Fuzzing

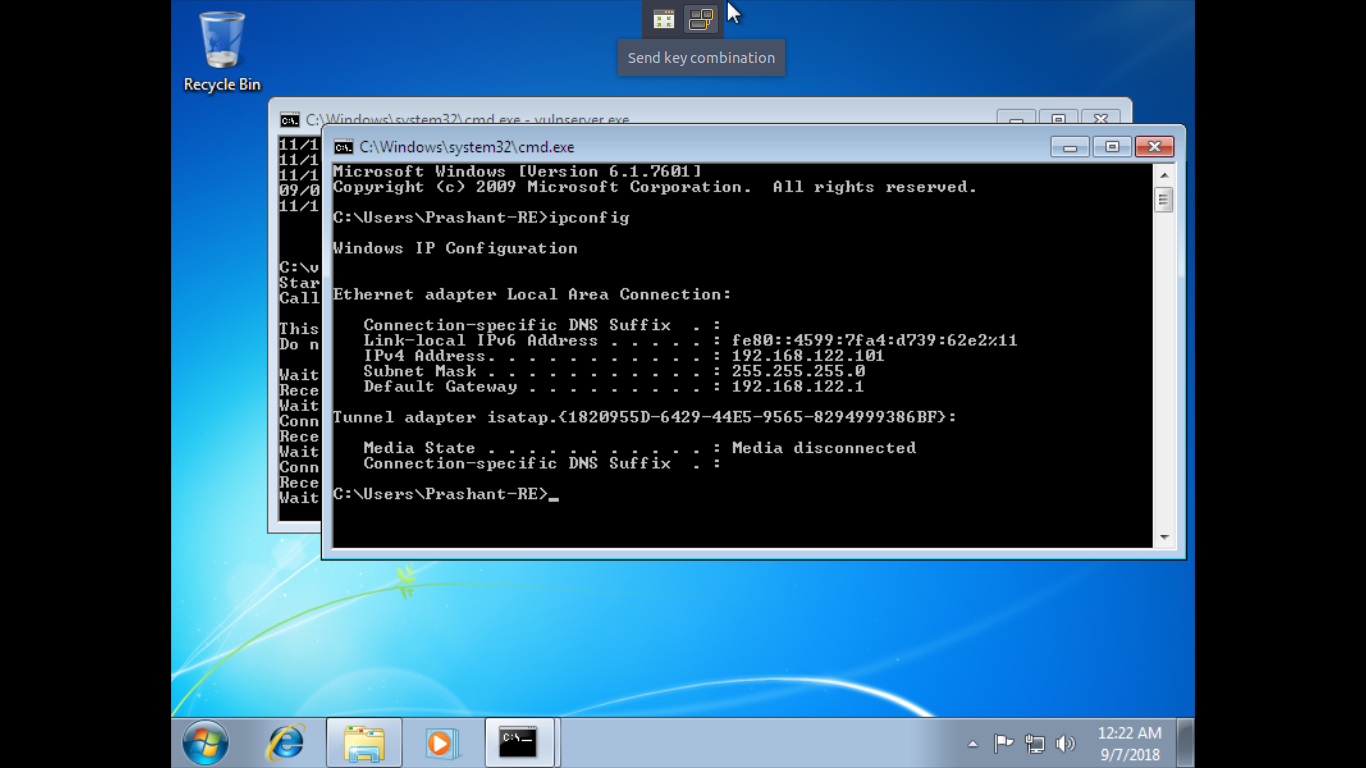
Fuzzing is sending a random input to an application , to try and make an application a **crash*, A proper Crash.***

**Pre-Requisite**

* A virtual Machine [Using KVM]
* Window7 in KVM[as Target]
* Linux system [As Host -> Ubantu 18.04]

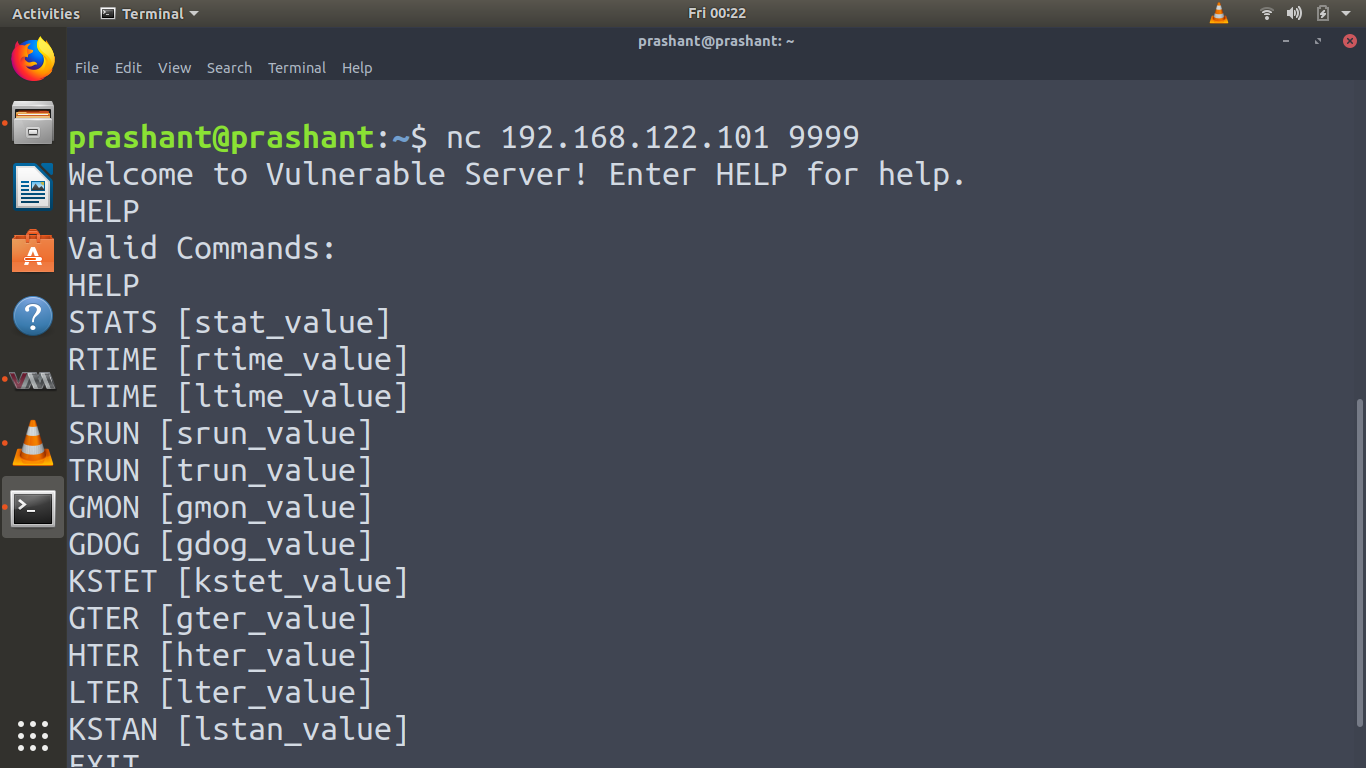
First, we will install **vulnserver** from <https://sites.google.com/site/lupingreycorner/vulnserver.zip?attredirects=0>

Now, Run vulnserver.exe



Now, go to terminal on ubantu... and run

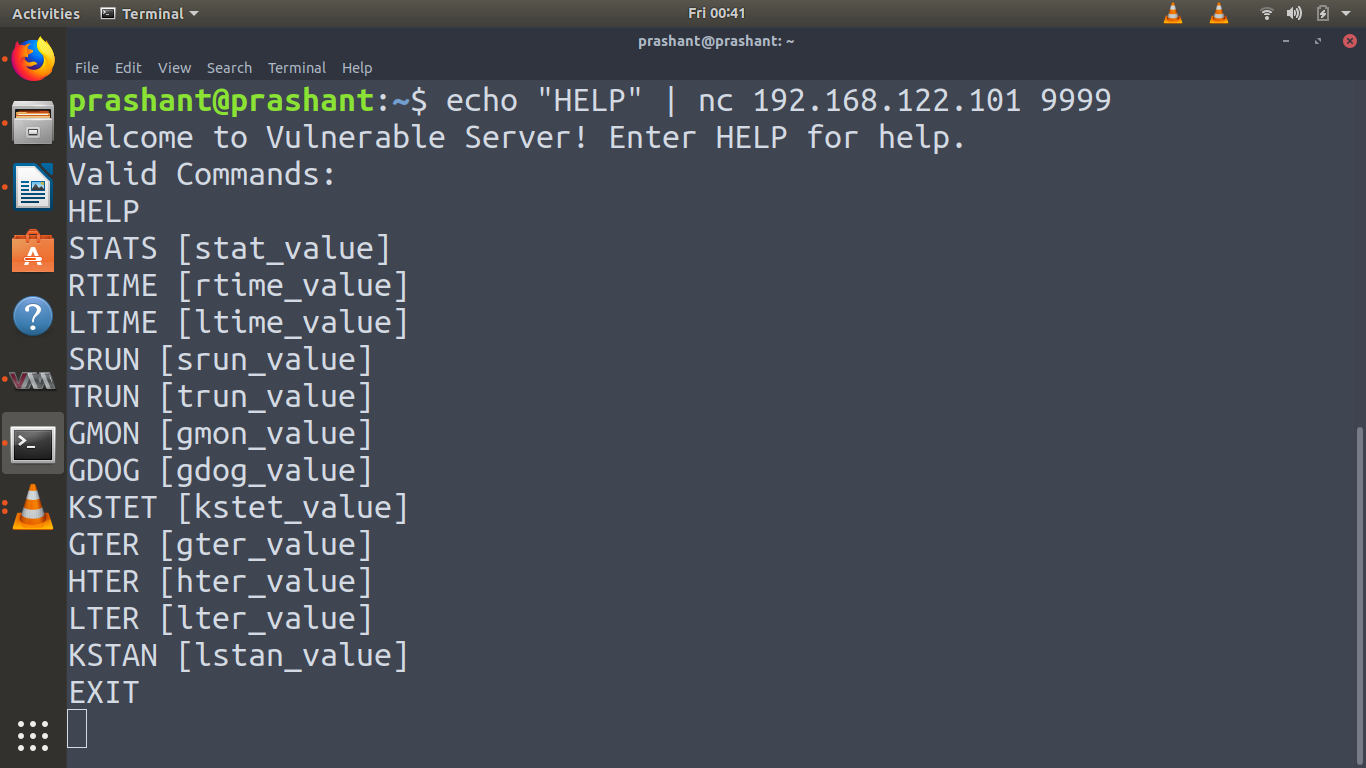
**$ nc <Your IPv4 address 9999>**

****

The system is case sensitive .

