**Review Questions**

|  |  |  |
| --- | --- | --- |
| **1.** | Which of the following are types of HTTP web authentication? (Choose all that apply.)   1. Digest 2. Basic 3. Windows 4. Kerberos | [Digest and basic are the types of HTTP web authentication.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N14) |
| **2.** | Which of the following is a countermeasure for a buffer overflow attack?   1. Input field length validation 2. Encryption 3. Firewall 4. Use of web forms | [Validating the field length and performing bounds checking are countermeasures for a buffer overflow attack.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N39) |
| **3.** | A hardware device that displays a login that changes every 60 seconds is known as a/an \_\_\_\_\_\_\_\_\_\_\_.   1. Login finder 2. Authentication server 3. Biometric authentication 4. Token | [A token is a hardware device containing a screen that displays a discrete set of numbers used for login and authentication.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N64) |
| **4.** | Which is a common web server vulnerability?   1. Limited user accounts 2. Default installation 3. Open shares 4. No directory access | [Default installation is a common web server vulnerability.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N89) |
| **5.** | A password of *P@SSWORD* can be cracked using which type of attack?   1. Brute force 2. Hybrid 3. Dictionary 4. Zero day exploit | [A hybrid attack substitutes numbers and special characters for letters.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N114) |
| **6.** | Which of the following is a countermeasure for authentication hijacking?   1. Authentication logging 2. Kerberos 3. SSL 4. Active Directory | [SSL is a countermeasure for authentication hijacking.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N142) |
| **7.** | Why is a web server more commonly attacked than other systems?   1. A web server is always accessible. 2. Attacking a web server does not require much hacking ability. 3. Web servers are usually placed in a secure DMZ. 4. Web servers are simple to exploit. | [A web server is always accessible, so a hacker can hack it more easily than less-available systems.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N167) |
| **8.** | A client/server program that resides on a web server is called a/an \_\_\_\_\_\_\_\_\_\_\_.   1. Internet program 2. Web application 3. Patch 4. Configuration file | [Web applications are client/server programs that reside on a web server.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N192) |
| **9.** | Which is a countermeasure to a directory-traversal attack?   1. Enforce permissions to folders. 2. Allow everyone access to the default page only. 3. Allow only registered users to access the home page of a website. 4. Make all users log in to access folders. | [A countermeasure to a directory-traversal attack is to enforce permissions to folders.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N217) |
| **10.** | What is it called when a hacker inserts programming commands into a web form?   1. Form tampering 2. Command injection 3. Buffer overflow 4. Web form attack | [Command injection involves a hacker entering programming commands into a web form in order to get the web server to execute the commands.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N242) |
| **11.** | Which of the following commands would start to execute a banner grab against a web server?   1. telnet [www.yahoo.com](http://www.yahoo.com/) 80 2. telnet HTTP [www.yahoo.com](http://www.yahoo.com/) 3. [http://www.yahoo.com:80](http://www.yahoo.com/) 4. HEAD [www.yahoo.com](http://www.yahoo.com/) | [To make an initial connection to the web server, use telnet to port 80.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N267) |
| **12.** | Which of the following exploits can be used against Microsoft Internet Information (IIS) Server? (Choose all that apply.)   1. IPP printer overflow attack 2. ISAPI DLL buffer overflow attack 3. Long URL attack 4. Proxy buffer overflow attack | [IPP printer overflow and ISAPI DLL buffer overflow attacks are types of buffer overflow attacks that can be used to exploit IIS Server.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N316) |
| **13.** | Where does the most valuable target information reside on a web server?   1. Web server home directory 2. Web application system files 3. Web application database 4. NTHOME directory | [The most valuable target data, such as passwords, credit card numbers, and personal information, reside in the database of a web application.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N341) |
| **14.** | Which of the following hacking tools performs directory-traversal attacks on IIS?   1. RPC DCOM 2. IIScrack.dll 3. WebInspect 4. IISExploit.exe | [IISExploit.exe is a tool used to perform automated directory-traversal attacks on IIS.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N366) |
| **15.** | Which program can be used to download entire websites?   1. WebSleuth 2. WSDigger 3. Wget 4. BlackWidow | [Wget is a command-line tool that can be used to download an entire website with all the source files.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N398) |
| **16.** | Web servers support which of the following authentication credentials? (Choose all that apply.)   1. Certificates 2. Tokens 3. Biometrics 4. Kerberos | [Certificates, tokens. and biometrics are all credentials that can authenticate users to web servers and web applications. Kerberos is a type of security system used to protect user authentication credentials.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N423) |
| **17.** | Which tool can be used to pull all email addresses from a website?   1. WebSleuth 2. WSDigger 3. Wget 4. BlackWidow | [WebSleuth can be used to index a website and specifically pull email addresses from all the pages of a website.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N448) |
| **18.** | What does SiteScope do?   1. Maps out connections in web applications 2. Views the HTML source for all web pages in a site 3. Gathers email address from websites 4. Tests exploits against web applications | [SiteScope maps out the connections within a web application and aids in the deconstruction of the program.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N473) |
| **19.** | What are the three primary types of attacks against IIS servers?   1. Directory traversal 2. Buffer overflows 3. Authentication attacks 4. Source disclosure attacks | [The three most common attacks against IIS are directory traversal, buffer overflows, and source disclosure.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N498) |
| **20.** | Which of the following is a common website attack that allows a hacker to deface a website? (Choose all that apply)   1. Using a DNS attack to redirect users to a different web server 2. Revealing an administrator password through a brute-force attack 3. Using a directory-traversal attack 4. Using a buffer overflow attack via a web form | [Using a DNS attack to redirect users to a different web server and revealing an administrator password through a brute-force attack are two methods of defacing a website.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=252422088&rowid=315&noteMenuToggle=0&leftMenuState=1#answer.N523) |

