N-CY Assignment 1

Sir Qaiser Shafi

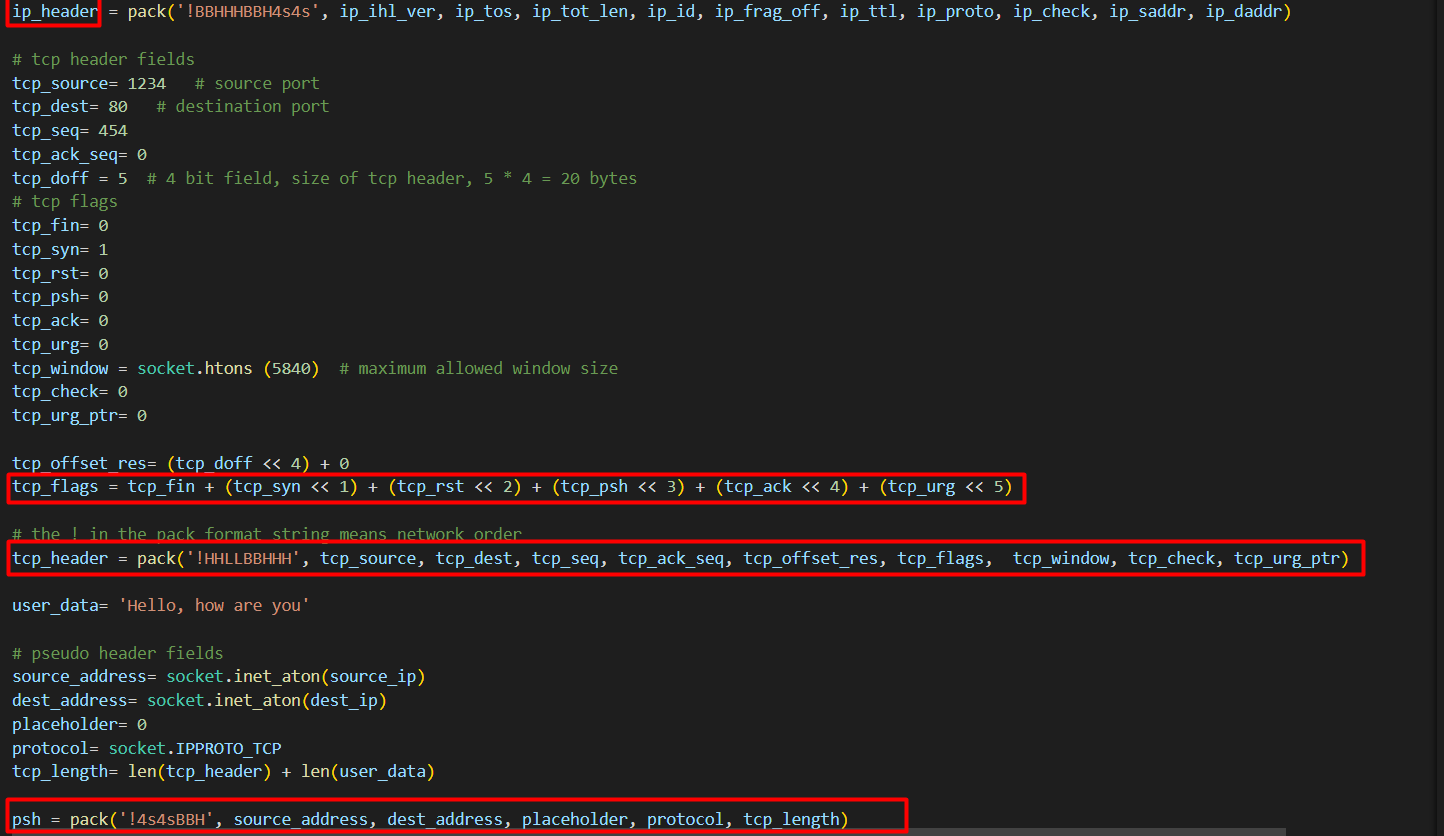
Ashar Khalil

20K-1724

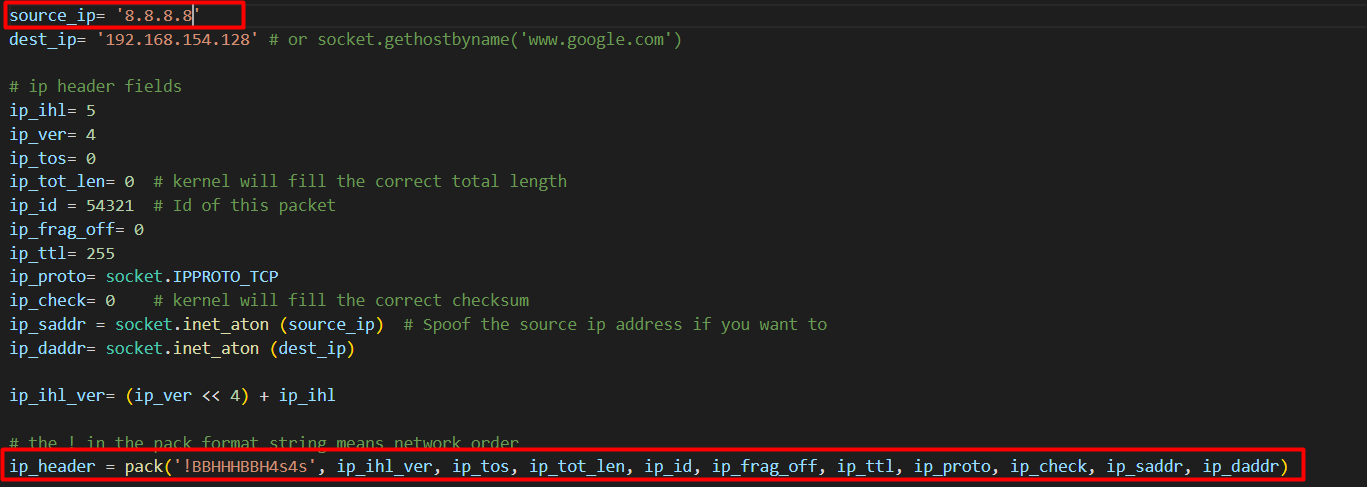
Q1: Make a setup of injecting