|  |  |
| --- | --- |
| Bezpieczeństwo Sieci Komputerowych | Data: 28.04.2016r. |
| Ćwiczenie nr 4  Autorzy: **Maciej Sawicki**  **Michał Kruszewski** | Prowadzący:  Dr Inż. Maciej Brzozowski |

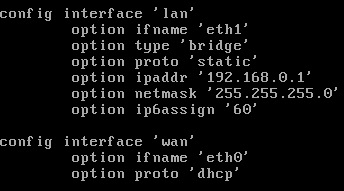
Zadanie 1.

Skonfiguruj dwie maszyny wirtualne OpenWrt w VirtualBox’ie zgodnie ze schematem powyżej. Sprawdź czy obie maszyny wirtualne mają dostęp do internetu.

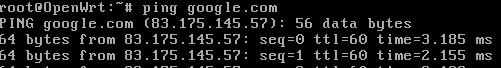
Opis interfejsów:

* Eth0 – wan (NAT), dhcp
* Eth1 – lan (Internal), static, 192.168.0.1/24

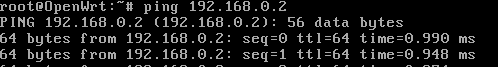
OpenWrt1 – klient (192.168.0.1)



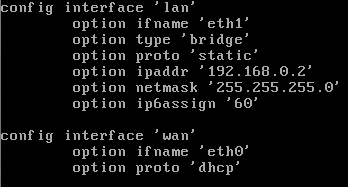
ping gogle.com



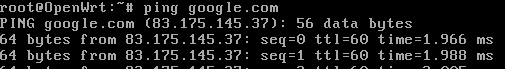
ping 192.168.0.2 (pingowanie serwera)



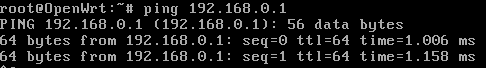
OpenWrt2 – serwer (192.168.0.2)



ping gogle.com



ping 192.168.0.1 (pingowanie klienta)

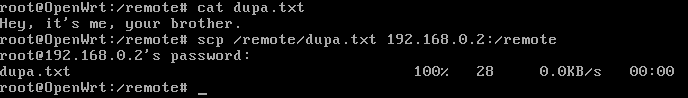


Zadanie 2.

Skopiować wybrany plik z lokalnego katalogu na zdalny serwer za pomocą polecenia *scp*. Pobrać plik ze zdalnego serwera.

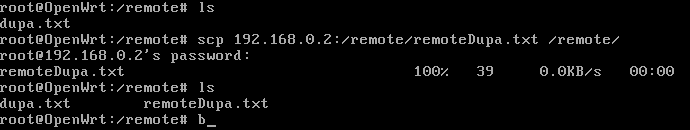
Skopiowano plik na zdalny serwer za pomocą polecenia:

scp /remote/dupa.txt 192.168.0.2:/remote



Pobrano plik ze zdalnego serwera za pomocą polecenia:

scp 192.168.0.2:/remote/remoteDupa.txt /remote/



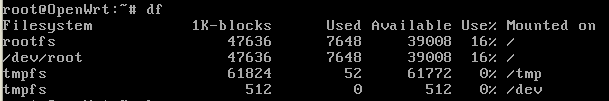
Zadanie 3.

Uruchomić dowolne polecenie na serwerze za pomocą *ssh*, np. sprawdzić ilość wolnego miejsca na dysku, albo wylistować zawartość wybranego katalogu.

Połączenie używając protokołu *ssh* za pomocą polecenia:

ssh 192.168.0.2



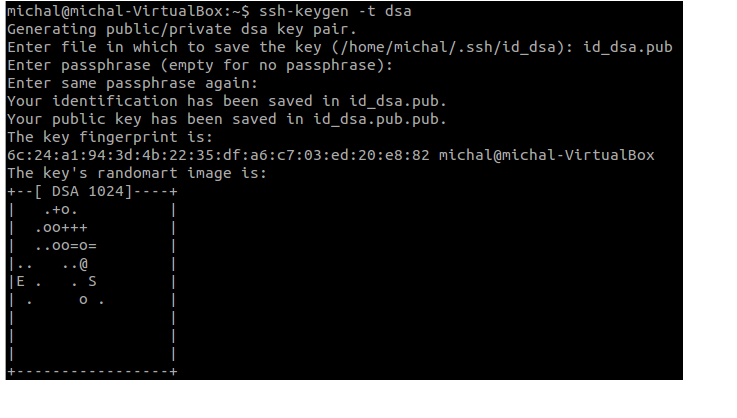


Zadanie 4.

Skonfigurować serwer ssh, aby umożliwiał autentykację wybranych użytkowników za pomocą klucza publicznego (pierwszy użytkownik z kluczem na hasło, drugi bez hasła).

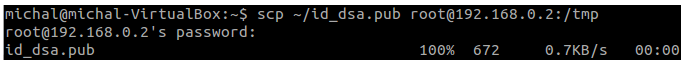
Utworzenie klucza publicznego w systemie linux:

ssh-keygen –t dsa



Przeniesienie utworzonego klucza na serwer:

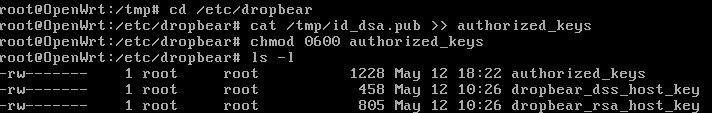
scp ~/.ssh/id\_dsa.pub root@192.168.0.2:/tmp



Dodanie klucza użytkownika (z przeniesionego uprzednio pliku do „bazy kluczy” na serwerze – pliku authorized\_keys), oraz ustawienie praw do zapisu i odczytu.

