Druhý projekt IPK

Scanner sieťových služieb - Varianta OMEGA

3.5.2020 Daniel Pohančaník

Implementácia

TCP Scanner

TCP scanner je implementovaný pomocou .NET knižnice TcpClient. Scanner sa najprv snaží nadviazať spojenie so serverom na danom porte. Ak sa pripojenie po spojenie podarí a príde acknowledgement správa tak je tento port registrovaný ako otvorený. Ak cieľový port spojenie ihneď odmietne, je považovaný za uzavretý. Ak do štyroch sekúnd nepríde odpoveď tak sa pokúša spojiť ešte raz. Ak sa to opäť nepodarí kvôli vypršaniu času na spojenie (štyri sekundy), tak je port označený za filtrovaný. Zamietnutie komunikácie cieľovým portom (uzavretý port) je odchytený pomocou výnimky ktorú vyhodí funkcia ConnectAsync() z knižnice TcpClient.

UDP Scanner

UDP sacnner požíva .NET knižnicu UdpClient. Funguje veľmi podobne ako TCP scanner. V prvom rade nadviažeme spojenie s portom pomocou funkcie Connect() s parametrom IPEndPoint, ktorý obsahuje informácie o porte aj o adrese. Následne za zakóduje a odošle jednoduchý string a čaká sa na odpoveď. Na odpoveď sa čaká tri sekundy. Ak do tej doby nepríde žiadna odpoveď tak port označíme za otvorený. Ak sa nejaká odpoveď vráti, čo je zvyčajne naznačené tým, že UdpClient vyhodí výnimku že spojenie bolo nasilu ukončené, tak sa port označí ako zatvorený.

Preklad adries

Preklad doménových názvov na IP adresy zabezpečuje .NET knižnica Dns a konkrétne jej funkcia GetHostAddresses(). V prípade, že má doménový názov nejaké aliasy (viac IP adries), tak je vybratá prvá vrátená adresa. Doménové meno „localhost“ je explicitne preložené na dresu 127.0.0.1. Aplikácia podporuje IPv4 aj IPv6 adresy.

Paralelizmus

Aplikácia podporuje viacvláknové skenovanie. Aplikácia vytvorí vlákna podľa počtu skenovaných portov pre UDP a TCP. Synchronizovanie vlákien nie je nijak riešené takže informácie o portoch sa objavujú na výstupe keď sú pripravené a tým pádom nemusia byť zoradené.

Poznámky k testovaniu

Aplikácia bola testovaná proti aplikácii nmap. Na testovanie bol použitý localhost (127.0.0.1) alebo server scanme.nmap.org. Pri testovaní s použitím localhost sa výsledky väčšinou zhodovali. Na servery scanme.nmap.org sa výsledky niekedy líšili hlavne počas skenovania UDP portov. Môj záver je, že aplikácia nmap dosahuje presnejšieho skenovania vďaka skenovaniu s využitím aplikačnej vrstvy pri niektorých portoch.