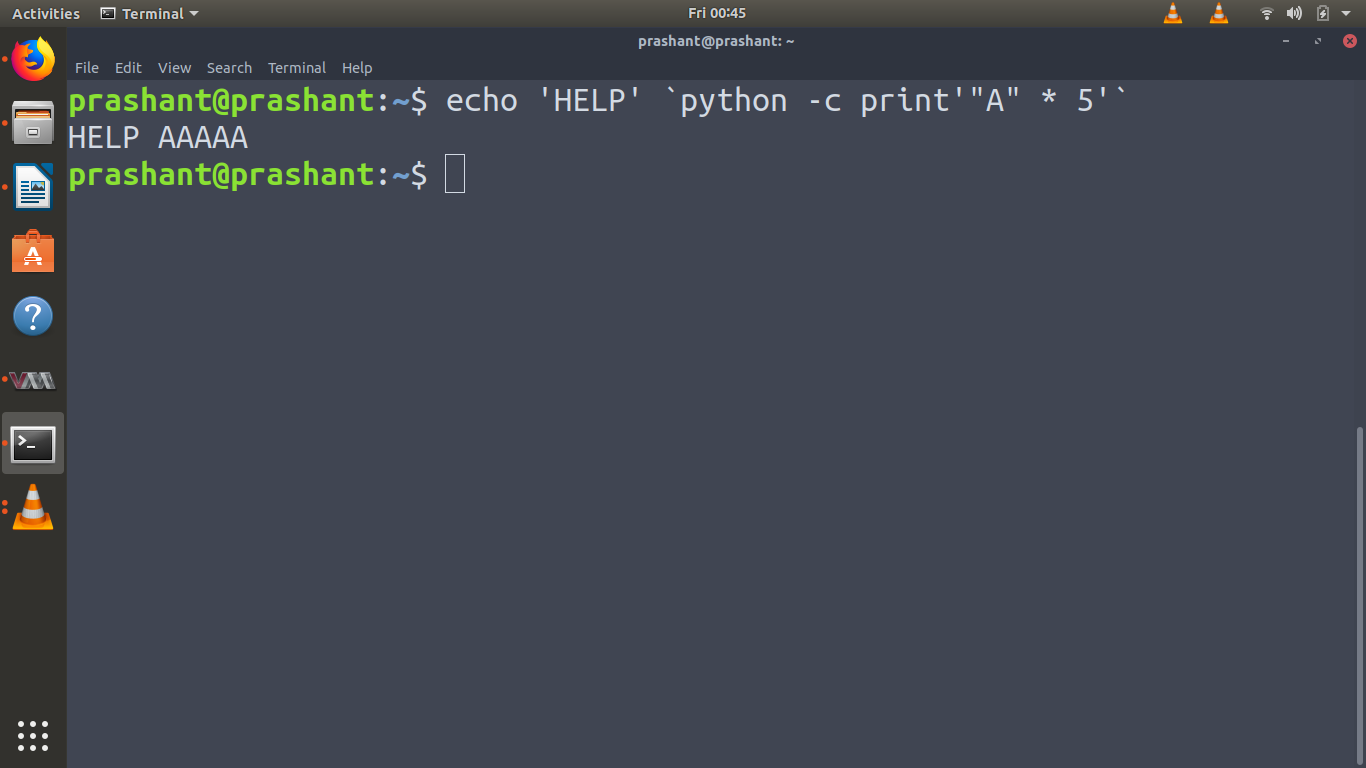
Not, lets type following to check if system is able to respond to echo from terminal

$ echo ‘HELP’ | nc **nc <Your IPv4 address 9999>**

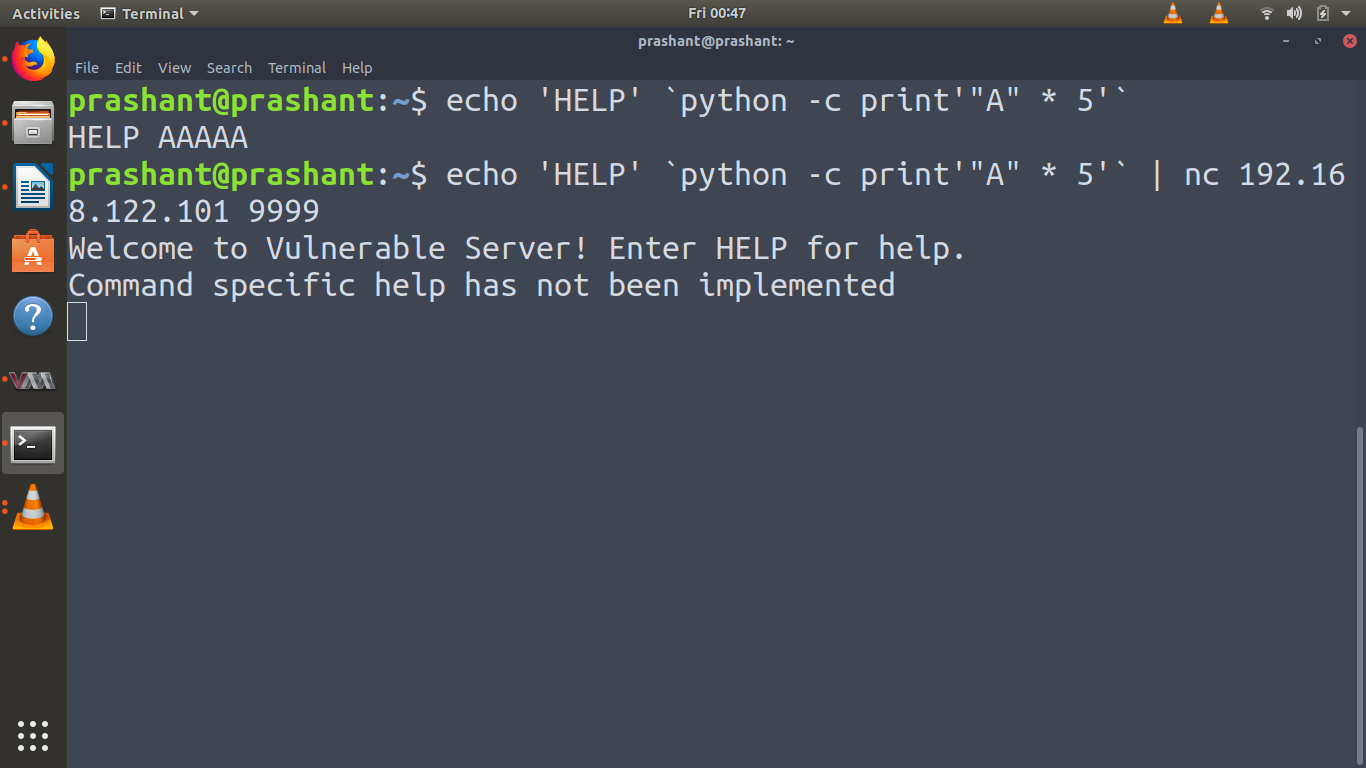


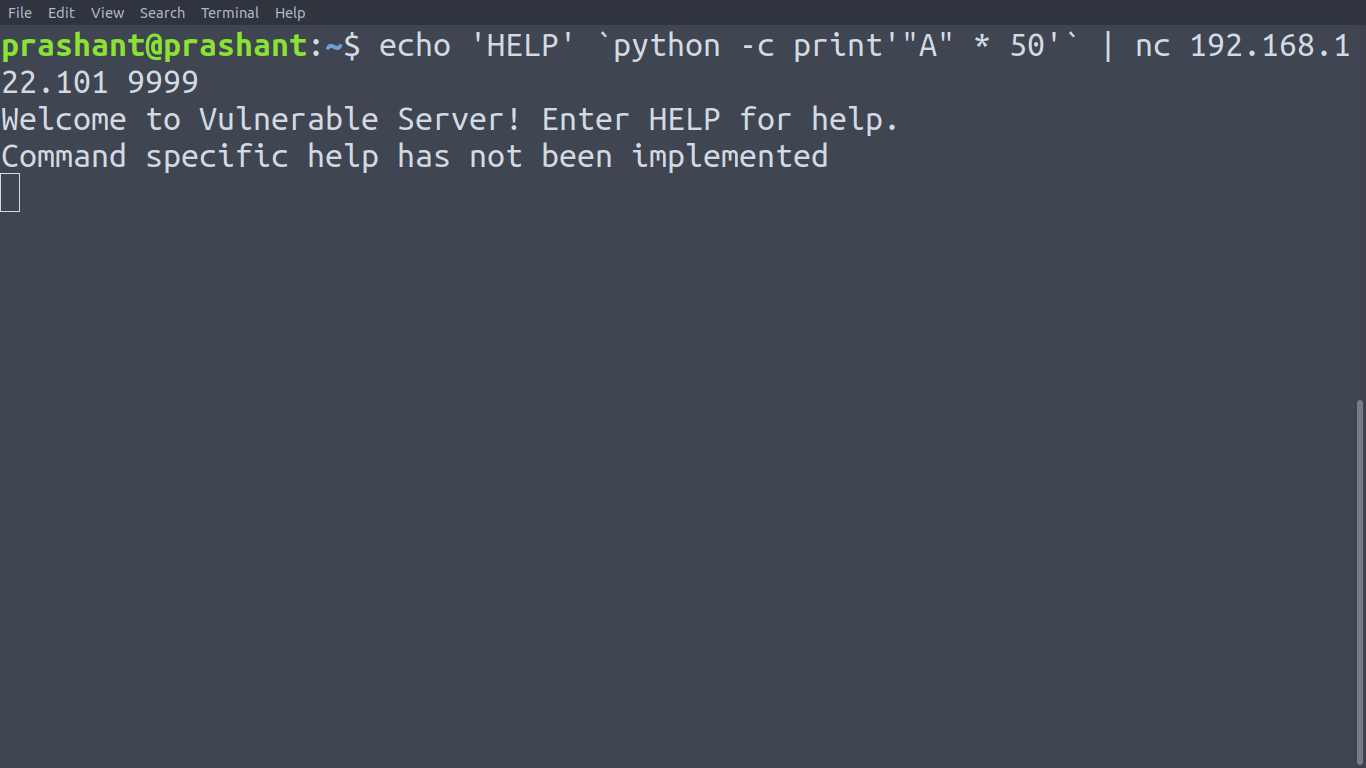
Now, try to send random character ro vulnserver

