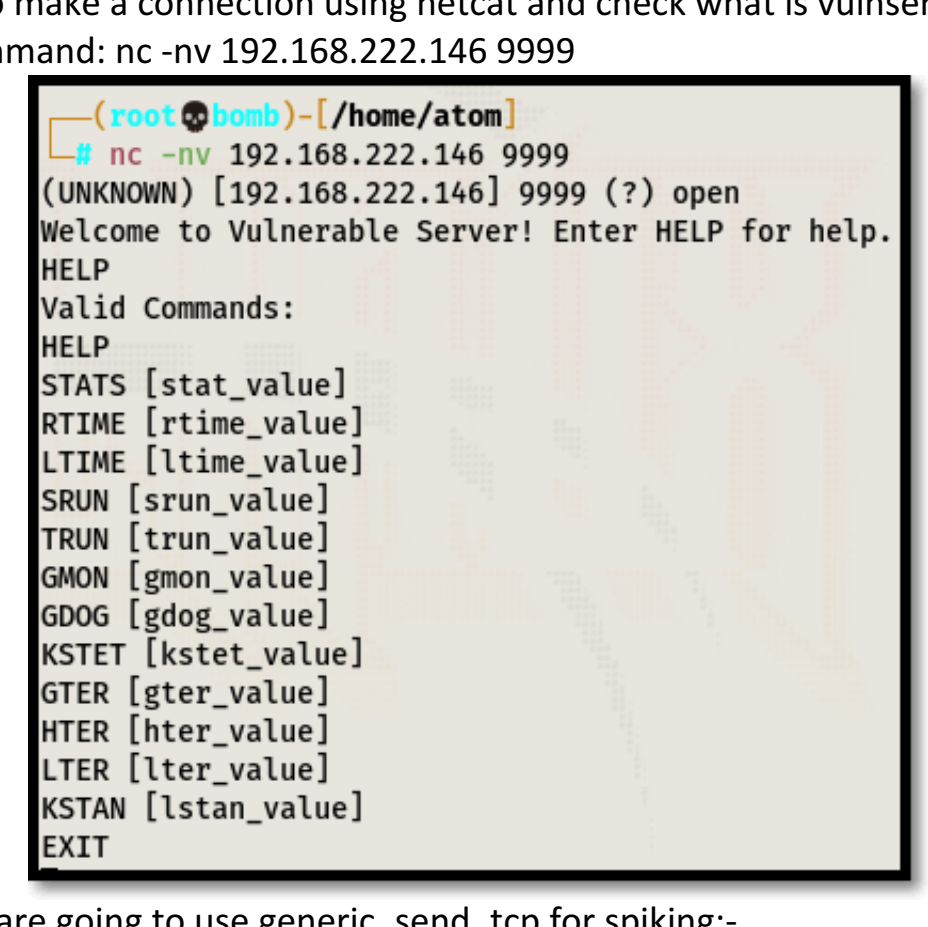
nmap -p- -A -T5 192.168.222.146 -oN nmap_win7.txt
Starting Nmap 7.92 (https://nmap.org) at 2022-01-10 22:44 IST
Nmap scan report for 192.168.222.146
Host is up (0.00052s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
9999/tcp open abyss?
MAC Address: 00:0C:29:FC:43:25 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 R1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.52 ms 192.168.222.146

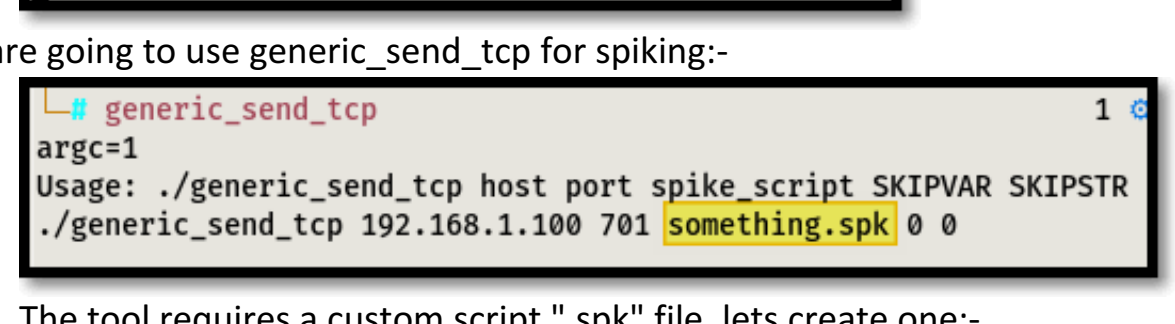
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 593.04 seconds

