

Nom : NGOUNE AGUEGUIA

Prénom : Noël Patrick

Devoir pratique de fin de Formation Linux

I- Manipulation des logs

- Notes : on se trouve dans le dossier contenant le fichier ``devoir.md`` donc dans le dossier ``devoir`` ou ``devoir_ngoune`` avant d'exécuter les commandes.
- Nombre de lignes :
CMD: `wc -l file/log-server.log`
REP: 5672 file/log-server.log
- Nombre de clients connectés :
CMD: `cut -d ' ' -f 1 file/log-server.log | sort -u | wc -l`
REP: 17
- Nombre de clients qui ont accédé avec succès :
CMD: `grep -E '[0-9]{2}' file/log-server.log | cut -d ' ' -f 1 | sort -u | wc -l`
REP: 9
- Nombre de clients qui ont accédé avec message d'erreur :
CMD : `grep -E '(5|4)[0-9]{2}' file/log-server.log | cut -d ' ' -f 1 | sort -u | wc -l`
REP: 13

II- Détection des intrusions

- Nombre de fois que l'hacker s'est connecté au serveur :
CMD: `cut -d ' ' -f 1 file/log-server.log | grep '^127.0.0.1' | wc -l`
REP: 626
- Identifier l'url le plus appelé par l'hacker :
CMD: `grep '^127.0.0.1' file/log-server.log | cut -d ' ' -f 11 | grep '^https' | sort | uniq -c | sort -hr | head -n 1`
REP: 325 "https://spmi:gitechsn.com/application/navigation/dashboard/global"

- Nombre de fois que le hacker s'est connecté avec son navigateur 'safari' :

CMD: `grep -iw 'safari' file/log-server.log | grep '^127.0.0.1' | wc -l`

REP: 623

- Système et la version de l'OS du hacker :

CMD: `grep '^127.0.0.1' file/log-server.log | grep '(.)' | cut -d '(' -f 2 | cut -d ')' -f 1 | sort | uniq -c | sort -hr`

REP: 373 Macintosh; Intel Mac OS X 10_15_7

139 Macintosh; Intel Mac OS X 11_0_1

111 Windows NT 10.0; Win64; x64

- Nombre d'attaques d'origine sénégalaise subies par le serveur :

CMD: `grep -E '^41.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}' file/log-server.log | wc -l`

REP: 3057

III- Script Shell

Enoncé : Script permettant de manipuler les logs serveur. Le script prendra en entrée le fichier de logs et donnera en sortie toutes les informations ci-dessus.

Réponse (lien GitHub du projet) : <https://github.com/ngoupatrick/tempon>

Capture écran script

```

#!/bin/bash
echo "*****"
echo "## Script permettant de manipuler les logs du serveur ##"
echo "*****"
echo ""
echo "1- Nombre de ligne du fichier $1"
wc -l $1
echo ""
echo "2- Nombre de clients connectés"
cut -d ' ' -f 1 $1 | sort -u | wc -l
echo ""
echo "3- Nombre de clients ayant accédé avec succès"
grep -E '2[0-9]{2}' $1 | cut -d ' ' -f 1 | sort -u | wc -l
echo ""
echo "4- Nombre de clients ayant accédé avec message d'erreur"
grep -E '(5|4)[0-9]{2}' $1 | cut -d ' ' -f 1 | sort -u | wc -l
echo ""
echo "5- Nombre de fois que le hacker s'est connecté au serveur"
cut -d ' ' -f 1 $1 | grep '^127.0.0.1' | wc -l
echo ""
echo "6- Les 03 URLs les plus invoqué par le hacker. Format de la réponse: (nbOccurrences URL)."
grep '^127.0.0.1' $1 | cut -d ' ' -f 11 | grep '^https' | sort | uniq -c | sort -hr | head -n 3
echo ""
echo "7- Nombre de fois que le hacker s'est connecté avec un navigateur 'safari'"
grep -iw 'safari' $1 | grep '^127.0.0.1' | wc -l
echo ""
echo "8- Les systèmes et les versions des OS du hacker. Format de la réponse (nbOccurrences SE)."
grep '^127.0.0.1' $1 | grep '(.)' | cut -d '(' -f 2 | cut -d ')' -f 1 | sort | uniq -c | sort -hr
echo ""
echo "9- Nombre d'attaques d'origine sénégalaise subies par le serveur"
grep -E '^41.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}' $1 | wc -l
~
~
"log_server.sh" 32L, 1425C
32,58 A11

```

Capture écran sortie

```
devoir.md Dockerfile file log_server_docker.sh log_server.sh
osboxes@osboxes:~/formation/tempon/devoir_ngoune$ ./log_server.sh file/log-server.log
*****
** Script permettant de manipuler les logs du serveur **
*****

1- Nombre de ligne du fichier file/log-server.log
5672 file/log-server.log

2- Nombre de clients connectés
17

3- Nombre de clients ayant accédé avec succès
9

4- Nombre de clients ayant accédé avec message d'erreur
13

5- Nombre de fois que le hacker s'est connecté au serveur
626

6- Les 03 URLs les plus invoqué par le hacker. Format de la réponse: (nb0ccurences URL).
325 "https://spmi.gitechsn.com/application/navigation/dashboard/global"
87 "https://spmi.gitechsn.com/application/navigation/dashboard/administration/general"
62 "https://spmi.gitechsn.com/application/navigation/view/43"

7- Nombre de fois que le hacker s'est connecté avec un navigateur 'safari'
623

8- Les systèmes et les versions des OS du hacker. Format de la réponse (nb0ccurences SE).
373 Macintosh; Intel Mac OS X 10_15_7
139 Macintosh; Intel Mac OS X 11_0_1
111 Windows NT 10.0; Win64; x64

9- Nombre d'attaques d'origine sénégalaise subies par le serveur
3057
osboxes@osboxes:~/formation/tempon/devoir_ngoune$ _
```

IV- Dockerisation du script (PS : Lire le « README.md »)

- 🔗 Lien GITHUB du Dockerfile: <https://github.com/ngoupatrik/tempon> dans le dossier « devoir_ngoune »
- 🔗 Lien HUB de l'image Docker :
https://hub.docker.com/repository/docker/ngoupatrik/log_server