The below python program prints 5 A in row , with HELP

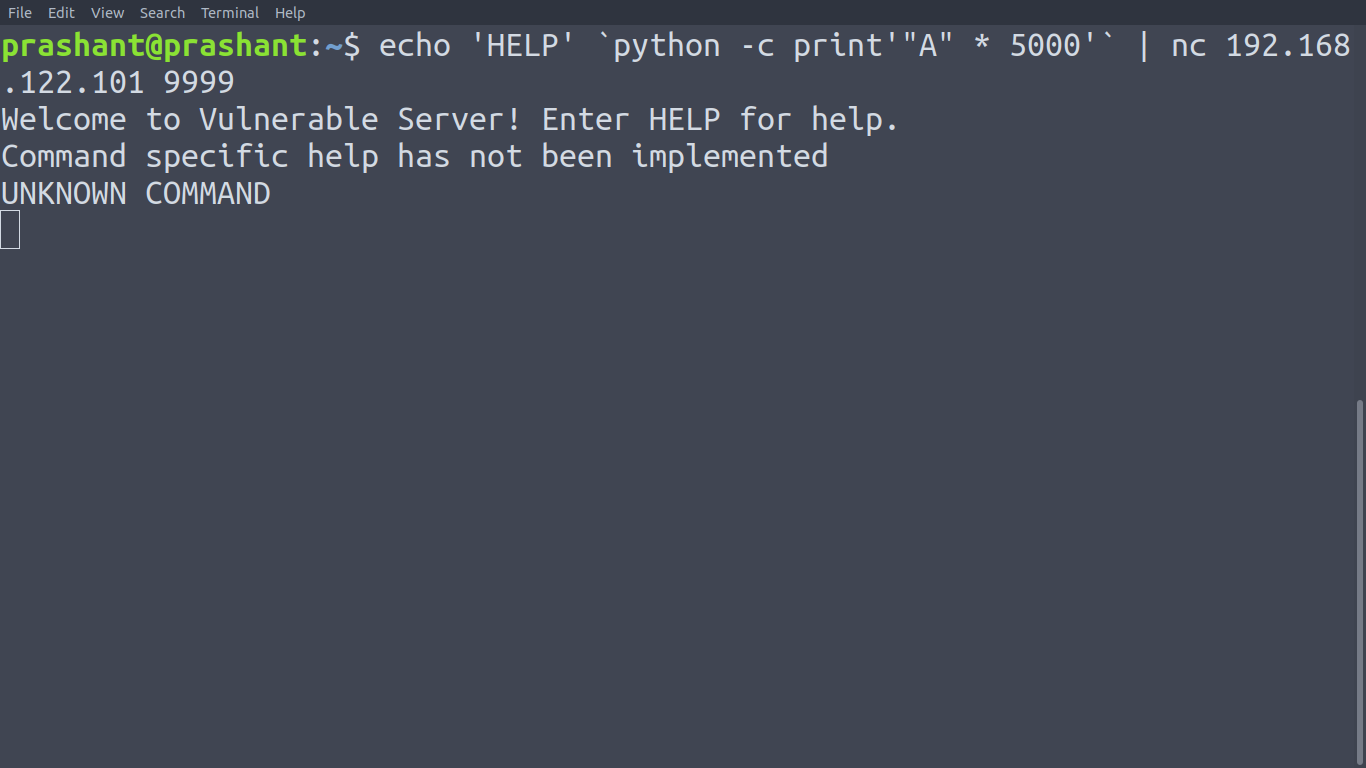


Now, lets send that to vulnserver



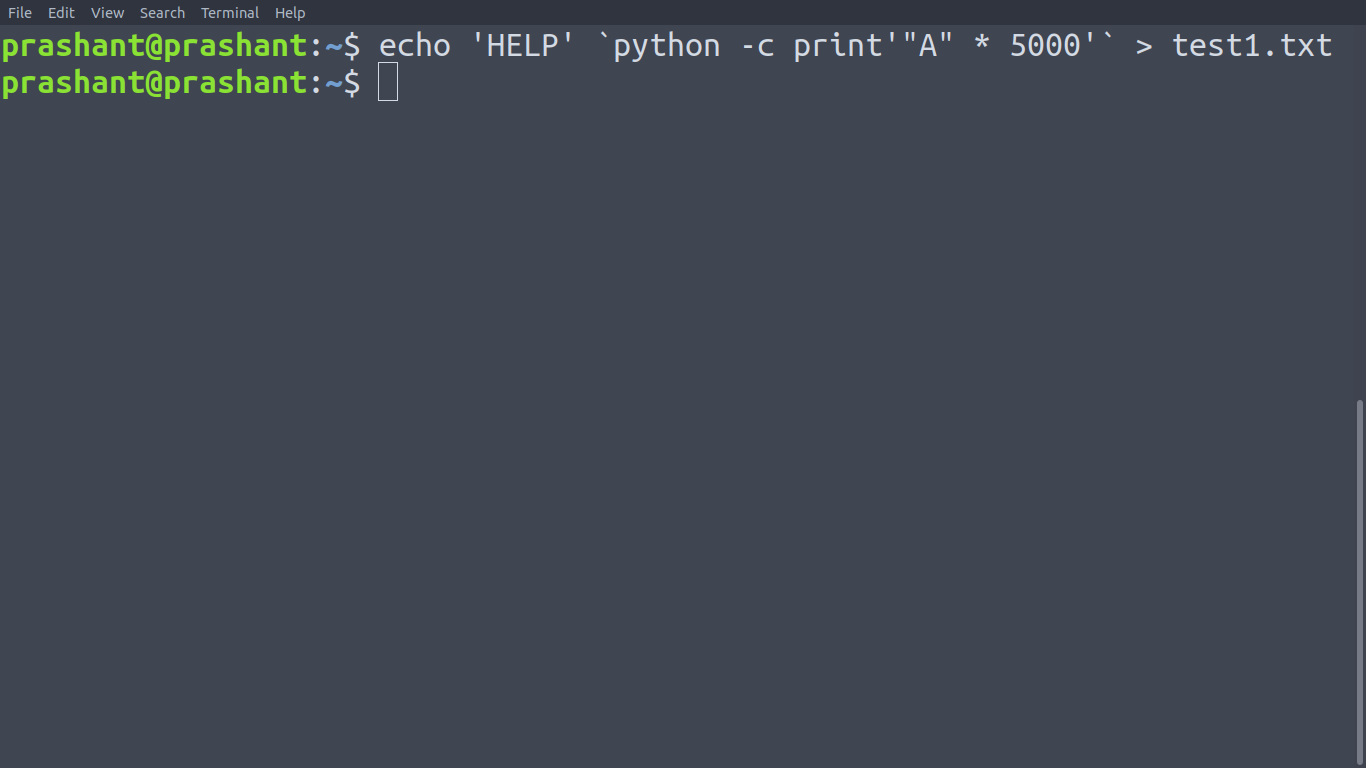
5 A’s seems small to crack the program , lets turn it to 50

Lets try to make it 5000

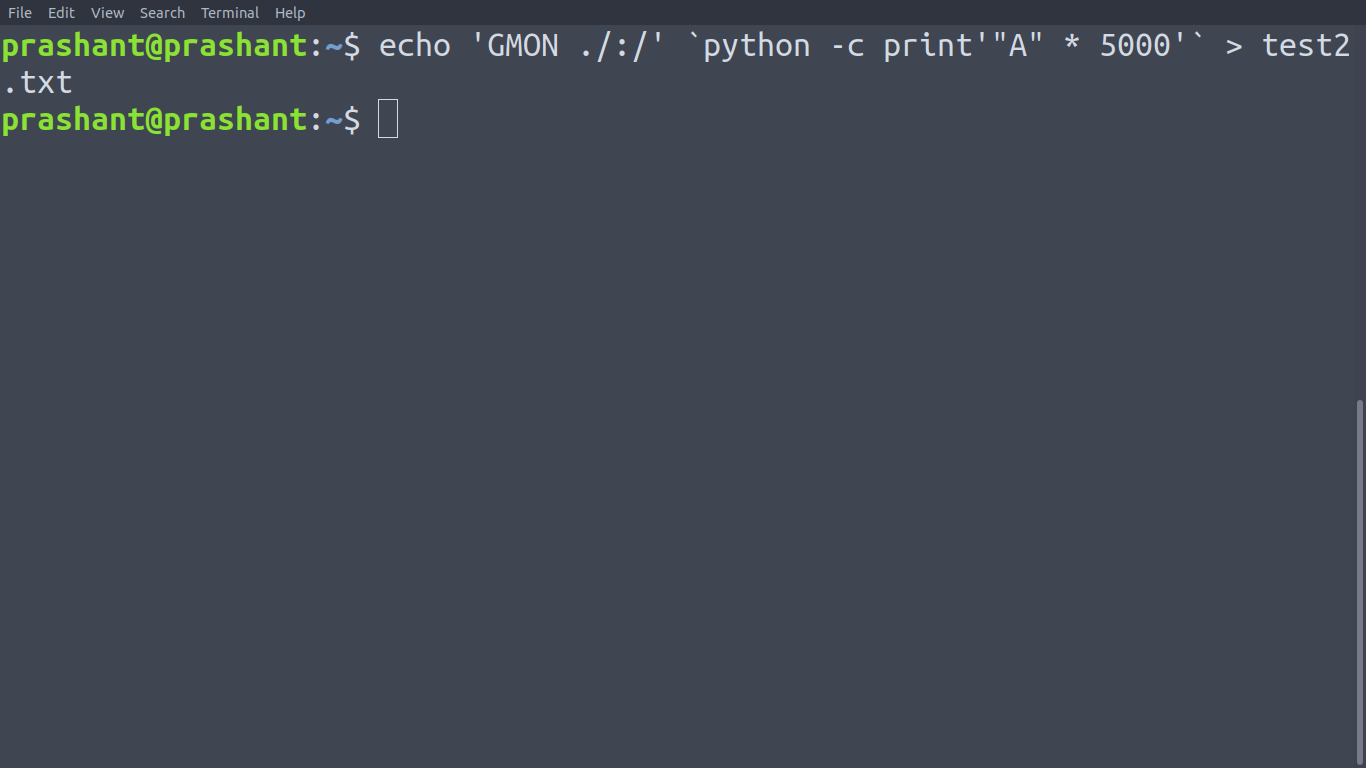


Nothing works

Now, save the generated A in a file as due to terminal interface , new line might be there in those lines



