1. Pick 3 nmap scan techniques we did not cover in class. Describe how each scan works and when it may be more useful than other scan techniques.

**-sI is a zombie host scan which allows a truly stealthy scan in which your IP address is never sent to the target (you seemingly need to specify an IP that is available/up). This is even more stealthy than -sS**

**--scanflags allows you to bypass IDS by crafting specific TCP flags.**

**-sW is a TCP window scan, which it seems to send an ACK request (similar to the sA scan), however it determines open ports if the window size is positive (from the RST packet). This is useful to determine what the firewall is filtering. However, this is an exploit for a very few number of systems currently on the internet.**

1. Some of the nmap scan techniques you read about take advantage of problems with protocol specifications OR the way they the protocols are implemented by software/hardware companies. Identify and describe at least 2 specific problems that arise from protocol specifications or their implementations. For each problem you identify, think about the root cause of the problem and explain how you would fix it if you were the protocol author or protocol implementer.

**-sW takes advantage of having a positive window size when certain ports are open and return a RST packet. The fix here would be to make sure all RST packets have a consistent window size, whether that is positive or not.**

**-sM takes advantage of a problem with BSD systems dropping packets if the port is open. A fix for this would be to (again) have a consistent response to events that the system doesn’t understand how to handle. I think in this case, all packets might want to be dropped instead of figuring out whether or not to send a RST packet.**