2) We found out the port were vulnserver is running:-
a) Port = 9999

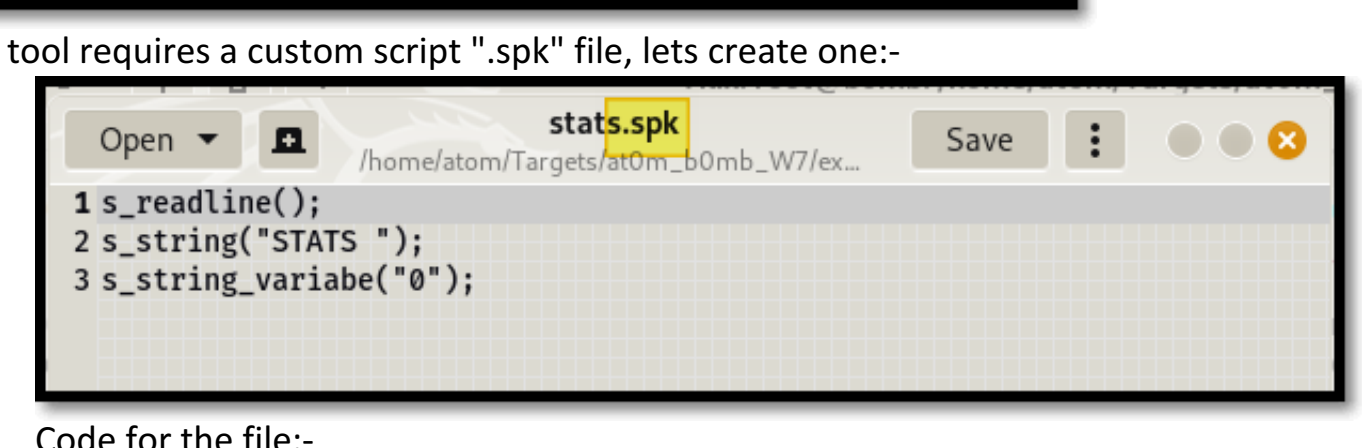
3) Let's try to make a connection using netcat and check what is vulnserver!
a) Command: nc -nv 192.168.222.146 9999

i) 