Trying new command

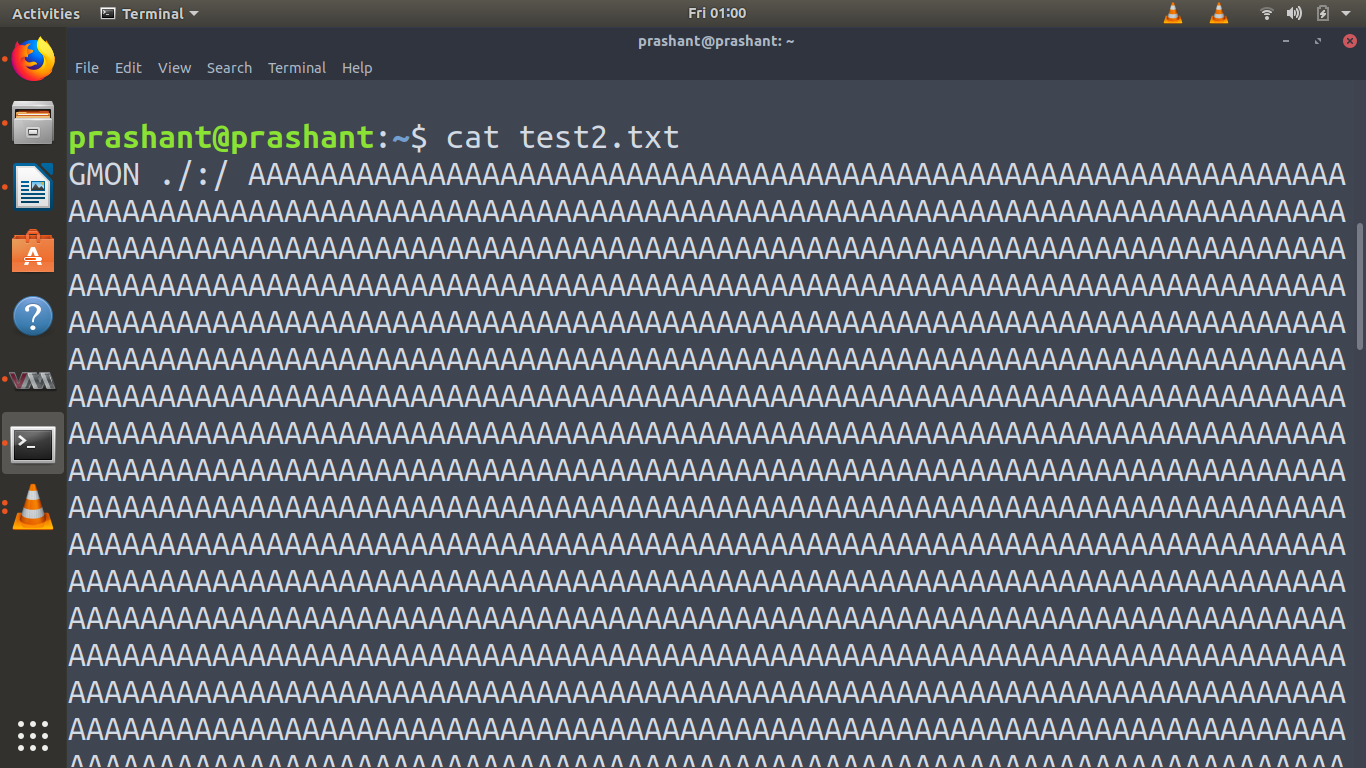


In some cases, it’s not a good Idea to send a randomise, we must do something to make it jump .....to make is redirect

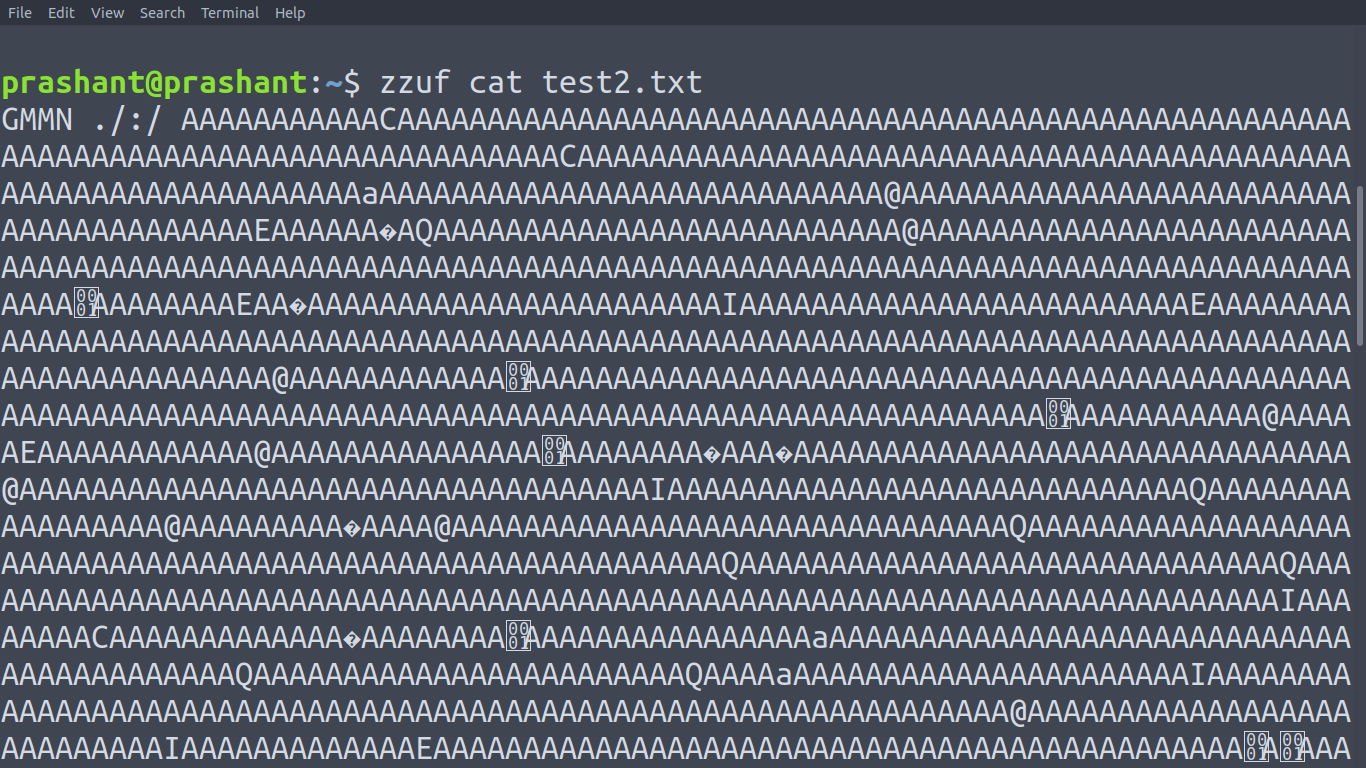
Now, at this point we will install **zzuf** tool in linux