TCP/IP custom made packet using python.

programming, the code should perform following properties.

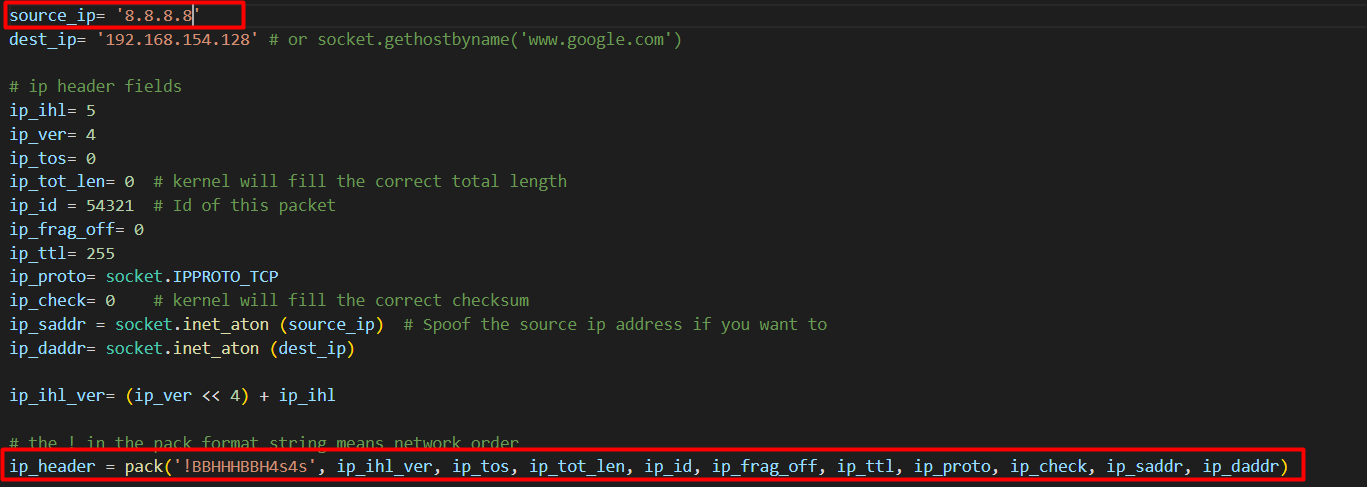
* Build custom TCP header.



