CSH6 Chapter 40 (Patch Management) Review Questions

1. Which type of enterprise patch management system consumes the most network bandwidth?
2. Which of the following is NOT a function of the Patch & Vulnerability Group?
3. Which of the following methods can legitimately reduce the efforts and costs of automated patch management?
4. Which sources can provide useful, reliable information about vulnerabilities, remediations and threats?
5. Organizations should consider using automated patch management solutions to ___
6. After application of a remediation for a vulnerability, the PVG should ___
7. What type of enterprise patch management tool is this? It uses a central computer that scans all associated computers and then determines which patches are required for each computer.
8. What is the NIST CSRC?
9. Flaws that can be exploited by a malicious entity to gain greater access or privileges than authorized are called ___
10. Which of the following steps is NOT appropriate for a PVG to use in prioritizing vulnerability remediation?
11. Which of the following statements about patch-management tools is INCORRECT?
12. If a programmer introduces undocumented and unauthorized functionality into production code, this problem is known as ___
13. A remediation database should contain ___
14. What role has primary responsibility for ensuring that IT resources are participating in automated patching processes?
15. Manual patching is too expensive to consider for a production environment because ___
16. A list managed by the PVG of IT equipment includes, among other details, the associated system name, the property number, the main user of the IT resource, the system administrator, the physical location, the connected network port[s], the software configuration and the hardware configuration. This list is known as the ___
17. What does the acronym SQA stand for in information technology?
18. Additional, especially written pieces of code designed to fix bugs in software are called ___
19. What type of enterprise patch management tool is this? It uses programs running on each associated computer to determine which patches are required and then installs them.
20. What is the meaning of a _fix_ or _hotfix_ in the language of a PVG?
21. What is the primary tool that can identify all installed patches, ensure consistent application throughout the organization, verify proper installation, and determine if there has been damage to previous patches?
22. Which of the following is/are (an) essential goal of SQA?
23. What is the first element of corporate systems that PVGs typically prioritize for patch management?
24. For PVGs, authenticating the downloaded remediation is an element of ___
25. What's a _patch_ in system operations management?
26. Before testing a remediation, it is wise for the PVG to ___
27. What does the acronym SLA stand for in information technology?
28. Which of the following considerations determines SQA design?
29. Why should the PVG inventory all the IT equipment is in use in an organization?

30. Which of the following are expected functions of a Patch and Vulnerability Group (PVG)?
31. Why should we use test-coverage monitors?
32. A Patch and Vulnerability Group (PVG) is ideally
33. Which group in a well-run corporate environment is responsible for monitoring security sources for information on the latest vulnerabilities, patches, non-patch remediations and threats?
34. Which of the following is/are a normal method of remediation used by a PVG?
35. Patches and other remediations should be tested by the PVG using ___
36. Your chapter on managing software patches and vulnerabilities recommends which of the following as primary sources of information about vulnerabilities, remediation, and threats?
37. Methods for taking advantage of software and configuration weaknesses are called?