First , run the file by simple cat

$ **cat test2.txt**



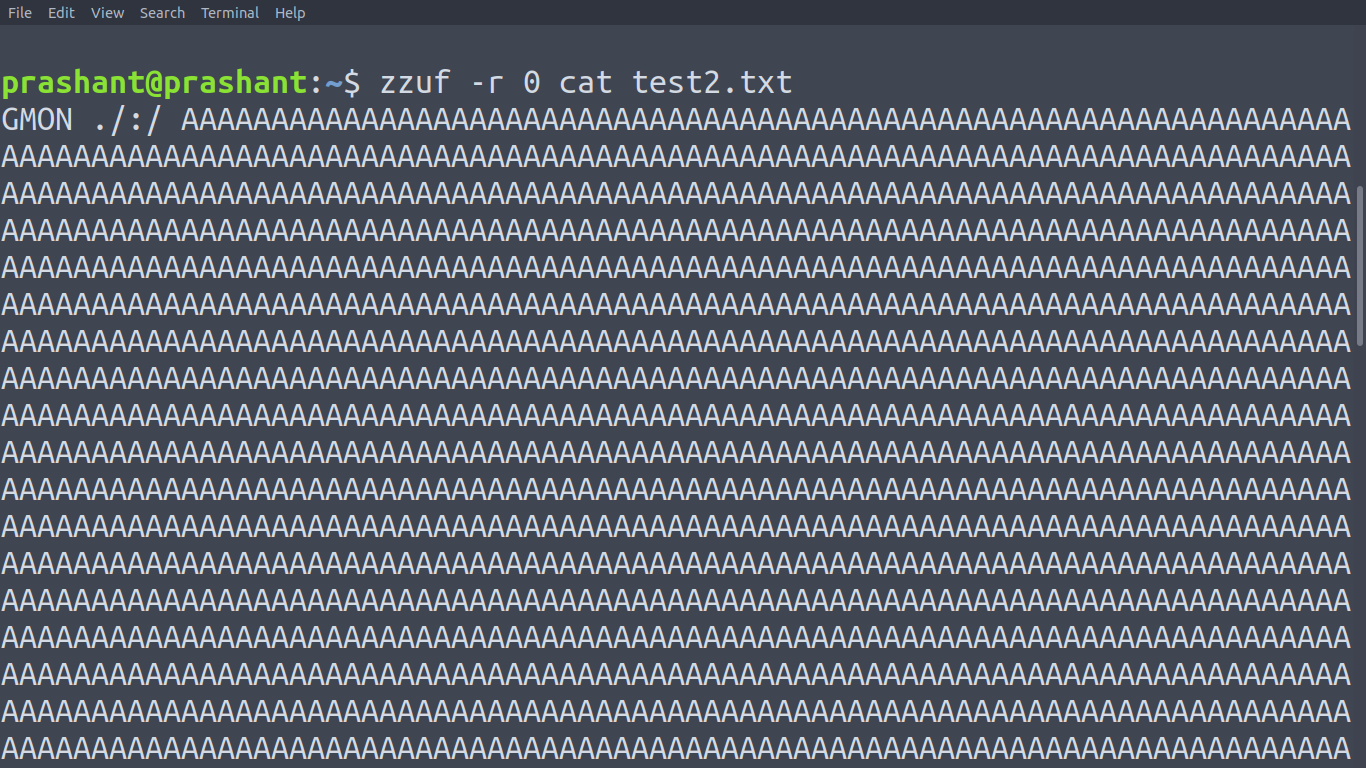
Now, try it with zzuf



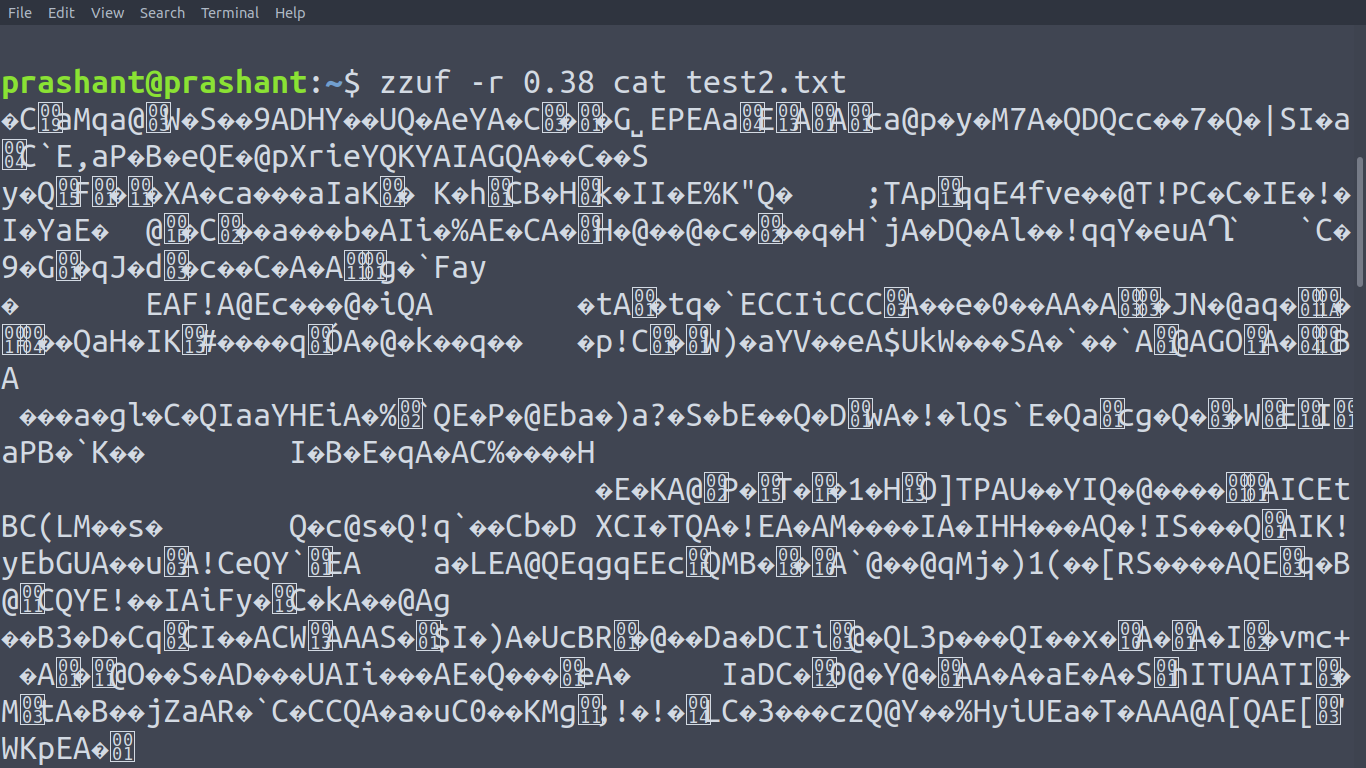
We will find several unknown character ?!?!

Now, lets find the core of file

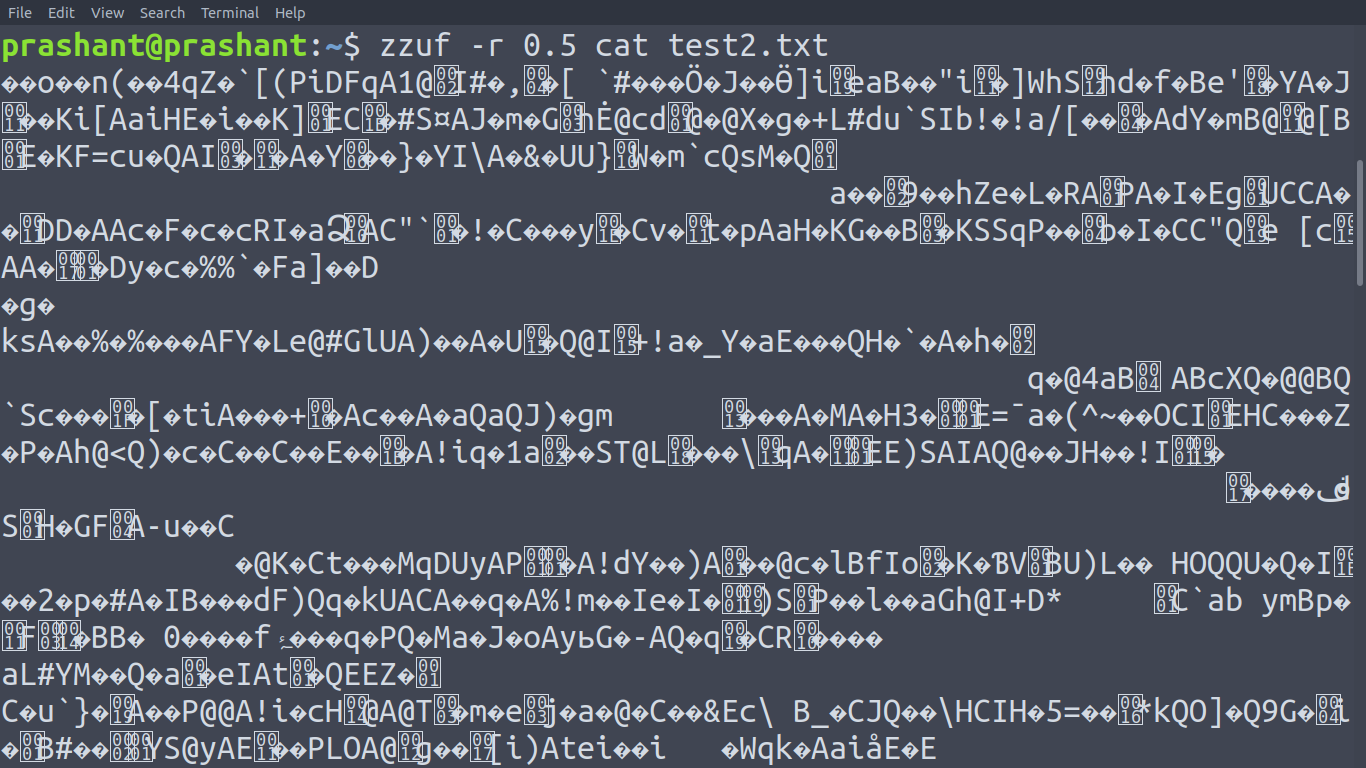
*when we change nothing*

**

*change 38%*

**

*changing 50%*

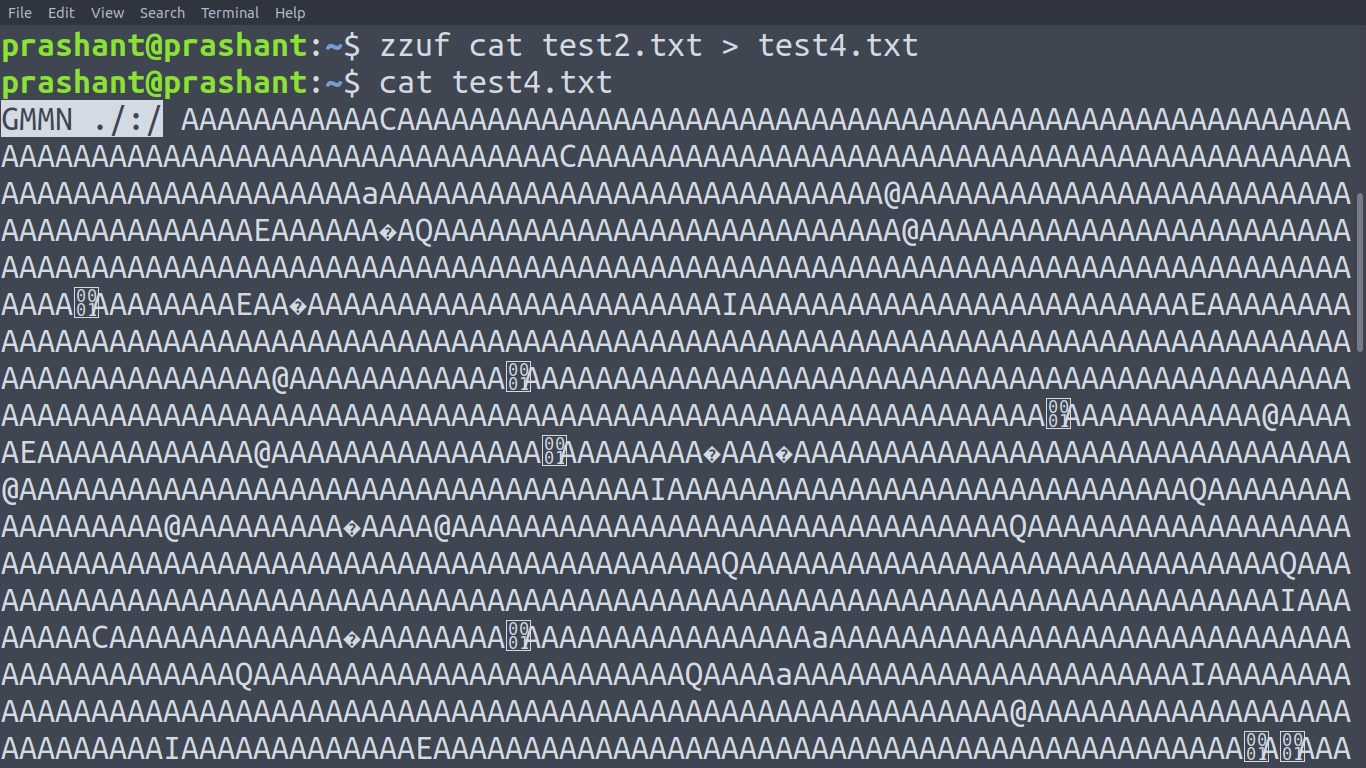
**

*Now, 11%*

**

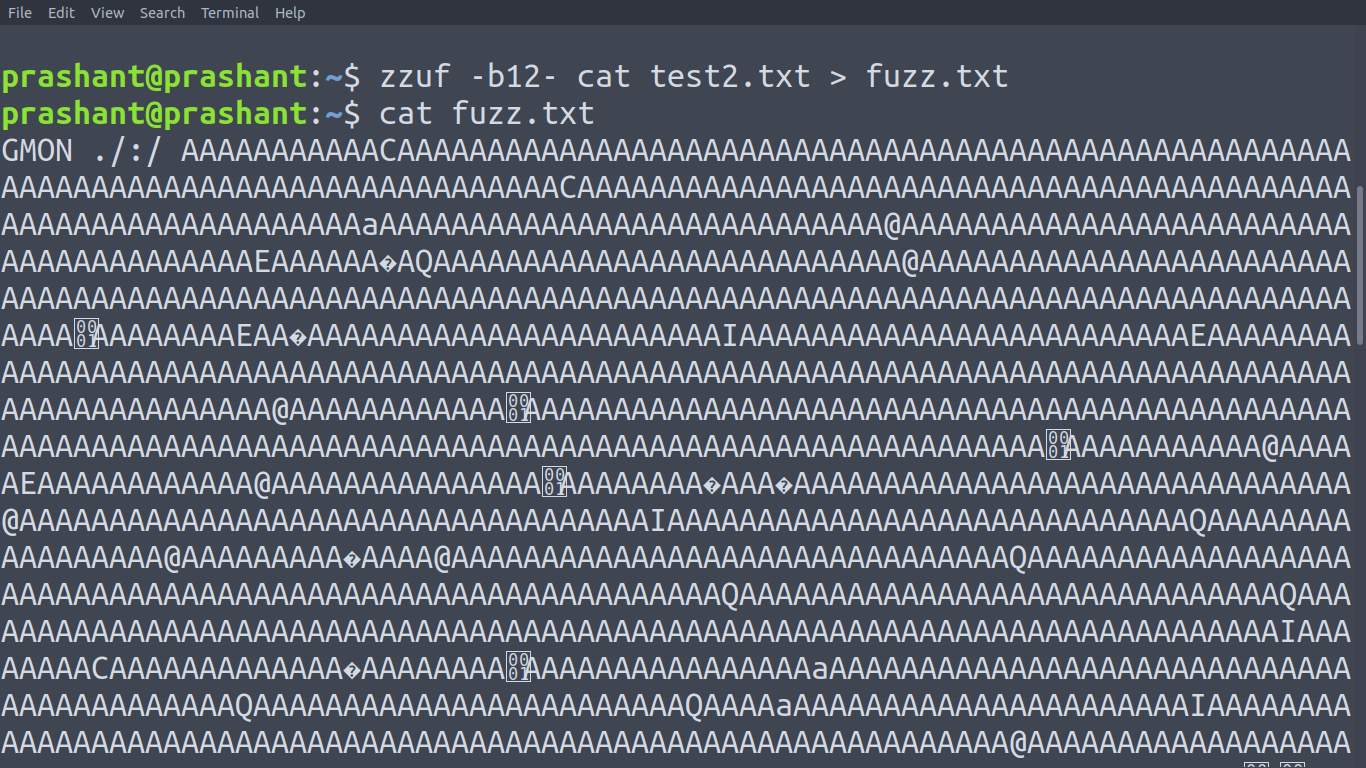
*Overall output depends on Operating system and architecture , mine operating system is Ubantu 18.04*

