Linux in Groningen

Johan Swenker

In Groningen hebben we, een jaar of 20 geleden, een Linux-werkgroep, opgericht. In de huidige Corona-periode komen we nog steeds bij elkaar, maar nu online. Dankzij Jitsi hebben we nu deelnemers uit Duitsland, Den Haag, Zwolle, Zuid-Drenthe en natuurlijk uit de stad. Hieronder geen verslag van die bijeenkomsten, maar een artikel met diverse onderwerpen die aan de orde zijn gekomen.

Fail2ban

Eén van ons gebruikt **fail2ban** om aanvallers te blokkeren. Maar dat leek niet te werken. Dus de vraag was, hoe kan ik zien dat fail2ban echt werkt?
Fail2ban is een netwerkfunctie die een gebruiker blokkeert (Engels: ban), als het inloggen te vaak mislukt (Engels: fail).

Nu is er gelukkig ook iemand met voldoende ervaring om te vertellen dat **fail2ban** de standaard Linux firewall *iptables* gebruikt om een aanvaller te blokkeren. Als het IP-adres van een aanvaller in de configuratie van iptables staat, dan wordt die aanvaller geblokkeerd. De configuratie van iptables kun je als root opvragen met het commando
`iptables -L -n`

```
nano:~# iptables -L -n |grep -v ^LOG
Chain INPUT (policy DROP)
target     prot opt source               destination
DROP       all  --  92.241.190.0/24      0.0.0.0/0
DROP       all  --  184.82.162.0/24      0.0.0.0/0
DROP       all  --  184.22.103.0/24      0.0.0.0/0
DROP       all  --  158.255.211.0/24     0.0.0.0/0
DROP       all  --  91.191.209.0/24      0.0.0.0/0
DROP       all  --  23.247.53.0/24       0.0.0.0/0
DROP       all  --  31.210.20.0/24       0.0.0.0/0
DROP       all  --  37.49.225.0/24       0.0.0.0/0
DROP       all  --  141.101.239.225      0.0.0.0/0
DROP       all  --  178.162.129.237      0.0.0.0/0
```

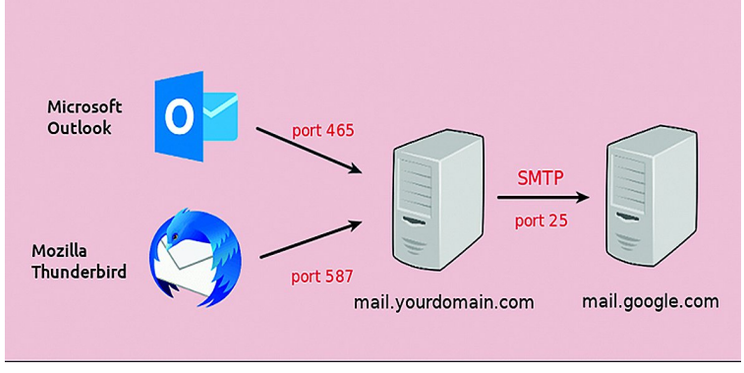
Later bleek dit maar het halve verhaal te zijn, want binnen iptables kun je met DROP-regels werken die losse IP-adressen blokkeren:
`iptables -A INPUT -p tcp -s $aanvaller_IP -j DROP`
blokkeert aanvaller_IP.

Maar iptables kan ook met verzamelingen van IP-adressen werken: *ipset*. Dit is de standaardmanier waarop fail2ban werkt. Of eigenlijk: zou moeten werken.

Na een configuratie-wijziging waarbij
`banaction = firewallcmd-ipset`
vervangen werd door:
`banaction = iptables-multiport`
werkt fail2ban zoals de bedoeling is.

Versleuteld e-mailtransport

E-mail versleutelen kan op verschillende manieren. Je kunt een versleuteld bestand als e-mail verzenden; je kunt het bericht zelf versleutelen met bijvoorbeeld **PGP** of **S/MIME**. In beide gevallen is het onderwerp nog steeds niet versleuteld, en dus af te luisteren. Je kunt ook het netwerkverkeer tussen de mailservers versleutelen. Merk op dat dit alleen het verkeer tussen de mail-servers onderling versleutelt. Op de mailserver kan een malafide mailbeheerder nog steeds het onderwerp zien.



