Part 3:

NO 1

We can read “/usr/share/nmap/nmap-services” in python and write it into a txt file. Then we use full scanner to scan the open port. And using the open ports we scanned as key value to search if the value is in the output text file.

NO. 2

we can add a random function in python. and put the range of the ports in to an array to list. Then you randomly scan the port from the array/list. After you scan it, you move it out from the array/list. In this way, you can randomly scan all the ports in your input port range.

NO. 3

Since its due in 30 mins. I think I don’t have time to modified yours. I would say there are multiple ways to detest the half scan such that we can use network intrusion detection systems and firewalls are usually configured to detect scans