Poulard Quentin

Notice d’utilisation du programme Python

° Tout d’abord il faut choisir le fichier de nous voulons ouvrir pour lire les informations a l’intérieur. Dans l’exemple du programme nous ouvrons le fichier DumpFile.txt\* écris dans la ligne with open

try:

with open("DumpFile.txt", encoding="utf8") as fh:

res=fh.read()

except:

print("Le fichier n'existe pas %s", os.path.abspath('fichieratraiter.txt'))

ress=res.split('\n')

La ligne ress=res.split(‘\n) sert a enlever tout les \n ecrit en fin de ligne

-----------------------------------------------------------------------------------------------------------------------------

° Ensuite la ligne fichier=open va crée et ouvrir un fichier ( dans l’exemple valeur.csv ) qui est le tableau exel ou seront écrit toute les données récolté . On ouvre le fichier en mode écriture pour pouvoir y écrire ( W ).

La ligne événement correspond au nom des colonnes du tableau dans lesquelles seront écrite les données

tableau\_evenements=np.array([])

fichier=open("test.csv", "w")#test est le fichier d'arrivée des extractions

evenement = "DATE ; SOURCE ; PORT ; DESTINATION ; FLAG ; SEQ ; ACK ; WIN ; OPTIONS ; LENGTH" #intitulé de mes colonnes

fichier.write(evenement + "\n") #écriture des titres dans le tableur

-----------------------------------------------------------------------------------------------------------------------------

° On lance le programme pour qu’il parcours toute les lignes

for event in ress:

if event.startswith('11:42'): #

Condition qui fait que si la ligne event ( peut l’appeler comme on veut ) commence par l’heure 11 :42 le programme continue a parcourir les lignes . Dans notre exemple toute les lignes commencent par 11 :42 , mais si vous voulez qu’il les parcoures toutes , metter une autre variable qui est toijours présente dans vos ligne

seq = ""

heure1 = ""

nomip = ""

port = ""

flag = ""

ack = ""

win = ""

options = ""

length = ""

On déclare toute nos variable qui correspondent au valeur qui iront dans chaque colonne. A chaque fois qu’une ligne est finis , cela remets les valeurs vide

-----------------------------------------------------------------------------------------------------------------------------

Ont rempli la premier colonne ( la colonne date )

texte=event.split(" ") On sépare les texte de la ligne a chaque fois qu’il y a un espaces car dans notre fichier la date est écrite en premier et a la fin de la date il y a un espace puis les autres données

heure1=texte[0] On récupère la première partie qui a été diviser par les espaces ( la premier commence a 0 ) est on l’affecte a la variable heure

Pour la deuxième colonne ( la colonne source )

texte=event.split(" ") On sépare la le texte de la ligne a chaque espace car il y a des adresses source qui n’ont pas de points comme les adresse IP ( exemple : BP-Linux8 , il n’y a pas de point mais il est séparer des autres donnée avec un espace juste après

AdrIP1=texte[2].split(".") On prend la 3 ème partie qui est séparer par des espaces ( car il y a un bien 2 espaces pour arriver a la source : 11:42:04.766694 IP BP-Linux8 ) et on la sépare aussi par des point pour les adresse IP.

if len(AdrIP1) == 2:

nomip=AdrIP1[0]

if len(AdrIP1) == 3:

nomip=AdrIP1[0]+ "." +AdrIP1[1]

if len(AdrIP1) == 4:

nomip=AdrIP1[0]+ "." +AdrIP1[1]+ "." +AdrIP1[2]

if len(AdrIP1) == 5:

nomip=AdrIP1[0]+ "." +AdrIP1[1]+ "." +AdrIP1[2]+ "." +AdrIP1[3]

if len(AdrIP1) == 6:

nomip=AdrIP1[0]+ "." +AdrIP1[1]+ "." +AdrIP1[2]+ "."+AdrIP1[3]+"."+ AdrIP1[4]

-----------------------------------------------------------------------------------------------------------------------------

° Pour la colonne flag

texte=event.split("[") On sépare ( coupe ) a partir du premier crochet dans la ligne car le flag est écrit dans les crochets

if len(texte) > 1:

flag1=texte[1].split("]") on prend la partie après le premier crochets et on coupe au deuxième crochet

flag=flag1[0] pour avoir avoir le flag il faut prendre la partie a gauche de deuxième crochet , donc [0] ( car 0 est la premier partie )

Pour la colonne séquence

texte=event.split(",") On sépare (coupe ) a la virgule car la séquence est écrite après la première virgule

if len(texte) > 1: #s'il y a plus de 1 partie à partir du crochet

if texte[1].startswith(" seq"): Si le texte [1] ( texte écrit après la virgule , [1] car c’est le deuxième bout après la séparation par « , » commence par " seq"

seq1=texte[1].split(" ") on coupe à l'espace et on prend le texte juste après

sequence=seq1[2] On a 2 parties séparer par « : » entre le split ',' et ce que le numéro de séquence en entier

--------------------------------------------------------------------------------------------------------------------------------------

