Daniel Frey
CS 3910-001
Assignment #7
4/28/19

- **Why do many consider this is the worst security issue we've ever seen on the internet?**
  Many consider this the worst security issue because of the amount of people that could be affected. Also, the type of data and information that could become compromised make the Heartbleed bug very serious. Keys and passwords are among the data that could be compromised. The impact from this bug had the potential to be very huge.

- **Why did you have to use a different TLS version to get the exploit to run? What is the difference in the TLS implementation that allows some exploits to work with one version but not another?**
  Only certain versions of TLS were vulnerable, therefore the exploit only worked on those vulnerable versions. Different versions of TLS included the heartbeat extension, some of which contained a flaw thus making them vulnerable.

- **What are 3 serious pieces of information that could be in the output of the exploit that could seriously compromise overall security of an organization?**
  Serious information that could be intercepted includes primary key material, secondary key material, and protected content. Primary key materials are the actual encryption keys. Secondary key materials are like usernames and passwords. Protected content is any information that was encrypted, like messages or bank information.

- **Based on the fact that Heartbleed was only rated a medium vulnerability, and ShellShock and Ghost were rated Critical (10), do you feel Heartbleed was the most serious? Why/Why Not? (1 paragraph)**
  I think that the Heartbleed but is the worst because, although not as critical as ShellShock and Ghost, it is considered a silent attack. Taking advantage of the Heartbleed bug leaves no trace behind on the system, so you would not know if you were targeted. Also, because Heartbleed attacks target the TLS layer, its target base is quite large. It does not matter what type the system is or what it runs, like ShellShock or Ghost, so this makes it worse. If private keys became compromised, then they could be used to decrypt past or future messages. Authentication material could be intercepted and be used even after the bug has been fixed, given that the credentials are not changed. ShellShock and Ghost typically deal with gaining access to the system, but Heartbleed could potentially allow you to gain access to many other systems if the proper authentication materials were intercepted. Furthermore, although it is possible to detect the Heartbleed attacks, it does not mean that they are necessarily able to be blocked.