Er zijn een paar verschillende netwerk-protocollen om mail te verzenden: **smtp** (25), **smtps** (465) en **submission** (587). Smtps is de versleutelde variant van smtp, net zoals https de versleutelde variant is van http.
Maar er is een klein (groot?) verschil: moderne smtp-servers kunnen overschakelen van een verbinding in klare tekst naar een versleutelde verbinding. Die smtps is dus overbodig!

In een zaal presenteren met Jitsi

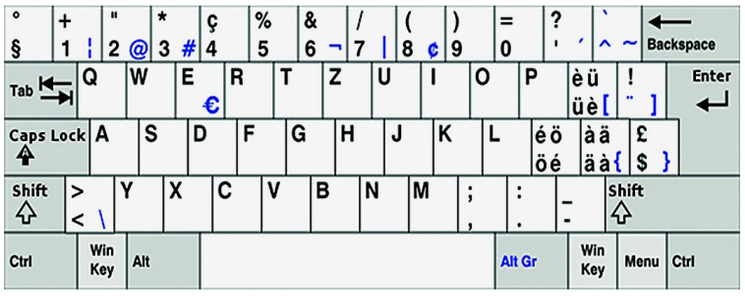
De afdeling Zuid-Drenthe is zich aan het voorbereiden op presentaties waarbij sommige toehoorders in de zaal zitten, andere toehoorders thuis Jitsi gebruiken, en er toch interactie is. De oplossing die daarvoor bedacht is, maakt gebruik van een pc met drie monitoren. Maar helaas: de pc had wel drie video-uitgangen, maar Linux kon er slechts twee tegelijk aansturen. Dit is gelukkig geen beperking van Linux. Het was een beperking van de hardware. Dat was dus eenvoudig op te lossen. De pc is nu voorzien van een grafische kaart met vier uitgangen. Ook hier weer een beperking: er kunnen slechts drie uitgangen tegelijk gebruikt worden. Maar dat iss genoeg voor dit doel.

Een heel vreemd toetsenbord

Een van ons had een paar laptops op de kop weten te tikken met een heel vreemd toetsenbord. Hij liet ons het toetsenbord zien. Dat is het mooie van Jitsi, het is tenslotte beeldbellen. Boven de **4** stond de **ç**, de toetsen rechts van de **p**, **l** en **m** hadden 4 of zelfs meer letters per toets. Maar allemaal van die bijzondere letters zoals **ø æ** en **ß**.
Wat voor toetsenbord is dit? Met het programma *xev* kun je op heel laag niveau zien welke toets is ingedrukt en hoe Linux dat interpreteert.

Voor details als je hiermee wilt gaan spelen op:
http://xahlee.info/linux/linux_xmodmap_tutorial.html
en in de manualpagina's vind je de uitleg voor *keymaps* en *xmodmap*.

Het bleek een Zwitsers toetsenbord te zijn. In Zwitserland spreken ze wel vier verschillende talen. Ze gebruiken echter één toetsenbordindeling, zodat een werknemer ook makkelijk in een ander filiaal en/of een ander taalgebied aan de slag kan. Bron:
https://de.wikipedia.org/wiki/Tastaturbelegung#Schweiz



Yum en https

Ik gebruik zelf Ubuntu en Debian, en ik weet dat **apt** gebruik kan maken van **https** om softwarepakketten uit een repository te halen. Op mijn werk beweerde een projectleider dat **yum** dat niet zou kunnen. Dan is het fijn dat er bij HCC ook mensen zijn die RedHat, CentOS of Fedora gebruiken, zodat ik een en ander kon navragen.

Uiteraard, ook yum ondersteunt https om softwarepakketten te downloaden. De configuratie-files voor yum staan in de directory **/etc/yum.repos.d**, en in zo'n configuratie-file kun je prima opgeven dat https gebruikt moet worden.

Maar ik moet toegeven, de documentatie van RedHat is niet erg duidelijk. Op de manualpagina van **yum.conf** wordt gesproken over een **baseurl**, met de aanvulling: *Can be an* **http://**, **ftp://** or **file://** URL. Dan zou je dus zeggen dat https niet mag. Maar als je bij RedHat gaat zoeken naar voorbeelden, dan vind je dat yum wel degelijk https ondersteunt.

