Notice d’utilisation

Python script:

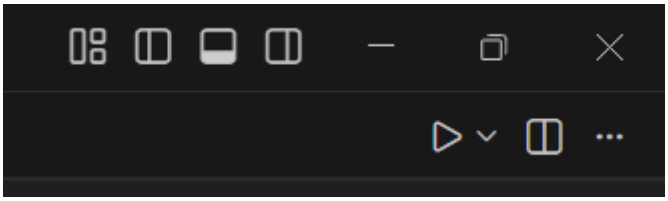
REQUIREMENTS:

To use the script that analyze a TCPDump file, you must have downloaded the MarkDown library with the command “pip install markdown” or “python -m pip install markdown”. Of course, you must have Python installed

The script is simple to use, but you must have checked that you downloaded it and the TCPDump file, then you open the python file and go all the way down here:

You have almost finished the job already, you must change the last line by the emplacement of your TCPDump file, mine is named DumpFile.txt in my Documents.

Once you did that, run the script:



And your browser will opend a “.html” file generated by the script where you can choose which file you want to see:

There are also statistics under about the events on the TCPDump file.

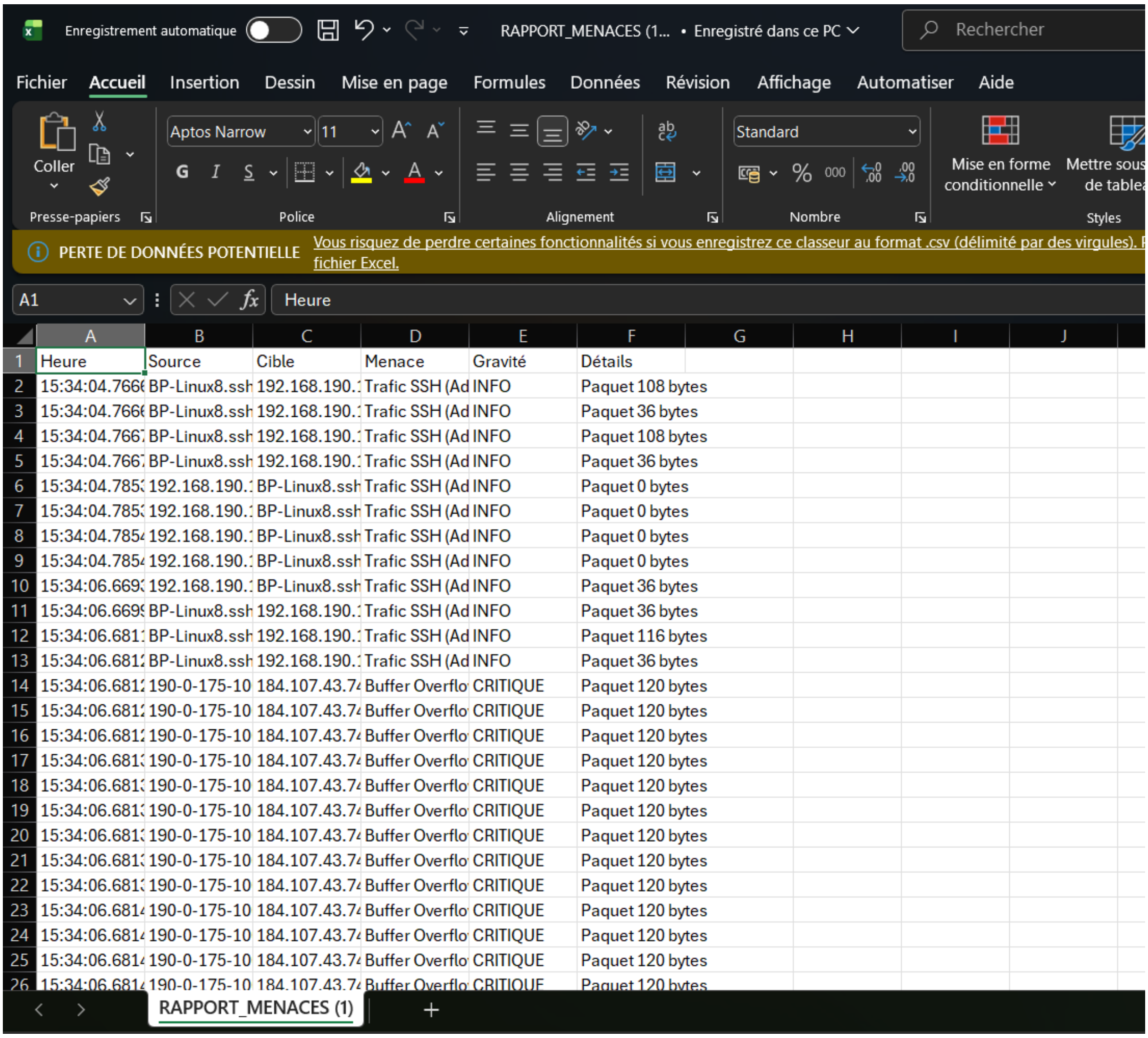
Excel:

REQUIREMENTS:

- Excel

First, click on the “CSV” button on the html page:

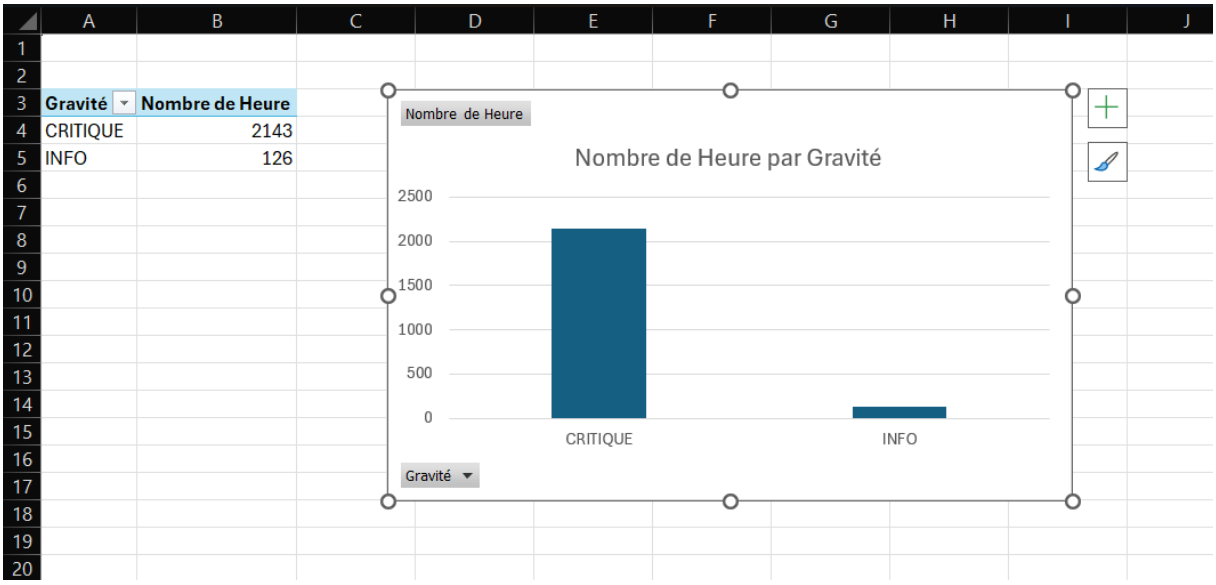
It will then ask you where you want to download it. Download it and then open it.



	A	B	C	D	E	F
1	Heure	Source	Cible	Menace	Gravité	Détails
2	15:34:04.766	BP-Linux8.ssh	192.168.190.	Trafic SSH (Ad	INFO	Paquet 108 bytes
3	15:34:04.766	BP-Linux8.ssh	192.168.190.	Trafic SSH (Ad	INFO	Paquet 36 bytes
4	15:34:04.767	BP-Linux8.ssh	192.168.190.	Trafic SSH (Ad	INFO	Paquet 108 bytes
5	15:34:04.767	BP-Linux8.ssh	192.168.190.	Trafic SSH (Ad	INFO	Paquet 36 bytes
6	15:34:04.785	192.168.190.	BP-Linux8.ssh	Trafic SSH (Ad	INFO	Paquet 0 bytes
7	15:34:04.785	192.168.190.	BP-Linux8.ssh	Trafic SSH (Ad	INFO	Paquet 0 bytes
8	15:34:04.785	192.168.190.	BP-Linux8.ssh	Trafic SSH (Ad	INFO	Paquet 0 bytes
9	15:34:04.785	192.168.190.	BP-Linux8.ssh	Trafic SSH (Ad	INFO	Paquet 0 bytes
10	15:34:06.669	192.168.190.	BP-Linux8.ssh	Trafic SSH (Ad	INFO	Paquet 36 bytes
11	15:34:06.669	BP-Linux8.ssh	192.168.190.	Trafic SSH (Ad	INFO	Paquet 36 bytes
12	15:34:06.681	BP-Linux8.ssh	192.168.190.	Trafic SSH (Ad	INFO	Paquet 116 bytes
13	15:34:06.681	BP-Linux8.ssh	192.168.190.	Trafic SSH (Ad	INFO	Paquet 36 bytes
14	15:34:06.681	190-0-175-10	184.107.43.7	Buffer Overflo	CRITIQUE	Paquet 120 bytes
15	15:34:06.681	190-0-175-10	184.107.43.7	Buffer Overflo	CRITIQUE	Paquet 120 bytes
16	15:34:06.681	190-0-175-10	184.107.43.7	Buffer Overflo	CRITIQUE	Paquet 120 bytes
17	15:34:06.681	190-0-175-10	184.107.43.7	Buffer Overflo	CRITIQUE	Paquet 120 bytes
18	15:34:06.681	190-0-175-10	184.107.43.7	Buffer Overflo	CRITIQUE	Paquet 120 bytes
19	15:34:06.681	190-0-175-10	184.107.43.7	Buffer Overflo	CRITIQUE	Paquet 120 bytes
20	15:34:06.681	190-0-175-10	184.107.43.7	Buffer Overflo	CRITIQUE	Paquet 120 bytes
21	15:34:06.681	190-0-175-10	184.107.43.7	Buffer Overflo	CRITIQUE	Paquet 120 bytes
22	15:34:06.681	190-0-175-10	184.107.43.7	Buffer Overflo	CRITIQUE	Paquet 120 bytes
23	15:34:06.681	190-0-175-10	184.107.43.7	Buffer Overflo	CRITIQUE	Paquet 120 bytes
24	15:34:06.681	190-0-175-10	184.107.43.7	Buffer Overflo	CRITIQUE	Paquet 120 bytes
25	15:34:06.681	190-0-175-10	184.107.43.7	Buffer Overflo	CRITIQUE	Paquet 120 bytes
26	15:34:06.681	190-0-175-10	184.107.43.7	Buffer Overflo	CRITIQUE	Paquet 120 bytes

