695.741 Assignment 1

Submit as either pdf or word to CANVAS

Part 1

For each malware: SQLSlammer, WannaCry, Duqu, Flame, Stuxnet, Opasrv, Melissa, and Koobface answer the following questions:

1. Choose any Vendor or Government DB and look up the above listed malware. Then answer the remaining questions. Examples of websites are included within Module 1- Assignment Part 1. Good Intel DB places to start: McAfee, Symantec, Trend Micro, MITRE.
2. Does the name and list of variants match 1:1 between the databases in Question 1? Describe the relationship you do see.
3. Use the National Vulnerability Database (https://nvd.nist.gov/), BugTraq (http://www.securityfocus.com/archives), and Full-Disclosure (http://seclists.org/fulldisclosure/) to list at least 3 advisories that relate to this worm.
4. Describe how the worm is propagated.
5. Describe how you would detect this propagation.
6. If the worm had a variant, describe at least one of these variants and if your proposed detection method would still be affective in detecting the variant.