SearchSecurity.com
Security School

Web Security School Final Exam

By Michael Cobb

1.) Which of the following services is not required to run a Windows server solely configured to run IIS and publish a Web site on the Internet?
a. IIS Admin Service
b. Net Logon
c. Performance Logs and Alerts
d. Protected Storage
e. World Wide Web Publishing Service

2.) Which of the following statements is true about script kiddies?
a. They target specific organizations.
b. They scan specific systems for specific weaknesses.
c. They use subtle and varied tactics.
d. They may use your system to scan or exploit other systems.
e. The number of network attacks does not increase during school holidays.

3.) Which of the following properties must a "reliable" system demonstrate to be able to deliver essential services?
a. Resistance to attacks.
b. Recognition of attacks and the extent of any damage.
c. Recovery of full and essential services after attack.
d. Adjustment to reduce effectiveness of future attacks.
e. All of the above.

4.) Your Web server should be placed in a DMZ or "perimeter network," because . . .
a. It will be safe from attack.
b. It won't be able to access the Internet otherwise.
c. It locates it on a different subnet to your Intranet.
d. It is easier to wire it to the Internet.
e. It has to trust traffic coming from the Internet.

5.) Which of the following would you allow to attack your Web site?
a. Crackers
b. Hackers
c. Script kiddies

d. Red Teams
e. None of the above

6.) You are running an e-commerce Web site that uses SSL to encrypt your customers’ address and credit card information when they purchase goods via the site. You have blocked all unused ports on your Web server except ports 25, 80, 1433 and 1434. Will your customers be able to pay for their orders?
a. Yes
b. No

7.) Which of the following is not a true statement about the advantages of backing up system log files on a dedicated server?
a. It provides redundancy.
b. It reduces the cost of backing up log files.
c. You can compare two sets of logs against one another.
d. It allows cross checking of log files.
e. It protects against hackers altering or deleting local log files.

8.) Phishing differs from adware and spyware because…
a. it is not a problem for organizations but individuals.
b. it installs malicious software on your PC.
c. it uses social engineering and technical subterfuge whereas the other two do not.
d. it is easier to stop.
e. None of the above.

9.) Which one of the following components does not need to be installed to run IIS on a Windows server?
a. Common Files
b. FrontPage Server Extensions
c. Internet Information Services Snap-in
d. World Wide Web Server
e. They all need to be installed

10.) Which of the following directories should be deleted from a live IIS Web server connected to the Internet?
a. E:\Inetpub\ftproot
b. F:\Inetpub\iissamples
c. G:\Inetpub\mailroot
d. H:\Inetpub\wwwroot
e. None of them

11.) True or False: Client-side validation of form data is the same as server-validation except that it happens on the client's machine.

12.) Which of the following file types do you need to delete from your production IIS Web server?
a. .htm
b. .asp
c. .inc
d. .bak
e. None of the above

13.) Which of the following are signs that computers on your network may have been infected by spyware?
a. PCs are running unusually slow.
b. Ads are popping up.
c. Home pages have been altered.
d. There's a dramatic increase in network traffic.
e. All of the above.

14.) Internet Explorer divides the Internet into zones, so that you can assign a web site to a zone with a suitable security level. To which level would you assign the site \\fileserver\documents?
a. Internet zone
b. Local intranet zone
c. Trusted sites zone
d. Restricted sites zone

15.) The NTFS file format allows you to…
a. Encrypt data as it travels over a network.
b. Encrypt files located on a computer’s hard drive.
c. Encrypt passwords for storage in a database.
d. Hide passwords with asterisks while they are entered in to a text box.
e. Encrypt digital certificates used to authenticate a Web site.

16.) True or False: You do not need a Terminal Server Client Access License to run Terminal Services to manage a Windows server remotely.

17.) Which phrase best fits the following sentence? Web form input is _________. The data is not blocked; it is allowed into the server and could be manipulated to compromise security.
a. always sent using POST
b. critical to an e-commerce site
c. safe to use
d. an "allowed path"
e. part of the HTTP protocol

18.) You run a Web site that provides ASP script examples, which are stored in an Access database. Which is the correct way to display the text <script> on a Web page?
a. <script>
b. &lt;script&gt;
c. <&lt;script&gt;>
d. &lt;<script>&gt;
e. &gt;script&lt;

19.) Microsoft’s cipher.exe program…
a. permanently overwrites all of the deleted data on a hard drive.
b. permanently encrypts all of the deleted data on a hard drive.
c. empties the Recycle Bin data on a hard drive.
d. deletes the System Page file on system shut down.
e. empties the Recycle Bin data on system shut down.

20.) True or False: Null sessions are required on Windows IIS Web servers in order to allow anonymous access to the Web site using the Internet Guest account.

ANSWERS

1.) **The correct answer is: b. Net Logon**
The Net Logon service along with the Workstation service are only required if the computer is running as part of a Windows domain. A public Web server should never be part of a Windows domain.

2.) **The correct answer is: d. They may use your system to scan or exploit other systems.**
Many script kiddies try to hack sites for fun, but some will then use a compromised system to attack other systems. Their approach to hacking is simple; scan as many systems as possible in pursuit of a vulnerability. Unfortunately, spikes in attacks do tie in with the school calendar suggesting that many teenagers are behind them.