Of het nodig is om https te gebruiken om softwarepakketten te downloaden, daarover kun je van mening verschillen. Alle pakketten die RedHat beschikbaar stelt zijn voorzien van een digitale handtekening. Dat is in principe voldoende om te detecteren dat onderweg het bestand aangepast is. Maar tegelijkertijd kun je als principe stellen:
al het netwerkverkeer moet versleuteld zijn, dus ook een download van een softwarepakket.

Atop om problemen op te lossen

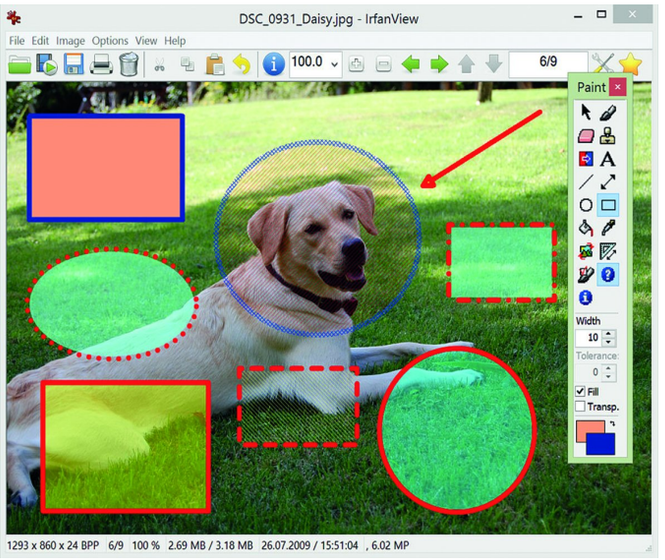
Een van ons heeft al een tijdje een probleem met een computer waarvan het geheugen soms volloopt; daarna gaat de computer swappen; en even later is de computer helemaal niet meer te gebruiken. Probeer er dan nog maar eens achter te komen wat er aan de hand was.

Dat is dan het mooie van een club als HCC. Er is altijd wel iemand die een zetje geeft in de juiste richting. Die richting was het commando **atop**. Met **atop -r** kun je de status van het systeem opvragen, van een willekeurig moment uit het verleden. Die status is heel uitgebreid: o.a. de belasting van de CPU, het geheugengebruik, en alle processen die toen liepen *(zie de afbeelding op de volgende pagina)*.

Dat was precies wat nodig was om verder te puzzelen. Dat puzzelen hebben we met z'n allen gedaan tijdens de Jitsi-bijeenkomst. Met Jitsi kunnen immers alle deelnemers hun beeldscherm delen. We hebben de echte boosdoener nog niet gevonden, maar binnen een Linux-club wordt een proces als **explorer.exe** natuurlijk wel als verdacht beschouwd.

