1) Could you highlight some commonly used tools and methods for conducting vulnerability scans? How do these tools assist cybersecurity professionals in identifying and assessing vulnerabilities within a network or system?

   Answer: Some of the commonly used tools for conducting vulnerability scans are Nessus and Nmap. Nessus utilizes GUI and a combination of threat intelligence databases. Nmap can map your network via CLI with a tac command to give you more information on CVE's.

2) How do vulnerability scanning techniques integrate with an organization's patch management processes? Explain the relationship between identifying vulnerabilities through scans and the subsequent steps involved in remediation and risk reduction.

   Answer: Patch management is making sure that you are patching something like code or configurations. If there is a vulnerability that needs a patch, then the patch process will mediate that issue. The steps that are involved are you scan for an issue/ vulnerability and then you look for remediation. If there is a patch available, you will follow the steps to either apply the patch or deploy the patch.