ZADÁNÍ:
1) Vytvořte jednoduchý síťový TCP, UDP skener v C/C++. Program oskenuje zadanou IP adresu a porty. Na standardní výstup vypíše, v jakém stavu se porty nacházejí (otevřený, filtrovaný, uzavřený) (13 b)
2) Vytvořte relevantní manuál/dokumentaci k projektu (7b)

UPŘESNĚNÍ ZADÁNÍ:

Ad 1)
Aplikace oskenuje zvolené porty na daném síťovém zařízení. Pakety musí být odeslané pomocí BSD sockets. Odchytávat odpovědi můžete např. pomocí knihovny libpcap.

TCP skenování:
Posílá pouze SYN pakety. Neprovádí tedy kompletní 3-way-handshake. Pokud přijde odpověď RST - port je označen jako uzavřený. Pokud po daný časový interval nepřijde ze skenovaného portu odpověď, je nutno ověřit dalším paketem a teprve potom port označit jako filtrovaný. Pokud na daném portu běží nějáká služba, je port označen jako otevřený. Více viz RFC 793.

UDP skenování:
U UDP skenování můžete uvažovat, že daný počítač při zavřeném portu odpoví ICMP zprávou typu 3, kódu 3 (port unreachable). Ostatní porty považujte za otevřené.

Volání programu:

```
./ipk-scan {-i <interface>} -pu <port-ranges> -pt <port-ranges> [<domain-name> | <IP-address>]
```

kde:

- -pt, pu port-ranges - skenované tcp/udp porty, povolený zápis např. -pt 22 nebo -pu 1-65535 nebo -pt 22,23,24
- domain-name | ip address - doménové jméno, nebo IP adresa skenovaného stroje
- -i eth0, kde argument představuje identifikátor rozhraní. Tento parametr je volitelný, v případě jeho nepřítomnosti se zvolí první IEEE 802 interface, který má přidělenou neloopbackovou IP adresu.

Příklad chování:

```
./ipk-scan -pt 21,22,143 -pu 53,67 localhost

Interesting ports on localhost (127.0.0.1):
PORT     STATE
21/tcp   closed
22/tcp   open
143/tcp  filtered
53/udp   closed
67/udp   open
```

Ad 2)
V dobré dokumentaci se OČEKÁVÁ následující: titulní strana, obsah, logické strukturování textu, výcuc relevantních informací z nastudované literatury, popis zajímavějších pasáží implementace, sekce o testování (ve které kromě vlastního programu otestujete nějaký obecně známý open-source nástroj), bibliografie, popisy k řešení bonusových zadání.

DOPORUČENÍ/OMEZENÍ:

- Programovací jazyk: C, C++, BSD sockets, libpcap
- Skenujte pouze počítače, které jsou ve Vašem vlastnictví (případně localhost).
- Pro vytvoření vlastních paketů, je potřeba root přístup. Lze programovat v laboratoři, vlastní instalaci FreeBSD, nebo virtuálním prostředí.
- Všechny implementované programy by měly být použitelné a řádně komentované. Pokud už přejímáte zdrojové kódy z různých tutoriálů či příkladů z Internetu (ne mezi sebou pod hrozbou ortelu disciplinární komise), tak je POVINNÉ správně vyznačit tyto sekce a jejich autory dle licenčních podmínek, kterými se distribuce daných zdrojových kódů řídí. V případě nedodržení bude na projekt nahlíženo jako na plagiát!
- U syntaxe vstupních voleb jednotlivým programům složené závorky {} znamenají, že volba je nepovinná (pokud není přítomna, tak se použije implicitní hodnota), oproti tomu [] znamená povinnou volbu. Přičemž pořadí jednotlivých voleb a jejich parametrů může být libovolné. Pro jejich snadné parsování se doporučuje použít funkci getopt().
- Výsledky vaší implementace by měly být co možná nejvíce multiplatformní mezi OS založenými na unixu, ovšem samotné přeložení projektu a funkčnost vaší aplikace budou testovány na referenčním Linux image (alternativní link http://jdem.cz/ez2je3) pro síťové předměty (přihlašovací údaje student / student).

ODEVZDÁNÍ:

Součástí projektu budou zdrojové soubory přeložitelné na referenčním operačním systému, funkční Makefile, soubor manual.pdf a Readme (viz obecné pokyny). Projekt odevzdejte jako jeden soubor xlogin00.tar, který vytvoříte programem tar.

LITERATURA:

- RFC 793 - Transmission Control Protocol
- RFC 791 - Internet Protocol
- RFC 768 - User Datagram Protocol
- HE RAW SOCKET PROGRAM EXAMPLES - https://www.tenouk.com/Module43a.html
- Port scanner - http://en.wikipedia.org/wiki/Port_scanner
- SYN skenování - https://nmap.org/book/synscan.html
- UDP skenování - http://nmap.org/nmap_doc.html#port_unreach

PATCH-NOTES:

- bude doplněno na základě případné diskuze na fóru
- 11.2. odstraněna překlepová věta z popisu dokumentace, přejmenovaná výsledná binárka na ipk-scan
- 22.3. opraveny linky referencí
- 29.3. doplněny informace k odevzdávaným souborům + aktualizován image referenční virtuálky.
- 9.4. přidán volitelný parametr -i specifikující rozhraní
- 16.4. Ethernet -> IEEE 802