ASSIGNMENT – 2

CSCI-6708 Advanced Network Security

Sumit Singh

B00882103

Sm435410@dal.ca

Exercise 1

1. Knowing the client details and constraints. Make sure you know and comprehend the nature and characteristics of the client organization's business, system, and network before executing any ethical hacking. This will instruct you on how to handle sensitive, confidential, or proprietary information that you may come across during ethical hacking.
2. An ethical hacker should Identify and report vulnerabilities to the organization. Ethical hackers report vulnerabilities to the organization and offer advice on how to fix them. Often, the ethical hacker conducts a re-test with the organization's permission to ensure that they have been thoroughly exposed.
3. Knowing the limit and when to stop is basic ethics of hacker. Tests should be conducted up to and not exceeding the agreed-upon limits. ethical hackers should perform **attacks** only if they have previously been agreed upon with the client.
4. When performing the test, maintain confidentiality and follow a Nondisclosure Agreement (NDA). The information obtained and gathered during the testing or attack might contain sensitive information and as an ethical hacker you must not disclose it.
5. As an ethical hacker, you need patience and thoroughness. A feature of ethical hacking professionals is keeping complete records of all testing, whether they were successful or not. Each test should be documented with the date, description, and results, and a duplicate copy of the log book should be retained.
6. A hacker must adhere to certain constraints in order to be ethical. As a result, a test strategy plan should specify the networks to be tested, the frequency of testing, the testing processes, and the plan's approval.
7. Empirical methods should be used by ethical hackers. Empirical approaches aid in the development of quantifiable goals, the identification and development of repeatable tests, and the future provision of accurate and valid tests.

References

[1]"Ethical Hacking Code of Ethics: Security, Risk & Issues - Panmore Institute", *Panmore Institute*, 2022. [Online]. Available: http://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues. [Accessed: 12- Feb- 2022].

[2]"Ethical Hacking - Computing and Software Wiki", *Wiki.cas.mcmaster.ca*, 2022. [Online]. Available: http://wiki.cas.mcmaster.ca/index.php/Ethical_Hacking#10_Commandments_of_Ethical_Hacking. [Accessed: 12- Feb- 2022].

[3]2022. [Online]. Available: https://info-savvy.com/scope-and-limitations-of-ethical-hacking/. [Accessed: 12- Feb- 2022].

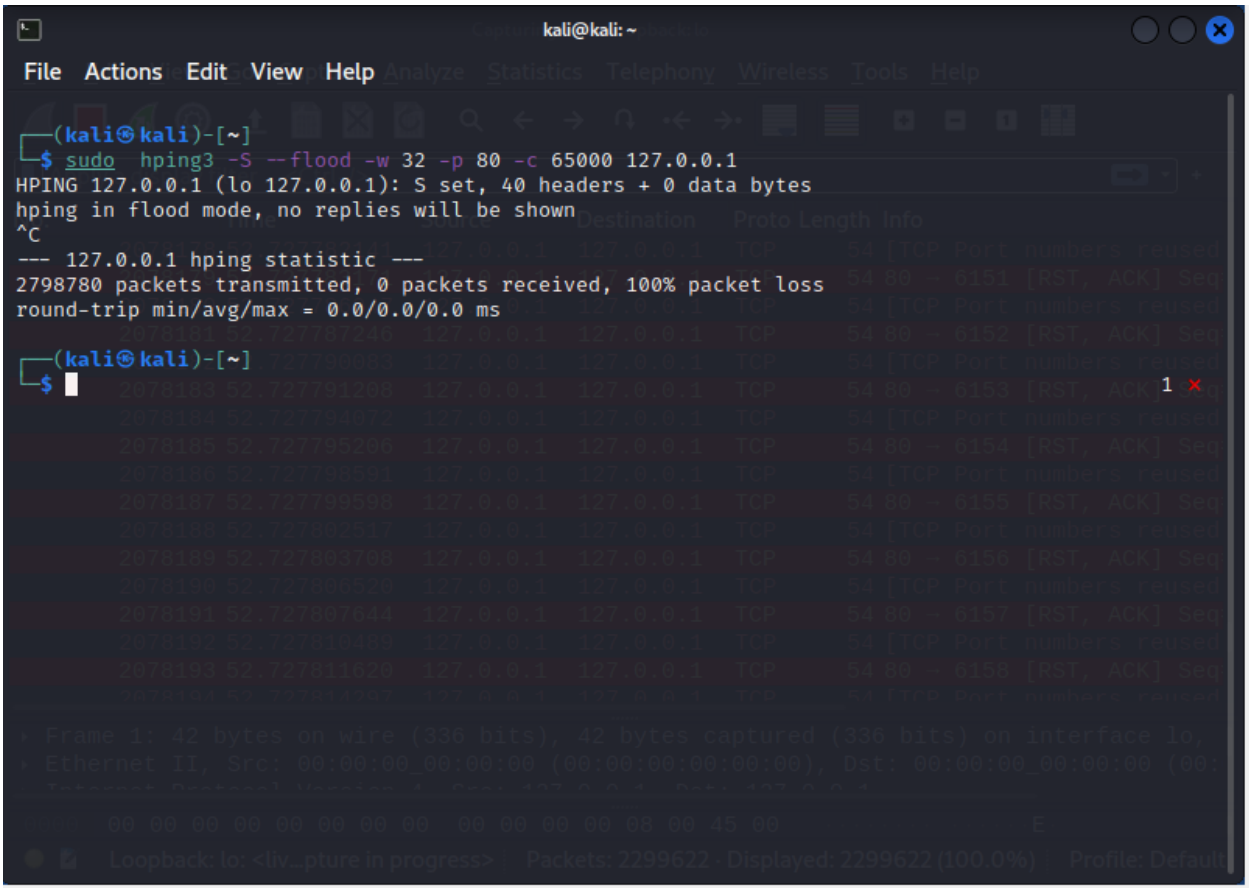
[4]*Citeseerx.ist.psu.edu*, 2022. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.184.6791&rep=rep1&type=pdf. [Accessed: 12- Feb- 2022].

