Rapport\_challenge\_secu

Baptiste Lanoue, Fabrice Petitfrere

08/03/2021

#logs <- read.table("C:/Users/bapti/Onedrive/Bureau/Securite\_challenge/logs\_fw-3.csv", sep=';', header=T)  
logs <- read.table("C:/Users/f.petitfrere.FRGINGER/Documents/Perso/Univ Lyon2/Challenge/Securite\_challenge/logs\_fw-3.csv", sep=';', header=T)  
names(logs)[1] <- "id"

print(head(logs))

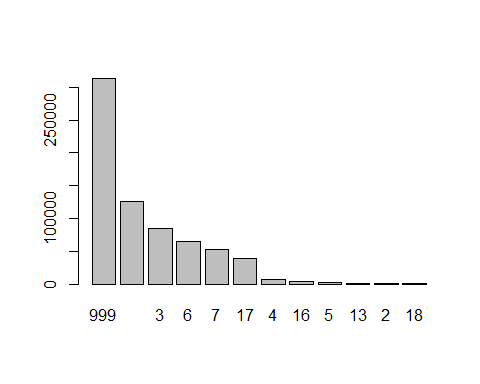
## id fw\_id datetime datetimestamp countryipsrc ipsrc  
## 1 2254336 1 2021-01-10 20:28:05 NA NA 45.129.33.10  
## 2 2254337 1 2021-01-10 20:28:06 NA NA 89.248.172.85  
## 3 2254338 1 2021-01-10 20:28:07 NA NA 192.35.168.236  
## 4 2254339 1 2021-01-10 20:28:09 NA NA 92.63.196.128  
## 5 2254340 1 2021-01-10 20:28:12 NA NA 92.63.196.128  
## 6 2254341 1 2021-01-10 20:28:16 NA NA 92.63.196.128  
## ipdst dstport proto action policyid tsrc tdst  
## 1 17.17.17.17 29857 TCP DENY 999 ens3 NA  
## 2 17.17.17.17 5552 TCP DENY 999 ens3 NA  
## 3 17.17.17.17 9581 TCP DENY 999 ens3 NA  
## 4 17.17.17.17 3711 TCP DENY 1 ens3 NA  
## 5 17.17.17.17 3711 TCP DENY 1 ens3 NA  
## 6 17.17.17.17 3711 TCP DENY 1 ens3 NA

Classement des règles les plus utilisés

rank <- table(logs$policyid)  
test <- rank[order(-rank)]  
  
library(ggplot2)

## Warning: package 'ggplot2' was built under R version 4.0.4

barplot(test)



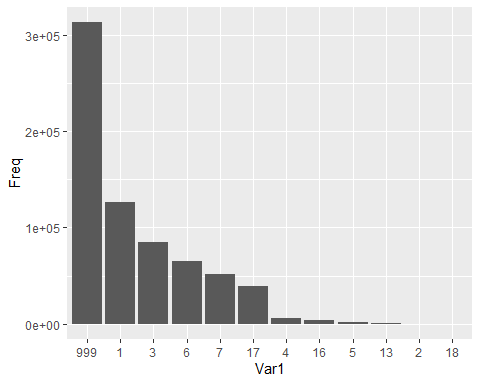
print(names(test))

## [1] "999" "1" "3" "6" "7" "17" "4" "16" "5" "13" "2" "18"

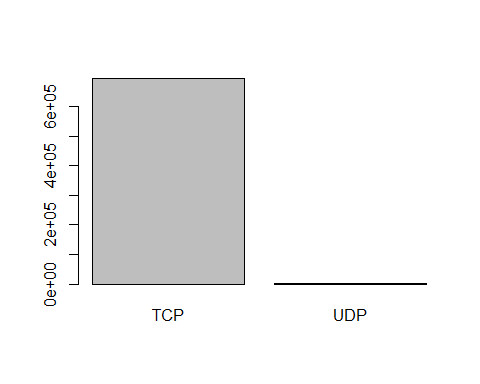
print(as.data.frame(test))

