FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Počítačové komunikace a sítě - IPK

Manuál k projektu č. 2

2019 Juraj Holub (xholub40)

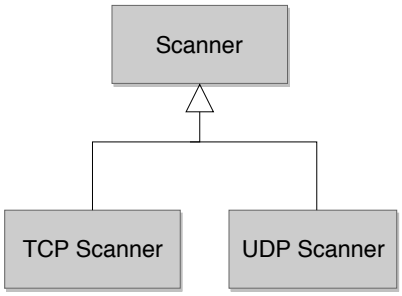
Obsah

1 Úvod

Port scan aplikácia je program, ktorý posiela klientské dotazy na rôzne porty hostujúceho serveru s cieľom nájsť aktívne porty. Takýto tip aplikácie môžu využívať administrátory s cieľom preverenia bezpečnosti ich siete. Predovšetkým je však tento tip aplikácie využívaný útočníkmi pre identifikovanie sieťovej služby a zistenie jej zraniteľnosti. Existuje veľa rôznych techník skenovania portov. Medzi najznámejšie patrí TCP SYN scan, TCP connect scan, UDP scan, SCTP INIT scan alebo napríklad TCP ACK scan. Táto aplikácia implementuje dve najznámejšie techniky: TCP SYN scan a UDP scan. [2]

2 Architektúra aplikácie

Program je implementovaný v jazyku C++11, využíva systémové knihovny pre vytváranie BSD socketov a prijíma odpovede pomocou knihovny libpcap . Program implementuje dve techniky skenovania, ktoré sa predovšetým líšia v transportnej vrstve. Objektová implementácia aplikácie je preto rozdelena na tri hlavné triedy:



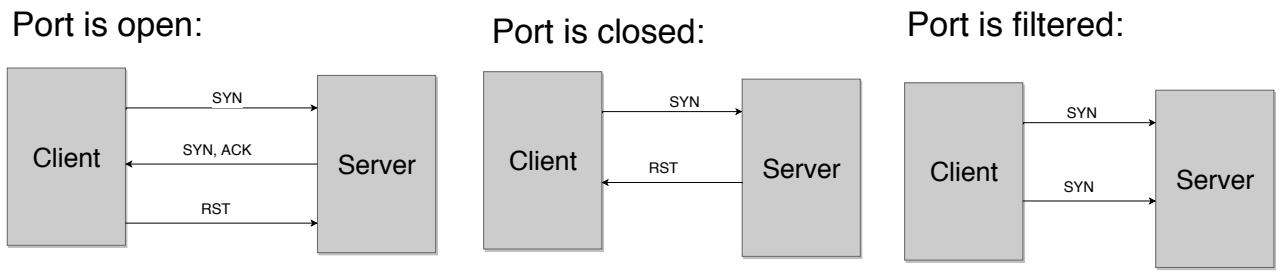
Obrázek 1: Scheme implemntácie aplikácie.

- **TCP Scanner**: Vytvorí a vyplní transportnú vrstvu TCP SYN raw packetom. Tento tip TCP packetu sa používa pre zahájenie spojenia pomocou 3-way handshaku. Následne sa zaháji spojenie zo skenovaným portom a na základe odpovede sa vyhodnocuje stav tohoto portu (viď. sekcia 3).
- **UDP Scanner**: Vytvorí a vyplní transportnú vrstvu UDP obálkov a pošle daný packet na skenovaný port. Následne sa čaká na odpoveď (viď. sekcia 4).
- **Scanner**: Oba tipy packetov používajú rovnakú sieťovú vrstvu, preto implementácia vytvárania IPv4 hlavičky zdieľajú obe podtriedy. Táto rodičovská trieda taktiež implementuje ďalšiu spoločnú funkcionalitu ako je výpočet kontrolného súčtu alebo získavanie IP adresy zariadenia na ktorom program beží.

3 TCP skenovanie

TCP SYN scan je najznámejší a najpopulárnejší spôsob skenovania portov. Ide o veľmy rýchly spôsob skenovania (nástroj nmap tvrdí, že dokáže skenovať rádovo tisícky portov za sekundu). Princíp skenovania využíva TCP 3-way-handshake pri naviazaní spojenia. Na začiatku klient zašle TCP packet z nastaveným SYN príznakom. [1] Na základe odpovede serveru môžeme port označiť ako:

- **Otvorený** v prípade, že server zašle späť TCP packet s nastavenými príznakmi SYN a ACK.
- **Zatvorený** v prípade, že server zašle späť TCP packet s nastaveným príznakom RST.
- **Filtrovaný** ak odpoveď zo serveru nepríde. V takomto prípade sa skúsi ešte raz zaslať SYN packet.



Obrázek 2: Princíp vyhodnotenia TCP SYN packet skenovania.

Implementovaný TCP scanner vytvára a zasiela SYN packet pomocou BSD socket knihovny a na odpoveď serveru využíva libpcap knihovnu. Libpcap knihovna umožnuje vytvorenie filtru, ktorý prijíma packety len z predom definovaného portu a IP adresy. Taktiež umožnuje nastavenie maximálnej doby čakania na packet čo je využívané pre rozpoznanie situácie, že packet sa stratil (bol odfiltorvaný sieťov).

