Nom: NGOUNE AGUEGUIA

Prénom : Noël Patrick

Devoir pratique de fin de Formation Linux

I- <u>Manipulation des logs</u>

- 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.
- O Nombre de lignes:

CMD: wc -l file/log-server.log

REP: 5672 file/log-server.log

O Nombre de clients connectés :

CMD: cut -d ' ' -f 1 file/log-server.log | sort -u | wc -l

REP: 17

O Nombre de clients qui ont accédé avec succès :

CMD: grep -E ' 2[0-9]{2} ' file/log-server.log | cut -d ' ' -f 1 | sort -u | wc -l REP: 9

O 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

O 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

O 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"

O 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

O 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

O 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

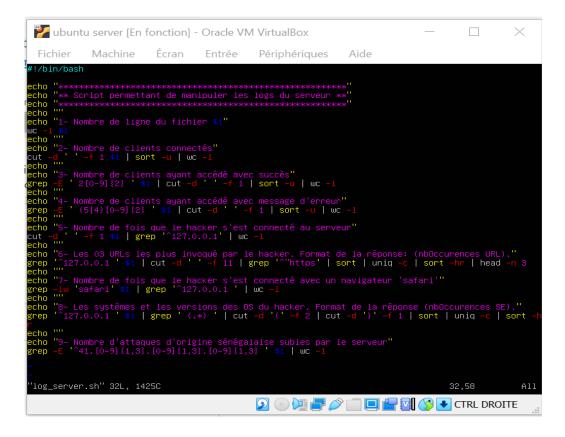
REP: 3057

III- Script Shell

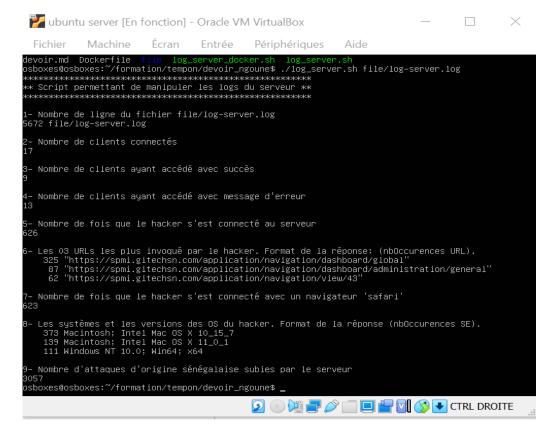
Enoncé : Script permettant de manipuler les logs serveur. Le script prendra en entrée le fichier de logs et donnera en sortie toutes les informations ci-dessus.

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

Capture écran script



Capture écran sortie



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

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