**Project Fasten Your Seatbelts**

**Security Handleiding**

Klas: IN104

Groep: 4

Door: Gian van Holt en Ahish Sewgobind



Inhoudsopgave

[Inleiding 3](#_Toc405533938)

[Software 4](#_Toc405533939)

[Hardware 4](#_Toc405533940)

[SPOOFING 4](#_Toc405533941)

[SSH 4](#_Toc405533942)

[Blokkeren van het internetprotocol ICMP 5](#_Toc405533943)

[Tutorial Permissions Linux files 6](#_Toc405533944)

[Mac-Adres 7](#_Toc405533945)

[Algemene voorwaarden 8](#_Toc405533946)

# Inleiding

De raspberries in de vliegtuigen van Corendon moet niet alleen software matig maar ook fysiek worden beveiligd. Dit om zo te behoeden dat het niet in verkeerde handen valt of juist misbruik van word gemaakt.

# Software

Doormiddel van ip tables regels en ook door de captive portal proberen we de software gedeelte zo goed mogelijk te beveiligen. Dit waren een paar voorbeelden qua software matige beveiligen.

# Hardware

De raspberries moeten in een beveiligde ruimte worden opgeslagen van de vliegtuig. Toegang word verleent doormiddel van een sleutel. Wel moet het mogelijk zijn om er gemakkelijk bij te komen maar zonder dat dit voor een werknemer of passagier hindert. Het moet mogelijk zijn dat beheerder en/of monteur van de technische dienst erbij kan om eventueel wat te doen zoals onderhoud.

Kabels worden allemaal weggewerkt, het zal niet mogelijk zijn om kabels te zien. Dit word of onderaan of bovenaan in de vliegtuig vastgemaakt denk dan aan onder op heup á knie hoogte en/of in de bagageruimte. De raspberries zijn verbonden met een switch die alle inkomende en uitgaande verbinding routeert. Ook dit is een beveiligde ruimte.

# SPOOFING

IP spoofing is wat ingewikkelder dan er fysiek bij een Raspberry bij te kunnen komen. Ook kun er neppe (Fake) DHCP servers zijn die door ‘externe’ worden beheerd, om zo ip adressen uit te geven.

Daardoor worden onbekende zaken zoveel mogelijk droppen. De reden waarom is om een “man in the middle” te voorkomen. Om zo te weerhouden dat er iemand kan meekijken naar alles wat je doet.

Bron:

http://xmodulo.com/spoof-mac-address-network-interface-linux.html

# SSH

Mogelijk is het om een firewall op te zetten voor inkomende verbinding doormiddel van kabel, denk aan SSH. Onbekende ip adressen worden dan geblokkeert.

Ook kan dit via “ip tables”. Een belangerijk term als het gaat om beveiligen.

Bron:

<http://www.hobbytronics.co.uk/raspberry-pi-ssh>

# Blokkeren van het internetprotocol ICMP

Hoe moet je een ping blokkeren? Zodat je bij het gebruik willen maken van ping een error melding krijgt.

Met het volgende manier kan je de ping blokkeren. Bij het uitproberen krijgt je de volgende melding: “Destination port unreachable”.

Voeg de volgende ip table line toe om dit toe te passen:

**iptables -A INPUT -p icmp --icmp-type echo-request -j REJECT**

Om ping te blokkeren zonder dat je een melding krijgt moet je de volgende regel toevoegen:

**iptables -A INPUT -p icmp --icmp-type echo-request -j DROP**

**iptables -A OUTPUT -p icmp --icmp-type echo-reply -j DROP**

Bron:

<http://crybit.com/iptables-rules-for-icmp/>

# Tutorial Permissions Linux files

Een file kan opgedeeld worden in 3 “user based permissions groups”

**Owner** – de owner permissies gelden voor alleen voor de Owner van de file, het heeft dus geen effect op andere gebruikers.