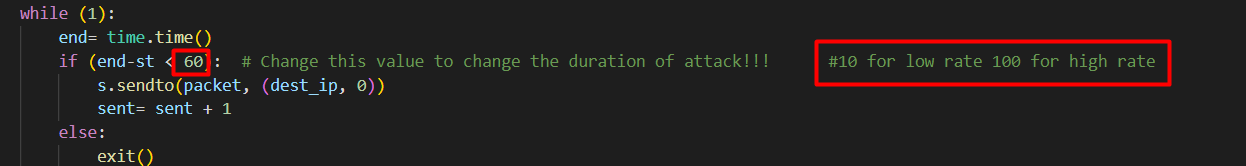
* Build custom IP header.



* Use Spoofed IP address.



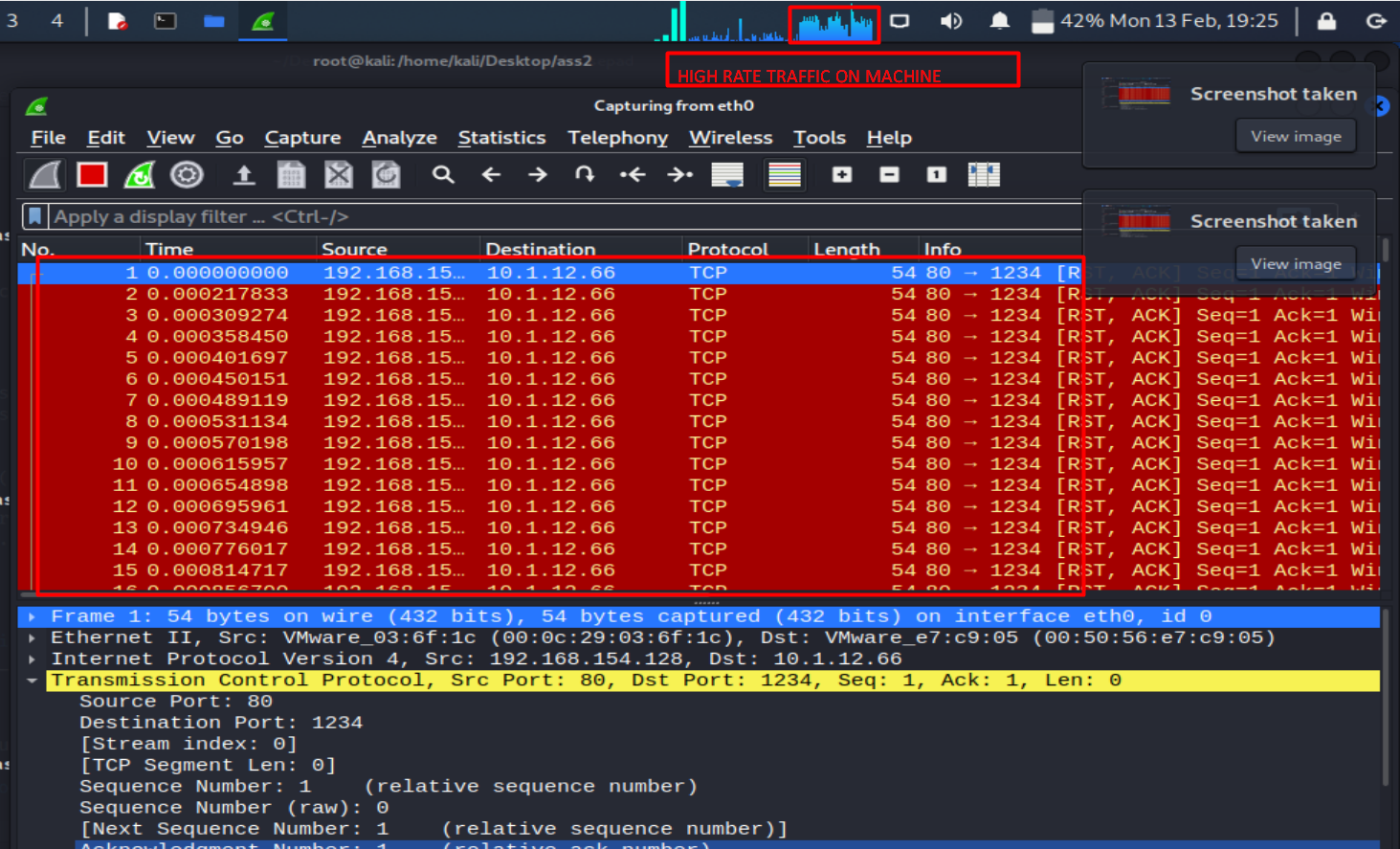
* Modify code for high-rate and low-rate Denial of service. Apply your own algorithm to justify.

