Linux - practicum week 3

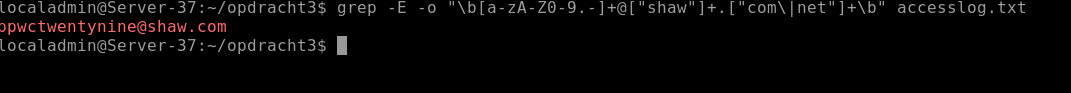
Zorg ervoor dat alle voortgang wordt bijgehouden in de Git repository.  
Opdracht 1: RegEx  
  
In de file apache-access-log.txt vind je een access-log.  
Schrijf een regex die mailadressen herkent van het bedrijf “shaw”. Het bedrijf staat zowel  
onder de tld com en .net geregistreerd.  
  
In de basis volgt het bedrijf Shaw de conventies van email-naamgeving van RFC 822.

Daarboven op hebben ze de volgende naamgevingssystemetiek.

* Generieke opbouw van een mailadres bij Shaw is: <mailnaam>@shaw.com of <mailnaam>@shaw.net
* Voor de <mailnaam> geldt:
  + Minimaal 2 karakters (karakter= cijfer, letter en speciale tekens), maximaal 99
  + Op laatste positie staat of een letter (“a” t/m “z” , “A” t/m “Z”), of een cijfer(“0” t/m “9”)
  + Op andere posities geen cijfers toegestaan, wel letters of de speciale tekens “.”, “\_” en “-“
  + Andere speciale tekens geheel niet toegestaan

De regex kun je als volgt controleren:  
grep -E -o "<YOUR\_REGEX>" access\_log

**grep -E -o "\b[a-zA-Z0-9.-]+@["shaw"]+.["com\|net"]+\b" accesslog**



Opdracht 2: monitoring en logging  
  
**a)** Zet een Linux (Ubuntu)server op die als monitor/log server kan dienen.   
  
Als monitor tool kun je de volgende tools gebruiken:  
Munin  
Nagios   
Prometheus  
(andere mogen ook na overleg met docent).  
  
Voor het opzetten van een centrale syslog server:  
Syslog  
Syslog NG  
Elastic Stack  
(andere mogen ook na overleg met docent).

Afbeelding met tekst

Automatisch gegenereerde beschrijving

**b)** Zet zelf een Ubuntu Linux server op die door de vorige server (in opdracht a)  
gemonitord wordt.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

**c)** Installeer op de server, die bij opdracht b gecreëerd is, Apache en/of NGNIX samen met  
PHP en MySQL/MariaDB. De logs van de hiervoor genoemde applicaties worden op de log  
server verzameld.

**d)** Zorg voor hardening script die de Apache Server beter beveiligd dan de standaard instellingen, bijv. via deze handleiding:  
<https://geekflare.com/apache-web-server-hardening-security/>

Apache Script:

#!/bin/bash

path=/etc/apache2/apache2.conf

cp $path /home/

echo "\nBackup is aangemaakt in home folder\n"

echo '#Hardening opties' >> $path

echo 'ServerTokens Prod' >> $path

echo "ServerToken veranderd, http afgeschermd\n"

echo 'TraceEnable off' >> $path

echo "Tracing uitgezet\n"

echo 'ServerSignature off' >> $path

echo "Signature uitgezet\n"

sed -i 's@^\(Timeout\) 300@\1 60@g' $path >> $path

echo "Timeout verlaagd\n"

echo "Apache serivce herstarten..."

service apache2 restart