Pour la colonne ack

if len(texte) > 2:

if texte[2].startswith(" ack"): Si le texte [2] ( texte écrit après la deuxième virgule ( troisième partie)) de la séparation par la virgule commence par "ack"

ack1=texte[2].split(" ") on coupe à l'espace et on prend le texte juste après

ack=ack1[2] On a 2 parties entre le split ',' et ce que je recherche

Sur certaine ligne il ni a pas de ack , il faut donc prendre la partie [1] d’après la séparation par la virgule

if texte[1].startswith(" ack"):

ack1=texte[1].split(" ") on coupe à l'espace et on prend le texte juste après

ack=ack1[2] On a 2 parties entre le split ',' et ce que je recherche

------------------------------------------------------------------------------------------------------------------------------------

Pour la colonne WIN

if len(texte) > 3: si le nombre de partie du texte séparée est supérieur à 3

Si il y a le ack , il faut prendre la 3 éme partie après la séparation par la virgule

if texte[3].startswith(" win"): Si le texte [3] commence par " win"

win1=texte[3].split(" ") on coupe à l'espace et on prend le texte juste après

win=win1[2] On prend le texte après l'espace pour avoir le numéro et n’on pas écrit WIN dans le tableau

Si il ny a pas la ack , on prend la deuxième partie

if texte[2].startswith(" win"): Si le texte [2] commence par " win"

win1=texte[2].split(" ") on coupe à l'espace et on prend le texte juste après

win=win1[2] On prend le texte après l'espace pour avoir le numéro et n’on pas écrit WIN dans le tableau

------------------------------------------------------------------------------------------------------------------------------------

Pour la colonne option

texte=event.split("[") On sépare a partir du « [»

if len(texte) > 2: +

options1=texte[2].split("]") On part de la séparation du crochet [ et au prend la troisième partie ( texte [2] ) après la séparation pour arriver a l’endroit ou est écrit option

options=options1[0] on prend la première partie ( partie a gauche du 2 ème ] ) pour avoir l’option

------------------------------------------------------------------------------------------------------------------------------------

Pour la colonne lenght

Si il y a la partie option su la ligne

texte=event.split("]")

if len(texte) > 2: vérifier le nombre de partie (split au crochet)

length1=texte[2].split(" ") on part du premier "[" et ce qu'on recherche est bien dans texte [2]. On split à l'espace pour avoir que le nombre

length=length1[2] On prend la partie 2 après les espaces pour avoir le nombre

SI il ya a pas la partie option sur la ligne

texte=event.split(",")

if len(texte) > 3:

if texte[3].startswith(" length"): Si ça commence par " length"

length1=texte[3].split(" ") on coupe à l'espace

length=length1[2] On veut bien le "2" pour avoir que le nombre (texte [1] avant l'espace c'est le mot "length").

------------------------------------------------------------------------------------------------------------------------------------

Pour que le programme s arrete et écrit dans le tableau

if event.startswith("11:42:55.536521") : 11:42:55.536521 est l’heure de la dernière ligne du fichier , donc si la ligne commence par sa

prog=0 on arrete la boucle et de parcourir les lignes du fichier txt

evenement=heure1+";"+nomip+ ";" +port+ ";" + nomip2+ ";"+flag+ ";" +sequence+ ";" +ack+ ";" +win+ ";" +options+ ";" +length

fichier.write(evenement + "\n") on écrire "evenement" dans le csv et \n pour revenir à la ligne (pour ne pas écrire sur la même ligne)

------------------------------------------------------------------------------------------------------------------------------------

Pour compter le nombre de fois que chaque addresse de source reviens

if nomip=="BP-Linux8": Si la variable de l’ip de la source est égale a la condition on ajoute 1 a la variable a qui nous servira a faire les graphique

a = a + 1

if nomip=="ns1.lan.rt":

b=b+1

if nomip=="190-0-175-100.gba.solunet.com.ar":

c=c+1

x=["www.aggloroanne.fr","ns1.lan.rt","BP-Linux8","190-0-175-100.gba.solunet.com.ar","par21s04-in-f4.1e100.net","mauves.univ-st-etienne.fr","par10s38-in-f3.1e100.net","par21s23-in-f10.1e100.net","par21s23-in-f2.1e100.net"] On met en abscisse la nom des adresse source

y=[e,b,a,c,d,f,g,h,i] On met en ordonnée les variable qui correspondent on nombre de fois que chaque source a envoyer quelque chose

fig, ax = plt.subplots(figsize=(20,10)) Choisi la taille du graphique

ax.set\_yticks(np.arange(0,4000,400)) Choisi la valeur max et min de l’ordonnée ainsi que le nombre d’espace entre chaque repère ( 400 – 0-400-800-1200 … )

ax.set\_title ("DDOS", color="#000000", y=1.05) titre du graphique ainsi que couleur et taille

fig.autofmt\_xdate(rotation=90) inclinaison du nom de l’abscisse

ax.bar(x, y)

fig.savefig("longueur.png", dpi=300 , bbox\_inches="tight") enregistrement du graphique en mode png pour pouvoir le récupérer dans la page html