4 UDP skenovanie

Na rozdiel od TCP SYN skenovania je UDP skenovanie portov všeobecne pomalšie a zložitejšie. UDP protokol nevytvára spojenie (connection-less). Otvorené porty potom nezasielajú spätnú informáciu na náš packet a ani zatvorené porty nemusia zasielať error packet. Avšak ak je packet zaslaný na zavrený port, tak väčšina hostov zasiela ICMP packet typu 3 s kódom 3 (Port unreachable). [1] Na základe tejto znalosti vyhodnocujeme skenované porty následovne:

- **Zatvorený** ak na náš UDP packet odpovedal host ICMP port unreachable packetom.
- **Otvorený** v opačnom prípade ale keďže nemáme žiadnu informáciu o tom či sa ICMP packet nestratil, tak skenovanie opakujeme viackrát.

5 Testovanie

Pre testovanie bola ako referenčný nástroj použitá open source utilita **nmap** . Pre overenie správnosti zasielaných packetov sa využil analyzátor sieťových protokolov **wireshark** . Príklad 5 ukazuje referenčný sken zvolených portov pomocou utility nmap. Naopak príklad 5 ukazuje sken portov pomocou tejto aplikácie. Výsledky skenovania sú zhodné ale za pozornosť stojí poukázať na fakt, že oba nástroje nedokázali pri skenovaní pomocou UDP packetov zistiť, že port 80 je otvorený.

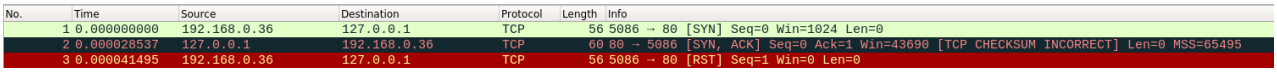
Listing 1: Príklad skenovania pomocou utility nmap.

```
user@pc:~$ sudo nmap -sU -sS -p25,80 localhost

Starting Nmap 7.60 ( https://nmap.org ) at 2019-04-12 14:01 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000026s latency).

PORT   STATE  SERVICE
25/tcp closed smtp
80/tcp open   http
25/udp closed smtp
80/udp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

Listing 2: Príklad skenovania portov touto aplikáciou.

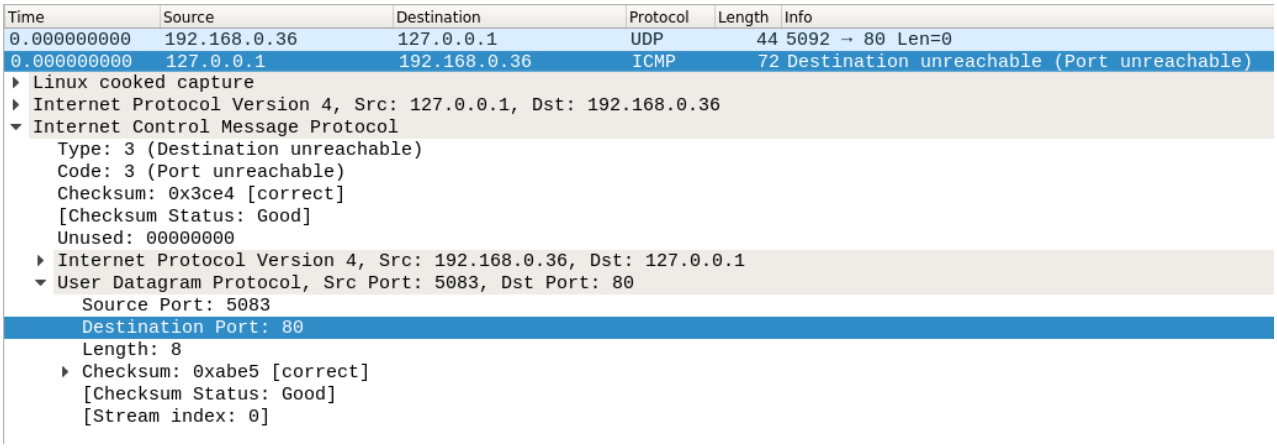
```
user@pc:~$ sudo ./ipk-scan -pt 25,80 -pu 25,80 localhost
PORT                STATE
25/tcp              closed
80/tcp              open
25/udp              closed
80/udp              closed
```

Obrázok 5 zobrazuje packety zasielané medzi klientom (port scanner) a skenovaným portom v prípade TCP SYN skenovania. Skenovaný port na SYN packet odpovedal TCP packetom s nastavenými príznakmy SYN a ACK a teda ho považujeme za otovorený.



Obrázek 3: TCP SYN scan portu 80.

Na obrázoku 5 je výsledok skenovania pomocou UDP packetu. Host zaslal ako odpoveď ICMP packet typu 3 s kódom 3 (Port unreachable) a preto port považujeme za zatvorený. V prípade, že by nebola žiadna ICMP zpráva prijatá, opakovalo by sa zaslanie UDP packetu ešte niekoľkokrát (implementovaná aplikácia by prípadne poslala požiadavok celkom 3-krát) a ak by nedošlo k ICMP odpovedi, port by sa označil za otvorený.



Obrázek 4: UDP scan portu 80 a následná odpoveď ICMP packetom (Port unreachable).

Reference

[1] Lyon, G. F. *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. 2009, ISBN 978-0-9799587-1-7.

[2] Shirey, R. RFC 2828 - Internet Security Glossary. [online], Poslední modifikace May 2000 [vid. 2019-12-04]. URL `https://tools.ietf.org/html/rfc2828#section-3`