IN3210/IN4210 - Exercise 6

Part 1 (TCP/IP Tools)

Use the SEED VM (or any other Linux) for the following tasks

- Start
  ```
  sudo tcpdump -n
  ```
  and create a TCP connection, e.g. with
  ```
  telnet uio.no 80
  ```
  Identify the TCP 3-way handshake.
- Use the tools `ifconfig` and `route -n` to identify the hosts current subnetwork. What is the network address? What is the maximum number of hosts in this subnetwork?
- Use
  ```
  netstat -ant
  ```
  to see all TCP sockets. Which services are running on the machine? With
  ```
  sudo netstat -antp
  ```
  you can even see the processes that have created the sockets.
- You can use the netcat tool to create a simple TCP server, e.g.:
  ```
  nc -l -p 9000
  ```
  and connect with a client, e.g.:
  ```
  nc localhost 9000
  ```
  If you type text in the console it will be send over the TPC connection. Use the netstat tool to observe the created sockets, also before connecting the client to the server and after the connection was terminated.

Part 2 (TCP/IP attacks)

This exercise is based on the SEED TCP/IP attack lab:
https://seedsecuritylabs.org/Labs_16.04/PDF/TCP_Attacks.pdf

You need to clone your virtual machine in order have three virtual machines connected in a network to perform this exercise. You may refer to this document for instructions on how to do this:
https://seedsecuritylabs.org/Labs_16.04/Documents/SEEDVM_VirtualBoxManual.pdf

Perform the following tasks:

- 3.1 Task 1: SYN Flooding Attack
- 3.2 Task 2: TCP RST Attacks on telnet and ssh Connections
  - Just use the tool Networx
  - Instead of attacking a telnet or ssh connection, you can use a TCP connection created with netcat (see part 1)
- 3.5 Task 5: Creating Reverse Shell using TCP Session Hijacking