1. Explain the exercise
2. Describe `setup.sh` script -> installing the utility and disable `tcp cookies`
3. Start the attack
4. Explain `start_attack.sh` script. -> output: `filter.pcap` file
5. Explain `wirefish.py`, it use the cliente source port to identify a connection.
6. SCP the file or use the one in the folder

```
scp otech2ak@users.deterlab.net:filter.pcap .
```

7. Show the loss of the package
8. Explain `tcp cookies` and how the mitigate the attack
9. Show the filtering with TCP cookies

10. EXTRA 1
11. Removing the spoofing, the attack will not work anymore because the attacker will receive the SYN+ACK message
12. Show filtering with RST
13. How to perform this attack anyway -> drop RST packet
14. Show filtering withot RST
15. How to mitigate the attack -> Drop packets coming from the attacker

16. EXTRA 2
17. Show new `conf.ns`
18. Explain why the attack don't work anymore -> no way to determine where to send the SYN+ACK message