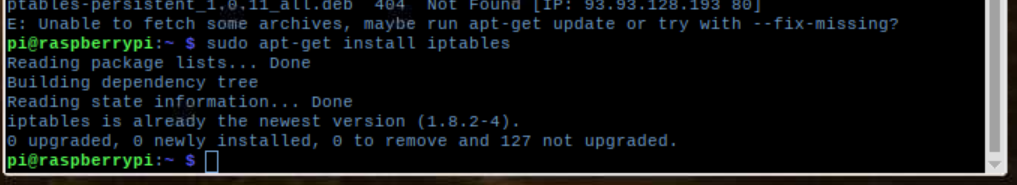
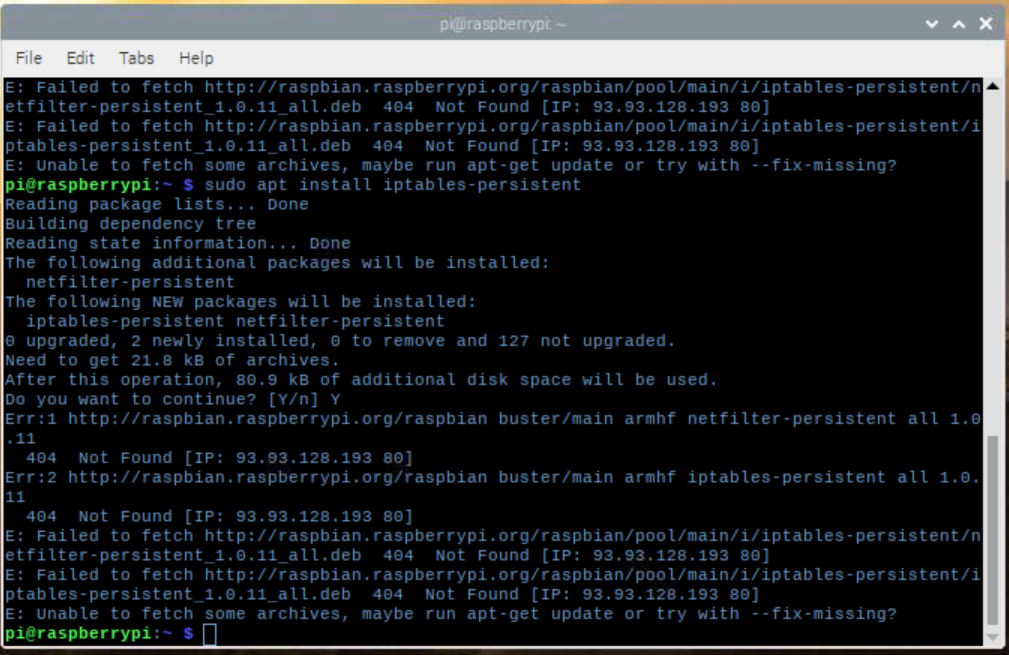
Extra uitdagende opdracht CSC

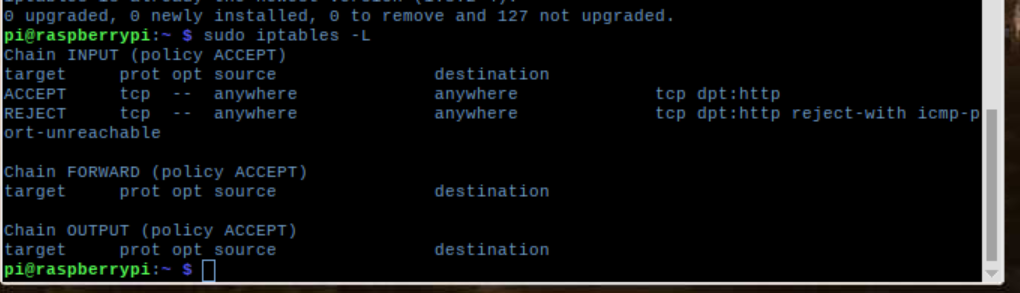
Alpha Consultants sg9a

Zorg ervoor dat:

