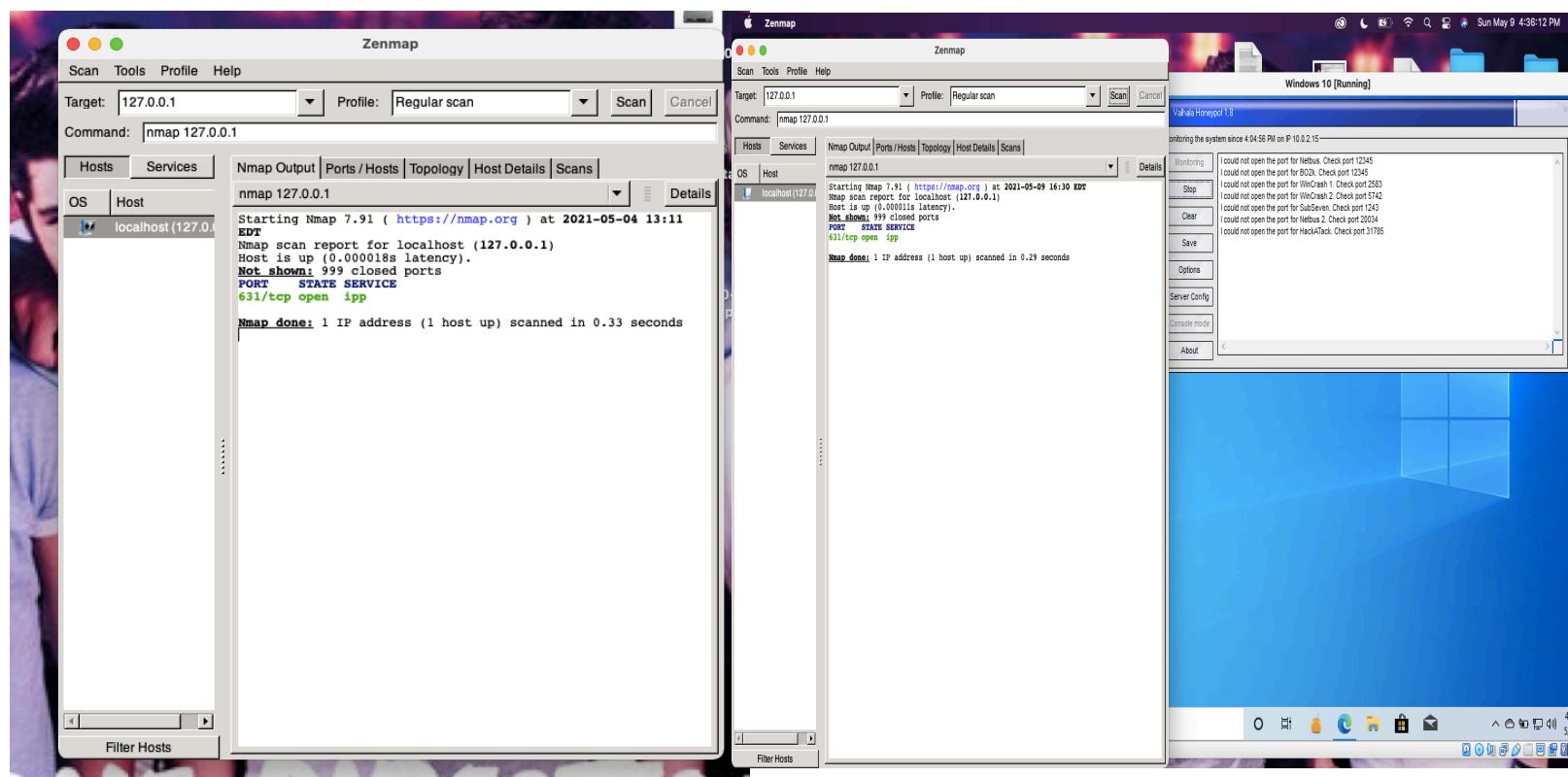
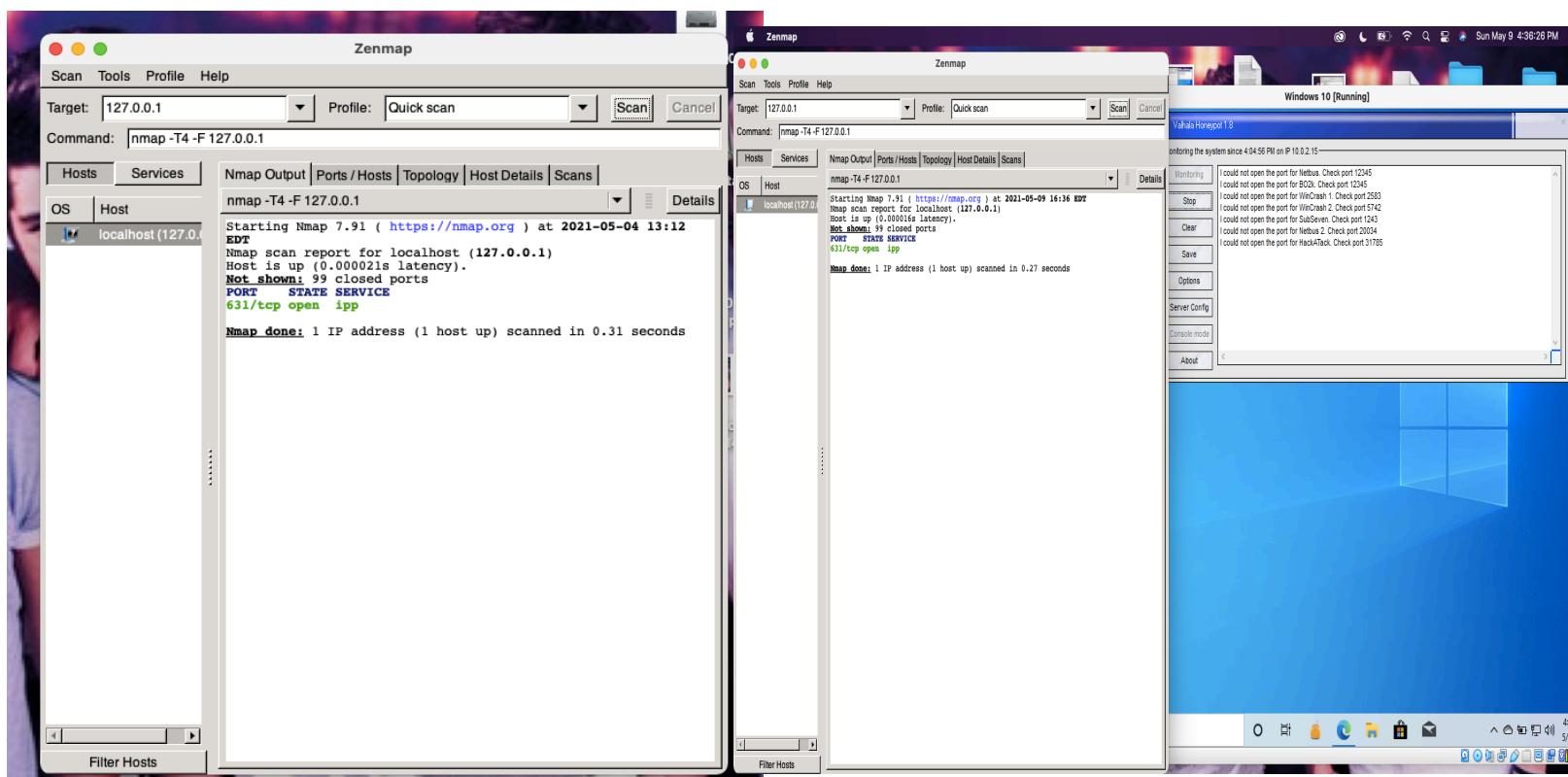


Candice Morris
5/11/21

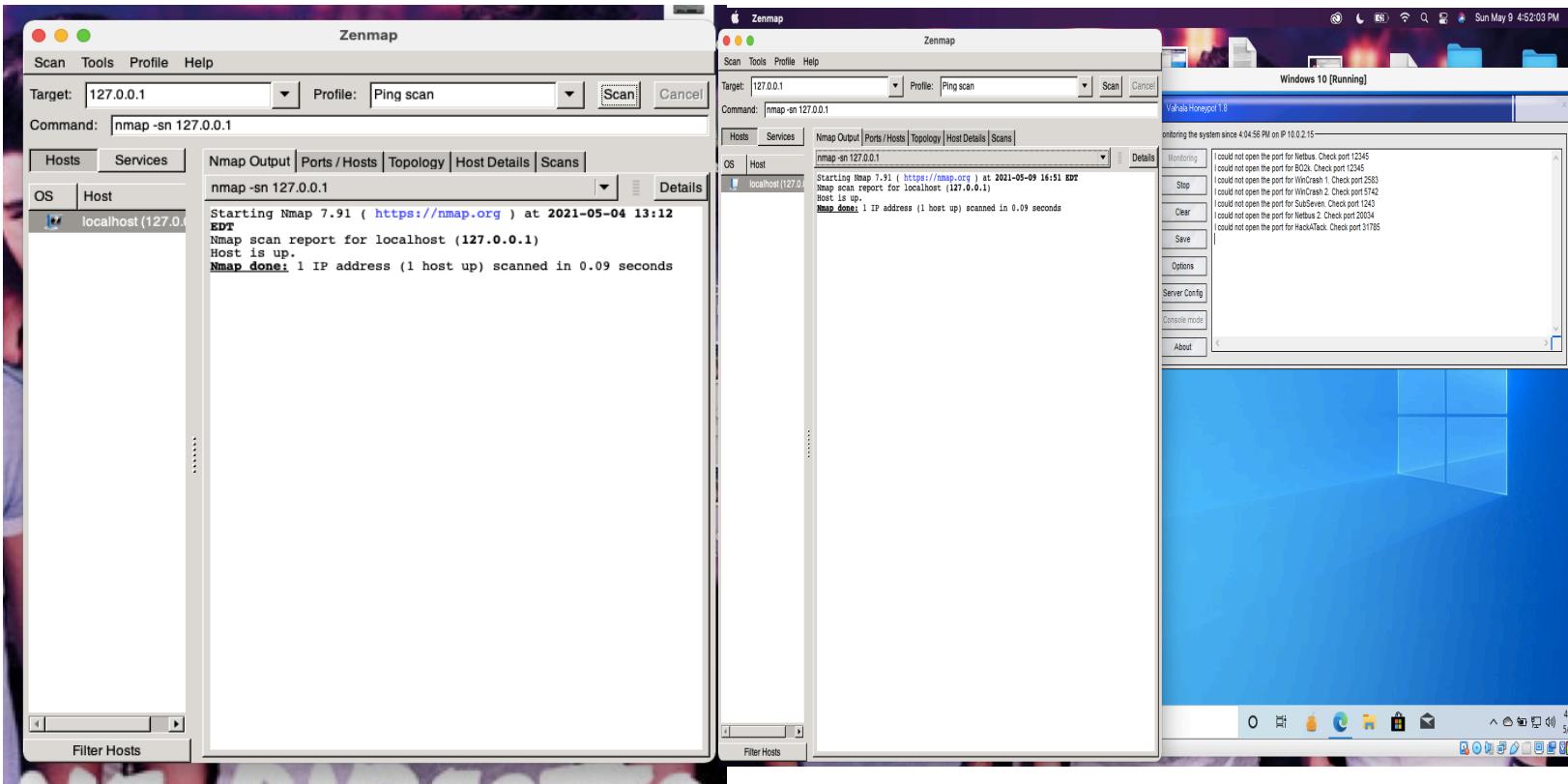
Regular Scan



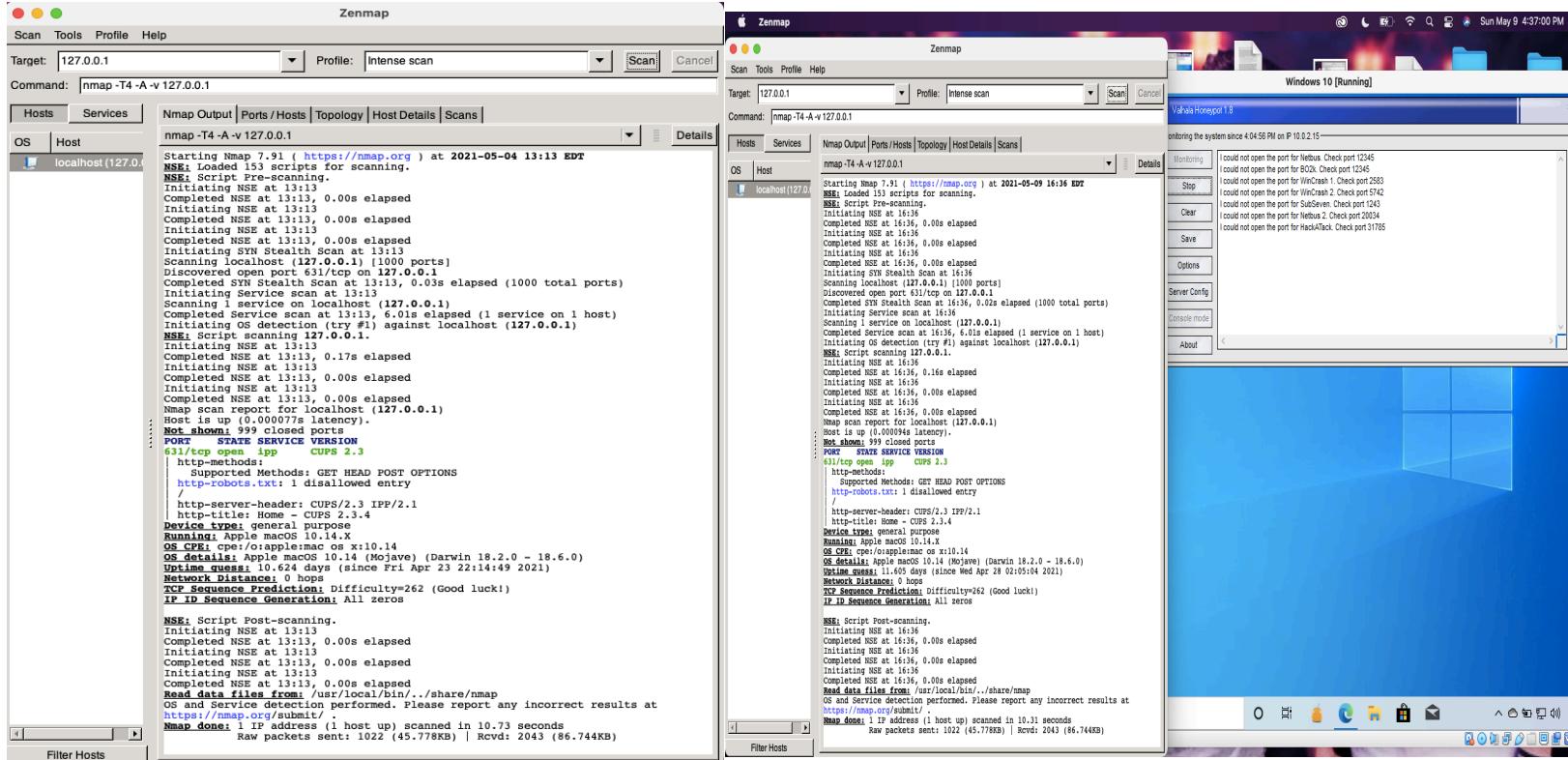
Quick Scan



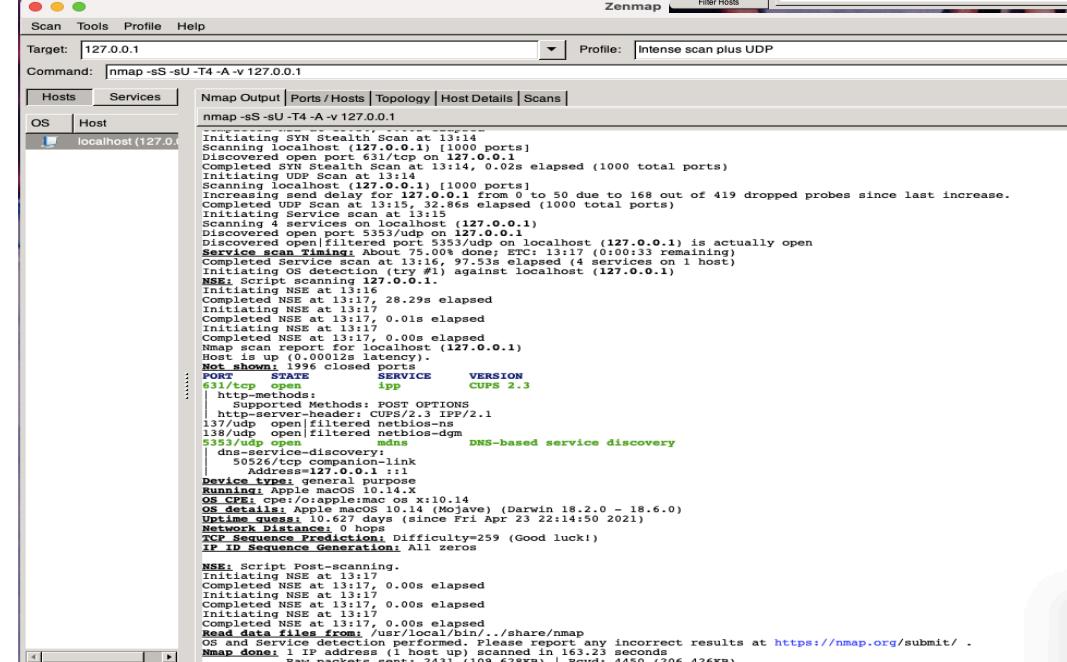
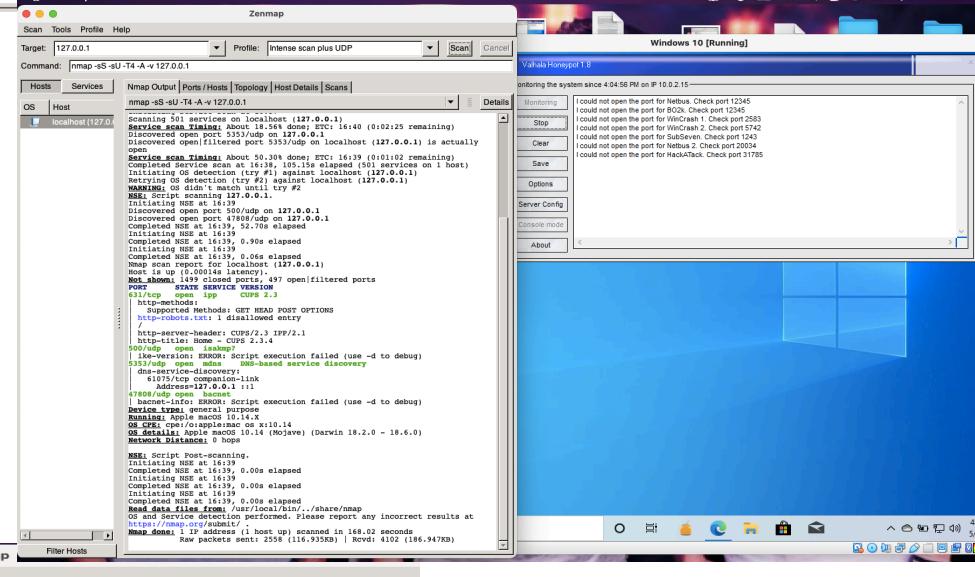
