# CSH6 Ch 41 (AV Technology) Review Questions

1. When an AV scanner looks for infections by using a list of known viruses, it is using___
2. How many malware varieties are typically released in a day worldwide?
3. A heuristic scanner that examines the logic of a suspect program by examining its code is illustrating the___
4. AV scanners can be installed
5. Because of Microsoft's decisions about Visual BASIC as a tool underlying its Office products, which kind of malware spread extensively starting in the 1990s?
6. An application that scans all incoming and outgoing network traffic looking for malware is illustrating the method called___
7. An AV scanner that is looking for suspicious behavior or file structures is using___
8. The list of viruses that have been found infecting users' computers is known as the___
9. A heuristic scanner that tries to emulate the functioning of a suspect program is illustrating the___
10. What is the current name of the organization that certifies AV products as complying with standards maintained by the Anti-Virus Product Vendors' Consortium?
11. Why is it now possible to receive malware through e-mail whereas that was not an issue in the 1980s?
12. Boot-sector viruses became less prevalent on systems running Windows because of the advent of alerts when the boot sector was being modified that appeared in___
13. To be most effective, an AV scanner should be configured to use___
14. Viruses in the wild are on___
15. Which of the following statements is/are true?
16. Which organization created a consortium of AV vendors to pay for systematic certification of AV products in the early 1990s?
17. System administrators must be sure to keep which elements of an AV up to date?
18. What was the primary method of distribution of viruses in the 1980s?
19. What was the primary motivation of malware writers in the 1980s when malware writing began to grow?
20. An AV scanner that is looking for new variants of known viruses is using___
21. An AV scanner is a program that___
22. How do CRCs play a role in AV intrusion detection and prevention?
23. Updates for desktop AV scanners are now typically distributed___
24. Typically, modern AV products update their product AV databases___
25. Viruses in the zoo are those that exist___
26. When an AV scans every file when it is opened by a process, it is illustrating___
27. Most malware today tends to infect___
28. How should we update our AV products?
29. What is the primary motivation of malware writers today?
30. An AV scanner that is monitoring known-suspicious system changes and behaviors is illustrating the use of___