1. You are the system administrator for a medium-sized business network. You noticed that one of your servers on your network has become extremely slow. You log on to the server and check its open connections using netstat. You discover that it is conducting numerous network access callouts to the internet over port 445, even though none of the other systems on the network have made this request. During your continued analysis, you see that the processor activity continues to rise and the network access requests are continuing to increase exponentially. You check the logs and see that no new software has been installed recently. Which type of malware might this server be infected with?
   1. Virus
   2. **Worm**
   3. Ransomware
   4. Rootkit

Explanation: A worm is a type of malware that is self-replicating and continues to attempt to spread out and find new victims. The indications above describe a worm infection on the server that is now trying to find new victims to spread itself into. This can occur without any user action, as described in the scenario above. (LESSON 02\_03 WORMS)

1. You are relaxing on the couch with your laptop and scrolling Facebook. There is an article that looks interesting about a new video game that is going to be released new month so you click on it. About 2 minutes later, you see an alert on your screen, “VIRUS DETECTED”. Instead of panicking, you launch Windows Defender, verify it has the latest virus definitions and updates, and then scan your hard drive for viruses. After several minutes of scanning, Windows Defender reports that no viruses were found. What type of virus might you have?
   1. Macro
   2. Program
   3. Encrypted
   4. **Hoax**

Explanation: A hoax is a category under viruses where an attacker tries to trick a victim into thinking they have a virus when they really don’t. This is commonly done using pop-up windows in your web browser that are designed to look like a virus scan detection report. Since your virus scanner is up-to-date and didn’t find any viruses during its scan, you most likely have been the attempted victim of a hoax. (LESSON 02\_02 VIRUSES)

1. You have just woken up in the morning and decided to check your email. You turn on your computer, but after 30 seconds you see a screen stating, “Your computer has been locked! You must pay 2 Bitcoin in order to receive the unlock code.” What kind of malware is on your computer?
   1. Virus
   2. Worm
   3. **Ransomware**
   4. Rootkit

Explanation: This scenario perfectly describes a ransomware attack, where a victim’s computer is held hostage until payment is received by the attacker. You should not pay the ransom, but instead format the hard drive, install a new copy of the operating system, and restore your files from a known-good backup copy. (LESSON 02\_06 RANSOMWARE)