VUT FIT - ISA projekt
Přenos souboru skrz skrytý kanál

Václav Sysel (xsysel09)

15. listopadu 2021

Obsah

1 Úvod

Zadáním projektu bylo naprogramovat aplikace, která by za použití ICMP Echo-request/Response zpráv byla schopná přenést soubor po síti. Ač se tato probelmatik může zdát jednoduchou, pro mě samotného se ukázala velmi zajímavou, až náročnou. Jediný způsob, jak posílat data skrz tento způsobe je poslat packet ICMP Echo a jeho položku data naplnit vlastními. Toto působí mnoho zajímavých problémů, například velké omezení na velikost jednoho balíčku (65507 bytů). Taktéž takovýto packet nejde zachytit, nedá se registrovat port na kterém by bylo možné ho zachytávat, ale musí se pouze odposlouchávat. Systém sám na packety odpovídá. Toto působí mnoho problémů se kterými je potřeba se vypořádat.

2 Návod k použití

Program se pouští z příkazové řádky dodáním cesty k souboru, adresou na server a přepínačem na server. Neboli:
secret -r file -s ip/hostname [-l] [-o] [-v]
-r přijímá cestu k souboru, soubor nemusí být umístěn v adresáři s programem, program si soubor otevře, na straně serveru se soubor ukládá do adresáře s programem.
-s vyžaduje ip adresu či hostname k serveru, bohužel, pokud by adresou měl být samotný počítače, je potřeba použít taktéž přepínač -o, tímto se program přepne, aby odposlouchával na zařízení loopback.
-l je přepínač, který přepíná mezi serverem a clientem, pokud je nenastaven, program se zapne jako client a bude data odesílat, pokud je nastaven, program se zapne jako server a bude data přijímat. -v přepne program do "upovídaného"módu, program vypisuje na standartní výstup, jaké druhy paketů momentálně posílá přes ICMP

3 Návrh aplikace

Aplikace se zkládá z mnoha modulů a hlaviček. Nejdůležitější je zmínit moduly secret, client, server, networking.
Server je vcelku nenáročný soubor, který slouží jako výchozí brána ke všem ostatním souborům. Načítá vstupy od uživatele a přepíná do modulu client/-server.
Velmi zajímavé jsou ony moduly client/server. Jsou silně inspirovány stavovým automatem. Nachází se v různých stavech a přepínají se mezi nimi, přičemž během provádí různé úkony, jako odesílání dat, ukládání dat, odpověď atd. Tyto moduly jsou silně závislé na modulu networking, který obsahuje všechny nutné funkce pro odesílání a odposlech packetů.

4 Protokol

SECRET PROTOCOL
Nebo alespoň takový je pracovní název. Odesílá data souborů po bytech, společně s vlasntími generovanými hlavičkami. Hlavičky jsou jednoduché ASCII, které předesílají informace. Pro spuštení komunikace client odešle hlavičku:
SECRET_START\n
<name of file>\n
pro odesální dat client odešle:
SECRET_DATA\n
<number of bytes>\n
<DATA>
A pro zaslání posledních dat a ukončení komunikace klient zašle:
SECRET_END\n
<number of bytes>\n
<DATA>
Na všechny tyto "protokoly"klient odpovídá pomocí zaslání potvrzení či prosby o zopakování příkazu, tzv.:
SECRET_ACCEPT\n
SECRET_REPEAT\n

5 Omezení

Jelikož na využití 128 AES šifry, je školní login příliš krátký, tak jsem zbytek klíče vyplnil prázdnými byty, tzv. nulami.