Exercise 2:

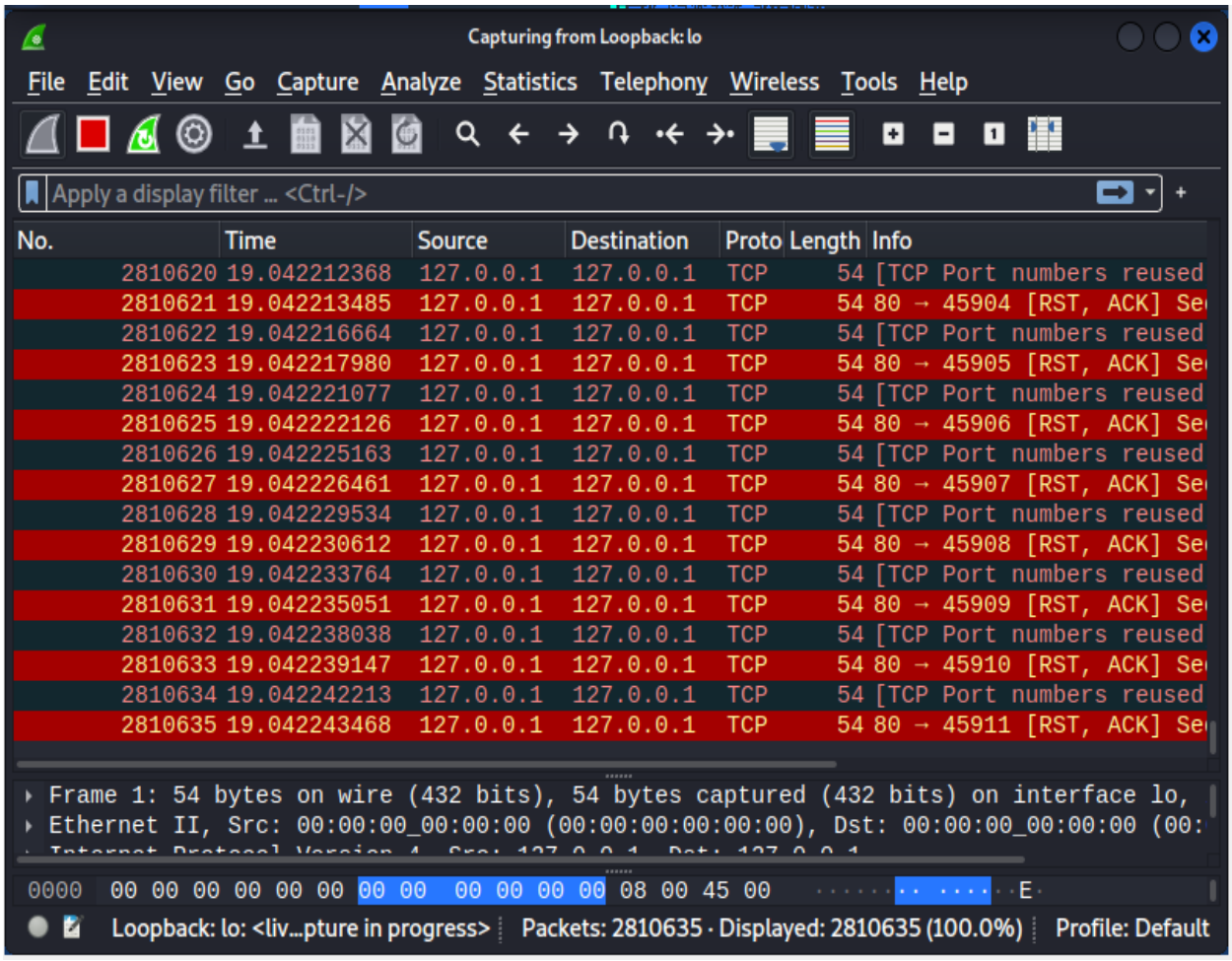
Experiment 1: Simulation of a TCP SYN DoS attack

