Leonard Marschke (leonard.marschke@hpi.de)

**Topic: Technical Reconnaissance**
**Maximum number of Points: 6**

Please be aware: Each action done inside the scenario or when interacting with it might be logged. These logs might get used for other purposes lateron.

Be aware: We do not disclose points for non-text tasks in this assignment. For flags you find on the systems (e.g. by attacking them) you will receive points. After you discovered a system (handed in the first flag), the Pruefungsamt will tell you how many points a system is worth (excluding undiscovered bonus flags) as well as how many flags a system contains (again without undiscovered bonus flags).

# Part I: Network Reconnaissance (6 P)

(6) 1. Give network scanning commands, which let you scan for all hosts in your range (IPv4 and IPv6, local and global) quickly (even though it might produce false negatives). Describe, which type of packets are sent and when the (host) detection does not work. Hand in your solution as flag `ex-6-scanning-command`.

2. Scan the whole network and create a network graph. The network graph should contain the following information:

    1. Networks (Network address, subnet mask, address configuration, gateways, DNS servers...)
    2. Hosts (IPs, name, OS, other metadata)
    3. Services of hosts (port and (guessed) service, versions)
    4. (Logical) networks
    5. Routers
    6. Bridges
    7. Switches
    8. Yourself & your machine
    9. Connections in the (local) network

    All available machines should be on the network plan. You should reflect the logical network structure.

    Prepare your network plan in a way that you can easily extend it later.

    Please be aware: As we might re-deploy parts of the scenario or the whole scenario, MAC addresses and SSH keys can change over time.

    At the time of writing this task, you should be able to see more than 25 different servers.

    We do not grade this task, but we will provide you with a sample solution after the deadline. Furthermore, we will discuss how all machines can be found in our exercise sessions. You will have to draw such a network plan in the practical exam to demonstrate that you are able to enumerate and scan networks like this one. If you need specific guidance on how to create the network plan feel free to drop us a mail or ask us in person during the tutoring sessions.

    VPN-Users be aware, that you might have a lossy link (packets get lost during transmission), so scan results might vary.

# Part II: Beginner attacks (0 P)

1. Find the Webserver that greets you. Check the server for interesting files. The interesting documents that you are looking for contain flags in our usual format. Check the Pruefungsamt on how many flags we planted there.

For this task, you might want to use a tool like `dirbuster` and/or `gobuster`. You do not need to download any wordlists but should use those distributed with you Kali.

You might note, how you found them (e.g. the command or the tool you used including it's parameters).

2. The same Webserver does hold another gift for you. Check the server for a git repository and download it's contents. Find the additional flag thats hidden on the server.

# Hints:

Hand in your solutions until 13th December 2023 11:59 p.m. online at `https://pruefungsamt.cip.institute`. All submissions have to be unique over different students. Be aware that handing in is only possible on site. You can hand-in each part at maximum 2 times.

Please answer questions that require a textual answer directly in the text field. You must use the markdown syntax. Please conform to this linter: `https://github.com/DavidAnson/markdownlint`. You can exclude the rules `MD013` and `MD026`.

If you need to hand in multiple files (and only then) please hand in `.tar.gz` archives without any unnecessary sub directories.

Please take note of the hand in requirements stated at the upload form (if there are any).

If you do not comply with the hand-in requirement we might subtract a few points from your submission.