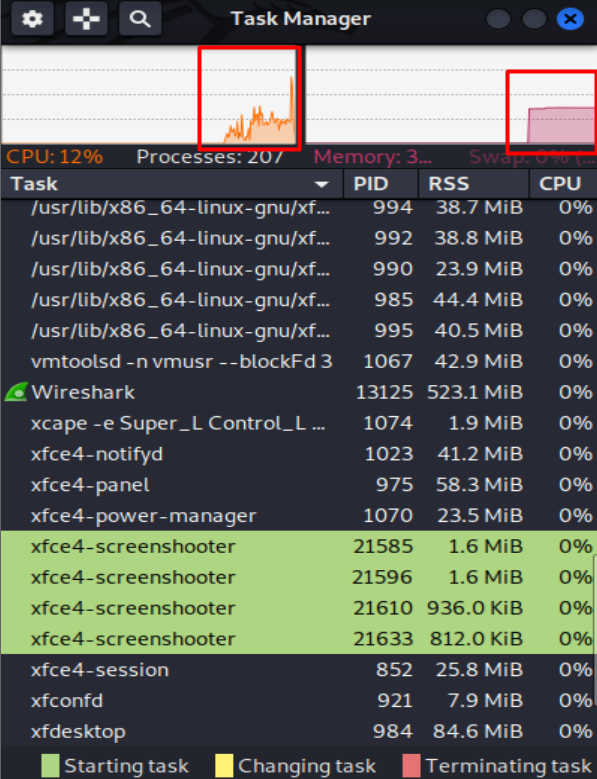


* Extra marks for building another malicious scenario out of this code other than DoS.

😊

Show results on resources being overwhelm on victim machine using change in RAM and processor utilization.





Q2: Modify this code to make it an “Port Scanning” script. It should be able to check custom range of ports using XMAS scanning technique.

