Windows Security Fundamentals Quiz

Overview

This quiz tests your knowledge of basic Windows security concepts that are essential for CyberPatriot competitions. It covers user account management, Windows security features, system hardening, and fundamental security concepts.

Time Allowed: 30 minutes
Total Points: 50
Passing Score: 40 points (80%)

Instructions

1. Read each question carefully
2. Write down your answers on a separate sheet of paper or create a text file with your answers
3. Number your answers to match the question numbers
4. Check your answers against the solution key when finished or submit your answers for review

---

Multiple Choice Questions (2 points each)

1. Which Windows feature provides a central location to view security status and manage security settings?

A. Windows Security Center
B. Windows Defender
C. Windows Firewall
D. Windows Security

2. Which of the following user account types has the most privileges on a Windows system?

A. Standard User
B. Administrator
C. Guest
D. Power User

3. What is the minimum recommended password length according to CyberPatriot guidelines?

A. 8 characters
B. 10 characters
C. 12 characters
D. 14 characters

4. Which Windows service should be disabled to prevent remote management of the registry?

A. Remote Registry
B. Remote Procedure Call (RPC)

C. Server Service
D. Remote Access Connection Manager

5. What is the recommended account lockout threshold for failed login attempts?

A. 3 attempts
B. 5 attempts
C. 10 attempts
D. 15 attempts

6. Which of the following is NOT a common location for malware persistence in Windows?

A. Run keys in the Registry
B. Startup folder
C. Scheduled Tasks
D. System32 folder (itself)

7. What Windows feature helps prevent unauthorized changes to the system by prompting for permission?

A. Windows Defender
B. User Account Control (UAC)
C. BitLocker
D. Windows Firewall

8. Which built-in Windows account should typically be disabled?

A. Administrator
B. Guest
C. System
D. DefaultAccount

9. What Windows tool is used to view and monitor security-related events?

A. Task Manager
B. Computer Management
C. Event Viewer
D. Resource Monitor

10. Which Windows component is responsible for enforcing password policies?

A. Local Security Authority (LSA)
B. Security Accounts Manager (SAM)
C. Group Policy
D. Windows Defender

11. What is the default location of the Windows user account database (SAM)?

A. C:\Users\SAM
B. C:\Windows\System32\config\SAM

C. C:\Windows\security\database
D. C:\Windows\Users\Accounts

12. Which of the following registry keys contains startup programs that run when a user logs in?

A. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
B. HKLM\SYSTEM\CurrentControlSet\Services
C. HKCU\Software\Microsoft\Windows\Start Menu
D. HKLM\SYSTEM\WinLogon

13. What Windows feature can encrypt the entire operating system drive to protect data?

A. EFS (Encrypting File System)
B. BitLocker
C. Windows Defender
D. NTFS Permissions

14. Which tool can be used to manage local security policy on Windows systems?

A. secpol.msc
B. gpedit.msc
C. lusrmgr.msc
D. services.msc

15. What command line tool can be used to view all user accounts on a Windows system?

A. net users
B. dir users
C. list accounts
D. view users

True/False Questions (1 point each)

16. The built-in Administrator account cannot be deleted, only disabled.

True or False

17. Windows 11 Home edition includes the Local Group Policy Editor (gpedit.msc).

True or False

18. Password complexity requirements enforce the use of uppercase letters, lowercase letters, numbers, and special characters.

True or False

19. Windows Update can be safely disabled in a competition environment to prevent unexpected changes.

True or False

20. User Account Control (UAC) only affects accounts in the Administrators group.

True or False

21. Files encrypted with EFS (Encrypting File System) can be accessed by any administrator on the system by default.

True or False

22. System Restore can be used to recover from malware infections with no data loss.

True or False

23. In Windows, the Guest account is enabled by default.

True or False

24. Windows Firewall can block both inbound and outbound traffic.

True or False

25. Windows Defender is automatically disabled if a third-party antivirus is installed.

True or False

Short Answer Questions (3 points each)

26. List three methods for adding a user to the Administrators group in Windows.

27. What is "least privilege" and why is it important for Windows security?

28. Name three Windows services that are commonly disabled for security purposes.

29. Explain the difference between NTFS permissions and share permissions.

30. Describe three ways malware can maintain persistence on a Windows system.

Scenario Questions (5 points each)

31. You suspect unauthorized access to a Windows system. Which three Event Viewer logs would you check, and what event IDs would be most relevant?

32. During a CyberPatriot competition, you discover multiple unauthorized user accounts on a Windows system. Describe your step-by-step approach to address this issue, including the commands or tools you would use and how you would verify your changes.

33. You need to secure a Windows workstation that will be accessed by multiple users. Outline five specific security measures you would implement, explaining why each is important.

Bonus Question (5 points)

34. Explain how credential caching works in Windows and what security risks it presents. How can you mitigate these risks?