Secure and Dependable Systems
Jacobs University Bremen
Dr. Jürgen Schönwälder

Module: CO-566
Date: 2022-03-10
Due: 2022-03-17

SADS 2022 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 192.168.56.2/26.

b) Run an `nmap` command to find listening (open) TCP ports in 192.168.56.2/26.

c) Run an `nmap` command to retrieve the date of HTTP servers running on 192.168.56.2/26.

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: *network exploration and port scanning (scapy)* (1+2 = 3 points)

Install the tool `scapy` on your host system. Scapy is a Python extension that enables you to send, sniff and dissect and forge network packets. It is a powerful tool for network exploration and penetration testing. Its strengths is flexibility, not necessarily speed.

a) Write a scapy script that performs a ICMP scan on the given IP prefix. Demonstrate that it works by running it against the virtual machine image. The script should generate lines in the following format:

```
$ sudo ./netscan.py 192.168.56.2/26
Received 262 packets, got 3 answers, remaining 61 packets
192.168.56.2        0        0        (alive)
192.168.56.4        0        0        (alive)
192.168.56.8        0        0        (alive)
```

The columns are separated by tab characters. The first column shows the IP address, the second column the ICMP type, the third column shows the ICMP code of the response packet, and the last column shows whether the host is alive or unreachable.

b) Write a scapy script that performs a TCP SYN scan on the port range 1..1024 on a given host. Demonstrate that it works by running it against the virtual machine image. The script should generate lines in the following format:

```
$ sudo ./synscan.py 192.168.56.2
Received 1633 packets, got 591 answers, remaining 433 packets
192.168.56.2    1       RA      (closed)
192.168.56.2    2       RA      (closed)
192.168.56.2    3       RA      (closed)
192.168.56.2    4       RA      (closed)
192.168.56.2    5       RA      (closed)
192.168.56.2    6       RA      (closed)
192.168.56.2    7       RA      (closed)
192.168.56.2    8       RA      (closed)
192.168.56.2    9       RA      (closed)
192.168.56.2    10      RA      (closed)
192.168.56.2    11      RA      (closed)
192.168.56.2    12      RA      (closed)
192.168.56.2    13      RA      (closed)
192.168.56.2    14      RA      (closed)
192.168.56.2    15      RA      (closed)
192.168.56.2    16      RA      (closed)
192.168.56.2    17      RA      (closed)
192.168.56.2    18      RA      (closed)
192.168.56.2    19      RA      (closed)
192.168.56.2    20      RA      (closed)
192.168.56.2    21      RA      (closed)
192.168.56.2    22      SA      (open)
```

The columns are separated by tab characters. The first column shows the IP address, the second column the port number, the third column shows the TCP flags of the response packet, and the last column shows whether the port is open or closed.