b) We are going to use generic_send_tcp for spiking:-

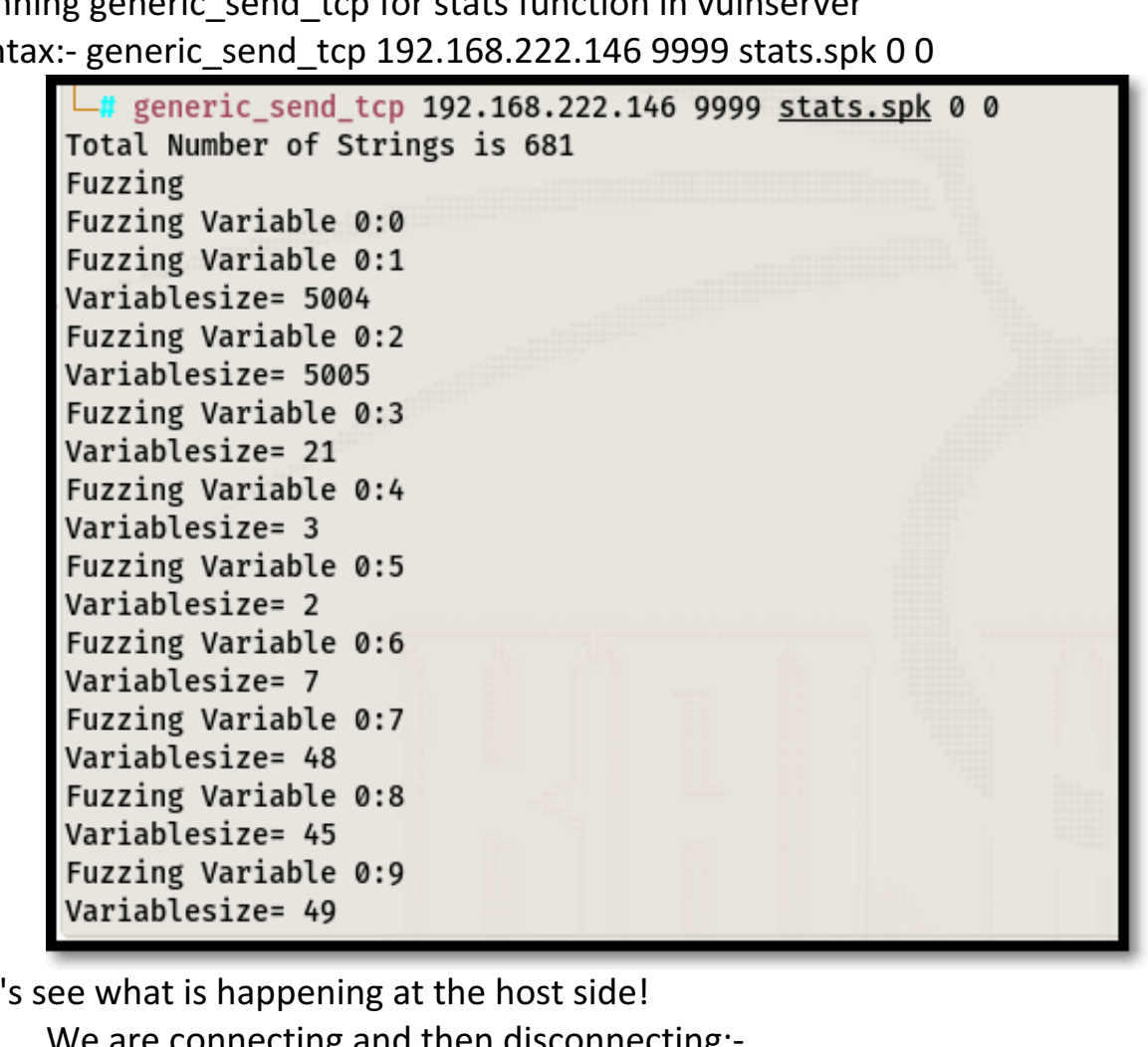
i) 

