CSC 438/539 Advanced Information Security
Spring 2013 Instructor: Dr. Natarajan Meghanathan

Question Bank on Module 9 – Malware

1) Suppose there is a new computer virus, VN1Q, which is both polymorphic and metamorphic. Ron has a new malwaredetection program, DetVirus, that is 95% accurate at detecting VN1Q. That is, if a computer is infected with VN1Q, then DetVirus will correctly detect this fact 95% of the time, and if a computer is not infected, then DetVirus will correctly detect this fact 95% of the time. It turns out that the VN1Q virus will only infect any given computer with a probability of 1%. Nevertheless, you are nervous and run DetVirus on your computer, and it unfortunately says that your computer is infected with VN1Q. Find the probability that your computer really is infected?
2) Suppose that a metamorphic virus, XYZVirus, is 98% useless bytes and 2% useful bytes. Unfortunately, XYZVirus has infected the login program on your Linux system and increased its size from 32K bytes to 1,032K bytes; hence, 1,000K bytes of the login program now consists of the XYZVirus. Bob has a cleanup program, XYZSweep, that is able to prune away the useless bytes of the XYZVirus, so that in any infected file it will consist of 96% useless bytes and 4% useful bytes. If you apply XYZSweep to the infected login program, what will be its new size?
3) Consider a network with 10,000 vulnerable hosts for a certain worm. After certain rounds of propagation of this worm, assume there are 4000 infected hosts. How many of the susceptible hosts will be infected in the next round of propagation, if the speed of propagation of the worm ($\beta$) = 0.00005? Use the epidemic-worm propagation model discussed in class.
4) How is the saturation time of a worm related to the speed of propagation (or the infection rate)?
5) Briefly explain the four phases of a virus' life.
6) Explain the difference between the following kinds of viruses:
    a. Transient virus and a Resident virus.
    b. Polymorphic virus and a Metamorphic virus
    c. Program virus and a Macro virus
7) Why do viruses prefer to attach themselves to larger files rather than smaller files? Justify.
8) Briefly explain how a bootstrap virus could infect your hard disk and how does it hide itself from identification.
9) What is the general strategy employed by viruses and worms to survive reboots?
10) Explain the principle of working of an encrypted virus.
11) Briefly explain the three types of signature schemes and some general strategies employed by virus scanners to detect metamorphic viruses?
12) Explain the sequence of steps employed by a worm to propagate.
13) What is a botnet and how is it used to launch an attack?
14) What is a zero-day attack? What characteristic of worm may help you to detect zero-day attacks? What software do you need to be running in your machine to detect such attacks?
15) What is the primary characteristic of the rootkits? Explain the two types of rootkits and the methods generally adopted to detect their infection.