Answer Review Questions

Answer the following review questions. You can find the answers at the end of this chapter.

1. Virtualization technology is often implemented as operating systems and applications that run in software. Often, it is implemented as a virtual machine. Of the following, which can be a security benefit when using virtualization?
   1. P atching a computer will patch all virtual machines running on the computer.
   2. If one virtual machine is compromised, none of the other virtual machines can be compromised.
   3. **If a virtual machine is compromised, the adverse effects can be compartmentalized**.
   4. Virtual machines cannot be affected by hacking techniques.
2. Eric wants to install an isolated operating system. What is the best tool to use?

**A. Virtualization**

* 1. UAC
  2. HIDS
  3. NIDS

1. Where would you turn off file sharing in Windows Vista? A. C ontrol Panel
   1. Local Area Connection
   2. **Network and Sharing Center**
   3. Firewall properties
2. Which option enables you to hide ntldr?
   1. **Enable Hide Protected Operating System Files**

B. D isable Show Hidden Files and Folders

* 1. Disable Hide Protected operating system Files
  2. Remove the -R Attribute

1. Which of the following should be implemented to harden an operating system? (Select the two best answers.)

**A. I nstall the latest service pack.**

1. **Install Windows Defender.**
2. Install a virtual operating system.
3. Execute PHP scripts.
4. In Windows 7, Vista, and XP, what is the best file system to use?
   1. FAT
   2. **NTFS**
   3. DFS
   4. FAT32
5. A customer’s computer uses FAT16 as its file system. What file system can you upgrade it to when using the **convert** command?
   1. **N TFS**
   2. H PFS
   3. FAT32
   4. NFS
6. Which of the following is not an advantage of NTFS over FAT32? A. N TFS supports file encryption.
   1. NTFS supports larger file sizes.
   2. NTFS supports larger volumes.
   3. **NTFS supports more file formats.**
7. What is the deadliest risk of a virtual computer?
   1. If a virtual computer fails, all other virtual computers immediately go offline.
   2. If a virtual computer fails, the physical server goes offline.
   3. If the physical server fails, all other physical servers immediately go offline.
   4. **If the physical server fails, all the virtual computers immediately go offline**.
8. Virtualized browsers can protect the OS that they are installed within from which of the following?
   1. DDoS attacks against the underlying OS
   2. P hishing and spam attacks
   3. Man-in-the-middle attacks
   4. **Malware installation from Internet websites**
9. Which of the following needs to be backed up on a domain controller to recover Active Directory?
   1. User data
   2. System files
   3. Operating system
   4. **System state**
10. Which of the following should you implement to fix a single security issue on the computer?
    1. Service pack
    2. Support website
    3. **Patch**
    4. Baseline
11. An administrator wants to reduce the size of the attack surface of Windows server 2008. Which of the following is the best answer to accomplish this? A. U pdate antivirus software.
    1. Install service packs.
    2. **Disable unnecessary services.**
    3. Install network intrusion detection systems.
12. You finished installing the operating system for a home user. What are three good methods to implement to secure that operating system? (Select the three best answers.)
    1. Install the latest service pack.
    2. **Install a hardware- or software-based firewall.**
    3. Install the latest patches.
    4. Install pcAnywhere.
13. Which of the following is a security reason to implement virtualization in your network?
    1. **To isolate network services and roles**
    2. T o analyze network traffic
    3. To add network services at lower costs
    4. To centralize patch management
14. Which of the following is one example of verifying new software changes on a test system?
    1. Application hardening
    2. Virtualization
    3. **Patch management**
    4. HIDS
15. You have been tasked with protecting an operating system from malicious software. What should you do? (Select the two best answers.) A. D isable the DLP.
    1. **Update the HIPS signatures.**
    2. Install a perimeter firewall.
    3. **Disable unused services.**
    4. Update the NIDS signatures.