Preview Test: Scenario 2 Quiz

Test Information

Description	This quiz covers readings and videos for Scenario 2. Please take the quiz after you have completed those materials.
Instructions	
Multiple Attempts	This test allows 3 attempts. This is attempt number 1.
Force Completion	This test can be saved and resumed later.
	Your answers are saved automatically.

Question Completion Status:

QUESTION 1

1. Which of the following describes a flaw in contemporary microprocessors?
   a. Heartbleed
   b. Wannacry
   c. Spectre and Meltdown
   d. Petya

6.667 points

QUESTION 2

1. How can you view the last modification time of a registry key using the Windows Registry Editor?
   a. Right-click and select Properties
   b. Export the key to a text file
   c. Check the Details tab
   d. Use the "echo" command in the command prompt

6.667 points

QUESTION 3

1. What registry location is used to observe traces of USB storage devices in Windows? Note that you can view the Windows registry by opening “regedit.exe”?
   a. HKEY_LOCAL_MACHINE\SOFTWARE\USB
   b. HKEY_CURRENT_USER\Control Panel\USBDevices

c. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\USBSTOR

d. HKEY_CURRENT_USER\Software\Microsoft\Windows\USB

6.667 points

QUESTION 4

1. Where are recently opened documents stored in the Windows registry?
   a. HKEY_LOCAL_MACHINE\Software\RecentDocs

   b. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

   c. HKEY_CURRENT_USER\Software\Microsoft\RecentFiles

   d. HKEY_LOCAL_MACHINE\RecentDocs

6.667 points

QUESTION 5

1. What information is contained in the subkey names under the Device Class Identifier in the USBSTOR registry location?
   a. File size

   b. Serial number

   c. Drive number

   d. Time stamp

6.667 points

QUESTION 6

1. Which of the following statements about the Meltdown attack is correct?
   a. Can be utilized to bypass network traffic

   b. Exploits browser history and cookies

   c. Only affects the operating system kernel

   d. Only affects Windows operating systems

6.667 points

QUESTION 7

1. Which of the following do U.S. state and federal statutes require an entity to notify when a data breach occurs
   a. Individuals who have had protected information stolen

   b. State attorney generals

   c. Consumer reporting agencies

d. All of the above

6.667 points

QUESTION 8

1. Which of the following could happen as a result of a successful Spectre or Meltdown attack?
   a. Protected personal information theft
   b. Data destruction
   c. Service denial
   d. Network espionage.

6.667 points

QUESTION 9

1. After determining a notifiable breach has occurred, the next step is:
   a. Determine if the information involved meets the definition of "personal information"
   b. Identify whether the affected data was encrypted.
   c. Consider to whom, how, and when the notification must be made.
   d. Identify whether the data breach is likely to cause harm.

6.667 points

QUESTION 10

1. Which U.S. state does not have a breach notification law?
   a. Utah
   b. Hawaii
   c. South Dakota
   d. None of the above

6.667 points

QUESTION 11

1. Which of the following is not an example of "personal information" under the varying definitions under U.S. data breach notification laws?
   a. Company logo
   b. Signature
   c. Telephone number
   d. IP address

6.667 points

QUESTION 12

1. Which of the following represents a Spectre vulnerability mitigation strategy?
   a. Frequent firmware updates with microcode updates
   b. Enabling a system firewall
   c. External caching
   d. None of the above

6.667 points

QUESTION 13

1. What is a hive in the Windows registry?
   a. A computer-specific configuration
   b. A user-specific configuration
   c. A logical group of keys, subkeys, and values
   d. A timestamp value

6.667 points

QUESTION 14

1. Both Meltdown and Spectre falls under which of the following categories?
   a. Registry invasion
   b. Distributed-Denial-of-Service attack
   c. Hardware vulnerability
   d. Man in the middle

6.667 points

QUESTION 15

1. Within how many days of identifying a reportable data breach must an organization notify affected individuals?
   a. 30 days
   b. 14 days
   c. It depends on the jurisdiction and the industry.
   d. 10 days