**Network Security and Measurement** Assignment 04

HAW Hamburg WS 2023

Prof. Dr. Thomas Schmidt, Raphael Hiesgen, M.Sc. Deadline: November 22, 2023

1. **Active Scanning**

   Let's consider a thought experiment: You want to scan the complete IPv4 address space looking for open telnet (TCP/23) ports.

   (a) Which addresses can you ignore? Justify your answer.

   (b) ZMap implements an approach that does not require states for each request. Explain the approach and discuss advantages.

   (c) Your measurement host is not constrained in hardware in terms of memory. Do you still need to implement the ZMap approach discussed in (b) to achieve the same coverage?

   (d) How much memory would you need to maintain states for each potential reply? Make a lower bound estimate. Explain your answer.

2. **iNET Prefix Scan**

   Scan programs are used by security researchers and attackers to discover services running on remote hosts. Arbitrarily scanning networks is sometimes not received well. Since we have our own prefix available (`141.22.28.0/24`), we can target that freely.

   *Tools:* nmap, zmap, massscan, etc.

   (a) Take a look at the scan programs. How do they differ? Which one would you choose to scan our local /24 network, and why?

   (b) Perform the scan. Measure the time and collect the results.

   (c) Write a small report. Did you notice anything unexpected?

   Additional information: You should be able to run the scanning tools on mobi8 *without* `sudo`. Read the `--help` or the related man pages for details. In case you want (or need) to specify which interface to use for the scan, mobi8 has a public IP address from our prefix assigned to the interface `bond0`.

3. **Identify Scanners**

   We already looked at flow data in an earlier exercise. This time we analyze it with a purpose: find packets that look like scanning behavior.

   *Tools:* tshark, dpkt, scapy, pandas, matplotlib, ...

   *Data:* MAWI data is located in `shared-data/haw/mawi/2023`. Use the traces for November 1 that you are familiar with from the previous assignment.

   (a) What activity pattern would you expect from a scanner? Explain how you would identify them in flow data. Take vertical and horizontal scans into account.

   (b) Write a script to perform your identification. Collect the port and host destinations for each source. How big is the share of scanners among sources and packets?

   (c) Make a graph that places each source in a graph according to the number of targeted hosts (x-axis) and the number of targeted ports (y-axis). Highlight those sources you identified as scanners.