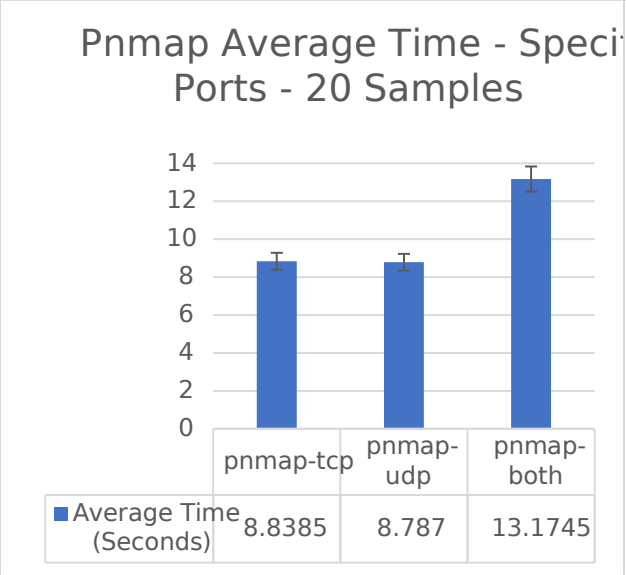
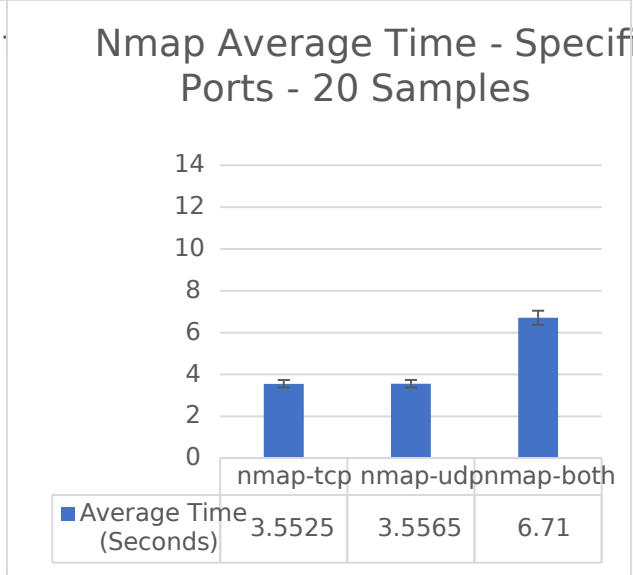
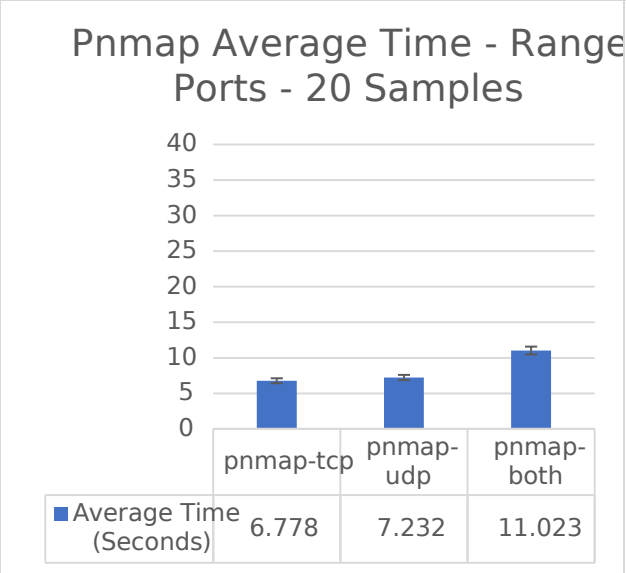
Tests and test results

