1. You are the system administrator for a real estate broker’s small office network which has about 15 computers. Last week, you installed a new computer for a new employee, Melanie, and you ensured all the operating system updates were performed, Windows Defender was turned on, and the homepage was set to http://realestate.com. When you arrived at work this morning, Melanie tells you that her computer is acting very strangely. Whenever she opens her web browser, it goes to http://realestate.xyz and multiple pop-up windows are displayed. What type of malware might Melanie have accidently installed on the new computer?
   1. Backdoor
   2. Logic bomb
   3. **Spyware**
   4. Rootkit

Explanation: Spyware and Adware tend to be a nuisance type of malware that usually tries to either collect your information and then resell it to advertisers to make a profit. It is common that your homepage will be changed in order to run additional ads and making the spyware developers additional revenue. (LESSON 03\_10 Preventing Malware)

1. You are working as part of the help desk for a large corporation. You receive a phone call from a user who is complaining that their computer is acting erratically, freezes up, and often reboots for no reason. You reboot the user’s computer and determine it is acting much slower than other computers in the office. You think something must be using up the network and processing resources of this computer, so you check the task manager and run a netstat command to determine what network connections are currently in use. The netstat command returns hundreds of resulting connections open, all of which appear to be outbound connections to various websites like NewYorkTimes.com, CNN.com, and WallStreetJournal.com. This is odd because there are no web browsers currently open when you run the scan. What do you think might be happening?
   1. The computer is infected with a virus
   2. **The computer is a zombie and now part of a botnet**
   3. The computer is infected with rootkit
   4. The computer is infected with a logic bomb

Explanation: A zombie is a computer that has been infected with malware and is now part of a botnet. Botnet utilize zombie computers to run distributed processing tasks (like cryptomining) or distributed networking tasks (like creating a distributed denial of service attack on well-known websites). The description provided sounds like the zombie is part of a few DDoS attacks that the botnet is running attempting to run against the three websites. (LESSON 03\_04 Botnets and Zombies)

1. You have just been hired as the new junior security analyst for a medium-sized software company. While you are sitting in the breakroom, you overhear an irate employee yelling at the manager for the software development team, “You’ll be sorry when I’m gone!” Afterwards, you hear the door slam and the irate employee angrily leave the office with a box of his personal effects. It sounds like he may have just be fired. A few minutes later, the manager asks you to review the employee’s last three weeks of coding projects which are about to be combined into the live production environment. The manager is worried that the employee might have done something to harm the company. As you start scanning the employee’s software code, what type of malware are you most likely trying to find?
   1. Rootkit
   2. Spyware
   3. Worm
   4. **Logic bomb**

Explanation: A logic bomb is a type of malware that executes when a certain condition is met. This could be a date, event, or other trigger. Logic bombs are commonly associated with disgruntled employees and have been used to delete files or cause destruction after an employee was fired. (LESSON 03\_07 Backdoors and Logic Bombs)

1. Your team lead has asked you to setup a whitelist and a blacklist on the server, as well as to ensure that the Exchange server doesn’t have any open mail relays. What is your team lead attempting to prevent with these precautions?
   1. **Spam**
   2. Viruses
   3. Worms
   4. Spyware

Explanation: Whitelisting, blacklisting, closing open mail relays, and training your end users are all precaustions to prevent spam from infiltrating your organization’s email servers. (LESSON 03\_10 Preventing Malware)