Text

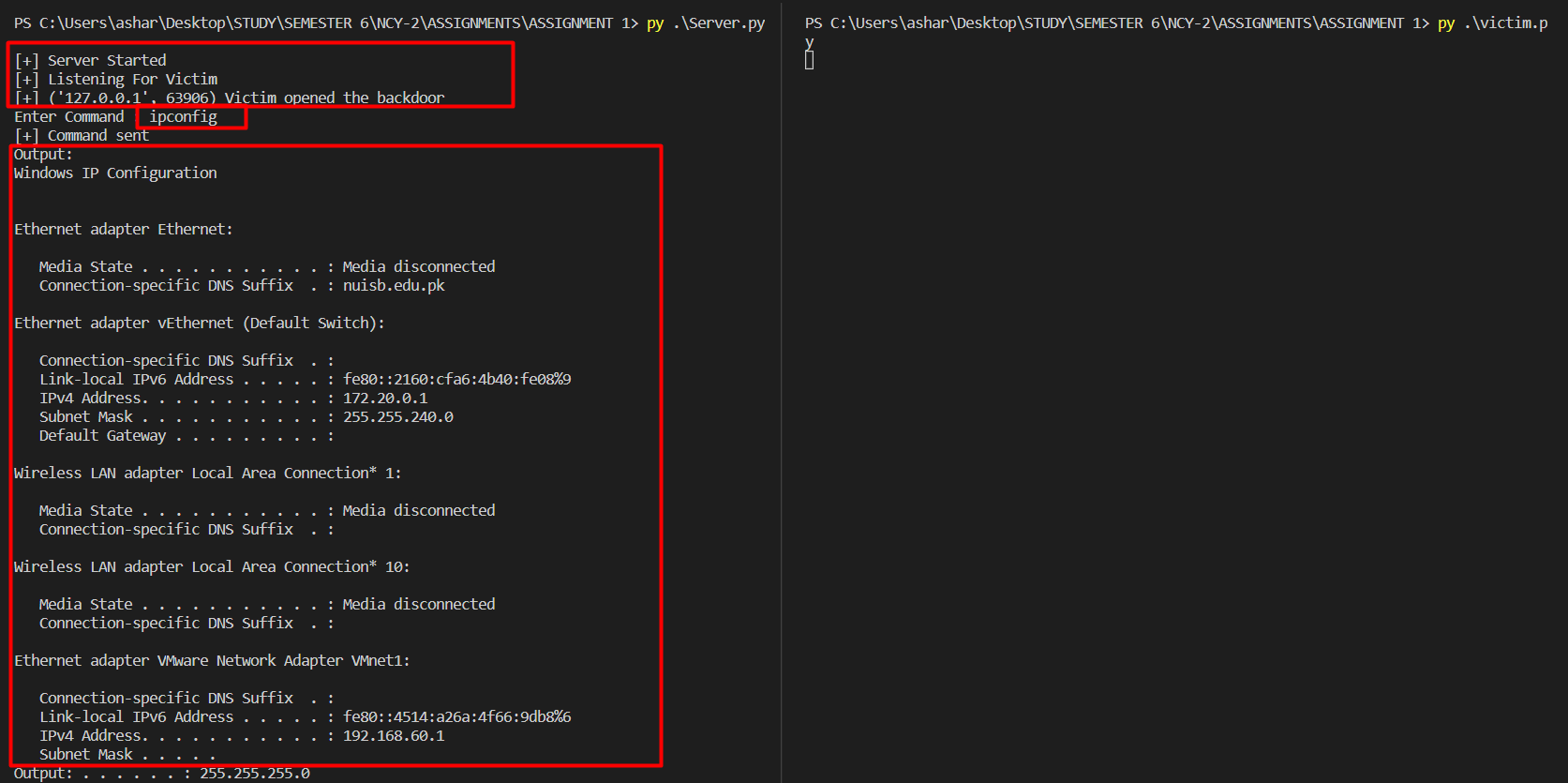
Description automatically generated

Q3: Implement a simple backdoor sub-process to any victim that is connected to a

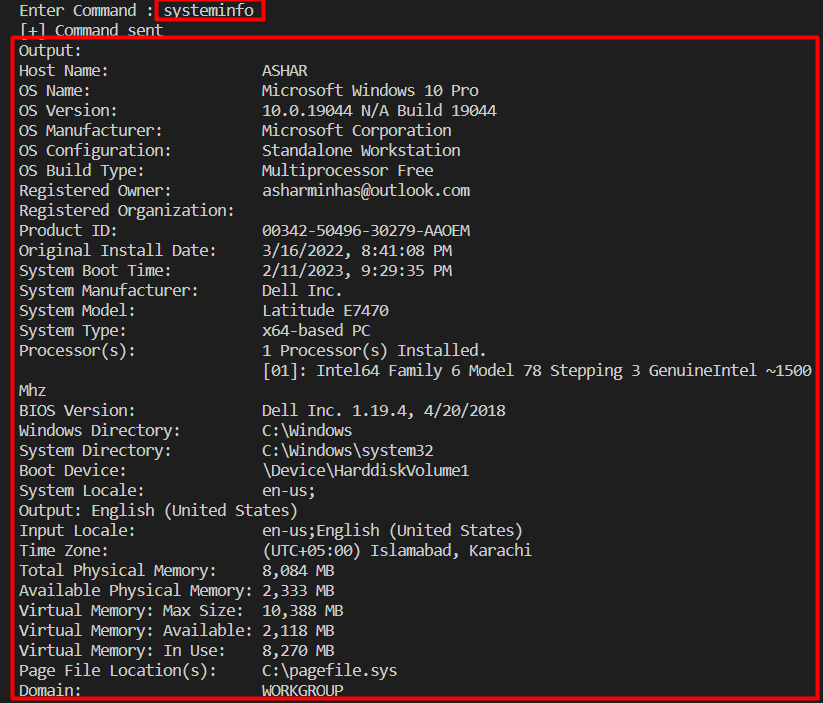
malicious server. Perform following operations on the connected victim.

