# IPK Projekt 2 - Varianta OMEGA: Scanner síťových služeb


## Autor: Simon Kobyda, FIT VUTBR


# Špecifikácia

Program oskenuje zvovené porty, ktoré potom vyhodnotí na closed, open alebo filtered.

# Technické informácie

- **Programovací jazyk**: C
- **Použité sieťové knižnice**:

```
#include <pcap.h>
#include <netinet/tcp.h>
#include <netinet/ip.h>
#include <sys/socket.h>
```

```
#include <netinet/in.h>
#include <arpa/inet.h>
#include <netdb.h>
```

# Stručný popis lifecyklu programu (výcuc naštudovaných informácii):

- Program naparsuje vstupné argumenty, z ktorých zistí TCP a UDP porty, interface a cieľovú adresu. Ak je cieľová adresa zadaná pomocou názvu domény, tak tú prekonvertuje na IP adresu.
- Nájde sa prvý interface pomocou funkcie **pcap_lookupdev**. V prípade, ak je cieľová doména loopback, tak sa interface nastaví na **lo**
- Zistia sa bližšie informácie pomocou funkcie **pcap_lookupnet**
- Handler na odchytávanie packetov sa vytvorí pomocou **pcap_open_live**
- Vytvorí sa socket typu **SOCK_RAW**
- Pre každý port sa naplnía **hlavičky headerov** (napr. SIN, TCP, IP…)
- Vytvorí filterovací výraz na filtrovanie odchytených packetov. Ten sa skompiluje a nastaví (**pcap_compile pcap_setfilter**)
- Je odoslaný packet pomocou **sendto**
- Jednotlivé packety sa čítajú pomocou **pcap_next**, a podľa hodnoty ich flagov sa určite stav portu

# Testovanie:

Na testovanie programu sa využili open-source software: grafický nástroj Wireshark a konzolový nástroj nmap.
Na testovanie scannovania portov na vzdialenom serveri sa využil server doménz www.nemeckay.net.

# Návody a bibliografia:

Linux manual pages
https://www.security-portal.cz/clanky/jednoduchý-tcpudp-scanner-v-c
https://www.tcpdump.org/pcap.html
https://www.binarytides.com/raw-sockets-c-code-linux/