**Week 1 – Firewall exercise**

An important thing to prevent attacks is to have a firewall in place. However, a firewall also allow us to see if our system is under attack by logging those attacks.

Ubuntu comes with a build in firewall called ufw (**u**ncomplicated **f**ire**w**all).

**Create an Ubuntu droplet on Digital Ocean**

**Enable the firewall instructions are here. WARNING: make sure to allow SSH before starting the firewall**

* Følg denne guide: <https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu-16-04>
* Installer firewall i terminalen på droplet: sudo apt-get install ufw.
* Gå ind i filen: sudo nano /etc/default/ufw
* Vær sikker på at IPV6 = yes

Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse

* Set default policy, således at alt indgående trafik er nægtet, mens alt udegående trafik tillades. For at sikre serveren.

sudo ufw default deny incoming

sudo ufw default allow outgoing

* Tillad SSH forbindelse: sudo ufw allow ssh
* Aktiver firewall: sudo ufw enable
* Eftersom at vi bruger en droplet, der er sat op med https, vil vi tillade forbindelser fra https: sudo ufw allow https
* For at se status på hvilke forbindelser der er tilladte og hvilke der er nægtet, samt se om logging er sat til og om hvorvidt firewallen er aktiv: sudo ufw status verbose

Et billede, der indeholder tekst

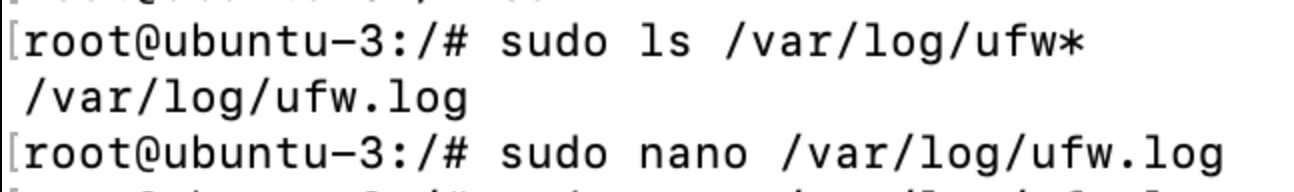
Automatisk genereret beskrivelse

**Enable logging for the firewall this answer gives the commands**

* Man kan se om firewallen logger ved at skrive: sudo ufw status verbose
* Hvis logging ikke er ”til” kan man skrive følgende: sudo ufw logging on

**Find the log, and find out (**[**this might be helpful**](https://help.ubuntu.com/community/UFW)**- look at the end)**

* For at se om der er en logfil: sudo ls /var/log/ufw\*
* Dette svar fik vi tilbage:



**From which IP addresses do you get visitors**

* Billedet nedenunder viser logfilen, som indeholder flere oplysninger. I firkanten markeret er **SRC (source)=** er den IP-adresse der forsøger at tilgå serveren og **DST (destination)=** er IP-adressen for serveren

**Where are those IP addresses located (**[**www.ip-tracker.org**](https://www.ip-tracker.org/)**)**

* Vi har taget tre IP-adresser der kom frem i logfilen og undersøgte, hvilke lande IP-adresserne kommer fra:
  + 92.118.37.86 er en IP-adresse fra Holland
  + 162.243.139.192 er en IP-adresse fra USA
  + 87.251.74.60 er en IP-adresse fra Rusland

Et billede, der indeholder vindue, stor, sidder, hvid

Automatisk genereret beskrivelse

**What ports do your visitors attempt to use**

* Besøgende forsøger bl.a. at komme ind på port:
  + 23 (Telnet protokol – ikke-krypteret tekst kommunikation)
  + 3333 (UDP og TCP)
  + 61 (NIFTP-Based Mail protocol)
* Dette billede stammer fra samme logfil, som ovenstående billede. Her ses bl.a. **SPT (source port) =** som er den port den besøgende sender fra og **DPT (destination port) =** som er den port den besøgende forsøger at komme igennem til serveren. Ude i højre side ses **SYN URGP (urgent pointer) = 0**, som indikere at den besøgende har forsøgt at tilgå serveren flere gange, men fra en ny forbindelse.

Et billede, der indeholder tekst

Automatisk genereret beskrivelse