

Reflection paper 2

For the past week and a half, I have been part of a team conducting vulnerability scans on the devices in our network. We typically set up the scans at the end of the day and let them run overnight due to the large number of devices we manage. This way, the results are ready for review the next morning, allowing us to identify what needs to be patched. Running the scans overnight also minimizes disruptions if a system goes down or crashes this also allows for end users to not be affected during their working hours. There was not any major vulnerabilities that needed to be patched because we are aware of the systems that we have in our network and we have a threat intelligence team that keeps track of any major vulnerabilities that could affect us but we do the scans just in case we miss something or for example if there is a mid level vulnerability that will give access to a system but attacker has to be physically present and they can't do it over the network we will patch those vulnerabilities but they do not take priority over an vulnerability that can be done over the network and where the attack complexity is low.

In conclusion, from this experience I have learned more about vulnerability and patch management and why it is important for the organization to keep the devices updated because attackers are always looking for a way in and one major way we can prevent this is by making sure all the devices in our network are updated from the latest vulnerabilities.