Probing devices services

A common task after identifying a target is to investigate its available services. In this lab, you will perform two different scans in order to get more information about the target. As in the previous hands-on, you will use the Nmap tool to discovery devices, now you will find the available services running on the devices previously detected. See the instructions below.

NMAP Scan

The quick scan will scan fewer ports than the default. Normally Nmap scans the most common 1000 ports for each scanned protocol. Using the scan type "Quick scan" the number of ports scanned is reduced to 100. Note, the target machine is the WIFI router IP address:

```
<TARGET_IP> = 192.168.1.1
```

Instructions:

- Open Zenmap
- Set the target IP
- Set the profile "Quick scan"

Observer the output and check if the scan was able to identify any service available on the target device. Next, run another scan using a different configuration:

- Open Zenmap
- Set the target IP
- Set the profile "Intense scan, all TCP ports"
- Edit the Command field and add the flag **-A**