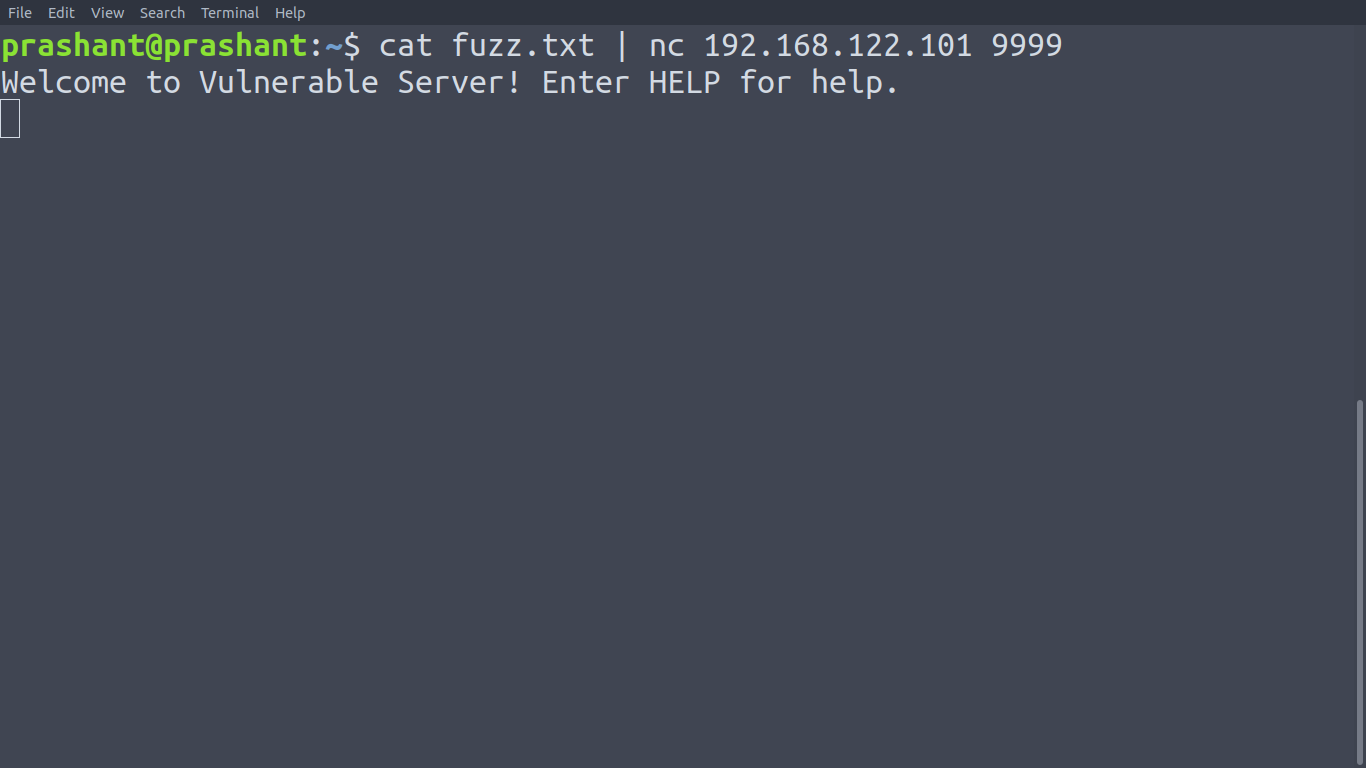
*Now, save standard change to a file*

**

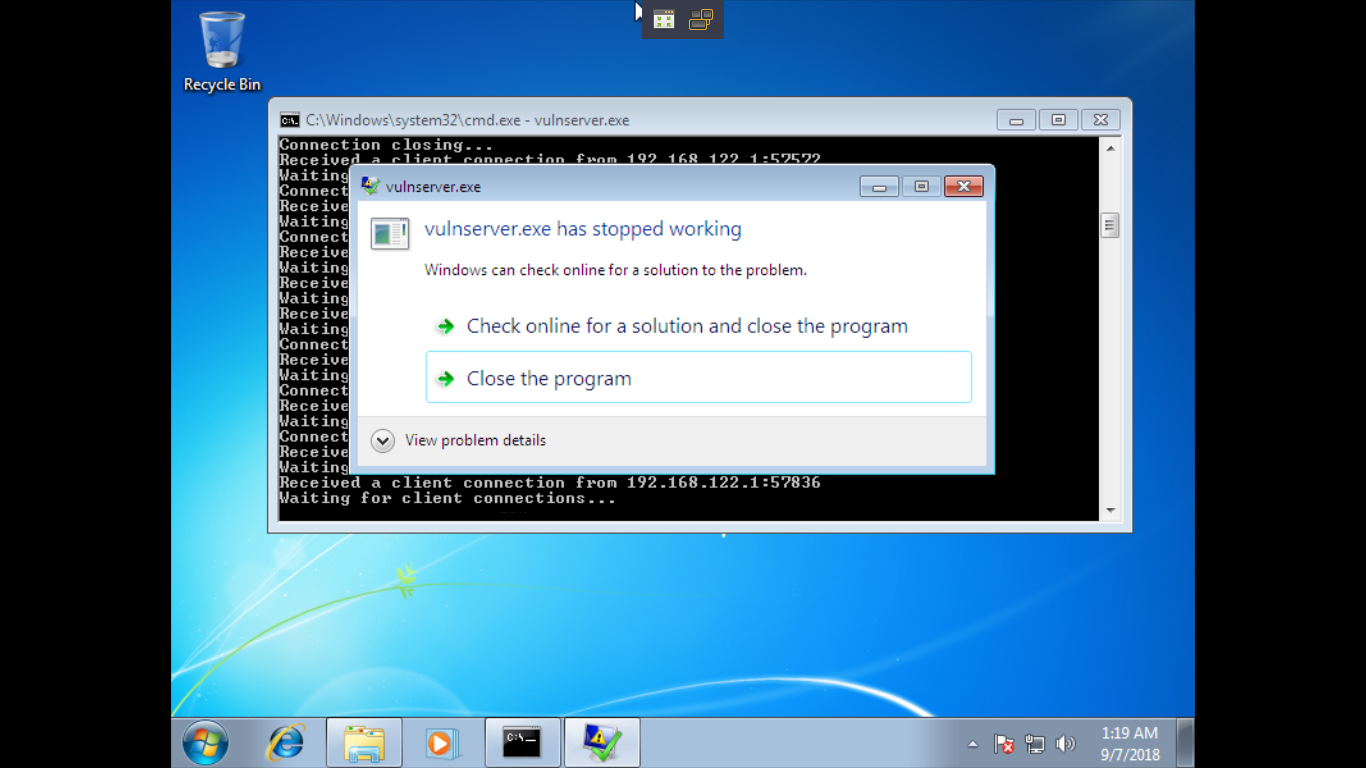
*Now, if we see above file description*

*We will find that , it change the first characters of GMON . We have to escape it that part so*

