

### SADS 2021 Problem Sheet #5

This sheet introduces you to some basic tools for penetration testing. Penetration testing is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. The test is performed to identify weaknesses and any issues uncovered should be reported to the system owner.

**Do not use penetration testing tools against systems that you have not been authorized to test. Doing so may be an illegal act. As a student of Jacobs University, you may want to read the documents you signed when you enrolled to understand consequences of misuse of our technical infrastructure.**

Download the VirtualBox image linked to the course web page and run it. To run the image, you need VirtualBox and the VirtualBox Extension Pack. Within VirtualBox, you need to have the HostNetwork vboxnet0 enabled (if missing, goto `File -> Host Network Manager...` and click `Create`). If all goes well, you should be able to start the virtual machine and reach it at the IPv4 address 192.168.56.2.

**Problem 5.1:** *network exploration and port scanning (nmap)* (1+1+1+1+2+1 = 7 points)

Install the tool `nmap` on your host system (not the virtual machine) and answer the following questions. Send us a transcript of your shell commands. (Hint: The `script` command can be used to produce a typescript of shell commands.)

- a) Run an `nmap` command to find active IP addresses in 192.168.56.2/24.
- b) Run an `nmap` command to find listening (open) TCP ports in 192.168.56.2/24.
- c) Run an `nmap` command to retrieve the date of HTTP servers running on 192.168.56.2/24.
- d) Run an `nmap` command to determine which version of SSH is running on 192.168.56.2.
- e) Run an `nmap` command to determine which authentication methods and cryptographic algorithms SSH running on 192.168.56.2 supports.
- f) Explain the decoy mode of `nmap`.

**Problem 5.2:** *moodle strangeness* (1+1+1 = 3 points)

Visit the Moodle page for this assignment. You may experience something unusual. If not, try some different web browsers.

- a) Explain what you have observed.
- b) Explain the code causing the behaviour you have observed.
- c) Discuss the possible impact of this vulnerability.