Yuvika Nibber

Assignment 3

1. A virus is when a program or a code is inserted into a computer without the user knowing about it. Some mechanisms a virus can use to conceal itself are encryption, polymorphism, metamorphism, stealth.
2. A logic bomb is a malicious program which is timed in a way it causes harm at a certain point. For example, the march 7 virus. It is set in a way that it will cause harm only on that day to the infected computer. It is inactive on all the other days/times.
3. Trojan is usually spread via email. It waits till the user opens the email/link and then spreads across your contacts. People usually open the mail thinking its from a person they know. When trojan is already inside the computer, it starts manipulating and adding its code to all the files in the computer/ executable files so it could spread itself to other computers. Trojans are very common because people usually tend to open the emails, they get and the link unless they are aware of it or are suspicious of the link.
4. Machine executable viruses are usually attached to the program that is executable. The macro virus on the other hand infects the applications that are most used.
5. The original code has been changed to interrupt the signatures. The semantics of the original code have not been changed. It changed the behavior of the original code which showed up in the metamorphic code.
6. Logic bomb
7. The USB stick could have a executable or macro virus. It can transmit a malicious worm or a trojan. We should scan the memory stick with an anti-virus software. We should check the memory stick in an emulation environment i.e., a controlled environment.
8. Backdoor
9. The loan could have been created because a hacker might have taken all the information and applied for the loan. The makes the person responsible for the repayments of the loan. The hacker attacked by phishing email attack. It got the users credit card details and other personal information. The types of malwares necessary are spyware, trojan horse malware.
10. Trojan, virus, worms, spyware, scareware, keylogger, adware, backdoor, wabbits, exploit, botnet, dialer, phishing, cookies, browser hijackers, mousetrapping, virus document, DDoS, fake AV etc. The countermeasures used to block these macro viruses are using digital signatures, checking for regular updates, deleting spam folder, not opening unknown/ suspicious emails. We can block these by using a good firewall or by cloud security or any good antivirus/ anti malware program.