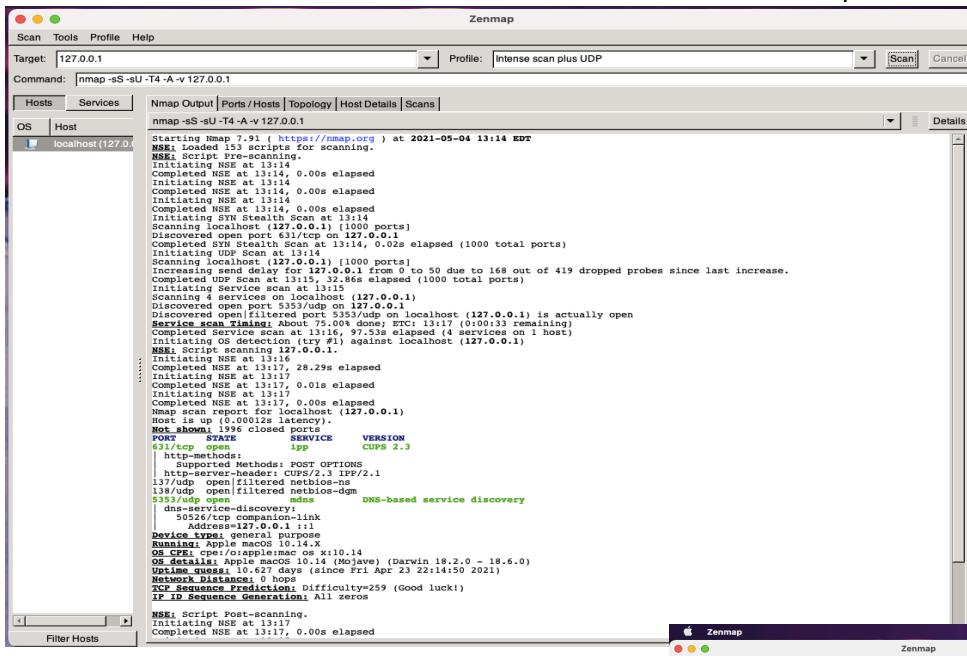
Ping Scan



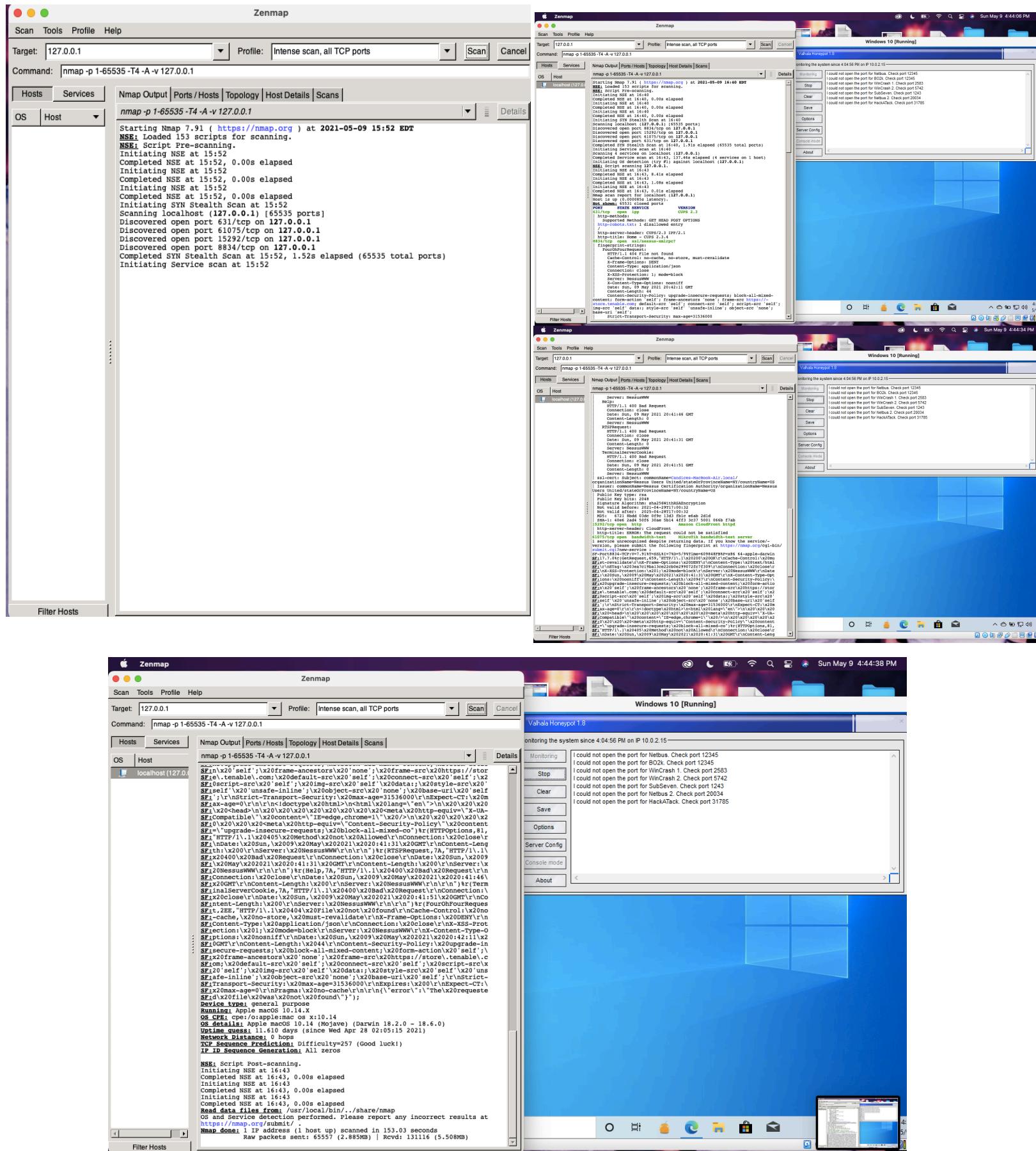
Intense Scan



Intense scan plus UDP



Intense scan with TCP



When running Valhalla and Zen map, the screenshots are compared to each other with nothing running and having a single host on every scan. While, on the first four scans it was similar to the same scans that were run in comparison and didn't bring up anything in those scans. In the last two intense scans, it brought up the other ports that were open; there was a website, amazon cloud, and etc. that showed up within the scans. The regular scan scanned nothing but the ipp service for each service that I deployed. The quick scan scanned nothing but the ipp service for each service that I deployed as well. the intense scan scanned nothing but the ipp services as well and nothing else. The only two other scans; the intense scan plus UDP and the intense scan, all TCP ports were the only two that scanned something else along with the ipp service. For the UDP ports that opened were a mdns service, and two other services that were open but couldn't be executed. It was an http and a bacnet service. For the TCP ports it scanned http services, ssl services and bandwidth services.

"What zenmap scan would be the most efficient/fastest way to determine all of the hosts that are available for pen testing on a given network (like 10.1.10.X in WaveLAN) and explain why".

- I believe the fastest and most accurate zenmap scan to run on a network like 10.1.10.X, would be an intense scan because even though it's not as fast as a quick scan or a regular or ping scan it is the most accurate to me to run on this network. For me when running a scan on any network, I found that the intense scan was the most effective scan for me to run compared to the other scans; plus, it also provided more information in the scan than the others did as well.