ii) The tool requires a custom script ".spk" file, lets create one:-

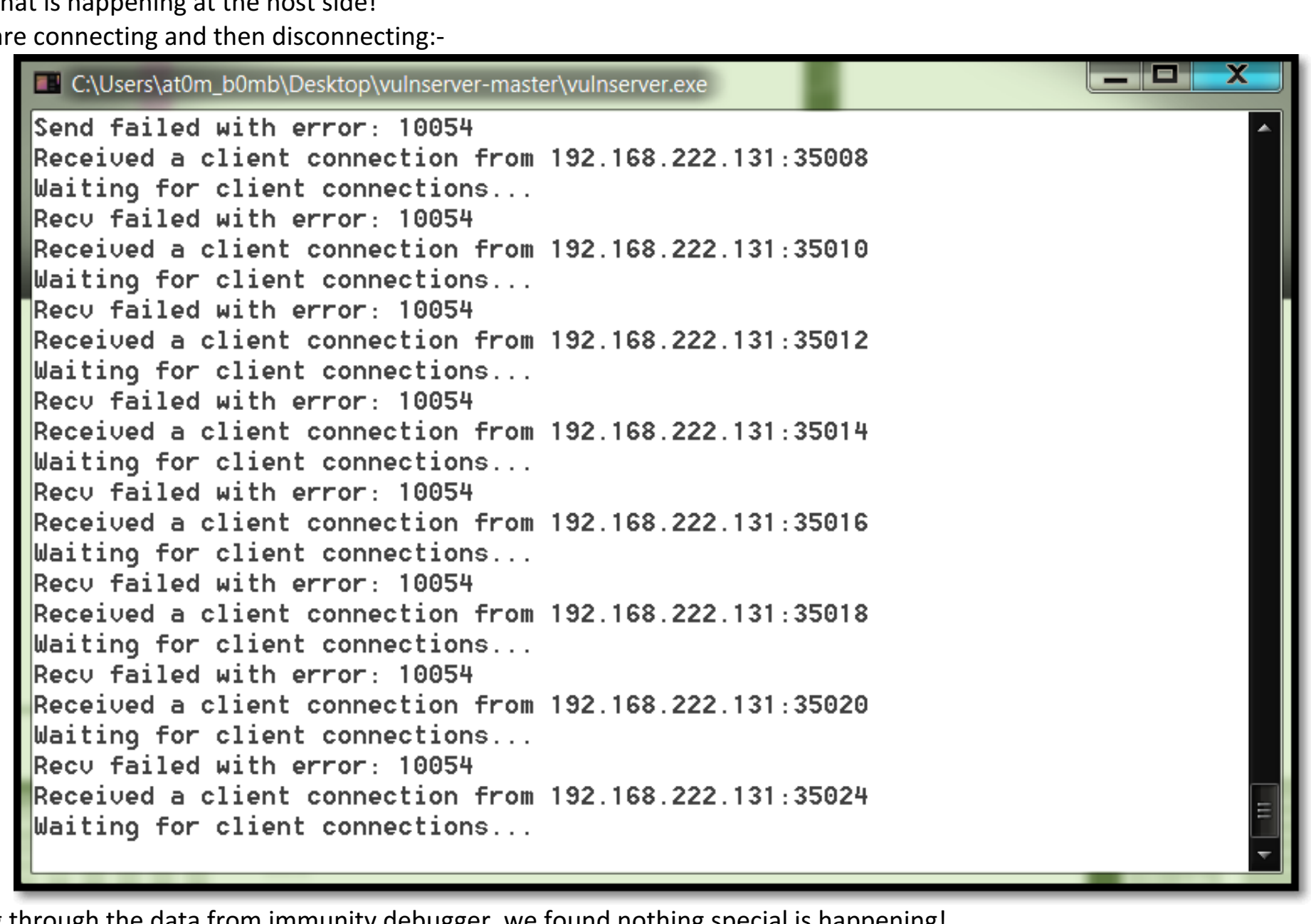


Code for the file:-
STATS FILE.spk
s_readline();
s_string("STATS ")
s_string_variable("0");