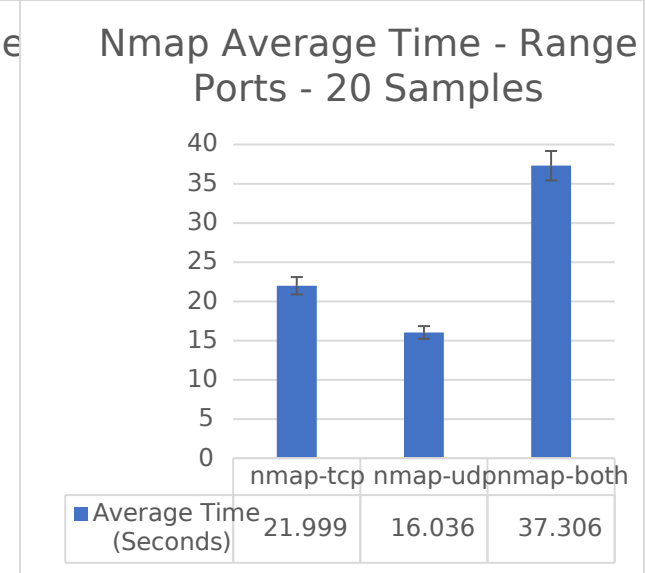
Specific Ports: 20, 80, 443

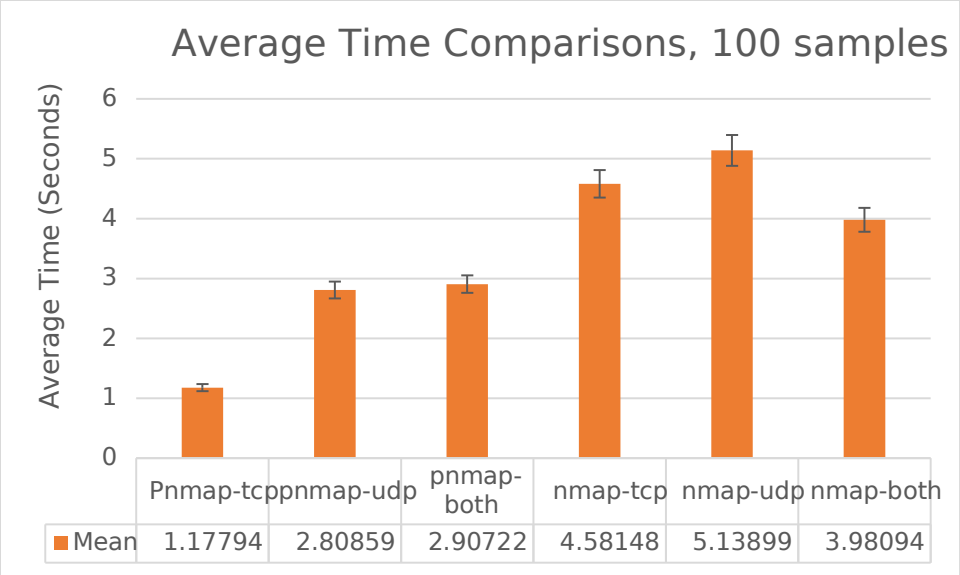




Range of Ports: 1-1024, inclusive







Analysis of results

20-sample tests were run on a separate system than the 100-sample tests.

The times for pnmap as compared to nmap are as shown in the chart above. Pnmap's performance with predetermined ports was generally slower than that of nmap (approximately 40 40.47%, and 50.93% slower than nmap for TCP, UDP, and both, respectively), with mild instability resulting in cases with failed name searches (~1/4 cases). In tests with a given range of ports, ho pnmap resulted in faster times than nmap (approximately 30.81%, 45.1%, and 29.54% faster tha nmap), though this could be linked to additional firewall avoidance features in nmap.

Standard deviation is slightly higher in simultaneous scans for UDP and TCP. This is likely a of early finishing of one scan before the other, as the timing will vary between UDP and TCP.

A secondary set of data was prepared for our 100-sample test. As noted above, there is tre longer times for nmap as opposed to pnmap.

While it may be expected that TCP may take longer than UDP due to the 3-way handshake, results show that TCP generally tends to run at approximately the same speed or faster than UDP may be explained by UDP's usual procedure in nmap: to determine that a port is open, it must *no* receive an ICMP port unreachable message, and therefore must wait through the entire allotted ti period before labelling the port. TCP by comparison needs only to receive confirmation via handsh