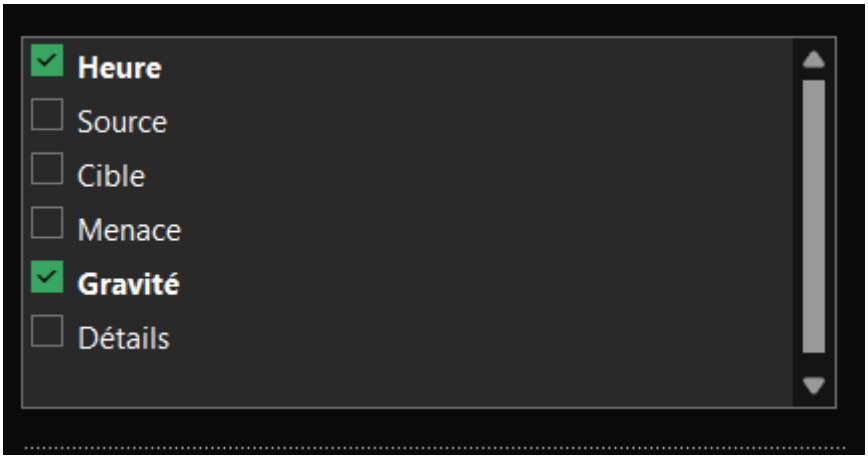
Next step, on “INSERTION” and “recommended graphics”

This will appear:

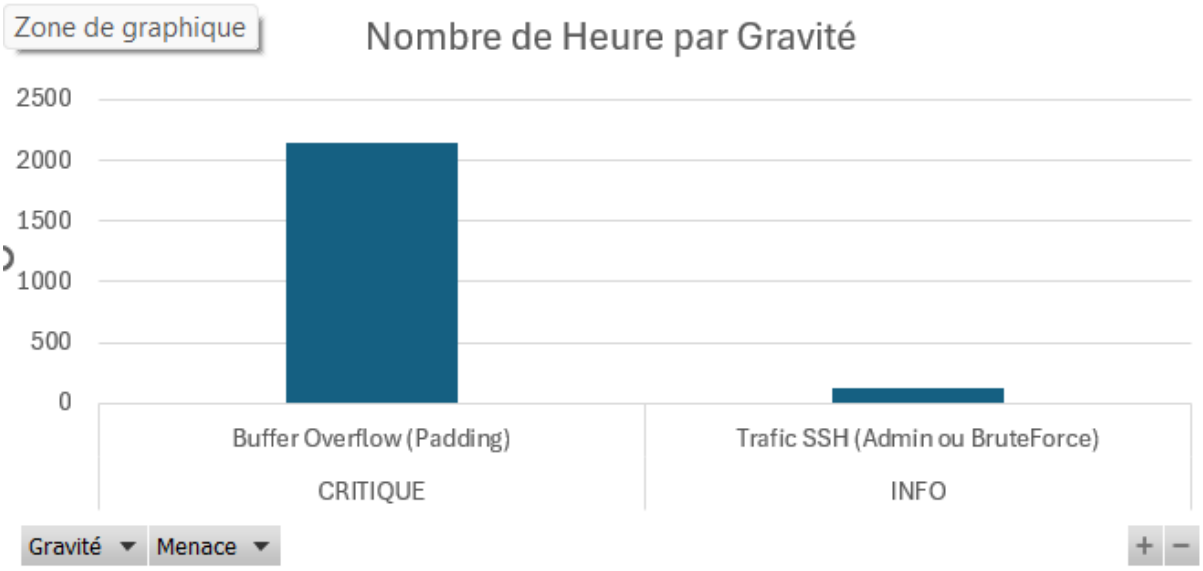


Gravité	Nombre de Heure
CRITIQUE	2143
INFO	126

Now look on the right of the application and select “menace”:



Now your graphics should look like that:



Now you know everything to use these tools.