1. Run following commands on victim machine

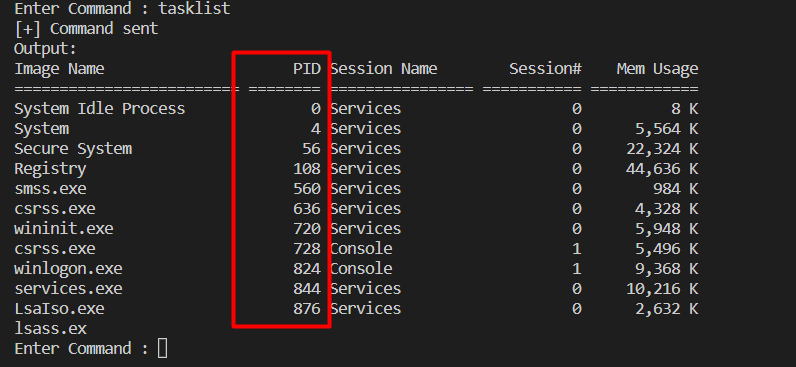
a. Ipconfig



b. Sysinfo

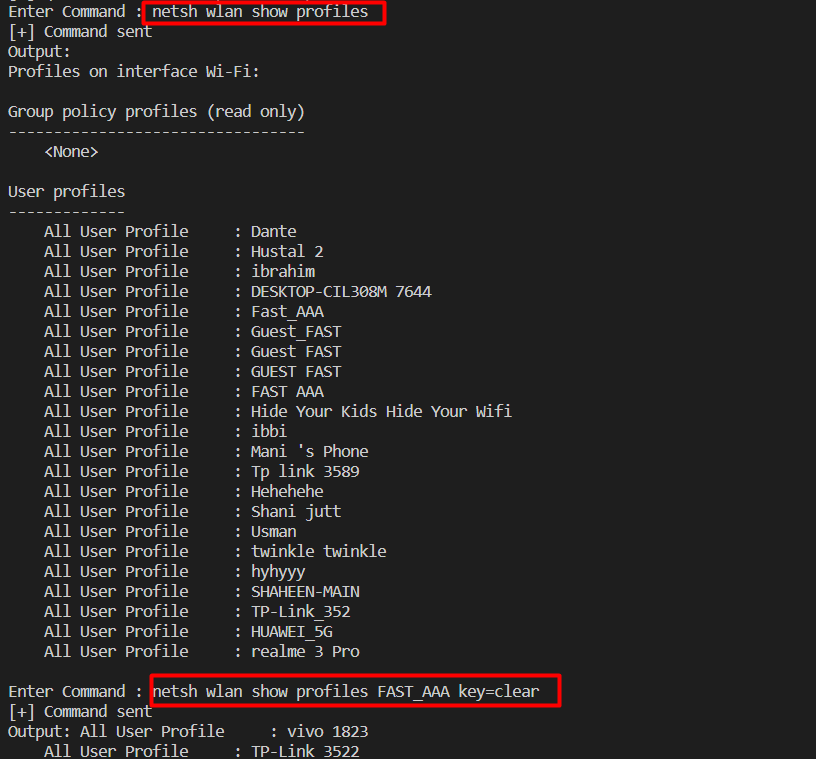


c. Process information and status



d. Extra marks for more commands that give more information of victim.

Wi-Fi passwords



2. Inject DoS(made in Q1) simple packet injector using this back door, use appropriate python function to inject.

* I made a http server to do this.
* I will get dos.py from server and then it will be executed easily on victim.

