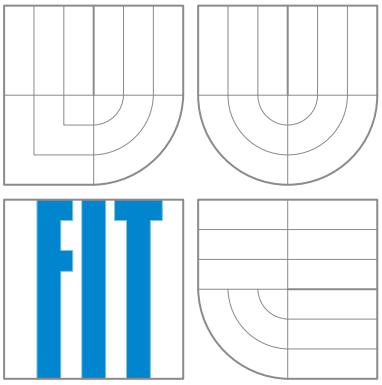

Prenos dát, počítačové siete a protokoly

Firewall

Autor: Bc. Tomáš Kubovčík, xkubov02@stud.fit.vutbr.cz

Fakulta Informačních Technologií
Vysoké Učení Technické v Brně

Zadanie

Cieľom tohto projektu bolo implementovať jednoduchý firewall pre operačný systém Linux, ktorý pozostáva z dvoch častí:

- **linuxový kernel modul** - samotný firewall
- **user space aplikácia** - jednoduchá aplikácia slúžiaca na obsluhu kernel modulu - pridávanie, mazanie pravidiel z modulu, pričom pri pridávaní pravidiel dochádza k syntaktickej analýze pravidiel

Podrobná špecifikácia projektu je dostupná v informačnom systéme v záložke **Projekt - Firewall**.

Popis implementácie

User space aplikácia

Táto aplikácia, ktorá komunikuje s kernel modulom prostredníctvom procfs bola implementovaná v jazyku Python, pričom pre syntaktickú analýzu pravidiel je tak isto použitý tento jazyk, najmä vďaka svojej jednoduchosti a efektívnosti.

Samotná aplikácia spĺňa požiadavky vyplývajúce zo zadania projektu, je však potrebné upresniť niekoľko podrobností implementácie. Pridávanie pravidiel do modulu prostredníctvom prepínača `-a` vyžaduje aby bolo pravidlo **uvedené v apostrofoch prípadne úvodzovkách ako parameter prepínača**:

```
./pdscli -a '10 deny ip from any to any'
```

prípadne

```
./pdscli -a "10 deny ip from any to any"
```

Ďalej je potrebné zmieniť správanie aplikácie pri načítavaní pravidiel zo súboru (prepínač `-f`). Pri jeho použití aplikácia podľa požiadavkov načíta pravidlá, pričom v prípade, že súbor obsahuje syntakticky nesprávne pravidlá sa do kernel modulu **uložia iba tie valídne** a **nevalídne sa vypíšu na štandardný výstup**.

Ak dojde k programu k chybe pri práci so súborom (otváranie neexistujúceho súboru/nedostatočné oprávnenia pre zápis/čítanie) program sa ukončí s chybovým kódom `1`. Ak vkladáme syntakticky nesprávne pravidlo, prípadne dojde k inej chybe, program skončí s kódom `2`. Drobným obmedzením môže byť rozsah/maximálna veľkosť ID/priority pravidiel, pretože pre **maximálnu veľkosť ID pravidla** sú vyhradené `4B`.

Rovnako je veľmi dôležité spomenúť, že pre zápis do `/proc` súboru **nie je** potrebné oprávnenie superusera (dekadický zápis oprávnení: `0666`).

Kernel modul

Ako východzia kostra pre implementáciu kernel modulu bola použitá odporúčaná kostra[1]. User space aplikácia teda komunikuje s kernel modulom prostredníctvom `procfs(/proc filesystem)`. Na základe [3] boli pre čítanie zo súboru využité **sekvenčné súbory**, a to najmä z dôvodu možného pretečenia `/proc` bufferu (pretečenie stránky). Mohlo by tak dochádzať k chybám pri výpise pravidiel obsiahnutých v kernel module, v prípade, že ich obsahuje veľký počet (stovky, tisícky, ...).

Pre uloženie pravidiel v kerneli module je použitý lineárne viazaný zoznam. Pri vkladaní pravidiel si modul overí či vkladané pravidlo nie je duplikátom už existujúceho pravidla. Ak je pravidlo duplicitou, znova sa nevkladá. V prípade, že sa vkladá rozdielne pravidlo s už existujúcim ID/prioritou existujúce pravidlo sa prepíše. Na ID pravidla sa hľadí ako na jeho prioritu a teda sa jednotlivé pravidlá podľa neho radia, pričom **nižšie číslo znamená vyššiu prioritu**. Pri vkladaní pravidiel zo súboru sa tieto pravidlá pridajú k už existujúcim - nepremazávajú sa, rovnako platí to čo už bolo uvedené (overovanie duplikátov, ...).

Filtrácia paketov je v module jednosmerná, filtrujú sa teda iba prichádzajúce pakety a odchádzajúcim modul nevenuje pozornosť. Samotné filtrovanie je postavené na spomínanej kostre[1] a materiáloch z predmetu ISA[2](napr. prednáška - Klasifikace paketů a filtrování dat).

Vývoj a testovanie

Kernel modul ako aj user space aplikácia boli vyvíjané pod operačným systémom Ubuntu (referenčný image `ISA2014`) a Elementary OS (ktorý je založený na ubuntu).

Literatúra

[1] Liu Feipeng. How to write a linux firewall in less than 1000 lines of code [online]. http://www.roman10.net/a-linux-firewall-using-netfilter-part-1overview/.

[2] Síťové aplikace a správa sítí [online]. https://www.fit.vutbr.cz/study/courses/index.php.cs?id=9391.

[3] The /proc file system [online]. http://wiki.tldp.org/lkmpg/en/content/ch05/2_6.