1. A rootkit is a set of programs installed on a system to maintain covert access to that system with administrator (root) privileges while hiding evidence of its presence.

2. A blended attack uses multiple methods of infection or propagation to maximize the speed of contagion and the severity of the attack.

3. A computer virus is a piece of software that can “infect” other programs or any type of executable content and tries to replicate itself.

4. Sometimes referred to as the “infection vector”, the infection mechanism is the means by which a virus spreads or propagates.

5. Sometimes known as a “logic bomb”, the trigger is the event or condition that determines when the payload is activated or delivered.

6. The four phases of a typical virus are: dormant phase, triggering phase, execution phase and propagation phase.

7. During the triggering phase the virus is activated to perform the function for which it was intended. 8. A stealth virus is explicitly designed to hide itself from detection by anti-virus software.

9. Mobile code refers to programs that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.

10. A drive-by-download is when a user views a Web page controlled by the attacker that contains a code that exploits the browser bug and downloads and installs malware on the system without the user’s knowledge or consent.

11. A botnet is a collection of bots capable of acting in a coordinated manner.

12. A bot can use a keylogger to capture keystrokes on the infected machine to retrieve sensitive information.

13. Countermeasures for malware are generally known as anti-virus mechanisms because they were first developed to specifically target virus infections.

14. Developed by IBM and refined by Symantec, the digital immune system provides a malware detection system that will automatically capture, analyze, add detection and shielding, or remove new malware and pass information about it to client systems so the malware can be detected before it is allowed to run elsewhere.

15. Generic decryption technology is an anti-virus approach that enables the anti-virus program to easily detect even the most complex polymorphic viruses and other malware, while maintaining fast scanning speeds.