

# **IPK Projekt 2 - Varianta OMEGA: Scanner síťových služeb**

**Autor: Simon Kobyda, FIT VUTBR**



# Špecifikácia

Program oskenuje zvopené 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 informácií):

- 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 odchytyvanie packetov sa vytvorí pomocou **pcap\_open\_live**
- Vytvorí sa socket typu **SOCK\_RAW**
- Pre každý port sa naplnia **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](http://www.nemeckay.net).

## Návody a bibliografia:

Linux manual pages

<https://www.security-portal.cz/clanky/jednoduchy-tcpudp-scanner-v-c>

<https://www.tcpdump.org/pcap.html>

<https://www.binarytides.com/raw-sockets-c-code-linux/>