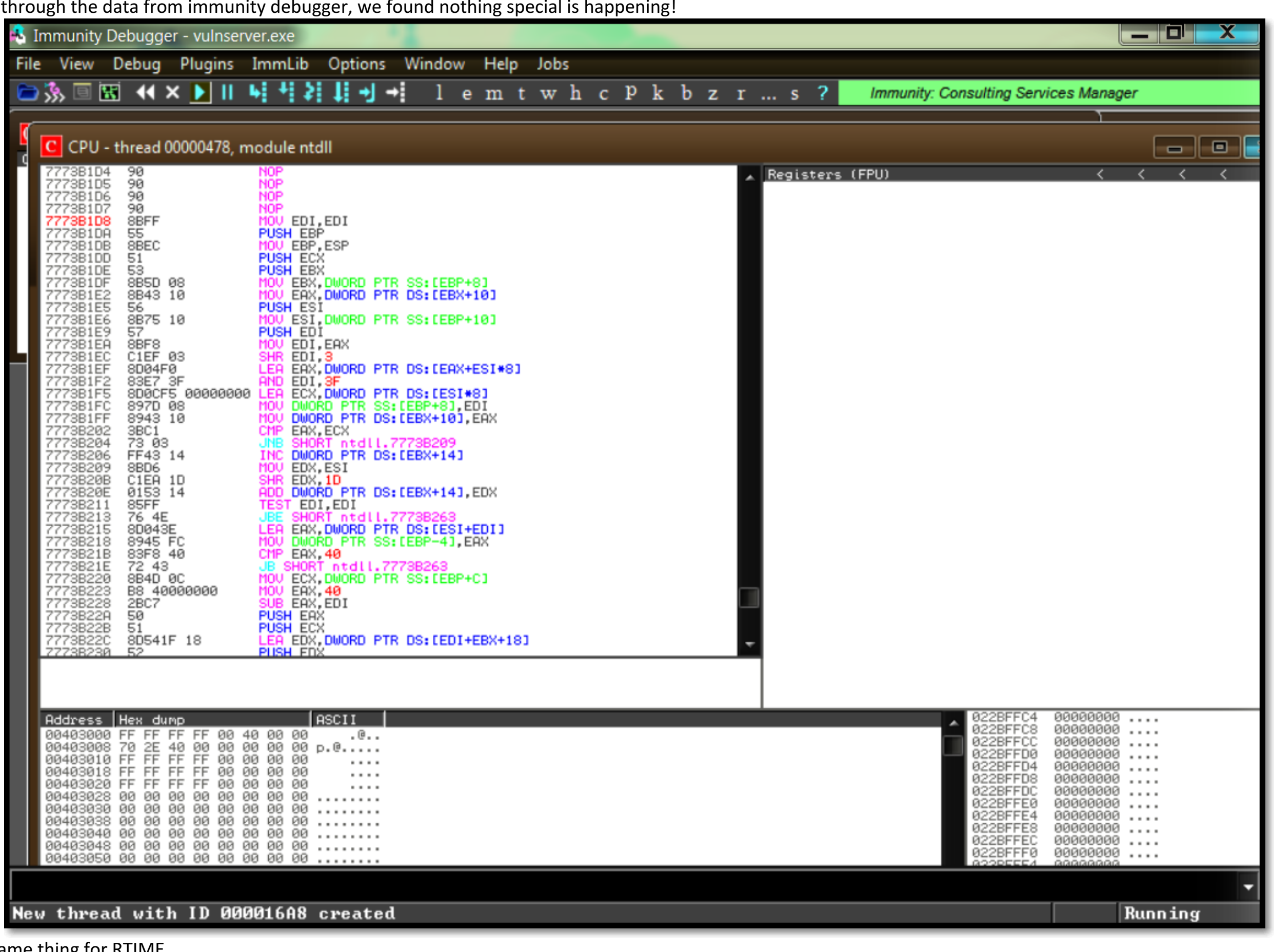
One. Running generic_send_tcp for stats function in vulnserver
Syntax:- generic_send_tcp 192.168.222.146 9999 stats.spk 0 0