**Answers**

|  |  |
| --- | --- |
| **1.** | Digest and basic are the types of HTTP web authentication. |
| **2.** | Validating the field length and performing bounds checking are countermeasures for a buffer overflow attack. |
| **3.** | A token is a hardware device containing a screen that displays a discrete set of numbers used for login and authentication. |
| **4.** | Default installation is a common web server vulnerability. |
| **5.** | A hybrid attack substitutes numbers and special characters for letters. |
| **6.** | SSL is a countermeasure for authentication hijacking. |
| **7.** | A web server is always accessible, so a hacker can hack it more easily than less-available systems. |
| **8.** | Web applications are client/server programs that reside on a web server. |
| **9.** | A countermeasure to a directory-traversal attack is to enforce permissions to folders. |
| **10.** | Command injection involves a hacker entering programming commands into a web form in order to get the web server to execute the commands. |
| **11.** | To make an initial connection to the web server, use telnet to port 80. |
| **12.** | IPP printer overflow and ISAPI DLL buffer overflow attacks are types of buffer overflow attacks that can be used to exploit IIS Server. |
| **13.** | The most valuable target data, such as passwords, credit card numbers, and personal information, reside in the database of a web application. |
| **14.** | IISExploit.exe is a tool used to perform automated directory-traversal attacks on IIS. |
| **15.** | Wget is a command-line tool that can be used to download an entire website with all the source files. |
| **16.** | Certificates, tokens. and biometrics are all credentials that can authenticate users to web servers and web applications. Kerberos is a type of security system used to protect user authentication credentials. |
| **17.** | WebSleuth can be used to index a website and specifically pull email addresses from all the pages of a website. |
| **18.** | SiteScope maps out the connections within a web application and aids in the deconstruction of the program. |
| **19.** | The three most common attacks against IIS are directory traversal, buffer overflows, and source disclosure. |
| **20.** | Using a DNS attack to redirect users to a different web server and revealing an administrator password through a brute-force attack are two methods of defacing a website. |