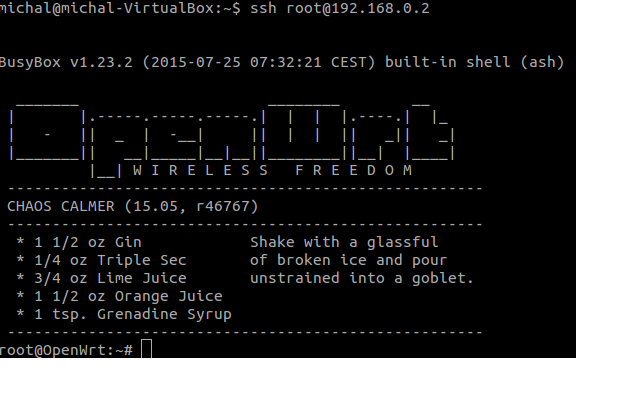
cat /tmp/id\_dsa.pub >> authorized\_keys

chmod 0600 authorized\_keys

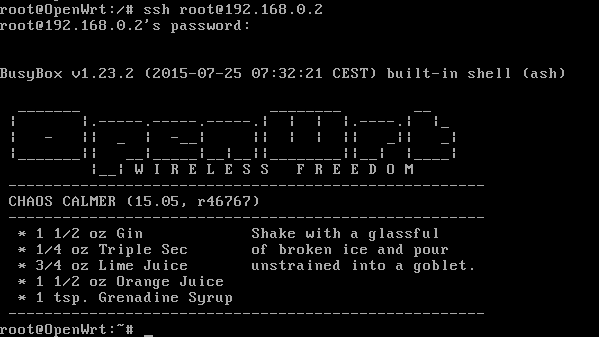


Połączenie z serwerem z poziomu linuksa, na podstawie klucza publicznego. Połączenie nie wymaga hasła.

ssh root@192.168.0.2



Połączenie ze strony drugiego klienta, z wymaganym hasłem.



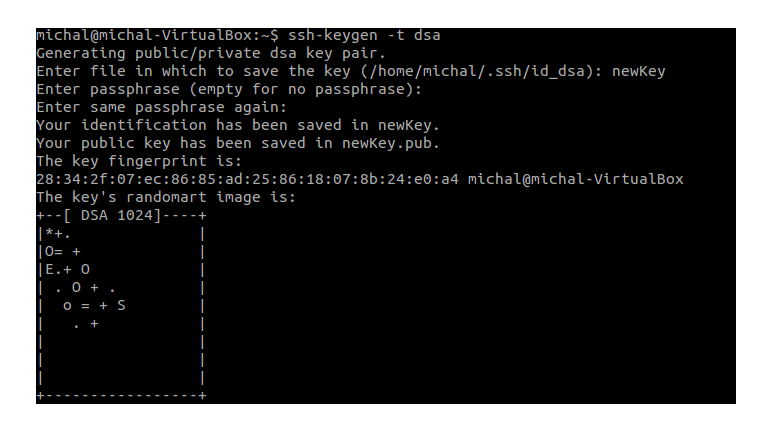
Zadanie 5.

Wygenerować na serwerze SSH nowe klucze. Sprawdzić, czy połączenie będzie możliwe. Zaktualizować klucze po stronie klienta, aby połączenie było możliwe.

Wygenerowanie nowego klucza do oddzielnego pliku oraz przeniesienie na serwer.

ssh-keygen it dsa

scp ~/newKey.pub root@192.168.0.2:/tmp



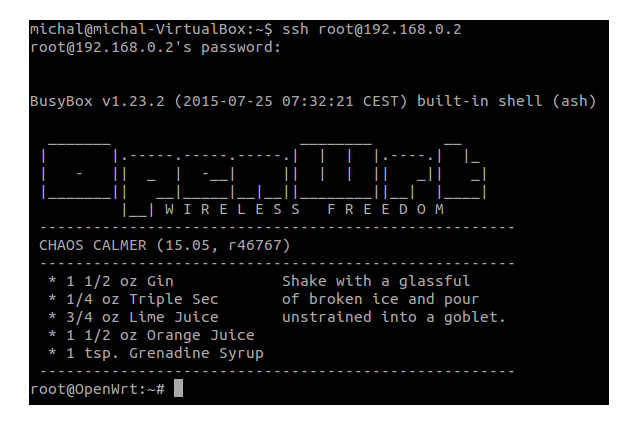
C:\Users\Michal\Downloads\documents-export-2016-05-12\copying newKey to openWRT.png

Zamiana kluczy po stronie serwera – przeniesienie zawartości newKey.pub do authorized\_keys (poprzez nadpisanie danych).

cat /tmp/newKey.pub > authorized\_keys



Próba połączenia klienta z serwerem.



Przeniesienie klucza używanego na serwerze do folderu ~/.ssh, a następnie ponowne łączenie z serwerem.

mv newKey ~/.ssh

mv newKey.pub ~/.ssh