**Group** de groep permissies gelden voor de groep die is aangewezen voor de file of directory.

**All users**- de All users permissie geld voor alle gebruikers van het systeem

Ook heb je 3 permissie types

read deze permissie zorgt ervoor dat de user based permissie groep het alleen kan lezen. er kunnen dus geen bewerkingen worden gedaan in de file of directory

write de write permissie zorgt ervoor dat je de file of directory kan bewerken.

execute The execute permissie zorgt ervoor dat je de gebruiker de file kan uitvoeren.

je kan de permissies zien door de” ls –l” command te gebruiken als je in de directory bent die de file of folder bevat.

de user based permission groups in een command worden aangegeven met:

**u**- Owner

**g**- Group

**o** or **a** - All Users

en de permissie types worden aangegeven met:

**r**- Read

**w** - Write

**x** – Execute

waarbij een + toevoegen betekent en een – verwijderen betekent

**a-rw bestand1**  staat dus als ALL users, Read write bestand1

alle gebruikers kunnen bestand1 dus lezen en bewerken.

Je kan de permissies aanpassen door de command chmod te gebruiken.

Stel je voor dat je een bestand hebt genaamd bestand1 en die heeft als permissie **\_rw\_rw\_rw,**

**de eerste \_rw geld voor the OWNER**

**De tweede \_rw geld voor de group**

**en de derde \_rw geld voor All users.**

***om bestand1 aan te passen kan je bijvoorbeeld de commad*** **chmod a-rw bestand1** gebruiken. deze bestand verwijderd de **write en read** voor all users

en om **Read** en **write** voor **all users** toe te voegen gebruik je  ***chmod a+rw bestand1***

Bron:

<https://www.linode.com/docs/tools-reference/linux-users-and-groups>

<http://ryanstutorials.net/linuxtutorial/permissions.php>

# Mac-Adres

Het volgende script kan worden toegepast als er een mangle table is aangemaakt die “INTERNET” heet.

**iptomac=$(arp -an | grep $1 | cut -d " " -f 4)**

**sudo iptables -t mangle -I NAAM -m mac --mac-source $iptomac -j RETURN**

Je maakt een variable aan die noem je “iptomac”. Daarin vermeld een commando er iets moet worden gekopieerd wanneer een apparaat verbonden is met het Corendon netwerk.

Iets is in dit geval het Mac-adres van een apparaat. Dit word vervolgens bewaard in de database. Voordat dit word bewaard moet het worden opgeslagen en dan verplaatst.

# Algemene voorwaarden

Corendon B.V levert aan haar reizigers de mogelijkheid om tegen betaling gebruik te maken van het internet tijdens de vlucht door middel van het WiFi netwerk in de vliegtuig. Mits u beschikt over een geschikte gebruikersnaam en wachtwoord en u akkoord gaat met de volgende gebruikersvoorwaarden:

1. De bandbreedte die per sessie ter beschikking word gesteld is onbeperkt. U heeft dus geen limiet en er komen geen extra kosten bij als u gebruikt maakt van het WiFi netwerk.
2. De kwaliteit en snelheid kan afhangen van een aantal verschillende factoren

waaronder atmosferische storingen en de kwaliteit van de door u gebruikte randapparatuur onder vallen.

1. U zult:
   1. Niets doen dat leidt tot overlast van het personeel of voor de andere reizigers die gebruik maken van de vliegtuig of het WIFI netwerk.
   2. Niet handelen in strijd met wettelijke bepalingen en het netwerk niet gebruiken voor criminele doeleinden zoals spamberichten, virussen en/of malware te verspreiden.
   3. Geen inbreuk te maken op de beveiliging van het netwerk en/of toegang proberen te verkrijgen tot de apparatuur van het vliegtuig, personeel of andere reizigers.
   4. Het dataverkeer tussen de door u gebruikte apparatuur en de accespoint is niet versleuteld. U bent dus uiteindelijk zelf verantwoordelijk voor de beveiliging van de apparatuur waar u gebruik van maakt
2. Corendon is niet aansprakelijk voor enige schade die u zou leiden in verband met het gebruik maken van het netwerk of van het internet. Als u het daar niet eens mee bent of als u kunt bewijzen dat de schade is aangebracht door of het WIFI net werk of het personeel kunt u een klachtbrief schrijven naar onze hoofdkantoor.