SKJ Projekt: UDP port knocking

Wstęp

Na projekt składają się 2 aplikacje: klient i serwer realizujące autoryzację metodą „UDP port knocking". Należy najpierw uruchomić klasę Server a następnie Client. Oczywiście przed uruchomieniem trzeba wprowadzić odpowiednie argumenty programu.

Dla serwera będzie to lista portów(np. 1024 1025 1026).

Dla kilenta adres serwera i lista portów(np. 172.23.129.147 1024 1025 1026).

Działanie aplikacji:

[Serwer]: Nasłuchuje na określonych w tablicy argumentów portach na pakiety od wielu klientów.

[Client]: Otwiera port UDP, a następnie wysyła na adres serwera na porty podane w tablicy argumentów pakiety, a następnie czeka na odpowiedź serwera.

[Server]: Po otrzymaniu odpowiedniej sekwencji pakietów z jednego adresu IP otwiera wybrany przez system wolny port TCP, a następnie na adres zautoryzowanego klienta wysyła komunikat UDP z numerem otwartego portu.

[Client]: Po otrzymaniu odpowiedzi od serwera klient otwiera gniazdo TCP, wysyła krótkie zapytanie i oczekuje odpowiedzi.

[Server]: Po otrzymaniu zapytania TCP od klienta, wysyła odpowiedź oraz zamyka gniazdo oraz port TCP, i kontynuuje nasłuchiwanie na portach UDP.

[Client] Po otrzymaniu odpowiedzi TCP od serwera kończy pracę.

Działanie serwera

Po uruchomieniu serwer tworzy kolejne wątki klasy PortListener, które przyjmują jako argumenty kolejne porty podane w argumentach programu i zaczynają nasłuchiwać na tych portach. Jeśli port się powtarza, to nowy wątek nie jest tworzony.

Podczas nasłuchiwania serwer gromadzi dane o portach na które zostały wysłane pakiety z poszczególnych adresów IP w hashmapie (portsMap) współdzielonej przez wszystkie wątki PortListenera. Jeśli któryś klient wyśle pakiety na odpowiednią sekwencję portów, dostaje autoryzację od serwera, a historia portów jest usuwana. Otwierany jest wtedy wolny, wybierany automatycznie przez system port TCP, a następnie wysyłany jest komunikat UDP z numerem tego portu w stronę klienta.

Następnie serwer nasłuchuje na zapytanie TCP od klienta, po jego otrzymaniu wysyła odpowiedź TCP i kończy komunikację, po czym wraca do nasłuchiwania na portach UDP.

Działanie klienta

Proces klient otrzymuje w argumentach programu adres serwera oraz listę portów na które ma wysyłać pakiety. Po uruchomieniu nowego wątku klienta, wysyłane są na serwer na poszczególne porty pakiety UDP, a następnie klient nasłuchuje odpowiedzi od serwera. Jeśli w ciągu 10 sekund odpowiedź nie nadejdzie, klient kończy pracę z błędem. W przeciwnym wypadku klient wysyła zapytanie TCP na otrzymany port serwera i oczekuje na odpowiedź TCP. Po jej otrzymaniu kończy pracę.

Wykonał: Szymon Głowacki, s20872