Command: sudo hping3 -S --flood -w 32 -p 80 -c 65000 127.0.0.1

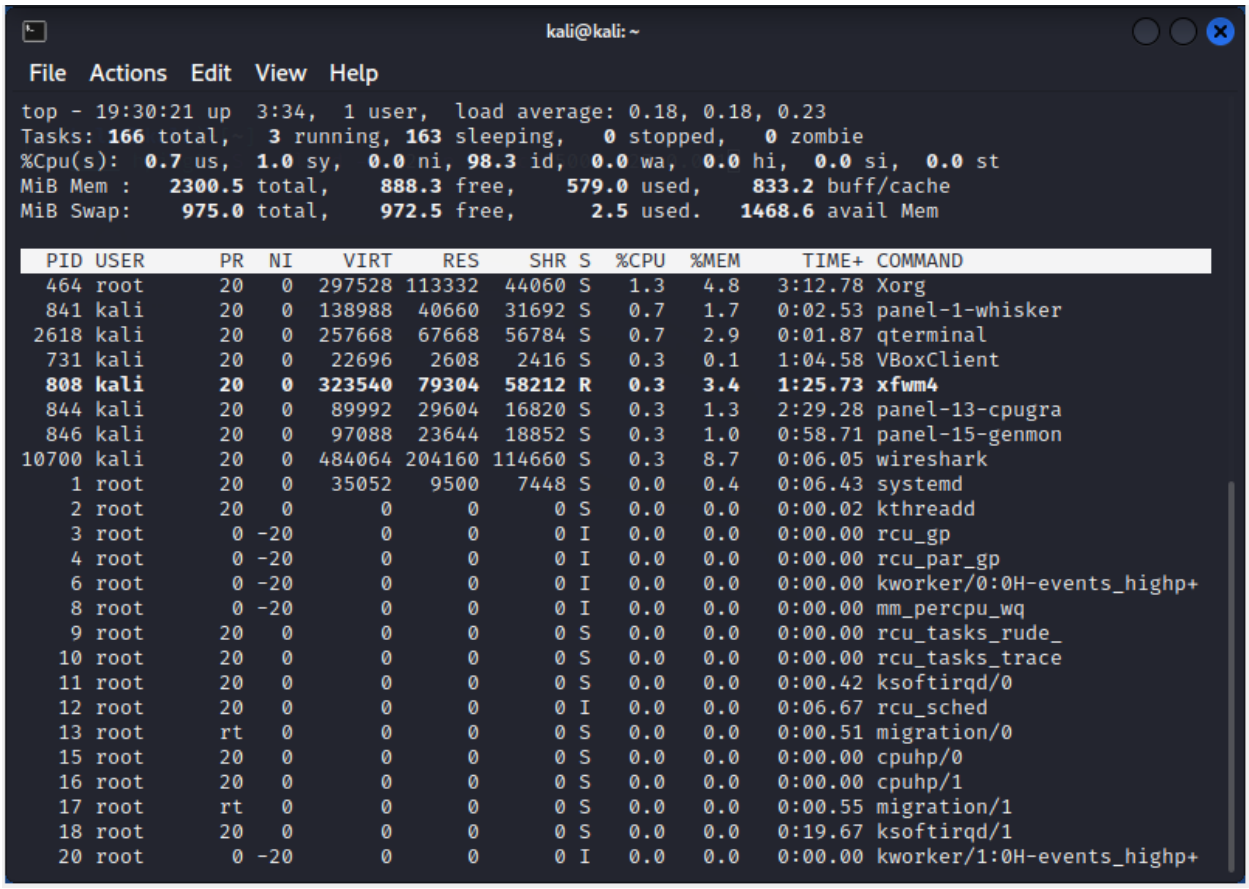
Screenshot of hping3 command terminal:



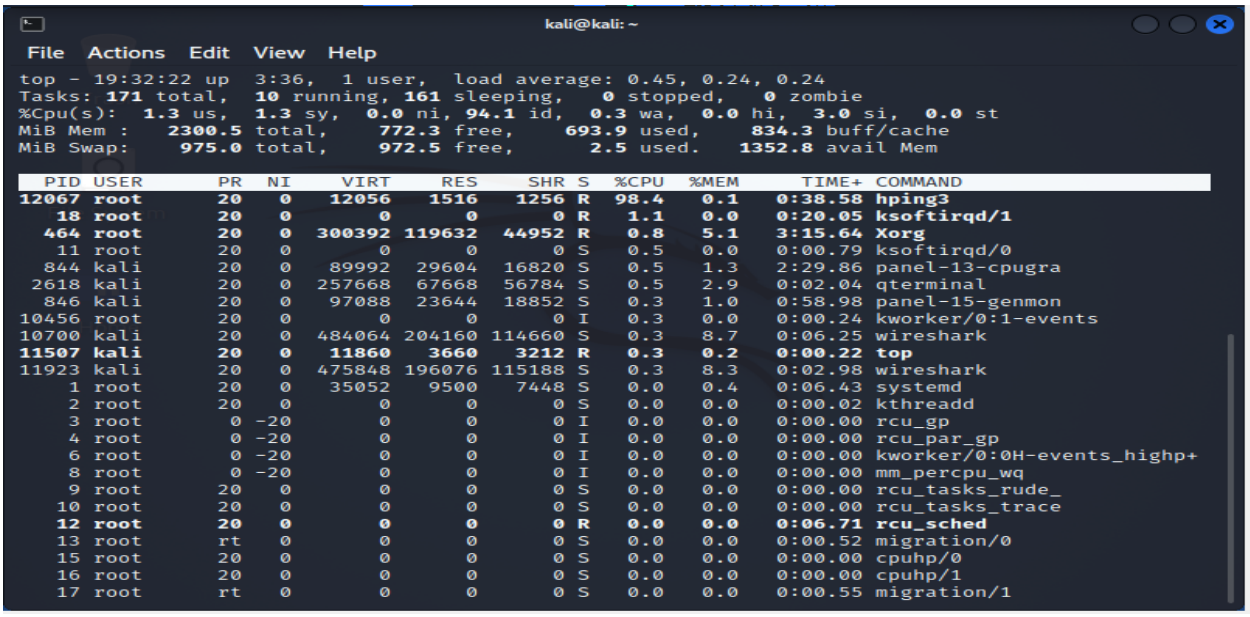
Screenshot of wireshard capture:



