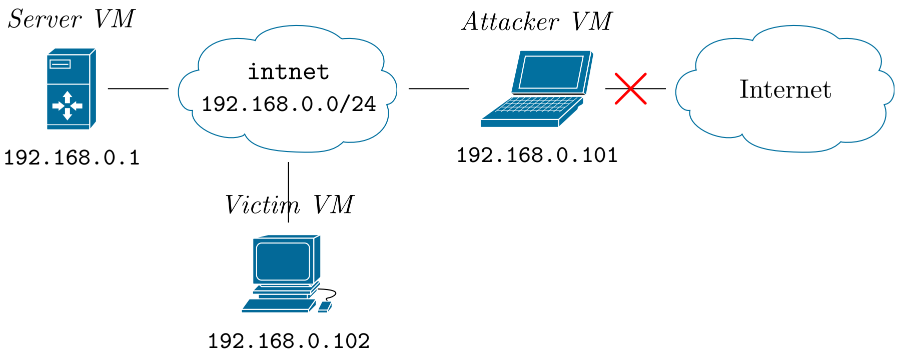
Exercises on Reconnaissance

Solve the following exercises and submit them until the communicated date.

LB-R 00.

a) Make sure that the *Server VM*, the *Attacker VM* and the *Victim VM* are configured properly as per the corresponding tutorials. This includes checking that they are interconnected as shown in the figure below. Document your verification steps.

b) Before beginning with any of the subsequent exercises, disconnect your host machine from the Internet. Verify thoroughly that you are in fact disconnected and document your steps. Your host machine **must not** be connected to the Internet at any time during the subsequent exercises unless explicitly instructed to do so.
Ensure that the *Server VM*, the *Attacker VM* and the *Victim VM* are all running at the same time (note that it is recommended **not** to boot all virtual machines within seconds of each other due to the simultaneous CPU and disk usage, which is likely to significantly slow down the boot processes as well as the host. Start the virtual machines one after another instead, i.e., start one machine only when the previous one has booted successfully). Except for the *Attacker VM*, no users should be logged in.



LB-R 01.

a) In the *Attacker VM*, use *Nmap* to scan the internal network between the virtual machines. Store the full console output in a file as you will need it for the following exercises. *Nmap* can be invoked by specifying a network address range in CIDR notation, e.g., `nmap 10.0.0.0/8`. For a more thorough analysis and detailed output, *Nmap* **must** be run with root privileges, i.e., it must be prefixed by the `sudo` command, and the *Nmap* options `-A` and `-v` must be used.

b) Based on the *Nmap* output from a), compile a list of discovered machines and addresses. You may use *Netdiscover* (usage: `netdiscover -r`, followed by the address range) for additional discovery. Like *Nmap*, *Netdiscover* **must** be run with root privileges. Based on all collected information, draw a network diagram from the *Attacker VM*'s perspective and compare it to the actual network topology.

c) Based on the *Nmap* output from a), compile a list of the most likely operating system for each discovered machine, including the operating system version and/or build number. Compare the guesses to the actual operating systems (including their version) running on the respective machines. On Linux, use the command `uname -a` to get the operating system version information. On Windows, use the `winver` command.

LB-R 02.

a) Shut all virtual machines down (**don't** just power them off! Otherwise, data will be lost and your virtual machines will get corrupted, requiring you to set them up again). You may now re-enable the Internet connection on your host machine as long as you do not start any of the programs from the previous exercises again.
Analyze the age of the operating system versions observed in exercise 01. a) and whether there are any severe security vulnerabilities known for each of them. If there are, list three of them and briefly describe their security implications.

b) Based on the *Nmap* output from exercise 01. a), compile a list of open ports and services for each of the machines. After having shut down all virtual machines, research what the purpose of each service is, which version of it is running (as far as this information is known) and whether any severe security vulnerabilities are known for it. Describe the security implications of the most severe vulnerability found for each machine.

c) Based on the vulnerabilities found in a) and b), summarize briefly which targets and attack vectors might be of interest for an attacker operating from the *Attacker VM*. For simplicity, assume that every vulnerability found is easily exploitable.