Intro

For this section, we will be scanning and enumerating a vulnerable virtual machine called Kioptrix.

It seems that we already know quite a bit of this. Lets make sure to make lists of what we are searching for, what should be prioritized, and what should be left for later. The outcome here should be a list telling the step-by-step of what and how should the enumeration and scanning be done.

Here we are going to have a section for nmap, one for HTTP/HTTPS, one for SMB, and one for SSH. Remember that all this is going to represent the Kioptrix virtual machine we are attacking.

We might have a section at the very end briefing all the take aways for each section, if the sections become too long and crowded.

Without further ado, lets get started!