*Now, send this file to vulnserver*

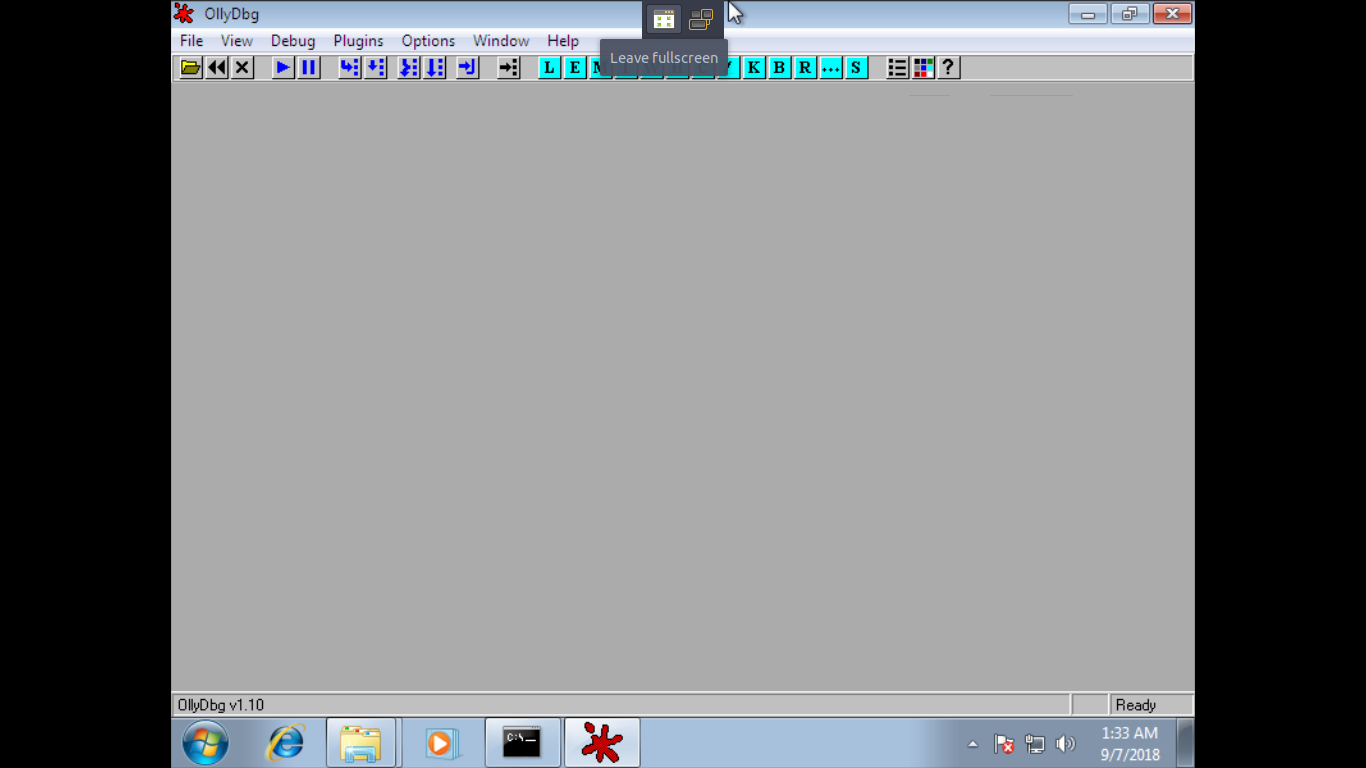
**

*Now, its cursor is keeps Blinking. Lets check the pc*

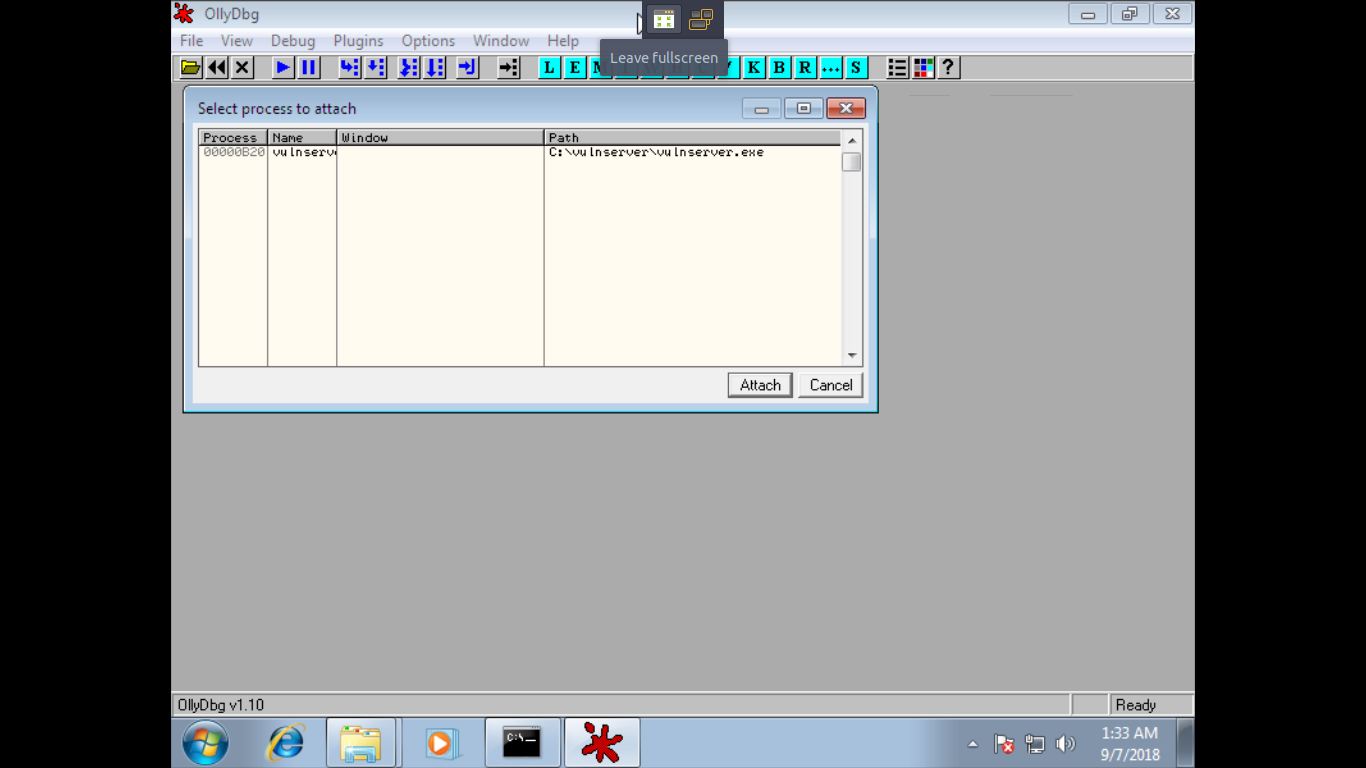
**

*Now , Our program is* **Crashed !!!**

Now, we have python and perl scripts to test on vulnerable

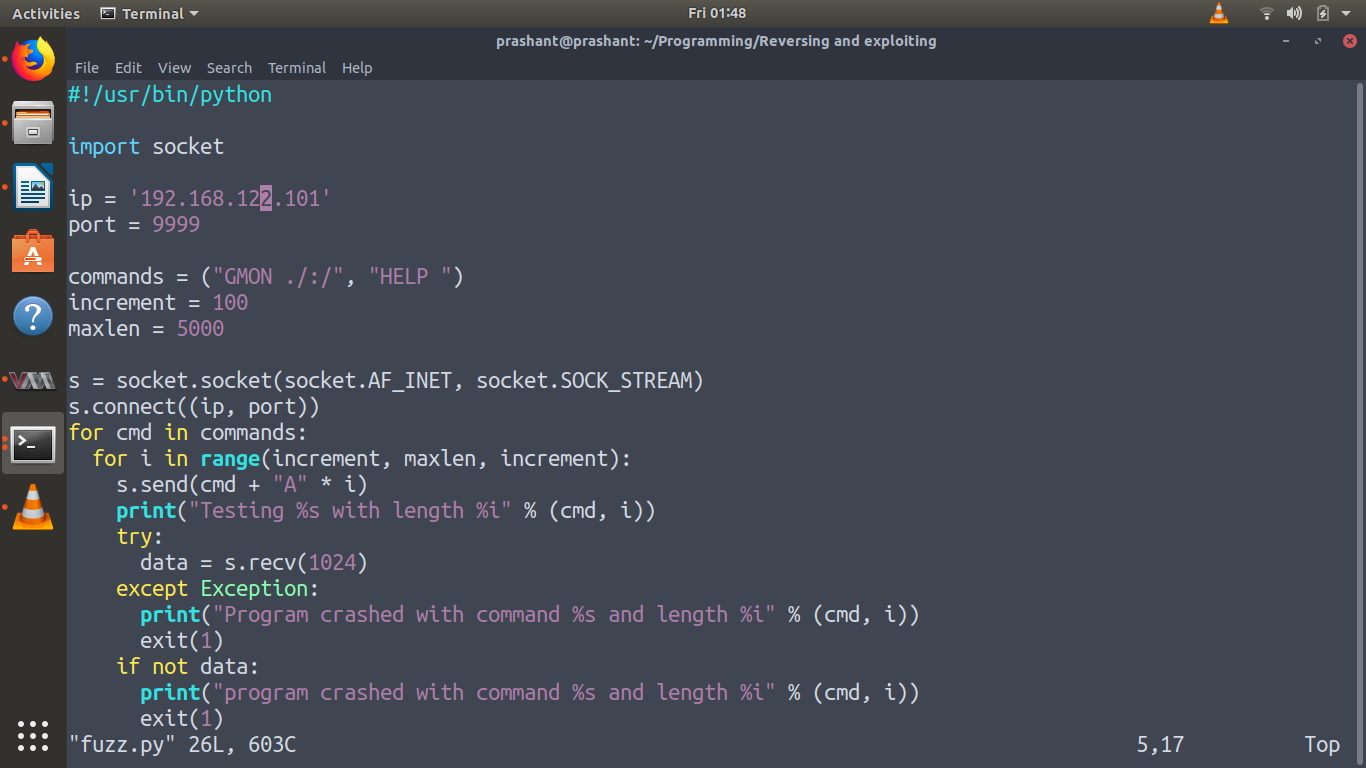
Now, open ollydb

Now, attach vulnserver software to it

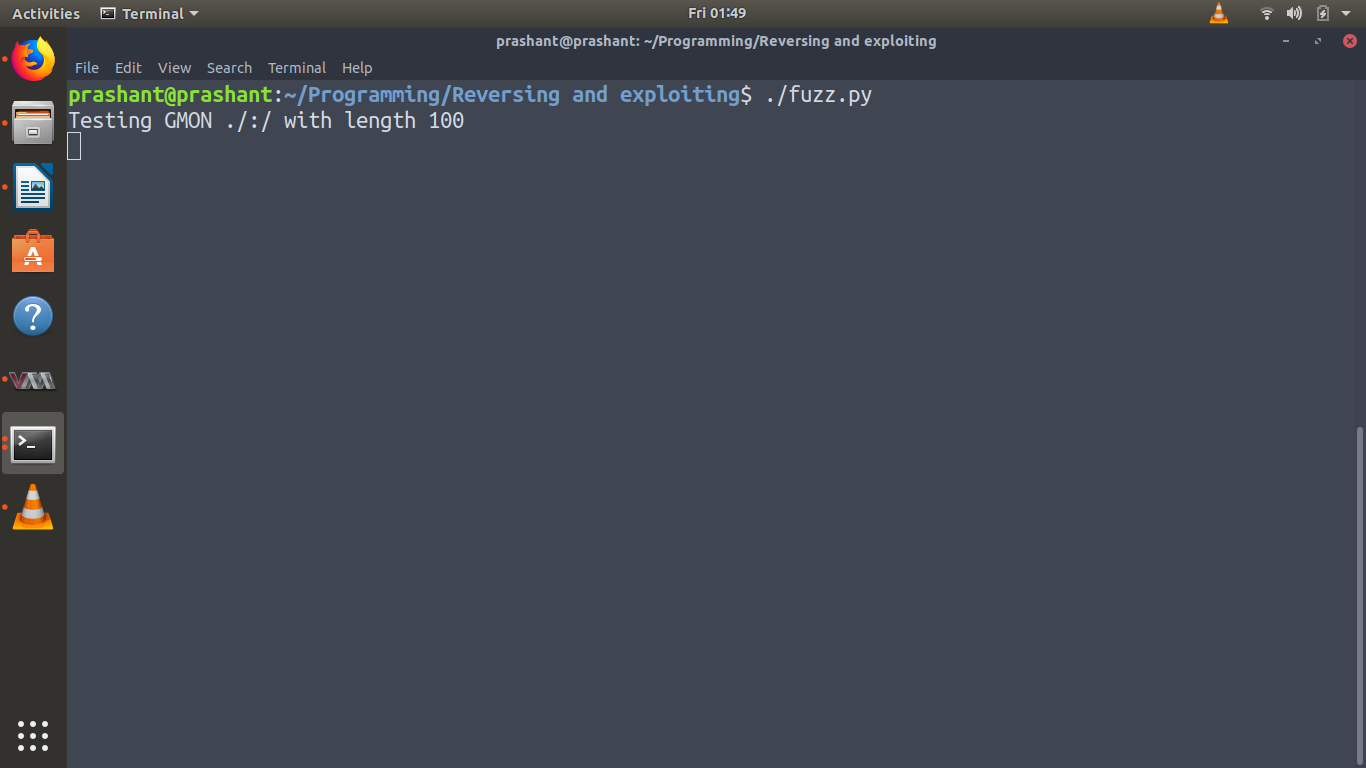