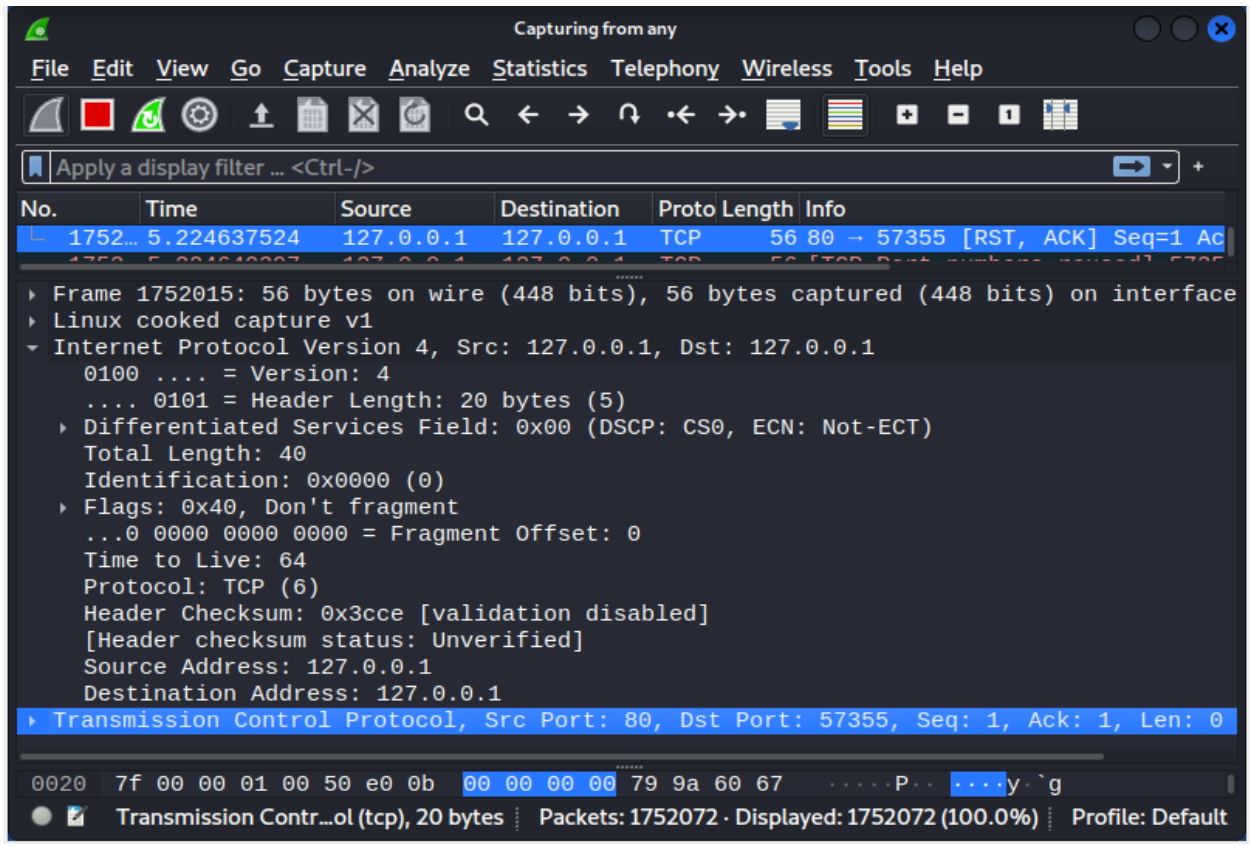
Screenshot of top command before attack:



Screenshot of top command during attack:



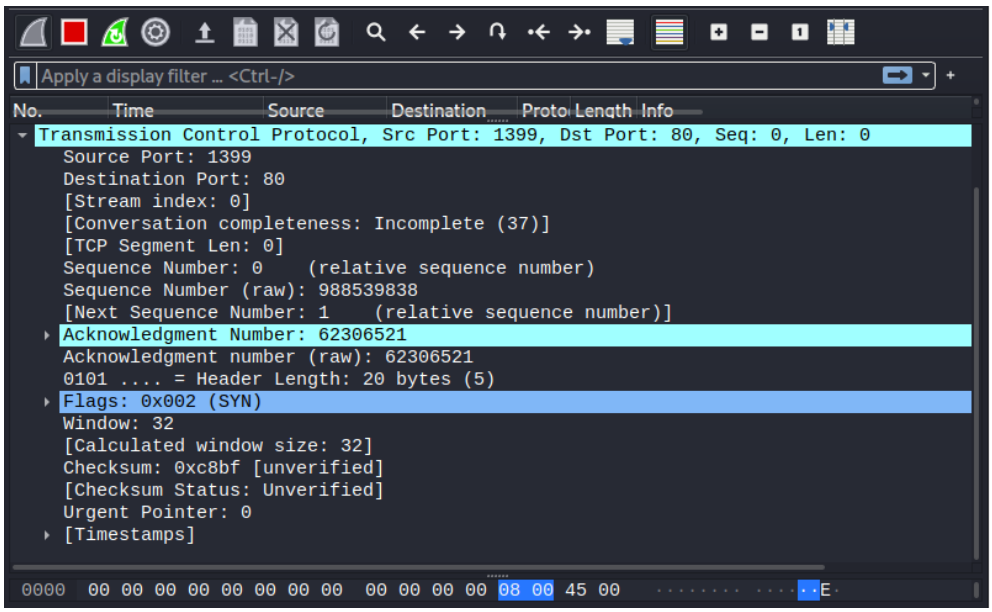
Screenshot of wireshark capture with details:



G.

a.

- Source IP: 127.0.0.1
- Destination IP: 127.0.0.1
- Protocol field: TCP (6)
- Total length: 40
- Header checksum: 0x3cce



b.

- Source port: 28274
- Destination port: 80
- Flags set: 0x002 (SYN)
- Window size: 32

