**Exercise – Logging og monitoring**

If your machine is hacked, you will not be able to look at the log files to see what happened. So it is good practice to log to a different machine. There are companies that offer this service, but we will try to set up a minimal system to do this ourselves to understand the principles.

Et billede, der indeholder tekst, whiteboard, hvid, bord

Automatisk genereret beskrivelse

Vi har til denne opgave først oprettet en log-server og en honeypot på vores droplet.

Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse

Dernæst har vi hentet dette projekt ned lokalt:  [github.com/securitydatspring2019/week-03-logger](https://github.com/securitydatspring2019/week-03-logger).

**Den generede jar fil fra projektet, har vi kopieret til log-serveren, således:**

$ scp <file> <username>@<IP address or hostname**>**:<Destination>

**Et billede, der indeholder indendørs, tv, monitor, skærm

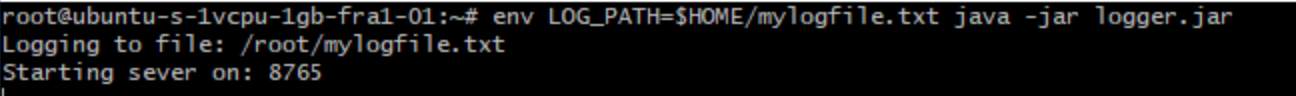
Automatisk genereret beskrivelse**

**På log-serveren har vi installeret Java, således:**

$ apt-get update

$ apt-get install openjdk-8-jre

For at starte en ”shell” med LOG-PATH, som enviroment variable og programmet, skriver vi følgende:

****

Dernæst slår vi firewall til, og tillader adgang gennem port 22 (SSH) og 8765 (porten på log-serveren)

**Et billede, der indeholder skærmbillede, bord, sidder, sort

Automatisk genereret beskrivelse**

På **honeypot,** skriver vi følgende, for at teste at vores logs bliver registeret på log-serveren.

**Et billede, der indeholder sidder, monitor, tv, skærm

Automatisk genereret beskrivelse**

På **log-serveren**, åbner vi logfilen, for at se hvornår nogen har forsøgt at få adgang.

**Et billede, der indeholder sort, foto, sidder, skærm

Automatisk genereret beskrivelse**

Dernæst laver vi en bruger på **honeypot**, for at kunne se specifikt hvem der forsøger at få adgang til serveren.

$ useradd -m test

$ passwd test

Vi skal tillade at oprette en ssh-forbindelse ved brug af password, ved først at gå ind i filen:

$ nano /etc/ssh/sshd\_config

Ændr PasswordAuthentication til ”yes”:

Et billede, der indeholder sidder, monitor, tv, skærm

Automatisk genereret beskrivelse

Opdater ændringerne, ved følgende kommando:

$ service ssh reload

Åben et script, således:

$ nano /etc/profile.d/logger.sh

og kopier følgende ind i scriptet (vigtigt at url er til log-serveren samt serverens port).

Et billede, der indeholder skærmbillede, monitor, skærm, tv

Automatisk genereret beskrivelse

Når nogen forsøger at logge ind på serveren, vil der oprettes en log inde på log-serveren, som fortæller hvem der er logget ind. Det kan ses på nedenstående billede:

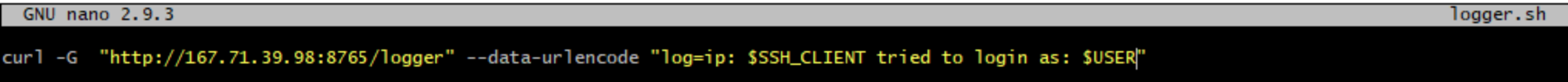
Et billede, der indeholder skærmbillede, monitor, skærm, sort

Automatisk genereret beskrivelse

1. **Can you find out which IP that user came from?**

Der findes en enviroment variable der hedder:  [SSH\_CLIENT](https://github.com/securitydatspring2019/week-03-logger) , der giver IP-adressen.

**Inde på honeypot serveren i filen skrives følgende:**



Nu er det muligt at se hvilken ip-adresse brugeren kommer fra.

Et billede, der indeholder skærmbillede, monitor, sort, skærm

Automatisk genereret beskrivelse

1. **Which other info do we have we could log?**

Nedenstående kommando giver en række enviroment variabler, hvori der ligger informationer, som kunne bruges til at logge.

$ env

**Med udgangspunkt I denne kommando, besvares nedenstående spørgsmål.**

curl -G "http://loggingsystem:8888/logger" --data-urlencode "log=Someone knocked"

1. **What does curl do in the first place**

Det er en Command Line Tool til at sende data fra en server til en anden.

1. **What is the -G option, and what is the strange option at the end**

-G : indikerer et get request og tilføjer dataen til urlen.

--data-urlencode **:** gør data url-kompatibel, bl.a. udskifter den mellemrum med %20%. Dette sørger curl ikke for.

1. **Can we omit any of the flags?**

Hvis vi udelader -G vil logbeskeden ikke komme med.

Vi kan godt udelade --data-urlencode , men det vil så betyde at logbeskeden manuelt skal gøres url-kompatibel.