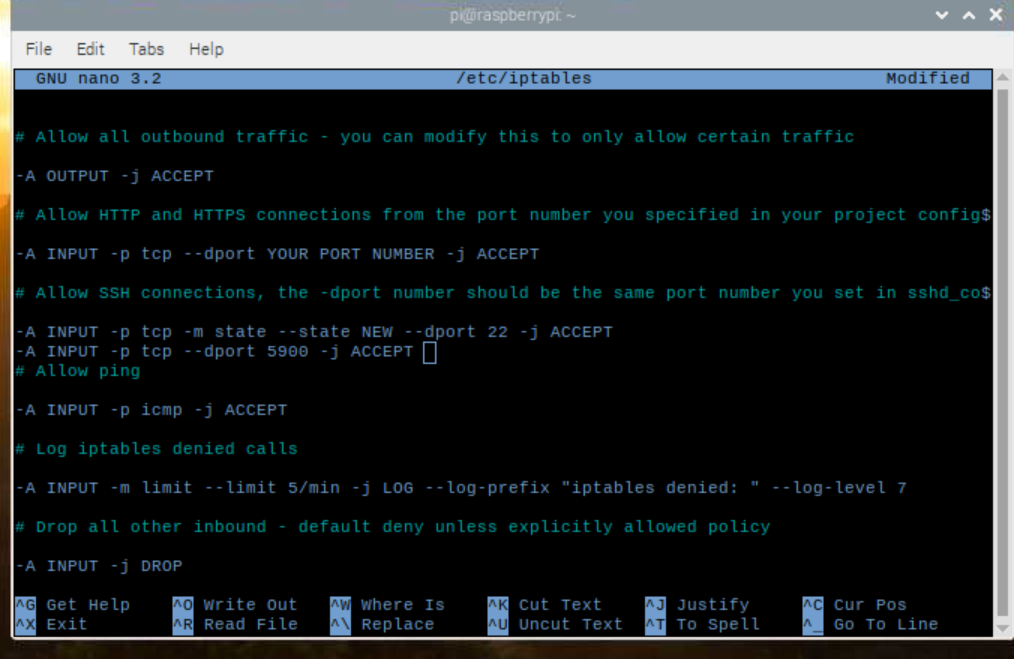
1. alleen van de diensten die je op de Raspberry Pi aan wilt bieden (SSH, waarschijnlijk VNC, mogelijk web server) worden toegelaten door iptables te configureren. In de cursus deden we dit eenmalig, nu willen we dat het blijft werken. Installeer daartoe het pakket iptables-persistent op de Raspberry Pi.



Iptables-persistent gaf een error dus ik heb iptables gebruikt.



De huidige configs.



Sudo nano /etc/iptables maakt een config file aan voor IPtables waar ik de code zo kan aanpassen dat het blockt en unblockt wat ik wil. Deze code blockt alle traffic behalve SSH en de ports die ik whitelist. 5900 is de port voor VNC en die daarboven is voor SSH

In /etc/network/interfaces zet ik een regel “pre-up iptables-restore < /etc/iptables zodat de raspberry elke keer de firewall opstart als de raspberry opstart.   
Met sudo iptables-restore < /etc/iptables laad ik deze regel in.

1. er veilige wachtwoorden op je Raspberry Pi gebruikt worden

Het wachtwoord gebruikt voor de raspberry Pi is samengesteld volgens het advies aangeboden in CSC4: Zelfstudie: Services en beveiliging.

Dit houdt in dat het wachtwoord bestaat uit:

Geen losse woorden  
een acroniem voor een langezin (bijvoorbeeld: Vwilasw,mhi20g!^@)  
(Vandaag wil ik lekker aan school werken, maar het is 20 graden!^@)  
De ^@ is toegevoegd zodat er geen dictionary attacks mogelijk zijn. En Brute Force attackers wel 100 miljoen + wachtwoorden moeten nagaan voordat ze op de juiste combinatie stuiten. Meer characters betekent dat ze meer tijd nodig hebben.