SearchSecurity.com
Security School

Web Security School Lesson 2 Quiz

By Michael Cobb

1.) Which option best completes this sentence?
"System monitoring is important because . . ."

a. it tells you how many people have visited your site.
b. it provides security against lapses in your perimeter defenses, flawed products, and both new and old vulnerabilities.
c. it means you don’t need to keep patches up to date.
d. it tells you what threats your site faces.
e. None of the above

2.) Web server A is set up to log system and IIS activity. Which is the best set up from the list below?

a. Log File Directory: %WinDir%\System32\LogFiles
b. Log File Directory: C:\Inetpub\wwwroot\LogFiles
c. Log File Directory: E:\Inetpub\wwwroot\LogFiles
d. Log File Directory: E:\Inetpub\LogFiles
e. Log File Directory: F:\LogFiles

3.) Which is the recommended setting for auditing Object Access?

a. Success: Off, Failure: Off
b. Success: Off, Failure: On
c. Success: On, Failure: Off
d. Success: On, Failure: On
e. None of the above

4.) You have a limited security budget to protect your Web server, and your system administrator is busy upgrading your server. Which is your best option for an intrusion-detection system (IDS)?

a. A hosted-based appliance IDS
b. A network-based appliance IDS

c. A hosted-based software IDS
d. A hosted-based software IDS
e. A network and host-based appliance IDS

5.) You have downloaded and run the CIS Benchmarks and Scoring Tool. You score 4.8 out of 10. What should you do next?

a. Make a backup of your existing configuration
b. Review the tool's list of tasks to improve your security
c. Identify the consequences of making configuration changes
d. Implement the hardening steps outlined in the Benchmark guide
e. All of the above

Answers

1.) **The correct answer is: b. it provides security against lapses in your perimeter defenses, flawed products, and both new and old vulnerabilities.**
Security monitoring is seen by many security experts as a much more realistic way of providing resilient security. It makes a network less dependent on keeping patches up to date, and you're more likely to discover and catch a hacker -- regardless of what vulnerability is exploited to gain access.

2.) **The correct answer is: e. Log File Directory: F:\LogFiles**
The log files are being stored on a different drive to the operating system and the Web site's content. The F drive should be an NTFS formatted drive.

3.) **The correct answer is: b. Success: Off, Failure: On**
Setting Object Access auditing determines whether to audit the event of a user accessing an object -- for example, a file, folder, registry key, printer and so forth. Before setting up auditing for files and folders, you must enable Object Access auditing by defining auditing policy settings for the Object Access event category. If you do not enable Object Access auditing, you will receive an error message when you set up auditing for files and folders, and no files or folders will be audited.

If you log every successful Object Access event, your log files will fill up with enormous amounts of data that will not tell you anything useful about an attack. The user accessing the object obviously had permission to access the object.

4.) **The correct answer is: b. A network-based appliance IDS**
A host-based IDS only provides information on a specific PC or server and provides no traffic information at all. Although option E would be ideal, with a limited budget and time, this option would not be possible. For easy deployment, an appliance is quicker than a software-based system.

5.) **The correct answer is: e. All of the above**
Always back up your system before making any changes to it. Next, review and understand the implications of the changes to your system that the tool recommends. Finally, you would implement the changes and check that the system still functions as expected.