

Laboratorium sieci komputerowych - ćw. 1

Podstawy pracy na systemie z rodziny Linux

Krzysztof Dąbrowski gr. 3

5 marca 2019

Spis treści

1	Wstęp	2
2	Kryptografia asymetryczna	2
2.1	Sposób działania	2
2.2	Zastosowanie	2
2.3	Generowanie kluczy	3
2.4	Przekazanie klucza	3
3	Zarządzanie uprawnieniami administratorskimi	3
4	Blokowanie zdalnego dostępu do komputera	3

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 związane z kryptografią asymetryczną oraz poznać wybrane programy narzędziowe zainstalowane na komputerach laboratoryjnych.

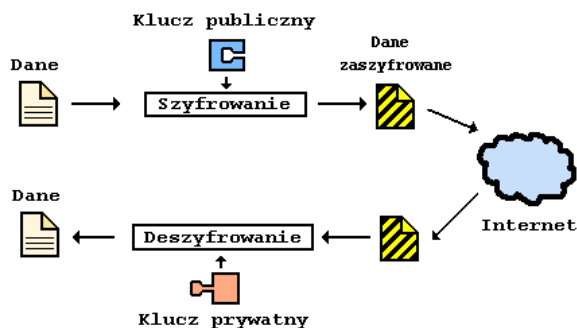
2 Kryptografia asymetryczna

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 kluczy asymetrycznych możliwe jest bezpieczne przesłanie wiadomości między 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 tego procesu nie były przesyłane żadne wrażliwe dane. Jest on więc bezpieczny nawet w przypadku podsłuchania.

2.3 Generowanie kluczy

Połączoną parę kluczy można wygenerować przy pomocy polecenia `ssh-keygen`. Przy domyślnych ustawieniach zostaną one zapisane 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

4 Blokowanie zdalnego dostępu do komputera