Manuál IPK projektu č.2 (2019/2020)

Autor: David Rubý

K implementaci tohoto projektu jsem použil programovací jazyk C# s knihovnou SharpPcap k zachycení veškerých příchozích i odchozích packetů.

Implementace

Po startu programu se rozparsují argumenty. Uloží se rozhraní, na kterém se má poslouchat, port, rozhodnutí, zda se má poslouchat na udp nebo tcp, počet packetů, které se mají zobrazit.

Dále se zjistí veškeré dostupné rozhraní daného zařízení a porovnají se s argumentem. Pokud zadané rozhraní není v seznamu dostupných rozhraní, nebo rozhraní nebylo zadáno uživatelem v argumentech, vypíší se veškerá dostupná rozhraní. Pokud rozhraní souhlasí, zvolí se toto rozhraní.

Vytvoří se `EVENT handeler` na tomto rozhraní, který spustí funkci `device_onPacketArrival`, která se postará o veškeré příchozí a odchozí packety. Rozhraní se otevře pro komunikaci a začne zachytávat packety.

Při zavolání funkce `device_onPacketArrival`, která se spustí při každém novém packetu se nejprve vyfiltrují IP adresy, porty, čas a data packetu. Dále se Ip adresy přeloží na `fqdn` (fully qualified domain name). Pokud překlad není možný, ponechá se IP adresa.

Při každém dokončení funkce se inktrementuje globální conter packetů a porovnává se s počtem packetů zadaných uživatelem. Pokud se vypíše dostatek packetů, program se ukončí.

Následně se vyfiltrují protokoly TCP a UDP. Pokud je specifikováno zachytávaní packetů na TCP a zachycení packet je TCP, pokračuje se dále, jinak se packet zahodí a aplikace čeká na další. To stejné platí pro UDP packety.

Pokud byl uživatelem specifikován port, zkontroluje se tento port s portem zdrojové a cílové aplikace tohoto packetu. Pokud zadaný port není shodný s aspoň jedním z těchto portů, packet se zahodí a čeká se na další packet. Pokud je port shodný s aspoň jedním z těchto portů, pokračuje se dále k výpisu.

Vypíše se čas packetu, výchozí IP adresa, výchozí port, IP adresa příjemce, port příjemce.

Data se převedou na String Hexadecimálních hodnot oddělených pomlčkou. Proto tento String rozdělím na pole hodnot. Ve smyčce si vytvářím String vždy po maximálně 16 hodnotách. Vypíšu velikost vypisovaného řetězce a samotný řetězec. Řětězec si převedu na ASCII zobrazení těchto hodnot a vypíšu je. Dále se pokračuje na další řádek, kde se provede to stejné a pokračuje, pro veškeré data packetu.

Funkce skončí a čeká se na další packet.