## Var1 Freq  
## 1 999 313289  
## 2 1 126337  
## 3 3 85273  
## 4 6 64802  
## 5 7 51973  
## 6 17 39302  
## 7 4 6391  
## 8 16 3611  
## 9 5 1954  
## 10 13 730  
## 11 2 373  
## 12 18 189

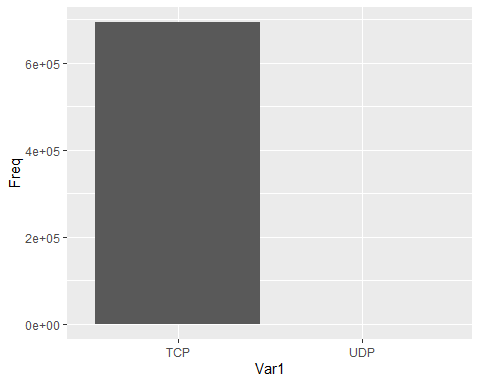
ggplot(as.data.frame(test), aes(x=Var1, y = Freq)) +   
 geom\_bar(stat="identity")



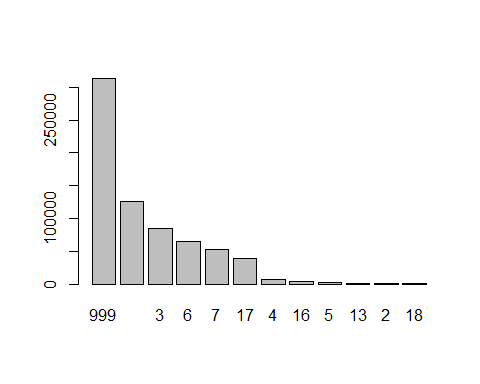
rank <- table(logs$proto)  
test <- rank[order(-rank)]  
barplot(test)



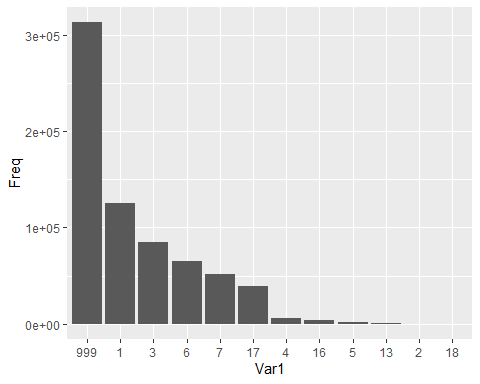
ggplot(as.data.frame(test), aes(x=Var1, y = Freq)) +   
 geom\_bar(stat="identity")



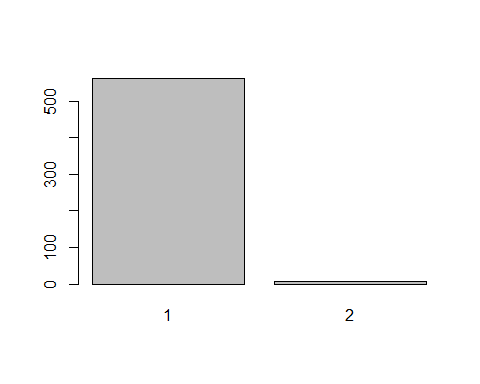
tcp <- logs[logs$proto =="TCP", ]  
  
rank <- table(tcp$policyid)  
test <- rank[order(-rank)]  
barplot(test)



