What is this about?

It is about How can we automate the recommendation of attack steps/sequences? How to quantify chances of success and impact of each step given preferences (e.g., stealth vs impact)?

In order to automate. Needs to have information first. Use EdRange as example and vulnerability scans such as OpenVAS for automation.

OpenVAS output the results as pdf and/or xml. It seems like xml is better to convert into machine understand language.

Use python for machine learning and xml converting.

For some unknown reason outlook unable to send xml files to myself. Pdf files is fine. So, I will use GitHub to get the scans results to my real computer instead of the VM.

Note: the free version of OpenVAS is only able to use in VM.

Got a new PC. Setting everything up again….

At least it runs very smooth.