Secure and Dependable Systems
Jacobs University Bremen
Dr. Jürgen Schönwälder

Course: CO21-320203
Date: 2020-04-23
Due: 2020-04-30

SADS 2020 Problem Sheet #9

This sheet introduces you to some basic tools for penetration testing and ethical hacking. 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 9.1: *network exploration and port scanning (nmap)* (2+2 = 4 points)

Install the tool `nmap` 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) How many IP addresses are used in 192.168.56.2/24 and which TCP ports are open?

b) Which version of SSH is installed on 192.168.56.2?

Problem 9.2: *guessing passwords (hydra)* (2+2+2 = 6 points)

Install the tool `hydra` 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) Alice loves flowers. Find the password of Alice on 192.168.56.2.

b) Bob is lazy and he never uses passwords longer than his name. Find Bob's password on 192.168.56.2.

c) Find the password of the root user on 192.168.56.2.