**

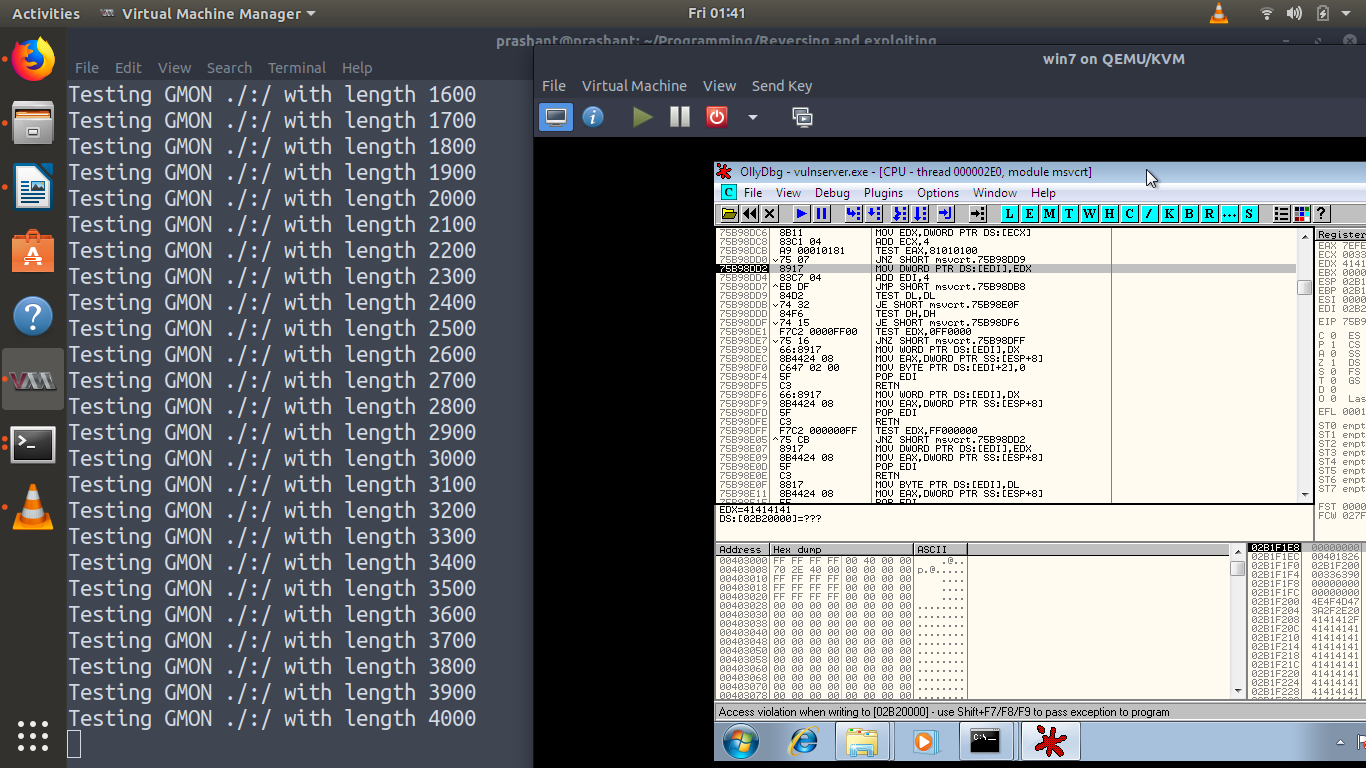
select and attach

Now, run the script with terminal

**

You will see

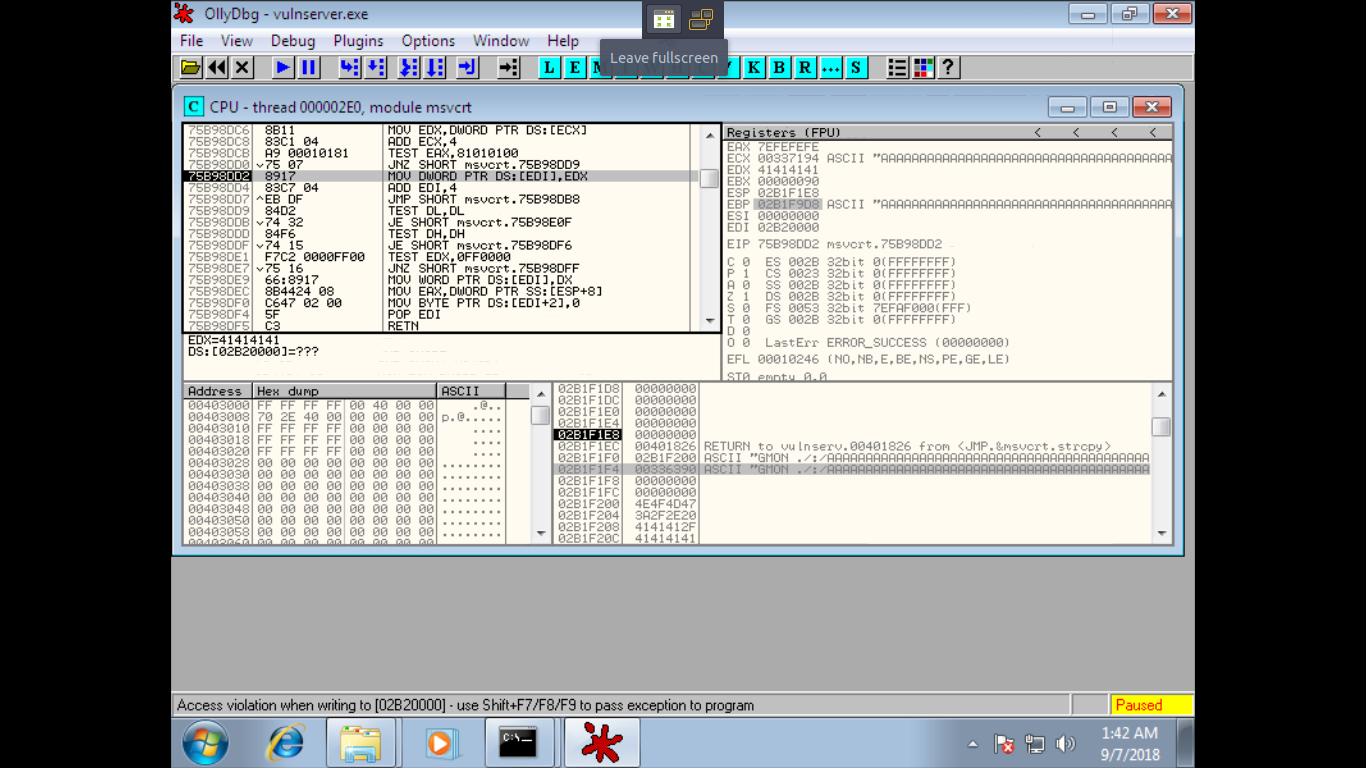
Now, it is it ...go to ollydb and press the play button

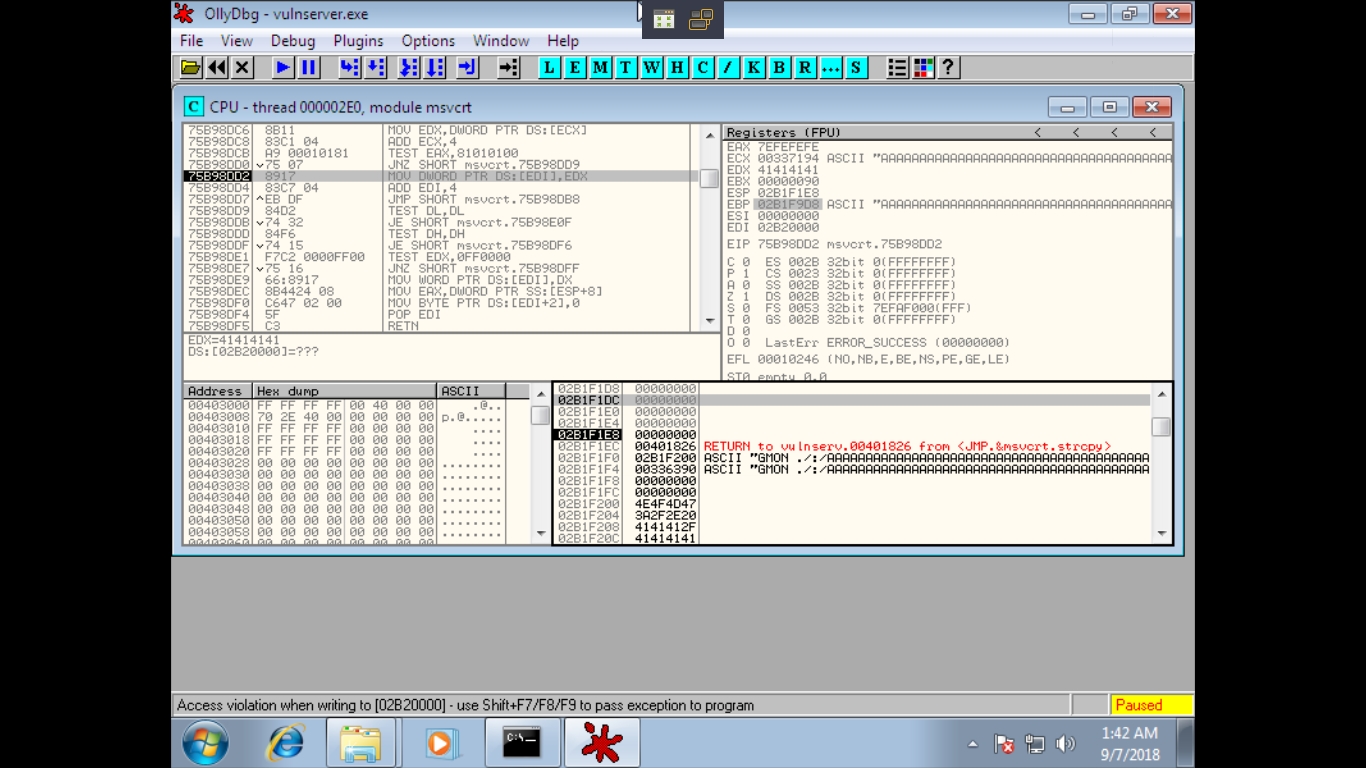
**

Now, the message appears that ***Access voilation ...***

All this means that system is crashed at length 4000 .

Other informations are





Returning Register values