General Purpose Graphics Processing Units (GPGPUs) are quickly becoming favored over CPUs as the processing unit for many tasks that benefit from being highly parallelized. One area seeing an increased use in GPGPU technology is cyber security where many tasks can be parallelized, particularly credential harvesting. One of the most common tasks for a penetration tester or cybercriminal is to collect encrypted passwords, called hashes, of network and system administrators. They can then take these hashes and “crack” them to produce plain text passwords. The GPU allows them to crack these encrypted passwords at a faster rate than ever before. Password protected data such as national security information, corporate techniques, and financial information can be expensive. In addition, compromised systems and networks can allow unknown actors access to vital hardware resources. Using a tool called Hashcat, I will measure the performance of both GPU and CPU password cracking and compare them to each other. I will then estimate based on recent GPU and CPU hardware releases which is more likely to become the de facto processing unit for hash cracking. Knowing how data, systems, and networks may be compromised is important because it allows for more accurate risk assessments and better security practices.