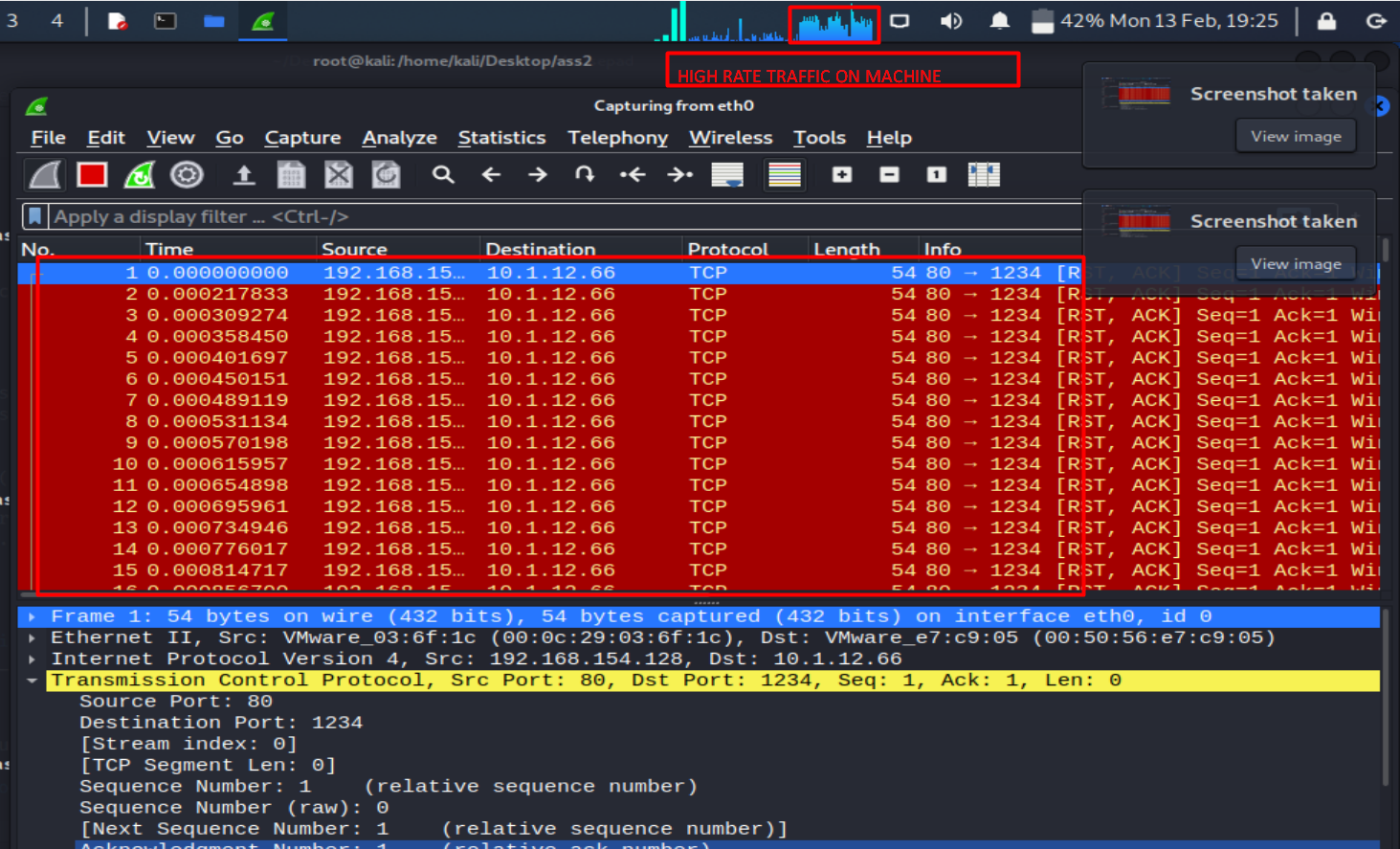
Text

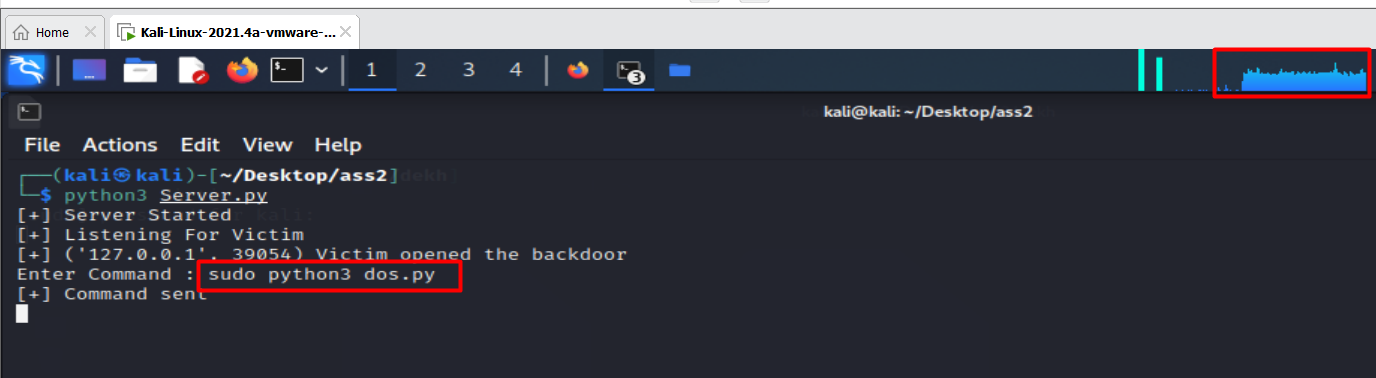
Description automatically generated

Text

Description automatically generated

3. Show high-rate traffic on victim machine using simple Wireshark dump





4: sysinternals are windows commands victim is on Linux so not possible in current scenario.