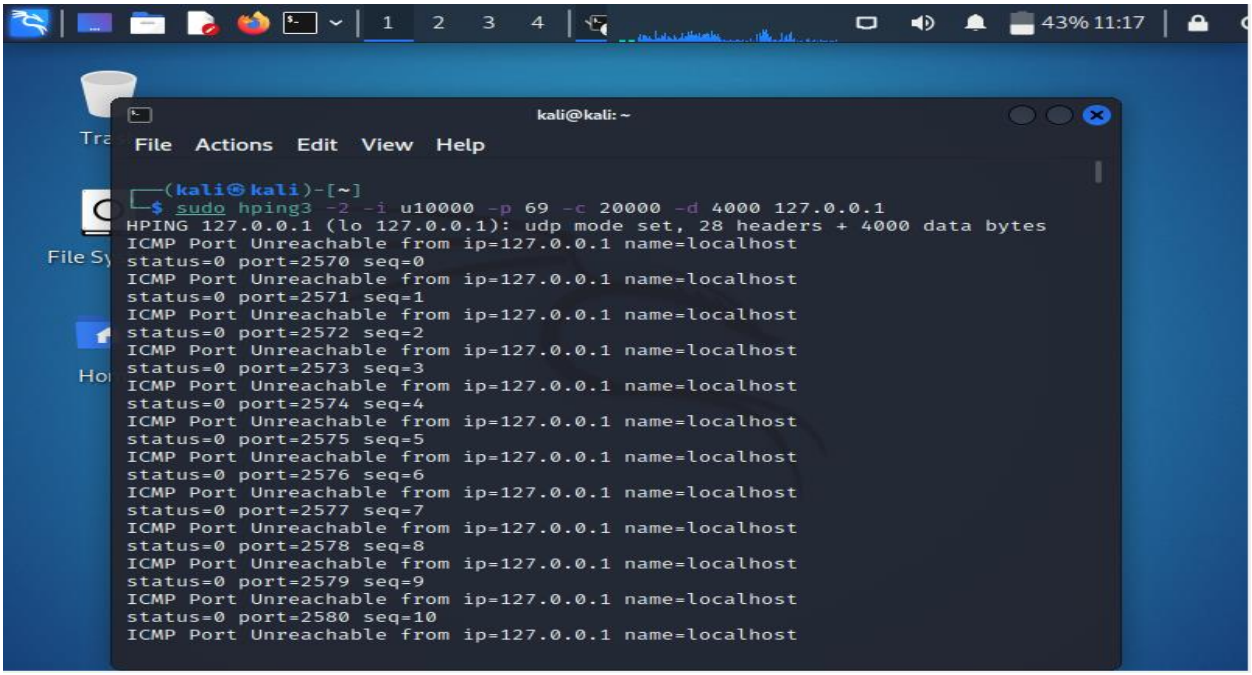
c. the clear difference that I observe from top command during the attack are as follows

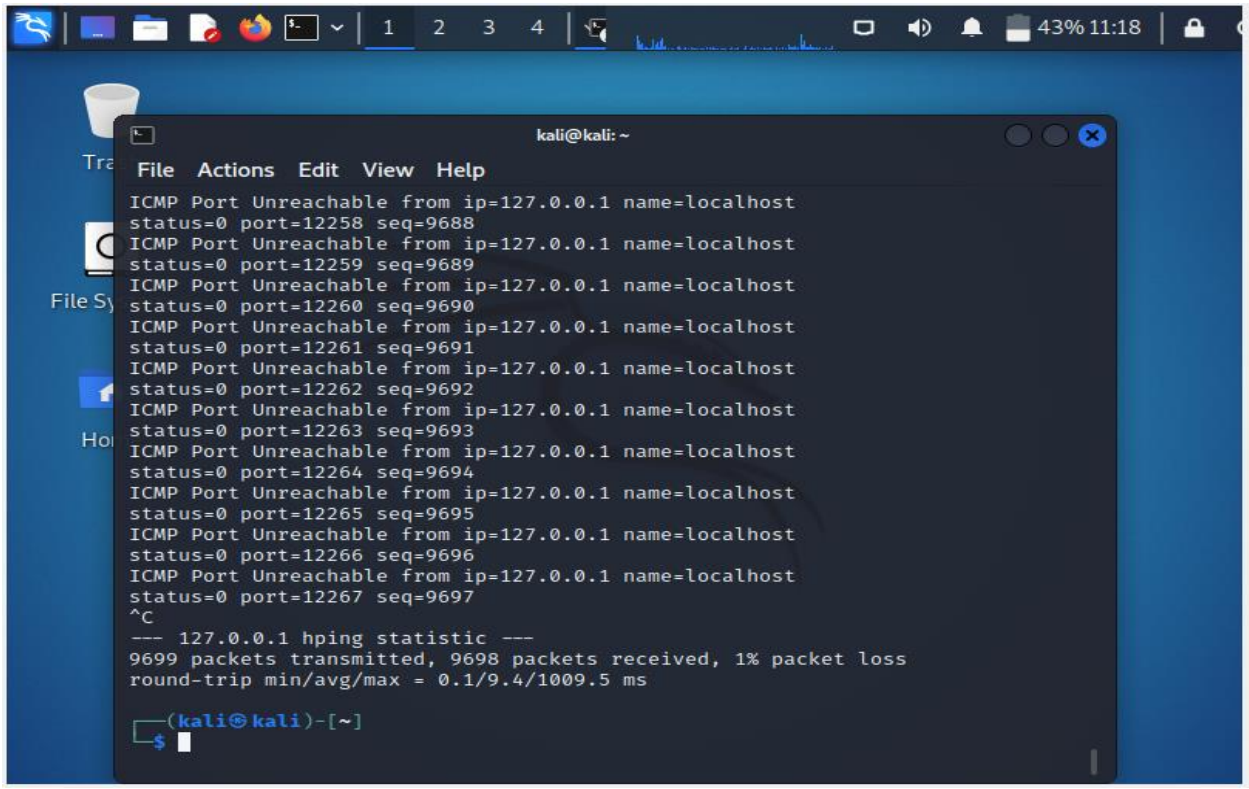
- CPU utilization is maximum that is almost close to 98% during the attack where as just 2 % before it
- Memory utilization by Hping3 command is same there is no significant difference in that.

