CSH6 Ch 27 (IDS & IPS) Review Questions

1. Which of the following is NOT a standard approach to monitoring for IDS?
2. Misuse detection involves filtering event streams to locate patterns related to ___
3. What's an _intrusion_ in a computer system or network?
4. An intrusion-detection system that continuously feeds data to the analysis engine for immediate alerts is described as ___
5. What are the possible goals of automated responses in intrusion detection and intrusion response?
6. An IDS compares observed network patterns against baselines performance captured during a training phase. This IDS is using ___
7. What's an IDS in security terminology?
8. Which of the following techniques are used in anomaly detection?
9. Which of the following is the most commonly-used monitoring approach for IDS today?
10. Which analytical method suffers from inability to detect new attacks?
11. Which of the following is a widely-used analysis strategy for intrusion-detection systems?
12. In general, audit information should be stored and processed in ___
13. Which of the following goals of intrusion response is NOT recommended?
14. "…[T]he action of collecting event data from an information source and then conveying that data to the analysis engine…." is called ___
15. A message or document from an intrusion-detection system that is generated periodically by the users (usual system or network managers) is a(n) ___
16. A security tool reports on attempted penetrations and denial-of-service attacks reaching it from the Internet. This tool is most likely a(n) ___
17. Which of the following is/are (an) information source(s) for intrusion-prevention systems?
18. Which of the following locations of sensors is/are common?
19. Anomaly detection involves filtering event streams to locate patterns related to ___
20. An IDS filters event streams and matches patterns against known attack signatures. This IDS is using ___
21. A message from an intrusion-detection system that is communicated immediately to the users (usual system or network managers) is a(n) ___
22. Where should one deploy IDS?
23. Which analytical method suffers from high false-positive rates?