Alternatieven voor Windows programma's

Je kunt natuurlijk *Wine* gebruiken om *IrfanView* te draaien. Maar als je dan aan Linux-mensen vraagt: mijn computer doet vreemd, hoe kan dat?
Tja, dan zal zelfs de minst fanatieke Linux-fan zich afvragen: is er geen alternatief voor IrfanView?



```
File  Edit  View  Terminal  Tabs  Help
ATOP - deb-06-2021          2021/09/22  11:56:21          --------------          10m0s elapsed
PRC | sys   97.87s  | user   9m22s  | #proc    198  | #tslpu     0  | #zombie    0  | #exit   1086  |
CPU | sys      16%  | user     93%  | irq        1%  | idle     77%  | wait      14%  | ipc     0.57  |
cpu | sys       8%  | user     46%  | irq        1%  | idle     37%  | cpu001 w   8%  | ipc     0.57  |
cpu | sys       8%  | user     47%  | irq        0%  | idle     40%  | cpu000 w   5%  | ipc     0.58  |
CPL | avg1    2.56  | avg5    2.19  | avg15   2.03  | csw   6806124  | intr 1854656  | numcpu     2  |
MEM | tot     3.7G  | free  158.2M  | cache 503.6M  | buff    9.1M  | slab  101.9M  | hptot   0.0M  |
    | tot   975.0M  | free   91.3M  |               |               | vmcom   8.4G  | vmlim   2.8G  |
    | scan  581188  | steal 250756  | stall      0  |               | swin   16813  | swout 120716  |
DSK |          sda  | busy      3%  | read   26157  | write   5019  | MBw/s    1.4  | avio 0.50 ms  |
NET | transport     | tcpi  345083  | tcpo  219375  | udpi     228  | udpo     191  | tcpao     99  |
NET | network       | ipi   345348  | ipo   219571  | ipfrw      0  | deliv 345315  | icmpo      6  |
NET | enp0s25  11%  | pcki  597238  | pcko  219601  | sp  100 Mbps  | si   11 Mbps  | so  211 Kbps  |
NET | tun0      0%  | pcki       1  | pcko       0  | sp   10 Mbps  | si    0 Kbps  | so    0 Kbps  |
Window resized to 101x39...
  PID SYSCPU USRCPU   VGROW  RGROW  RDDSK   WRDSK RUID     ST  EXC  THR S  CPUNR  CPU  CMD        1/54
 2728 32.09s  2m55s  504.7M 241.1M 35504K      0K rootf-k  --    -   43 S      1  35%  Web Content
 1878 19.40s  1m46s  66552K  3064K 42256K  360.4M rootf-k  --    -   68 S      1  21%  firefox-esr
 3772 11.79s 89.66s      0K -18.3M 17540K      0K rootf-k  --    -   13 S      1  17%  mpv
 1534  5.14s 63.05s   6292K -6392K 34576K      0K rootf-k  --    -   10 S      1  12%  cinnamon
 1556  3.65s 43.01s  -3072K -61.2M 95544K    740K rootf-k  --    -   62 S      1   8%  thunderbird
  851  8.63s 15.80s  15232K   764K   624K      0K root     --    -    3 S      0   4%  Xorg
 5599  1.97s 14.77s  113.4M 66408K 10408K      0K rootf-k  --    -   20 S      0   3%  Web Content
 4559  2.44s 13.05s  241.1M 106.4M 66332K      0K rootf-k  --    -   22 S      1   3%  Web Content
 7996  1.94s 12.97s  91100K 49020K  7972K      0K rootf-k  --    -   20 S      0   3%  Web Content
 2373  1.10s  8.69s  31436K -8656K 15704K      0K rootf-k  --    -   20 S      0   2%  Web Content
 9220  0.86s  6.53s   7408K  9936K  6244K      0K rootf-k  --    -   21 S      0   1%  Web Content
 1191  2.23s  3.91s      0K -2032K   592K      0K rootf-k  --    -    3 S      1   1%  pulseaudio
 2322  0.61s  4.24s  14784K -14.0M  3820K      0K rootf-k  --    -   19 S      1   1%  WebExtensions
   36  2.33s  0.00s      0K     0K     0K      0K root     --    -    1 S      1   0%  kswapd0
 4801  0.24s  1.17s  18224K -2732K  3756K      0K rootf-k  --    -   21 S      1   0%  Web Content
 9986  0.22s  1.18s      0K -1748K  2032K      0K rootf-k  --    -    3 S      1   0%  xfce4-terminal
 2254  0.19s  0.99s   1024K -3228K  7916K      0K rootf-k  --    -   19 S      0   0%  Web Content
  576  0.13s  0.58s      0K 14016K 31112K   2288K debian-t  --    -    1 S      0   0%  tor
  490  0.44s  0.17s    920K   780K    40K     48K root     --    -    1 R      1   0%  atop
   29  0.37s  0.00s      0K     0K     0K      0K root     --    -    1 S      1   0%  khugepaged
 9687  0.36s  0.00s      0K     0K     0K      0K root     --    -    1 I      1   0%  kworker/1:2-ev
 8592  0.29s  0.00s      0K     0K     0K      0K root     --    -    1 I      0   0%  kworker/0:1-mm
  901  0.11s  0.14s      0K  -212K  2648K      0K rootf-k  --    -    1 S      0   0%  dbus-daemon
```

Met atop is een uitgebreid stasus van de pc op te roepen

Zelf zoek ik altijd naar alternatieven met een normale zoekmachine. Zoekkreten zoals *linux* in combinatie met de naam van het Windows-programma is voor mij vaak voldoende.
In de club werd aangegeven dat **alternativeto.net** de plaats was om alternatieven te vinden.
Bij het zoeken op **alternativeto.net** naar IrfanView viel het mij op dat veel programma's beschreven werden als een image-viewer, terwijl IrfanView duidelijk meer kan. Als je echter verder bladert naar de opinions, dan blijken veel programma's toch meer te kunnen dan alleen het tonen van plaatjes.

Ondertussen wordt nu met veel genoegen *nomacs* gebruikt in plaats van IrfanView.