Review Questions

1. Which security feature in Windows 7 prevents malware by limiting user privilege levels?
   a. Windows Defender
   b. User Account Control (UAC)
   c. Microsoft Security Essentials
   d. Service SIDs
2. The default privilege level for services is LocalSystem. True or False?
3. When compared to Windows XP, which networking features have been updated or added in Windows 7 to enhance security? (Choose all that apply.)
   a. TCP/IPv4
   b. Network Access Protection (NAP)
   c. Point-to-Point Tunneling Protocol (PPTP)
   d. Internet Connection Sharing
   e. Windows Firewall
4. When compared to Windows Vista, which data protection feature is new in Windows 7?
   a. Local security policy
   b. BitLocker Drive Encryption
   c. EFS
   d. BitLocker To Go
   e. Network Access Protection (NAP)
5. Which of the following passwords meet complexity requirements? (Choose all that apply.)
   a. passw0rd$
   b. ##$$@@
   c. ake1vyue
   d. a1batr0$$
   e. A%5j
6. Which password policy setting should you use to prevent users from reusing their passwords too quickly?
   a. Maximum password age
   b. Minimum password age
   c. Minimum password length
   d. Password must meet complexity requirements
   e. Store passwords using reversible encryption
7. Which account lockout policy setting is used to configure the time frame in which incorrect logon attempts must be conducted before an account is locked out?
   a. Account lockout duration
   b. Account lockout threshold
   c. Reset account lockout counter after
   d. Account lockout release period
8. The ______ local policy controls the tasks users are allowed to perform.

9. Which type of AppLocker rule condition can uniquely identify any file regardless of its location?

   a. Publisher

   b. Hash

   c. Network zone

   d. Path

10. How would you create AppLocker rules if you wanted to avoid updating the rules when most software is already installed?

    a. Manually create rules for each application

    b. Automatically generate rules

    c. Create default rules

    d. Download rule templates

11. Evaluating DLL files for software restrictions has a minimal impact on performance because of caching. True or False?

12. Which utilities can be used to compare the settings in a security template against a computer configuration? (Choose all that apply.)

    a. Secedit

    b. Windows Defender

    c. Security Templates snap-in

    d. Group Policy Object Editor

    e. Security Configuration and Analysis tool

13. To which event log are audit events written?

    a. Application

    b. Security

    c. System

    d. Audit

    e. Advanced Audit

14. An _____ is used to describe the structure of an application and trigger UAC when required.

15. What are you disabling when you configure UAC to not dim the desktop?

    a. Admin Approval Mode

    b. file and registry virtualization

    c. user-initiated prompts

    d. secure desktop

16. Microsoft Security Essentials requires a subscription fee after a 90-day trial period. True or false?

17. Which of the following does Action Center monitor? (Choose all that apply.)

    a. Network Firewall

    b. Windows Update

    c. User Account Control

    d. Internet security settings

    e. Virus protection

18. To prevent spyware installation, you should configure Windows Defender to perform _____

19. Which type of encryption is the fastest, strongest, and best suited to encrypting large amounts of information?
    a. Symmetric
    b. 128 bit
    c. Asymmetric
    d. Hash
    e. Public key
20. To encrypt a file by using EFS, the file must be stored on an NTFS-formatted partition. True or False?
21. How can you recover EFS-encrypted files if the user profile holding the digital certificate is accidentally deleted? (Choose all that apply.)
    a. Restore the file from backup.
    b. Restore the user certificate from a backup copy.
    c. Another user with access to the file can decrypt it.
    d. Decrypt the file by using the recovery certificate.
    e. Decrypt the file by using the EFS recovery snap-in.
22. Which of the following is not true about BitLocker Drive Encryption?
    a. BitLocker Drive Encryption requires at least two disk partitions.
    b. BitLocker Drive Encryption is designed to be used with a TPM.
    c. Two encryption keys are used to protect data.
    d. Data is still encrypted when BitLocker Drive Encryption is disabled.
    e. You must use a USB drive to store the startup key.
23. BitLocker Drive Encryption is user aware and can be used to protect individual files on a shared computer. True or False?
24. Which is the preferred setting for Windows Update?
    a. Install updates automatically
    b. Download updates but let me choose whether to install them
    c. Check for updates but let me choose whether to download and install them
    d. Never check for updates
25. Which categories of updates can be downloaded and installed automatically by Windows Update? (Choose all that apply.)
    a. *Critical*
    b. Important
    c. Recommended
    d. Optional
    e. Feature update

Case Projects

Case Project 7-1: Virus Prevention

Buddy's Machine shop has been infected with a virus for the second time in six months. Several machines cannot run antivirus software because it interferes with specialized software used to carve machine parts from blocks of metal. What can you do to mitigate the risk of viruses infecting the computers?