3.) **The correct answer is: e. All of the above.**
Security is about ensuring a system can deliver essential services and maintain essential properties such as integrity, confidentiality and performance, despite the presence of intrusions; in other words, reliability in the face of adversity. Therefore it must have all of the above four key properties.

4.) **The correct answer is: c. It locates it on a different subnet to your Intranet.**
Systems placed in the DMZ are still open to attack since they are connected to the Internet. However, by placing them on a different subnet to your internal resources you make it harder for an attacker who has compromised your Web server to gain access to your internal systems.

5.) **The correct answer is: d. Red Teams**
Red Teams are invited to attack a system to uncover system weaknesses. This ethical hacking is a controlled simulation of an attack against a Web site to find security holes in order to fix them before a real intrusion occurs. The other answer options would all result in malicious attacks.

6.) **The correct answer is: b. No**
Unfortunately, your customers would not be able to send their credit card details, as you have blocked port 443, which is used by HTTPS. HTTPS is the secure version of HTTP and encrypts the session data using SSL.

7.) **The correct answer is: b. It reduces the cost of backing up log files.**
Although it is recommended that you should log system events both locally and to a remote log server, it increases your costs as you need an additional server and resources to maintain it.

8.) **The correct answer is: e. None of the above.**
Phishing is a problem for organizations because it can affect their reputation. All three use social engineering and technical subterfuge to try and gain access to information. Technical subterfuge involves installing malicious software on a PC. Finally, they are all threats that are very difficult to stop and require security awareness training to reduce their potential impact.

9.) **The correct answer is: b. FrontPage Server Extensions**
While FrontPage Server Extensions enables authoring and administration of Web sites with FrontPage, it is not an essential component and can introduce additional security weaknesses. Common Files contains program files required by IIS, while the Snap-in provides the administrative interface for IIS.

10.) **The correct answer is: b. F:\Inetpub\iissamples**
You should never leave product documentation files and sample scripts on a production Web server; therefore, you should delete the F:\Inetpub\iissamples directory.

11.) **The correct answer is: False**
Client-side validation gives you the opportunity to validate and filter form data at the user's browser before it is sent to your server. Server-side validation is more sophisticated and more powerful than client-side validation and, unlike client-side validation, cannot be circumvented by the user.

12.) **The correct answer is: d. .bak**
Many Web authoring tools allow users to create an automatic backup copy of their work. If developers are allowed to save their work directly to the server — something I strongly advise against — these backup files are saved to the server as well, usually with the extension .bak. Anyone pointing their browser to one of these .bak files can view the script code by viewing the source returned by the server, since the Web server doesn't process the page and the script tags remain intact. To avoid this problem, ensure that all .bak files are deleted every time developers finish updating the site. To be on the safe side, associate .bak files to the scripting engine to ensure that the pages will be executed and that only the results are sent to the client.

13.) **The correct answer is: e. All of the above.**
All of the answers are possible signs that computers have been infected by spyware. Other signs may be unusual toolbars appearing on browsers, and antispyware or antivirus programs not working correctly.

14.) **The correct answer is: b. Local intranet zone**
The local intranet zone typically contains any addresses that don't require a proxy server, such as sites specified on the Connections tab, network paths such as \\computername\foldername and local intranet sites (typically addresses that don't contain periods, such as http://internal). The default security level for the Local intranet zone is Medium.

15.) **The correct answer is: b. Encrypt files located on a computer’s hard drive.**
An NTFS formatted drive supports encrypting files and folders using the Encryption File System (EFS). NTFS also supports access control lists that let an administrator control who can access specific files.

16.) **The correct answer is: True**
A maximum of two concurrent connections are automatically allowed on a Terminal server in Remote Administration mode.

17.) **The correct answer is: d. an "allowed path"**

Allowed paths are part of services that a system provides, intentionally and by design. Hackers often try to expose vulnerabilities in the allowed paths that a system or architecture offers.

18.) **The correct answer is: b. &lt;script&gt;**
If an HTML page needs to display the actual characters < >, they should be replaced with &lt; and &gt; to distinguish them from actual markup tags. If the special characters in the scripts stored in the database are not encoded when they are published, an attacker can insert malicious code into a script example and run the script when he requests the Web page displaying the example.

19.) **The correct answer is: a. permanently overwrites all of the deleted data on a hard drive.**
Microsoft's cipher.exe can be used to manage encrypted data by using the Encrypting File System. It also has the ability to permanently overwrite all of the deleted data on a hard drive. This improves security by ensuring that even an attacker with complete physical control of a Windows machine is unable to recover previously deleted data. It is available from Microsoft.com.

20.) **The correct answer is: False**
A null session occurs when a computer connects to another computer and no authentication is required. This is also called an "anonymous connection," which should not be confused with anonymous authentication in IIS. Anonymous authentication in IIS refers to allowing a user to have access to Web resources by automatically assigning them to the Internet Guest account without having to provide a user name and password. They are, however, accessing the server as a regular user in the security context of the Internet Guest account.

Null sessions should be disabled to reduce the risk of unauthorized individuals obtaining information about system resources, accounts or sensitive information.