Links that I used

1. <https://forum.hackthebox.eu/discussion/1730/a-script-kiddie-s-guide-to-passing-oscp-on-your-first-attempt>
2. <https://oscp.infosecsanyam.in/one-page-methodology>
3. <https://guide.offsecnewbie.com/privilege-escalation/windows-pe>
4. Join this discord link today, this link expires in 24 hours = https://discord.gg/6BpCsc

Before Buying PwK labs ( 3-4 months )

1. (1 week) Get an idea of
   1. What questions are there in the exam, like how many points each question and about what type of questions. (This you will find in blogs that people write after passing OSCP. e.g. [link](https://forum.hackthebox.eu/discussion/1730/a-script-kiddie-s-guide-to-passing-oscp-on-your-first-attempt).
   2. Like this link try to find other links that helps you understand what actually people did and how they prepared.
2. (1 months - Vulnhub) Once you have an idea, start preparing your own pentesting methodology.
   1. Now just jump right into doing boxes from HTB and Vulnhub. Note that do only those boxes that are labeled “OSCP like boxes” [link](https://www.google.com/search?client=firefox-b-d&q=oscp+like+boxes). One list for “OSCP like boxes for HTB” and other list is for “OSCP like boxes for Vulnhub”.
   2. Start will Vulnhub boxes, as vulnhub is free. Then once Vulnhub boxes are done move to HTB boxes, but you need to buy subscription (1K per month)
   3. Start with only “Linux Boxes” and “Windows Boxes”, the boxes are labelled in the list. Leave the “More challenging than OSCP”.
   4. During this phase you will stuck up like in every other step, so I would suggest to not to look for “Walkthrough” of the lab right away. The walkthrough must be your last option when nothing is working and you are wasting your lot of time.
      1. **Methodology**: methodology is like a sequence of steps and check when you first see a box, like to check whether a box is linux or windows could also be a methodology step. Refer the end of my document to see my methodology.
      2. Create a port wise like of steps. Like, if port 80 is open what checks will you perform to find vulnerability. similarly for all the well known ports.
      3. Here you could take help of blogs like this [link](https://oscp.infosecsanyam.in/one-page-methodology).
      4. Like this there are many such blogs and try to read as many such blogs as possible and create your own methodology, and don’t panic, because these blogs will be like 70-80% same just written in different fashion for easier understanding. Have a habit to read every blog and bookmark the ones that you feel are the best.
3. (1 month - Vulnhub) After 2 months, even if your methodology seems incomplete move to the hard OSCP boxes. “More challenging than OSCP”. Note that, this is not optional step, you need to do “More challenging than OSCP” boxes to pass, as some part of it definitely is in the exam.
   1. Complete all the boxes in “OSCP like boxes” list. Note, this list gets updated so try to find a list which have more boxes.
4. ( 1 month – HTB) Buy HTB subscription (1K per month). Start with the “Windows boxes” and “Linux boxes” from the list.
5. ( 1 month – HTB hard boxes) Now complete the rest of “More challenging than OSCP boxes from HTB.

Buy PwK

1. (1 month) Note that you need to do all the exercises from the PwK pdf + you need to crack 10 boxes with different vulnerability, and send a Lab Report to get extra points. All people do this Lab Report.
2. Do not go through the PwK pdf, its useless if you ask me. Directly go to the lab, and try to solve the boxes in PwK lab environment.
3. Like do all the exercises and crack 10 machines in 3-4 days. And then dedicate all the remaining 26 days to crack all other boxes, there are about 80-120 boxes to crack.
4. After the 30 day period is over, schedule exam as quickly as possible (given you feel comfortable that you can crack it). Note you could re-schedule your exam 2 times.

My methodology

( after 4-5 months of constant modification I created it )



