Laboratorium sieci komputerowych - ćw. 1
Podstawy pracy na systemie z rodziny Linux

Krzysztof Dąbrowski gr. 3

7 marca 2019

Spis treści

1 Wstęp

Celem zajęć laboratoryjnych było zaznajomienie się z podstawami pracy i administracji systemów z rodziny Linux. Przed przystąpieniem do pracy należało opanować podstawowe pojęcia związanie z kryptografią asymetryczną oraz poznać wybrane programy narzędziowe zainstalowane na komputerach laboratoryjnych.

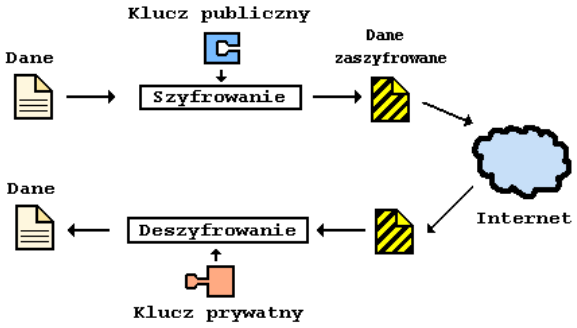
2 Kryptografia asymetryczna

Jest to część kryptografii, gdzie operacja szyfrowania i odszyfrowywania informacji znacząco się od siebie różnią.

2.1 Sposób działania

Algorytmy stosowane w kryptografii asymetrycznej pozwalają na wygenerowanie pary powiązanych ze sobą kluczy. Jedne z nich jedynie na szyfrowanie danych, a drugi na ich odszyfrowanie. Klucz szyfrujący jest też nazywany *publicznym* a odszyfrowujący *prywatnym*.

Dzięki zastosowaniu kluczny asymetrycznych możliwe jest bezpieczne przesłanie wiadomości miedzy stronami chcącymi się porozumieć.



Rysunek 1: Schemat transmisji danych

2.2 Zastosowanie

Dzięki wykorzystaniu kryptografii asymetrycznej możliwe jest nawiązanie połączenia z serwerem bez potrzeby przesyłania hasła. Przeprowadzenie uwierzytelnienia w ten sposób polega na zaszyfrowaniu przez serwer danych kluczem publicznym osoby chcącej się zalogować. Następnie serwer oczekuje na odesłanie odszyfrowanej danej. Ponieważ odszyfrowanie jest możliwe tylko przez posiadacza klucza prywatnego, to serwer jest w ten sposób w stanie potwierdzić autentyczność osoby logującej się.

Należy zwrócić uwagę, że podczas takiego procesu nie są przesyłane żadne wrażliwe dane. Jest on więc bezpieczny nawet w przypadku podsłuchania. W przeciwieństwie to tradycyjnego logowania.

2.3 Generowanie kluczy

Połączoną parę kluczy można wygenerować przy pomocy polecenia `ssh-keygen`. Przy domyślnch ustawieniach zostaną one zapisanie w katalogu `~/.ssh`.

2.4 Przekazanie klucza

Jedyną pozostałą czynnością jest przekazanie klucza publicznego do serwera, do którego planuje się logować. Można to łatwo osiągnąć przy pomocy polecenia `ssh-copy-id`.

Po wykonaniu tych czynności możliwe jest logowanie przez `ssh` bez podawania hasła.

3 Zarządzanie uprawnieniami administratorskimi

W systemach zazwyczaj nie pracuje się na koncie administratorskim. Zamiast tego powinno się korzystać ze standardowego konta. Gdy potrzebne są specjalne uprawnienia należy wykonać dane polecenie z użytkownikiem zmienionym na administratora (root).

3.1 Zmiana użytkownika

Do zmiany użytkownika wykorzystać można polecenie `su`.

Najczęściej jednak zachodzi potrzeba wykonania pojedynczego polecenia jako root. Służy do tego polecenie `sudo`. W przeciwieństwie do trwałej zmiany użytkownika po wywołaniu `sudo` użytkownik zostanie poproszony o podanie hasła do konta, z którego aktualnie korzysta, a nie z tego, jako które chce wykonać polecenie.

3.2 Dostęp do sudo

Decyzję o tym czy użytkownik może korzystać z polecenia `sudo` system podejmuje na podstawie informacji zawartych w pliku `/etc/sudoers`. Zawiera on listę grup i użytkowników, którzy mają taką możliwość.

Plik ten może posiadać nawiązania do wybranych katalogów. W takiej sytuacji do podjęcia decyzji o dostępie do `sudo` brane są pod uwagę również wszystkie pliki znajdujące się we wskazanym katalogu.

4 Blokowanie zdalnego dostępu do komputera