Experiment 2: Simulation of a UDP Flood DoS attack

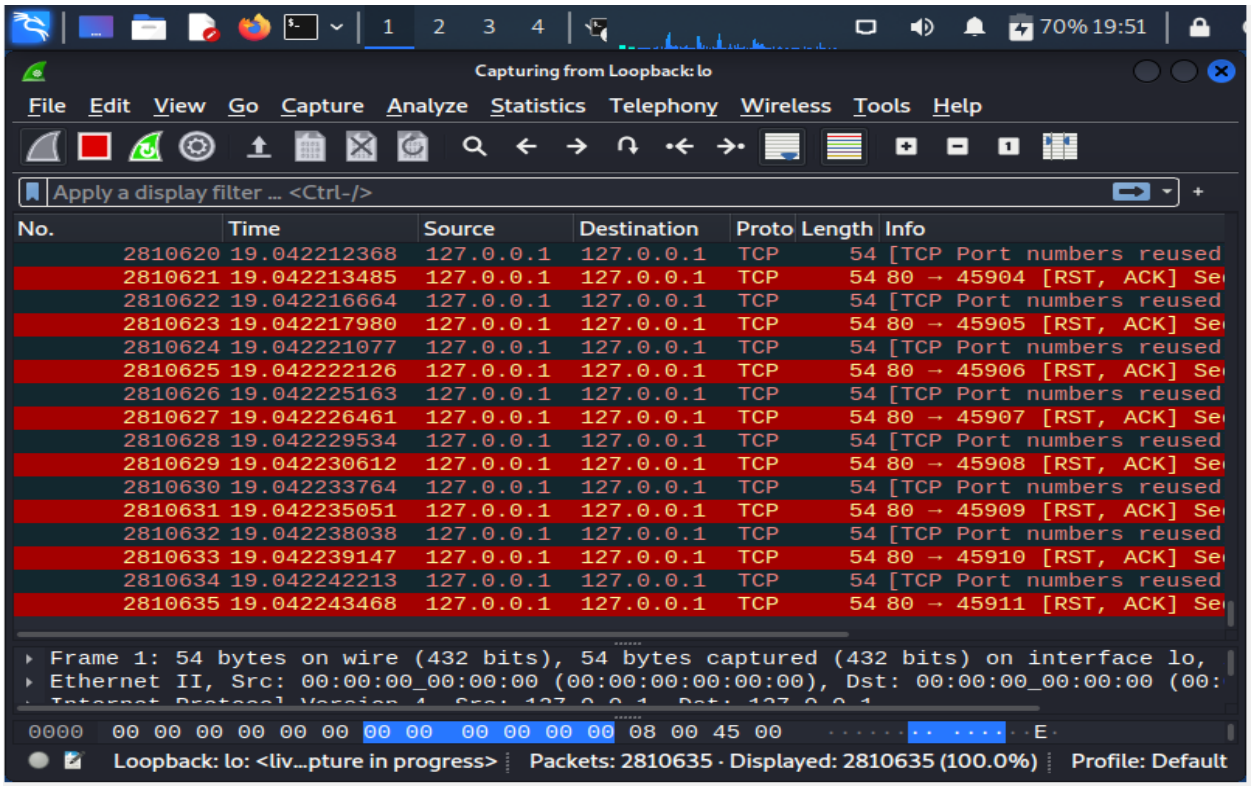
Command: sudo hping3 -2 -I u10000 -p 69 -c 20000 -d 4000 127.0.0.1

Screenshot of hping3 command terminal:

