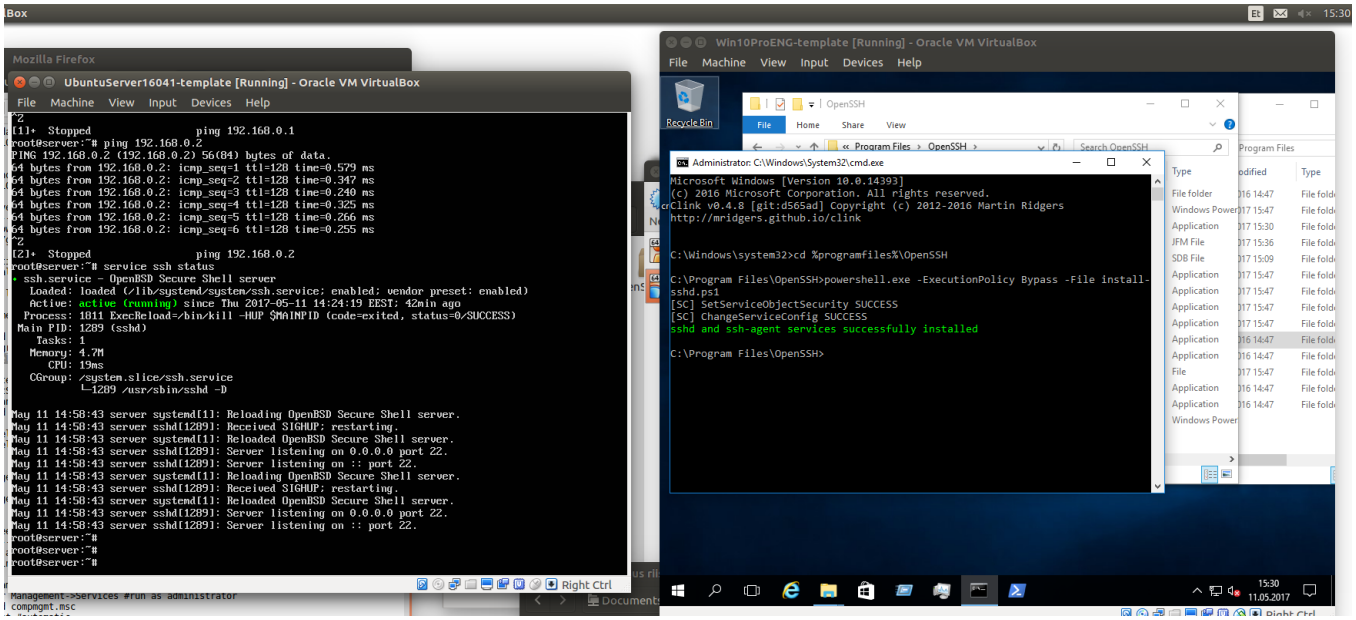
Praktikum 9 SSH Windows + Linux

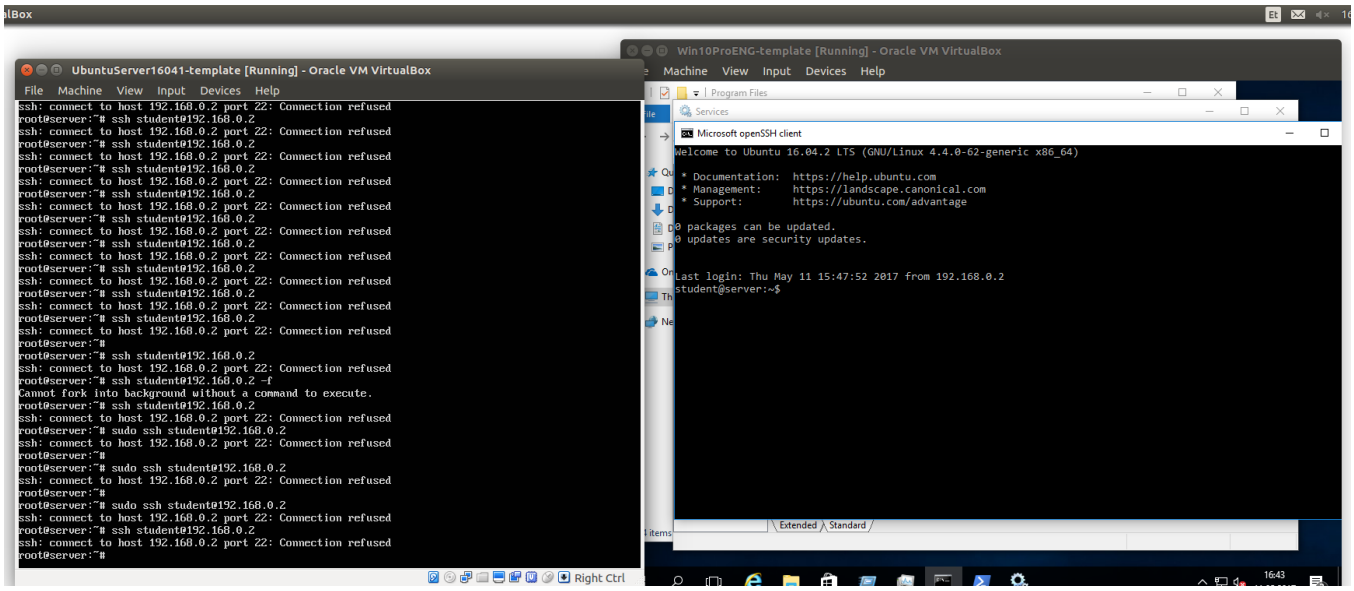
Contents

Windows ja Linuxi server on paigaldatud ja jooksevad virtuaalmasinates. IP addressid on konfigureeritud ja SSH töötab:



Pilt 1 SSH töötab mõlemal virtuaalmasinal

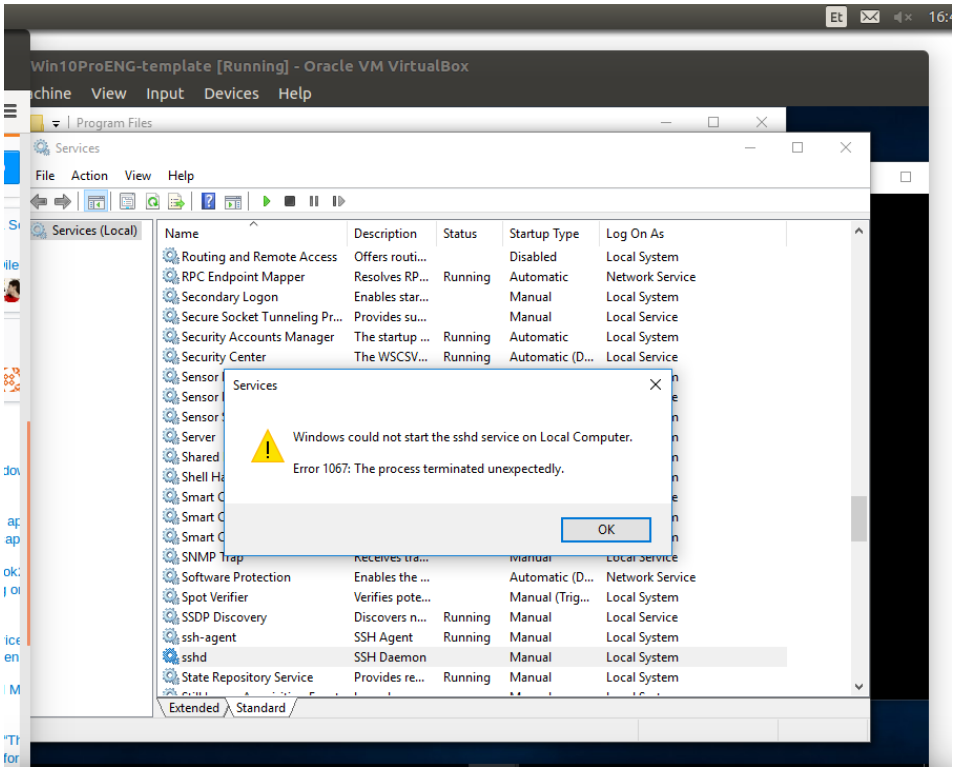
Windowsist saab sisse logida SSH kaudu Linuxisse, aga kahjuks ei saa Linuxist Windowsisse sisse logida:



Pilt 2 SSH'ga ühenduse loomine ühelt virtuaalmasinalt teise virtuaalmasinasse

Eelmine praktikum sain ma teises kooliarvutis mõlemasse sisse logida ilma probleemideta (pilte kahujks pole).

Niisiis proovisin teha ühte tuntud parandust, mis ma leidsin veebist, kus ma kustutan ära regedit.exe kaudu kõik SSH konfiguratsioonid ja proovin uuesti installida windowsile SSH peale. Kahjuks ei toonud see oodatud tulemust. Pildil näha, mis probleem on:



Pilt 3 Miks ma ei saanud Windows 10 SSH korralikult käima

Lisapunktid

1. Tugevama krüpto valik.

Tänapäeval on sisuliselt tugevaim krüpto RSA 4096 baiti, kuigi võib Linuxis kasutada ka 16384-bit võtmeid. Soovitatud on kasutada elliptilist algoritmi.

2. Selgitus, miks valitud krüpto on tugevam.

RSA krüpto murdmiseks on vaja hästi võimsaid arvuteid, ei ole täpselt teada, aga arvatakse, et kvantarvutid on võimelised RSA krüpto ära murdma. Kuigi võib kasutada RSA krüptot, mis on vähemalt 4096 baiti, on pigem soovitatud kasutada elliptilisi algoritme, sest võrreldes RSA'ga on elliptilised palju kiiremad ja võtmed on suuruselt väiksemad, kui tahetakse sama turvalisust, kui tehes RSA'ga.