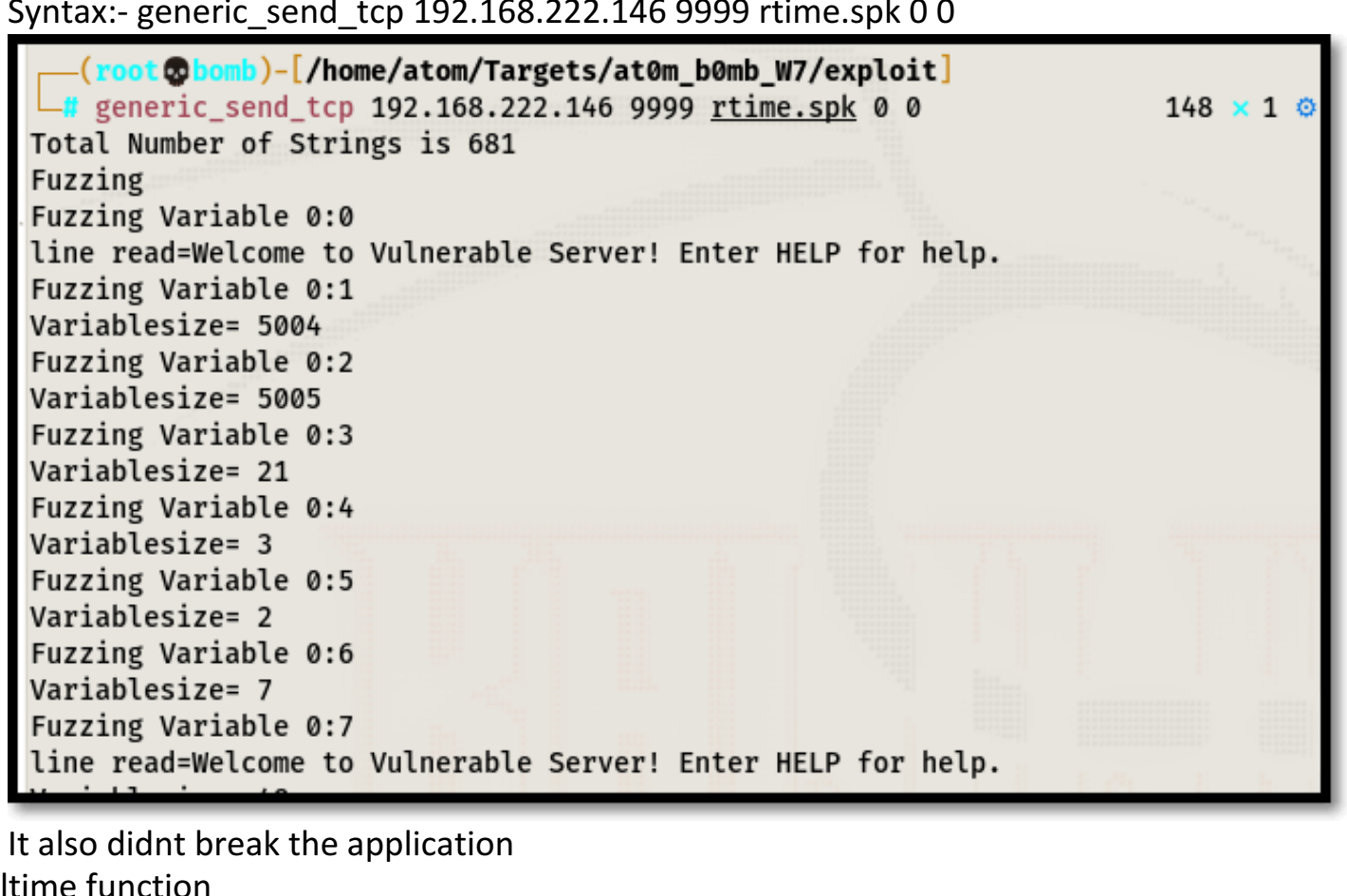
Let's see what is happening at the host side!
We are connecting and then disconnecting:-



After going through the data from immunity debugger, we found nothing special is happening!



Two. Doing the same thing for RTIME

- Code for spk file:-
  s_readline();
  s_string("RTIME ")
  s_string_variable("0");
- Running generic_send_tcp
  - Syntax:- generic_send_tcp 192.168.222.146 9999 rtime.spk 0 0
  - 

  - It also didnt break the application

- Now trying ltime function
  - Code for spk file:-
    s_readline();
    s_string("LTIME ")
    s_string_variable("0");
  - Lets use the similar syntax and check what happens!
    Nothing happened
- Now lets move on to srun
  - Code for srun:-
    s_readline();
    s_string("SRUN ")
    s_string_variable("0");
  - Lets run it and see what happens:-
    Nothing happened
- Now lets try trun:-
  - Code for trun.spk
    s_readline();
    s_string("TRUN ")
    s_string_variable("0");
  - Now lets start the exploit:-