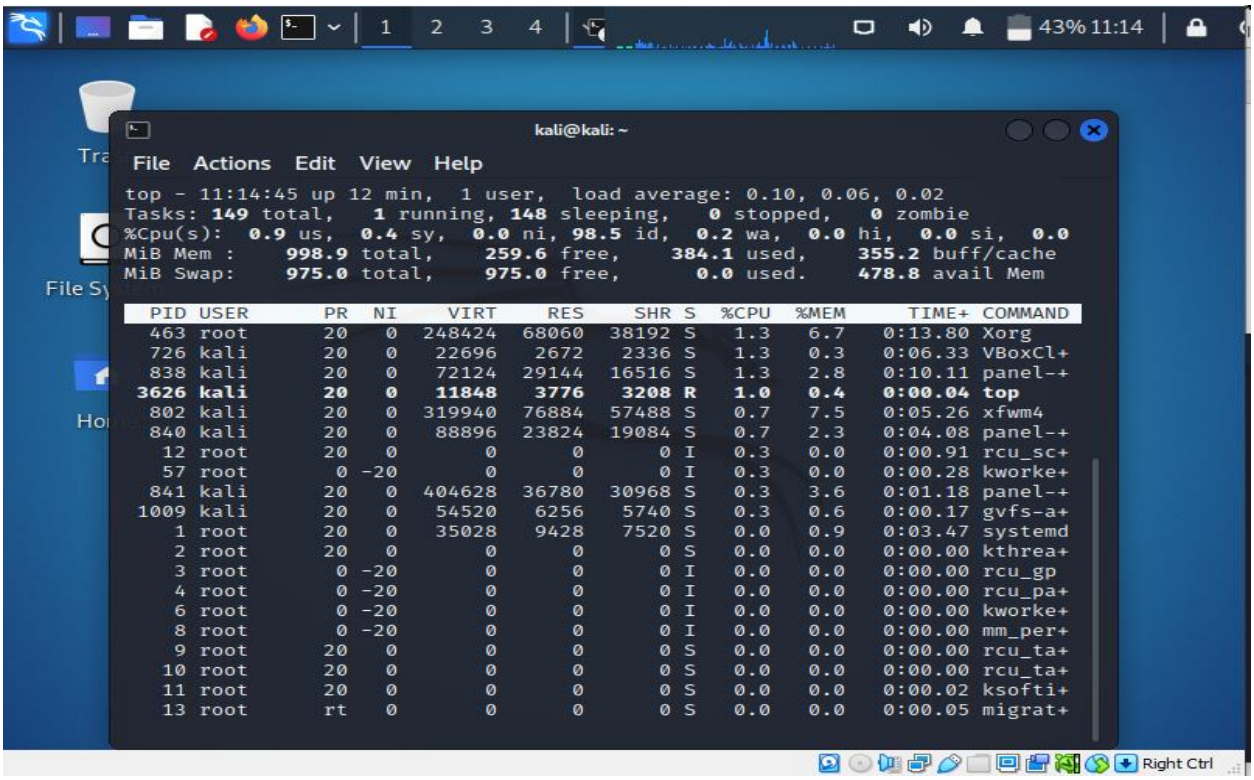




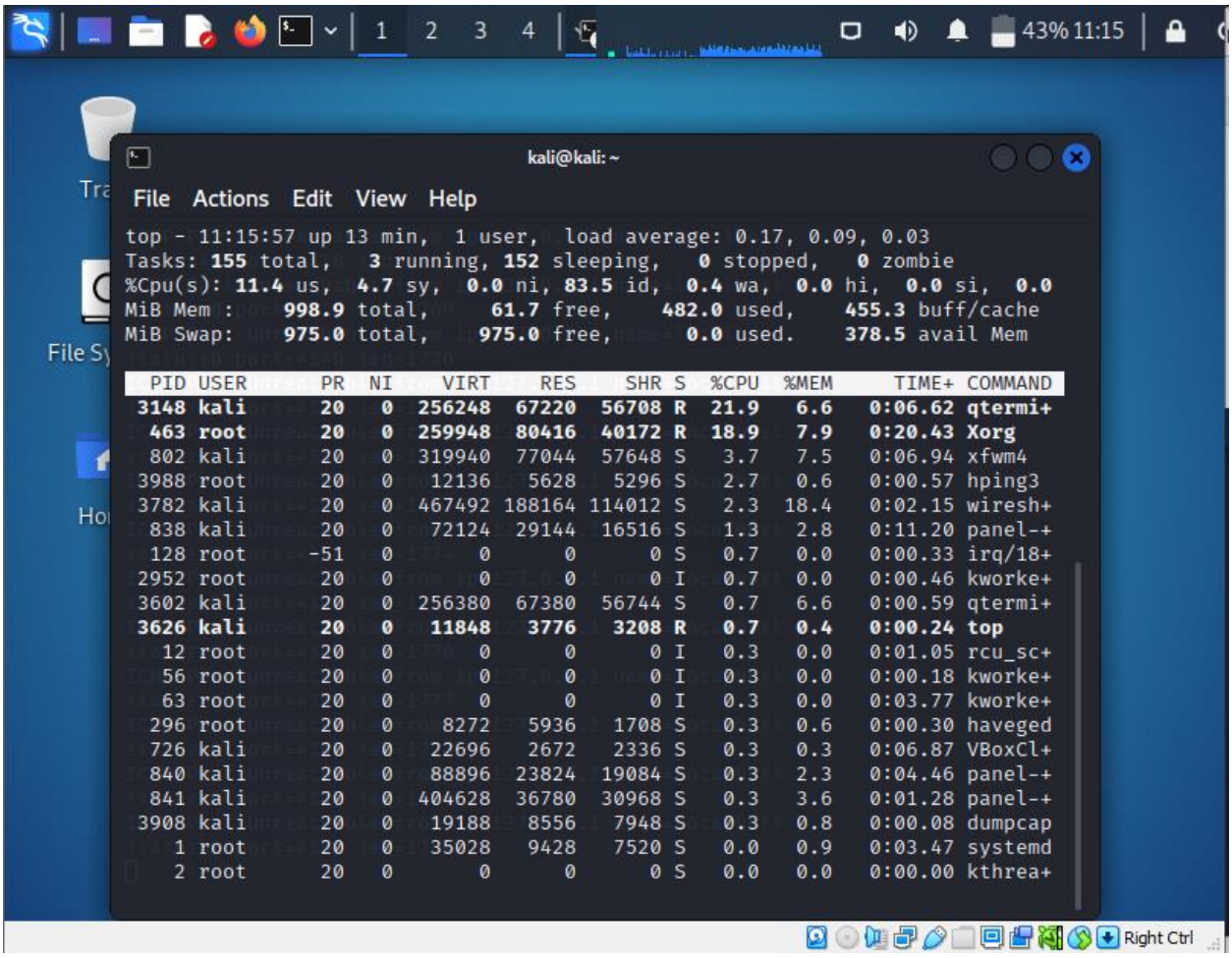
Screenshot of wireshard capture:



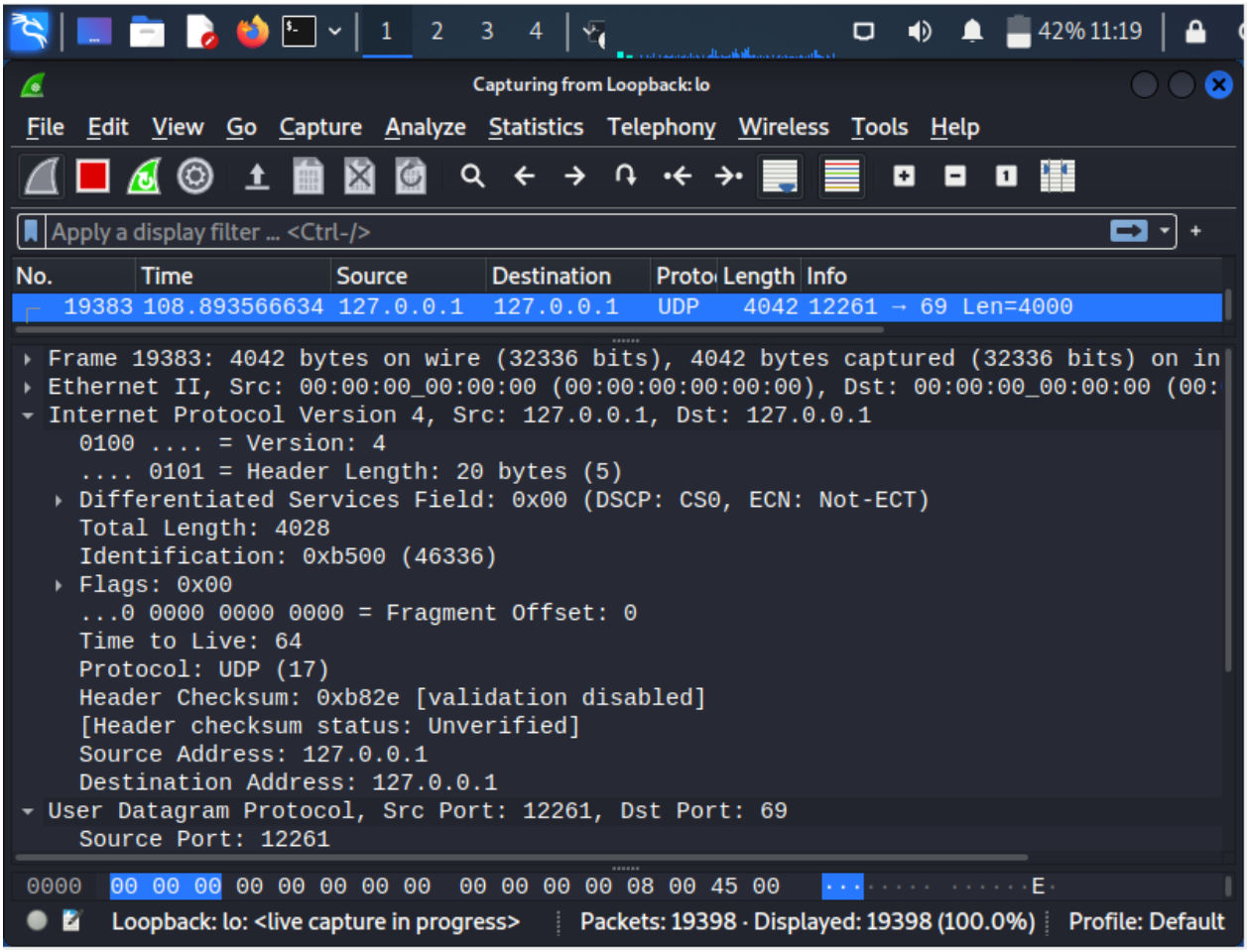
Screenshot of top command before attack:



Screenshot of top command during attack:

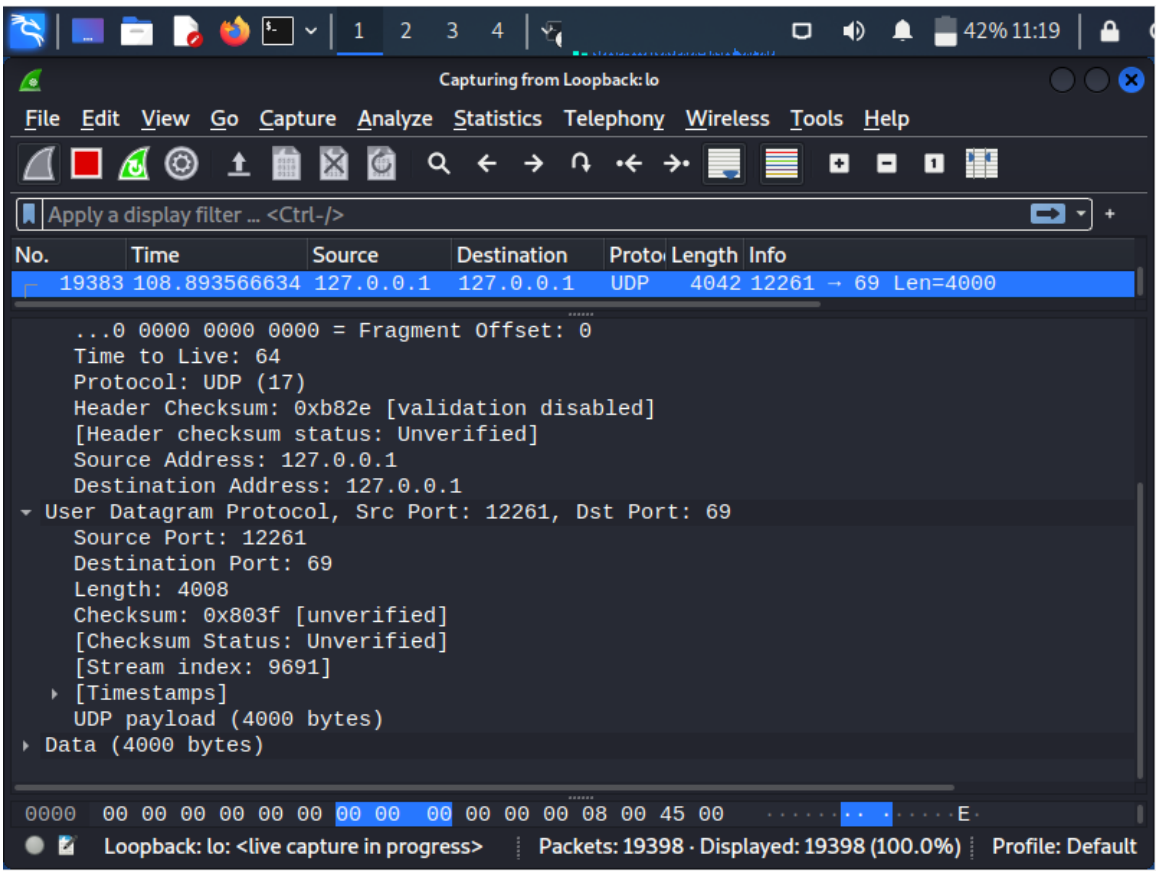


G.



a.

- Source IP: 127.0.0.1
- Destination IP: 127.0.0.1
- Protocol field: UDP (17)
- Total length: 4028
- Header checksum: 0xb82e



b.

- Source port: 12261
- Destination port: 69
- Head checksum: 0x803f

c. As we are just sending 100 requests per seconds we don't see any significant difference in top command during attack. Following at the slight differences that I see.

- CPU utilization is increased but not to the extremes, jump of 20-40% can be observed in utilization.
- Memory utilization by Hping3 command is same there is no significant difference in that, the only thing is wireshark is consuming more memory for recording the data.