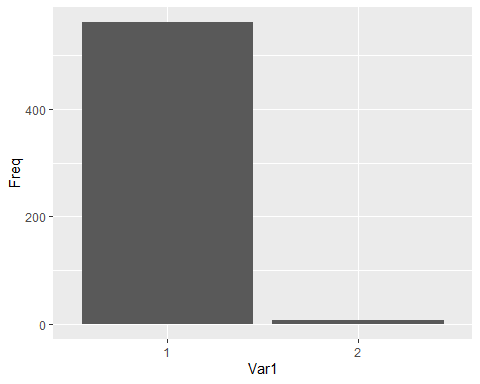
ggplot(as.data.frame(test), aes(x=Var1, y = Freq)) +   
 geom\_bar(stat="identity")



udp <- logs[logs$proto =="UDP", ]  
rank <- table(udp$policyid)  
test <- rank[order(-rank)]  
barplot(test)



ggplot(as.data.frame(test), aes(x=Var1, y = Freq)) +   
 geom\_bar(stat="identity")



udp <- logs[logs$proto =="TCP", ]  
  
analy <- table(udp$policyid, udp$dstport, udp$action)  
analy <- as.data.frame(analy)  
colnames(analy)<- c("policyid","dtsport","action","freq")  
  
library(dplyr)

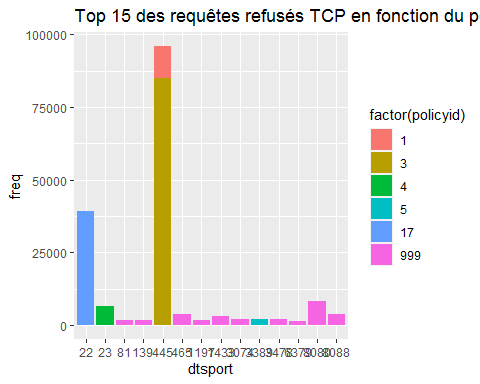
## Warning: package 'dplyr' was built under R version 4.0.3

##   
## Attaching package: 'dplyr'

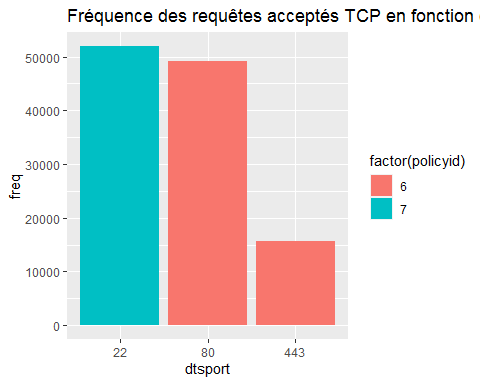
## The following objects are masked from 'package:stats':  
##   
## filter, lag

## The following objects are masked from 'package:base':  
##   
## intersect, setdiff, setequal, union

df1 <- filter(analy, freq > 0)  
  
DENY <- filter(df1, action == "DENY")  
NOTDENY <- filter(df1, action != "DENY")  
  
test <- DENY[order(-DENY[,"freq"]),]  
  
by\_port <- test %>% group\_by(dtsport)  
  
by\_port <- by\_port[0:15,]  
  
p <- ggplot(by\_port, aes(x = dtsport, y = freq, fill = factor(policyid)))  
p + geom\_bar(stat="identity") + ggtitle("Top 15 des requêtes refusés TCP en fonction du port et de la règle")



c <- ggplot(NOTDENY, aes(x = dtsport, y = freq, fill = factor(policyid)))  
c + geom\_bar(stat="identity") + ggtitle("Fréquence des requêtes acceptés TCP en fonction du port et de la règle")



logs$datetime <-strptime(logs$datetime, "%Y-%m-%d %H:%M:%S")

#logs$datetime$mday

Deny <- subset(logs, logs$action == "DENY" & logs$proto=="TCP")  
notDeny<- subset(logs, logs$action != "DENY" & logs$proto=="TCP")

plot(table(Deny$datetime$yday),type="s", col="orange", ylab = "Nbr de Hits")  
lines(table(notDeny$datetime$yday),type="s", col="blue", ylab = "Nbr de Hits")  
legend("right", legend=c("Permit", "Deny"),  
 col=c("blue", "orange"), lty = 1, cex=0.8)

